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

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

where $\mathfrak{b}_2$ belongs to a finite set of ideals in k_i depending only on V. But using the remarks after (3) we have

$$f_1(\xi) \equiv \xi_1^2 f_1(\alpha_i, 1, \xi_2, \xi_3) = A\xi_1^2(\xi_2 - \beta_i\xi_3) \mod (\xi_0 - \alpha_i\xi_1)$$

and

$$f_2(\xi) \equiv \xi_1 f_2(\alpha_i, 1, \xi_2, \xi_3) \mod (\xi_0 - \alpha_i\xi_1),$$

and $f_2(\alpha_i, 1, \xi_2, \xi_3)$ is divisible by $(\xi_2 - \beta_i\xi_3)$.

Now suppose that the $\mathfrak{a}_i$ satisfy (ii). Since the $\mathfrak{a}_i$ form complete sets of conjugates over $\mathbb{Q}$ and are coprime, the argument in the first half of the proof shows that each prime factor of $\mathfrak{a}_i$ in k_i is a first degree prime. Moreover, if $\mathfrak{p}_i|\mathfrak{a}_i$ and $\mathfrak{p}_j|\mathfrak{a}_j$ with $\mathfrak{p}_i$ and $\mathfrak{p}_j$ lying above the same good prime p, then we could find σ as above such that $\sigma\mathfrak{p}_i$ was not prime to $\mathfrak{p}_j$; this would imply that $(\sigma\mathfrak{p}_i, \mathfrak{p}_j)$ divides $(\sigma\alpha_i - \alpha_j)$, whence $\sigma\alpha_i = \alpha_j$ and therefore $L_j = \sigma L_i$ and $\mathfrak{p}_j = \sigma\mathfrak{p}_i$. Now choose ξ_1 divisible by every bad prime and by no good prime, and choose ξ_0 not divisible by any bad prime and such that for each prime $\mathfrak{p}_i$ dividing $\mathfrak{a}_i$ with $\mathfrak{p}_i^n \parallel \mathfrak{a}_i$ we have $\mathfrak{p}_i^n \parallel (\xi_0 - \alpha_i\xi_1)$. All this is possible by the Chinese Remainder Theorem, for every prime dividing $\mathfrak{a}_i$ is first degree in k_i and we are imposing on ξ_0 one p-adic condition for each p dividing Λ. Moreover a prime $\mathfrak{q}_i$ which divides $\xi_0 - \alpha_i\xi_1$ but not $\mathfrak{a}_i$ is good, and hence is prime to every other $\mathfrak{a}_j$ and to Λ. We choose ξ_2, ξ_3 by a similar recipe, but with the additional condition that no $\mathfrak{q}_i$ divides $\xi_2 - \beta_i\xi_3$. □

Let h denote the height function; then in the notation above we have

$$h(P') = \max(|\xi_0|, |\xi_1|),\ h(P'') = \max(|\xi_2|, |\xi_3|).$$

It follows from (4) and Lemma 1 that

$$h(P) \leqslant C_3(h(P')h(P''))^2/\Lambda. \tag{5}$$

In order to prove Theorem 1, we shall obtain a lower bound for the number of rational points P in U with preassigned allowable $\mathfrak{a}_i$ such that $h(P) < H$. For simplicity, we confine ourselves to the case when none of the $\mathfrak{a}_i$ is divisible by any bad prime; hence in particular they are coprime. The natural way to proceed is to perform the count on $V \setminus \cup L_i$ and then allow for those rational points which lie on one of the lines other than the L_i. The latter step presents no difficulties because almost all the rational points on these lines come either from very special sets of ξ_i or from values of Λ much larger in terms of N than those which we shall be considering.

Lemma 2. — (i) *If P is a rational point on L_i' or L_i'' then we have $\xi_2 - \beta_i\xi_3 = 0$ or $\xi_0 - \alpha_i\xi_1 = 0$ respectively.*
(ii) *The number of rational points on L', L'' or some L_{ijk} with preassigned $\mathfrak{a}_1, \ldots, \mathfrak{a}_5$ and with $h(P')h(P'') < N$ is bounded by $C(\log N)^4$.*

Proof. — We have already proved (i). Suppose for example that P is on L'; then the ideals $(\xi_0 - \alpha_i\xi_1)$ and $\mathfrak{a}_i$ differ by a factor drawn from a finite set depending only on V. This means that $\xi_0 - \alpha_i\xi_1 = \epsilon\gamma_i$ where γ_i is an integer in k_i^* drawn from a finite set depending for preassigned $\mathfrak{a}_i$ only on V and ϵ is a unit in k_i. By multiplying γ_i by a suitable unit in k_i we can ensure that $|\sigma\gamma_i| > C$ for every embedding $\sigma : k_i \to \mathbb{C}$. This and $h(P') < N$ imply that $|\sigma\epsilon| < CN$ for every σ; since $[k_i : \mathbb{Q}] \leqslant 5$, there are at most $C(\log N)^4$ units ϵ with this property. If α_i is not in $\mathbb{Z}$ a knowledge of ϵ and γ_i uniquely determines ξ_0 and ξ_1. If however each α_i is in $\mathbb{Z}$ then there are only two possible values of ϵ for each γ_i, and a knowledge of more than one of the $\xi_0 - \alpha_i\xi_1$ determines ξ_0 and ξ_1. In either case $P = P'$, so a knowledge of P' determines P.

Finally suppose for example that P is on L_{123}. For $i = 1, 2, 3$ we know that $(\xi_0 - \alpha_i\xi_1)$, $(\xi_2 - \beta_i\xi_3)$ and $\mathfrak{a}_i$ differ by factors drawn from a finite set of ideals depending only on V. Since if L_{123} is rational the set $\{L_1, L_2, L_3\}$ is a union of complete sets of conjugates over $\mathbb{Q}$, an argument like that of the previous paragraph shows that for any preassigned $\mathfrak{a}_i$ there are at most $C(\log N)^2$ possible P' with $h(P') < N$, and a similar result holds for P''. □

The next step will be to estimate, under suitable conditions, the number of rational points in U which satisfy

$$h(P') \leqslant N', \quad \tfrac{1}{2}N'' \leqslant h(P'') < N'' \tag{6}$$

for given $\mathfrak{a}_i$ and given N', N''. The pairs P', P'' which satisfy

$$\xi_0 - \alpha_i\xi_1 \equiv \xi_2 - \beta_i\xi_3 \equiv 0 \mod \mathfrak{a}_i \tag{7}$$

are precisely those given by

$$\xi_0 = \Lambda\eta_0 + a\eta_1,\ \xi_1 = \eta_1,\ \xi_2 = \Lambda\eta_2 + b\eta_3,\ \xi_3 = \eta_3 \tag{8}$$

for some integers η_i, where a, b have been chosen so that

$$a - \alpha_i \equiv b - \beta_i \equiv 0 \mod \mathfrak{a}_i$$

for each i. (That we can find a, b with these properties depends on the facts that the $\mathfrak{a}_i$ are coprime and divisible only by first degree primes.) We can clearly assume that both a and b are absolutely bounded by Λ. The condition that ξ_0, ξ_1 are coprime is equivalent to η_1 being prime to both Λ and η_0; and similarly for ξ_2, ξ_3. The first condition (6) is equivalent to

$$|\eta_1| \leqslant N', \quad |\eta_0 + a\Lambda^{-1}\eta_1| \leqslant \Lambda^{-1}N' \tag{9}$$

and the second condition (6) is equivalent to either

$$\tfrac{1}{2}N'' \leqslant |\eta_3| < N'', \quad |\eta_2 + b\Lambda^{-1}\eta_3| < \Lambda^{-1}N'' \tag{10}$$

or

$$|\eta_3| < \tfrac{1}{2}N'', \quad \tfrac{1}{2}\Lambda^{-1}N'' \leqslant |\eta_2 + b\Lambda^{-1}\eta_3| < \Lambda^{-1}N''. \tag{11}$$

To obtain all the rational points on V which satisfy (6) and have the given values of the $\mathfrak{a}_i$, we let the η_i run through all sets satisfying (9) and either (10) or (11), and reject all those for which ξ_0, ξ_1 are not coprime, or ξ_2, ξ_3 are not coprime, or $(\xi_0 - \alpha_i\xi_1, \xi_2 - \beta_i\xi_3)$ is a strict multiple of $\mathfrak{a}_i$ for some i. We shall say that a set of η_i *fails* at a prime p if p divides both ξ_0 and ξ_1, or both ξ_2 and ξ_3, or if there is a prime factor $\mathfrak{p}$ of p in k_i such that $\mathfrak{p}\mathfrak{a}_i$ divides both $\xi_0 - \alpha_i\xi_1$ and $\xi_2 - \beta_i\xi_3$ for some i. We shall call a set of η_i *allowable* if it does not fail for any p; note that such a set may still give rise to a point on one of the 27 lines. Whether the η_i fail at p only depends on the values of the $\eta_i \bmod p$. For any prime p, let n_p be the number of sets $\eta_0, \dots, \eta_3 \bmod p$ which fail at p. Here n_p depends on the $\mathfrak{a}_i$ as well as on V and p. It is not hard to give an explicit formula for n_p, but all we shall need are the obvious estimates, for p a good prime, that $n_p = 2p^3 + O(p^2)$ if $p|\Lambda$ and $n_p = O(p^2)$ otherwise. Because the $\mathfrak{a}_i$ are allowable, $n_p < p^4$ for all p.

Lemma 3. — *Assume that the $\mathfrak{a}_i$ are coprime and that none of them is divisible by any prime in k lying above a bad prime. Suppose that*

$$\Lambda < n^{1/2} \quad \textit{and} \quad \log \max(N', N'') < n,$$

where $n = \min(N', N'')$. Then, provided that N' and N'' are large enough, the number of rational points in U which satisfy (6) *and give rise to these $\mathfrak{a}_i$ differs from*

$$3(N'N''/\Lambda)^2 \prod_{p<T} (1 - p^{-4}n_p)$$

by at most $C(N'N''/\Lambda)^2(\log\log n)^{-1/2}$, for any T satisfying

$$3\log n/\log\log\log n > T > \log n/\log\log\log n.$$

Proof. — It is well known that there is an absolute constant C_4 such that

$$\sum_{p<x} \log p < C_4 x \quad \text{provided} \quad x > 2; \tag{12}$$

thus the condition on T ensures that $T\log T$ is large compared to $\log n$ and that $Q < n^{C/\log\log\log n}$ where Q denotes the product of all the primes less than T. We assume n so large that all the bad primes are less than T, and to fix ideas we assume that $n = N'$. In what follows we shall use square brackets to denote integral parts. The set of pairs η_0, η_1 satisfying (9) contains

$$[2N'/Q][2\Lambda^{-1}N'/Q]$$

disjoint parallelograms each of which consists of a complete set of pairs incongruent $\bmod Q$; and the pairs left over are contained in a further

$$[2N'/Q] + [2\Lambda^{-1}N'/Q] + 1 \leqslant CN'/Q$$

such parallelograms. A similar argument holds for the pairs η_2, η_3 which satisfy either (10) or (11); this time the number of filled parallelograms differs from

$$3N''^2/\Lambda Q^2$$

by at most CN''/Q, and the pairs left over are contained in a further CN''/Q such parallelograms. Each product of two filled parallelograms contains $\prod_{p<T}(p^4 - n_p)$ sets which do not fail at any prime less than T. Hence the number of sets of η_i which satisfy (9) and either (10) or (11) and which do not fail at any prime less than T differs from

$$12(N'N''/\Lambda)^2 \prod_{p<T}(1 - p^{-4}n_p) \tag{13}$$

by at most $CN'N''^2Q\Lambda^{-1}$. In going from sets η_i to pairs P', P'' we lose a factor 4. The sets with $\eta_0 = \eta_1 = 0$ or $\eta_2 = \eta_3 = 0$ have already been rejected because they fail at every p. The number of other sets η_i which satisfy $\xi_0 - \alpha_i\xi_1 = 0$ or $\xi_2 - \beta_i\xi_3 = 0$ for some i with α_i, β_i in $\mathbb{Z}$ is bounded by $CN'N''^2\Lambda^{-1}$, which can be absorbed into the previous error term; since those of them which are allowable give rise to a point on some L_i' or L_i'', we can rule them out now.

Next let p be a prime satisfying $T \leqslant p \leqslant N'$. By an argument similar to that in the previous paragraph, the number of sets η_i which satisfy (9) and either (10) or (11) but which fail at p is at most

$$C(p^{-2}\Lambda^{-1}N'^2 + p^{-1}N')(p^{-2}\Lambda^{-1}N''^2 + p^{-1}N'')n_p. \tag{14}$$

There are at most $C \log \Lambda / \log T$ primes not less than T which divide Λ, and for each of them $p \leqslant \Lambda$ and $n_p < Cp^3$. Thus the sum of the expressions (14) taken over all such primes is bounded by

$$CN'^2N''^2\Lambda^{-2}(\log \Lambda / \log T)T^{-1}.$$

If p does not divide Λ then $n_p < Cp^2$. The sum of the expressions (14) over primes p not dividing Λ and such that $T \leqslant p \leqslant N'$ is bounded by

$$CN'^2N''^2\Lambda^{-2}T^{-1} + CN'N''^2\Lambda^{-1} \log\log N' + CN'^2N''/\log N',$$

because $\sum p^{-1}$ taken over these primes is bounded by $C \log\log N'$.

Now suppose that $p > N'$. If p divides ξ_0 and ξ_1 we must have $\xi_0 = \xi_1 = 0$, and we have already ruled out all η_i with this property. If there is a prime $\mathfrak{p}$ above p such that $\mathfrak{p}\mathfrak{a}_i$ divides $\xi_0 - \alpha_i\xi_1$ and $\xi_2 - \beta_i\xi_3$ for some i, then p must divide $\prod(\xi_0 - \alpha_i\xi_1)$; we have already ruled out all η_i for which this vanishes and it is absolutely bounded by CN'^5, so for preassigned η_0, η_1 at most five primes $p > N'$ come into consideration. For each of these p there are at most

$$CN''(p^{-1}\Lambda^{-1}N'' + 1)$$

pairs η_2, η_3 such that $\mathfrak{p}\mathfrak{a}_i$ divides $\xi_2 - \beta_i \xi_3$. Hence the number of sets η_i which fail in this way for some $p > N'$ but which have not been previously rejected is bounded by

$$CN'^2\Lambda^{-1}N''(N'^{-1}\Lambda^{-1}N'' + 1) \;=\; CN'N''\Lambda^{-2}(N'' + \Lambda N').$$

Again, p can only divide ξ_2 and ξ_3 without them both vanishing if $p \leqslant N''$; and in this case there are at most

$$C(p^{-2}\Lambda^{-1}N''^2 + p^{-1}N'')$$

pairs η_2, η_3 with this property. Multiplying by $CN'^2\Lambda^{-1}$ to allow for the choice of η_0, η_1 and summing over all p with $N' < p \leqslant N''$, we find that the number of sets η_i which fail in this way for some $p > N'$ but which have not been previously rejected is at most

$$CN'N''\Lambda^{-2}(N'' + N'\Lambda \log\log N'').$$

Gathering these estimates together, we find that the number of sets η_i which do not fail at any prime differs from (13) by a sum of terms each of which is dominated by

$$C\left(\frac{N'N''}{\Lambda}\right)^2 \frac{\log T + \log\Lambda}{T\log T}. \tag{15}$$

We must also rule out the sets η_i which do not fail at any p but which give rise to a point on one of the 27 lines. But we have already ruled out the η_i which satisfy the condition in Lemma 2(i), and those which satisfy the condition in Lemma 2(ii) can be absorbed into the error term (15). □

Corollary 1. — *Assume that the $\mathfrak{a}_i$ are coprime, that none of them is divisible by any bad prime, that H is large enough and that $\Lambda < H^{1/11}$. Write*

$$T = \log H/3\log\log\log H.$$

Then the number of rational points in U of height at most H which give rise to these $\mathfrak{a}_i$ is at least

$$\{C\prod_{p<T}(1 - p^{-4}n_p) - C(\log\log H)^{-1/2}\}H\Lambda^{-1}\log H. \tag{16}$$

Proof. — For each r with $0 \leqslant r \leqslant \log H/6\log 2$ apply Lemma 3 with $N' = 2^r\Lambda^{1/4}H^{1/6}$ and $N'' = 2^{-r}C_3^{-1/2}\Lambda^{1/4}H^{1/3}$, where C_3 is as in (5). It follows from (5) that every point with these $\mathfrak{a}_i$ satisfying (6) has $h(P) < H$; and we have

$$C\Lambda^{1/4}H^{1/4} \geqslant r = \min(N', N'') \geqslant C\Lambda^{1/4}H^{1/6}$$

and $\max(N', N'') \leqslant C\Lambda^{1/4}H^{1/3}$, so that all the conditions of Lemma 3 are satisfied. Moreover the sets defined by (6) as r varies are disjoint. Hence the number of rational

points in U of height at most H and with these $\mathfrak{a}_i$ is at least

$$\sum_r H\Lambda^{-1}\{C\prod_{p<T}(1-p^{-4}n_p) - C(\log\log H)^{-1/2})\},$$

which is the result claimed □

Remark 1. — *The most we can say about* $\prod_{p<T}(1-p^{-4}n_p)$ *in general is that it is at least* $(\log T)^{-C}$*; so the error term in Lemma 3 is not always smaller than the leading term, and (16) is not always positive. But this blemish is coped with by the averaging process employed in the proof of Theorem 1.*

To complete the proof of Theorem 1, we have to sum the expression (16) over a sufficiently large collection of allowable sets $\mathfrak{a}_i$. Recall that the L_i form $r-2$ complete sets of conjugates over $\mathbb{Q}$. After renumbering, we can assume that no two of $L_1,\dots,L_{r-2}$ are conjugate over $\mathbb{Q}$. For each i let $\lambda_i = \operatorname{Norm}\mathfrak{a}_i$; thus a good prime p divides at most one of $\lambda_1,\dots,\lambda_{r-2}$ and such a p can divide λ_i only if it has a first degree factor in k_i. Moreover $\Lambda = \lambda_1\dots\lambda_{r-2}$. We take T as in the Corollary to Lemma 3, and assume H so large that all the bad primes are less than T. Now write $M = H^{1/11(r-2)}$; bearing in mind Lemma 1(ii), we shall allow the $\mathfrak{a}_i$ to run through all sets such that each pair $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime in k, no $\mathfrak{a}_i$ is divisible by any prime in k above a bad prime, and each $\lambda_i \leqslant M$. In view of the Corollary to Lemma 3, in order to prove Theorem 1 it is only necessary to prove the following result:

Lemma 4. — *We have*

$$\sum\Lambda^{-1} < C(\log H)^{r-2},\quad \sum\Lambda^{-1}\prod_{p<T}(1-p^{-4}n_p) > C(\log H)^{r-2}, \tag{17}$$

where the sum is taken over the sets $\mathfrak{a}_i$ *specified above.*

Proof. — It is well known that for any algebraic number field K and any $X > 1$ there is a constant $C(K)$ such that

$$\sum(\operatorname{Norm}\mathfrak{a})^{-1} = (C(K)+o(1))\log X, \tag{18}$$

where the sum is taken over all integer ideals $\mathfrak{a}$ with $\operatorname{Norm}\mathfrak{a} < X$. Now

$$\sum\Lambda^{-1} = \sum(\lambda_1\dots\lambda_{r-2})^{-1} \leqslant \prod_{i=1}^{r-2}(\sum\lambda_i^{-1}) \tag{19}$$

where the sums on the left and in the middle are taken over the same collection as in (17) and the sum on the right is taken over all integer ideals in k_i of norm at most M. By (18), the expression on the right of (19) is bounded by $C(\log H)^{r-2}$.

The proof of the second inequality (17) is similar but more complicated. We can multiply each term in the sum on the left by an expression of the form $\prod(1+c_p)$, where the c_p vary from one term to another but are uniformly $O(p^{-2})$; for in doing so we multiply the terms by uniformly bounded factors. Bearing in mind the information

about the n_p which appears just before the statement of Lemma 3, it is therefore enough to prove that

$$\sum \Lambda^{-1} \prod (1-p^{-1})^2 > C(\log H)^{r-2}, \tag{20}$$

where the product is over those $p < T$ which divide Λ and where the sum is over the same collection as in (17). Recall that $\sum_1^{r-2}[k_i : \mathbb{Q}] = 5$. If we multiply the left hand side of (20) by $(\sum n^{-2})^{10}$, which does not affect the truth or falsehood of the inequality provided we make a compensating adjustment of the value of C, we obtain an expression which exceeds $\sum \Lambda^{-1} \prod (1-p^{-1})^2$ where now the sum is taken over all sets of $\mathfrak{a}_i$ with each $\lambda_i \leqslant M$ and the product is taken over all first degree primes $\mathfrak{p}_i$ in some k_i which divide $\mathfrak{a}_i$ and have $p = \operatorname{Norm} \mathfrak{p}_i < T$. This expression is equal to

$$\prod_{i=1}^{r-2} (\sum \lambda_i^{-1} \prod (1-p^{-1})^2);$$

so to prove the second inequality (17) it is enough to prove

$$S = \sum \lambda_i^{-1} \prod (1-p^{-1})^2 > C \log H.$$

But if we choose a first degree prime $\mathfrak{p}_i$ in k_i with $p = \operatorname{Norm} \mathfrak{p}_i < T$, the left hand side can be written as

$$(1 + p^{-1}(1-p^{-1})^2) S_1 + S_2 \tag{21}$$

plus some terms arising from $\mathfrak{p}_i^2 | \mathfrak{a}_i$ which we ignore; here S_1 consists of those terms for which $\mathfrak{p}_i$ does not divide $\mathfrak{a}_i$ and $\operatorname{Norm} \mathfrak{a}_i \leqslant Mp^{-1}$, and S_2 consists of those terms for which $\mathfrak{p}_i$ does not divide $\mathfrak{a}_i$ and $\operatorname{Norm} \mathfrak{a}_i > Mp^{-1}$. If we multiply the first term in (21) by

$$(1 + p^{-1}(1-p^{-1})^2)^{-1}(1-p^{-1}) = 1 + O(p^{-2})$$

and delete certain terms, the effect is precisely to delete the factors $(1-p^{-1})^2$ in S corresponding to $\mathfrak{p}_i$. We can do this for each $\mathfrak{p}_i$ in turn, and this reduces the inequality which we are seeking to prove to (18). □

It may appear that by a slight refinement of the argument we could obtain a two-sided estimate for $N(U, H)$ under the hypotheses of the Theorem. But this seems not to be so. The problem is that we need estimates like those of Lemma 3 in three essentially different kinds of case: when $N'' \geqslant N' \geqslant \Lambda^{1/2}$, when $N'' \geqslant \Lambda^{1/2} \geqslant N'$ and when $\Lambda^{1/2} \geqslant N'' \geqslant N'$. The first can be dealt with by the methods of Lemma 3, and we can also deal with the second though the arguments are more complicated. But we do not at present see how to deal with the third case.

Received 23 September 1996

JOHN B. SLATER, Computing Laboratory, University of Kent, Canterbury CT2 7NF, United Kingdom
E-mail : J.B.Slater@ukc.ac.uk

SIR PETER SWINNERTON-DYER, Isaac Newton Institute, 20 Clarkson Rd, Cambridge CB3 0EH, United Kingdom • *E-mail :* hpfs100@newton.cam.ac.uk