Astérisque

ROGER HEATH-BROWN

Counting rational points on cubic surfaces

Astérisque, tome 251 (1998), p. 13-30

<http://www.numdam.org/item?id=AST_1998__251__13_0>

Astérisque **251**, 1998, p. 13–29

COUNTING RATIONAL POINTS ON CUBIC SURFACES

by

Roger Heath-Brown

Abstract. — Let $F[W, X, Y, Z]$ be a rational cubic form, and let $N^{(0)}(R)$ be the number of rational zeros of F of height at most R, which do not lie on any rational line in the surface $F = 0$. We show that

$$N^{(0)}(R) \ll_{\varepsilon, F} R^{4/3+\varepsilon}$$

for any fixed $\varepsilon > 0$, subject to a suitable hypothesis on the size of the rank of elliptic curves. For the proof one counts points on the cubic curves obtained from hyperplane sections of the surface $F = 0$.

1. Introduction

For any cubic form $F(W, X, Y, Z) \in \mathbb{Z}[W, X, Y, Z]$ let

$$N_F(R) = N(R) = \#\{\mathbf{x} \in \mathbb{Z}^4 : \ F(\mathbf{x}) = 0, \ |\mathbf{x}| \leqslant R, \ \mathbf{x} \text{ primitive}\},$$

where $|\mathbf{x}|$ is the Euclidean length of $\mathbf{x}$, and an integer vector $\mathbf{x} = (x_1, \ldots, x_n)$ is defined to be primitive if $\mathbf{x} \neq \mathbf{0}$ and $x_1, \ldots, x_n$ have no common factor. We are concerned here with the size of $N(R)$ as R tends to infinity. If the surface $F = 0$ contains a rational line, then there will be $cR^2 + O_\varepsilon(R^{1+\varepsilon})$ primitive points on that line, counted by $N(R)$, for any positive ε and an appropriate constant $c > 0$. One would expect that such 'trivial' points greatly outnumber the remaining 'non-trivial' points and we therefore define $N^{(0)}(R)$ to be the number of points $\mathbf{x}$ counted by $N(R)$, such that $\mathbf{x}$ does not lie on any rational line in the surface $F = 0$. There are some very precise conjectures about the size of $N^{(0)}(R)$, (see Franke, Manin, and Tschinkel [2], for example). However very little has been proved in general. Indeed, as far as the author is aware the following question is still open.

1991 ***Mathematics Subject Classification.*** — Primary 11G35; Secondary 11D41, 11E76, 11G05.

Key words and phrases. — Cubic Surface, Rational Points, Height, Upper Bound, Elliptic Curve, Rank.

Question 1. — *Is it true that* $N_F(R) \ll_{\varepsilon,F} R^{2+\varepsilon}$, *for any irreducible* F *and any* $\varepsilon > 0$ *?*

The notation $\ll_{\varepsilon,F}$ means that the implied constant may depend on both ε and F. A very general result has been given by Pila [8] which shows in particular that

$$N_F(R) \ll_{\varepsilon} R^{7/3+\varepsilon},$$

for any $\varepsilon > 0$, uniformly for all absolutely irreducible cubic forms F.

One might indeed be more ambitious and ask for a positive answer to the following.

Question 2. — *Is there a constant* $\theta < 2$ *such that*

$$N^{(0)}(R) \ll_F R^{\theta},$$

for every F*?*

This would demonstrate that points on rational lines really do dominate the rate of growth of $N_F(R)$. Progress has been made in certain special cases, and the author has recently shown [3] that

$$N^{(0)}(R) \ll_{\varepsilon,F} R^{4/3+\varepsilon} \tag{1}$$

for any $\varepsilon > 0$, and any non-singular F such that the surface $F = 0$ contains three coplanar rational lines. In particular (1) holds for

$$F(W, X, Y, Z) = W^3 + X^3 + Y^3 + Z^3.$$

Ideally however one would hope for an affirmative answer to the following question.

Question 3. — *Is it true that* $N^{(0)}(R) \ll_{\varepsilon,F} R^{1+\varepsilon}$, *for any* F *and any* $\varepsilon > 0$ *?*

This is only known to be true in rather trivial cases, such as those in which $N^{(0)}(R)$ is equal to 0, or forms of the shape $W^3 - XYZ$, for example.

We shall be concerned with Question 2, and it is our goal to describe an approach which yields a satisfactory answer, subject to the following natural hypothesis about elliptic curves.

Rank Hypothesis. — *For any rational elliptic curve* E *let* C_E *denote the conductor and let* r_E *denote the rank. Then we have*

$$r_E = o(\log C_E) \quad as \quad C_E \to \infty.$$

To put this into context, we observe that

$$r_E = O(\log C_E) \tag{2}$$

for all rational elliptic curves, and

$$r_E \ll \frac{\log C_E}{\log\log C_E} = o(\log C_E) \tag{3}$$

for any rational elliptic curve with at least one rational point of order 2. These assertions ought to be well-known. However we include proofs in §6, for the sake of completeness. We remark that Mestre [7] has shown, subject to the conjecture of Birch and Swinnerton-Dyer, that (3) holds for every modular rational elliptic curve E, providing the associated L-function satisfies the Riemann Hypothesis.

We can now state our principal result.

Theorem 1. — *If the Rank Hypothesis holds then*

$$N^{(0)}(R) \ll_{\varepsilon,F} R^{4/3+\varepsilon}$$

for any non-singular form F and any $\varepsilon > 0$.

The proof of Theorem 1 involves taking hyperplane sections through the surface $F = 0$, to produce a number of cubic curves, most of which will be non-singular. We then estimate the number of points on each of these curves. We remark that this line of attack can be considerably generalized. Thus one can take a completely arbitrary variety, and attempt to count how many points may lie on each of its plane sections. However we shall not explore this possibility here.

To count points on our cubic curves we introduce the following definitions. Let $G(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ be a cubic form, and let $||G||$ denote the maximum modulus of the coefficients of G. Now define $N(G, R)$ to be the number of primitive points $\mathbf{x} \in \mathbb{Z}^3$ in the sphere $|\mathbf{x}| \leqslant R$ for which $G(\mathbf{x}) = 0$, with the proviso that if $L(\mathbf{x})$ is a rational linear factor of G, then any points on $L(\mathbf{x}) = 0$ are to be excluded. Of course this latter case can only arise when G is singular.

Our principal results on $N(G, R)$ are then the following.

Theorem 2. — *Let $G(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ be an absolutely irreducible singular cubic form. Then*

$$N(G, R) \ll_{\varepsilon} R^{2/3+\varepsilon}||G||^{\varepsilon}, \tag{4}$$

for any $\varepsilon > 0$.

Theorem 3. — *Let $G(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ be a non-singular cubic form. Then if the Rank Hypothesis holds we will have*

$$N(G, R) \ll_{\varepsilon} R^{\varepsilon}||G||^{\varepsilon},$$

for any $\varepsilon > 0$.

In Theorem 2 the exponent $2/3$ is best possible, as the example $G(X, Y, Z) = XY^2 - Z^3$ shows. This vanishes at (a^3, b^3, ab^2), which takes at least $\gg R^{2/3}$ primitive values in the sphere of radius R.

For Theorem 3, it is easy to show that

$$N(G,R) \ll_{\varepsilon,G} R^{\varepsilon},$$

and the real difficulty lies in establishing a good dependence on $||G||$. We shall also have to handle the case in which G is reducible, but the estimates we shall obtain (in §5) depend on the coefficients of G in a more delicate manner than in the cases above. It would be interesting to obtain unconditional bounds of the type given by Theorem 3, with R^{ε} replaced by a term with a larger exponent. The best such result currently available seems to be the estimate

$$N(G,R) \ll_{\varepsilon} R^{4/3+\varepsilon},$$

due to Pila [8]. This holds uniformly in G, for any fixed $\varepsilon > 0$.

2. Proof of Theorem 2

We begin our treatment of Theorem 2 by observing that G has exactly one singular point, which is therefore rational. We take the singular point to be the primitive integer vector $\mathbf{x}_0$. Elimination theory shows that $|\mathbf{x}_0| \ll ||G||^A$ for a suitable absolute constant A.

At this point it is convenient to introduce a convention concerning the large number of absolute constants which will occur in what follows. All such constants will be denoted by the same letter A, which therefore has a potentially different meaning at each occurence. This notation allows us to write $|\mathbf{x}_0|^A \ll ||G||^A$, for example, given that $|\mathbf{x}_0| \ll ||G||^A$. Such a convention needs to be treated with caution, but it avoids the notational complications of introducing A, A', A''' etc.

Proceeding with our argument, there will be an invertible integer change of variables, T say, which sends $\mathbf{x}_0$ to the point $(1,0,0)$ and with coefficients which are $O(||G||^A)$. This takes G to a form G' with $||G'|| \ll ||G||^A$. The form $G'(X,Y,Z)$ may now be written as $XQ(Y,Z) + C(Y,Z)$ where Q and C are quadratic and cubic forms respectively, and $||Q||, ||C|| \ll ||G||^A$. If $G(\mathbf{x}) = 0$ for some primitive vector $\mathbf{x}$, the corresponding triple $T\mathbf{x} = (X,Y,Z)$ will also be primitive. Thus if $Y = Z = 0$, then $X = \pm 1$. Otherwise we may set $Y = ry$, $Z = rz$ with y, z coprime, so that

$$XQ(y,z) + rC(y,z) = 0. \tag{5}$$

The polynomials Q and C are coprime, since the original cubic G is supposed to be absolutely irreducible. It follows from an application of the Euclidean algorithm that there are a quadratic form Q', a linear form L', and a non-zero constant K_1, all of which are integral, which satisfy

$$Q(Y,Z)Q'(Y,Z) + C(Y,Z)L'(Y,Z) = K_1 Y^4$$

identically. Here K_1 may depend on the original form G, and on the linear transformation T. It is clear, when one examines the algorithm, that the constant K_1