The Density of Rational Points on Curves and Surfaces

D.R. Heath-Brown
Mathematical Institute, Oxford

1 Introduction

Let $n \geq 3$ be an integer and let $F(\mathbf{x}) = F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an absolutely irreducible form of degree d, producing a hypersurface of dimension $n-2$ in $\mathbb{P}^{n-1}$. This paper is primarily concerned with the number of rational points on this hypersurface, of height at most B, say. In order to describe such points we choose representatives $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ with the x_i not all 0, and such that $\gcd(x_1, \ldots, x_n) = 1$. Moreover we shall insist that if i is the smallest index for which $x_i \neq 0$, then $x_i > 0$. We shall define Z_n to be the set of all such representatives $\mathbf{x}$. Our primary interest is then with the quantity

$$N(B) = N(F; B) = \#\{\mathbf{x} \in Z_n : F(\mathbf{x}) = 0, \max_{1 \leq i \leq n} |x_i| \leq B\}.$$

We begin with a rather trivial result.

Theorem 1 *For any $n \geq 2$ we have*

$$N(F; B) \ll B^{n-1}. \tag{1.1}$$

This remains true if F is allowed to have coefficients in $\overline{\mathbb{Q}}$.

Here, and throughout the paper, the implied constant may depend on n and d. However where there is a dependence on F we shall say so explicitly. The result shows in particular that there is an integer vector $\mathbf{x}$ with $F(\mathbf{x}) \neq 0$ satisfying $|\mathbf{x}| \ll_{n,d} 1$, and this is a fact that we shall use repeatedly. We do not claim that Theorem 1 is new.

It is trivial that the exponent $n-1$ above is best possible, in the case $d = 1$. However for $d = 2$ we have

$$N(B) \ll_{F,\varepsilon} B^{n-2+\varepsilon}, \tag{1.2}$$

for any $\varepsilon > 0$. This can be proved by the circle method, for example. Our next result is a version of this which is independent of F.

Theorem 2 *Let $F(\mathbf{x})$ be a quadratic form of rank at least 3, in n variables. Then*

$$N(B) \ll_{\varepsilon} B^{n-2+\varepsilon},$$

for any fixed $\varepsilon > 0$.

As with Theorem 1, this estimate is almost trivial. Again we do not claim that the result is new.

We will be interested in the extent to which one can prove results of this kind when $d \geq 3$. Let us first consider the case $n = 3$, corresponding to curves in $\mathbb{P}^2$. When $d \geq 3$ and the curve has genus 1, we have Néron's result

$$N(B) \sim c_F (\log B)^{r/2} \ll_{F,\varepsilon} B^{\varepsilon}, \tag{1.3}$$

for any $\varepsilon > 0$, where c_F is a positive constant depending on F, and r is the rank of the Jacobian of the curve. For genus 2 or more we even have

$$N(B) \ll_F 1, \tag{1.4}$$

by the celebrated theorem of Faltings [8]. Unfortunately it is hard to produce versions of these results with a good explicit dependence on F. None the less it has been shown by Pila [27], via quite different methods, that

$$N(B) \ll_{\varepsilon} B^{1+1/d+\varepsilon}, \tag{1.5}$$

for $n = 3$ and any $\varepsilon > 0$. Indeed Pila shows in general that

$$N(B) \ll_{\varepsilon} B^{n-2+1/d+\varepsilon}. \tag{1.6}$$

It is remarkable that these results are completely independent of F. Pila's estimates are deduced from a bound relating to integral points on affine curves due to Bombieri and Pila [2]. (See also Pila [28].) Bombieri and Pila showed that if $f(x, y) \in \mathbb{Z}[x, y]$ is an absolutely irreducible polynomial of degree d, then

$$\#\{(x, y) \in \mathbb{Z}^2 : f(x, y) = 0, |x|, |y| \leq B\} \ll_{\varepsilon} B^{1/d+\varepsilon}. \tag{1.7}$$

Our principal strategy in this paper will be to generalize this latter result. In particular we shall consider a projective version of it, and we shall replace the cube of side $2B$ by a more general box. This will prove very convenient for applications. We therefore take $\mathbf{B} = (B_1, \dots, B_n)$ with each $B_i \geq 1$, and define a counting function

$$N(\mathbf{B}) = N(F; \mathbf{B}) = \#\{\mathbf{x} \in Z_n : F(\mathbf{x}) = 0, |x_i| \leq B_i, (1 \leq i \leq 1)\}.$$

It will be convenient to write

$$V = \prod_{i=1}^{n} B_i$$

and

$$T = \max\{\prod_{i=1}^{n} B_i^{f_i}\},$$

with the maximum taken over all integer n-tuples $(f_1, \dots, f_n)$ for which the corresponding monomial

$$x_1^{f_1} \dots x_n^{f_n}$$

occurs in $F(\mathbf{x})$ with non-zero coefficient. When $d \geq n \geq 3$ and F is non-singular, we may bound T from below as follows. We order the variables X_i so that $B_1 \geq B_2 \geq \ldots \geq B_n$, and observe that some monomial $x_1^{d-1}x_i$ must occur in $F(\mathbf{x})$, where $1 \leq i \leq n$. Thus $T \geq B_1^{d-1}B_n \geq V^{d/n}$. Indeed, for a non-singular ternary quadratic form, the same estimate $T \geq V^{2/3}$ still holds. To see this, observe as above that $T \geq B_1B_2 \geq V^{2/3}$ if there is a term in x_1^2 or x_1x_2. If neither of these is present there must be terms in both x_1x_3 and x_2^2, since F is non-singular. In this case we have $T \geq \max(B_1B_3, B_2^2) \geq V^{2/3}$.

Our principal result for curves is the following.

Theorem 3 *Let $n = 3$ and $\varepsilon > 0$. If F is irreducible over $\mathbb{Q}$, then*

$$N(F; B_1, B_2, B_3) \ll_\varepsilon T^{-d^{-2}}V^{d^{-1}+\varepsilon}. \tag{1.8}$$

In particular we have

$$N(F; B) \ll_\varepsilon B^{2/d+\varepsilon}. \tag{1.9}$$

Moreover if F is non-singular we have

$$N(F; B_1, B_2, B_3) \ll_\varepsilon V^{2/(3d)+\varepsilon}. \tag{1.10}$$

As with the result of Bombieri and Pila, we have estimates that are completely independent of F. In fact this arises through an application of the following result, in which we write $||F||$ for the height of the form F, defined as the maximum modulus of the coefficients of F.

Theorem 4 *Let $F(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ be a form in $n = 3$ variables, of degree d. Suppose that F is irreducible over $\mathbb{Q}$, and that the coefficients of F are coprime. Then either $N(F; B) \leq d^2$ or $||F|| \ll B^{d(d+1)(d+2)/2}$.*

This enables us to absorb a dependence of the type $||F||^\varepsilon$ in the estimate, into the term V^ε (or B^ε). A similar technique can be applied to higher dimensional varieties, see §§5,6& 8.

One should note that the exponent in (1.9) is appreciably smaller than that in (1.5). Moreover, if we take $B_1 = B_2 = B$ and $B_3 = 1$ in (1.8) we recover the exponent $1/d$ of (1.7). We may also observe that if $F(x_1, x_2, x_3) = x_1^d - x_2^{d-1}x_3$, then the solutions $(m^{d-1}n, m^d, n^d)$ show that

$$N(F; B) \gg B^{2/d},$$

so that (1.9) is, in a suitable sense, best possible. Finally it should be pointed out that we do not require F to be absolutely irreducible for Theorem 3. Indeed for forms which are irreducible over $\mathbb{Q}$ but reducible over $\overline{\mathbb{Q}}$ a stronger estimate is a consequence of the following result.

Corollary 1 *Theorem 3 holds for any $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, x_2, x_3]$ which is irreducible over $\overline{\mathbb{Q}}$ and of degree d. Indeed if F is not a multiple of a rational form then $N(F; B) \leq d^2$.*

The first statement clearly follows from the second. To prove the latter one merely writes F as a linear combination $\sum \lambda_i F_i$ of rational forms F_i, with linearly independent λ_i. Some F_i is not a multiple of F, but all rational zeros of F must satisfy $F = F_i = 0$. The result then follows by Bézout's Theorem.

At this point we remark that we shall use the term 'absolutely irreducible' to describe a polynomial, or an equation, which is irreducible over $\overline{Q}$. When we only say 'irreducible', the relevant field must be understood from the context. When the relevant field is $\overline{Q}$ we shall use the two terms interchangeably. However, in the context of curves and higher dimensional varieties, we shall use the phrase 'irreducible' to mean irreducible over $\overline{Q}$.

When the B_i are unequal, Theorem 3 is new even in the case $d = 2$. In the author's work [13; page 24], the estimate

$$N(F; B_1, B_2, B_3) \ll_\varepsilon V^{1/2},$$

given by [13; Lemma 2] was employed. By substituting the bound (1.8) we can strengthen [13; Theorem 2] as follows

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

$$\ll_\varepsilon \{1 + (\frac{R_1 R_2 R_3 \Delta_0^2}{\Delta})^{1/3+\varepsilon}\} d_3(\Delta)$$

for any $\varepsilon > 0$.

In the original version the exponent $1/3 + \varepsilon$ was replaced by $1/2$. We may of course replace $d_3(\Delta)$ by $(R_1 R_2 R_3)^\varepsilon$ if we wish, by virtue of Theorem 4.

One can also estimate the number of points on a curve in $\mathbb{P}^3$.

Theorem 5 *Let C be an irreducible curve in $\mathbb{P}^3$, of degree d, not necessarily defined over the rationals. Then C has $O_\varepsilon(B^{2/d+\varepsilon})$ points $\mathbf{x} \in Z_4$ in the cube $\max |x_i| \leq B$.*

This will be established by projecting C onto a suitable plane, and counting the points on the resulting plane curve. If C is non-planar one would expect to loose information by such a process. However in our applications of Theorem 5 we are usually unable to tell whether or not C is planar.

It is interesting to compare the estimates given by Theorems 3 and 5 with those obtained very recently by Elkies [6]. Elkies' emphasis is on algorithms for finding rational points. Thus he shows in [6; Theorem 3] that one can find the rational points of height at most B, on a curve C of degree d, in time $O_{C,\varepsilon}(B^{2/d+\varepsilon})$. It follows in particular that there are $O_{C,\varepsilon}(B^{2/d+\varepsilon})$ points to be found. Elkies does not consider issues of uniformity with respect to the curve, although it seems quite plausible that his methods will yield a good dependence on the height of C, or even complete independence as in the present work.

At first sight the approach taken in the two papers is rather different, but closer inspection reveals interesting parallels. Indeed Elkies goes on to examine the situation for varieties of higher dimension, presenting a heuristic argument that produces the same exponents $3/\sqrt{d}$ and $(n-1)d^{-1/(n-2)}$ which arise from Theorem 14 below.

We now discuss the case $n = 4$, corresponding to surfaces in $\mathbb{P}^3$. The example $F(\mathbf{x}) = x_1^d + x_2^d - x_3^d - x_4^d$, for which all vectors (a, b, a, b) are solutions, shows that we may have $N(B) \gg B^2$ even when F is non-singular. It is thus natural to exclude trivial solutions by defining $N_1(B)$ to count the same rational points as does $N(B)$, but excluding any that lie on lines in the surface $F(\mathbf{x}) = 0$. We may then conjecture that

$$N_1(B) \ll_{F,\varepsilon} B^{1+\varepsilon} \tag{1.11}$$

for any $\varepsilon > 0$, as soon as $d \geq 3$. In so far as the weaker bound (1.2) has not hitherto been established for general forms, even in the cubic case, the above conjecture is a long way off. We may observe that if $d \geq 3$, the surface

$$x_1^d + x_2^d - x_2^{d-2} x_3 x_4 = 0$$

is absolutely irreducible, and contains no lines other than those in the planes $x_2 = 0$, $x_3 = 0$ and $x_4 = 0$. However there are rational points $(0, ab, a^2, b^2)$, which show that $N_1(B) \gg B$ in this case. Thus the exponent 1 in (1.11) would be best possible.

We shall make some modest progress towards the above conjecture by establishing the following result.

Theorem 6 *For any absolutely irreducible form $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, \dots, x_4]$ of degree 3 or more, we have*

$$N_1(F; B) \ll_\varepsilon B^{52/27+\varepsilon}.$$

An inspection of the proof shows that the exponent $52/27$ may be replaced by $17/9$ when F has degree 4 or more. However we can improve substantially on this for large values of d, as follows.

Theorem 7 *For any absolutely irreducible form $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, \dots, x_4]$ of degree d, we have*

$$N_1(F; B) \ll_\varepsilon B^{1+3/\sqrt{d}+\varepsilon}.$$

Theorem 6 answers questions raised by the author [14], by showing that points on any lines in the surface $F = 0$ that are defined over $\mathbb{Q}$ will dominate $N(B)$. Surfaces of the type $G(x_1, x_2) = G(x_3, x_4)$, where G is a binary form, have been investigated fairly extensively. Thus Hooley [16], [22] has shown, in effect, that $N_1(B) = o(B^2)$ when G is a cubic form, and also [19] when G is a quartic form of the special type $G = ax^4 + bx^2y^2 + cy^4$. For binary forms of degree $d \geq 5$, the most general case that has been covered is that of forms of the type $G = Ax^d + By^d$, which have been handled by Bennet, Dummigan and Wooley [1]. There has however been much work on the forms $G = x^d + y^d$, to which we shall allude later. The sieve methods used by Hooley [16], [22] save a

power of $\log B$ relative to B^2, whereas the other techniques used hitherto, which trace their origins to Hooley's work [17] on sums of 4 cubes, save a power of B.

As a consequence of Theorem 6, we can show, in the spirit of the above works, that most numbers represented by a binary form G have essentially only one representation. To make this precise, we shall say that an invertible 2×2 matrix M is an automorphism of the binary form G if $G(M\mathbf{x}) = G(\mathbf{x})$ identically in $\mathbf{x}$. We then regard integral solutions of $G(\mathbf{x}) = n$ as equivalent if and only if they are related by such an automorphism with a rational matrix M.

Theorem 8 *Let $G(x, y) \in \mathbb{Z}[x, y]$ be a binary form of degree d, with no factor of multiplicity $d/2$ or more. Then the number of automorphisms of G is finite, and bounded solely in terms of d. Moreover the number of positive integers $n \leq X$ represented by the form G is of exact order $X^{2/d}$, providing that $G(1, 0) > 0$. Of these integers n there are $O_{\varepsilon,G}(X^{52/(1+26d)+\varepsilon})$ for which there are two or more inequivalent integral representations.*

We remark that Roth's Theorem is used in the proof, so that the implied constant is ineffective. It seems likely, however, that this can be avoided.

The statement that the number of representable integers is of exact order $X^{2/d}$ is not new, and is only included for comparison with the size of the exceptional set. Indeed, for irreducible forms G, the lower bound is a classical result of Erdős and Mahler [7], dating from 1938. In fact Theorem 8 should enable one to deduce an asymptotic formula for the number of representable integers up to X, such integers being counted once only, irrespective of the number of representations.

For a form $G(x, y) = x^e g(x, y)$ with $e > d/2$ one can obtain $cX^{1/(d-e)}$ representable integers merely by choosing $x = 1$. This is the reason that such forms G are excluded in the theorem. We note also that if G is a power of a quadratic form, another excluded case, then there may be infinitely many automorphisms, and almost all integers represented by G will have at least two inequivalent representations.

In formulating Theorem 8 we have chosen to consider as wide a class of forms G as possible. However for the most interesting case, in which G has no repeated factors, one can give an appreciably stronger bound, with exponent

$$\frac{12d}{9d^2 - 6d + 16} + \varepsilon,$$

for the size of the exceptional set. This may be achieved by using Theorem 10 in place of Theorem 6, and taking $e = 1$ in the treatment of $S(X, C)$ in §7. This remark is due to Professor Hooley.

In fact Theorem 6 does not directly entail the estimate (1.2), since the surface $F = 0$ may contain infinitely many lines. However we may indeed establish the following result.

Theorem 9 *For any absolutely irreducible form $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, \ldots, x_4]$ of degree $d \geq 2$, we have*

$$N(F; B) \ll_\varepsilon B^{2+\varepsilon}.$$

In higher dimensions the validity of (1.2) remains open. We stress this by stating formally the following conjectures.

Conjecture 1 *For $d \geq 3$ and $n \geq 5$ we have*

$$N(F;B) \ll_{\varepsilon,F} B^{n-2+\varepsilon}.$$

Conjecture 2 *For given $d \geq 3$ and $n \geq 5$ we have*

$$N(F;B) \ll_{\varepsilon} B^{n-2+\varepsilon}$$

uniformly in F.

We can do considerably better than Theorem 6 if we insist that F is non-singular. In this case we have the following.

Theorem 10 *For any non-singular form $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, \ldots, x_4]$ of degree d, we have*

$$N_1(F;B) \ll_{\varepsilon} B^{4/3+16/9d+\varepsilon}. \tag{1.12}$$

For large d a further improvement is possible.

Theorem 11 *For any non-singular form $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, \ldots, x_4]$ of degree d, we have*

$$N_1(F;B) \ll_{\varepsilon} B^{1+\varepsilon} + B^{3/\sqrt{d}+2/(d-1)+\varepsilon}. \tag{1.13}$$

In particular

$$N_1(F;B) \ll_{\varepsilon} B^{1+\varepsilon}, \tag{1.14}$$

providing that $d \geq 13$. Let $N_2(F;B)$ denote the number of points counted by $N(F;B)$, but not contained in any curve of degree $\leq d-2$ contained in the surface. Then

$$N_2(F;B) \ll_{\varepsilon} B^{3/\sqrt{d}+2/(d-1)+\varepsilon}. \tag{1.15}$$

Let $N_3(F;B)$ denote the number of points counted by $N(F;B)$, but not contained in any genus zero curve of degree $\leq d-2$ contained in the surface. Then

$$N_3(F;B) \ll_{\varepsilon,F} B^{3/\sqrt{d}+2/(d-1)+\varepsilon}. \tag{1.16}$$

Thus (1.14) shows that (1.11) holds for $d \geq 13$, when F is non-singular.

The significance of curves of degree at most $d-2$ lying in the surface, is due to the following crucial result, due to Colliot-Thélène, and proved in the appendix.

Theorem 12 *Let S be a non-singular surface in $\mathbb{P}^3$, of degree d. Then for each degree $\delta \leq d-2$ there is a constant $N(\delta, d)$, independent of S, such that the surface S contains at most $N(\delta, d)$ irreducible curves of degree δ.*

In the case $d = 3$ we have the familiar fact that a non-singular cubic surface has 27 lines. We can therefore take $N(1, 3) = 27$.

Since Theorem 12 shows that there are $O_d(1)$ curves of degree $\leq d - 2$ in the surface, the estimate (1.16) may be interpreted as saying that, apart from a very small number of exceptions, all points lie on a finite number of curves of genus zero in the surface.

We remark that (1.13) improves on (1.12) as soon as $d \geq 6$, so that it is only the cases $d = 3, 4$ and 5 of Theorem 10 which are of real interest. It is possible to improve the exponent $3/\sqrt{d}+2/(d-1)$ slightly, but we shall not go into this.

There has been much work done for the special surfaces

$$F(\mathbf{x}) = x_1^d + x_2^d - x_3^d - x_4^d = 0.$$

In particular it has been shown that for these forms F we have

$$N_1(B) \ll B^{4/3+\varepsilon} \quad (d = 3)$$

due to Heath-Brown [13],

$$N(B)_1 \ll B^{5/3+\varepsilon} \quad (4 \leq d \leq 7) \tag{1.17}$$

due to Hooley [18] and [20], and

$$N(B)_1 \ll B^{3/2+1/(d-1)+\varepsilon} \quad (d \geq 8)$$

due to Skinner and Wooley [30]. These are superseded by Theorem 11 for $d \geq 6$. Indeed Browning, in work to appear, has shown that (1.13) may be replaced by

$$N_1(F; B) \ll_\varepsilon B^{2/3+\varepsilon} + B^{3/\sqrt{d}+2/(d-1)+\varepsilon}$$

for these particular surfaces.

For general diagonal cubic surfaces Hooley [23] showed that $N_1(B) \ll_{F,ep} B^2(\log B)^{-1/3}$, thereby demonstrating that points on rational lines would dominate $N(B)$. Moreover, also for diagonal cubic surfaces, the author [15] gave a conditional treatment of the bound $N_1(B) \ll_{F,ep} B^{3/2+\varepsilon}$. This is superior to Theorem 10, but assumes the Riemann Hypothesis for the L-functions of elliptic curves.

We can apply our results to integral points on affine surfaces. We shall focus attention on the surface $x_1^d + x_2^d + x_3^d = N$, and in view of the arithmetical significance of this we will consider only solutions with $x_i > 0$. Let $r(N)$ be the number of solutions to this equation. Then if $d \geq 2$ we have $r(N) \ll_{d,\varepsilon} N^{1/d+\varepsilon}$. No improvement in the exponent $1/d$ has hitherto been given, for any value of d. The bound is of course best possible for $d = 2$, and for $d = 3$ it was shown by Mahler [26] that $r(N) = \Omega(N^{1/12})$. However it may be conjectured that $r(N) \ll_{d,\varepsilon} N^\varepsilon$ as soon as $d \geq 4$. The mean value of $r(N)$ is also of importance. Hua's inequality [24] shows that

$$\sum_{n \leq B^d} r(n)^2 \ll_{d,\varepsilon} B^{7/2+\varepsilon}$$

when $d \geq 3$. Again, no improvement on the exponent $7/2$ has been given hitherto, although the author [15] and Hooley [21] have shown independently that the exponent may be reduced to $3 + \varepsilon$ in the case $d = 3$, under certain standard hypotheses concerning the Hasse-Weil L-functions of cubic 3-folds.

We shall prove the following result.

Theorem 13 *For $N \leq B^d$ we have*

$$r(N) \ll_\varepsilon B^{\theta+\varepsilon}$$

where

$$\theta = \frac{2}{\sqrt{d}} + \frac{2}{d-1}.$$

It follows that

$$\sum_{n \leq B^d} r(n)^2 \ll_\varepsilon B^{3+\theta+\varepsilon}.$$

We note that $\theta < 1$ for $d \geq 8$ and $\theta < 1/2$ for $d \geq 24$. The exponent θ may be reduced slightly with further work.

Turning to hypersurfaces of higher dimension, we have the following result.

Theorem 14 *Let $\varepsilon > 0$, and suppose that $B_1, \ldots, B_n \geq 1$ and a form F, irreducible over $\mathbb{Q}$, are given. Then there exists D depending only on n, d and ε, and an integer k satisfying*

$$k \ll_\varepsilon (V^d/T)^{d^{-(n-1)/(n-2)}} V^\varepsilon (\log ||F||)^{2n-3},$$

with the following properties. For each $j \leq k$ there is an integral form $F_j(\mathbf{x})$, in n variables, having degree at most D, such that

1. *$F(\mathbf{x}) \nmid F_j(\mathbf{x})$ for $1 \leq j \leq k$,*
2. *For every point $\mathbf{x}$ counted by $N(\mathbf{B})$ there is an integer $j \leq k$ such that $F_j(\mathbf{x}) = 0$.*

Thus in particular, every point of height at most B lies in one of at most $O_{\varepsilon,F}(B^{(n-1)d^{-1/(n-2)}+\varepsilon})$ proper subvarieties $F(\mathbf{x}) = F_j(\mathbf{x}) = 0$. The reader should note however that such a result is trivial without a bound on the degree of the forms F_j. Indeed one may construct a form F_1 (with degree dependent on B) such that $F_1(\mathbf{x}) = 0$ for every integral vector $\mathbf{x}$ in the cube $\max |x_i| \leq B$.

Theorem 14 is in fact the fundamental result in this paper. In the case $n = 3$, each point counted by $N(F; \mathbf{B})$ lies on one of the intersections $F(\mathbf{x}) = F_j(\mathbf{x}) = 0$. By Bézout's Theorem, each intersection contains at most dD points, whence

$$N(F; \mathbf{B}) \ll_\varepsilon (V^d/T)^{d^{-2}} V^\varepsilon (\log ||F||)^3.$$

The dependence on $||F||$ can be eliminated by an appeal to Theorem 4, so that Theorem 3 follows.

The exponents involving $1/\sqrt{d}$ appearing in our various results all arise from the case $n = 4$ of Theorem 14. It would be remarkable if such an exponent were optimal. We therefore pose the following question.

Question *Is the exponent $d^{-(n-1)/(n-2)}$, which appears in Theorem 14, best possible for values $n \geq 4$?*

This would seem to be the single most important issue in relation to possible sharpenings of our results.

Theorem 14 clearly opens up the prospect of results on $N(F; \mathbf{B})$ for $n \geq 5$. We intend to return to this in a future paper.

This introduction would not be complete without reference to other approaches to problems of this nature. In particular, although the methods developed in this paper lead in a great many cases to results superior to those obtained hitherto, this is by no means universally so. The result (1.17) of Hooley is a good case in point. Hooley uses a sieve method, which can be thought of as counting integer vectors $\mathbf{x}$ for which a polynomial equation $f(X, \mathbf{x}) = 0$ has an integral solution X. In this approach the overall number of solutions will, in essence, depend on the size of $\mathbf{x}$ alone. In contrast, the techniques of the present paper produce a bound which involves the sizes both of X and $\mathbf{x}$. Thus the sieve method has potential advantages in situations in which X is large compared to $\mathbf{x}$. A slightly different sieve approach, originating in work of Cohen [3], and described by the author [10; Appendix 2], has the advantage of applying to arbitrary algebraic hypersurfaces, but produces only $N(F; B) \ll_{\varepsilon, F} B^{n-3/2+\varepsilon}$. This is inferior to the result (1.6) of Pila [27]. Exponential sum methods, such as those of the author [12], yield sharper results, but only for non-singular varieties. The quality of these latter results improves as n increases. Indeed they establish Conjecture 1, for non-singular F, as soon as $n \geq 10$. Other methods such as those of Schmidt [29], depend on elementary differential geometry. They improve slightly on Cohen's result, and apply also to certain non-algebraic hypersurfaces. However none of these approaches is as effective as that of Bombieri and Pila, for the problems considered in the present paper.

In the course of this work, the author has consulted a number of people about issues in algebraic geometry—Jean-Louis Colliot-Thélène, Robin Hartshorne, Miles Reid, Nick Shepherd-Barron, Sir Peter Swinnerton-Dyer, and Yuri Tschinkel. A number of helpful comments were also made by Christopher Hooley. The help of all these people is gratefully acknowledged.

Parts of this investigation were carried out while the author was a visitor at the Institute for Advanced Study, in Princeton. The hospitality and financial support of the Institute is also gratefully acknowledged.

2 Preliminaries

In this section we establish various preliminary results.

We begin by establishing Theorem 1. This is a trivial induction exercise. The result is immediate for $n = 2$. In general, write

$$F(\mathbf{x}) = \sum_{j=0}^{d} x_1^j F_j(x_2, \ldots, x_n),$$

and suppose that k is a value for which F_k does not vanish identically. Then, by our induction assumption, there are $O_{n,d}(B^{n-2})$ vectors $(x_2, \dots, x_n)$ for which $F_k = 0$, and for each of these there are $O(B)$ choices for x_1. For the remaining vectors $(x_2, \dots, x_n)$, of which there are $O_n(B^{n-1})$, there are at most d choices for x_1. This produces a total of $O_{n,d}(B^{n-1})$ vectors $\mathbf{x}$, which completes the induction.

We turn now to the proof of Theorem 4. We shall write $M = (d+1)(d+2)/2$ and $N = d^2 + 1$, for convenience, and suppose that $F(\mathbf{x}) = 0$ has solutions $\mathbf{x}^{(1)}, \dots, x^{(N)} \in Z_n$, where $|\mathbf{x}^{(i)}| \ll B$. Consider the $N \times M$ matrix C, whose i-th row consists of the M possible monomials of degree d in the variables $x_1^{(i)}, x_2^{(i)}, x_3^{(i)}$. Then if the vector $\mathbf{f} \in \mathbb{Z}^M$ has entries which are the corresponding coefficients of F, we will have $C\mathbf{f} = \mathbf{0}$. Since $\mathbf{f} \neq \mathbf{0}$ it follows that C has rank at most $M-1$. Thus $C\mathbf{g} = \mathbf{0}$ has a non-zero integer solution $\mathbf{g}$, constructed out of the sub-determinants of C. It follows that there is such a $\mathbf{g}$ with $|\mathbf{g}| \ll_d B^{dM}$. Let $G(\mathbf{x})$ be the ternary form, of degree d, corresponding to the vector $\mathbf{g}$. Then $G(\mathbf{x})$ and $F(\mathbf{x})$ have at least d^2+1 common zeros, namely the vectors $\mathbf{x}^{(i)}$. This will contradict Bézout's Theorem, unless $G(\mathbf{x})$ is a constant multiple of $F(\mathbf{x})$. In the latter case $||F|| \ll_d ||G|| \ll_d B^{dM}$, as required. This completes the proof of Theorem 4.

Many of our arguments will use elementary facts about lattices. In the following lemma we use $|\mathbf{x}|$ for the Euclidean length of the vector $\mathbf{x}$. Moreover we allow all implied constants to depend on n.

Lemma 1

(i) For any primitive vector $\mathbf{c} \in \mathbb{Z}^n$ the set $\Lambda = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{c}.\mathbf{x} = 0\}$ is a lattice of dimension $n-1$ and determinant $\det(\Lambda) = |\mathbf{c}|$.

(ii) Let $\mathbf{c}^{(1)}, \mathbf{c}^{(2)} \in \mathbb{Z}^n$ be non-parallel primitive vectors, and let $\mathbf{p}^{(0)}$ be the vector of length $n(n-1)/2$, whose coordinates are the determinants $c_i^{(1)}c_j^{(2)} - c_j^{(1)}c_i^{(2)}$, for $i < j$. Write h for the highest common factor of the entries in $\mathbf{p}^{(0)}$, and set $\mathbf{p} = h^{-1}\mathbf{p}^{(0)}$. Then the set $\Lambda = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \in < \mathbf{c}^{(1)}, \mathbf{c}^{(2)} >\}$ (where $< \mathbf{c}^{(1)}, \mathbf{c}^{(2)} >$ denotes the $\mathbb{Q}$-vector space generated by $\mathbf{c}^{(1)}$ and $\mathbf{c}^{(2)}$) is a lattice of dimension 2 and determinant $\det(\Lambda) = |\mathbf{p}|$.

(iii) Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice of dimension m. Then Λ has a basis $\mathbf{b}^{(1)}, \dots, \mathbf{b}^{(m)}$ such that if one writes $\mathbf{x} \in \Lambda$ as $\mathbf{x} = \sum_j \lambda_j \mathbf{b}^{(j)}$, then

$$\lambda_j \ll |\mathbf{x}|/|\mathbf{b}^{(j)}|. \tag{2.1}$$

Moreover one has

$$\det(\Lambda) \ll \prod_{j=1}^{m} |\mathbf{b}^{(j)}| \ll \det(\Lambda). \tag{2.2}$$

(iv) Let $\mathbf{x} \in Z_n$ lie in the cube $|x_i| \leq B$. Then there is a primitive vector $\mathbf{y} \in \mathbb{Z}^n$, for which $\mathbf{x}.\mathbf{y} = 0$, and such that $|\mathbf{y}| \ll B^{1/(n-1)}$.

(v) Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice of dimension m. Then the sphere $|\mathbf{x}| \leq R$ contains $O(R^m/\det(\Lambda))$ points of Λ, providing that $R \gg \det(\Lambda)$.

(vi) Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice of dimension 2. Then the sphere $|\mathbf{x}| \leq R$ contains $O(1 + R^2/\det(\Lambda))$ primitive points of Λ.

(vii) Let $P \subset \mathbb{R}^2$ be a parallelogram, centred on the origin, having area A. Then P contains $O(1 + A)$ primitive integer vectors.

Statement (i) of the lemma is a special case of Heath-Brown [11; Lemma 1].

For part (ii), we first note that it is trivial that Λ is a two-dimensional lattice. Choose a basis $\mathbf{b}^{(1)}, \mathbf{b}^{(2)}$ for Λ, and set $\mathbf{c}^{(i)} = a_{i1}\mathbf{b}^{(1)} + a_{i2}\mathbf{b}^{(2)}$, for $i = 1, 2$. If $\mathbf{q}^{(0)}$ is the vector formed from the determinants $b_i^{(1)}b_j^{(2)} - b_j^{(1)}b_i^{(2)}$ for $i < j$, then $|\mathbf{q}^{(0)}|$ is the area of the parallelogram spanned by $\mathbf{b}^{(1)}$ and $\mathbf{b}^{(2)}$, so that $|\mathbf{q}^{(0)}| = \det(\Lambda)$. Moreover, we will have $\mathbf{p}^{(0)} = (a_{11}a_{22} - a_{12}a_{21})\mathbf{q}^{(0)}$, so that $\mathbf{p}$ will be a scalar multiple of $\mathbf{q}^{(0)}$. To complete the proof of part (ii) it therefore suffices to show that $\mathbf{q}^{(0)}$ is primitive. However if p were a prime dividing $\mathbf{q}^{(0)}$ then the reductions modulo p of $\mathbf{b}^{(1)}$ and $\mathbf{b}^{(2)}$ would be proportional. There would then be integers λ_1, λ_2, not both multiples of p, and an integral vector $\mathbf{b}$, such that $\lambda_1\mathbf{b}^{(1)} + \lambda_2\mathbf{b}^{(2)} = p\mathbf{b}$. Since we then have $\mathbf{b} \in \Lambda$, this would contradict the fact that $\mathbf{b}^{(1)}, \mathbf{b}^{(2)}$ is a basis for Λ.

For statement (iii) we note that Davenport [4; Lemma 5] shows the existence of a basis $\mathbf{b}^{(j)}$ with the property (2.1). Moreover in the course of the proof he shows [4; (14)] that

$$\prod_{j=1}^{m} |\mathbf{b}^{(j)}| \ll \det(\Lambda).$$

It is of course trivial that

$$\prod_{j=1}^{m} |\mathbf{b}^{(j)}| \gg \det(\Lambda),$$

for any basis.

For part (iv) we note that the lattice of integral vectors $\mathbf{y}$ satisfying $\mathbf{x}.\mathbf{y} = 0$ has dimension $n - 1$ and determinant $|\mathbf{x}|$, by statement (i). According to part (iii) there is therefore a basis element $\mathbf{y}'$, say, with $|\mathbf{y}'| \ll |\mathbf{x}|^{1/(n-1)}$, which is sufficient.

Since the condition $R \gg \det(\Lambda)$ ensures that the basis vectors in part (iii) all satisfy $|\mathbf{b}^{(j)}| \ll R$, the fundamental parallelpiped formed from these will fit inside a suitable constant multiple of the sphere $|\mathbf{x}| \leq R$. Statement (v) of the lemma then follows.

To establish part (vi) we note that Λ has a basis $\mathbf{b}^{(1)}, \mathbf{b}^{(2)}$ as in part (iii). Thus if $\mathbf{x} = \lambda_1\mathbf{b}^{(1)} + \lambda_2\mathbf{b}^{(2)}$ satisfies $|\mathbf{x}| \leq R$, then $\lambda_j \ll R/|\mathbf{b}^{(j)}|$, for $j = 1, 2$. There are therefore

$$\ll R^2|\mathbf{b}^{(1)}|^{-1}|\mathbf{b}^{(2)}|^{-2} \ll R^2 \det(\Lambda)^{-1}$$

posible pairs λ_1, λ_2 with $\lambda_1\lambda_2 \neq 0$. Moreover, since $\mathbf{x}$ is to be primitive, we can only have $\mathbf{x} = \pm\mathbf{b}^{(1)}$ or $\pm\mathbf{b}^{(2)}$ when $\lambda_1\lambda_2 = 0$. This suffices for part (vi).

For the final assertion, we begin by constructing a rectangle P' including P, centred on the origin, and having area $A' \ll A$. We may then produce an ellipse E centred on the origin, and having area $A'' \ll A' \ll A$. The desired estimate is then a corollary of Heath-Brown [11; Lemma 2].

We shall also want some results from elimination theory. We first state without proof the following basic result.

Lemma 2 *Let integers $m \geq n \geq 2$ and $d \geq 1$ be given. Then there exist intgers m', d' depending at most on m and d, as follows. Let $F_1(\mathbf{x}), \ldots, F_m(\mathbf{x})$ be forms in n variables, with coefficients in $\overline{\mathbb{Q}}$, each with degree at most d. Let $\mathbf{f}_i$ be the coefficient vector of F_i. Then there exist polynomials $E_i(\mathbf{f}_1, \ldots, \mathbf{f}_m)$ for $1 \leq i \leq m'$ over $\overline{\mathbb{Q}}$, with the following properties.*

1. *Each E_i has total degree at most d'.*
2. *The polynomials E_i are homogeneous functions in each $\mathbf{f}_j$.*
3. *The simultaneous equations $F_i(\mathbf{x}) = 0$, for $1 \leq i \leq m$, have a non-zero solution over $\overline{\mathbb{Q}}$ if and only if $E_i(\mathbf{f}_1, \ldots, \mathbf{f}_m) = 0$ for $1 \leq i \leq m'$.*

Note that the lemma does not assert that the E_i are non-zero.

¿From this we shall deduce the following.

Lemma 3 *Let $F(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, x_2, x_3, x_4]$ be a form of degree d. For any $\mathbf{y} \neq \mathbf{0}$, let $H_{\mathbf{y}}(x_i, x_j, x_k)$ be a form got by eliminating one variable from the equations $F(\mathbf{x}) = \mathbf{y}.\mathbf{x} = 0$. Then for any positive integer $\delta < d$ there is an integer $m = O_d(1)$, and forms $E_{i,\delta}(\mathbf{y}) \in \overline{\mathbb{Q}}[y_1, y_2, y_3, y_4]$, with $1 \leq i \leq m$, whose degrees are bounded in terms of d, and which vanish simultaneously precisely at those points $\mathbf{y} \neq 0$ for which $H_{\mathbf{y}}$ has a factor of degree δ.*

Again we do not assert that the forms $E_{i,\delta}$ are non-zero. We note that it does not matter how we eliminate one of the variables to produce $H_{\mathbf{y}}$, since if one of the resulting forms has a factor of degree d they all will.

To deduce the above result from Lemma 2 we consider possible factors of degree δ in

$$y_1^d F(\mathbf{x}) = F(-y_2x_2 - y_3x_3 - y_4x_4, y_1x_2, y_1x_3, y_1x_4) = f(x_2, x_3, x_4),$$

say. If G is a non-zero form of degree δ, the relation

$$\lambda f(x_2, x_3, x_4) = G(x_2, x_3, x_4)H(x_2, x_3, x_4) \tag{2.3}$$

produces a system $L_i(\lambda, \mathbf{h}) = 0$ of homogeneous linear equations in λ and the coefficients $\mathbf{h}$, say, of H. The coefficients of the L_i are polynomials in the y_i and in the coefficients $\mathbf{g}$, say, of G. According to Lemma 2 we produce polynomials $E_j(\mathbf{y}, \mathbf{g})$ in these latter variables, which vanish precisely when (2.3) has a non-zero solution. (In this case Lemma 2 is a well-known result in linear algebra,

the polynomials E_j arising as determinants.) If λ were to vanish in such a solution, then the form H must vanish too, since a polynomial ring over a field has no zero-divisors. Thus, if G is non-zero, then G divides f precisely when the polynomials $E_j(\mathbf{y}, \mathbf{g})$ all vanish. Since the divisibility of f by G is unaffected by replacing G by cG, or $\mathbf{y}$ by $c'\mathbf{y}$, for any non-zero c, c', we see that the various bi-homogeneous parts $B_k(\mathbf{y}, \mathbf{g})$ of $E_j(\mathbf{y}, \mathbf{g})$ must vanish precisely when $G|f$. We note that the degrees of the forms B_k, and the number of forms that arise, are $O_d(1)$.

A second application of Lemma 2 now produces forms $J_l(\mathbf{y})$, which vanish simultaneously if and only if there is a non-zero set of coefficients $\mathbf{g}$ for G which make all the forms $B_k(\mathbf{y}, \mathbf{g})$ vanish. As we have seen, this is precisely equivalent to the requirement that f should have a factor of degree δ. We rename the forms $J_l(\mathbf{y})$ as $J_{l,1}(\mathbf{y})$, to denote the fact that x_1 was eliminated in forming f. Thus, in a precisely analogous way, we produce forms $J_{l,i}(\mathbf{y})$ for $i = 2, 3, 4$. If $H_{\mathbf{y}}$ has a factor of degree δ, then all four of the possible forms f have such a factor, so that $J_{l,i}(\mathbf{y}) = 0$ for each l and each i. Conversely this latter condition imples that each of the four possible forms f factors. Since at least one of the y_i is non-zero, this implies that $H_{\mathbf{y}}$ has a factor of degree d. We may therefore take the forms $E_{i,\delta}$ to be the various $J_{l,i}$. Clearly both the number of such forms, and their degrees, are bounded in terms of d.

3 Proof of Theorem 14

Before beginning the proof of the above theorem we shall require a preliminary result. Let

$$S(F; \mathbf{B}, p) = \{\mathbf{x} \in Z_n : F(\mathbf{x}) = 0, |x_i| \leq B_i, (1 \leq i \leq 1), p \nmid \nabla F(\mathbf{x})\},$$

and

$$S(F; \mathbf{B}) = \{\mathbf{x} \in Z_n : F(\mathbf{x}) = 0, |x_i| \leq B_i, (1 \leq i \leq 1), \nabla F(\mathbf{x}) \neq \mathbf{0}\}.$$

We then have the following lemma.

Lemma 4 *Let $B = 2 + \max |B_i|$ and $r = [\log(||F||B)]$, and suppose that*

$$P \geq \log^2(||F||B).$$

Then there are distinct primes $p_1, \ldots, p_r$, such that $P \ll p_i \ll P$ and

$$S(F; \mathbf{B}) = \bigcup_{i=1}^{r} S(F; \mathbf{B}, p_i).$$

We remark that this result is the sole point at which a dependence on $||F||$ enters our arguments. To prove Lemma 4 we merely choose the primes p_i as the first r primes $p_i > AP$, for a suitable constant A. Since $P \gg r^2$ this yields

$P \ll p_i \ll P$. Now if $\mathbf{x}$ is in $S(F;\mathbf{B})$, then some partial derivative $\partial F/\partial x_j$, say, must be non-zero. Since

$$\frac{\partial F}{\partial x_j} \ll_n ||F||B^{d-1},$$

it follows that

$$\#\{p > AP : p|\frac{\partial F}{\partial x_j}\} \ll_{n,d} \frac{\log ||F||B}{\log AP}.$$

Thus there are fewer than r such primes, if A is large enough. We therefore see that there is some prime p_i which does not divide $\partial F/\partial x_j$, whence $\mathbf{x} \in S(F;\mathbf{B},p_i)$, as required for the lemma.

To prove Theorem 14 we begin by considering singular points. Any singular points of $F(\mathbf{x}) = 0$ satisfy

$$\frac{\partial F(\mathbf{x})}{\partial x_i} = 0, \quad (1 \le i \le n).$$

Since F is irreducible, at least one of the forms $\partial F/\partial x_i$ is not identially zero. Clearly such a form cannot be a multiple of F since its degree is $d-1$. We therefore include one of the partial derivatives of F amongst the forms F_i described in Theorem 14 to take care of the singular points of $F(\mathbf{x})$.

It therefore remains to examine non-singular points, and here we apply Lemma 4. This shows that we may consider points that are non-singular modulo a suitable prime p, at a cost of a factor $\log(||F||B)$ in our final estimate for k.

With this understanding, we now define k to be the number of non-singular points $\mathbf{t} \in \mathbb{P}^{n-1}(\mathbb{F}_p)$ on $F(\mathbf{t}) = 0$. Thus $k \ll p^{n-2} \ll P^{n-2}$, and we split the points $\mathbf{x} \in S(F;\mathbf{B},p)$ into k sets

$$S(\mathbf{t}) = \{\mathbf{x} \in S(F;\mathbf{B},p) : \mathbf{x} \equiv \rho\mathbf{t} \,(\mathrm{mod}\ p) \text{ for some } \rho \in \mathbb{Z}\}.$$

Our aim is to show that if P is chosen so that

$$P \gg (V^d/T)^{(n-2)^{-1}d^{-(n-1)/(n-2)}}V^{\varepsilon}\log^2||F||, \tag{3.1}$$

then for each set $S(\mathbf{t})$ there is a corresponding form F_j such that $F_j(\mathbf{x}) = 0$ for all $\mathbf{x} \in S(\mathbf{t})$. Note that the term $\log^2||F||$ has been included above so as to ensure that P is acceptable for Lemma 4.

¿From now on we shall focus our attention on a fixed $\mathbf{t}$. Since $\mathbf{t}$ is non-zero we may suppose without loss of generality that $t_i = 1$ for some i, and, again without loss of generality, we may take $i = 1$. If

$$\frac{\partial F}{\partial x_i}(\mathbf{t}) = 0, \quad (2 \le i \le n) \tag{3.2}$$

then

$$0 = dF(\mathbf{t}) = \mathbf{t}.\nabla F(\mathbf{t}) = \frac{\partial F}{\partial x_1}(\mathbf{t}),$$

whence $\nabla F(\mathbf{t}) = \mathbf{0}$. This contradiction shows that one of the partial derivatives in (3.2) must be non-vanishing, and we assume, without loss of generality, that

$$\frac{\partial F}{\partial x_2}(\mathbf{t}) \neq 0. \tag{3.3}$$

We proceed to lift $\mathbf{t}$ to a p-adic solution $\mathbf{u} \in \mathbb{Z}_p^n$ of $F(\mathbf{u}) = 0$. In view of (3.3), Hensel's Lemma may be used to produce a solution in which $u_1 = 1$. We now require the following result.

Lemma 5 *Let $F(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ be a form in n variables, and suppose that $\mathbf{u} \in \mathbb{Z}_p^n$ satisfies $u_1 = 1$ and*

$$F(\mathbf{u}) = 0, \quad p \nmid \frac{\partial F}{\partial x_2}(\mathbf{u}).$$

Then, for any integer $m \geq 1$ there exists $f_m(Y_3, Y_4, \ldots, Y_n) \in \mathbb{Z}_p[Y_3, \ldots, Y_n]$, such that if $F(\mathbf{v}) = 0$ for some $\mathbf{v} \in \mathbb{Z}_p^n$ with $v_1 = 1$ and $\mathbf{v} \equiv \mathbf{u} \pmod{p}$, then

$$v_2 \equiv f_m(v_3, \ldots, v_n) \pmod{p^m}. \tag{3.4}$$

One could alternatively formulate Lemma 5 to say that, for given $v_3, \ldots, v_n$, the equation $F(\mathbf{v}) = 0$ has a unique solution v_2, and that this solution is given by a $\mathbb{Z}_p$-integral power series $v_2 = f(v_3, \ldots, v_n)$. One could then use such a result in what follows to replace the sequence of polynomials f_m.

For the proof of Lemma 5 let

$$\frac{\partial F}{\partial x_2}(\mathbf{u}) = \mu,$$

say, and define the polynomials f_m inductively by taking $f_1(Y_3, \ldots, Y_n) = u_2$, (constant) and

$$f_{m+1}(Y_3, \ldots, Y_n) = f_m(Y_3, \ldots, Y_n) - \mu^{-1} F(1, f_m(Y_3, \ldots, Y_n), Y_3, \ldots, Y_n),$$

for $m \geq 1$. Clearly Lemma 5 now holds for $m = 1$. We prove the general case by induction on m. Thus we may suppose that

$$v_2 \equiv f_m(v_3, \ldots, v_n) \pmod{p^m},$$

and we write

$$v_2 = f_m(v_3, \ldots, v_n) + \lambda p^m,$$

where $\lambda \in \mathbb{Z}_p$. Then

$$\begin{aligned} 0 &= F(\mathbf{v}) \\ &\equiv F(1, f_m(v_3, \ldots, v_n), v_3, \ldots, v_n) \\ &\qquad + \lambda p^m \frac{\partial F}{\partial x_2}(1, f_m(v_3, \ldots, v_n), v_3, \ldots, v_n) \pmod{p^{m+1}}. \end{aligned} \tag{3.5}$$

Since $\mathbf{v} \equiv \mathbf{u} \pmod{p}$, the induction hypothesis (3.4) shows that

$$f_m(v_3, \ldots, v_n) \equiv u_2 \pmod{p},$$

and hence that

$$\frac{\partial F}{\partial x_2}(1, f_m(v_3, \dots, v_n), v_3, \dots, v_n) \equiv \mu \pmod{p}.$$

The congruence (3.5) then implies

$$\lambda p^m \equiv -\mu^{-1} F(1, f_m(v_3, \dots, v_n), v_3, \dots, v_n) \pmod{p^{m+1}},$$

whence

$$v_2 \equiv f_{m+1}(v_3, \dots, v_n) \pmod{p^{m+1}},$$

as required for the induction step.

We are now ready to examine our set $S(\mathbf{t})$. Let $\mathbf{x} \in S(\mathbf{t})$, so that the reduction modulo p of $\mathbf{x}$ represents the same projective point as does $\mathbf{t}$. Thus $p \nmid x_1$ so that we may interpret $x_1^{-1}\mathbf{x} = \mathbf{v}$, say, as a vector in $\mathbb{Z}_p^n$. We then see that $v_1 = 1$ and $v_i = u_i + y_i$ for $2 \le i \le n$, for suitable $y_i \in p\mathbb{Z}_p$. We shall define a collection of monomials of degree D, by choosing a set of exponents

$$\mathcal{E} \subseteq \{(e_1, \dots, e_n) \in \mathbb{Z}^n : e_i \ge 0, (1 \le i \le n), \sum_{i=1}^{n} e_i = D\},$$

and considering monomials of the form

$$X_1^{e_1} \dots X_n^{e_n} = \mathbf{X}^{\mathbf{e}},$$

say. We shall write $E = \#\mathcal{E}$, and suppose that $E \le \#S(\mathbf{t})$. Now take distinct elements $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(E)}$ of $S(\mathbf{t})$ and consider the $E \times E$ determinant

$$\Delta = \det(\mathbf{x}^{(i)\mathbf{e}})_{1 \le i \le E,\, \mathbf{e} \in \mathcal{E}},$$

with rows corresponding to the different vectors $\mathbf{x}^{(i)}$ and columns corresponding to the various exponent n-tuples $\mathbf{e}$. Our first task is to show that Δ must vanish, if p is sufficiently large in terms of the various B_i.

We begin by considering Δ modulo a large power p^m of p. We have

$$\Delta = \Big(\prod_{1 \le i \le E} x_1^{(i)} \Big)^D \det(\mathbf{v}^{(i)\mathbf{e}})_{1 \le i \le E,\, \mathbf{e} \in \mathcal{E}},$$

with $\mathbf{v}^{(i)} = (x_1^{(i)})^{-1}\mathbf{x}^{(i)}$, as above. According to Lemma 5 we deduce that

$$\Delta \equiv \Big(\prod_{1 \le i \le E} x_1^{(i)} \Big)^D \Delta_0 \pmod{p^m},$$

where

$$\Delta_0 = \det(M_0), \quad M_0 = (\mathbf{w}^{(i)\mathbf{e}})_{1 \le i \le E,\, \mathbf{e} \in \mathcal{E}},$$

with

$$w_1^{(i)} = 1, \quad w_2^{(i)} = f_m(v_3^{(i)}, \dots, v_n^{(i)}),$$

and

$$w_j^{(i)} = v_j^{(i)} \quad (3 \le j \le n).$$

We now set $v_j^{(i)} = u_j + y_j^{(i)}$ for $3 \le j \le n$, so that $p | y_j^{(i)}$. Thus

$$\mathbf{w}^{(i)\mathbf{e}} = w_1^{(i)e_1} \dots w_n^{(i)e_n} = g_{\mathbf{e}}(y_3^{(i)}, y_4^{(i)}, \dots, y_n^{(i)})$$

for an appropriate set of polynomials $g_{\mathbf{e}}(Y_3, \dots, Y_n) \in \mathbb{Z}_p[Y_3, \dots, Y_n]$. We now introduce an ordering on the exponent vectors

$$\mathbf{f} = (f_3, \dots, f_n), \quad (f_j \in \mathbb{Z}, \ \ f_j \ge 0),$$

by setting $\mathbf{f} \prec \mathbf{f}'$ if either

1. $\sum f_j < \sum f_j'$, or
2. $\sum f_j = \sum f_j'$, and there is some j such that $f_h = f_h'$ for $h < j$ but $f_j < f_j'$.

As the reader will observe, it is important, in what follows, to have $\mathbf{f} \prec \mathbf{f}'$ in case 1, but the ordering when $\sum f_j = \sum f_j'$ is immaterial. We shall order the monomials $\mathbf{Y}^{\mathbf{f}}$ in the analogous way.

We proceed to perform column operations on M_0 as follows. We look for the 'smallest' monomial $\mathbf{Y}^{\mathbf{f}}$, say, occuring in any of the polynomials $g_{\mathbf{e}}$. If this monomial occurs in more than one such polynomial we take the occurence for which the coefficient has the smallest p-adic order. We swap columns to bring this term into the first column, and then subtract p-adic integer multiples of the new first column from all those columns containing the monomial $\mathbf{Y}^{\mathbf{f}}$, so as to remove it entirely, except from the first column. This process is then repeated with the remaining $n-1$ columns, looking again for the 'smallest' monomial, moving it to column 2 and removing it from all subsequent columns. We procced in this way to obtain an expression

$$\Delta_0 = \det(M_1), \quad M_1 = \big(h_e(y_3^{(i)}, \dots, y_n^{(i)})\big)_{1 \le i \le E, \ 1 \le e \le E},$$

in which one has polynomials $h_e(\mathbf{Y}) \in \mathbb{Z}_p[\mathbf{Y}]$, with successively larger 'smallest' monomial terms. The number of monomials of total degree f is

$$\left(\begin{array}{c} f+n-3 \\ n-3 \end{array} \right) = n(f),$$

say. Thus if $e > n(0) + n(1) + \dots + n(f-1)$, the 'smallest' term in $h_e(\mathbf{Y})$ must have total degree at least f. Since $p | y_j^{(i)}$ for $3 \le j \le n$ we deduce that every element in the e-th column of M_1 must be divisible by p^f. We note that

$$\sum_{i=0}^{f} n(i) = \left(\begin{array}{c} f+n-2 \\ n-2 \end{array} \right),$$

and that

$$\sum_{i=0}^{f} in(i) = (f+1)\binom{f+n-2}{n-2} - \binom{f+n-1}{n-1}.$$

It therefore follows that if

$$\binom{f+n-2}{n-2} \le E < \binom{(f+1)+n-2}{n-2}, \tag{3.6}$$

then Δ_0 is divisible by

$$p^{n(1)+2n(2)+\ldots+fn(f)+(f+1)(E-n(0)-n(1)-\ldots-n(f))} = p^{\nu},$$

say, where

$$\nu = (f+1)E - \binom{f+n-1}{n-1}. \tag{3.7}$$

If we choose our original prime power p^m to have $m = \nu$ we may therefore conclude as follows.

Lemma 6 *Let E lie in the range (3.6), and suppose that ν is given by (3.7). Then*

$$\nu_p(\Delta) \ge \nu.$$

We shall compare this result with information on the size of Δ. Since $|x_j^{(i)}| \le B_j$, every element of the column corresponding to exponent vector $\mathbf{e}$ has modulus at most $\mathbf{B}^{\mathbf{e}}$. Thus an elementary estimate yields

$$|\Delta| \le E^E \prod_{\mathbf{e}\in\mathcal{E}} \mathbf{B}^{\mathbf{e}}.$$

We shall set

$$\sum_{\mathbf{e}\in\mathcal{E}} \mathbf{e} = \mathbf{E}, \tag{3.8}$$

say, and require that

$$p^{\nu} > E^E \mathbf{B}^{\mathbf{E}}. \tag{3.9}$$

Then Δ must vanish.

In forming Δ we assumed that $\#S(\mathbf{t}) \ge E$, and we took $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(E)}$ to be any distinct elements of $S(\mathbf{t})$. Thus if we set $\#S(\mathbf{t}) = K$ and consider the matrix

$$M_2 = \left(\mathbf{x}^{(i)\mathbf{e}}\right)_{1\le i\le K,\ \mathbf{e}\in\mathcal{E}},$$

where $\mathbf{x}^{(i)}$ now runs over all elements of $S(\mathbf{t})$, we see that M_2 can have rank at most $E-1$. This is trivial when $K \le E-1$, and otherwise every $E \times E$ minor vanishes, by what we have proved. It follows that $M_2\mathbf{c} = \mathbf{0}$ for some non-zero vector $\mathbf{c} \in \mathbb{Z}^E$. Thus, if we set

$$G(\mathbf{X}) = \sum_{\mathbf{e}\in\mathcal{E}} c_{\mathbf{e}} \mathbf{X}^{\mathbf{e}}, \tag{3.10}$$

we have produced a non-zero polynomial, of degree D, and such that $G(\mathbf{x}) = 0$ for every $\mathbf{x} \in S(\mathbf{t})$.

It remains to select the exponent set $\mathcal{E}$ so as to ensure that $F(\mathbf{x}) \nmid G(\mathbf{x})$. We write

$$F(X_1, \ldots, X_n) = \sum_{\mathbf{f}} a_{\mathbf{f}} X_1^{f_1} \ldots X_n^{f_n},$$

and consider the Newton polyhedron P, defined as the convex hull of the points $\mathbf{f} \in \mathbb{R}^n$ for which $a_{\mathbf{f}} \neq 0$. Clearly P is a subset of the affine hyperplane given by $\sum f_i = d$. Any vertex of P will be an exponent vector $\mathbf{f}$, with $a_{\mathbf{f}} \neq 0$. Now consider such a vertex $\mathbf{f}^*$, say, at which

$$\sum_{i=1}^{n} f_i^* \log B_i$$

is maximal. We proceed to choose numbers B_i' in the range $[B_i\,,\, 1 + B_i]$, such that the values of $\log B_i'$ are linearly independent over $\mathbb{Q}$, and such that

$$\sum_{i=1}^{n} f_i \log B_i'$$

is maximal only at the vertex $\mathbf{f}^*$ of P. Let the maximal value be M_F.

Suppose now that $G(\mathbf{X})$ is given by (3.10), and that $G(\mathbf{x})$ is a multiple of $F(\mathbf{X})$, so that $G(\mathbf{X}) = F(\mathbf{X})K(\mathbf{X})$, say. Let

$$K(X_1, \ldots, X_n) = \sum_{\mathbf{k} \in \mathcal{K}} b_{\mathbf{k}} X_1^{k_1} \ldots X_n^{k_n},$$

with $b_{\mathbf{k}} \neq 0$, and suppose that

$$\sum_{i=1}^{n} k_i \log B_i'$$

is maximal at $\mathbf{k} = \mathbf{k}^*$, say, with maximal value M_K. Clearly $\mathbf{k}^*$ is unique, since the $\log B_i'$ are linearly independent over $\mathbb{Q}$. Now all terms

$$a_{\mathbf{f}} X_1^{f_1} \ldots X_n^{f_n} . b_{\mathbf{k}} X_1^{k_1} \ldots X_n^{k_n}$$

arising from the product $F(\mathbf{X})K(\mathbf{X})$ will have

$$\sum_{i=1}^{n} (f_i + k_i) \log B_i' < M_F + M_K,$$

with the exception of the term for $\mathbf{f} = \mathbf{f}^*$ and $\mathbf{k} = \mathbf{k}^*$. It follows that the monomial

$$X_1^{f_1^* + k_1^*} \ldots X_n^{f_n^* + k_n^*}$$

occurs in $G(\mathbf{x})$ with non-zero coefficient.

We now define

$$\mathcal{E} = \{(e_1, \dots, e_n) \in \mathbb{Z}^n : e_i \geq 0,\ (1 \leq i \leq n),\ \sum_{i=1}^{n} e_i = D,\ e_i < f_i^* \text{ for some } i\}.$$

In the light of the above discussion it is then apparent that we cannot have $F(\mathbf{X})|G(\mathbf{X})$.

It remains to choose the parameter D. We see from (3.9) that it suffices to require that

$$p \gg_D \prod_{i=1}^{n} B_i^{E_i/\nu}.$$

However it is an elementary matter to calculate that if $D \geq d$ then

$$E = \left(\begin{array}{c} D+n-1 \\ n-1 \end{array} \right) - \left(\begin{array}{c} D-d+n-1 \\ n-1 \end{array} \right) = \frac{dD^{n-2}}{(n-2)!} + O(D^{n-3}).$$

Here we follow the convention that implied constants may depend on n and d. Moreover, since (3.6) implies that

$$E = \frac{f^{n-2}}{(n-2)!} + O(f^{n-3}),$$

we deduce that

$$f = d^{1/(n-2)}D + O(1).$$

Thus (3.7) yields

$$\begin{aligned} \nu &= \frac{(n-2)f^{n-1}}{(n-1)!} + O(f^{n-2}) \\ &= d^{(n-1)/(n-2)}(n-2)\frac{D^{n-1}}{(n-1)!} + O(D^{n-2}). \end{aligned} \tag{3.11}$$

In order to find the vector $\mathbf{E}$ defined in (3.8), we write $\mathcal{E} = \mathcal{E}_1 \setminus \mathcal{E}_2$, where

$$\mathcal{E}_1 = \{(e_1, \dots, e_n) \in \mathbb{Z}^n : e_i \geq 0,\ (1 \leq i \leq n),\ \sum_{i=1}^{n} e_i = D\}$$

and

$$\mathcal{E}_2 = \{(e_1, \dots, e_n) \in \mathbb{Z}^n : e_i \geq 0,\ (1 \leq i \leq n),\ \sum_{i=1}^{n} e_i = D,\ e_i \geq f_i^* \text{ for all } i\}.$$

Then

$$\begin{aligned} \sum_{\mathbf{e} \in \mathcal{E}_1} e_i &= \frac{1}{n} \sum_{\mathbf{e} \in \mathcal{E}_1} \sum_{i=1}^{n} e_i \\ &= \frac{D}{n} \#\mathcal{E}_1 \\ &= \frac{D}{n} \left(\begin{array}{c} D+n-1 \\ n-1 \end{array} \right), \end{aligned}$$

and similarly,

$$\begin{aligned}\sum_{\mathbf{e}\in\mathcal{E}_2} e_i &= (f_i^* + \frac{D-d}{n})\#\mathcal{E}_2 \\ &= (f_i^* + \frac{D-d}{n})\left(\begin{array}{c} D-d+n-1 \\ n-1 \end{array}\right).\end{aligned}$$

Thus

$$\begin{aligned}E_i &= \sum_{\mathbf{e}\in\mathcal{E}} e_i \\ &= \frac{D}{n}\left(\begin{array}{c} D+n-1 \\ n-1 \end{array}\right) - (f_i^* + \frac{D-d}{n})\left(\begin{array}{c} D-d+n-1 \\ n-1 \end{array}\right) \\ &= (d-f_i^*)\frac{D^{n-1}}{(n-1)!} + O(D^{n-2}).\end{aligned}$$

In view of (3.11) we find that

$$E_i/\nu = (n-2)^{-1}(d-f_i^*)d^{-(n-1)/(n-2)} + O(D^{-1}),$$

whence it suffices to have

$$p \gg (V^d/T)^{(n-2)^{-1}d^{-(n-1)/(n-2)}}V^{O(1/D)}.$$

The condition (3.1) is therefore sufficient, providing that we take $D \geq D(n,d,\varepsilon)$. This completes the proof of Theorem 14.

4 Curves in $\mathbb{P}^3$

In this section we shall prove Theorem 5, by projecting the curve C onto a suitable planar curve. The following result shows how this may be done without changing the degree of the curve. Recall that the degree of a curve in $\mathbb{P}^3$ may be defined as the number of points of intersection with a generic plane.

Lemma 7 *Let $C \subset \mathbb{P}^3$ be an irreducible projective curve of degree d. Then there are non-zero integer vectors $\mathbf{y}$ and $\mathbf{c}$ with $|\mathbf{y}|, |\mathbf{c}| \ll 1$, such that $\mathbf{y}.\mathbf{c} \neq 0$, and so that the projection of C parallel to $\mathbf{y}$, onto the plane $\mathbf{x}.\mathbf{c} = 0$ produces an irreducible curve of degree d. Moreover each fibre contains at most d points.*

It is a familiar fact that the generic projection of C onto a plane will indeed be an irreducible curve of degree d. Thus the thrust of the result is that we can choose a projection with $|\mathbf{y}| \ll 1$. One difficulty in the proof is that we do not have a convenient basis for the ideal of polynomials vanishing on C.

Before proving Lemma 7, we show how Theorem 5 follows. Write π for the projection given by Lemma 7. If $\mathbf{x} \in Z_4$, with $|\mathbf{x}| \ll B$, then

$$\pi(\mathbf{x}) = \mathbf{x} - \frac{(\mathbf{x}.\mathbf{c})}{(\mathbf{y}.\mathbf{c})}\mathbf{y},$$

whence $(\mathbf{y}.\mathbf{c})\pi(\mathbf{x})$ is an integral vector, with $|(\mathbf{y}.\mathbf{c})\pi(\mathbf{x})| \ll B$. Although the vectors $(\mathbf{y}.\mathbf{c})\pi(\mathbf{x})$ may not be primitive, there are, according to Lemma 7, at most d values of $\mathbf{x}$ for which $(\mathbf{y}.\mathbf{c})\pi(\mathbf{x})$ is projectively equivalent to a given point in the plane $\mathbf{z}.\mathbf{c} = 0$. Thus it will suffice to show that the curve $\pi(C)$ has $O_\varepsilon(B^{2/d+\varepsilon})$ points in the region $|\mathbf{z}| \ll B$.

According to parts (i) and (iii) of Lemma 1, we can choose a basis for the lattice of integer vectors in the plane $\mathbf{z}.\mathbf{c} = 0$, with respect to which $\mathbf{z}$ will have coordinates $(\lambda_1, \lambda_2, \lambda_3)$ with $\lambda_i \ll B$. Since Lemma 7 produces a curve $\pi(C)$ of degree d, we may apply Theorem 3 to show that the number of primitive points $(\lambda_1, \lambda_2, \lambda_3)$ on the curve $\pi(C)$, lying in the region $\lambda_i \ll B$, is indeed $O_\varepsilon(B^{2/d+\varepsilon})$. This establishes Theorem 5.

The remainder of this section is devoted to the proof of Lemma 7. The result is trivial if C is planar, since any $\mathbf{y}$ not lying in the same plane as C may be used. We therefore assume that C is non-planar. For the proof we shall find a plane P, given by an equation $\mathbf{x}.\mathbf{a} = 0$, so that P intersects C in exactly d points $\mathbf{x}_i$, say. We shall want $\mathbf{a}$ to be a non-zero integer vector satisfying $|\mathbf{a}| \ll 1$. We first demonstrate that this will suffice for our result. We choose the vector $\mathbf{y}$ to correspond to a point in the plane P, not on one of the lines $< \mathbf{x}_i, \mathbf{x}_j >$ for $i \neq j$. Theorem 1 shows that this is possible with $|\mathbf{y}| \ll 1$. We then choose any integer vector $\mathbf{c}$ for which $\mathbf{y}.\mathbf{c} \neq 0$ and $|\mathbf{c}| \ll 1$, via a further application of Theorem 1. The projection π from C along $\mathbf{y}$ onto the plane $\mathbf{x}.\mathbf{c} = 0$ is then a regular map, as $\mathbf{y}$ is not on C, so that its image $\pi(C)$ is an irreducible curve. Moreover the points $\pi(\mathbf{x}_1), \ldots, \pi(\mathbf{x}_d)$ are distinct, and lie on the intersection of the curve $\pi(C)$ and the line $\pi(P)$. Thus $\pi(C)$ has degree at least d. On the other hand, if $\pi(C)$ had degree greater than d there would be a line L intersecting $\pi(C)$ in more than d points. The inverse image $\pi^{-1}(L)$ would then be a plane intersecting C in more than d points, which is impossible, since C is non-planar. If the fibre over a point of $\pi(C)$ contained more than d points, this would produce a line meeting C in more than d points. Any plane containing this line would meet C in more than d points, and hence would contain C. This would again contradict our assumption that C is non-planar.

The remainder of the proof is devoted to finding a suitable plane P. According to Bézout's Theorem, in the form given by Harris [9; Theorem 18.3], for example, it will suffice that P passes through none of the singular points of C, and is nowhere tangent to C.

We begin by finding some equations of degree at most d, satisfied on C. We begin by choosing linearly independent vectors $\mathbf{e}_1, \ldots, \mathbf{e}_4$ not lying on C, and we change coordinates to use this as a new basis. We shall change coordinates to use this as a new basis. The projection from C along $\mathbf{e}_1$ onto the plane spanned by $\mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4$, is a regular map, and the image is therefore an irreducible curve C_1, with equation $f_1(x_2, x_3, x_4) = 0$. The curve C_1 can have degree at most d, by the argument above. We therefore have an absolutely irreducible equation $f_1(x_2, x_3, x_4) = 0$ of degree at most d, satisfied everywhere on C. In the same way, we can produce absolutely irreducible equations $f_2(x_1, x_3, x_4) = 0$ and $f_3(x_1, x_2, x_4) = 0$, of degree at most d. We shall think of each f_i as being a form in (x_1, x_2, x_3, x_4), being independent of x_i.

Let I be the intersection

$$I: \quad f_1(\mathbf{x}) = f_2(\mathbf{x}) = f_3(\mathbf{x}) = 0.$$

If I were to contain a component of dimension 2, the polynomials f_i, being absolutely irreducible, would have to be constant multiples of each other. This could only happen if they were each constant multiples of x_4. In this case however C would be contained in the plane $x_4 = 0$, contrary to assumption. Now let Γ be a component of I of dimension 1. We proceed to show that the 3×4 matrix M_1, with rows $\nabla f_1(\mathbf{x}), \nabla f_2(\mathbf{x})$ and $\nabla f_3(\mathbf{x})$, has rank at least 2 at a generic point P_0 of Γ. Suppose, on the contrary, that M_1 has rank at most 1 at P_0. Since $\partial f_i/\partial x_i$ vanishes identically for $i = 1, 2$ and 3, it then follows that there is some pair of indices $i \neq j$ for which

$$\frac{\partial f_i}{\partial x_j}(P_0) = \frac{\partial f_j}{\partial x_i}(P_0) = 0.$$

Suppose, to be specific, that $i = 1, j = 2$. Then we have equations

$$f_1(0, x_2, x_3, x_4) = \frac{\partial f_1}{\partial x_2}(0, x_2, x_3, x_4) = 0$$

and

$$f_2(x_1, 0, x_3, x_4) = \frac{\partial f_2}{\partial x_1}(x_1, 0, x_3, x_4) = 0,$$

holding on Γ. If one of the partial derivatives, $\partial f_1/\partial x_2$ say, vanishes identically, the form f_1 would take the shape $f_1(x_3, x_4)$. Since C lies on $f_1 = 0$, it would follow that C lies in a plane, which we assumed was not the case. We may therefore suppose that neither of the partial derivatives above vanishes identically. Since f_1 is absolutely irreducible, the first pair of equations shows that Γ must be a line through the point $(1, 0, 0, 0)$. Similarly the second pair of equations shows that Γ must be a line through the point $(0, 1, 0, 0)$. Hence Γ must be the line $x_3 = x_4 = 0$. The equation $f_3(x_1, x_2, 0, x_4) = 0$ has to hold on this line, which implies that $x_4 | f_3(x_1, x_2, 0, x_4)$. Since f_3 is irreducible, this implies that $f_3(x_1, x_2, 0, x_4) = cx_4$. However $f_3 = 0$ is an equation for the original curve C, which was assumed to be non-planar. This establishes our claim about the matrix M_1, and shows that each one-dimensional component Γ of I contains only finitely many points where M_1 has rank at most 1. Indeed, since there are only finitely many components, and only finitely many of these are points, we may conclude that there are only finitely many points $\mathbf{x}_i$ on I which are either point components of I or for which M_1 has rank at most 1.

Now let $\Delta_i(\mathbf{a}, \mathbf{x})$ for $1 \leq i \leq 16$ be the 3×3 determinants formed from the matrix M_2 with rows $\nabla f_1(\mathbf{x}), \nabla f_2(\mathbf{x}), \nabla f_3(\mathbf{x})$ and $\mathbf{a}$, and consider the system of equations

$$\mathbf{a}.\mathbf{x} = 0, \quad f_i(\mathbf{x}) = 0 \quad (1 \leq i \leq 3), \quad \Delta_i(\mathbf{a}, \mathbf{x}) = 0 \quad (1 \leq i \leq 16). \tag{4.1}$$

Choose a value of $\mathbf{p}$ (not necessarily integral) which does not lie on the dual variety Γ^*, for any one-dimensional component Γ of I, and such that $\mathbf{p}.\mathbf{x}_i \neq 0$

for each of points $\mathbf{x}_i$ found above. This is possible, since Γ^* has dimension at most 2 (see Harris [9; page 197]). Then if $\mathbf{x}$ were a solution to (4.1) with $\mathbf{a} = \mathbf{p}$, it would lie in the intersection I. Moreover it cannot be one of the points $\mathbf{x}_i$, whence $\mathbf{x}$ lies on a curve Γ in I, and M_1 has rank at least 2. Each tangent space $T_{\mathbf{x}}(\Gamma)$ has projective dimension at least one, and its elements are orthogonal to each of the $\nabla f_i(\mathbf{x})$. It follows that M_1 has rank exactly 2, that Γ is non-singular at $\mathbf{x}$, and that

$$T_{\mathbf{x}}(\Gamma) = \{\mathbf{y} : \ \mathbf{y}.\nabla f_i(\mathbf{x}) = 0 \ (1 \leq i \leq 3)\}.$$

Since $\Delta_i(\mathbf{p}, \mathbf{x}) = 0$ for each i we see that $\mathbf{p}$ is in the linear span of the vectors $\nabla f_i(\mathbf{x})$, whence

$$T_{\mathbf{x}}(\Gamma) \subset \{\mathbf{y} : \ \mathbf{y}.\mathbf{p} = 0\}.$$

This however contradicts our assumption that $\mathbf{p}$ is not in Γ^*. Thus (4.1) has no solutions $\mathbf{x}$ when $\mathbf{a} = \mathbf{p}$.

Lemma 2 shows that there is a necessary and sufficient condition for (4.1) to be solvable for $\mathbf{x}$, given by the vanishing of a system of forms $G_i(\mathbf{a})$. These forms will have degrees which are bounded in terms of d. The condition is non-empty, since (4.1) is not always solvable, as we have shown. We now make a linear change of variables to revert to our original coordinate system. Then, using Theorem 1, we can find a non-zero integer vector $\mathbf{a} \ll 1$ for which (4.10 has no solution. Thus, if $\mathbf{x}$ lies on C and is also on the plane $\mathbf{a}.\mathbf{x} = 0$, we must have $\Delta_i(\mathbf{a}, \mathbf{x}) \neq 0$ for some i, since $f_i(\mathbf{x}) = 0$ are amongst the equations for C. It follows that M_2 has rank at least 3, and hence that M_1 has rank at least 2. We can then deduce, as above, that M_1 has rank exactly 2, that C is non-singular at $\mathbf{x}$, and that

$$T_{\mathbf{x}}(C) = \{\mathbf{y} : \ \mathbf{y}.\nabla f_i(\mathbf{x}) = 0 \ (1 \leq i \leq 3)\}.$$

Since M_2 has strictly larger rank than M_1, we see that $\mathbf{a}$ is not in the span of the vectors $\nabla f_i(\mathbf{x})$, so that the tangent space cannot be contained in the plane $\mathbf{a}.\mathbf{x} = 0$. The plane $\mathbf{a}.\mathbf{x} = 0$ therefore has the required properties, and Lemma 7 is proved.

5 Quadratic Hypersurfaces

This section is devoted to the proof of Theorem 2. Our key tool is the following result, for which see Heath-Brown [13; Theorem 3].

Lemma 8 *Let q be a non-singular integral ternary quadratic form, with coefficients bounded in modulus by $||q||$, say. Suppose that the binary form $q(x_1, x_2, 0)$ is also non-singular. Then for any integer k the equation $q(\mathbf{x}) = 0$ has only $O_\varepsilon((||q||R)^\varepsilon)$ primitive integer solutions in the cube $|x_i| \leq R$, with $x_3 = k$.*

We first prove a weaker version of Theorem 2, namely the estimate

$$N(B) \ll_\varepsilon ||F||^\varepsilon B^{n-2+\varepsilon}. \tag{5.1}$$

Having done this we shall use a technique similar to that developed for Theorem 4, to deduce Theorem 2 itself.

To prove (5.1) we shall begin by making a change of variables, $\mathbf{x} = M\mathbf{y}$ to produce $F(M\mathbf{y}) = T(\mathbf{y})$, say. We shall write T_{ij} for the coefficients of T, so that the T_{ij} are quadratic polynomials in the entries M_{ij}. We now consider the function

$$f(M) = \det(M).T_{11}.\det(T_{ij})_{i,j\le 2}.\det(T_{ij})_{i,j\le 3}.$$

This does not vanish identically, since it is possible to choose M so as to make T diagonal, with at least 3 non-zero entries. Since $f(M)$ is a form of degree $n+12$ in the entries M_{ij} of the matrix M, we see from Theorem 1 that there is an integral matrix M, with $\max|M_{ij}| \ll 1$ such that $f(M) \neq 0$. If $\mathbf{x} \in \mathbb{Z}^4$ then $\det(M)\mathbf{y} \in \mathbb{Z}^4$. Thus it suffices to consider solutions of $T(\mathbf{y}) = 0$, with $|\mathbf{y}| \ll B$. Here $||T|| \ll ||F||$.

For any choice of $\mathbf{u} = (y_3, \dots, y_n)$ with $y_i \ll B$, we shall set

$$q(x, y, z) = T(x, y, z\mathbf{u}).$$

The determinant of this form is a quadratic polynomial $D(\mathbf{u})$, say. Moreover, $D(\mathbf{u})$ does not vanish identically, since

$$D(1, 0, 0, \dots, 0) = \det(T_{ij})_{i,j\le 3} \neq 0,$$

by choice of M. We also see that $q(x, y, 0)$ is non-singular, because

$$\det(T_{ij})_{i,j\le 2} \neq 0,$$

again by choice of M. Thus if $\mathbf{u}$ is a value for which $D(\mathbf{u}) \neq 0$ then Lemma 8 shows that there are $O_\varepsilon((||F||B)^\varepsilon)$ possible values of y_1, y_2 making $T(\mathbf{y}) = 0$. This produces $O_\varepsilon(||F||^\varepsilon B^{n-2+\varepsilon})$ solutions in total. On the other hand, since $D(\mathbf{u})$ does not vanish identically, there can be only $O(B^{n-3})$ values of $\mathbf{u}$ for which $D(\mathbf{u}) = 0$, by Theorem 1. For each of these we can specify y_2 in $O(B)$ ways, and then there are at most 2 corresponding values of y_1, since $T_{11} \neq 0$, by choice of M. There are therefore $O(B^{n-2})$ solutions for which $D(\mathbf{u}) = 0$, which completes the proof of (5.1).

To derive Theorem 2 from (5.1) we shall adapt the treatment of Theorem 4. Let $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(N)} \in Z_n$ be the complete set of solutions of $F(\mathbf{x}) = 0$ in the region $|\mathbf{x}^{(i)}| \ll B$. Set $M = n(n+1)/2$ for convenience, and consider the $N \times M$ matrix C, whose i-th row consists of the M possible monomials of degree 2 in the variables $x_1^{(i)}, \dots, x_n^{(i)}$. Then if the vector $\mathbf{f} \in \mathbb{Z}^M$ has entries which are the corresponding coefficients of F, we will have $C\mathbf{f} = \mathbf{0}$. Since $\mathbf{f} \neq \mathbf{0}$ it follows that C has rank at most $M-1$. Thus $C\mathbf{g} = \mathbf{0}$ has a non-zero integer solution $\mathbf{g}$, constructed out of the sub-determinants of C. It follows that there is such a $\mathbf{g}$ with $|\mathbf{g}| \ll_d B^{2M-2}$. Let $G(\mathbf{x})$ be the quadratic form corresponding to the vector $\mathbf{g}$. Then $G(\mathbf{x})$ and $F(\mathbf{x})$ have N common zeros, namely the vectors $\mathbf{x}^{(i)}$. If $G(\mathbf{x})$ is a rational multiple of $F(\mathbf{x})$ then

$$N(F; B) \le N(G; B) \ll_\varepsilon ||G||^\varepsilon B^{n-2+\varepsilon},$$

by (5.1). In this case we have $N(F; B) \ll_\varepsilon B^{2+\varepsilon}$, as required, on re-defining ε.

If $G(\mathbf{x})$ is not a rational multiple of $F(\mathbf{x})$ then the points $\mathbf{x}^{(i)}$ satisfy $F(\mathbf{x}) = G(\mathbf{x}) = 0$. As above, we may apply a linear transformation so that F contains the term x_1^2 with non-zero coefficient. We can then eliminate x_1 from the equations $F(\mathbf{x}) = G(\mathbf{x}) = 0$ to deduce that $H(x_2, \ldots, x_n) = 0$, for some non-zero form H of degree at most 4. Theorem 1 shows that this has $O(B^{n-2})$ solutions in the relevant region, and for each of these solutions $(x_2, \ldots, x_n)$ the equation $F(\mathbf{x}) = 0$ determines at most two values of x_1. It follows that $N \ll B^{n-2}$ in this case, and Theorem 2 follows.

6 General Surfaces

In this section we shall consider Theorems 6, 7 and 9. We begin with Theorem 6. We shall apply part (iv) of Lemma 1 in the case in which $n = 4$, so that

$$\mathbf{y} \ll B^{1/3}. \tag{6.1}$$

The points on $F(\mathbf{x}) = 0$ which also lie in the plane $\mathbf{x}.\mathbf{y} = 0$ are in 1–1 correspondence with points on a curve $G_{\mathbf{y}}(\lambda_1, \lambda_2, \lambda_3) = 0$, where

$$G_{\mathbf{y}}(\lambda_1, \lambda_2, \lambda_3) = F(\lambda_1 \mathbf{x}^{(1)} + \lambda_2 \mathbf{x}^{(2)} + \lambda_3 \mathbf{x}^{(3)}).$$

Moreover primitive points on $F = 0$ correspond to primitive points on $G_{\mathbf{y}} = 0$, and vice-versa. If $\mathbf{x} = \sum \lambda_j \mathbf{x}^{(j)}$ lies in the box $\max |x_i| \leq B$, then Lemma 1, part (iii), yields $|\lambda_j| \ll B|\mathbf{x}^{(j)}|^{-1}$. We then apply Theorem 3 with $B_j = cB|\mathbf{x}^{(j)}|^{-1}$, for a suitable constant $c > 0$. If we order the indices so that $|\mathbf{x}^{(1)}| \geq |\mathbf{x}^{(2)}| \geq |\mathbf{x}^{(3)}|$, we will have $T \gg B^d |\mathbf{x}^{(1)}|^{-d}$, whence

$$N(G_{\mathbf{y}}; c\frac{B}{|\mathbf{x}^{(1)}|}, c\frac{B}{|\mathbf{x}^{(2)}|}, c\frac{B}{|\mathbf{x}^{(3)}|}) \ll_{c,\varepsilon} B^{2/d+\varepsilon}(|\mathbf{x}^{(2)}|.|\mathbf{x}^{(3)}|)^{-1/d}, \tag{6.2}$$

providing that $G_{\mathbf{y}}$ is irreducible over $\mathbb{Q}$.

We now sum over the possible vectors $\mathbf{y}$, counting them according to the values of the various $\mathbf{x}^{(j)}$. Consider the case in which $C_j < |\mathbf{x}^{(j)}| \leq 2C_j$ for $1 \leq j \leq 3$. The vector $\mathbf{y}$ lies in the integer lattice defined by $\mathbf{y}.\mathbf{x}^{(3)} = 0$, and this lattice has determinant $|\mathbf{x}^{(3)}|$, by Lemma 1, part (i). In our situation we take $\mathbf{y} \ll Y = C_1C_2C_3$, in view of (2.2), whence part (v) of Lemma 1 shows that the number of possible vectors $\mathbf{y}$ is $O(Y^3|\mathbf{x}^{(3)}|^{-1})$. Thus there are $O(C_1^3C_2^3C_3^2)$ possible values of $\mathbf{y}$ for each $\mathbf{x}^{(3)}$. We sum this over the $O(C_3^4)$ possible vectors $\mathbf{x}^{(3)}$, and conclude that there are $O(C_1^3C_2^3C_3^6)$ values of $\mathbf{y}$ for which $C_j < |\mathbf{x}^{(j)}| \leq 2C_j$ for $1 \leq j \leq 3$. For each such $\mathbf{y}$ we have

$$N(G_{\mathbf{y}}; c\frac{B}{|\mathbf{x}^{(1)}|}, c\frac{B}{|\mathbf{x}^{(2)}|}, c\frac{B}{|\mathbf{x}^{(3)}|}) \ll_{c,\varepsilon} B^{2/d+\varepsilon}(C_2C_3)^{-1/d},$$

by (6.2), producing a total contribution

$$\ll_{\varepsilon} B^{2/d+\varepsilon} C_1^3 C_2^{3-1/d} C_3^{6-1/d}.$$

Since the indices are ordered with $C_1 \gg C_2 \gg C_3$, and

$$C_1C_2C_3 \ll |\mathbf{x}^{(1)}|.|\mathbf{x}^{(2)}|.|\mathbf{x}^{(3)}| \ll |\mathbf{y}| \ll B^{1/3},$$

by (2.2) and (6.1), we obtain an estimate

$$\begin{aligned} &\ll_\varepsilon B^{2/d+\varepsilon}(C_1C_2C_3)^{4-2/3d} \\ &\ll_\varepsilon B^{2/d+\varepsilon}B^{4/3-2/9d} \\ &\ll_\varepsilon B^{4/3+16/9d+\varepsilon}, \end{aligned}$$

for the contribution to $N(B)$ corresponding to the case in which $G_{\mathbf{y}}$ is irreducible over $\mathbb{Q}$, and $C_j < |\mathbf{x}^{(j)}| \leq 2C_j$. Finally we let the C_j run over powers of 2 and sum the resulting bounds to obtain an estimate which we state formally as follows.

Lemma 9 *The contribution to $N(B)$ corresponding to those vectors $\mathbf{y}$ for which $G_{\mathbf{y}}$ is irreducible over $\mathbb{Q}$ is $O_\varepsilon(B^{4/3+16/9d+\varepsilon})$.*

We must now tackle the case in which $G_{\mathbf{y}}$ is reducible over $\mathbb{Q}$. If $G_{\mathbf{y}}(\lambda_1, \lambda_2, \lambda_3) = 0$, then we must have $H(\lambda_1, \lambda_2, \lambda_3) = 0$ for some factor H of $G_{\mathbf{y}}$. We may suppose that H is irreducible over $\mathbb{Q}$, though not necessarily absolutely irreducible. Of course, any solution corresponding to a linear factor H produces a point $\mathbf{x}$ lying on a line in the surface $F = 0$ which is define over $\mathbb{Q}$. We next dispose of the case in which H has degree $d' \geq 3$ or more. Here the analysis leading up to Lemma 9 goes through just as before, and leads to a contribution

$$\ll_\varepsilon B^{4/3+16/9d'+\varepsilon} \ll_\varepsilon B^{52/27+\varepsilon}. \tag{6.3}$$

We turn now to the case in which there is a quadratic factor. We shall assume in what follows that $d \geq 3$. Lemma 3 shows that there is a set of conditions $E_m(\mathbf{y}) = 0$ which are necessary and sufficient for $G_{\mathbf{y}}$ to have a quadratic factor. In general an elimination procedure of the above type may lead to an empty set of equations $E_m = 0$. However in our case this does not happen, since the generic plane section of the surface $F = 0$ is known to be irreducible, see Harris [9; Proposition 18.10]. At least one of the forms E_m must therefore be non-zero, and we may therefore conclude as follows.

Lemma 10 *There is a non-zero form $E(\mathbf{y})$ with degree bounded in terms of d, such that if $G_{\mathbf{y}}$ has a quadratic factor, then $E(\mathbf{y}) = 0$.*

It should be stressed that the only respect in which this differs from the statement that the generic plane section of the surface $F = 0$ is irreducible, lies in our control over the degree of E.

We can now apply Theorem 1 to show that there are $O(Y^3)$ vectors $\mathbf{y}$ with $Y < \mathbf{y} \leq 2Y$, such that $G_{\mathbf{y}}$ has a quadratic factor, H say. Then if H were singular, but irreducible over $\mathbb{Q}$, we would find that $H(\lambda_1, \lambda_2, \lambda_3) = 0$ has $O(1)$

primitive solutions $(\lambda_1, \lambda_2, \lambda_3)$. If H is non-singular, we may apply Theorem 3, with $B_i \ll B|\mathbf{x}^{(i)}|^{-1}$, to deduce that

$$\begin{aligned} N(H; c\frac{B}{|\mathbf{x}^{(1)}|}, c\frac{B}{|\mathbf{x}^{(2)}|}, c\frac{B}{|\mathbf{x}^{(3)}|}) &\ll_{c,\varepsilon} B^{1+\varepsilon}(|\mathbf{x}_1|.|\mathbf{x}_2|.|\mathbf{x}_3|)^{-1/3} \\ &\ll_{c,\varepsilon} B^{1+\varepsilon}|\mathbf{y}|^{-1/3}, \end{aligned}$$

by (2.2). The range $Y < \mathbf{y} \leq 2Y$ therefore contributes $O_\varepsilon(B^{1+\varepsilon}Y^{8/3})$. Thus if we sum Y over powers of 2, with $Y \ll B^{1/3}$, we obtain a contribution $O_\varepsilon(B^{17/9+\varepsilon})$. If we combine this with the bounds given by (6.3) and by Lemma 9, we obtain the assertion of Theorem 6.

We turn now to Theorem 7. Here our starting point is the case $n = 4$ of Theorem 14, which shows that every point $\mathbf{x}$ on the surface $F(\mathbf{x}) = 0$ which lies in the cube $|\mathbf{x}| \leq B$, must also satisfy one of the equations $F_j(\mathbf{x}) = 0$. Here

$$j \leq k \ll_\varepsilon B^{3/\sqrt{d}+\varepsilon} \log^5 ||F||.$$

The intersection $F(\mathbf{x}) = F_j(\mathbf{x}) = 0$ consists of at most dD curves C, with degrees at most dD. If C is a line, not defined over $\mathbb{Q}$, it contains at most one rational point. We can therefore suppose that C has degree at least 2. To estimate the number of points on such a curve C, we apply Theorem 5. Thus each curve contributes $O_{d,\varepsilon}(B^{1+\varepsilon})$ points, so that

$$N_1(F; B) \ll_\varepsilon B^{1+3/\sqrt{d}+\varepsilon} \log^5 ||F||.$$

We proceed to show that the factor $\log^5 ||F||$ can be eliminated from this estimate, by the method used in §5 for proving the case $d = 2$ of Theorem 9. We take $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(N)}$ to be the complete set of solutions of $F(\mathbf{x}) = 0$ in the region $|\mathbf{x}^{(i)}| \ll B$, excepting any that lie on lines in the surface which are defined over $\mathbb{Q}$. Proceeding as before, we reach two possible cases. In the first case, when the form G is a constant multiple of F, we deduce that

$$\begin{aligned} N_1(F; B) &= N_1(G; B) \\ &\ll_\varepsilon B^{1+3/\sqrt{d}+\varepsilon} \log^5 ||G|| \\ &\ll_\varepsilon B^{1+3/\sqrt{d}+\varepsilon} \log^5 B, \end{aligned}$$

which suffices for Theorem 7. In the second case, all the points $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(N)}$ lie on one of at most $O_d(1)$ curves C of degree at most d^2, lying in the surface. By definition of $N_1(F; B)$ these curves have degrees $\delta \geq 2$. Thus Theorem 5 shows that each curve contains at most $O_{\delta,\varepsilon}(B^{1+\varepsilon})$ points, whence

$$N = N_1(F; B) \ll_{\varepsilon,d} B^{1+\varepsilon}$$

in this case. This completes the proof of Theorem 7.

Turning finally to Theorem 9, we see from Theorem 2 that it suffices to take $d \geq 3$. In view of Theorem 6, we will have to estimate the contribution from

lines on the surface S given by $F = 0$. These lines correspond to points in the Grassmannian $\mathbb{G}(1,3) = G$, say. Indeed those lines that lie in the surface S correspond to points of an algebraic subset V, say of G, (the Fano variety $F_1(S)$, see Harris [9; example 6.19]). The set V is defined by $O_d(1)$ equations of degree at most d. The lines that lie in a plane P correspond to points on a plane $P' \subset G$. For a generic plane $P \subset \mathbb{P}^3$ the intersection $P \cap S$ is irreducible, (see Harris [9; Proposition 18.10]) and so contains no lines. Hence there is a plane $P \subset \mathbb{P}^3$ for which the corresponding P' is disjoint from V.

If we choose coordinates so that P consists of points $(0, x, y, z)$, then the Plücker coordinates p_{ij} of the lines in P all have $p_{12} = p_{13} = p_{14} = 0$. We now choose A, B such that $F(0, A, B, 1) \neq 0$. This is clearly possible since $x_1 \nmid F(x_1, x_2, x_3, x_4)$. Then the intersection of G, given by

$$p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} = 0,$$

with the linear space L, given by $p_{12} = Ap_{14}$ and $p_{13} = Bp_{14}$, will be the union of the plane P' with a second plane P'', given by the equations $p_{12} = Ap_{14}$, $p_{13} = Bp_{14}$ and $Ap_{34} - Bp_{24} + p_{23} = 0$. This second plane corresponds to the set of lines passing through the point $(0, A, B, 1)$. By construction none of these lines lie in S, so that P'' is also disjoint from V.

It follows that

$$L \cap V = L \cap G \cap V = (P' \cup P'') \cap V = \emptyset,$$

from which we conclude that every component of V has dimension at most 1. A line in G corresponds to the set of lines in $\mathbb{P}^3$ which lie in a given plane and pass through a given point. At most finitely many of these can be contained in S, whence V cannot contain a line.

Any line that does not pass through two distinct rational points can contribute at most 1 to $N(F; B)$. There are $O(P^{4/3})$ lines to consider so the total contribution from lines which are not defined over $\mathbb{Q}$ is $O(P^{4/3})$. We therefore focus our attention on those lines which are defined over $\mathbb{Q}$. These correspond to rational points lying in V. We re-scale these so as to be primitive integral points, and count the number of such points with height at most Y, say. To do this we shall investigate projections of V onto various linear spaces. Choose a vector $\mathbf{p} \in \mathbb{P}^5$ not lying on V, and a hyperplane H not containing $\mathbf{p}$. Let π be the projection from V to H along $\mathbf{p}$. Then π is a regular map, and the image $\pi(V)$ is therefore a closed algebraic set, with components of dimension at most 1. One can produce a set of defining equations for $\pi(V)$ via elimination theory, and one sees that there will be $O_d(1)$ equations, with degrees bounded in terms of d. To be specific, let $f_i(\mathbf{x}) = 0$ be a suitable set of defining equations for V, and let $\mathbf{h} \in H$. According to Lemma 2, the system of equations $f_i(\lambda\mathbf{p} + \mu\mathbf{h}) = 0$ will have a non-zero solution λ, μ, if and only if $\mathbf{h}$ satisfies a system of polynomial equations $E_j(\mathbf{h}) = 0$. Since $\mathbf{p} \notin V$, we must have $\mu \neq 0$ and $\mathbf{h} \neq 0$ in any such solution. The projection $\pi(V)$ is therefore given by the equations $E_j(\mathbf{h}) = 0$. If these are not homogeneous, then $\mathbf{h}$ must clearly be a

zero of each of their homogeneous components. One therefore obtains in this way a collection of $O_d(1)$ conditions, of degrees $O_d(1)$.

If C is an irreducible component of V, then $\pi(C)$ will be an irreducible component of $\pi(V)$. Since C cannot be a line, it follows that $\pi(C)$ cannot be a point. Moreover, if $\pi(C)$ is a line, then C is planar, lying in a plane P_C, say, containing $\mathbf{p}$. We now choose $\mathbf{p}$ not lying in any of the planes P_C, nor on V. Thus it suffices for some form of degree $O_d(1)$ to be non-vanishing at $\mathbf{p}$. In view of Theorem 1 we can choose an integral point of this type, such that $|\mathbf{p}| \ll 1$. Similarly we can choose a hyperplane H given by $\mathbf{c}.\mathbf{h} = 0$ with $\mathbf{c}$ integral, so that $|\mathbf{c}| \ll 1$ and $\mathbf{p} \notin H$. It then follows that every component C of V projects to a curve in H which is not a line. Moreover we can choose coordinates in H so that points of height at most Y in $\mathbb{P}^5$ project to points of height $O(Y)$. Since no component C projects to a point, it follows that the inverse image of any point on $\pi(C)$ contains $O(1)$ points.

In order to estimate the number of points in V it therefore suffices to estimate the number of points in $\pi(V)$. Clearly we may iterate this process, reducing the problem to one of points on a plane curve. In this case Theorem 3 gives a bound $O_\varepsilon(Y^{1+\varepsilon})$, so that we may conclude that V itself contains $O_\varepsilon(Y^{1+\varepsilon})$ points of height at most Y.

Each line $L \subset S$ which is defined over $\mathbb{Q}$ intersects $\mathbb{Z}^4$ in a lattice Λ, say, of rank 2. If the lattice has determinant Δ, then Lemma 1, part (vi), shows that the line will contain $O(1 + B^2/\Delta)$ points of Z_4 from the cube $\max|x_i| \le B$. However the determinant Δ is merely the height of the corresponding Plücker coordinate vector, which we take to be primitive. The lines in which we are interested arise from the intersection of the surface S with various planes $\mathbf{x}.\mathbf{y} = 0$, with $|\mathbf{y}| \ll B^{1/3}$. There are therefore $O(B^{4/3})$ such lines, so that lines with $\Delta \ge B^2$ contribute $O(B^{4/3})$ to $N(F;B)$. Moreover, as we have just shown, there are $O_\varepsilon(Y^{1+\varepsilon})$ lines with $Y < \Delta \le 2Y$. When $Y \ll B^2$, such lines therefore contribute $O_\varepsilon(B^2Y^\varepsilon)$. Finally we may sum over values of Y running over powers of 2, to obtain an overall contribution $O_\varepsilon(B^{2+2\varepsilon})$ from lines in S. This completes the proof of Theorem 9.

We conclude by remarking that the above method fails for $d = 2$ only because the analogue of Lemma 9 would contain an exponent $4/3 + 16/9d = 20/9 > 2$. The treatment of points on lines in the surface still applies satisfactorily.

7 Binary Forms

This section is devoted to the proof of Theorem 8. It will be convenient to make a linear change of variable so that $G(1,0) \neq 0$. Clearly this has no effect on the conclusion of Theorem 8. Throughout this section, all implied constants may depend on the form G. We shall not mention this dependence explicitly. We begin by defining

$$S(X,C) = \\ \#\{(x,y) \in \mathbb{Z}^2 : 1 \le G(x,y) \le X,\ C < \max(|x|,|y|) \le 2C,\ \text{h.c.f.}(x,y) = 1\},$$

subject to the assumption that $C \gg X^{1/d}$. We observe that if x, y is counted by $S(X, C)$ then there is some factor $x - ay$ of $G(x, y)$ such that $|x - ay| \ll X^{1/d}$. Thus if $C \geq cX^{1/d}$ with a sufficiently large constant c, we will have

$$C \ll |x - a'y| \ll C$$

for every factor with $a' \neq a$. If $x - ay$ divides G with multiplicity e it then follows that $|x - ay|^e C^{d-e} \ll X$. If a is irrational we have $|x - ay| \gg_\varepsilon C^{-1-\varepsilon}$, by Roth's Theorem. If a is rational, we cannot have $x - ay = 0$, since $n \neq 0$. It follows that $|x - ay| \gg 1$ if a is rational. In either case we may use our assumption that $e \leq (d-1)/2$ to deduce that

$$C^{1-d\varepsilon} \leq C^{d-2e-e\varepsilon} \ll_\varepsilon |x - ay|^e C^{d-e} \ll X,$$

whence $C \ll X^2$, say. Thus $S(X, C) = 0$ unless $C \ll X^2$.

We proceed to estimate the contribution to $S(X, C)$ corresponding to a particular value of a. Such a contribution arises from primitive lattice points in the parallelogram $|y| \leq 2C,\ |x - ay| \ll (XC^{e-d})^{1/e}$. According to Lemma 1, part (vii), there are

$$\ll 1 + C(XC^{e-d})^{1/e} = 1 + C^2(XC^{-d})^{1/e} \leq 1 + C^2(XC^{-d})^{2/(d-1)}$$

such points, using once more the assumption that $e \leq (d-1)/2$. It therefore follows that

$$S(X, C) \ll 1 + (X/C)^{2/(d-1)}.$$

We may now sum up for values of $C \ll X^2$, running over powers of 2, to conclude that if

$$S'(X, C) = \\ \#\{(x, y) \in \mathbb{Z}^2 : 1 \leq G(x, y) \leq X,\ \max(|x|, |y|) > C,\ \text{h.c.f.}(x, y) = 1\}$$

then

$$S'(X, C) \ll \log X + (X/C)^{2/(d-1)},$$

for $C \gg X^{1/d}$.

We now set

$$r(n) = \#\{(x, y) \in \mathbb{Z}^2 : n = G(x, y)\}$$

and

$$r_1(n; C) = \#\{(x, y) \in \mathbb{Z}^2 : n = G(x, y),\ \max(|x|, |y|) \leq C\},$$
$$r_2(n; C) = \#\{(x, y) \in \mathbb{Z}^2 : n = G(x, y),\ \max(|x|, |y|) > C\},$$

where $C \gg X^{1/d}$. Then

$$\begin{aligned}\sum_{n\le X} r_2(n;C) &= \sum_{h\ll X^{1/d}} S'(\frac{X}{h^d},\frac{C}{h})\\ &\ll \sum_{h\ll X^{1/d}} \{\log X + (\frac{X}{h^d}\frac{h}{C})^{2/(d-1)}\}\\ &\ll X^{1/d}\log X + (\frac{X}{C})^{2/(d-1)}\sum_{h\ll X^{1/d}} h^{-2}\\ &\ll X^{1/d}\log X + (\frac{X}{C})^{2/(d-1)}. \qquad (7.1)\end{aligned}$$

The sum $\sum r_1(n;C)$ is trivially $O(C^2)$, whence

$$\sum_{n\le X} r(n) \ll C^2 + X^{1/d}\log X + (\frac{X}{C})^{2/(d-1)} \ll X^{2/d},$$

on choosing $C = cX^{1/d}$ with an appropriate constant c. This bound shows that there are $O(X^{2/d})$ positive integers $n \le X$ represented by G.

If n has two inequivalent representations $G(x,y) = n$, then either $r_2(n;C)$ is positive, or there is a point (x_1,x_2,x_3,x_4) on the surface

$$E(\mathbf{x}) = G(x_1,x_2) - G(x_3,x_4) = 0,$$

satisfying $|x_i| \le C$, but for which (x_1,x_2) and (x_3,x_4) are not related by an automorphism. We shall let $\mathcal{N}(C)$ denote the number of such points. We now claim that

$$\mathcal{N}(C) \ll_\varepsilon C^{52/27+\varepsilon}, \qquad (7.2)$$

and that the form G has $O(1)$ automorphisms. It will then follow that

$$\sum_{n\le X} r_1(n;C)^2 \le \mathcal{N}(C) + O(\sum_{n\le X} r_1(n;C)) \ll C^2.$$

If $G(1,0) > 0$ we trivially have

$$\sum_{n\le X} r_1(n;C) \gg C^2$$

if $C = cX^{1/d}$ with a sufficiently small constant c, since then $\max(|x|,|y|) \le C$ implies $|G(x,y)| \le X$, and a positive proportion of such pairs x,y will have $G(x,y) > 0$. It now follows via Cauchy's inequality that $r_1(n;C) > 0$ for $\gg C^2$ positive integers $n \le X$. Thus the number of such integers represented by G has exact order $X^{2/d}$, as claimed in Theorem 8.

For integers n with two or more essentially different representations, we observe as above that either $r_2(n;C) > 0$ or the representations are counted by

$\mathcal{N}(C)$. Thus the number of such integers will be

$$\begin{aligned} &\leq \quad \mathcal{N}(C) + \sum_{n \leq X} r_2(n; C) \\ &\ll_\varepsilon \quad C^{52/27+\varepsilon} + X^{1/d} \log X + (\frac{X}{C})^{2/(d-1)} \\ &\ll_\varepsilon \quad X^{52/(1+26d)+\varepsilon}, \end{aligned}$$

by (7.1) and (7.2), on choosing $C = X^{27/(1+26d)}$. This completes the proof of Theorem 8, subject to the claims made above.

We therefore turn to the consideration of integral points on the surface $E(\mathbf{x}) = G(x_1, x_2) - G(x_3, x_4) = 0$, in the cube $\max |x_i| \leq C$. We shall show that E has no rational linear or quadratic factor. Suppose to the contrary that there is such a factor. Set $x_1 = x$, $x_2 = 0$, $x_3 = a$ and $x_4 = 1$. Then $E(\mathbf{x})$ reduces to $Ax^d - B$, where $A = G(1, 0)$ and $B = G(a, 1)$ Thus $Ax^d - B$ has a rational linear, or quadratic factor, for every integral a. It follows that B/A is always an exact d-th power, or, if d is even, an exact $d/2$-th power. This implies that $G(x, y)$ is a perfect d-th power, or, if d is even, a perfect $d/2$-th power. However our assumption about the multiplicity of the factors of G shows that this is impossible.

We can now apply Theorem 6 to each factor of $E(\mathbf{x})$ to show that

$$N_1(E; Y) \ll_\varepsilon Y^{52/27+\varepsilon}.$$

If $\mathcal{N}^{(*)}(C)$ denotes the number of integral zeros of E, not necessarily primitive, lying in the cube $|x_i| \leq C$, but not on any line in the surface $E = 0$, then we conclude that

$$\begin{aligned} \mathcal{N}^{(*)}(C) \quad &= \quad 1 + \sum_{h \ll C} N_1(E; B/h) \\ &\ll_\varepsilon \quad 1 + \sum_h (C/h)^{52/27+\varepsilon} \\ &\ll_\varepsilon \quad C^{52/27+\varepsilon}. \end{aligned}$$

The contribution to $\mathcal{N}(C)$ from points not lying on lines in the surface $E = 0$ is thus $O_\varepsilon(C^{52/27+\varepsilon})$, in accordance with (7.2).

Lines in $\mathbb{P}^3$ may be classified into two types, given respectively by pairs of equations

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 = 0, \quad b_3x_3 + b_4x_4 = 0,$$

and

$$x_1 = a_1x_3 + a_2x_4, \quad x_2 = a_3x_3 + a_4x_4.$$

A little thought shows that if a line of the first type lies in the surface $E(\mathbf{x}) = 0$, then the points on it must satisfy $G(x_1, x_2) = G(x_3, x_4) = 0$, since G is not a d-th power. Such points therefore correspond to the excluded value $n = 0$.

Similarly, lines of the second type for which $a_1a_4 = a_2a_3$ also produce values with $G(x_1, x_2) = G(x_3, x_4) = 0$. The remaining lines produce automorphisms

$$G(a_1x + a_2y, a_3x + a_4y) = G(x, y). \tag{7.3}$$

Indeed, if the a_i are rational, the corresponding points produce equivalent solutions of $G(x, y) = n$, in the sense of Theorem 8. Thus points counted by $\mathcal{N}(C)$ which lie on lines in the surface $E = 0$ must lie on lines that correspond to irrational automorphisms.

We claim that there are only finitely many automorphisms, rational or irrational. Since any line which is not defined over $\mathbb{Q}$ contains at most $O(C)$ integral points (not necessarily primitive), we will be able to conclude that lines corresponding to irrational automorphisms contribute $O(C)$ to $\mathcal{N}(C)$. We will then have $\mathcal{N}(C) \ll_\varepsilon C^{52/27+\varepsilon}$, as required for (7.2).

It remains to prove that there are finitely many automorphisms. The automorphisms of G form a group, which acts on the roots of the polynomial $G(x, 1)$. Specifically, the automorphism (7.3) maps a root α by

$$\alpha \mapsto \frac{a_1\alpha + a_2}{a_3\alpha + a_4}. \tag{7.4}$$

The condition on the multiplicity of the factors of G implies that there are at least 3 different roots α. For an automorphism which fixed every root α, one would have a quadratic equation

$$a_3\alpha^2 + (a_4 - a_1)\alpha - a_2 = 0$$

with three distinct roots. This would entail $a_1 = a_4$ and $a_2 = a_3 = 0$. One would then deduce from (7.3) that the common value of a_1 and a_4 must be a d-th root of unity. If we factor the group of automorphisms by the subgroup consisting of scalar multiples of d-th root of unity, the quotient still acts on the roots α by the formula (?), and the action is now faithful. The quotient group is thus isomorphic to a subgroup of the symmetric group S_d. We conclude that there are at most $d.d!$ automorphisms.

8 Non-Singular Surfaces

In this section we shall prove Theorems 10 and 11. The argument for Theorem 10 begins in exactly the same way as for Theorem 6, and indeed, Lemma 9 shows that the contribution from planes $\mathbf{x}.\mathbf{y} = 0$ for which $G_{\mathbf{y}}$ is irreducible over $\mathbb{Q}$ is satisfactory.

We therefore consider the possibility that $G_{\mathbf{y}}$ factors. In this case $G_{\mathbf{y}}$ is a singular form, so that $\mathbf{y}$ lies on the dual surface $\hat{F}(\mathbf{y}) = 0$. We proceed to show that $\hat{F}$ cannot be linear. Since $\hat{F}(\nabla F(\mathbf{x}))$ vanishes on $F(\mathbf{x}) = 0$ we have $F(\mathbf{x})|\hat{F}(\nabla F(\mathbf{x}))$. Hence if $\hat{F}$ were linear we would deduce that $\hat{F}(\nabla F(\mathbf{x}))$ must vanish identically. Taking $\hat{F}(\mathbf{y})$ to have the shape $\mathbf{h}.\mathbf{y} = 0$ we would then have

$\mathbf{h}.\nabla F(\mathbf{x}) = 0$ identically in $\mathbf{x}$. On taking the partial derivative with respect to x_j, say, we conclude that

$$\sum_{i=1}^{4} h_i \frac{\partial^2 F(\mathbf{x})}{\partial x_i \partial x_j} = 0.$$

If we substitute $\mathbf{h}$ for $\mathbf{x}$ this yields

$$\frac{\partial F}{\partial x_j}(\mathbf{h}) = 0,$$

and since j is arbitrary we have $\nabla F(\mathbf{h}) = 0$. This would contradict the assumption that F is non-singular, so that $\hat{F}$ cannot be linear.

We may now apply Theorem 9, to show that there can be $O_\varepsilon(B^{2/3+\varepsilon})$ possible vectors $\mathbf{y}$ with $|\mathbf{y}| \ll B^{1/3}$. Let H be a factor of $G_{\mathbf{y}}$ irreducible over $\mathbb{Q}$, and suppose that H has degree e. According to Theorem 3 and Corollary 1, the number of points $(\lambda_1, \lambda_2, \lambda_3)$, with $|\lambda_i| \ll B$, which satisfy $H(\lambda_1, \lambda_2, \lambda_3) = 0$, will be $O_\varepsilon(B^{2/e+\varepsilon})$. When $e \geq 3$, such factors H produce a total contribution $O_\varepsilon(B^{4/3+\varepsilon})$, after allowing for $O_\varepsilon(B^{2/3+\varepsilon})$ possible $\mathbf{y}$. This is satisfactory. For $e = 2$ we get an estimate $O_\varepsilon(B^{5/3+\varepsilon})$ in an analogous fashion. This too will be satisfactory providing that $d \leq 5$.

It remains to consider the possibility of quadratic factors H of $G_{\mathbf{y}}$, when F has degree $d \geq 6$. However Theorem 14 then shows that the surface $F = 0$ contains $O(1)$ plane quadrics, so that $G_{\mathbf{y}}$ can have a quadratic factor for at most $O(1)$ values of $\mathbf{y}$. Each such factor produces $O_\varepsilon(B^{1+\varepsilon})$ points, giving a total contribution to $N(F; B)$ of $O_\varepsilon(B^{1+\varepsilon})$. This suffices for Theorem 10.

We turn now to Theorem 11. Our argument begins in precisely the same way as was used in §6, for Theorem 7. Thus every point on the surface $F(\mathbf{x}) = 0$, contained in the cube $|x_i| \leq B$, lies on one of

$$\ll_\varepsilon B^{3/\sqrt{d}+\varepsilon} \log^5 ||F||$$

curves C. Moreover the degree δ of any such curve is $O(1)$. To estimate the number of points on such a curve C, we again apply Theorem 5, to conclude that there are $O_\varepsilon(B^{2/(d-1)+\varepsilon})$ points lying on C whenever $\delta \geq d-1$. Thus there are a total of $O_\varepsilon(B^{3/\sqrt{d}+2/(d-1)+\varepsilon} \log^5 ||F||)$ points lying on the available collection of curves C of degree $d-1$ or more. This shows that

$$N_2(F; B) \ll_\varepsilon B^{3/\sqrt{d}+2/(d-1)+\varepsilon} \log^5 ||F||. \tag{8.1}$$

To bound $N_1(F; B)$, we observe, by Theorem 14, that there are $O(1)$ curves C remaining. Lines defined over $\mathbb{Q}$ are excluded, by definition of $N_1(F; B)$, and other lines contribute $O(1)$ each. Thus Theorem 5, with $2 \leq \delta \leq d-2$, provides a bound $O_\varepsilon(B^{1+\varepsilon})$ for each of the remaining curves, whence

$$N_1(F; B) \ll_\varepsilon B^{1+\varepsilon} + B^{3/\sqrt{d}+2/(d-1)+\varepsilon} \log^5 ||F||. \tag{8.2}$$

Finally, we note that the analogues in $\mathbb{P}^3$ of the bounds (1.3) and (1.4) show that curves of genus at least 1, and degree at most $d-2$, contribute $O_{\varepsilon,F}(B^\varepsilon)$,

so that (8.1) implies (1.16). As in Corollary 1, we may in fact restrict attention to curves defined over the rationals in applying the analogues of (1.3) and (1.4).

As in §6 we have to eliminate the factor $\log^5 ||F||$ from (8.1) and (8.2), and we apply the same technique. In the case of (8.2) the argument is exactly as before. For the bound (8.1) we take $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(N)}$ to be the complete set of solutions of $F(\mathbf{x}) = 0$ in the region $|\mathbf{x}^{(i)}| \ll B$, excepting any that lie on curves of degree at most $d-2$ in the surface. This time we have must have $\delta \geq d-1$ for the curves C arising in the second case, so that

$$N = N_2(F; B) \ll_\varepsilon B^{2/(d-1)+\varepsilon}.$$

As before this is sufficient.

9 Sums of 3 Powers

This section will be devoted to the proof of Theorem 13. We shall take $F(\mathbf{x}) = x_1^d + x_2^d + x_3^d - Nx_4^d$, and consider points with $0 < x_1, x_2, x_3 \leq B$ and $x_4 = 1$. Such points have $\mathbf{x} \in Z_4$, and lie in the box $|x_i| \leq B_i$, with $B_1 = B_2 = B_3 = B$ and $B_4 = 1$, so that we have $V = B^3$ and $T = B^d$, in the notation of Theorem 14. An application of Theorem 14 therefore shows that our points lie on one of $O_\varepsilon(B^{2/\sqrt{d}+\varepsilon})$ curves, each having degree $O_\varepsilon(1)$. If such a curve has degree $D \geq d-1$, Theorem 5 then shows that there are $O_\varepsilon(B^{2/D+\varepsilon})$ corresponding points. This produces a total of $O_\varepsilon(B^{\theta+\varepsilon})$ points, with $\theta = 2/\sqrt{d} + 2/(d-1)$, as in Theorem 13. This is acceptable.

We now turn to curves C of degree at most $d-2$. Let $\theta : \mathbb{P}^3 \to \mathbb{P}^3$ be the map

$$\theta(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, N^{1/d} x_4).$$

Then $\theta(C)$ is a curve of degree at most $d-2$, lying in the non-singular surface S, given by $y_1^d + y_2^d + y_3^d - y_4^d = 0$. According to Theorem 14 there are $O(1)$ such curves, $C_1, \dots, C_t$, say. Clearly t and the curves C_i depend only on d and not on N. Since the point $(0, 0, 0, 1)$ does not lie on the surface $x_1^d + x_2^d + x_3^d - Nx_4^d = 0$, it cannot lie on the curve C, so that the projection

$$\pi(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3)$$

is a regular map from C to a curve $\pi(C)$ in $\mathbb{P}^2$. Similarly π is a regular map from each C_i to a curve $\pi(C_i) = \Gamma_i$, say in $\mathbb{P}^2$. It is clear from the definitions that $\pi\theta = \pi$. Thus if $\theta(C) = C_i$, then $\pi(C) = \pi(C_i) = \Gamma_i$. It follows that if $(x_1, x_2, x_3, 1)$ lies on a curve C, then (x_1, x_2, x_3) lies on one of $O(1)$ curves Γ_i, which are independent of N. If Γ_i is not defined over $\mathbb{Q}$ then it has $O(1)$ rational points, by Corollary 1. Similarly if the genus of Γ_i is 2 or more, we deduce from Faltings' Theorem (1.4) that there are $O(1)$ rational points. In these cases (x_1, x_2, x_3) is a scalar multiple of one of $O(1)$ points. At most one such scalar multiple can satisfy the additional relation $x_1^d + x_2^d + x_3^d = N$. If Γ_i has genus 1, it follows from (1.3) that there are $O_\varepsilon(B^\varepsilon)$ possible points (x_1, x_2, x_3), up to multiplication by scalars, and again there can be at most one admissible scalar

multiple for each value of N. We therefore conclude that there are $O_\varepsilon(B^\varepsilon)$ solutions to $x_1^d + x_2^d + x_3^d = N$, corresponding to points on curves C for which $\pi(C) = \Gamma_i$ has positive genus.

It remains to consider the possibility that $\pi(C) = \Gamma_i$ is defined over $\mathbb{Q}$ and has genus zero. We shall assume, as we clearly may, that the curve has infinitely many rational points. We proceed to show that Γ_i can be parameterized. Write the curve in affine coordinates as $f(x, y) = 0$, where $f(x, y) \in \mathbb{Q}[x, y]$ is absolutely irreducible. We may clearly choose the coordinates so that at most finitely many points lie at infinity. According to Eichler [5; page 139] there are two possibilities. It may happen that the function field $\mathbb{Q}(x, y)$ is a rational function field $\mathbb{Q}(z)$ for some $z \in \mathbb{Q}(x, y)$. Alternatively, we may have $\mathbb{Q}(x, y) = \mathbb{Q}(u, v)$ where $g(u, v) = 0$ for some quadratic polynomial $g(u, v) \in \mathbb{Q}[u, v]$ having the property that $g(a, b) = 0$ has no rational solutions a, b. In this second case we may write u and v as rational functions

$$u(x, y) = U(x, y)/W(x, y), \quad v(x, y) = V(x, y)/W(x, y),$$

where $U(x, y), V(x, y), W(x, y) \in \mathbb{Z}[x, y]$ and $f(x, y) \nmid W(x, y)$. Now, if we have a rational point (a_1, a_2, a_3) on Γ_i and $a_3 \neq 0$, then $f(b_1, b_2) = 0$ with $b_1 = a_1/a_3$, $b_2 = a_2/a_3$. Thus if $W(a_1/a_3, a_2/a_3) \neq 0$ we see that

$$c_1 = \frac{U(a_1/a_3, a_2/a_3)}{W(a_1/a_3, a_2/a_3)}, \quad c_2 = \frac{V(a_1/a_3, a_2/a_3)}{W(a_1/a_3, a_2/a_3)},$$

is a rational solution of $g(c_1, c_2) = 0$. This contradiction would show, in this second case, that every rational point (a_1, a_2, a_3) on Γ_i would have to satisfy either $a_3 = 0$ or $W(a_1/a_3, a_2/a_3) = 0$. Since $f(x, y) \nmid W(x, y)$ this allows only finitely many points, which again contradicts our initial assumptions. Thus we must be in the first case, in which $\mathbb{Q}(x, y) = \mathbb{Q}(z)$ for some $z \in \mathbb{Q}(x, y)$.

We now revert to the projective formulation of the curve Γ_i. ¿From the fact that $\mathbb{Q}(x, y) = \mathbb{Q}(z)$ we conclude that there are integral binary forms $f_1(u, v), f_2(u, v)$ and $f_3(u, v)$, with no common factor, such that, if $\mathbf{x}$ lies on Γ_i, then it is proportional to $(f_1(u, v), f_2(u, v), f_3(u, v))$ for some (u, v). Moreover there are coprime forms $u(\mathbf{x}), v(\mathbf{x}) \in \mathbb{Z}[x_1, x_2, x_3]$ whose ratio is non-constant on Γ_i, such that the appropriate values of u and v may be given by $u = u(\mathbf{x})$ and $v = v(\mathbf{x})$. Thus a rational point $\mathbf{x}$ on $\pi(C)$ will be a non-zero rational scalar multiple of $(f_1(u, v), f_2(u, v), f_3(u, v))$ for some primitive $(u, v) \in \mathbb{Z}^2$, except in a finite number of cases. These exceptions arise when $f_i(u, v) = 0$ for $i = 1, 2, 3$ and $u = u(\mathbf{x}), v = v(\mathbf{x})$, and hence there are $O(1)$ of them. We therefore see that, apart from these exceptions, the relevant points on the curve C are given by solutions of

$$\lambda^d(f_1(u, v)^d + f_2(u, v)^d + f_3(u, v)^d) = N, \quad \lambda \in \mathbb{Q}, \ \ u, v \in \mathbb{Z}, \ \ (u, v) = 1.$$

Since the forms f_i have no common factor there will be relations of the type

$$\sum_{i=1}^{3} g_i(u, v) f_i(u, v) = Gu^r, \quad \sum_{i=1}^{3} h_i(u, v) f_i(u, v) = Hv^r.$$

Here $g_i(u,v), h_i(u,v)$ are integral forms, and G, H are non-zero integer constants. We note that $\lambda f_i(u,v)$ must be integral for $i = 1,2,3$, in order to produce integral values of x_i. Since u and v are coprime, it follows that the denominator of λ must divide GH, and hence can take only $O(1)$ values. Setting $\lambda = \mu/\nu$ with μ, ν coprime, we have $\mu^d | N$, so that μ takes $O_\varepsilon(N^\varepsilon)$ values.

It remains to consider the number of solutions in u, v that the Thue equation

$$f_1(u,v)^d + f_2(u,v)^d + f_3(u,v)^d = \nu^d \mu^{-d} N \tag{9.1}$$

may have. We shall write $f(u,v)$ for the form on the left-hand side. Recall that μ, ν and the form f may be considered as fixed. Suppose firstly that f has two distinct rational factors, f' and f'', say, both irreducible over $\mathbb{Q}$. Then $f'(u,v) = N'$ and $f''(u,v) = N''$ for certain factors N', N'' of $\nu^d \mu^{-d} N$. These two equations determine $O(1)$ values of u, v, by elimination, so that (9.1) has $O_\varepsilon(N^\varepsilon)$ solutions. There remains the possibility that f is a power of an irreducible form f' say, in which case we have to consider solutions of an equation $f'(u,v) = N'$. If f' has degree 3 or more we can apply the result of Lewis and Mahler [25], which shows that there are $O(A^{\omega(N')})$ such solutions, with a constant A depending only on f'. Our construction shows that this latter form is one of a finite set, independent of N. There are therefore $O_\varepsilon(N^\varepsilon)$ solutions in this case.

When f' has degree two the equation $f'(u,v) = N'$ will have $O_\varepsilon(N^\varepsilon)$ solutions, providing that the variables u, v can be bounded by powers of N. Since we assumed that the forms f_i had no common factor, we may take f_1, say, to be coprime to f'. However if $f'(u,v) \ll N$ then $u/v - \alpha \ll N/|v|$, for some root α of $f'(X,1)$ (unless $v = 0$). Similarly, from $f_1(u,v) \ll N$ we have $u/v - \beta \ll N/|v|$ for some root β of $f_1(X,1)$, unless $v = 0$. Since f' and f_1 are coprime we will have $\alpha \neq \beta$, and hence $N/|v| \gg 1$. It follows that $v \ll N$, whether or not $v \neq 0$. Similarly we have $u \ll N$. This gives us the necessary bounds on u and v.

We have therefore shown that the equation (9.1) has $O_\varepsilon(N^\varepsilon)$ solutions, except possibly when the form $f(u,v)$ on the left hand side is a constant multiple of a power of a rational linear function $L(u,v)$, say. In this last case, we may make an appropriate linear change of variable, invertible over $\mathbb{Z}$, so that we actually have $f(u,v) = cv^{dk}$ for some $k \in \mathbb{N}$ and some non-zero integer constant c. We have therefore to ask whether an identity of the form

$$f_1(u,v)^d + f_2(u,v)^d + f_3(u,v)^d = cv^{dk} \tag{9.2}$$

is possible, with coprime integral forms f_i of degree k. If $f_i(u,v)$ has leading term $a_i u^k$ in u, we will have $a_1^d + a_2^d + a_3^d = 0$. Thus d must be odd, and in view of Wiles' proof of Fermat's Last Theorem [31], we may assume that $a_2 = -a_1$ and $a_3 = 0$. Since we then have $v^d | f_3(u,v)^d$ and $v^d | cv^{dk}$ we conclude that $v^d | f_1(u,v)^d + f_2(u,v)^d$. However

$$\begin{aligned} & f_1^{d-1} - f_1^{d-2} f_2 + \ldots - f_1 f_2^{d-2} + f_2^{d-1} \qquad (9.3) \\ \equiv\ & (a_1^{d-1} - a_1^{d-2} a_2 + \ldots - a_1 a_2^{d-2} + a_2^{d-1}) u^{(d-1)k} \pmod{v}, \end{aligned}$$

and $a_1^{d-1} - a_1^{d-2}a_2 + \ldots - a_1a_2^{d-2} + a_2^{d-1} = da_1^{d-1}$, since $a_2 = -a_1$. Moreover $a_1 \neq 0$, for otherwise the forms f_i would not be coprime. It follows that the expression (9.3) is coprime to v, and hence that $v^d | f_1(u,v) + f_2(u,v)$. We cannot have $f_2(u,v) = -f_1(u,v)$ since the parameterization could not then produce solutions in positive integers. It follows that the degree k of the forms f_i must be at least d. The relations (9.1) and (9.2) show that μ, ν and N determine $|v|$, and that $v \ll N^{1/dk} \ll B^{1/k} \ll B^{1/d}$. Then, from $f_1(u,v) \ll N^{1/d}$, we deduce that $u - \alpha v \ll N^{1/dk}$, for soome factor $u - \alpha v$ of $f_1(u,v)$. Thus $u \ll |\alpha v| + N^{1/dk} \ll B^{1/d}$. It therefore follows finally that a curve Γ_i of genus 0 contributes $O(B^{1/d})$ points, which is satisfactory for Theorem 13.

References

[1] M.A. Bennett, N.P. Dummigan and T.D. Wooley, The representation of integers by binary additive forms, *Compositio Math.,* 111 (1998), 15-33.

[2] E. Bombieri and J. Pila, The number of integral points on arcs and ovals, *Duke Math. J.,* 59 (1989), 337-357.

[3] S.D. Cohen, The distribution of Galois groups and Hilbert's irreducibility theorem, *Proc. London Math. Soc. (3),* 43 (1981), 227-250.

[4] H. Davenport, Cubic forms in 16 variables, *Proc. Roy. Soc. A,* 272 (1963), 285-303.

[5] M. Eichler, *Introduction to the theory of algebraic numbers and functions,* (Academic Press, London, 1966).

[6] N.D. Elkies, Rational points near curves and small nozero $|x^3 - y^2|$ via lattice reduction, *to appear.*

[7] P. Erdős and K. Mahler, On the number of integers that can be represented by a binary form, *J. London Math. Soc.,* 13 (1938), 134-139.

[8] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.,* 73 (1983), 349-366.

[9] J. Harris, *Algebraic geometry,* (Springer, Berlin, 1995).

[10] D.R. Heath-Brown, Cubic forms in ten variables, *Proc. London Math. Soc. (3),* 47 (1983), 225-257.

[11] D.R. Heath-Brown, Diophantine approximation with square-free numbers, *Math. Zeit.,* 187 (1984), 335-344.

[12] D.R. Heath-Brown, The density of rational points on non-singular hypersurfaces, *Proc. Indian Acad. Sci. (Math. Sci.),* 104 (1994), 13-29.

[13] D.R. Heath-Brown, The density of rational points on cubic surfaces, *Acta Arithmetica,* 79 (1997), 17-30 .

[14] D.R. Heath-Brown, Counting rational points on cubic surfaces, *Astérisque,* 251 (1998), 13-29.

[15] D.R. Heath-Brown, The circle method and diagonal cubic forms, *Phil. Trans. Roy. Soc. London,* A 356 (1998), 673-699.

[16] C. Hooley, On binary cubic forms, *J. Reine Angew. Math.* 226 (1967), 30-87.

[17] C. Hooley, On the representations of a number as the sum of four cubes: I, *Proc. London Math. Soc. (3),* 36 (1978), 117-140.

[18] C. Hooley, On another sieve method and the numbers that are a sum of two h-th powers, *Proc. London Math. Soc. (3),* 43 (1981), 73-109.

[19] C. Hooley, On binary quartic forms, *J. Reine Angew. Math.,* 366 (1986), 32-52.

[20] C. Hooley, On another sieve method and the numbers that are a sum of two h-th powers. II, *J. Reine Angew. Math.,* 475 (1996), 55-75.

[21] C. Hooley, On Hypothesis K^* in Waring's problem, *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995),* 175-185, London Math. Soc. Lecture Note Ser., 237, (Cambridge Univ. Press, Cambridge, 1997).

[22] C. Hooley, On binary cubic forms: II, *J. Reine Angew. Math.,* 521 (2000), 185-240.

[23] C. Hooley, On the rational points on cubic surfaces, *Glasgow Math. J.,* 42 (2000), 225-237.

[24] L.-K. Hua, On Waring's problem, *Quart. J. Math. Oxford Ser.,* 9 (1938), 199-202.

[25] D.J. Lewis and K. Mahler, On the representation of integers by binary forms, *Acta Arith.,* 6 (1960/61), 333-363.

[26] K. Mahler, A note on hypothesis K of Hardy and Littlewood, *J. London Math. Soc.,* 11 (1936), 136-138.

[27] J. Pila, Density of integral and rational points on varieties, *Astérisque,* 228 (1995), 183-187.

[28] J. Pila, Density of integer points on plane algebraic curves, *Internat. Math. Res. Notices,* 18 (1996), 903-912.

[29] W.M. Schmidt, Integer points on hypersurfaces, *Monatsh. Math.,* 102 (1986), 27-58.

[30] C. M. Skinner and T.D. Wooley, Sums of two k-th powers, *J. Reine Angew. Math.,* 462 (1995), 57-68.

[31] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2),* 141 (1995), 443-551.

Mathematical Institute,
24-29, St. Giles',
Oxford OX1 3LB
England

rhb@maths.ox.ac.uk

Appendix

J.-L. Colliot-Thélène
Orsay

Throughout this appendix the ground field is algebraically closed of characteristic zero.

Proposition 1 *Let $X \subset \mathbb{P}^3$ be a smooth projective surface. If the number of reduced and irreducible curves C of degree d lying on X is not finite, then there exists such a curve $C \subset X$ whose self-intersection $(C.C)$ is nonnegative.*

For the proof we let G denote the open set of the Hilbert scheme of curves in $\mathbb{P}^3$ corresponding to integral (i.e. reduced and irreducible) curves of degree d. This is a scheme of finite type over the ground field. Let $W \subset G \times \mathbb{P}^3$ be the reduced closed subset whose points are pairs (c, x) where c is a point with associated curve C and $x \in \mathbb{P}^3$ lies on C. For each $c \in G$, the fibre of $W \to G$ above c is just the projective integral curve C.

Let $Z \subset G \times X$ be the trace of W on $G \times X$. The projection map $Z \to G$ is projective. Its image is a closed subset $F \subset G$. A curve C with associated point c lies on X if and only if c belongs to F, and the inverse image of such a c in Z is precisely the curve $C \subset X$. If each component of F is of dimension zero, then F is finite, and there are only finitely many curves C of degree d lying on X. If that is not the case, then F contains at least one irreducible curve T. Two distinct fibres C_0 and C_1 of $Z \to G$ above rational points of T define integral curves in the same algebraic family on X. Hence $(C_0.C_0) = (C_0.C_1) \geq 0$, as claimed.

Proposition 2 *Let $X \subset \mathbb{P}^3$ be a smooth projective surface of degree n and let $C \subset X$ be a reduced and irreducible curve, possibly singular, of degree d in $\mathbb{P}^3$. If $n > d+1$, then the intersection number $(C.C)$ of C on the surface X is strictly negative.*

The canonical sheaf K on X is $\mathcal{O}_X(n-4)$. The formula for the arithmetic genus of $C \subset X$ is well known to be

$$2p_a(C) - 2 = (C.C) + (C.K) = (C.C) + (n-4)d$$

(see [3; Chapter V, Exercise 1.3, page 366]). Here one should recall that $p_a(C)$ is by definition the dimension of $H^1(C, \mathcal{O}_C)$.

Suppose first that C is contained in a plane $\mathbb{P}^2 \subset \mathbb{P}^3$. Then the formula for the arithmetic genus of $C \subset \mathbb{P}^2$ is

$$2p_a(C) - 2 = d(d-3).$$

Thus

$$(C.C) + (n-4)d = d(d-3),$$

and hence

$$(C.C) = d(d+1-n)$$

is strictly negative as soon as $n > d+1$.

Suppose that C is not contained in a plane, hence in particular $d \geq 3$. In classical parlance, such a curve is called nondegenerate. For such curves we have the Castelnuovo bound : If d is even, $p_a(C) \leq (d^2/4) - d + 1$; if d is odd, $p_a(C) \leq (d^2-1)/4 - d + 1$.

Comparing with the formula for $p_a(C)$, we find that $(C.C) < 0$ if $n > d/2+2$, whether d is even or odd. This completes the proof of the proposition.

Let us comment on the Castelnuovo bound. Standard textbooks give the Calstelnuovo bound for the genus $g(C)$ of smooth nondegenerate curves $C \subset \mathbb{P}^3$, see [3; Theorem IV.6.4, page 351], for example. (See also [2; page 116]). However the whole argument is valid for reduced, irreducible, local complete intersection curves such as the ones under consideration here. Indeed, the proof uses the Riemann-Roch theorem for the curve C, and it uses a General Position Lemma, to the effect that the section of C by a sufficiently general plane in $\mathbb{P}^3$ consists of d distinct points, no three of which are on a line. The General Position Lemma lemma is valid for singular (reduced, irreducible) curves ([2; page 109]; see also [4] and references therein – this reference was pointed out to me by D. Perrin). A proof of the Riemann-Roch theorem for (possibly singular) curves given as divisors on a surface (such curves are automatically local complete intersections) may be found in [1; Chapter VII, Section 1] (combine theorem (1.4), theorem (1.15) and Remark (1.17)).

Proposition 3 *If for each nonsingular surface $X \subset \mathbb{P}^3$ of degree n the number of curves C of degree d lying on X is finite, then there is an integer $N(n,d)$ such that any nonsingular surface $X \subset \mathbb{P}^3$ of degree n contains at most $N(n,d)$ curves of degree d.*

Let $W \subset \mathbb{P}(H^0(\mathbb{P}^3, \mathcal{O}(n)))$ be the open set corresponding to nonsingular surfaces of degree n. Let $Z \subset G \times W$ be the closed set whose points are pairs of points (c, f) with c corresponding to an integral curve C of degree d lying on the surface X defined by f. The projection map $Z \to W$ is a proper morphism. By hypothesis, any fibre of this morphism is finite, i.e. the morphism $Z \to W$ is quasi-finite. Being both proper and quasi-finite, the morphism $Z \to W$ is finite, see [3; exercise III.11.2, page 280]. This implies the existence of an integer N such that any fibre has at most N points.

Remark. Computing dimensions, one sees that for n big enough with respect to the degree, the general surface of degree n contains no (reduced, irreducible) curve of degree d at all.

Gathering the three propositions together, we conclude as follows.

Theorem *For each pair n, d of positive integers with $n > d+1$, there exists an integer $N(n,d)$ such that for any smooth projective surface $X \subset \mathbb{P}^3$ of degree*

n, there are at most $N(n,d)$ reduced and irreducible curves of degree d lying on X.

Remark. From this one may conclude an analogous result where one omits the condition 'reduced and irreducible'. Indeed an effective Cartier divisor $C \subset X$ of degree d in $\mathbb{P}^3$ defines a divisor $\sum_i n_i C_i$ with $n_i > 0$, where each C_i is an integral curve of degree d_i, and the sum $\sum_i n_i d_i$ is equal to d.

References

[1] A. Altman, S. Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics **146**, Springer-Verlag, 1970.

[2] E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris, *Geometry of algebraic curves,* Vol. I. (Springer, Berlin, 1985).

[3] R. Hartshorne, *Algebraic geometry*, (Springer, Berlin, 1977).

[4] R. Hartshorne, The genus of space curves, Ann. Univ. Ferrara - Sez. VII - Sc. Mat. **vol. XL** (1994) 207-223.

C.N.R.S., UMR 8628
Mathématiques
Bâtiment 425
Université de Paris-Sud
F-91405 Orsay, France

colliot@math.u-psud.fr