Pila's proof of the André-Oort conjecture – pt.1

Blaise Boissonneau
PhD student of Franziska Jahnke

WWU, Münster

February 9, 2021

Goal

Conjecture (André-Oort)

Let X be a Shimura variety and let Σ be a set of special points in X. Let V be the Zariski closure of Σ. Then the irreducible components of V are special subvarieties.

In 2011, Pila proved AOC in the case where X is a product of modular curves, elliptic curves, and copies of $\mathbb{C}^\times$ (see [Pil11]). We will expose his proof in this talk and in next week's talk, following Scanlon's formulation (see [Sca17], sec. 5.2).

The j-invariant

We recall some properties of the function $j : \mathbb{H} \mapsto \mathbb{A}^1(\mathbb{C})$:

- j is surjective.
- j is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, and induces an isomorphism $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{A}^1(\mathbb{C})$.
- j is complex analytic or real analytic when we identify $\mathbb{C}$ with $\mathbb{R}^2$ in the usual way.
- For any $\tau \in \mathbb{H}$, we consider the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$. We have $E_\tau \cong E_{\tau'}$ iff $j(\tau) = j(\tau')$.

With help of the last fact, we can consider $\mathbb{A}^1(\mathbb{C})$ as a moduli space of elliptic curves, that is, to each point $j(\tau) \in \mathbb{A}^1(\mathbb{C})$ corresponds an isomorphism class of elliptic curves. When seen as a moduli space, we call $\mathbb{A}^1(\mathbb{C})$ the j-line.

The j-line is the prototypical example of a modular curve.

Modular curves

Definition (congruence subgroups)

- The *principal congruence subgroup* of order n is $\Gamma(n) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod n\}$.
- A *congruence subgroup* is any subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(n)$ for some n.

Recall that $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H} = \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$ by:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \tau \to \frac{a\tau+b}{c\tau+d}$$

Proposition (C.13.12 in [Sil86])

Let Γ be a congruence subgroup, then there exist a smooth affine curve Y_Γ and a complex analytic function $j_\Gamma : \mathbb{H} \mapsto Y_\Gamma$ invariant under the action of Γ and inducing an isomorphism $\mathbb{H}/\Gamma \cong Y_\Gamma$.

We call Y_Γ a modular curve and j_Γ its canonical covering. Note that if $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then $j_\Gamma = j$ and $Y_\Gamma = \mathbb{A}^1(\mathbb{C})$.

Special points

Fix a modular curve Y and consider its canonical covering $j_\Gamma : \mathbb{H} \mapsto Y$. We can then see Y as a weak moduli space of elliptic curves: to each $y \in Y$ corresponds $\{E_\tau \mid \tau \in \mathbb{H}, j_\Gamma(\tau) = y\}$. Since $j_\Gamma(\tau) = j_\Gamma(\tau')$ iff τ and τ' are Γ-conjugates, those classes only contain isomorphic elliptic curves; but some isomorphic elliptic curves might lie in different classes. When seen as a weak moduli space, we call Y the j_Γ-line.

Definition (Special points)

- If Y is the j_Γ-line, then we call $y \in Y$ special if the corresponding class of elliptic curves has Complex Multiplication (CM).
- If A is an abelian variety, then we call $a \in A$ special if it is a torsion point. This include the case where A is an elliptic curve or $\mathbb{C}^\times$.

A point $(x, y) \in X \times Y$ is special if x and y are both special.

Special subvarieties of modular curves

Let $X = Y_1 \times \cdots \times Y_n$ be a product of modular curves. Fix a partition S of $\{1, \cdots, n\}$. If $s \in S$ is not a singleton, fix $g_i \in \mathrm{GL}_2(\mathbb{Q})$ for each $i \in s$. We call a subvariety Z of X special if $Z = \prod_{s \in S} Z_s$, each Z_s is a subvariety of $\prod_{i \in s} Y_i$, and:

- If s is a singleton, Z_s is a singleton containing only a special point;
- If s is not a singleton, $Z_s = (\prod_{i \in s} j_{\Gamma_i} \circ g_i)(\mathbb{H})$.

In the case where $X = \mathbb{A}^n(\mathbb{C})$, then special subvarieties can equivalently be defined with the help of modular polynomials Φ_n:

Proposition (folklore (Hilbert?))

For each $n > 0$, there exists a minimal polynomial $\Phi_n \in \mathbb{Z}[X, Y]$ such that $\Phi_n(j(n\tau), j(\tau)) = 0$.

A special subvariety of $\mathbb{A}^n(\mathbb{C})$ is then defined by equations of the form $x_k = z$ for z special or $\Phi_n(x_i, x_j) = 0$.

Pila's theorem

Definition (special subvarieties of abelian varieties)

Let A be an abelian variety, let $B \geqslant A$ be an algebraic subvariety, and let $a \in A$ be special (i.e. torsion); then we call $a + B$ a special subvariety.

For a product of the form $Y_1 \times \cdots \times Y_n \times A$, special subvarieties are $Z \times B$ with Z special in $Y_1 \times \cdots \times Y_n$ and B special in A.

Theorem (Pila – AOC)

Let $X = Y_1 \times \cdots \times Y_n \times E_1 \times \cdots \times E_m \times (\mathbb{C}^\times)^\ell$ with Y_i modular curves and E_i elliptic curves defined over $\mathbb{Q}^{\text{alg}}$. Let $Z \subset X$ be an irreducible subvariety. If the set of special points in $Z(\mathbb{C})$ is Zariski dense in $Z(\mathbb{C})$, then Z is a special subvariety.

Steps of the proof

The proof uses o-minimality in a similar manner as for the proof of the Manin-Mumford conjecture.

- Construct a covering $\pi : \mathfrak{Z} \mapsto Z(\mathbb{C})$, definable in an o-minimal structure, such that the preimage of special points are *nice*.
- Characterize the algebraic part of $\mathfrak{Z}$ with the help of a special locus.
- Count the rational points in the transcendental part of $\mathfrak{Z}$ by applying Pila-Wilkie, conclude that $Z(\mathbb{C})$ must have only finitely many special points outside of its special locus.
- Now the set of special points in the special locus is dense in Z, giving us that Z is a special subvariety.

o-minimal structures

Recall that the following structures are o-minimal:

- $\mathbb{R}$ as a pure ordered field,
- $\mathbb{R}_{\text{exp}}$ with a symbol for the *real* exponential map,
- $\mathbb{R}_{\text{an}}$ with a symbol for each analytic function *restricted to the interval* $[0, 1]$,
- $\mathbb{R}_{\text{an,exp}}$ with restricted analytic functions and full exponential.

Covering abelian varieties

This was done in the proof of Manin-Mumford. We recall the details:

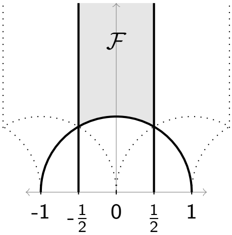
- Since $A(\mathbb{C})$ is a complex Lie group, it has an exponential map $\exp : \mathfrak{A} \mapsto A(\mathbb{C})$.
- $\ker(\exp)$ is a full lattice in $\mathfrak{A}$, so we can find an $\mathbb{R}$-basis of $\mathfrak{A}$ in $\ker(\exp)$.
- We see exp as going from $\mathbb{R}^{2g}$ – where $g = \dim(A(\mathbb{C}))$ – and restrict it to the fundamental domain $[0,1)^{2g}$.
- The restricted exp is definable in $\mathbb{R}_{\text{an}}$.
- Special points of A, i.e. torsion points, correspond exactly to rational points of $[0,1)^{2g}$.

We will use this covering for products of elliptic curves. For $\mathbb{C}^\times$, we use the much simpler map $z \to e^{2\pi i z}$, restricted to the band $0 \leqslant \Re(z) < 1$, definable in $\mathbb{R}_{\text{an,exp}}$.

As for modular curves, the covering $j_\Gamma : \mathbb{H} \mapsto Y$ is very nice. We need to restrict it to a fundamental domain. We will do it for $\mathbb{A}^1(\mathbb{C})$, but the same goes for any modular curve Y.

Covering modular curves

Consider $\mathcal{F} = \left\{ z \in \mathbb{C} \;\middle|\; -\frac{1}{2} \leqslant \Re(z) < \frac{1}{2} \;\&\; |z| \geqslant 1 \right\}$:



Recall that $j(\tau) = J(e^{2\pi i\tau})$ with $J(q) = \frac{1+744q+\cdots}{q}$.

- $\exp : \tau \to e^{2\pi i\tau} = e^{-2\pi\Im(\tau)}(\cos(2\pi\Re(\tau)) + i\sin(2\pi\Re(\tau)))$ is definable in $\mathbb{R}_{\text{an,exp}}$ when restricted to $\mathcal{F}$.
- $\left|e^{2\pi i\tau}\right| = e^{-2\pi\Im(\tau)} \leqslant e^{-\pi\sqrt{3}}$, thus $\exp(\mathcal{F})$ is included in the square $S = \left\{ z \in \mathbb{C} \;\middle|\; |\Re(z)| \leqslant e^{-\pi\sqrt{3}} \;\&\; |\Im(z)| \leqslant e^{-\pi\sqrt{3}} \right\}$.
- $J|_S$, seen as a function of $\mathbb{R}^2$, is definable in $\mathbb{R}_{\text{an}}$ as it is the quotient of a restricted analytic function by a polynomial.

In the end, $j|_{\mathcal{F}} = J|_S \circ \exp|_{\mathcal{F}}(2\pi i\tau)$ is definable in $\mathbb{R}_{\text{an,exp}}$.

Prespecial points

By definition, preimages by j_Γ of special points of a modular curve Y are exactly $\tau \in \mathbb{H}$ such that E_τ has CM.

Proposition

E_τ has CM, i.e it has a non-trivial endomorphism, iff $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

Now we cover $X = Y_1 \times \cdots \times Y_n \times E_1 \times \cdots \times E_m \times (\mathbb{C}^\times)^\ell$ with

$$\Pi = j_{\Gamma_1} \times \cdots \times j_{\Gamma_n} \times \exp : \mathbb{H}^n \times \mathbb{R}^{2(m+\ell)} \mapsto X(\mathbb{C}),$$

and we consider π, its restriction to a fundamental domain $\mathfrak{X}$. π is then definable in $\mathbb{R}_{\text{an,exp}}$ and the prespecial points are quadratic imaginaries – in $\mathbb{R}^2$ – for the $2n$ first coordinates and (some) rational points for the next $2(m+\ell)$.

The algebraic part

We will apply Pila-Wilkie counting theorem to $\mathfrak{Z} = \pi^{-1}(Z(\mathbb{C}))$. First, we need to determine its algebraic part.

We define the special Locus $\mathsf{SpL}(Z)$ to be the union of all positive dimensional weakly special subvarieties of Z, and we have the following:

Lemma (to be done next week)

$$\pi(\mathfrak{Z}^{\mathsf{alg}}) = \mathsf{SpL}(Z).$$

It now suffices to prove that $\mathfrak{Z}^{\mathsf{tr}}$ contains only finitely many prespecial points; then by assumption the set of special points in $\mathsf{SpL}(Z)$ is dense in Z and we conclude.

Note: the proof of this lemma already uses Pila-Wilkie.

The transcendental part

We obtain an upper bound on the number of prespecial points in the transcendental part by the mean of Pila-Wilkie:

$$\#\mathfrak{Z}^{\mathrm{tr}}(\mathbb{Q}, t) \leqslant Ct^{\epsilon}.$$

On the other hand, we obtain a lower bound as follow:

Lemma (to be done next week)

If X is defined over a number field k, then there is a constant $C = C(X, k)$ such that for any prespecial point $x \in \mathfrak{X}$, we have:

$$[k(\pi(x)) : k] \geqslant CH(x)^{\frac{1}{2}}$$

.

This means that a given prespecial point will give rise to many others. If some prespecial point had big enough height, these lower and upper bounds would become incompatible; thus there is a bound on the height of prespecial points in $\mathfrak{Z}^{\mathrm{tr}}$, so there must be only finitely many of them.

To be continued

If you have any question or remark, don't hesitate!

Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag, 1986.

Jonathan Pila, *O-minimality and the André-Oort conjecture for* $\mathbb{C}^n$, Ann. of Math. (2), 173(3) (2011), 1779–1840.

Thomas Scanlon, *O-minimality as an approach to the André-Oort conjecture*, in: *Around the Zilber-Pink conjecture*, Panoramas et Synthèses, no. 52 (2017), 111–165.