ACTA ARITHMETICA
LXXIX.1 (1997)

The density of rational points on cubic surfaces

by

D. R. Heath-Brown (Oxford)

For Professor J. W. S. Cassels on his 75th birthday

1. Introduction. Let $F(W,X,Y,Z)\in\mathbb{Z}[W,X,Y,Z]$ be a cubic form, and define

$$N_F(P)=N(P)=\#\{\mathbf{x}\in\mathbb{Z}^4 : F(\mathbf{x})=0,\ |\mathbf{x}|\le P\},$$

where $|\mathbf{x}|$ is the Euclidean length of $\mathbf{x}$. This paper is concerned with the behaviour of $N(P)$ as P tends to infinity. It is clear that if the surface $F=0$ contains a rational line, then points on that line will contribute $cP^2+O(P)$ to $N(P)$ for an appropriate constant $c>0$. It appears that these contributions play the dominant rôle in determining the behaviour of $N(P)$, and we therefore define $N^{(0)}(P)$ to be the number of points $\mathbf{x}$ counted by $N(P)$, for which there is no rational line in the surface $F=0$ which contains $\mathbf{x}$. Of course it is quite possible that the surface $F=0$ contains no rational lines, in which case $N^{(0)}(P)=N(P)$. Alternatively it may happen that all points lie on rational lines. This will certainly be the case whenever F is degenerate, but also occurs in examples such as $F=WX^2-YZ^2$. Here a point (a,b,c,d) with $(b,d)\ne(0,0)$ lies on the line $b^2W=d^2Y$, $dX=bZ$, while if $b=d=0$, say, then the point is on the line $X=Z=0$. In general, however, we may regard $N^{(0)}(P)$ as counting "non-trivial" points on $F=0$. Thus, taking

$$F=W^3+X^3+Y^3+Z^3, \tag{1}$$

for example, we will be counting points which are not of the form $(a,-a,b,-b)$ or a permutation thereof. Manin has given some precise conjectures concerning the size of $N^{(0)}(P)$ (see Franke, Manin, and Tschinkel [2], for example) but we shall be concerned here with the following rather weaker assertion.

Conjecture. *For any fixed F and any $\varepsilon>0$, we have $N^{(0)}(P)\ll P^{1+\varepsilon}$.*

This has been established in only a few uninteresting cases, such as those above in which $N^{(0)}(P) = 0$, or those in which $F = 0$ has no non-zero solutions, or forms of the shape $W^3 - XYZ$, for example. Indeed, the estimate $N^{(0)}(P) \ll P^{2+\varepsilon}$ has yet to be proven in all cases.

We shall be concerned with approximations to the conjecture in which one allows an exponent somewhat larger than $1+\varepsilon$. The only form which has been extensively investigated is the diagonal one given by (1). Suppose that $N^{(0)}(P) \ll P^{\theta}$ for this form. Then there will be $O(x^{\theta/3})$ positive integers $n \le x$ with two or more distinct representations as a sum of two cubes of non-negative integers. Hooley [3] has shown, in effect, that $N^{(0)}(P) \ll P^{5/3+\varepsilon}$. His method employed a sieve argument, along with bounds for exponential sums derived from the work of Deligne. When one tries to generalize Hooley's method to other forms, it is apparent that one will require the surface $F = 0$ to have a rational plane containing 3 concurrent lines. The lines themselves need not be rational. It seems possible that Hooley's method could be generalized to cover all forms of this type. In the example (1) the plane $W + X = 0$ contains the lines given by

$$W + X = Y + \omega^j Z = 0, \qquad \omega = \exp(2\pi i/3), \qquad j = 1, 2, 3,$$

which are concurrent at $(1, -1, 0, 0)$.

An alternative proof of Hooley's result for the form (1) has recently been given by Wooley [4], using much more elementary techniques. As we shall see, Wooley's method generalizes to forms for which the surface contains 3 rational, non-concurrent, coplanar lines. For the form (1) these are given by

$$W + X = Y + Z = 0, \quad W + Y = X + Z = 0, \quad W + Z = X + Y = 0,$$

all of which lie in the plane $W + X + Y + Z = 0$. The primary goal of this paper is to improve on the exponent 5/3 of Hooley and Wooley, for the form (1). Our proof owes much to Wooley's ideas, and it is therefore natural to apply it to an arbitrary form for which the surface contains 3 rational coplanar lines. We hope that investigation of the more general situation will make clearer the rationale behind the initial transformation that we make to our form. Moreover, we believe that consideration of the general cubic surface, and rational lines in such a surface, helps to explain the disposal of various special cases that arise, as in Lemma 4 below, for example.

Our principal result is the following.

Theorem 1. *Let $F(W, X, Y, Z) \in \mathbb{Z}[W, X, Y, Z]$ be a non-singular cubic form such that the surface $F = 0$ contains 3 rational, coplanar lines. Then for any $\varepsilon > 0$ we have*

$$N^{(0)}(P) \ll P^{4/3+\varepsilon},$$

where the implied constant depends only on F and ε.

In the original version of this paper it was assumed that the 3 lines were non-concurrent, as will generally be the case. However, the referee kindly pointed out that, with little extra labour, one can handle the special case of concurrent lines. Indeed, it seems likely that the result might be further extended to cover singular surfaces, and hence in particular, the case of "coincident lines" (that is to say, the case in which F can be transformed into $WX^2 - ZQ(W,X,Y,Z)$, or even $W^3 - ZQ(W,X,Y,Z)$, by a rational linear change of variables). In spite of these remarks, we hope it will be apparent to the reader that the main value of Theorem 1 lies in the exponent obtained, rather than the class of surfaces to which the result applies.

As already remarked there will be the following trivial corollary when Theorem 1 is applied to the example (1).

Corollary. *Let $\varepsilon > 0$ be given. Then there are at most $O(x^{4/9+\varepsilon})$ positive integers up to x, with two or more distinct representations as a sum of two cubes of non-negative integers.*

It should be pointed out that Hooley [3] has also shown that the number of integers of the type considered in the corollary is at least of order $x^{1/3}\log x$. Thus for the form (1) one has

$$N^{(0)}(P) \gg P\log P.$$

We remark at the outset that it suffices for the proof of Theorem 1 to consider primitive integer vectors (W,X,Y,Z). That is to say, we shall assume that W,X,Y,Z have no common factor. Once Theorem 1 has been established for the counting function for such vectors the stated result easily follows. Moreover, it is clear that, for the purposes of the proof of the theorem, we may replace F by any form equivalent to it over the rationals. It follows that we may take the plane in which the 3 rational lines lie to be $Z = 0$. The lines may then be written in the shape $Z = L_i(W,X,Y) = 0$ for $i = 1,2,3$. Here L_i are non-zero rational linear forms, no two of which are proportional. Thus, if F is written as $C(W,X,Y) - ZQ(W,X,Y,Z)$, where C and Q are cubic and quadratic respectively, then each of the forms L_i must divide C. If the L_i are linearly independent they may be taken to be W, X and Y respectively, by a further change of variable. Alternatively, if they are linearly dependent, they can be taken to be W, X and $W + X$. After re-scaling both the variables and the form F appropriately we now conclude that F may be assumed to take either the form

$$F(W,X,Y,Z) = WXY - ZQ(W,X,Y,Z) \tag{2}$$

or

$$F(W,X,Y,Z) = WX(W+X) - ZQ(W,X,Y,Z). \tag{3}$$

Here Q is an appropriate integral quadratic form. Clearly it suffices to consider $N^{(0)}(P)$ for one of these new forms. For F given by (1), Wooley [4] arrives at forms of the first shape above by a strange "slicing argument" whereas in reality only a linear change of variables is required. To be completely explicit, one has

$$2^6 3^2(W^3+X^3+Y^3+Z^3) = W'X'Y' - Z'(3W'^2+3X'^2+3Y'^2+36Z'^2)$$

for the form (1), where

$$W' = 6(W+Z-X-Y), \quad X' = 6(X+Z-W-Y), \quad Y' = 6(Y+Z-W-X),$$
$$Z' = -(W+X+Y+Z).$$

We shall describe here the next stage of the argument. For forms of the type (2), $Z=0$ implies that one of W,X or Y is zero. We will therefore be on a rational line for any such solution. We may argue similarly for forms of the type (3). Since our goal is to count primitive solutions of $F=0$ with $|W|,|X|,|Y|,|Z| \le P$, we may therefore assume, with no loss of generality, that $1 \le Z \le P$. We shall show, in Section 4, that we may take $W = aU$, $Z = bU$ for appropriate coprime integer parameters a and b, with $b \ge 1$. Since (W,X,Y,Z) is assumed to be primitive, the vector (U,X,Y) will also be primitive. As $U \ne 0$ we then conclude that $q(U,X,Y)=0$, where q is an integral ternary quadratic form given by

$$q(U,X,Y) = q(U,X,Y;a,b) = 2aXY - 2bQ(aU,X,Y,bU) \tag{4}$$

in case (2), or

$$q(U,X,Y) = q(U,X,Y;a,b) = 2aX(aU+X) - 2bQ(aU,X,Y,bU) \tag{5}$$

in case (3). (Here the factor 2 ensures that the matrix for q has integer entries.) Our goal is therefore to bound the number of primitive solutions of $q(U,X,Y)=0$, for each pair (a,b). We see here the main distinction between our approach and Wooley's, for the latter considers zeros of a quadratic polynomial, which is essentially $q_0(X,Y) = q(U,X,Y;a,b)$, as U, a and b vary.

Our main tool in handling zeros of ternary quadratic forms is the following result.

Theorem 2. *Let q be an integral ternary quadratic form with matrix $\mathbf{M}$. Let $\Delta = |\det \mathbf{M}|$, and assume that $\Delta \ne 0$. Write Δ_0 for the highest common factor of the 2×2 minors of $\mathbf{M}$. Then the number of primitive integer solutions of $q(\mathbf{x})=0$ in the box $|x_i| \le R_i$ is*

$$\ll \left\{1 + \left(\frac{R_1R_2R_3\Delta_0^2}{\Delta}\right)^{1/2}\right\} d_3(\Delta).$$

It is easy to improve the exponent of Δ_0 to $3/2$. However, this is of no consequence, since one should think of Δ_0 as being bounded in the above result, as it will be in our application. It is unfortunate that Δ_0 should occur at all, but the result would be untrue without it, as one easily sees from consideration of forms of the type $q(\mathbf{x}) = k(x_1^2+x_2^2-x_3^2)$. Of course, for a fixed form q, one has an asymptotic formula $c_q P + o(P)$, for the number of primitive solutions in a sphere of radius P, with $c_q \ll \Delta^{-1}$ when $\Delta_0 \ll 1$. However, the dependence of the error term on q would be too complex to allow the deduction of a result of the type given by Theorem 2. With more work one ought to be able to improve the exponent $1/2$ to $1/3$, which would be best possible.

It is interesting to contrast Theorem 2 with the corresponding existence statement. The literature contains several such results. For example, Cassels [1] has shown that if q is an integral quadratic form in n variables, then if $q(\mathbf{x})$ has any non-trivial integral zero, it will have one with $|\mathbf{x}| \ll_n \|q\|^{(n-1)/2}$, where $\|q\|$ is the maximum modulus of the coefficients of q. We take q to be a diagonal ternary form, with coefficients coprime in pairs, and all having the same order of magnitude. Then there will be at least one primitive solution with $|\mathbf{x}| \ll \Delta^{1/3}$. In this case Theorem 2 shows that there are $O(\Delta^{\varepsilon})$ such solutions. Thus Theorem 2 is, in one sense, essentially best possible.

Theorem 2 is ineffective when Δ is small, and in this case we shall apply the following generalization of the result used by Wooley.

THEOREM 3. *Let q be a non-singular integral ternary quadratic form, with coefficients bounded in modulus by $\|q\|$, say. Suppose that the binary form $q(0, x_2, x_3)$ is also non-singular. Then for any integer k the equation $q(\mathbf{x}) = 0$ has only $O((\|q\|R)^{\varepsilon})$ primitive integer solutions in the cube $|x_i| \le R$, with $x_1 = k$.*

2. Quadratic forms. In this section we shall prove Theorems 2 and 3. We begin with two simple estimates for the number of zeros. The significance of these results is that the bounds are completely independent of the form involved. Indeed, there is no difficulty in establishing the estimates for forms of arbitrary degree.

LEMMA 1. *Let $f(\mathbf{x})$ be a non-zero binary form of degree d. Then $f(\mathbf{x}) = 0$ has at most $2d$ primitive integral solutions.*

This is trivial, since all solutions must be scalar multiples of at most d basic solutions.

LEMMA 2. *Let $f(\mathbf{x})$ be a ternary form of degree d, with no rational linear factor, and let positive numbers $X_1 \le X_2 \le X_3$ be given. Then there will be*

$$O_d(1 + (X_1X_2X_3)^{1/2})$$

primitive integral solutions of $f(\mathbf{x})$ in the box $|x_i| \le X_i$.

In the quadratic case one ought to be able to reduce the exponent to $1/3$ with more work. For the proof we begin by showing that any vector $\mathbf{x}$ in the above box lies on a plane $\sum_{i=1}^{3} a_i x_i = 0$, with integral coefficients $a_i \ll X_i^{-1}\sqrt{X_1X_2X_3}$ not all zero. This is a simple application of the pigeonhole principle. There are $\gg Y^3(X_1X_2X_3)^{-1}$ sets of coefficients with $|a_i| \le X_i^{-1}Y$, and the corresponding values of $\sum_{i=1}^{3} a_i x_i$ are all $\ll Y$, so that two such values must agree if $Y^2 \gg X_1X_2X_3$ with a sufficiently large implicit constant. Each of the planes above contains at most $2d$ primitive solutions of $f(\mathbf{x}) = 0$, by the previous lemma. Note that the corresponding binary form cannot vanish, since f has no rational linear factor. Moreover, the number of planes is

$$\ll \left(1 + \frac{\sqrt{X_1X_2X_3}}{X_1}\right)\left(1 + \frac{\sqrt{X_1X_2X_3}}{X_2}\right)\left(1 + \frac{\sqrt{X_1X_2X_3}}{X_3}\right) \ll \sqrt{X_1X_2X_3},$$

providing that $X_1X_2 \ge X_3$. However, if $X_1 < 1$ then the result follows from the previous lemma, since we will be considering primitive solutions of $f(0, x_2, x_3) = 0$. It remains to consider the case in which $X_1X_2 < X_3$ and $X_1 \ge 1$. Here each pair of values of x_1, x_2 produces at most d values of x_3, except when f takes the form

$$\sum_{j=0}^{d-1} x_3^j f_j(x_1, x_2)$$

and each of the forms $f_j(x_1, x_2)$ vanishes for the numbers x_1, x_2 in question. However, this can only happen when $x_1 = x_2 = 0$, since the original form f has no rational linear factor. This case therefore gives rise to at most two values of x_3 for which $\mathbf{x}$ is primitive. Thus when $X_1X_2 < X_3$ we may use the bound $O(X_1X_2)$ for the number of solutions of $q(\mathbf{x}) = 0$. The required result then follows here too, since X_1X_2 is now at most $\sqrt{X_1X_2X_3}$.

One can of course do better than Lemma 2 if one does not require uniformity in f. The following result is well known.

Lemma 3. *Let q be a non-singular integral ternary quadratic form. Then there are $O_q(P)$ primitive integer solutions of $q(\mathbf{x}) = 0$ lying in the cube $|x_i| \le P$.*

In the quadratic case we may regard Lemma 2 as a precursor to Theorem 2. To prove the latter, the key observation is that the equation $q(\mathbf{x}) = 0$ forces $\mathbf{x}$ to lie on a certain sublattice of $\mathbb{Z}^3$. Thus we shall begin by considering congruence conditions on $\mathbf{x}$. Let p be an odd prime and suppose that $p^e \,\|\, \Delta$ and $p^f \,\|\, \Delta_0$, so that $0 \le f \le e$. We may diagonalize the form q in the ring $\mathbb{Z}/p^e\mathbb{Z}$, using a unimodular matrix $\mathbf{P}$ say. The form $q(\mathbf{x})$ then becomes $Ay_1^2 + By_2^2 + Cy_3^2$, say, where $\mathbf{y} = \mathbf{P}\mathbf{x}$. Both Δ and Δ_0 are invariant under such a change of variables, so that we may assume that

$$p^{\alpha}\|A, \quad p^{\beta}\|B, \quad p^{\gamma}\|C,$$

with $\alpha \le \beta \le \gamma$ and $\alpha+\beta+\gamma=e$, $\alpha+\beta=f$. We now see that if $q(\mathbf{x})=0$ then $Ay_1^2+By_2^2 \equiv 0 \pmod{p^{\gamma}}$. When α and β have opposite parities this implies that

$$\nu_p(y_1) \ge \left[\frac{\gamma-\alpha+1}{2}\right], \qquad \nu_p(y_2) \ge \left[\frac{\gamma-\alpha}{2}\right] - \left[\frac{\beta-\alpha}{2}\right].$$

Here $\nu_p()$ is the p-adic valuation, as usual. It follows that $\mathbf{y}$ must lie on a sublattice of $\mathbb{Z}^3$ of index p^g, where

$$g = \left[\frac{\gamma-\alpha+1}{2}\right] + \left[\frac{\gamma-\alpha}{2}\right] - \left[\frac{\beta-\alpha}{2}\right] \ge \gamma-\beta.$$

This sublattice therefore has determinant at least $p^{\gamma-\beta}$.

The alternative case, in which α and β have the same parity, needs slightly more work. It is convenient to put $\beta-\alpha=2h$. Either $p^{\kappa} \mid y_1$, with

$$\kappa = \left[\frac{1+\gamma-\alpha}{2}\right],$$

or $p^k \,\|\, y_1$ for some k with $h \le k < \kappa$. In the former case $p^{\kappa'} \mid y_2$ with

$$\kappa' = \left[\frac{1+\gamma-\beta}{2}\right],$$

so that $\mathbf{y}$ lies on a sublattice of $\mathbb{Z}^3$ of index p^j, where $j=\kappa+\kappa' \ge \gamma-\beta$. In the other case we have $p^{k-h} \mid y_2$, and

$$\{(y_2p^{h-k})(y_1p^{-k})^{-1}\}^2 \equiv -(Ap^{-\alpha})(Bp^{-\beta})^{-1} \pmod{p^{\gamma-\alpha-2k}}.$$

Since the number on the right is coprime to p there will be at most 2 possible values for

$$(y_2p^{h-k})(y_1p^{-k})^{-1}$$

modulo $p^{\gamma-\alpha-2k}$. Taken together with the fact that $p^k \mid y_1$ and $p^{k-h} \mid y_2$, each of these values specifies a sublattice of $\mathbb{Z}^3$ of index $p^{\gamma-\alpha-h} \ge p^{\gamma-\beta}$, in which $\mathbf{y}$ must lie.

Now comparing the above results, we see that $\mathbf{y}$ must lie in one of at most $1+2(\kappa-h)$ integer lattices, each of determinant a power of p at least $p^{\gamma-\beta}$ in size. We note here that $1+2(\kappa-h) \le 2+\gamma-\beta \le d_3(p^{\gamma})$ for $\gamma>0$. Now, since $\mathbf{x}$ and $\mathbf{y}$ are related by a unimodular transformation modulo p^e, it follows that $\mathbf{x}$ is restricted similarly to one of at most $d_3(p^{\gamma})$ such lattices. Of course this statement is trivial when $\gamma=0$.

Finally, we must consider the situation when $p=2$. Here $4q$ can be diagonalized, as $Ay_1^2+By_2^2+Cy_3^2$, say, using an integer matrix of determinant

4. Then $ABC = 4\Delta$, and if

$$2^{\alpha} \,\|\, A, \quad 2^{\beta} \,\|\, B, \quad 2^{\gamma} \,\|\, C,$$

with $\alpha \le \beta \le \gamma$, then $\alpha + \beta + \gamma = e + 2$, where $2^e \,\|\, \Delta$, and $|\alpha + \beta - f| \le 4$, where $2^f \,\|\, \Delta_0$. Proceeding as before we find that $\mathbf{y}$ lies in one of at most $2d_3(2^{\gamma})$ integer lattices whose determinant is a power of 2, of size $2^{\gamma-\beta}$ or more. Thus $\mathbf{x}$ lies in a corresponding integer lattice whose determinant is a power of 2, at least $2^{\gamma-\beta-2}$.

We can now combine all these conditions, for the various prime divisors of Δ, using the Chinese Remainder Theorem. To do this we remark that $\gamma - \beta \ge e - 2f$ for each odd prime, and $\gamma - \beta - 2 \ge e - 2f - 8$ for $p = 2$. This shows that $\mathbf{x}$ must lie in one of at most $2d_3(\Delta)$ lattices Λ, of determinant at least $\Delta/(2^8\Delta_0^2)$.

We now rescale the variables by writing $\mathbf{x} = \mathbf{R}\mathbf{t}$, where $\mathbf{R}$ is the matrix $\mathrm{Diag}(R_1, R_2, R_3)$. Thus the region $|x_i| \le R_i$ becomes the cube $|t_i| \le 1$, and the lattice Λ becomes Λ' with determinant at least $\Delta(2^8\Delta_0^2 R_1R_2R_3)^{-1}$. We shall write

$$m_1 \le m_2 \le m_3$$

for the successive minima of Λ' with respect to the unit cube, so that

$$m_1m_2m_3 \gg \Delta(\Delta_0^2 R_1R_2R_3)^{-1}.$$

If $m_3 > 1$, then the lattice points will be restricted to the plane defined by the vectors giving the first and second successive minima. Correspondingly, the relevent solutions of $q(\mathbf{x}) = 0$ will be restricted to a plane, so that it suffices to consider zeros of a certain binary quadratic $q'(\mathbf{z})$, say. However, in this case Lemma 1 shows that there are at most 4 primitive solutions. Note that the form q' cannot vanish identically as q does not factorize. If $m_3 \le 1$, the lattice Λ' will have generators $\mathbf{t}_i$ for $i = 1, 2, 3$ such that $y_i \ll m_i^{-1}$ whenever $\mathbf{t} = y_1\mathbf{t}_1 + y_2\mathbf{t}_2 + y_3\mathbf{t}_3$ is in the unit cube. It follows that all primitive solutions of $q(\mathbf{x}) = 0$ in the box $|x_i| \le R_i$ correspond to primitive zeros of $\widetilde{q}(\mathbf{y}) = 0$ in the region $y_i \ll m_i^{-1}$. Here $\widetilde{q}$ is the non-singular integral quadratic form obtained from q by using the vectors $\mathbf{R}\mathbf{t}_i$ as a basis. Since

$$(m_1m_2m_3)^{-1/2} \ll \left\{\frac{\Delta_0^2 R_1R_2R_3}{\Delta}\right\}^{1/2},$$

the bound required for Theorem 2 is now an immediate consequence of Lemma 2.

We conclude this section by establishing Theorem 3. Since $q(0, x_2, x_3)$ is non-singular there is an invertible rational matrix $\mathbf{M}$, with first row $(1, 0, 0)$, such that $q(\mathbf{x}) = d(\mathbf{M}\mathbf{x})$, for some diagonal form d. Moreover, we can choose $\mathbf{M}$ so that the numerators and denominators of the entries are all $O(\|q\|^A)$

for some fixed exponent A. The equation $q(k,x_2,x_3)=0$ then becomes

$$\alpha L_1(k,x_2,x_3)^2+\beta L_2(k,x_2,x_3)^2=\gamma k^2,$$

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. We can clear the denominators of all the rational numbers involved to arrive at an equation of the same shape, with all the coefficients of order $\|q\|^A$, possibly with a new constant value of A. When $k\neq 0$, standard facts about representations by binary quadratic forms now show that L_1 and L_2 can take at most $O(\|q\|^{\varepsilon}R^{\varepsilon})$ values in the box $L_i\ll R\|q\|^A$. This yields a satisfactory bound for the number of pairs x_2, x_3. When $k=0$ the required result follows from Lemma 1. This completes the proof of Theorem 3.

3. Proof of Theorem 1—three special cases. The first special case to be considered arises from those pairs (a,b) for which the form q, given by (4) or (5), is singular. Here we shall prove the following.

LEMMA 4. *Suppose the ternary form $q(U,X,Y;a,b)$ is singular. Then either $q(U,X,Y)=0$ has only two primitive solutions (U,X,Y), or any such solution corresponds, via the substitutions $W=aU$, $Z=bU$, to a point on the surface $F(W,X,Y,Z)=0$ lying on a rational line.*

Since q is singular it will be of the shape $q'(L_1,L_2)$ for some integral binary form q'. Here L_1, L_2 are appropriate linearly independent rational linear forms in U, X and Y. There are three cases to consider. Firstly q' may have rank 2, and fail to factorize over the rationals. In this case $q(U,X,Y)=0$ implies $L_1=L_2=0$, so that (U,X,Y) must be a multiple of some non-zero vector $\mathbf{x}_0\in\mathbb{Q}^3$. Since we require (U,X,Y) to be primitive there are just two possible solutions. In the second case q' has rank 1 or 2 and factorizes over the rationals, giving

$$q(U,X,Y)=q'(L_1,L_2)=L_3L_4,$$

say, with non-zero rational linear forms L_3, L_4. Then $L_3(U,X,Y)=0$, say, implies $q(U,X,Y)=0$. Now b was taken to be strictly positive at the outset of our discussion. Thus

$$L_3(b^{-1}Z,X,Y)=0 \tag{6}$$

implies $q(U,X,Y)=0$ and hence $F(W,X,Y,Z)=0$. So for given values of a and b, we have $F(W,X,Y,Z)=0$ whenever $bW=aZ$ and (6) holds. This therefore produces a rational line in our surface, containing the solution in question. Finally, in the case in which q' vanishes identically, our solution would lie in a plane $bW=aZ$ contained in the surface $F=0$. This is impossible, since the original form F cannot factorize. This completes the proof of the lemma.

The second special case we shall consider is that in which Theorem 3 is inapplicable, that is to say that the form

$$q'(X,Y)=q(0,X,Y)=2aXY-2bQ(0,X,Y,0) \text{ or } 2aX^2-2bQ(0,X,Y,0)$$

is singular. We shall write Q_{ij} for the coefficients of the form Q. Thus the condition for q' to be singular is that $D(a,b)$, say, vanishes, where

$$D(a,b)=4b^2Q_{22}Q_{33}-(a-2bQ_{23})^2 \text{ or } 4b(bQ_{22}-a)Q_{33}-4b^2Q_{23}^2.$$

The first of these quadratic forms cannot vanish identically. If the second were to vanish identically we would have $Q_{33}=0$, in which case $(0,0,1,0)$ is a singular point for the form F as given by (3). Since this contradicts our original assumption we may conclude that $D(a,b)$ cannot vanish identically. Then Lemma 1 shows that q' can be singular for at most 4 coprime pairs a, b, with $a,b\ll_F 1$ in each case. For such pairs, either Lemma 4 will apply, or the form q is non-singular, in which case there are $O(P)$ primitive solutions (U,X,Y), by Lemma 3.

The final special case is that in which $a=0$. Here we must have $b=1$, since a and b are coprime. Now, as above, either Lemma 4 applies, or q is non-singular, so that Lemma 3 gives a bound $O(P)$ for the number of primitive solutions (U,X,Y).

4. Completion of the proof of Theorem 1. We begin this section by showing how the parameters a, b and U are determined. We write, temporarily, $L_1=W$, $L_2=X$, $L_3=Y$ in case (2), and $L_1=W$, $L_2=X$, $L_3=W+X$ in case (3). It then follows that Z must factorize as $Z=a_1a_2a_3$, where $a_i\mid L_i$ for $i=1,2,3$. We proceed to show that there is some index i for which

$$Z/a_i,\, L_i/a_i\ll P^{2/3}. \tag{7}$$

Suppose, for the sake of argument, that $a_1\ge a_2\ge a_3\ge 1$. Then

$$Z/a_1=a_2a_3\le (a_1a_2a_3)^{2/3}=Z^{2/3}\le P^{2/3}.$$

Thus if $|L_1|/a_1\le P^{2/3}$ we may take $i=1$. On the other hand, if $|L_1|/a_1\ge P^{2/3}$, then

$$a_1=L_1(L_1/a_1)^{-1}\ll P^{1/3},$$

since $L_i\ll P$ for each i. In this case we therefore have

$$Z/a_i\le Z/a_3=a_1a_2\le a_1^2\ll P^{2/3}$$

for every index i. However, since

$$\left(\frac{L_1}{a_1}\right)\left(\frac{L_2}{a_2}\right)\left(\frac{L_3}{a_3}\right)=\frac{L_1L_2L_3}{Z}=Q(W,X,Y,Z)\ll P^2,$$

there is always at least one value of i for which $L_i/a_i\ll P^{2/3}$. This completes the proof of (7).

For forms of the type (2) we may now rename the variables so that $L_i = W$, for the index i in (7). Similarly, for forms of the type (3), if $L_i = X$ we need merely interchange W and X, while if $L_i = W + X$ we substitute $W' = W + X$, $X' = -X$ to obtain a form of the same type, with $L_i = W'$. In view of (7) we may now set $W = aU$, $Z = bU$ with

$$a, b \ll P^{2/3}, \tag{8}$$

by writing $U = a_i$. We can assume that $(a, b) = 1$, by incorporating any common factor into U. This will not affect the bound (8). We note also that the vector (U, X, Y) will be primitive, since (W, X, Y, Z) is.

We proceed to count solutions of $q(U, X, Y) = 0$ for each pair a, b. In view of (8) we see that Lemma 4 contributes $O(P^{4/3})$ to $N^{(0)}(P)$, as does the first term in Theorem 2, since there will be $O(P^{4/3})$ possible pairs a, b. Moreover, cases in which $q(0, X, Y; a, b)$ is singular, or $a = 0$, will contribute only $O(P)$, as in Section 3. We therefore turn our attention to the remaining terms.

In order to apply Theorem 2 effectively we shall require the following lemma.

LEMMA 5. *For the quadratic form $q = q(U, X, Y; a, b)$ we have $\Delta_0 \ll_F 1$, providing that a and b are coprime.*

We write $\mathbf{M}$ for the matrix of q, and we proceed to consider the 2×2 minors of $\mathbf{M}$. The ij minor will be a certain integer form $M_{ij}(a, b)$, say. Elimination theory then shows that if $m(x, y)$ is the highest common factor of all the forms $M_{ij}(x, y)$ then there are positive integers K and d, depending only on F, such that Δ_0 divides both $Km(a, b)a^d$ and $Km(a, b)b^d$. Since a and b are coprime it follows that $\Delta_0 \mid Km(a, b)$. This establishes the lemma, providing that $m(x, y)$ is constant.

We therefore consider the possibility that each minor $M_{ij}(x, y)$ is divisible by some linear factor $\beta x - \alpha y$, where α and β are algebraic numbers, not both zero. In this case we see that all the 2×2 minors of $q(U, X, Y; \alpha, \beta)$ must vanish, so that the form will have rank at most 1. We can therefore write

$$q(U, X, Y; \alpha, \beta) = L(U, X, Y)^2,$$

for an appropriate linear form L, with algebraic coefficients. It follows that

$$2F(\alpha U, X, Y, \beta U) = Uq(U, X, Y; \alpha, \beta) = UL(U, X, Y)^2.$$

Then, if $\alpha \neq 0$ for example, we have

$$2F(W, X, Y, Z) = \alpha^{-1} W L(\alpha^{-1} W, X, Y)^2 + (Z - \alpha^{-1}\beta W) Q'(W, X, Y, Z)$$

identically, for a suitable quadratic form Q'. However, a form F of the above shape has a singularity where

$$L(\alpha^{-1}W, X, Y) = Z - \alpha^{-1}\beta W = Q'(W, X, Y, Z) = 0,$$

and this contradicts our original assumption. A precisely analogous argument applies when $\beta \neq 0$.

We may therefore conclude that the minors $M_{ij}(x, y)$ can have no common algebraic factor, and the lemma follows.

In order to apply Theorem 2 we shall also need to know how $\varDelta$ varies, for the form q. It is easy to see that $\varDelta = |G(a, b)|$ for an appropriate integral form G of degree 5. We now employ the following lemma.

Lemma 6. *Let G be a non-zero form of degree n and let $G_0 \geq 1$. Suppose further that $A, B \geq 1$ are given. Then one of the following two cases holds.*

(i) $|G(a, b)| \gg \min(A, B)^n$ *for all pairs of integers (a, b) with $A \leq |a| \leq 2A$ and $B \leq |b| \leq 2B$.*

(ii) $A \ll B \ll A$ *and the number of pairs of integers a, b for which*

$$A \leq |a| \leq 2A, \qquad B \leq |b| \leq 2B$$

and $|G(a, b)| \leq G_0$, is $O(G_0^{1/n}A)$.

For the proof we begin by observing that if A and B are not of the same order of magnitude, with A, say, being the larger, then the size of G will be determined by the term in $G(a, b)$ in which the exponent of a is maximal. Thus $|G(a, b)| \gg A^k B^{n-k} \gg B^n$, for some k. This gives us case (i). In the alternative case we can factorize G, and some factor $\mu a - \nu b$ must be of order $G_0^{1/n}$. Here at least one of μ and ν is non-zero, μ, say. Then for each of $O(A)$ values of b there will correspond $O(G_0^{1/n})$ possible values of a, and the result follows in case (ii).

We are now ready to start counting solutions of $q(U, X, Y) = 0$, with q given by (4) or (5), as described earlier. Here we shall use Theorem 2, in which we have already dealt with the first term. To account for the second term we observe that the corresponding values of R_i are $P/\max(|a|, b), P$ and P. Thus it remains to account for a contribution

$$\ll P^{3/2+\varepsilon}\{\varDelta \max(|a|, b)\}^{-1/2} \tag{9}$$

for each pair a, b. We divide the ranges for

$$\min(|a|, b), \quad \max(|a|, b) \quad \text{and} \quad \varDelta$$

into intervals $(T_1, 2T_1]$, $(T_2, 2T_2]$ and $(T_3, 2T_3]$ respectively, so that (9) can be estimated as $O(P^{3/2+\varepsilon}(T_2T_3)^{-1/2})$. Note that, by (8), we have $1 \ll T_1, T_2 \ll P^{2/3}$.

We may derive an alternative estimate by applying Theorem 3 to each individual value of U. Here we note that

$$U = W/a = Z/b \ll P/T_2,$$

leading to a contribution $O(P^{1+\varepsilon}T_2^{-1})$.

We begin by examining the situation in which T_1 and T_2 have different orders of magnitude, corresponding to case (i) of Lemma 6. The lemma then yields $T_3 \gg T_1^5$, so that our two alternative bounds are

$$O(P^{3/2+\varepsilon}(T_1^5T_2)^{-1/2}) \quad \text{and} \quad O(P^{1+\varepsilon}T_2^{-1}).$$

It follows that we may estimate the contribution in this case as

$$\ll \{P^{3/2+\varepsilon}(T_1^5T_2)^{-1/2}\}^{2/5}\{P^{1+\varepsilon}T_2^{-1}\}^{3/5} = P^{6/5+\varepsilon}T_1^{-1}T_2^{-4/5}$$

for each pair a, b. Since there are $O(T_1T_2)$ such pairs this gives a total

$$\ll P^{6/5+\varepsilon}T_2^{1/5} \ll P^{4/3+\varepsilon},$$

which is satisfactory.

We now turn to the situation in which T_1 and T_2 have the same order of magnitude, corresponding to case (ii) of Lemma 6. This time our two alternative estimates become

$$O(P^{3/2+\varepsilon}(T_2T_3)^{-1/2}) \quad \text{and} \quad O(P^{1+\varepsilon}T_2^{-1}).$$

This leads to a contribution

$$\ll \{P^{3/2+\varepsilon}T_2^{-1/2}T_3^{-1/2}\}^{2/5}\{P^{1+\varepsilon}T_2^{-1}\}^{3/5} = P^{6/5+\varepsilon}T_2^{-4/5}T_3^{-1/5}$$

for each pair a, b. This time case (ii) of Lemma 6 shows that there are $O(T_2T_3^{1/5})$ possible pairs, giving a total

$$\ll P^{6/5+\varepsilon}T_2^{1/5} \ll P^{4/3+\varepsilon},$$

again. This completes the proof of Theorem 1, on summing over the appropriate values of T_1, T_2 and T_3.

Acknowledgements. This paper was written while the author was visiting the Mathematics Department of Oklahoma State University, and the Centre for Number Theory Research, at Macquarie University. Their hospitality and financial support are gratefully acknowledged.

References

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

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

[3] C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. Reine Angew. Math. 314 (1980), 146–173.

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

Magdalen College
Oxford OX1 4AU, England

Received on 30.8.1995
and in revised form on 11.6.1996 (2852)