代数幾何学シンポジウム記録
1994年度 pp.3-9

Problems on computability concerning distribution of rational points on algebraic varieties

Yasuo Morita (Tohoku University)

§0. Introduction.

If V is a projective variety defined over a field k, then we denote by $V(k)$ the set of all $k-$rational points on V.

We are interested in the following problem :

Main Problem. *Find an algorithm to calculate $V(k)$ for any given projective variety V defined over a finite algebraic number field k.*

In general, the answer to this question should be "There exists no such algorithm" because we have a negative answer to the following problem (cf. [D]) :

Hilbert's 10-th Problem. *Find an algorithm to tell whether or not there exists an integer solution to any give Diophantine equation*

$$f(x_1, \ldots, x_m) = 0 \text{ for } x_1, \ldots, x_m \in \mathbb{Z} \qquad (f(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]).$$

On the other hand, we have the following partial affirmative conjecture, which almost all experts on Arithmetic Geometry believe :

Effective Mordell conjecture. *There would exist an algorithm to solve the Main Problem if we restrict to the case of algebraic curves* ($\dim V = 1$).

Hence it is natural and important to study the main problem more closely in the case of algebraic surfaces ($\dim V = 2$). In this paper, we shall give some problems concerning the computability of the distribution of rational points on algebraic surfaces.

§1. What is an algorithm ?

Hilbert's 10-th problem was studied by logicians, and they have clear idea of what should be an algorithm :

They have discovered the notion of Turing machines, and the notion of recursive functions :

A Turing machine is a very simple computer, which is easy to analyze but too simple for a practical use. We will not explain the exact definition of a Turing machine (cf. [C]).

The definition of recursive functions is given by the following :

Definition. The class of *recursive functions* is the smallest class of functions which contains

constant functions $x \longmapsto c$,
the successor function $x \longmapsto x+1$, and
projections $(x_1, \ldots, x_m) \longmapsto x_i$ $(i = 1, \ldots, m)$,

and which are stable by *composition of functions, recursive definitions, and minimalization* (for the definition of minimalization, see *e.g.* [C] or [Hi]).

Roughly speaking, a recursive function is a function which can be constructed from trivial functions by using recursive definitions.

It is known that these two notions coincide. Namely, we have the following :

Theorem. *A function* $f : \mathrm{N} \longrightarrow \mathrm{N}$ *is recursive if and only if there exists a Turing machine to calculate the values of* f.

Further, logicians believe that these two equivalent notions also coincide with our vague idea of *computable functions* :

Church's hypothesis. *The values of a function* $f : \mathrm{N} \longrightarrow \mathrm{N}$ *can be calculated in a finite step if and only if* f *is a recursive function.*

We use the expression that there is an *algorithm* to solve a problem if there exists a recursive function to calculate it. Hence the following theorem gives a negative answer to Hilbert's 10-th problem (see [D] and [D-M-R] for more details) :

Theorem. *The exists a polynomial* $P(t, x_1, \ldots, x_m) \in \mathbb{Z}[t, x_1, \ldots, x_m]$ *such that the function* $\chi : \mathbb{Z} \longrightarrow \{1, 0\}$ *defined by*

$$\chi(t) = \begin{cases} 1 & \text{if } P(t, x_1, \ldots, x_m) = 0 \text{ has an integer solution} \\ 0 & \text{otherwise} \end{cases}$$

is not recursive.

Remark. We use the word that a constant c can be calculated *effectively* if there exists an algorithm to calculate c. Note that this expression can be used even if we need more memories than the number of elementary articles in the universe, and need longer time than the span of the universe.

In the case of Algebraic Number Theory, we have such constants as the *discriminant*, the *regulator*, the *class number*, e.t.c. All of them can be calculated effectively, and, in fact, we have computer programs to calculate them. Hence most invariants in Algebraic Number Theory is computable.

On the other hand, in the case of Algebraic Geometry, there exist many numerical constants which we do not know any algorithms to calculate.

The author emphasizes that *we should study the problem of calculating numerical constants in Algebraic Geometry.*

On of the typical examples of this problem is the following :

Example. Find an algorithm to calculate the *Kodaira dimension* $\kappa(V)$ for a given smooth projective algebraic varieties V defined over $\mathbb{C}$.

Though this problem would be quite difficult in general, the author thinks that we should have an algorithm in the 2-dimensional case.

§2. 1-dimensional case (algebraic curves).

We have fairly good knowledge in the 1-dimensional case :

Let C be a smooth projective curve defined over an algebraic number field k. Then we denote by $g(C)$ the genus of C.

If the genus $g(C) = 0$, then $C \times_k \overline{k}$ is isomorphic to the projective line $\mathbb{P}^1$. Further, C itself is isomorphic to the projective line $\mathbb{P}^1$ if and only if $C(k) \neq \emptyset$. Furthermore, since every such algebraic curve C can be realized as a quadratic curve in the projective plane $\mathbb{P}^2$, by using the theory of quadratic forms, we can classify them. In particular, there exists an algorithm to check whether or not $C(k) \neq \emptyset$.

If $g(C) = 1$, C is an elliptic curve defined over k if and only if $C(k) \neq \emptyset$. Further, by the **Birch Swinnerton-Dyer conjecture** (*i.e.* by the finiteness of the Tate - Shafarevich group), there exists an algorithm to calculate $C(k)$ if $C(k) \neq \emptyset$ (cf. *e.g.* [Sil], p. 305). But we do *not* know any algorithm to check whether or not $C(k) \neq \emptyset$.

If $g(C) > 1$, G. Faltings proved that $C(k)$ is a finite set (the **Mordell Conjecture**). It is conjectured that there exists an algorithm to calculate $C(k)$ (the **effective Mordell Conjecture**).

Remark. It seems that almost all experts in Arithmetic Geometry believe that the effective Mordell Conjecture is true. There is even a rumor that G. Wüstoholz and other people proved this conjecture by using the Baker method.

Though this rumor might not be true, it is believed that a proof of the effective Mordell Conjecture will be obtained in a near future.

§3. 2-dimensional case (algebraic surfaces).

Let S be an algebraic surface (a projective 2-dimensional algebraic variety). Then we can (i) resolve singularities and construct a smooth model, and (ii) blow down exceptional curves and construct a smooth minimal model. By this reason, in standard texts of algebraic surfaces, an algebraic surface is assumed to be smooth and minimal.

Well, for a give algebraic surface S defined over an algebraic number field k, we have an algorithm to construct a normal k−model. So, from our point of view, we may assume that S is normal. Since the set of singularities on S is a computable k−rational finite set, we can blow up all singular points on S and construct another k−model. We repeat this process a finite number of times, and can construct a smooth k−model. Hence we may assume that S is smooth.

Now we want to blow down exceptional curves on S. But some exceptional curves may not be defined over k. Hence we can not always construct a k−rational geometrically minimal model (i.e. a model which is minimal over the algebraic closure $\overline{k}$ of k). (There is a k−rational geometrically minimal model if the Kodaira dimension of S is non-negative, because two exceptional curves on such a surface S do not intersect.) Further, we have serious difficulties to find exceptional curves on a given algebraic surface. Namely, it seems that we do not know any algorithm to find an exceptional curve on a given surface. Hence the author proposes :

Problem. *Find an algorithm to discover an exceptional curve on a given (non-minimal) algebraic surface.*

Remark. Of course, we can ask the corresponding problem in a higher dimensional case. But the author doubts the existence of a solution in the general case. The author thinks that this problem may have an affirmative solution in our case because the codimension of exceptional curves on an algebraic surface is 1.

§4. Abelian varieties and surfaces of general type.

Let V be an algebraic variety defined over an algebraic number field k.

If V is an *abelian variety*, then the situation is similar to the case of an elliptic curve :
It is difficult to check whether or not $A(k) \neq \emptyset$. But if $A(k) \neq \emptyset$, then $A(k)$ is a finitely generated abelian group. Further, if the Tate Shafarevich group is finite, then we can effectively calculate a generator of $A(k)$.

If V is of *general type*, then we have the following :

Conjecture (Bombieri Vojta). *There would exist a non-empty open dense k−subset U of V such that $U(k)$ is a finite set.*

Hence, if S is an algebraic surface of general type defined over k, then there would exist a finite number of rational and elliptic curves defined over $\overline{k}$ such that the set of $k-$rational points on the complement is a finite set.

This is only a conjecture, and we do not know how to calculate these rational and elliptic curves, and we do not know how to calculate the set of $k-$rational points on the complement.

The author hopes that there exists an algorithm to calculate all rational and elliptic curves defined over $\overline{k}$ on a given algebraic surface of general type. The author doubts the existence of an algorithm to calculate $k-$rational points on the complement.

§5. **Proper elliptic surfaces.**

Let S be a smooth minimal surface defined over an algebraic number field k. *We assume* $\kappa(S) = 1$. Then S has a structure of an elliptic surface

$$\pi : S \longrightarrow C.$$

Here C is a smooth algebraic curve and the general fibre of π is an elliptic curve.

Since a proper elliptic surface has only one elliptic fibering, the algebraic curve C and the morphism $\pi : S \longrightarrow C$ are defined over k. Hence any rational $k-$point $s \in S(k)$ is contained in the fibre $\pi^{-1}(c)$ for a certain $k-$rational point $c \in C(k)$. Further, there exists a one-to-one correspondence from the set of rational points on a generic fibre to the set of $k-$rational sections of π. It is conjectured that these sets can be calculated.

If the genus $g(C)$ of the base curve C is greater than 1, then there exist only a finite number of rational points on C. Hence we can calculate $S(k)$ if we can prove the effective Mordell conjecture. Hence the difficult case is the case of $g(C) = 0$ or 1.

Now *we assume* $g(C) = 1$ *and* $C(k) \neq \emptyset$. Hence C is an elliptic curve defined over k, and there may exist infinitely many $k-$rational points on C. Let O be an origin of the elliptic curve E.

Remark. We can also study the case such that $g(C) = 0$ and $C(k) \neq \emptyset$. In this case, we have $C \simeq \mathbb{P}^1$. But the situation becomes a bit more complicated because there are more rational maps from algebraic curves onto $\mathbb{P}^1$ than rational maps from algebraic curves onto a given elliptic curve.

If $\iota : C \longrightarrow S$ is a $k-$rational section, and if c is a $k-$rational point on C, then $\iota(C) \cap \pi^{-1}(c)$ is a $k-$rational point on S.

Let $\iota : C \longrightarrow S$ be a morphism such that $(\pi \circ \iota)(O) = O$ and $\pi \circ \iota : C \longrightarrow C$ is not a constant map. For simplicity , we call such a morphism $\iota : C \longrightarrow S$ a ***multi-section.*** If $\iota : C \longrightarrow S$ is a $k-$rational multi-section, then $O' = \iota(O)$ is a $k-$rational point, the image $E = \pi(C)$ has a structure of an elliptic curve with O' as its origin, and $\pi : (E, O') \longrightarrow (C, O)$ is an $k-$isogeny. Hence E also contains many $k-$rational points. Further, for any $k-$rational point c on C, $\iota(C) \cap \pi^{-1}(c)$ is a $k-$rational cycle on S. Sometimes this set contains $k-$rational points.

Conversely, let E be an algebraic curve on S that is not contained in any fibre. Since $g(C) = 1$, we have $g(E) \geq 1$. It follows that either $g(E) \geq 2$ or π induces an isogeny $\pi\,|_E\colon E \longrightarrow C$ of elliptic curves. Hence, if E is a $k-$rational algebraic curve contained in S which has infinitely many $k-$rational points, then E is an elliptic curve defined over k, $\pi\,|_E\colon E \longrightarrow C$ is a $k-$isogeny of elliptic curves, and the inverse of this isogeny is a $k-$rational multi-section $\iota : C \longrightarrow E \hookrightarrow S$.

Problem. *Find an algorithm to calculate the set of all multi-sections $\iota : C \longrightarrow S$ on $\pi : S \longrightarrow C$.*

There may exist other types of $k-$rational points (*i.e.* $k-$rational points not coming from $k-$rational multi-sections) on some $k-$rational fibres. For example, usually, there exist more $k-$rational points on degenerating fibres.

Problem. *Is it true that, except a finite number of fibres, all $k-$rational points on a $k-$rational fibre are produced from multi-sections of π.*

Remark. This problem is base on the hope that, since the canonical bundle of a proper elliptic surface is effective, the set of rational points on it should behaves better than other cases. Hence the assumption that $\kappa(S) = 1$ is essential in this problem. We note that if $\kappa(S) = 1$, then the automorphism group of the fibre space $\pi : S \longrightarrow C$ is a finite group.

We add one more problem :

Problem. *Normalize the height function on S and calculate the exact contribution of multi-sections of π to the height zeta function of S.*

References

[B-M] V. V. Batyrev et Yu. I. Manin, Sur le nombre des points rationnels de hauteur borné des varietés algèbriques, Math. Ann., **286**(1990), 27-43.

[B-P-V] W. Barth, C. Peters and Van de Ven, Compact complex surfaces, Erg. der Mat., 3. Folge, Band 4, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1984.

[C] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo Hong Kong Barcelona Budapest, 1984.

[C-S] G. Cornell and J. H. Silverman, Arithmetic Geometry, Springer-Verlag, New York Berlin Heidelberg London Paris Tokyo, 1985.

[D] M. Davis, Hilbert tenth problem is unsolvable, Amer. Math. Monthly, **80**(1973), 233-269.

[D-M-R] M. Davis, Y. Matijasevich and J. Robinson, Hilbert's tenth problem. Diophantine equations: Positive aspect of a negative solution, Proc. Symp. in Pure Math., **28**(1976), 323-378.

[F] G. Faltings, Endlichkeitssätze für Abelsche Varietäten über Zahl- körpern, Invent. Math., **73**(1983), 349-366.

[H] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York - Heidelberg - Berlin 1977.

[Hi] 廣瀬健, 帰納的関数, 共立出版, 1989.

[M1] 森田康夫, 不定方程式の可解性と代数多様体の有点について, 数解析研究所講究録, **844**(1993), 1-16.

[S] J.-P. Serre, Lecture on the Mordell-Weil theorem, Vieweg, Braunsweg, 1989.

[Sil] J H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., **106**, Springer-Verlag, New York Berlin Heidelberg Tokyo, 1986.

Mathematical Institute
Faculty of Science
Tohoku University
Aoba, Sendai 980-77
Japan