Astérisque

JOHN B. SLATER
PETER SWINNERTON-DYER

Counting points on cubic surfaces, I

Astérisque, tome 251 (1998), p. 1-12
<http://www.numdam.org/item?id=AST_1998__251__1_0>

Astérisque **251**, 1998, p. 1–11

COUNTING POINTS ON CUBIC SURFACES, I

by

John B. Slater and Sir Peter Swinnerton-Dyer

Abstract. — Let V be a nonsingular cubic surface defined over $\mathbb{Q}$, let U be the open subset of V obtained by deleting the 27 lines, and denote by $N(U,H)$ the number of rational points in U of height less than H. Manin has conjectured that if $V(\mathbb{Q})$ is not empty then

$$N(U,H) = C_1 H(\log H)^{r-1}(1+o(1)) \tag{1}$$

for some $C_1 > 0$, where r is the rank of $NS(V/\mathbb{Q})$, the Néron-Severi group of V over $\mathbb{Q}$. In this note we consider the special case when V contains two rational skew lines; and we prove that for some $C_2 > 0$ and all large enough H,

$$N(U,H) > C_2 H(\log H)^{r-1}.$$

This is the one-sided estimate corresponding to (1). It seems probable that the arguments in this paper could be modified to prove the corresponding result when V contains two skew lines conjugate over $\mathbb{Q}$ and each defined over a quadratic extension of $\mathbb{Q}$; but we have not attempted to write out the details.

Let V be a nonsingular cubic surface defined over $\mathbb{Q}$, let U be the open subset of V obtained by deleting the 27 lines, and denote by $N(U,H)$ the number of rational points in U of height less than H, and by k the least field of definition of the 27 lines. Once we have chosen our coordinate system, we shall define the *bad primes* for V as those p for which V has bad reduction at p or which ramify in any of the fields k_i defined below. In what follows we shall use $A_1, A_2, \dots$ and $C_1, C_2, \dots$ to denote positive constants depending only on V; the distinction between the A_j and the C_j is that the A_j will be rational and will be determined by divisibility considerations. Similarly $B_1, B_2, \dots$ will each belong to a finite set of elements of k^* and $\mathfrak{b}_1, \mathfrak{b}_2, \dots$ will belong to a finite set of non-zero fractional ideals of k, in each case depending only on V. The A_j, B_j and $\mathfrak{b}_j$ will always be units outside the bad primes, though this is not important. Letters A, B, C without subscripts will have the same properties, but will not necessarily have the same values from one occurrence to the next.

1991 ***Mathematics Subject Classification.*** — Primary 11G25; Secondary 14G25.
Key words and phrases. — Cubic surfaces, Manin conjecture.

Manin has conjectured that if $V(\mathbb{Q})$ is not empty then

$$N(U,H) = C_1 H(\log H)^{r-1}(1+o(1)) \tag{1}$$

for some $C_1 > 0$, where r is the rank of $NS(V/\mathbb{Q})$, the Néron-Severi group of V over $\mathbb{Q}$. In this note, which is the first of a sequence of papers concerned with various aspects of this conjecture, we consider the special case when V contains two rational skew lines; and we prove

Theorem 1. — *Suppose that V contains two rational skew lines. Then for some $C_2 > 0$ and all large enough H,*

$$N(U,H) > C_2 H(\log H)^{r-1}.$$

This is the one-sided estimate corresponding to (1). It seems probable that the arguments in this paper could be modified to prove the corresponding result when V contains two skew lines conjugate over $\mathbb{Q}$ and each defined over a quadratic extension of $\mathbb{Q}$; but we have not attempted to write out the details.

The truth or falsehood of Theorem 1 is not affected by a linear transformation of variables, though the value of C_2 may be; so without loss of generality we can assume that the two given skew lines on V have the form

$$L' : X_0 = X_1 = 0 \qquad \text{and} \qquad L'' : X_2 = X_3 = 0,$$

and that their five transversals on V have the form

$$L_i : X_0 = \alpha_i X_1,\ X_2 = \beta_i X_3 \quad \text{for} \quad 1 \leqslant i \leqslant 5$$

where the α_i, β_i are integers in k. We shall denote by k_i the least field of definition of L_i, so that k is the compositum of the k_i; since the α_i are all distinct, as are the β_i, we have $k_i = \mathbb{Q}(\alpha_i) = \mathbb{Q}(\beta_i)$. Since L', L'' and the L_i are a base for $NS(V/\mathbb{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$, their traces are a base for $NS(V/\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$; and it follows at once that the L_i form $r-2$ complete sets of conjugates over $\mathbb{Q}$. Because V contains L' and L'', its equation can be written in the form

$$f_1(X_0, X_1, X_2, X_3) = f_2(X_0, X_1, X_2, X_3) \tag{2}$$

where f_1 is homogeneous quadratic in X_0, X_1 and homogeneous linear in X_2, X_3 and the opposite is true for f_2. We can assume that the coefficients of f_1 and f_2 are rational integers and that we cannot take out an integer factor from (2). With these conditions, the bad primes for V include those which divide $\prod_{i<j}(\alpha_i - \alpha_j)^2$ or $\prod_{i<j}(\beta_i - \beta_j)^2$ and those which divide one side or other of (2). The resultant of f_1 and f_2, considered as homogeneous polynomials in X_0 and X_1, has degree 5 in X_2 and X_3; so it has the form

$$A_1 \prod (X_2 - \beta_i X_3).$$

Similarly the resultant of f_1 and f_2, considered as homogeneous polynomials in X_2 and X_3, has the form

$$A_2 \prod (X_0 - \alpha_i X_1). \tag{3}$$

Moreover $f_1(\alpha_i, 1, X_2, X_3)$ is the product of $(X_2 - \beta_i X_3)$ and a non-zero integer in k_i; and $f_2(\alpha_i, 1, X_2, X_3)$ is divisible by $(X_2 - \beta_i X_3)$. In particular, for each i both f_1 and f_2 are in the ideal in $\mathfrak{o}_i[X_0, \ldots, X_3]$ generated by $X_0 - \alpha_i X_1$ and $X_2 - \beta_i X_3$, where $\mathfrak{o}_i$ is the ring of integers of k_i.

Our argument depends on the following recipe for generating the rational points on V, subject to certain anomalies. Let

$$P' = (\xi_0, \xi_1, 0, 0) \text{ and } P'' = (0, 0, \xi_2, \xi_3)$$

be any rational points on L' and L'' respectively, expressed in lowest terms; thus ξ_0, ξ_1 are coprime integers, as are ξ_2, ξ_3. Note that each point P' corresponds to two pairs ξ_0, ξ_1 and similarly for P''. The third intersection of $P'P''$ with V is

$$P = (\xi_0 f_2(\xi), \xi_1 f_2(\xi), \xi_2 f_1(\xi), \xi_3 f_1(\xi)). \tag{4}$$

The expression (4) is not necessarily in lowest terms; indeed the highest factor which we can take out is precisely $(f_1(\xi), f_2(\xi))$, where the bracket denotes the highest common factor. The point P is geometrically well-defined unless $\xi_0 - \alpha_i \xi_1 = \xi_2 - \beta_i \xi_3 = 0$ for some i; and every rational point of V can be uniquely obtained in this way except for those which lie on some L_i. More generally, if we drop the condition that P' and P'' are rational we can in this way generate every point on V except those that lie on some L_i.

Since we wish to exclude from our count the rational points on the 27 lines, it will be important to know how they are generated under this recipe. We have already dealt with the L_i. If P is to be on L' for example, we must choose P' to be P and P'' to be the unique point satisfying $f_1(P', P'') = 0$ in an obvious notation; since

$$\begin{aligned} f_1(X_0, X_1, X_2, X_3) = (X_0 - \alpha_i X_1) g_i(X_0, X_1, X_2, X_3) \\ + (X_2 - \beta_i X_3) h_i(X_0, X_1) \end{aligned}$$

and the highest common factor of $(\xi_0 - \alpha_i \xi_1)$ and $h_i(\xi_0, \xi_1)$ in k_i divides the resultant of $(X_0 - \alpha_i X_1)$ and $h_i(X_0, X_1)$ and is therefore bounded, there is a rational integer A_3 such that $A_3(\xi_2 - \beta_i \xi_3)$ is divisible by $(\xi_0 - \alpha_i \xi_1)$ for each i. Next, let L_i' be the third intersection of V with the plane containing L' and L_i; since the one point of L'' in this plane is $(0, 0, \beta_i, 1)$, the points of L_i' are generated precisely when this point is taken to be P''. A similar argument holds for the line L_i'' which is the third intersection of V with the plane containing L'' and L_i. The remaining ten lines are the ones other than L' and L'' which meet three of the L_i. To fix ideas, consider the line L_{123} which meets L_1, L_2 and L_3. The condition that P is on L_{123} induces a one-one correspondence between P' and P'' in which three of the pairs are given by

$$P' = (\alpha_i, 1, 0, 0),\ P'' = (0, 0, \beta_i, 1) \text{ for } i = 1, 2, 3;$$

so this correspondence has the form

$$\frac{(\alpha_3-\alpha_2)(\xi_0-\alpha_1\xi_1)}{(\alpha_3-\alpha_1)(\xi_0-\alpha_2\xi_1)}=\frac{(\beta_3-\beta_2)(\xi_2-\beta_1\xi_3)}{(\beta_3-\beta_1)(\xi_2-\beta_2\xi_3)}.$$

For any pair P', P'' each fraction is in lowest terms, up to a factor belonging to a finite set of ideals depending only on V; so for $i=1$

$$(\xi_0-\alpha_i\xi_1)=\mathfrak{b}_1(\xi_2-\beta_i\xi_3)$$

as ideals, where $\mathfrak{b}_1$ belongs to a finite set of principal ideals of k_i depending only on V. A similar result holds for $i=2,3$.

Assume that $\xi_0-\alpha_i\xi_1$ and $\xi_2-\beta_i\xi_3$ do not both vanish for any i, and denote by $\mathfrak{a}_i$ the ideal

$$\mathfrak{a}_i=(\xi_0-\alpha_i\xi_1,\xi_2-\beta_i\xi_3).$$

Conversely, suppose that the $\mathfrak{a}_i$ are integral ideals, each $\mathfrak{a}_i$ lying in k_i and two $\mathfrak{a}_i$ being conjugate over $\mathbb{Q}$ if the corresponding L_i are. In what follows, sets $\mathfrak{a}_i$ will always be assumed to have these properties. We shall say that the $\mathfrak{a}_i$ are *allowable* for V if there exist coprime pairs ξ_0,ξ_1 and ξ_2,ξ_3 which give rise to this set of $\mathfrak{a}_i$. If the $\mathfrak{a}_i$ are allowable then their product is an ideal in $\mathbb{Z}$, and we can therefore define a positive integer Λ such that $(\Lambda)=\prod\mathfrak{a}_i$.

Lemma 1. — (i) *Suppose that the $\mathfrak{a}_i$ are allowable for V. Then the only primes in k which can divide more than one of the $\mathfrak{a}_i$ are those which lie above bad primes in $\mathbb{Q}$, and the highest common factor of any two of the $\mathfrak{a}_i$ in k belongs to a finite set depending only on V. If p is a good prime, then for given i there is at most one prime $\mathfrak{p}$ in k_i which divides both p and $\mathfrak{a}_i$, and it is a first degree prime in k_i. Moreover $(f_1(\xi),f_2(\xi))=B_1\Lambda$ where B_1 belongs to a finite set of rationals depending only on V.*

(ii) *Conversely, a sufficient condition for the $\mathfrak{a}_i$ to be allowable is that they are coprime in k and that none of them is divisible by any prime in k above a bad prime.*

Proof. — Since $(\mathfrak{a}_i,\mathfrak{a}_j)$ divides $(\xi_0-\alpha_i\xi_1,\xi_0-\alpha_j\xi_1)$ and therefore also $(\alpha_i-\alpha_j)$, the first assertion in (i) is trivial. Since $k_i=\mathbb{Q}(\alpha_i)$, a prime $\mathfrak{p}$ in k_i which is not first degree can only divide $\xi_0-\alpha_i\xi_1$ if either the prime p below it in $\mathbb{Q}$ divides both ξ_0 and ξ_1 or $\alpha_i\equiv c \bmod \mathfrak{p}$ for some c in $\mathbb{Z}$. In the latter case there is an automorphism σ of k not fixing k_i elementwise and such that $\sigma\mathfrak{p}$ is not prime to $\mathfrak{p}$; and $(\sigma\mathfrak{p},\mathfrak{p})$ divides $(\alpha_i-\sigma\alpha_i)$, whence p is a bad prime. If there were two primes $\mathfrak{p}'$ and $\mathfrak{p}''$ above p in k_i both of which divide $\mathfrak{a}_i$, then there would similarly be a σ such that $\sigma\mathfrak{p}''$ was not prime to $\mathfrak{p}'$ in k, and $\mathfrak{a}_i$ and $\sigma\mathfrak{a}_i$ would both be divisible by $(\mathfrak{p}',\sigma\mathfrak{p}'')$; hence again p would be a bad prime. This proves the second assertion in (i). As for the third, we know that the resultant of f_1 and f_2, considered as functions of X_2 and X_3, is (3); so $(f_1(\xi),f_2(\xi))$ divides $A_2\prod(\xi_0-\alpha_i\xi_1)$. It is therefore enough to prove that

$$(f_1(\xi),f_2(\xi),\xi_0-\alpha_i\xi_1)=\mathfrak{b}_2(\xi_0-\alpha_i\xi_1,\xi_2-\beta_i\xi_3)$$