Séminaire BOURBAKI Juin 2024
75e année, 2023–2024, no 1226, p. 643 à 669
doi: 10.24033/ast.1243

UNIFORMITY IN DIOPHANTINE GEOMETRY

by **Thomas Scanlon**

Introduction

Mordell (1922/23) concluded his study of polynomial equations of degrees three and four in rational numbers by saying "in conclusion, I might note that the preceding works suggest to me the truth the following statements, concerning indeterminate equations, none of which, however, I can prove." The last of the statements was that "the same theorem" (namely that there are only finitely many rational solutions) "holds for any homogeneous equation of genus greater than unity, say, $f(x, y, z) = 0$." Mordell's conjecture as such was proven with the celebrated work of Faltings (1983).

The problem of effectively bounding the number of solutions by a function of purely geometric data has remained elusive over the past four decades. This exposé focuses on some recent spectacular progress giving such bounds and also resolving related questions.

What we might mean by effective bounds depends on the situation. When considering Mordell's conjecture as a statement about rational points on curves, one might hope to bound the number of such rational points by a constant depending only on the genus of the curve and the degree over the rational numbers of the number field in which one seeks the solutions. Alternatively, we might hope to find bounds on the sizes as measured, say by height, of the points on such a curve depending on such data as the heights of the coefficient of the defining equations and the genus of the curve. The problem in the first presentation remains open in general. Effective proofs of Mordell's conjecture due to Bombieri (1990) and Vojta (1992) give methods for bounding the number of rational points on a curve from some arithmetic information about the curve. The kind of uniform bounds that we discuss in this exposé align with and improve these bounds by eliminating the dependence on the arithmetic data.

Using the theorem of Mordell (1922/23) and Weil (1929) that the group of rational points on an abelian variety is finitely generated as an abelian group, Lang reformulated the Mordell conjecture in a more geometric form which then naturally generalizes to a statement about higher dimensional varieties.

Start with a finitely generated field K of characteristic zero and C a smooth projective curve of genus at least two over K. Fixing any base point on C (which we may assume to be K-rational, for otherwise $C(K) = \varnothing$ which is finite) we have an embedding of C as a closed algebraic subvariety of its Jacobian, $\mathrm{Jac}(C)$, which is an abelian variety defined over K. Let $\Gamma := \mathrm{Jac}(C)(K)$ be the finitely generated group of K-rational points on the Jacobian. Since the embedding induces a bijection on rational points, we may realize $C(K)$ as the intersection $C(\mathbb{C}) \cap \Gamma$. After making a few other observations, one sees that the Mordell conjecture is equivalent to the assertion that for any abelian variety A over the complex numbers, finitely generated group $\Gamma \leqslant A(\mathbb{C})$, and algebraic curve $C \subseteq A$ of genus at least two, $\Gamma \cap C(\mathbb{C})$ is finite. This formulation of the Mordell conjecture suggests the Mordell–Lang conjecture which asserts that for any abelian variety A defined over the complex numbers, finite *rank* subgroup $\Gamma \leqslant A(\mathbb{C})$ (by which we mean that $\mathrm{rk}\,\Gamma := \dim_{\mathbb{Q}} \Gamma \otimes \mathbb{Q} < \infty$), and closed subvariety $X \subseteq A$, the intersection $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.

The formulation of the Mordell–Lang conjecture suggests geometric approaches to its proof based on such methods as the geometry of numbers and the complex analytic geometry of the presentation of an abelian variety as a complex torus, that is, as the quotient of a finite dimensional complex vector space by a lattice. Historically, some partial results towards Mordell's conjecture used this kind of geometric reasoning, notably with the proof of Mordell's conjecture over function fields by Manin (1963) and the gap principle of Mumford (1965a), but the original proofs of the full theorem are fundamentally arithmetic in nature making use of Arakelov theory.

The main theorem of Gao, Ge, and Kühne (2021) takes the following form.

Theorem 0.1. *There is a function $c(g,d)$ depending on two natural number arguments so that for any abelian variety A over the complex numbers given with an appropriately chosen very ample line bundle L, algebraic subvariety X, and finite rank subgroup $\Gamma \leqslant A(\mathbb{C})$, there is a finite (possibly empty) sequence of connected algebraic subgroups $B_1, \ldots, B_m \leqslant A$ and points $\gamma_1, \ldots, \gamma_m$ so that*

$$X(\mathbb{C}) \cap \Gamma = \bigcup_{i=1}^{m} (\gamma_i + B_i(\mathbb{C})) \cap \Gamma$$

where

$$m \leqslant c(\dim A, \deg_L(X))^{1+\mathrm{rk}\,\Gamma}$$

and $\deg_L(B_i) \leqslant c(\dim A, \deg_L(X))$ *for each i.*

In the special case that X is a curve of genus greater than one embedded in its Jacobian, there are no translates of positive dimensional algebraic subgroups of A contained in X so that Theorem 0.1 asserts simply that the number of points in the intersection $X(\mathbb{C}) \cap \Gamma$ is at most $c^{1+\operatorname{rk}\Gamma}$ where c depends only on the degree of X as a subvariety of A. This uniform result for curves may be obtained by combining the main theorem of Dimitrov, Gao, and Habegger (2021) with the results of Kühne (2021) and answers positively a problem raised by Mazur (1986).

While the proof of Theorem 0.1 does take into account some of the geometric methods anticipated by Lang's formulation of the Mordell–Lang conjecture, refined height estimates and equidistribution theorems are at its heart. The method used yields uniform versions of the Bogomolov conjecture about points of small height on subvarieties of abelian varieties. We will delay the statement of this theorem until after we have reviewed some of the theory of heights in Section 1.2.

A crucial new ingredient in these proofs is the study of "non-degenerate varieties" which may be defined in terms of differential geometric properties of the Betti map. We delay a description of this condition to Section 3.

An alternative approach to the uniform Mordell–Lang and Bogomolov conjectures is given by Yuan (2021). Yuan's method is based on a refined theory of adèlic line bundles developed by Yuan and Zhang (2021) and circumvents the analysis of non-degenerate varieties.

The main body of this exposé is organized as follows. We begin in Section 1 by recalling some of the theory of abelian varieties and of height functions. We recall some of the earlier work on these problems in Section 2. In particular, in Subsection 2.1 we recall the methods of Mumford and Vojta which were then refined and extended by Rémond for analyzing points which are nearly parallel relative to the height pairing. In Subsection 2.2 we survey some of the work on points of small height, discussing specifically the Manin–Mumford and Bogomolov conjectures. Section 3 is devoted to Betti maps and their interaction with algebraic subvarieties of abelian varieties. We enter into some of the technical details of the uniform Mordell–Lang conjecture in Section 4 where we outline the proof of the crucial new height inequality of Dimitrov, Gao, and Habegger (2021). We explain how points of small height are to be analyzed in Section 5. Finally, in Section 6 the new height inequalities and equidistribution theorems are combined to deduce the new uniform diophantine geometric theorems.

1. Basic properties of the arithmetic and geometry of abelian varieties

1.1. Abelian varieties

Abelian varieties lie at the core of the theorems we are considering. This subject is classical and well exposed in several excellent textbooks and course notes, including Lang (1983), Lange (2023), Milne (2008), and Mumford (2008). In this section we recall some of the basic theory.

By definition, an abelian variety A over a field K is a connected, projective algebraic group. It is a consequence of this definition that the group structure on A is commutative so that the adjective "abelian" which was chosen to honor Abel's work on abelian integrals remains consistent with our common practice of calling commutative groups "abelian".

When $K = \mathbb{C}$ is the field of complex numbers, then since A is projective, the group $A(\mathbb{C})$ is a compact, commutative, connected, complex Lie group. As such, $A(\mathbb{C})$ fits into an exact sequence of complex Lie groups

$$0 \longrightarrow \Lambda_A \longrightarrow T_0 A(\mathbb{C}) \xrightarrow{\exp_A} A(\mathbb{C}) \longrightarrow 0$$

where $T_0 A$ is the tangent space of A at the identity element 0, $\exp_A$ is the Lie exponential map of A, and $\Lambda_A := \ker \exp_A$ is a lattice in $T_0 A(\mathbb{C})$. Fixing a basis of $T_0(\mathbb{C})$ we may regard it as $\mathbb{C}^g$ where $g = \dim A$ and $A(\mathbb{C})$ as the quotient $\mathbb{C}^g/\Lambda_A$, a complex torus.

Passing to universal covers, it is easy to see that the data of a map of complex tori $\psi\colon A(\mathbb{C}) \to B(\mathbb{C})$ between complex abelian varieties is equivalent to that of a linear map $\widetilde{\psi}\colon T_0 A(\mathbb{C}) \to T_0 B(\mathbb{C})$ which takes Λ_A to Λ_B. In this way, the space of complex tori of dimensions g may be parameterized by the space of lattices in $\mathbb{C}^g$ up to the action of $\mathrm{GL}_g(\mathbb{C})$. Since not every complex torus is (the analytification of) an abelian variety, we must restrict the space of lattices in order to describe moduli spaces of abelian varieties.

Let $\mathfrak{h}_g$ be the g^{th} Siegel upper halfspace consisting of symmetric $g \times g$ complex matrices whose imaginary parts are positive definite. For a sequence $D = \langle d_1, \ldots, d_g \rangle$ of positive integers with $d_i | d_{i+1}$ for $1 \leqslant i < g$ we overload our notation writing $D = \mathrm{diag}(d_1, \ldots, d_g)$ for the diagonal matrix with d_i in the (i,i)-entry for $1 \leqslant i \leqslant g$.

The algebraic group $\mathrm{Sp}_{2g,D}$ is defined by

$$\mathrm{Sp}_{2g,D} := \{ g \in \mathrm{GL}_{2g} : g \begin{pmatrix} 0 & -D \\ D & 0 \end{pmatrix} g^{\mathsf{T}} = \begin{pmatrix} 0 & -D \\ D & 0 \end{pmatrix} \} .$$

Writing elements of $\mathrm{Sp}_{2g}(\mathbb{R})$ as 2×2 matrices of $g \times g$ real matrices, we have a transitive action of $\mathrm{Sp}_{2g}(\mathbb{R})$ on $\mathfrak{h}_g$ via the formula

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \tau = (A\tau + B)(C\tau + D)^{-1} .$$

Via this action, we may see $\mathfrak{h}_g$ as the quotient of Sp_{2g} by the unitary group.

Form the semidirect product $\mathbb{R}^{2g} \rtimes \mathrm{Sp}_{2g,D}(\mathbb{R})$ via the usual action of GL_{2g} on $2g$-dimensional space. This group $\mathbb{R}^{2g} \rtimes \mathrm{Sp}_{2g,D}(\mathbb{R})$ acts on $\mathbb{C}^g \times \mathfrak{h}_g$ via the rule

$$(r_1, \ldots, r_{2g}, M) \cdot (z, \tau) := (z + (r_1, \ldots, r_g)D + (r_{g+1}, \ldots, r_{2g})\tau, M \cdot \tau) .$$

Given $\tau \in \mathfrak{h}_g$, we form the lattice $\Lambda_{\tau,D} := D\mathbb{Z}^g + \tau\mathbb{Z}^g$. The complex torus $\mathbb{C}^g/\Lambda_{D,\tau}$ is an abelian variety with a polarization of type D. Moreover, (the analytification of) every complex abelian variety arises in this way.

The coarse moduli space of g-dimensional abelian varieties with a polarization of type D may be realized as $\mathrm{Sp}_{2g,D}(\mathbb{Z})\backslash\mathfrak{h}_g$. Taking appropriate arithmetic subgroups $\Gamma \leqslant \mathrm{Sp}_{2g,D}(\mathbb{Z})$ the quotient $\mathscr{A}_{g,D,\Gamma} = \Gamma\backslash\mathfrak{h}_g$ may be seen as a quasiprojective variety over the algebraic numbers giving a fine moduli space for polarized g-dimensional abelian varieties with some level structure and the universal abelian variety $\mathfrak{A}_{g,D,\Gamma} \to \mathscr{A}_{g,D,\Gamma}$ may be realized as the quotient $(\mathbb{Z}^{2g} \rtimes \Gamma)\backslash(\mathbb{C}^g \times \mathfrak{h}_g)$. For example, if $N \geqslant 3$ and Γ is the kernel of the reduction map from $\mathrm{Sp}_{2g,D}(\mathbb{Z}) \to \mathrm{Sp}_{2g,D}(\mathbb{Z}/N\mathbb{Z})$ then $\mathscr{A}_{g,D,\Gamma} = \mathscr{A}_{g,D,N}$ is the moduli space of abelian varieties with a polarization of type D and full level N structure.

For almost all of the problems we consider, the specific choice of polarization type and level structure is irrelevant. Indeed, even when one must keep track of these data in the course of a proof, one can usually reduce to the case of principally polarized abelian varietes. We shall simply write $\mathfrak{A}_g \to \mathscr{A}_g$ for some suitable choice of a universal abelian variety of dimension g.

Given an algebraically closed field k of characteristic zero, K an algebraically closed extension of k, and A an abelian variety over K, the K/k-trace of A, $\mathrm{Tr}_{K/k} A$, is an abelian variety over k given together with an embedding $\rho\colon (\mathrm{Tr}_{K/k} A)_K \hookrightarrow A$ of its base change to K in A. We write $A^{K/k}$ for the image of ρ. The map ρ is universal for maps from abelian varieties over k to A in the sense that if B is an abelian variety defined over k and $\psi\colon B_K \to A$ is a map of algebraic groups from the base change of B to K to A then there is a unique map $\widetilde{\psi}\colon B \to \mathrm{Tr}_{K/k} A$ for which $\psi = \rho \circ \widetilde{\psi}_K$.

1.2. Heights

Heights give a precise sense to the arithmetic size of points on algebraic varieties. For accounts of the theory of heights see Bombieri and Gubler (2006) or Lang (1995).

We mostly restrict our attention to heights of $\mathbb{Q}^{\mathrm{alg}}$-valued points of algebraic varieties. However, we should note that theories of heights make sense for points valued in other fields, for example, in algebraic extensions of function fields and that this more general theory makes an appearance with the function field Bogomolov conjecture.

Consider a number field K. By a normalized place v on K we mean an absolute value $|\ |_v$ which comes by pullback from an embedding of K into $\mathbb{R}$, $\mathbb{C}$, or a finite extension of $\mathbb{Q}_p$. Let us write K_v for the completion of K with respect to this absolute value. We define $d_v := [K_v : \mathbb{R}]$ if $|\ |_v$ is not ultrametric and $d_v := [K_v : \mathbb{Q}_p]$ if K_v is a finite extension of the p-adic numbers.