BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 80, Number 5, September 1974

HIGHER DIMENSIONAL DIOPHANTINE PROBLEMS

BY SERGE LANG

As on previous occasions [**L 5**], [**L 6**], I shall discuss some general conjectures concerning diophantine analysis on varieties. These involve rational points, integral points, and the possibility of treating by diophantine methods questions which in the past have been handled by congruence methods.

1. **Rational points.** A classical conjecture of Mordell states that a curve of genus $\geqq 2$ over the rational numbers has only a finite number of rational points. Let K be a finitely generated field over the rational numbers. Then the same statement should hold for a curve defined over K, and a specialization argument due to Néron shows in fact that this latter statement is implied by the corresponding statement over number fields (cf. [**L 1**, Chapter VII, §6]).

Let V be a variety in projective space, defined over the complex numbers, and therefore over some finitely generated field over the rationals. We shall say that V has the **Mordell property** if it has only a finite number of rational points in any finitely generated field over $\boldsymbol{Q}$. One possibility to extend Mordell's conjecture to higher dimensional varieties is as follows.

(1.1) *Let D be a bounded domain in $\boldsymbol{C}^n$ (it should be irrelevant whether D is symmetric or not). Let Γ be a discrete group of automorphisms, acting freely on D, and assume that the quotient $\Gamma\backslash D$ is compact, and embedded as a variety V in projective space. Then V has the Mordell property.*

One must assume that Γ operates freely (the isotropy group at each point is the identity), otherwise the quotient may have singularities, whose effect is analogous to decreasing the genus in the case of curves. Similarly, one must assume that the quotient is compact, otherwise one is faced with a situation which may be like that of modular curves which may have a low genus 0 or 1. The Mordell conjecture is a special case of the above, because a curve of genus $\geqq 2$ is a quotient of the disc. On the other hand, it has always been useful to regard a curve of genus $\geqq 2$ as a

---

An address delivered before the New York meeting of the Society on April 13, 1974 by invitation of the Committee to Select Hour Speakers for Eastern Sectional Meetings; received by the editors March 12, 1973.

AMS (MOS) subject classifications (1970). Primary 32H20, 14G99, 53C99, 14K05.

subvariety of its Jacobian, and one had the conjecture:

(1.2) *Let V be a subvariety of an abelian variety which does not contain the translation of an abelian subvariety of dimension $\geqq 1$. Then V has the Mordell property.*

I therefore looked for a way to unify this with the previous one, and it seems that the most natural hypothesis on V is hyperbolicity. There are alternative conditions defining this property, not known at present to be equivalent. The following two conditions are the most relevant for us.

H 1. *The Kobayashi metric is strictly positive and V is complete.*

(For the Kobayashi metric, see [**K 1**].)

H 2. *The sectional holomorphic curvature is bounded above by a negative constant, and V is complete.*

(Cf. Kobayashi [**K 1**, Chapter III, Theorem 4.11].) The second condition could be weakened slightly to require the property only of an unramified covering. The first condition is usually taken as the definition. Then we conjecture that:

(1.3) *If V is a projective hyperbolic variety, then V has the Mordell property.*

A variety satisfying the hypotheses of (1.1) is always hyperbolic. It does not seem to be known if the universal covering space of a hyperbolic variety is a bounded domain. Note that (1.2) is related to (1.3). I owe to Griffiths the remark that if a subvariety of an abelian variety does not contain the translate of an abelian subvariety of dimension $\geqq 1$, then its curvature is strictly negative. Indeed, the holomorphic curvature is decreasing on submanifolds [**K 1**, Chapter III, Theorem 1.1], and if the curvature were to be 0 at a point, then this would imply that there is a flat torus passing through that point, i.e. an abelian subvariety. Thus (1.3) implies (1.1) and (1.2), assuming all varieties nonsingular. The question also arises whether the universal covering space of a subvariety of an abelian variety as in (1.2) is a bounded domain.

There are "obvious" geometric ways of generating rational points on some varieties, for instance, if they contain a straight line or an elliptic curve. Neither is possible for hyperbolic varieties, cf. [**K 1**, Chapter V, Theorem 1.1]. If V admits a bounded domain as universal covering space, then we can see this from the Liouville theorem that a bounded holomorphic function is constant. Another way of generating rational points is by means of an infinite group of automorphisms, also impossible for hyperbolic varieties [**K 1**, Chapter V, Corollary 2.3].

As usual, the absolute Mordell property has a relative formulation for algebraic families of hyperbolic varieties: If there is an infinity of sections, then the family contains split subfamilies, and almost all sections are due to constant sections. In the split case, i.e. when one deals with the product of a hyperbolic variety and a fixed variety, we are thus led to consider the following conjecture, whose proof would give a generalization of a theorem of De Franchis for curves of genus $\geqq 2$ (cf. [**L 1**, Chapter VII, Historical Note]):

(1.4) *Let V be a projective hyperbolic variety and W any algebraic variety. Then there is only a finite number of surjective rational maps of W onto V.*

2. **Integral points.** Let V be an affine variety. We shall say that V has the **Siegel property** if V has only a finite number of points in any finitely generated ring (without divisors of zero) over the integers $\boldsymbol{Z}$. Siegel's theorem is that a curve of genus $\geqq 1$ has this property. Some time ago, I conjectured that affine subsets of abelian varieties have this property [**L 3**], [**L 1**]. One possible approach is through the methods which have been developed in connection with the theory of transcendental numbers, as suggested in [**L 3**]. Let A be an abelian variety defined over a number field K. We suppose that A is embedded in projective space. Let A_K be the group of points on A rational over K. The Mordell-Weil theorem states that A_K is finitely generated. The notion of height of a point can be defined in general. For simplicity let us assume further that $K=\boldsymbol{Q}$. If $(x_0, \cdots, x_{d'})$ are projective coordinates for a point P in A_K, with $x_i \in \boldsymbol{Z}$ $(i=0, \cdots, m)$ relatively prime to each other, then the height is defined by

$$H(P) = \max_i |x_i(P)|.$$

Let $P^1, \cdots, P^n$ be a basis for the Mordell-Weil group A_K, modulo torsion. Given $P \in A_K$ there exists a torsion point Q and integers q_j such that

$$P = q_1P^1 + \cdots + q_nP^n + Q.$$

By the quadraticity of the Néron-Tate height [**N**], [**L 2**], there exist constants C_1, C_2 such that $C_1^{q^2} \leqq H(P) \leqq C_2^{q^2}$ for all $P \in A_K$. More precisely, $\log H(P)$ is equal to a quadratic function of P, plus a linear function, plus a bounded function. If φ, ψ are two positive functions, let us use the Vinogradov notation, and write $\varphi \ll \psi$ if there exists a constant C such that $\varphi \leqq C\psi$. We write $\varphi \gg\ll \psi$ if $\varphi \ll \psi$ and $\psi \ll \varphi$. Then we have $\log H(P) \gg\ll q^2$.

We may view the complex points $A_{\boldsymbol{C}}$ as parametrized by abelian functions on $\boldsymbol{C}^d$ ($\dim A = d$), relative to a suitably normalized exponential

map, represented by theta functions, $\exp: \boldsymbol{C}^d \to A_C$, normalized so that the differential at the origin is algebraic. For $i=1, \cdots, d'$ let

$$f_i(z) = x_i(\exp(z)), \qquad z \in \boldsymbol{C}^d.$$

If $\exp u$ is an algebraic point on A, we call u an algebraic point of the exponential map, or also an abelian logarithm of an algebraic point on A. Let

$$\exp w = Q, \qquad \exp u^j = P^j, \quad \text{with } w, u^j \in \boldsymbol{C}^d.$$

Then w is a division point of a period. We have

$$\exp(q_1 u^1 + \cdots + q_n u^n + w) = P.$$

Suppose that A_K contains infinitely many integral points with respect to the affine coordinates $y_i = x_i/x_1$, so that $y_1 = 1$. If P is such an integral point, then for some coordinate, say y_0, we have

$$|y_0(P)| = H(P) \geqq C^{q^2}.$$

Let $x_i = y_i/y_0$, so that $x_1 = 1/y_0$. Then $|x_1(P)| \leqq C^{-q^2}$.

Suppose that A_K contains infinitely many integral points. Selecting a subsequence of these if necessary, we may assume without loss of generality that the following condition holds. In their expression as a linear combination of a basis of the Mordell-Weil group, the same torsion point Q occurs. For all such points, we have $|y_0(P)| = H(P)$. These integral points converge to a point on the divisor of zeros of f_1, say to a point $P^0 = \exp u^0$. In the case of dimension 1, as already pointed out in [**L 4**], Siegel's theorem that there is only a finite number of integral points on an elliptic curve follows from an approximation statement of type

$$|q_1 u^1 + \cdots + q_n u^n - r\omega - u^0| > e^{-\tau(q)},$$

where τ is a function of q which is $o(q^2)$, r is a fixed rational number, and ω is a period. Indeed, after a projective linear transformation over $\boldsymbol{Z}$, we may assume that $f = (f_1, \cdots, f_d)$ gives an analytic isomorphism in a neighborhood of u^0. Then $|f(z)-f(u^0)|$ and $|z-u^0|$ have the same order of magnitude, so that the inequality in terms of the algebraic function on A can be transferred to an inequality on the universal covering space, in terms of the abelian logarithms.

Recently, Masser was able to prove the desired diophantine inequality, with a function $\tau(q) = q^\varepsilon$, for elliptic curves with complex multiplication [**M 2**].

In the higher dimensional case one does not have much information about the point u^0. First, it may be that $\exp u^0$ is not algebraic. Second, in order to prove the finiteness of integral points, one needs a conjecture of the following type.

(2.1) *Let x be a nonconstant abelian function. If $\tau(q)=o(q^2)$, then we have*

$$|x(P)| \geqq e^{-\tau(q)}$$

for all $P \in A_K$ not lying in the divisor of zeros of x, and $9 \gg\ll \log H(P)$ sufficiently large.

Of course, one conjectures the much stronger inequality with a function $\tau(q) = C \log q$ with a sufficiently large constant C, or even a constant C only epsilon larger than the "Dirichlet exponent" which guarantees that points can always be found to satisfy the inequality. Cf. [**L 4**].

Thus the conjecture applies to a single function. It is then a problem to prove diophantine inequalities first simultaneously for all the coordinates $(f_1, \cdots, f_d)$, and then to eliminate one after the other to get similar inequalities with one function. I was able to generalize part of Masser's results for *all* the coordinates in [**L 9**], although the measure function $\tau(q)$ which I obtain is poor. It is enough to prove the transcendence of $\exp(\alpha^1 u^1 + \cdots + \alpha^n u^n)$ when the α^j are algebraic, and when, for each i, some component α_i^j does not lie in the field of complex multiplication. This is a small beginning in the desired direction.

From the point of view of integral points, we are also led to relationships between the values of functions and their heights. For simplicity, let A be a simple abelian variety defined over K, and let φ be a nonconstant abelian function. I expect that the height of $\varphi(P)$ tends to infinity, for P ranging over any infinite subset of A_K. This is implied by (1.2). Indeed, if the height of $\varphi(P)$ is bounded, then φ takes on only a finite number of values, and the points P lie in the divisors of such values. Another problem here is whether one can extend to one coordinate the quadraticity of the height.

However, even as the height goes to infinity rapidly, from the point of view of Mordell-type conjectures, I also would expect a rather strong limitation on the speed with which the absolute value of the coordinate goes to infinity, in line with (2.1). For instance one expects an inequality $|\varphi(P)| \geqq q^C$, for $P \in A_K$ such that $\varphi(P)$ is defined, and $q^2 \gg\ll \log H(P)$ sufficiently large, as mentioned above.

The absolute value $|\varphi(P)|$ can also be interpreted geometrically as being of the order of magnitude of a power of the distance of P to the divisor of zeros of φ, when $|\varphi(P)|$ tends to 0. Thus the above inequality can be interpreted as giving a limitation to the closeness between a point in A_K and the divisor of zeros of (φ). Considering φ^{-1} instead of φ gives an interpretation in terms of poles.

Even on an elliptic curve without complex multiplication, if ω_1, ω_2 are fundamental periods and u^0 is an algebraic point for the Weierstrass $\wp$

function, it is still a problem to prove an inequality of type

(2.2) $$|q_0u^0 + q_1\omega_1 + q_2\omega_2| > \exp(-q^\varepsilon), \qquad q = \max |q_j|.$$

A similar inequality can be asked p-adically. It is known and easy to prove that if f is an elliptic function and $f(u)$ is algebraic, then the denominators of $f(u/p^n)$ are bounded when p is a prime number and $n \to \infty$. It is a problem to generalize this to abelian varieties, and to give inequalities (lower bounds) for the closeness of u/p^n to the divisor of zeros or poles of f if u/p^n does not lie in such a divisor.

Thus one is led to consider single functions rather than a set of local uniformizing parameters in proving desired diophantine inequalities. In this line, when an abelian variety does not have complex multiplication, or when it is not strongly normalized (for the definition, cf. **[L 4]**), it is still unknown that

(2.3) *If u is an algebraic point for the exponential map, $u \neq 0$, then every coordinate of u is transcendental.*

In the special case when A has complex multiplication and the exponential map is strongly normalized, I proved it as a corollary of a theorem of Bombieri **[B 1]**, **[L 9]**.

For inequalities giving measures of transcendence in cases simpler than (2.2) and (2.3), cf. Baker **[Ba 1]]** **[Ba 2]**, Feldman **[F]**, Coates **[Co 1]**, **[Co 2]**, Masser **[M 1]**.

3. **Algebraic points.** There is a certain class of results which in the past has been obtained essentially by congruence methods. For instance, the Mordell-Weil theorem. On the other hand, one knows that two algebraically independent functions cannot take algebraic values at any point when suitably normalized and when they satisfy a differential equation **[Sch]**, **[L 8]**. This suggests that the Mordell-Weil theorem, which concerns one function, the Weierstrass $\wp$-function, and its derivative, should be provable by methods related to those used in the theory of transcendental numbers and diophantine approximations.

Furthermore, it is also reasonable to expect that one can attack the isogeny theorem (still a conjecture due to Serre) by these methods. It states:

(3.1) *Let A, B be elliptic curves defined over a number field, K, and without complex multiplication. If their Galois representations $V_p(A)$ and $V_p(B)$ are isomorphic, then the curves are isogenous.*

Let us recall briefly the definitions involved in this statement. For more details, see Serre **[Se]** and **[L 7**, Chapter XVI]. Let $A^{(p)}$ denote the group of points on A whose order is a power of a prime p. Let A_{p^n} denote the

group of points on A of order dividing p^n. Let $V_p(A)$ be the set of all infinite vectors $(a_0, a_1, a_2, \cdots)$ where $a_0 \in A^{(p)}$ and $pa_{i+1} = a_i$ for all i. Then $V_p(A)$ is a vector space over $\boldsymbol{Q}_p$, and the Galois group $G = \mathrm{Gal}(\bar{K}/K)$ operates on $V_p(A)$ in a natural way. If $\sigma \in G$ then $\sigma(a_0, a_1, \cdots) = (\sigma a_0, \sigma a_1, \cdots)$. Serre proved the theorem when one of the two curves has a j-invariant which is not integral for some prime number.

One can approach the problem by disregarding the representation aspects and concentrating on the degrees of the fields of division points $K(A_{p^n})$. (One reason for this lies in [**L 7**, Theorem 1, Chapter 16, §1]. If $K(A^{(p)}) = K(B^{(p)})$, then the p-adic Galois representations on $V_p(A)$ and $V_p(B)$ become isomorphic over a finite extension of K. Thus enough knowledge about the degree of the fields of division points implies automatically the isomorphism of the representations.) If A does not have complex multiplication, a theorem of Serre asserts that the degree of p^n-division points satisfies the inequality

$$[K(A_{p^n}) : K] \gg p^{4n}.$$

The Galois group $\mathrm{Gal}(K(A^{(p)})/K)$ is closed in $\mathrm{GL}_2(\boldsymbol{Z}_p)$, and is a Lie subgroup. Therefore it is a priori clear that the degrees above have order of increase p^n, or p^{2n}, or p^{3n}, or p^{4n}. The fields $K(A^{(p)})$ and $K(B^{(p)})$ have the field of all p^nth roots of unity in common.

A very simple argument based on the fact that $\mathrm{SL}_2(\boldsymbol{Z}_p)$ does not contain a closed, normal, nontrivial subgroup of infinite index shows that either

$$[K(A_{p^n}, B_{p^n}) : K] \ll p^{4n},$$

or the fields $K(A^{(p)})$ and $K(B^{(p)})$ are linearly disjoint over a finite extension of the field of all p^nth roots of unity (see [**L 7**, Corollary of Theorem 1, Chapter XVI, §1]). We must then have

$$[K(A_{p^n}, B_{p^n}) : K] \gg p^{7n}.$$

Thus to prove the isogeny theorem, it suffices to prove:

(3.2) *Let A, B be elliptic curves without complex multiplication, defined over a number field K. Let $\varepsilon > 0$. Then*

$$[K(A_{p^n}, B_{p^n}) : K] \gg p^{n(4+\varepsilon)}.$$

The number 4 in the exponent reflects "dimension 4".

The proofs of transcendence for the classical numbers, values of the exponential or Weierstrass function at algebraic numbers, actually have nothing to do with transcendental numbers. Assuming that these values are

algebraic, one derives a contradiction by juggling with arithmetic and analytic inequalities. In fact, a basic theorem ([**Sch**] and [**L 8**]) gives an upper bound for the number of points where certain functions satisfying a differential equation can take values in a fixed number field K. The degree $[K:\boldsymbol{Q}]$ is bounded from below by this number of points and other factors. (Cf. [**L 8**, Theorem 1, Chapter III, §1, and Theorem 2, Chapter II, §2].)

The situation here is completely analogous. Suppose that the elliptic curves A, B are not isogenous. We consider the *five* algebraically independent functions

$$e^{2\pi iz}, \quad \wp_A(\omega_1 z), \quad \wp_A(\omega_2 z), \quad \wp_B(\omega_3 z), \quad \wp_B(\omega_4 z),$$

where $\wp_A$, $\wp_B$ are the Weierstrass functions associated with A and B, and where $[\omega_1, \omega_2]$, $[\omega_3, \omega_4]$ are fundamental periods of $\wp_A$ and $\wp_B$, respectively. One can form the usual approximating function with coefficients in the field of division points,

$$\sum \alpha_{(\lambda)} \wp_A(\omega_1 z)^{\lambda_1} \wp_A(\omega_2 z)^{\lambda_2} \wp_B(\omega_3 z)^{\lambda_3} \wp_B(\omega_4 z)^{\lambda_4} e^{2\pi iz\lambda_0},$$

and activate the standard arguments which have previously been used in proving transcendence results (possibly with variations, using several variables). Although I obtain not completely trivial estimates (lower bounds) for the degrees of the fields of p^nth division points, I fall short of the desired $4+\varepsilon$. The difficulty here is exactly the same as that which one meets when trying to prove a statement like (2.2). Even for one elliptic curve the difficulty arises in trying to prove by these methods the known Serre theorem giving the lower bound $[K(A_{p^n}):K] \gg p^{4n}$. Actually, in this case, a simple Lie theoretic argument (bottom of p. IV-11 in Serre's book [**Se**]) shows that it suffices to prove

$$[K(A_{p^n}):K] \gg p^{n(2+\varepsilon)}$$

showing that the Galois group of $K(A^{(p)})$ has dimension >2 in order to jump immediately to 4. Indeed, if the dimension were 3, one would be led to a contradiction of the Šafarevič theorem, through the irreducibility of the Galois representation on $V_p(A)$. Cf. [**L 7**, Chapter XVII, §§1, 2].

Thus instead of *using* Serre type theorems as in Coates [**Co 1**] to prove transcendence and approximation results, one would *prove* lower bounds on degrees of fields of division points by the methods of diophantine approximations-transcendental numbers. It may also be that these two types of results generate feedback on each other, and by a suitable recursive procedure, one can use one after the other to strengthen results in both directions.

BIBLIOGRAPHY

[Ba 1] A. Baker, *On the periods of the Weierstrass ℘-function*, Symposia Mathematica, vol. IV (INDAM, Rome, 1968/69), Academic Press, New York, 1970, pp. 155–174.

[Ba 2] ———, *An estimate for the ℘-function at an algebraic point*, Amer. J. Math. **92** (1970), 619–622. MR **43** #7409.

[Bo] E. Bombieri, *Algebraic values of meromorphic maps*, Invent. Math. **10** (1970), 267–287. MR **46** #5328.

[Co 1] J. Coates, *An application of the division theory of elliptic functions to diophantine approximation*, Invent. Math. **11** (1970), 167–182. MR **44** #3963.

[Co 2] ———, *Linear forms in the periods of the exponential and elliptic functions*, Invent. Math. **12** (1971), 290–299. MR **45** #3330.

[F] N. Feldman, *An elliptic analogue of an inequality of Gelfond*, Trudy Moskov. Mat. Obšč. **18** (1968), 65–76=Trans. Moscow Math. Soc. **18** (1968), 71–84. MR **40** #1345.

[K 1] S. Kobayashi, *Hyperbolic manifolds and holomorphic mappings*, Pure and Appl. Math., 2, Dekker, New York, 1970. MR **43** #3503.

[K 2] ———, *Some problems on intrinsic distances and measures*, Carathéodory Centennial (to appear).

[L 1] S. Lang, *Diophantine geometry*, Interscience Tracts in Pure and Appl. Math., no. 11, Interscience, New York, 1962. MR **26** #119.

[L 2] ———, *Les formes bilinéaires de Néron et Tate*, Séminaire Bourbaki: 1963/64, Exposé 274, fasc. 3, Secrétariat mathématique, Paris, 1964. MR **31** #1252.

[L 3] ———, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. No. 6 (1960), 27–43. MR **24** #A86.

[L 4] ———, *Diophantine approximation on toruses*, Amer. J. Math. **86** (1964), 521–533. MR **29** #2220.

[L 5] ———, *Some theorems and conjectures in diophantine equations*, Bull. Amer. Math. Soc. **66** (1960), 240–249. MR **22** #9469.

[L 6] ———, *Transcendental numbers and diophantine approximations*, Bull. Amer. Math. Soc. **77** (1971), 635–677. MR **44** #6615.

[L 7] ———, *Elliptic functions*, Addison-Wesley, Reading, Mass., 1974.

[L 8] ———, *Introduction to transcendental numbers*, Addison-Wesley, Reading, Mass., 1966. MR **35** #5397.

[L 9] ———, *Diophantine approximations on abelian varieties with complex multiplication* (to appear).

[M 1] D. Masser, *Transcendence properties of elliptic functions* (to appear).

[M 2] ———, *Algebraic points of an elliptic function* (to appear).

[N] A. Néron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. (2) **82** (1965), 249–331. MR **31** #3424.

[Sch] T. Schneider, *Einführung in die transzendenten Zahlen*, Springer-Verlag, Berlin, 1957. MR **19**, 252.

[Se] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968. MR **41** #8422.