348

ASTÉRISQUE

2012

SÉMINAIRE BOURBAKI
VOLUME 2010/2011
EXPOSÉS 1027-1042

(1037) *A proof of the André-Oort conjecture via mathematical logic*

Thomas SCANLON

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Séminaire BOURBAKI Avril 2011
63e année, 2010-2011, no 1037, p. 299 à 315

A PROOF OF THE ANDRÉ-OORT CONJECTURE VIA MATHEMATICAL LOGIC [after Pila, Wilkie and Zannier]

by **Thomas SCANLON**

INTRODUCTION

Extending work of Bombieri and Pila on counting lattice points on convex curves [**4**], Pila and Wilkie proved a strong counting theorem on the number of rational points in a more general class of sets *definable* in an o-minimal structure on the real numbers [**37**]. Following a strategy proposed by Zannier, the Pila-Wilkie upper bound has been leveraged against Galois-theoretic lower bounds in works by Daw, Habegger, Masser, Peterzil, Pila, Starchenko, Yafaev and Zannier [**6, 18, 25, 31, 36, 38**] to prove theorems in diophantine geometry to the effect that for certain algebraic varieties the algebraic relations which may hold on its "special points" are exactly those coming from "special varieties". Of these results, Pila's unconditional proof of the André-Oort conjecture for the j-line is arguably the most spectacular and will be the principal object of this resumé. Readers interested in a survey with more details about some of the other results along these lines, specifically the Pila-Zannier reproof of the Manin-Mumford conjecture and the Masser-Zannier theorem about simultaneous torsion in families of elliptic curves, may wish to consult my notes for the Current Events Bulletin lecture [**42**].

Acknowledgements. I wish to thank M. Aschenbrenner, J. Pila and U. Zannier for their advice and especially for suggesting improvements to this text.

1. STATEMENT OF THE ANDRÉ-OORT CONJECTURE

The collection of theorems and conjectures broadly known under the rubric of the André-Oort conjecture arose from a conjecture proposed by André about curves in Shimura varieties [**1**] and a related conjecture of Oort that a subvariety of a moduli

space of principally polarized abelian varieties which contains a Zariski dense set of moduli points of abelian varieties with complex multiplication must be a variety of Hodge type [**29**]. The assertion now generally regarded as *the* André-Oort conjecture takes as its starting point the theory of Shimura varieties as presented in terms of Deligne's Shimura data and predicts that the Zariski closure of a set of special points in a Shimura variety must be a finite union of varieties of Hodge type. The full André-Oort conjecture paints a beautiful picture of the way in which the diophantine geometry of Shimura varieties reflects the presentation of these varieties as quotients of homogeneous spaces by the action of an arithmetic group. However, since too much theoretical overhead is required to correctly state this conjecture and even more is required to do the subject justice, not to mention the fact that Noot's excellent survey [**28**] is already available, we shall restrict to the case considered in [**36**].

Let us recall some of the classical complex analytic theory of elliptic curves as one would find in such sources as [**43**] or [**45**].

Let $\mathfrak{h} := \{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0\}$ be the upper half plane consisting of those complex numbers with positive imaginary part. For $\tau \in \mathfrak{h}$, let $E_\tau := \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ be the one-dimensional complex torus (which is necessarily an elliptic curve, that is, a connected, one-dimensional algebraic group) obtained as the quotient of the additive group of the complex numbers by the lattice generated by 1 and τ. The group $\mathrm{PSL}_2(\mathbb{R})$ acts transitively on $\mathfrak{h}$ via fractional linear transformations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z := \frac{az+b}{cz+d}$. A simple computation shows that $E_\tau \cong E_\sigma$ just in case there is some $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ with $\gamma \cdot \tau = \sigma$. Hence, as a set, we may identify the set of isomorphism classes of complex elliptic curves with $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathfrak{h}$. The analytic j-function (or "modular function") $j : \mathfrak{h} \to \mathbb{C}$ is a surjective holomorphic function which is exactly $\mathrm{PSL}_2(\mathbb{Z})$-invariant in the sense that $j(\tau) = j(\sigma)$ if and only if $\sigma = \gamma \cdot \tau$ for some $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$. Thus, using j we may identify $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathfrak{h}$ with $\mathbb{C} = \mathbb{A}^1(\mathbb{C})$ and we say that a number $\xi \in \mathbb{C}$ is the j-invariant of an elliptic curve E if there is some $\tau \in \mathfrak{h}$ for which $\xi = j(\tau)$ and $E \cong E_\tau$.

From the general theory of covering spaces, one sees that

$$\mathrm{Hom}(E_\tau, E_\sigma) = \{\lambda \in \mathbb{C} \ : \ \lambda(\mathbb{Z} + \mathbb{Z}\tau) \subseteq \mathbb{Z} + \mathbb{Z}\sigma\}.$$

Specializing to the case of $\tau = \tau'$ one sees that the endomorphism ring of E_τ is strictly larger than $\mathbb{Z}$ just in case τ is a quadratic imaginary number. In this case we say that E_τ has complex multiplication or that it is a CM-elliptic curve. From the above considerations, we see that a number $\xi \in \mathbb{A}^1(\mathbb{C})$ is the j-invariant of a CM-elliptic curve just in case ξ is the value of j on a quadratic imaginary number. In this way, we may regard the moduli points of CM-elliptic curves as the special values of the modular function. We say that a point $(\xi_1, \ldots, \xi_n) \in \mathbb{A}^n(\mathbb{C})$ is a *special point* just in case each ξ is a CM-moduli point.

For a positive integer $N \in \mathbb{Z}_+$ the N^{th} Hecke correspondence is the following set

$$T_N(\mathbb{C}) := \{(j(\tau), j(N\tau)) \ : \ \tau \in \mathfrak{h}\}.$$

The Hecke correspondence T_N is actually an algebraic subvariety of $\mathbb{A}^2$ defined by the vanishing of the so-called N^{th} modular polynomial $\Phi_N(x, y)$. From the definition of T_N it is obvious that $T_N(\mathbb{C})$ contains a Zariski dense set of special points as if τ is a quadratic imaginary number, then so is $N\tau$. Pila's theorem asserts that in a precise sense these are the only interesting varieties which contain a dense set of special points.

THEOREM 1.1. — *Let $n \in \mathbb{Z}_+$ be a positive integer and $X \subseteq \mathbb{A}^n_{\mathbb{C}}$ an irreducible subvariety of affine n-space over the complex numbers. If X contains a Zariski dense set of special points, then X is a special variety. That is, it is a component of a variety defined by equations of the form $\Phi_M(x_i, x_j) = 0$ and $x_\ell = \xi$ where Φ_M is a modular polynomial and ξ is a special point.*

Remark 1.2. — Theorem 1.1 is not the strongest theorem proven in [**36**]. Using the methods outlined in this survey, Pila proved some cases of Pink's generalization of the André-Oort conjecture to mixed Shimura varieties in which the ambient variety is taken to be a product of a finite sequence of curves where each factor is a modular curve, an elliptic curve or the multiplicative group.

Remark 1.3. — Approximations to and conditional generalizations of Theorem 1.1 were proven some time ago. Restricting to the case that X is a curve, Edixhoven already proved Theorem 1.1 under the hypothesis of the generalized Riemann hypothesis in [**13, 14**] while André shortly thereafter gave an unconditional proof [**2**]. Edixhoven and Yafaev proved the André-Oort conjecture allowing the ambient variety to be an arbitrary Shimura variety but taking the subvariety X to be a curve under an hypothesis about constancy of the Hodge structure in [**15**]. Yafaev then proved the André-Oort conjecture under the Generalized Riemann Hypothesis for CM-fields where the subvariety is again a curve. In more recent work, building on results of Ullmo and Yafaev [**49**], Klingler and Yafaev [**22**] have proven the full André-Oort conjecture under either the technical hypothesis of [**15**] or under GRH. Working locally, Moonen proved a p-adic analogue of the André-Oort conjecture for moduli spaces of abelian varieties [**27**].

All of the known proofs share a common fundamental structure. Geometric reasoning leads to upper bounds on the number of special points lying on a given non-special variety outside of its positive dimensional special subvarieties. Arguments of an analytic number theoretic nature combined with some Galois-theoretic considerations produce lower bounds which outstrip the upper bounds if there are too many special

points. In the papers preceding [**36**], the upper bounds generally come from intersection theory whereas in [**36**], the upper bounds come from the Pila-Wilkie counting theorem for o-minimal theories.

2. FIRST STEPS TOWARDS THE PROOF

The reader is likely familiar with the ploy of introducing the theory of elliptic curves via complex analysis only to shift the perspective to algebraic number theory and algebraic geometry as soon as diophantine issues arise. However, in the case of Theorem 1.1, the proof proceeds through the complex analytic presentation.

Let us begin with $X \subseteq \mathbb{A}^n$ an affine algebraic variety and let us fix some polynomials $F_1(x_1, \dots, x_n), \dots, F_\ell(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ for which

$$X(\mathbb{C}) = \{(a_1, \dots, a_n) \in \mathbb{A}^n(\mathbb{C}) \ : \ F_i(a_1, \dots, a_n) = 0 \text{ for } i \leq \ell\}.$$

We wish to describe the set of special points on X. That is, we wish to describe the set of n-tuples of quadratic imaginary numbers $(\tau_1, \dots, \tau_n)$ for which $F_1(j(\tau_1), \dots, j(\tau_n)) = \cdots = F_\ell(j(\tau_1), \dots, j(\tau_n)) = 0$.

Consider the following real analytic set

$$\begin{aligned} \mathfrak{X} \ := \ & \{(x_1, \cdots, x_n, y_1, \dots, y_n) \in \mathbb{R}^n \times (\mathbb{R}_+)^n \ : \\ & F_t(j(x_1 + i\sqrt{y_1}), \dots, j(x_n + i\sqrt{y_n})) = 0 \text{ for } t \leq \ell\}. \end{aligned}$$

The set of special points of $X(\mathbb{C})$ is the image of the set of rational points on $\mathfrak{X}$ under the map

$$(x_1, \dots, x_n, y_1, \dots, y_n) \mapsto (j(x_1 + i\sqrt{y_1}), \dots, j(x_n + i\sqrt{y_n})).$$

Thus, we have succeeded in reducing the admittedly difficult André-Oort conjecture to the intractable problem of describing the set of rational points on a real analytic variety. Since each subset of $\mathbb{Z}^{2n}$ may be realized as the zero set of a real analytic function, knowing merely that $\mathfrak{X}$ is real analytic yields no useful information. On the other hand, even knowing that $\mathfrak{X}$ is defined by particularly simple equations does not seem to help as, for instance, the problem of describing the rational points on an algebraic variety is notoriously difficult.

The strength of this reduction comes from $\mathfrak{X}$ avoiding these extremes of a general real analytic variety on one hand and of an algebraic variety on the other. The geometry of $\mathfrak{X}$ is simple in that, at least when it is restricted to an appropriate fundamental domain, it is definable in an o-minimal expansion of the real field. For such sets, the counting theorem of Pila and Wilkie gives subpolynomial (in a bound on the height) bounds for the number rational points lying in the set provided that one excludes those points lying on semi-algebraic curves.