Logic meets number theory in o-minimality

The work of PETERZIL, PILA, STARCHENKO, and WILKIE

Logic Colloquium, Vienna 2014

Matthias Aschenbrenner
University of California, Los Angeles

Kobi Peterzil

Jonathan Pila

Sergei Starchenko

Alex Wilkie

The citation for the Karp Prize 2014 mentions ...

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

- J. PILA and A. J. WILKIE, The rational points of a definable set
  Duke Math. J. **133** (2006), 591–616.

- Y. PETERZIL and S. STARCHENKO, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one
  Selecta Math. (N.S.) **10** (2004), 525–550.
- ______, Definability of restricted theta functions and families of abelian varieties
  Duke Math. J. **162** (2013), 731–765.

...plus four more papers!

The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic:
PRESBURGER, SKOLEM, GÖDEL (1920s/30s);
DAVIS-PUTNAM-ROBINSON, MATIYASEVICH (1950–70).

The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic: PRESBURGER, SKOLEM, GÖDEL (1920s/30s); DAVIS-PUTNAM-ROBINSON, MATIYASEVICH (1950–70).

In number theory, questions about $\mathbb{Z}$ are often studied by relating them to the (more tractable) fields $\mathbb{R}$ (of real numbers) and $\mathbb{Q}_p$ (of p-adic numbers). These structures turned out to be well-behaved also from the point of view of mathematical logic:

Logic meets Number Theory

The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic: PRESBURGER, SKOLEM, GÖDEL (1920s/30s); DAVIS-PUTNAM-ROBINSON, MATIYASEVICH (1950–70).

In number theory, questions about $\mathbb{Z}$ are often studied by relating them to the (more tractable) fields $\mathbb{R}$ (of real numbers) and $\mathbb{Q}_p$ (of p-adic numbers). These structures turned out to be well-behaved also from the point of view of mathematical logic:

- TARSKI (1940s) for $\mathbb{R}$;

Logic meets Number Theory

The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic: PRESBURGER, SKOLEM, GÖDEL (1920s/30s); DAVIS-PUTNAM-ROBINSON, MATIYASEVICH (1950–70).

In number theory, questions about $\mathbb{Z}$ are often studied by relating them to the (more tractable) fields $\mathbb{R}$ (of real numbers) and $\mathbb{Q}_p$ (of p-adic numbers). These structures turned out to be well-behaved also from the point of view of mathematical logic:

- TARSKI (1940s) for $\mathbb{R}$;
- AX-KOCHEN, ERŠOV (1960s) & MACINTYRE (1976) for $\mathbb{Q}_p$.

Logic meets Number Theory

The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic: PRESBURGER, SKOLEM, GÖDEL (1920s/30s); DAVIS-PUTNAM-ROBINSON, MATIYASEVICH (1950–70).

In number theory, questions about $\mathbb{Z}$ are often studied by relating them to the (more tractable) fields $\mathbb{R}$ (of real numbers) and $\mathbb{Q}_p$ (of p-adic numbers). These structures turned out to be well-behaved also from the point of view of mathematical logic:

- TARSKI (1940s) for $\mathbb{R}$;
- AX-KOCHEN, ERŠOV (1960s) & MACINTYRE (1976) for $\mathbb{Q}_p$.

More recent applications of mathematical logic to problems of a number-theoretic flavor, initiated by HRUSHOVSKI, involved deep “pure” model-theoretic results (geometric stability theory) applied to fields enriched with extra operators.

Logic meets Number Theory

The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic: PRESBURGER, SKOLEM, GÖDEL (1920s/30s); DAVIS-PUTNAM-ROBINSON, MATIYASEVICH (1950–70).

In number theory, questions about $\mathbb{Z}$ are often studied by relating them to the (more tractable) fields $\mathbb{R}$ (of real numbers) and $\mathbb{Q}_p$ (of p-adic numbers). These structures turned out to be well-behaved also from the point of view of mathematical logic:

- TARSKI (1940s) for $\mathbb{R}$;
  - ↳ o-minimality;
- AX-KOCHEN, ERŠOV (1960s) & MACINTYRE (1976) for $\mathbb{Q}_p$.

More recent applications of mathematical logic to problems of a number-theoretic flavor, initiated by HRUSHOVSKI, involved deep “pure” model-theoretic results (geometric stability theory) applied to fields enriched with extra operators.

The citation for the Karp Prize 2014 mentions . . .

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

- J. PILA and A. J. WILKIE, The rational points of a definable set
  Duke Math. J. **133** (2006), 591–616.

- Y. PETERZIL and S. STARCHENKO, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one
  Selecta Math. (N.S.) **10** (2004), 525–550.

- ______, Definability of restricted theta functions and families of abelian varieties
  Duke Math. J. **162** (2013), 731–765.

. . . plus four more papers!

The citation for the Karp Prize 2014 mentions . . .

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

- J. PILA and A. J. WILKIE, The rational points of a definable set
  Duke Math. J. **133** (2006), 591–616.

- Y. PETERZIL and S. STARCHENKO, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one
  Selecta Math. (N.S.) **10** (2004), 525–550.

- ______, Definability of restricted theta functions and families of abelian varieties
  Duke Math. J. **162** (2013), 731–765.

. . . plus four more papers!

1. A *variety* $V \subseteq \mathbb{C}^n$ is the zero set of finitely many polynomials $P_1, \ldots, P_m \in \mathbb{C}[X_1, \ldots, X_n]$:

   $$V = \left\{ x \in \mathbb{C}^n : P_1(x) = \cdots = P_m(x) = 0 \right\}.$$

   Hypersurface = zero set of a single polynomial.
2. The varieties form the closed sets of a topology on $\mathbb{C}^n$, the ZARISKI *topology.* Below: dense = ZARISKI-dense.
3. A variety V is *irreducible* if it is not the union of two varieties properly contained in V.
4. Every variety V is the union of a finite number of irreducible varieties; this decomposition is unique if one removes those subsets that are contained in another one, and the elements of this unique decomposition are called *irreducible components* of V.

Diophantine Geometry studies how the *geometric* features of a variety $V \subseteq \mathbb{C}^n$ interact with its *diophantine* properties. For example, given an "interesting" set $K \subseteq \mathbb{C}$, how does the geometry of V influence the structure of $V(K) := K^n \cap V$?

Diophantine Geometry studies how the *geometric* features of a variety $V \subseteq \mathbb{C}^n$ interact with its *diophantine* properties. For example, given an "interesting" set $K \subseteq \mathbb{C}$, how does the geometry of V influence the structure of $V(K) := K^n \cap V$?

A general principle

If V is a *special* variety and $X \subseteq V$ is a variety which contains a dense set of *special* points, then X, too, has to be *special.* (Whatever "special" means.)

Diophantine Geometry studies how the *geometric* features of a variety $V \subseteq \mathbb{C}^n$ interact with its *diophantine* properties. For example, given an “interesting” set $K \subseteq \mathbb{C}$, how does the geometry of V influence the structure of $V(K) := K^n \cap V$?

A general principle

If V is a *special* variety and $X \subseteq V$ is a variety which contains a dense set of *special* points, then X, too, has to be *special.* (Whatever “special” means.)

A conjecture, due to ANDRÉ (1989) and OORT (1995), states that so-called SHIMURA varieties V obey such a principle.

Diophantine Geometry studies how the *geometric* features of a variety $V \subseteq \mathbb{C}^n$ interact with its *diophantine* properties. For example, given an "interesting" set $K \subseteq \mathbb{C}$, how does the geometry of V influence the structure of $V(K) := K^n \cap V$?

A general principle

If V is a *special* variety and $X \subseteq V$ is a variety which contains a dense set of *special* points, then X, too, has to be *special.* (Whatever "special" means.)

A conjecture, due to ANDRÉ (1989) and OORT (1995), states that so-called SHIMURA varieties V obey such a principle.

PILA-ZANNIER found a general procedure using o-minimality to prove instances of the "general principle." This allowed PILA to give the first unconditional proof (not relying, e.g., on the RIEMANN Hypothesis) of ANDRÉ-OORT for the case $V = \mathbb{C}^n$.

Here is an archetypical example of the "general principle." Put

$$\mathbb{U} := \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \geqslant 1\} \qquad \text{(roots of unity).}$$

The elements of $\mathbb{U}$ are our *special points.*

Here is an archetypical example of the "general principle." Put

$$\mathbb{U} := \left\{ z \in \mathbb{C} : z^n = 1 \text{ for some } n \geqslant 1 \right\} \qquad \text{(roots of unity).}$$

The elements of $\mathbb{U}$ are our *special points.*

Theorem (Laurent, 1984)

Let $X \subseteq (\mathbb{C}^\times)^n$ be irreducible. If $X(\mathbb{U})$ is dense in X, then X is defined by equations

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} = b \qquad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z},\ b \in \mathbb{U}).$$

Here is an archetypical example of the "general principle." Put

$$\mathbb{U} := \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \geqslant 1\} \qquad \text{(roots of unity).}$$

The elements of $\mathbb{U}$ are our *special points.*

Theorem (Laurent, 1984)

Let $X \subseteq (\mathbb{C}^\times)^n$ be irreducible. If $X(\mathbb{U})$ is dense in X, then X is defined by equations

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} = b \qquad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z},\ b \in \mathbb{U}).$$

This is an instance of the Manin-Mumford Conjecture (= Raynaud's Theorem). The Pila-Zannier method (extended by Peterzil-Starchenko) gives (yet) another proof.

The main idea

- We have an analytic surjection

$$e\colon \mathbb{C}^n \to (\mathbb{C}^\times)^n, \qquad e(z_1, \dots, z_n) = (e^{2\pi i z_1}, \dots, e^{2\pi i z_n}).$$

The main idea

- We have an analytic surjection

$$e\colon \mathbb{C}^n \to (\mathbb{C}^\times)^n, \qquad e(z_1,\dots,z_n) = (e^{2\pi i z_1},\dots,e^{2\pi i z_n}).$$

Note: $\zeta \in \mathbb{U}^n \iff \zeta = e(z)$ for some $z \in \mathbb{Q}^n$.

The main idea

- We have an analytic surjection

$$e\colon \mathbb{C}^n \to (\mathbb{C}^\times)^n, \qquad e(z_1, \dots, z_n) = (e^{2\pi i z_1}, \dots, e^{2\pi i z_n}).$$

  Note: $\quad \zeta \in \mathbb{U}^n \quad \Longleftrightarrow \quad \zeta = e(z)$ for some $z \in \mathbb{Q}^n$.
- e has a fundamental domain:

$$D := \{(z_1, \dots, z_n) \in \mathbb{C}^n : 0 \leqslant \mathrm{Re}(z_i) < 1 \text{ for each } i\}.$$

The main idea

- We have an analytic surjection

$$e\colon \mathbb{C}^n \to (\mathbb{C}^\times)^n, \qquad e(z_1,\ldots,z_n) = (e^{2\pi i z_1},\ldots,e^{2\pi i z_n}).$$

Note: $\zeta \in \mathbb{U}^n \iff \zeta = e(z)$ for some $z \in \mathbb{Q}^n$.

- e has a fundamental domain:

$$D := \{(z_1,\ldots,z_n) \in \mathbb{C}^n : 0 \leqslant \mathrm{Re}(z_i) < 1 \text{ for each } i\}.$$

Then with $\widetilde{e} := e \restriction D$, we still have

$$\zeta \in \mathbb{U}^n \iff \zeta = \widetilde{e}(z) \text{ for some } z \in D \cap \mathbb{Q}^n.$$

The method of PILA-ZANNIER

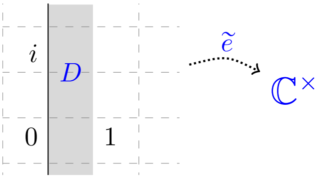
e is “logically” badly behaved (its kernel is $\mathbb{Z}^n$), but $\tilde{e}$ and thus

$$\tilde{X} := \tilde{e}^{-1}(X)$$

are definable in the o-minimal structure

$$\big(\mathbb{R}; <, 0, 1, +, \times, \exp, \sin\restriction[0, 2\pi]\big),$$

with $\tilde{X}(\mathbb{Q}) = \tilde{e}^{-1}\big(X(\mathbb{U})\big)$.



(Identify $\mathbb{C}$ with $\mathbb{R}^2$.)

$$e^{a+ib} = e^a(\cos b + i \sin b)$$

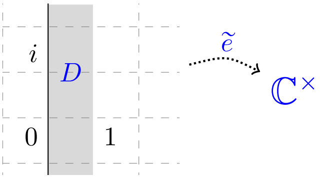
e is “logically” badly behaved (its kernel is $\mathbb{Z}^n$), but $\tilde{e}$ and thus

$$\tilde{X} := \tilde{e}^{-1}(X)$$

are definable in the o-minimal structure

$$\big(\mathbb{R}; <, 0, 1, +, \times, \exp, \sin \restriction [0, 2\pi]\big),$$

with $\tilde{X}(\mathbb{Q}) = \tilde{e}^{-1}\big(X(\mathbb{U})\big)$.



(Identify $\mathbb{C}$ with $\mathbb{R}^2$.)

$$e^{a+ib} = e^a(\cos b + i \sin b)$$

(Definability in an o-minimal structure is obvious in this case, but by far non-obvious in many other applications of the PILA-ZANNIER method → PETERZIL-STARCHENKO.)

The citation for the Karp Prize 2014 mentions . . .

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

- J. PILA and A. J. WILKIE, The rational points of a definable set
  Duke Math. J. **133** (2006), 591–616.

- Y. PETERZIL and S. STARCHENKO, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one
  Selecta Math. (N.S.) **10** (2004), 525–550.

- ______, Definability of restricted theta functions and families of abelian varieties
  Duke Math. J. **162** (2013), 731–765.

. . . plus four more papers!

Split $$\widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \ \dot\cup\ \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$$ (to be defined).

Split $$\widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \dot{\cup} \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$$ (to be defined).

Strategy

1. The upper bound: *Prove that* $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ *is "small."*

Split $\widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot\cup\, \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ is "small."*

2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ actually is finite.*

The method of PILA-ZANNIER

Split $\widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot{\cup}\, \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that* $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ *is "small."*
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that* $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ *actually is finite.*
3. Analyze $\widetilde{X}^{\mathrm{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that* A *is an affine subspace of* $\mathbb{C}^n$ *defined over* $\mathbb{Q}$.

The method of PILA-ZANNIER

Split $$\tilde{X} = \underbrace{\tilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot\cup\, \underbrace{\tilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$$ (to be defined).

Strategy

1. <u>The upper bound:</u> *Prove that $\tilde{X}^{\mathrm{trans}}(\mathbb{Q})$ is "small."*
   [Follows from definability of $\tilde{X}$ and a theorem of PILA-WILKIE.]
2. <u>The lower bound:</u> Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\tilde{X}^{\mathrm{trans}}(\mathbb{Q})$ actually is finite.*
3. <u>Analyze $\tilde{X}^{\mathrm{alg}}(\mathbb{Q})$:</u> Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathbb{C}^n$ defined over $\mathbb{Q}$.*

The method of PILA-ZANNIER

Split $$\widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot\cup\, \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$$ (to be defined).

Strategy

1. The upper bound: *Prove that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ is "small."*
   [Follows from definability of $\widetilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ actually is finite.*
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER's φ-function.]
3. Analyze $\widetilde{X}^{\mathrm{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathbb{C}^n$ defined over $\mathbb{Q}$.*

The method of PILA-ZANNIER

Split $\widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot{\cup}\, \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ is "small."*
   [Follows from definability of $\widetilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ actually is finite.*
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER's φ-function.]
3. Analyze $\widetilde{X}^{\mathrm{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathbb{C}^n$ defined over $\mathbb{Q}$.*
   [Uses AX' functional analogue of LINDEMANN-WEIERSTRASS.]

Split $\quad \widetilde{X} = \underbrace{\widetilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot\cup\, \underbrace{\widetilde{X}^{\mathrm{trans}}}_{\text{transcendental part}} \quad$ (to be defined).

Strategy

1. The upper bound: *Prove that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ is "small."*
   [Follows from definability of $\widetilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\widetilde{X}^{\mathrm{trans}}(\mathbb{Q})$ actually is finite.*
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER's φ-function.]
3. Analyze $\widetilde{X}^{\mathrm{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathbb{C}^n$ defined over $\mathbb{Q}$.*
   [Uses AX' functional analogue of LINDEMANN-WEIERSTRASS.]

O-minimal structures were introduced 30 years ago (van den Dries, Pillay-Steinhorn) in order to provide an analogue for the model-theoretic tameness notion of *strong minimality* in an ordered context (“o-minimal” = “order-minimal”).

O-minimal structures were introduced 30 years ago (VAN DEN DRIES, PILLAY-STEINHORN) in order to provide an analogue for the model-theoretic tameness notion of *strong minimality* in an ordered context ("o-minimal" = "order-minimal").

Let $\boldsymbol{R} = (\mathbb{R}; <, \dots)$ be an expansion of the ordered set of reals.

O-minimal structures were introduced 30 years ago (VAN DEN DRIES, PILLAY-STEINHORN) in order to provide an analogue for the model-theoretic tameness notion of *strong minimality* in an ordered context ("o-minimal" = "order-minimal").

Let $\boldsymbol{R} = (\mathbb{R}; <, \dots)$ be an expansion of the ordered set of reals.

(O-minimality can be developed if instead of $(\mathbb{R}; <)$ we take any linearly ordered set $(R; <)$ without endpoints, and it is indeed useful to have the extra flexibility.)

O-minimal structures were introduced 30 years ago (VAN DEN DRIES, PILLAY-STEINHORN) in order to provide an analogue for the model-theoretic tameness notion of *strong minimality* in an ordered context ("o-minimal" = "order-minimal").

Let $\boldsymbol{R} = (\mathbb{R}; <, \dots)$ be an expansion of the ordered set of reals.

(O-minimality can be developed if instead of $(\mathbb{R}; <)$ we take any linearly ordered set $(R; <)$ without endpoints, and it is indeed useful to have the extra flexibility.)

Below, "definable" means "definable in $\boldsymbol{R}$, possibly with parameters." A map $f: S \to R^n$, where $S \subseteq R^m$, is called definable if its graph $\Gamma(f) \subseteq R^{m+n}$ is.

Definition

$$\boldsymbol{R} \text{ is } \textbf{o-minimal} \quad :\Longleftrightarrow \left\{ \begin{array}{l} \text{all definable subsets of } \mathbb{R} \text{ are finite} \\ \text{unions of singletons and (open)} \\ \text{intervals} \end{array} \right.$$

$$\Longleftrightarrow \left\{ \begin{array}{l} \text{all definable subsets of } \mathbb{R} \text{ have} \\ \text{finitely many connected compo-} \\ \text{nents} \end{array} \right.$$

$$\Longleftrightarrow \left\{ \begin{array}{l} \text{the definable subsets of } \mathbb{R} \text{ are} \\ \text{those that are already definable in} \\ \text{the reduct } (\mathbb{R}; <) \text{ of } \boldsymbol{R} \end{array} \right.$$

Why do we care about o-minimality?

Although the o-minimality axiom only refers to definable subsets of $\mathbb{R}$, it implies finiteness properties for the definable subsets of $\mathbb{R}^n$ for arbitrary $n \geqslant 1$.

Why do we care about o-minimality?

Although the o-minimality axiom only refers to definable subsets of $\mathbb{R}$, it implies finiteness properties for the definable subsets of $\mathbb{R}^n$ for arbitrary $n \geqslant 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only *finitely many connected components*.

Why do we care about o-minimality?

Although the o-minimality axiom only refers to definable subsets of $\mathbb{R}$, it implies finiteness properties for the definable subsets of $\mathbb{R}^n$ for arbitrary $n \geqslant 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only *finitely many connected components*.
- Definable maps $S \to \mathbb{R}^n$ ($S \subseteq \mathbb{R}^m$) are very regular, e.g.,
    - *piecewise differentiable* up to some fixed finite order;

Why do we care about o-minimality?

Although the o-minimality axiom only refers to definable subsets of $\mathbb{R}$, it implies finiteness properties for the definable subsets of $\mathbb{R}^n$ for arbitrary $n \geqslant 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only *finitely many connected components*.
- Definable maps $S \to \mathbb{R}^n$ ($S \subseteq \mathbb{R}^m$) are very regular, e.g.,
  - *piecewise differentiable* up to some fixed finite order;
  - the *finite* fibers have uniformly bounded cardinality.

Why do we care about o-minimality?

Although the o-minimality axiom only refers to definable subsets of $\mathbb{R}$, it implies finiteness properties for the definable subsets of $\mathbb{R}^n$ for arbitrary $n \geqslant 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only *finitely many connected components*.
- Definable maps $S \to \mathbb{R}^n$ ($S \subseteq \mathbb{R}^m$) are very regular, e.g.,
  - *piecewise differentiable* up to some fixed finite order;
  - the *finite* fibers have uniformly bounded cardinality.
- *Dimension* of definable sets is very well-behaved, e.g., invariant under definable bijections: no space-filling curves.

As logicians we know that geometric and topological constructions of a finitary nature preserve definability.

As logicians we know that geometric and topological constructions of a finitary nature preserve definability.

Example

If $S \subseteq \mathbb{R}^n$ is definable, then so is its closure

$$\mathrm{cl}(S) = \big\{x \in \mathbb{R}^n : \forall \varepsilon > 0\, \exists y \in S : \,|x - y| < \varepsilon\big\}.$$

(Here we assume that $\boldsymbol{R}$ expands $(\mathbb{R}; <, 0, 1, +, \times)$.)

As logicians we know that geometric and topological constructions of a finitary nature preserve definability.

Example

If $S \subseteq \mathbb{R}^n$ is definable, then so is its closure

$$\mathrm{cl}(S) = \{x \in \mathbb{R}^n : \forall \varepsilon > 0\, \exists y \in S : |x - y| < \varepsilon\}.$$

(Here we assume that $\boldsymbol{R}$ expands $(\mathbb{R}; <, 0, 1, +, \times)$.)

Each o-minimal structure $\boldsymbol{R}$ gives rise to a self-contained universe for a kind of “tame topology” (no pathologies) as envisaged by GROTHENDIECK (1980s).

O-minimal structures: examples

$\mathbb{R}_{\text{alg}} = (\mathbb{R}; <, 0, 1, +, \times)$
TARSKI, 1940s

O-minimal structures: examples

$\mathbb{R}_{\text{an}} = \big(\mathbb{R}_{\text{alg}}, \{f\colon [-1,1]^n \to \mathbb{R}$ restricted analytic, $n \in \mathbb{N}^{\geqslant 1}\}\big)$

van den Dries, 1986

van den Dries-Denef, 1988

$\mathbb{R}_{\text{alg}} = (\mathbb{R}; <, 0, 1, +, \times)$

Tarski, 1940s

O-minimal structures: examples

$\mathbb{R}_{\mathrm{an}} = \big(\mathbb{R}_{\mathrm{alg}}, \{f\colon [-1,1]^n \to \mathbb{R}$ restricted analytic, $n \in \mathbb{N}^{\geqslant 1}\}\big)$

VAN DEN DRIES, 1986

VAN DEN DRIES-DENEF, 1988

$\mathbb{R}_{\mathrm{exp}} = (\mathbb{R}_{\mathrm{alg}}, \exp)$

WILKIE, 1991

$\mathbb{R}_{\mathrm{alg}} = (\mathbb{R}; <, 0, 1, +, \times)$

TARSKI, 1940s

O-minimal structures: examples

$\mathbb{R}_{\mathrm{an,exp}} = (\mathbb{R}_{\mathrm{an}}, \exp)$

VAN DEN DRIES-MILLER, 1992

MACINTYRE-MARKER-VAN DEN DRIES, 1994

$\mathbb{R}_{\mathrm{an}} = \big(\mathbb{R}_{\mathrm{alg}}, \{f\colon [-1,1]^n \to \mathbb{R}$ restricted analytic, $n \in \mathbb{N}^{\geqslant 1}\}\big)$

VAN DEN DRIES, 1986

VAN DEN DRIES-DENEF, 1988

$\mathbb{R}_{\mathrm{exp}} = (\mathbb{R}_{\mathrm{alg}}, \exp)$

WILKIE, 1991

$\mathbb{R}_{\mathrm{alg}} = (\mathbb{R}; <, 0, 1, +, \times)$

TARSKI, 1940s

O-minimal structures: examples

$\mathbb{R}_{\text{an,exp}} = (\mathbb{R}_{\text{an}}, \exp)$

van den Dries-Miller, 1992

Macintyre-Marker-van den Dries, 1994

$\mathbb{R}_{\text{an}} = \big(\mathbb{R}_{\text{alg}}, \{f \colon [-1,1]^n \to \mathbb{R}$ restricted analytic, $n \in \mathbb{N}^{\geqslant 1}\}\big)$

van den Dries, 1986

van den Dries-Denef, 1988

$\mathbb{R}_{\text{exp}} = (\mathbb{R}_{\text{alg}}, \exp)$

Wilkie, 1991

semialgebraic sets

$\mathbb{R}_{\text{alg}} = (\mathbb{R}; <, 0, 1, +, \times)$

Tarski, 1940s

The citation for the Karp Prize 2014 mentions ...

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

- J. PILA and A. J. WILKIE, The rational points of a definable set
  Duke Math. J. **133** (2006), 591–616.

- Y. PETERZIL and S. STARCHENKO, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one
  Selecta Math. (N.S.) **10** (2004), 525–550.

- ______, Definability of restricted theta functions and families of abelian varieties
  Duke Math. J. **162** (2013), 731–765.

...plus four more papers!

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\boldsymbol{R} = (\mathbb{R}; <, 0, 1, +, \times, \dots)$ of $\mathbb{R}_{\text{alg}}$.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\boldsymbol{R} = (\mathbb{R}; <, 0, 1, +, \times, \dots)$ of $\mathbb{R}_{\mathrm{alg}}$.

More than ten years ago, WILKIE realized that the geometry of definable sets influences the distribution of integer points (= points with integer coordinates) on 1-dimensional definable sets.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\boldsymbol{R} = (\mathbb{R}; <, 0, 1, +, \times, \dots)$ of $\mathbb{R}_{\mathrm{alg}}$.

More than ten years ago, WILKIE realized that the geometry of definable sets influences the distribution of integer points (= points with integer coordinates) on 1-dimensional definable sets.

Around the same time, and developing earlier ideas of BOMBIERI-PILA (1989), PILA studied rational points on curves and surfaces definable in $\mathbb{R}_{\mathrm{an}}$.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\boldsymbol{R} = (\mathbb{R}; <, 0, 1, +, \times, \dots)$ of $\mathbb{R}_{\mathrm{alg}}$.

More than ten years ago, WILKIE realized that the geometry of definable sets influences the distribution of integer points (= points with integer coordinates) on 1-dimensional definable sets.

Around the same time, and developing earlier ideas of BOMBIERI-PILA (1989), PILA studied rational points on curves and surfaces definable in $\mathbb{R}_{\mathrm{an}}$.

These developments culminated in the theorem of PILA-WILKIE (2006):

Definable sets which are sufficiently “transcendental” contain few rational points.

O-minimal structures: diophantine properties

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ define the **height** of $x = \frac{a}{b}$ by $H(x) := \max\{|a|, |b|\}$, and set $H(0) := 0$.

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ define the **height** of $x = \frac{a}{b}$ by $H(x) := \max\{|a|, |b|\}$, and set $H(0) := 0$.

We also define a height function $\mathbb{Q}^n \to \mathbb{N}$, still denoted by H:

$$H(x_1, \dots, x_n) := \max\left\{H(x_1), \dots, H(x_n)\right\}.$$

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ define the **height** of $x = \frac{a}{b}$ by $H(x) := \max\{|a|, |b|\}$, and set $H(0) := 0$.

We also define a height function $\mathbb{Q}^n \to \mathbb{N}$, still denoted by H:

$$H(x_1, \ldots, x_n) := \max\left\{H(x_1), \ldots, H(x_n)\right\}.$$

Given $X \subseteq \mathbb{R}^n$ and $t \in \mathbb{R}$, put

$$X(\mathbb{Q}, t) \ := \ \left\{x \in X \cap \mathbb{Q}^n : H(x) \leqslant t\right\} \quad \text{(a finite set).}$$

O-minimal structures: diophantine properties

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ define the **height** of $x = \frac{a}{b}$ by $H(x) := \max\{|a|, |b|\}$, and set $H(0) := 0$.

We also define a height function $\mathbb{Q}^n \to \mathbb{N}$, still denoted by H:

$$H(x_1, \ldots, x_n) := \max\left\{H(x_1), \ldots, H(x_n)\right\}.$$

Given $X \subseteq \mathbb{R}^n$ and $t \in \mathbb{R}$, put

$$X(\mathbb{Q}, t) \ := \ \left\{x \in X \cap \mathbb{Q}^n : H(x) \leqslant t\right\} \quad \text{(a finite set).}$$

We'd like to understand the asymptotic behavior of $|X(\mathbb{Q}, t)|$.

Example

$$\left\{\begin{array}{l} X = \Gamma(P) \text{ where } P\colon \mathbb{R}^{n-1} \to \mathbb{R} \\ \text{is a polynomial function with in-} \\ \text{teger coefficients of degree } d \end{array}\right\} \Rightarrow |X(\mathbb{Q}, t)| \sim C t^{2(n-1)/d}$$

O-minimal structures: diophantine properties

Example

$$\left\{ \begin{array}{l} X = \Gamma(P) \text{ where } P\colon \mathbb{R}^{n-1} \to \mathbb{R} \\ \text{is a polynomial function with in-} \\ \text{teger coefficients of degree } d \end{array} \right\} \Rightarrow |X(\mathbb{Q}, t)| \sim Ct^{2(n-1)/d}$$

Question

When does $|X(\mathbb{Q}, t)|$ grow sub-polynomially as $t \to \infty$?

O-minimal structures: diophantine properties

Example

$$\left\{\begin{array}{l} X = \Gamma(P) \text{ where } P\colon \mathbb{R}^{n-1} \to \mathbb{R} \\ \text{is a polynomial function with in-} \\ \text{teger coefficients of degree } d \end{array}\right\} \Rightarrow |X(\mathbb{Q},t)| \sim Ct^{2(n-1)/d}$$

Question

When does $|X(\mathbb{Q},t)|$ grow sub-polynomially as $t \to \infty$?

Given $X \subseteq \mathbb{R}^n$ we let

$$X^{\mathrm{alg}} := \left\{\begin{array}{l} \text{union of all infinite connected semial-} \\ \text{gebraic subsets of } X \end{array}\right\}$$ *algebraic part of X*

$$X^{\mathrm{trans}} := X \setminus X^{\mathrm{alg}}$$ *transcendental part of X.*

(A caveat: even if X is definable, then X^{alg} in general is not.)

Theorem (Pila-Wilkie, 2006)

Let $X \subseteq \mathbb{R}^n$ be definable. Then for each $\varepsilon > 0$ there is some $t_0 = t_0(\varepsilon)$ such that

$$|X^{\mathrm{trans}}(\mathbb{Q}, t)| \leqslant t^{\varepsilon} \qquad \text{for all } t \geqslant t_0.$$

O-minimal structures: diophantine properties

Theorem (Pila-Wilkie, 2006)

Let $X \subseteq \mathbb{R}^n$ be definable. Then for each $\varepsilon > 0$ there is some $t_0 = t_0(\varepsilon)$ such that

$$|X^{\mathrm{trans}}(\mathbb{Q}, t)| \leqslant t^{\varepsilon} \qquad \text{for all } t \geqslant t_0.$$

Remark

- The theorem continues to hold if given $d \geqslant 1$, we replace

$$\begin{aligned} \mathbb{Q} &\rightsquigarrow \text{set of algebraic numbers of degree} \leqslant d \\ H &\rightsquigarrow \text{a suitable height function on } \mathbb{Q}^{\mathrm{alg}}. \end{aligned}$$

(Pila, 2009)

Two crucial ingredients in the proof:

- a parametrization theorem for bounded definable sets by maps with *bounded* derivatives (generalizing YOMDIN and GROMOV);
- a result about covering the rational points of such parametrized sets by few algebraic hypersurfaces (no definability assumptions here).

O-minimal structures: diophantine properties

Theorem I (parametrization)

Let $X \subseteq (0,1)^n$ be definable, non-empty, and $p \in \mathbb{N}$. There is a finite set Φ of definable maps $\phi\colon (0,1)^{\dim X} \to (0,1)^n$ such that

- the union of the images of the $\phi \in \Phi$ equals X;
- each $\phi \in \Phi$ is C^p with $||\phi^{(\alpha)}|| \leqslant 1$ for $|\alpha| \leqslant p$.

O-minimal structures: diophantine properties

Theorem I (parametrization)

Let $X \subseteq (0,1)^n$ be definable, non-empty, and $p \in \mathbb{N}$. There is a finite set Φ of definable maps $\phi\colon (0,1)^{\dim X} \to (0,1)^n$ such that

- the union of the images of the $\phi \in \Phi$ equals X;
- each $\phi \in \Phi$ is C^p with $||\phi^{(\alpha)}|| \leqslant 1$ for $|\alpha| \leqslant p$.

Theorem II (covering by hypersurfaces)

Let $m < n$ and d be given. Then there are $p \in \mathbb{N}$ and $\varepsilon, C > 0$ with the following properties:

- if $\phi\colon (0,1)^m \to \mathbb{R}^n$ is C^p with image X such that $||\phi^{(\alpha)}|| \leqslant 1$ for $|\alpha| \leqslant p$, then for each t, $X(\mathbb{Q}, t)$ is contained in the union of Ct^{ε} hypersurfaces of degree d;
- $\varepsilon = \varepsilon(m,n,d) \to 0$ as $d \to \infty$.

Toy case of the PILA-WILKIE Theorem:

$X = \Gamma(f)$ where $f\colon (0,1) \to (0,1)$ is definable.

Toy case of the PILA-WILKIE Theorem:

$X = \Gamma(f)$ where $f\colon (0,1) \to (0,1)$ is definable.

Let $\varepsilon > 0$ be given. Choose d so that $\varepsilon(1,2,d) \leqslant \varepsilon$, and then choose C, p as in Theorem II. Let Φ be a parametrization of X as in Theorem I. Then $X(\mathbb{Q},t)$ is contained in the union of $C_1 t^{\varepsilon}$ hypersurfaces of degree d, where $C_1 := C \cdot |\Phi|$.

O-minimal structures: diophantine properties

Toy case of the PILA-WILKIE Theorem:

$X = \Gamma(f)$ where $f\colon (0,1) \to (0,1)$ is definable.

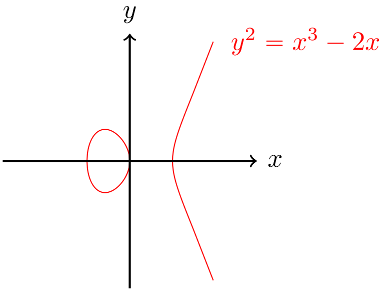
Let $\varepsilon > 0$ be given. Choose d so that $\varepsilon(1,2,d) \leqslant \varepsilon$, and then choose C, p as in Theorem II. Let Φ be a parametrization of X as in Theorem I. Then $X(\mathbb{Q},t)$ is contained in the union of $C_1 t^{\varepsilon}$ hypersurfaces of degree d, where $C_1 := C \cdot |\Phi|$.

The hypersurfaces H of degree d come in a definable (in fact, semialgebraic) family. So for each such H, either $X \cap H$ is infinite (and then $X \cap H \subseteq X^{\mathrm{alg}}$) or finite of uniformly bounded size (by o-minimality). This allows us to count $X^{\mathrm{trans}}(\mathbb{Q},t)$. $\square$

Elliptic curves: viewed algebraically

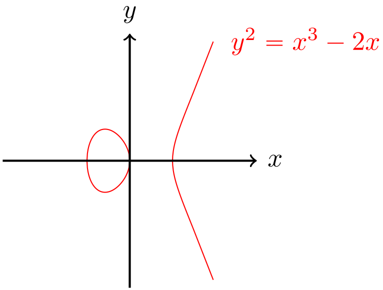
PILA's Theorem deals with *elliptic curves*:

$$y^2 = x^3 + ax + b \qquad \text{where } a, b \in \mathbb{C},\ 4a^3 \neq -27b^2.$$



PILA's Theorem deals with *elliptic curves*:

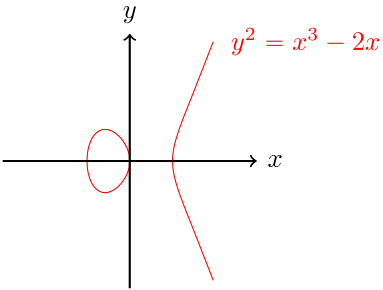
$$y^2 = x^3 + ax + b \qquad \text{where } a, b \in \mathbb{C},\ 4a^3 \neq -27b^2.$$



- plotted in $\mathbb{R}^2$ instead of $\mathbb{C}^2$;
- "elliptic" here has nothing to do with ellipses.

PILA's Theorem deals with *elliptic curves*:

$$y^2 = x^3 + ax + b \qquad \text{where } a, b \in \mathbb{C},\ 4a^3 \neq -27b^2.$$



- plotted in $\mathbb{R}^2$ instead of $\mathbb{C}^2$;
- "elliptic" here has nothing to do with ellipses.

It is natural to add a "point 0 at infinity":

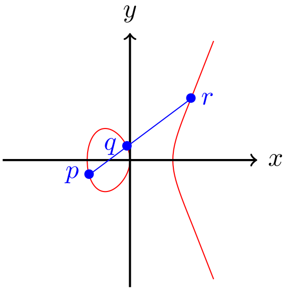
$$E = \left\{(x, y) \in \mathbb{C}^2 : y^2 = x^3 + ax + b\right\} \cup \{0\}$$

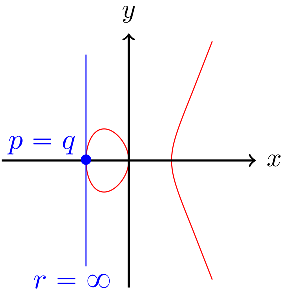
Elliptic curves: viewed algebraically

Let E be an elliptic curve. Then E can be made into an abelian group with 0 as its identity element.

Let E be an elliptic curve. Then E can be made into an abelian group with 0 as its identity element. For $p, q, r \in E$,

$$p + q + r = 0 \qquad \Longleftrightarrow \qquad p,\ q,\ r \text{ lie on a line.}$$

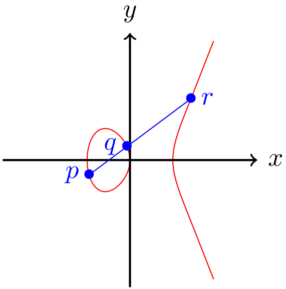


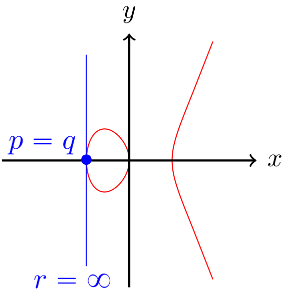


Elliptic curves: viewed algebraically

Let E be an elliptic curve. Then E can be made into an abelian group with 0 as its identity element. For $p, q, r \in E$,

$$p + q + r = 0 \qquad \Longleftrightarrow \qquad p,\ q,\ r \text{ lie on a line.}$$





This makes E into an *algebraic* group (the group operations are given by rational functions of the coordinates).

Elliptic curves: viewed analytically

Let E be an elliptic curve.

Elliptic curves: viewed analytically

Let E be an elliptic curve. Then there is a complex analytic surjective group morphism $\pi\colon \mathbb{C} \to E$ whose kernel is a lattice, which (after a change of coordinates) we may express as

$$\Lambda = \mathbb{Z} + \mathbb{Z}\tau \quad \text{where } \tau \in \mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}.$$

Elliptic curves: viewed analytically

Let E be an elliptic curve. Then there is a complex analytic surjective group morphism $\pi\colon \mathbb{C} \to E$ whose kernel is a lattice, which (after a change of coordinates) we may express as

$$\Lambda = \mathbb{Z} + \mathbb{Z}\tau \quad \text{where } \tau \in \mathbb{H} := \left\{z \in \mathbb{C} : \operatorname{Im} z > 0\right\}.$$

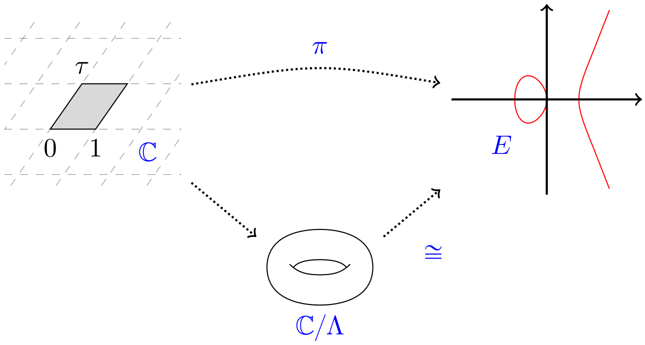
Conversely, for every $\tau \in \mathbb{H}$ there is an elliptic curve $E = E_\tau$ and an analytic group morphism $\mathbb{C} \twoheadrightarrow E$ with kernel $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$.

Elliptic curves: viewed analytically

Let E be an elliptic curve. Then there is a complex analytic surjective group morphism $\pi\colon \mathbb{C} \to E$ whose kernel is a lattice, which (after a change of coordinates) we may express as

$$\Lambda = \mathbb{Z} + \mathbb{Z}\tau \quad \text{where } \tau \in \mathbb{H} := \left\{ z \in \mathbb{C} : \operatorname{Im} z > 0 \right\}.$$

Conversely, for every $\tau \in \mathbb{H}$ there is an elliptic curve $E = E_\tau$ and an analytic group morphism $\mathbb{C} \twoheadrightarrow E$ with kernel $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$.



Thus $\mathbb{H}$ is a parameter space for elliptic curves.

Thus $\mathbb{H}$ is a parameter space for elliptic curves. But the map

$$\tau \mapsto \text{(isomorphism class of } E_\tau\text{)}$$

is not one-to-one:

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

acts on $\mathbb{H}$ via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau = \frac{a\tau+b}{c\tau+d}$, and for $\sigma, \tau \in \mathbb{H}$:

$$E_\sigma \cong E_\tau \quad \Longleftrightarrow \quad \sigma = A\tau \text{ for some } A \in \mathrm{SL}(2,\mathbb{Z}).$$

Thus $\mathbb{H}$ is a parameter space for elliptic curves. But the map

$$\tau \mapsto \text{(isomorphism class of } E_\tau\text{)}$$

is not one-to-one:

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

acts on $\mathbb{H}$ via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau = \frac{a\tau+b}{c\tau+d}$, and for $\sigma, \tau \in \mathbb{H}$:

$$E_\sigma \cong E_\tau \quad \Longleftrightarrow \quad \sigma = A\tau \text{ for some } A \in \mathrm{SL}(2,\mathbb{Z}).$$

The j-invariant (19th century: Klein ...)

There exists a holomorphic surjection $j\colon \mathbb{H} \to \mathbb{C}$ such that

$$j(\sigma) = j(\tau) \quad \Longleftrightarrow \quad E_\sigma \cong E_\tau.$$

Elliptic curves: viewed analytically

Thus $\mathbb{H}$ is a parameter space for elliptic curves. But the map

$$\tau \mapsto (\text{isomorphism class of } E_\tau)$$

is not one-to-one:

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

acts on $\mathbb{H}$ via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau = \frac{a\tau+b}{c\tau+d}$, and for $\sigma, \tau \in \mathbb{H}$:

$$E_\sigma \cong E_\tau \quad \Longleftrightarrow \quad \sigma = A\tau \text{ for some } A \in \mathrm{SL}(2,\mathbb{Z}).$$

The j-invariant (19th century: KLEIN . . .)

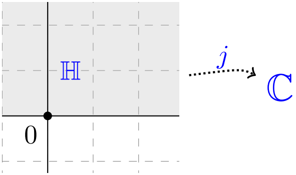
There exists a holomorphic surjection $j \colon \mathbb{H} \to \mathbb{C}$ such that

$$j(\sigma) = j(\tau) \quad \Longleftrightarrow \quad E_\sigma \cong E_\tau.$$

(So the “correct” parameter space is $\mathbb{C} \cong \mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$.)

PILA's Theorem

This is an analogue of LAURENT's Theorem with

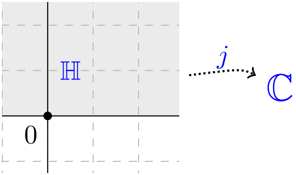


$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots$$
$$(q = e^{2\pi i\tau})$$

instead of $z \mapsto e^{2\pi i z} \colon \mathbb{C} \to \mathbb{C}^\times$.

PILA's Theorem

This is an analogue of LAURENT's Theorem with



$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots$$
$$(q = e^{2\pi i\tau})$$

instead of $z \mapsto e^{2\pi i z} : \mathbb{C} \to \mathbb{C}^\times$.

Theorem (PILA, 2011)

Let $X \subseteq \mathbb{C}^n$ be an irreducible variety. If X contains a dense set of special points, then X is special.

Of course, we need to define what "special" should mean.

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

$$\mathrm{End}(E) \cong \left\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\right\}.$$

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

$$\mathrm{End}(E) \cong \left\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\right\}.$$

Usually $\mathrm{End}(E) = \mathbb{Z}$. But it may be bigger:

$\mathrm{End}(E) \neq \mathbb{Z} \quad \Longleftrightarrow \quad \tau$ satisfies a quadratic equation over $\mathbb{Q}$.

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

$$\mathrm{End}(E) \cong \left\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\right\}.$$

Usually $\mathrm{End}(E) = \mathbb{Z}$. But it may be bigger:

$$\mathrm{End}(E) \neq \mathbb{Z} \quad \Longleftrightarrow \quad \tau \text{ satisfies a quadratic equation over } \mathbb{Q}.$$

The $j(\tau) \in \mathbb{C}$ with $\tau \in \mathbb{H}$ quadratic over $\mathbb{Q}$ ("E has CM") will be our *special points.* KRONECKER: special $\Rightarrow$ algebraic integer.

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

$$\mathrm{End}(E) \cong \left\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\right\}.$$

Usually $\mathrm{End}(E) = \mathbb{Z}$. But it may be bigger:

$\mathrm{End}(E) \neq \mathbb{Z} \quad \Longleftrightarrow \quad \tau$ satisfies a quadratic equation over $\mathbb{Q}$.

The $j(\tau) \in \mathbb{C}$ with $\tau \in \mathbb{H}$ quadratic over $\mathbb{Q}$ ("E has CM") will be our *special points.* KRONECKER: special $\Rightarrow$ algebraic integer.

Why are these points special?

One possible explanation from algebraic number theory:

- A finite field extension K of $\mathbb{Q}$ has abelian GALOIS group $\Longleftrightarrow K \subseteq \mathbb{Q}(\zeta)$ for some $\zeta \in \mathbb{U}$. (KRONECKER-WEBER)
- If E_τ has CM, all abelian extensions of $\mathbb{Q}(\tau)$ can similarly be constructed from $\mathbb{U}$, $j(\tau)$, and torsion points of E_τ.

What should be the *special* varieties $V \subseteq \mathbb{C}^n$?

What should be the *special* varieties $V \subseteq \mathbb{C}^n$?

While e is a group morphism, j is not. ($\mathbb{H}$ is not even a group!) Still, there are algebraic relations between $j(\tau)$ and $j(n\tau)$:

The nth classical modular polynomial ($n \in \mathbb{N}^{\geqslant 1}$)

There is an irreducible $\Phi_n \in \mathbb{Z}[X, Y]$ such that for $x, y \in \mathbb{C}$:

$$\Phi_n(x, y) = 0 \quad \iff \quad x = j(\tau),\ y = j(n\tau) \text{ for some } \tau \in \mathbb{H}.$$

The Φ_n are symmetric in X and Y.

What should be the *special* varieties $V \subseteq \mathbb{C}^n$?

While e is a group morphism, j is not. ($\mathbb{H}$ is not even a group!) Still, there are algebraic relations between $j(\tau)$ and $j(n\tau)$:

The nth classical modular polynomial ($n \in \mathbb{N}^{\geqslant 1}$)

There is an irreducible $\Phi_n \in \mathbb{Z}[X, Y]$ such that for $x, y \in \mathbb{C}$:

$$\Phi_n(x, y) = 0 \iff x = j(\tau),\ y = j(n\tau) \text{ for some } \tau \in \mathbb{H}.$$

The Φ_n are symmetric in X and Y.

For example,

$$\begin{aligned}\Phi_2 = X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + \\ 40773375XY + 8748000000X + Y^3 - 162000Y^2 + \\ 8748000000Y - 157464000000000\end{aligned}$$

If $\tau \in \mathbb{H}$ is quadratic, then so is $n\tau \in \mathbb{H}$, so $\{\Phi_n = 0\}$ contains a dense set of special points.

If $\tau \in \mathbb{H}$ is quadratic, then so is $n\tau \in \mathbb{H}$, so $\{\Phi_n = 0\}$ contains a dense set of special points.

Definition

A variety $V \subseteq \mathbb{C}^n$ is *special* if it is an irreducible component of a variety defined by equations

$$\Phi_n(x_i, x_j) = 0 \quad \text{and} \quad x_i = a \text{ where } a \in \mathbb{C} \text{ is special.}$$

If $\tau \in \mathbb{H}$ is quadratic, then so is $n\tau \in \mathbb{H}$, so $\{\Phi_n = 0\}$ contains a dense set of special points.

Definition

A variety $V \subseteq \mathbb{C}^n$ is *special* if it is an irreducible component of a variety defined by equations

$$\Phi_n(x_i, x_j) = 0 \quad \text{and} \quad x_i = a \text{ where } a \in \mathbb{C} \text{ is special.}$$

The proof of PILA's Theorem follows the earlier pattern:

If $\tau \in \mathbb{H}$ is quadratic, then so is $n\tau \in \mathbb{H}$, so $\{\Phi_n = 0\}$ contains a dense set of special points.

Definition

A variety $V \subseteq \mathbb{C}^n$ is *special* if it is an irreducible component of a variety defined by equations

$$\Phi_n(x_i, x_j) = 0 \quad \text{and} \quad x_i = a \text{ where } a \in \mathbb{C} \text{ is special.}$$

The proof of PILA's Theorem follows the earlier pattern:

1. The upper bound: j has a natural (semialgebraic) fundamental domain D, and $j \restriction D$ is definable in $\mathbb{R}_{\mathrm{an,exp}}$.

PILA's Theorem

If $\tau \in \mathbb{H}$ is quadratic, then so is $n\tau \in \mathbb{H}$, so $\{\Phi_n = 0\}$ contains a dense set of special points.

Definition

A variety $V \subseteq \mathbb{C}^n$ is *special* if it is an irreducible component of a variety defined by equations

$$\Phi_n(x_i, x_j) = 0 \quad \text{and} \quad x_i = a \text{ where } a \in \mathbb{C} \text{ is special.}$$

The proof of PILA's Theorem follows the earlier pattern:

1. The upper bound: j has a natural (semialgebraic) fundamental domain D, and $j \upharpoonright D$ is definable in $\mathbb{R}_{\mathrm{an,exp}}$.
2. The lower bound: C. L. SIEGEL's theorem (1935) on the growth of the class number of quadratic number fields.

If $\tau \in \mathbb{H}$ is quadratic, then so is $n\tau \in \mathbb{H}$, so $\{\Phi_n = 0\}$ contains a dense set of special points.

Definition

A variety $V \subseteq \mathbb{C}^n$ is *special* if it is an irreducible component of a variety defined by equations

$$\Phi_n(x_i, x_j) = 0 \quad \text{and} \quad x_i = a \text{ where } a \in \mathbb{C} \text{ is special.}$$

The proof of Pila's Theorem follows the earlier pattern:

1. The upper bound: j has a natural (semialgebraic) fundamental domain D, and $j \restriction D$ is definable in $\mathbb{R}_{\text{an,exp}}$.
2. The lower bound: C. L. Siegel's theorem (1935) on the growth of the class number of quadratic number fields.
3. Analysis of the algebraic part: A Lindemann-Weierstrass Theorem for j.

Further developments

Many recent results employ and further develop ingredients from this circle of ideas:

- in number theory: ULLMOV-YAFAEV, KLINGER-ULLMO-YAFAEV, PILA-TSIMERMAN, MASSER-ZANNIER, HABEGGER-PILA ...
- in logic: PETERZIL-STARCHENKO, FREITAG-SCANLON, BIANCONI, THOMAS, JONES-THOMAS, JONES-THOMAS-WILKIE, BAYS-KIRBY-WILKIE, CLUCKERS-COMTE-LOESER, ...

> *"It is now widely accepted that a new method has emerged in this subject."*

If you want to know more

SCANLON's excellent surveys:

- *O-minimality as an approach to the André-Oort conjecture*, Panor. Synth., to appear.
- *Counting special points: logic, Diophantine geometry, and transcendence theory,* Bull. Amer. Math. Soc. **49** (2012), 51–71.
- *A proof of the André-Oort conjecture via mathematical logic* [*after Pila, Wilkie and Zannier*], Séminaire Bourbaki: Vol. 2010/2011, Astérisque **348** (2012), 299–315.