Logic meets number theory in o-minimality
The work of Peterzil, Pilas, Starchenko, and Wilkie

Logic Colloquium, Vienna 2014

Matthias Aschenbrenner
University of California, Los Angeles

UCLA
The citation for the Karp Prize 2014 mentions . . .


...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:
The history of interactions between these two subjects dates back almost to the beginnings of mathematical logic: PÉRESBURGER, 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 \( \mathbb{R} \);
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
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.
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 $\mathbb{R}$; $\rightarrow$ 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 $\mathbb{C}^n$.


- Y. Peterzil and S. Starchenko, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one.

- ______, Definability of restricted theta functions and families of abelian varieties.

...plus four more papers!
The citation for the Karp Prize 2014 mentions . . .

- J. Pila, O-minimality and the André-Oort conjecture for $\mathbb{C}^n$

- J. Pila and A. J. Wilkie, The rational points of a definable set

- Y. Peterzil and S. Starchenko, Uniform definability of the
  Weierstrass $wp$-functions and generalized tori of dimension one

- ______, Definability of restricted theta functions and families of
  abelian varieties

. . . plus four more papers!
A variety \( V \subseteq \mathbb{C}^n \) is the zero set of finitely many polynomials \( P_1, \ldots, P_m \in \mathbb{C}[X_1, \ldots, X_n] \):

\[
V = \{ x \in \mathbb{C}^n : P_1(x) = \cdots = P_m(x) = 0 \}.
\]

Hypersurface = zero set of a single polynomial.

The varieties form the closed sets of a topology on \( \mathbb{C}^n \), the ZARISKI topology. Below: dense = ZARISKI-dense.

A variety \( V \) is irreducible if it is not the union of two varieties properly contained in \( V \).

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

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

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

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

The elements of $U$ are our *special points*. 

**Theorem (Lang, 1984)** Let $X \subseteq \mathbb{C}^n \setminus \mathbb{Q}$ be irreducible. If $X \cap U$ is dense in $X$, then $X$ is defined by equations

$$X_{\alpha_1} \cdots X_{\alpha_n} = b_1, \ldots, b_n \in U \subset \mathbb{Q}.$$

This is an instance of the MANIN-MUMFORD Conjecture (= Raynaud’s Theorem). The PILA-ZANNIER method (extended by Peterzil-Starchenko) gives (yet) another proof.
Here is an archetypical example of the “general principle.” Put

\[ \mathbb{U} := \left\{ z \in \mathbb{C} : z^n = 1 \text{ for some } n \geq 1 \right\} \] (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

\[ X_1^{\alpha_1} \cdots X_n^{\alpha_n} = b \quad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z}, \ b \in \mathbb{U}). \]
Here is an archetypical example of the “general principle.” Put

$$\mathbb{U} := \{ z \in \mathbb{C} : z^n = 1 \text{ for some } n \geq 1 \}$$

(roots of unity).

The elements of \( \mathbb{U} \) are our \textit{special points}.

\begin{itemize}
  \item \textbf{Theorem (LAURENT, 1984)}
  \item \textit{Let} \( X \subseteq (\mathbb{C}^*)^n \) \textit{be irreducible. If} \( X(\mathbb{U}) \) \textit{is dense in} \( X \), \textit{then} \( X \) \textit{is defined by equations}

  \[ X_1^{\alpha_1} \cdots X_n^{\alpha_n} = b \quad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z}, \ b \in \mathbb{U}). \]
\end{itemize}

This is an instance of the \textbf{MANIN-MUMFORD Conjecture} (= \textbf{RAYNAUD’s Theorem}). The \textbf{PILA-ZANNIER} method (extended by \textbf{PETERZIL-STARCHENKO}) gives (yet) another proof.
The method of PILA-ZANNIER

The main idea

- We have an analytic surjection

\[ e : \mathbb{C}^n \to (\mathbb{C}^\times)^n, \quad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}). \]
The main idea

- We have an analytic surjection

\[ e : \mathbb{C}^n \to (\mathbb{C}^\times)^n, \quad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}). \]

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

- We have an analytic surjection

\[ e : \mathbb{C}^n \to (\mathbb{C}^\times)^n, \quad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}). \]

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

- \( e \) has a fundamental domain:

\[ D := \{(z_1, \ldots, z_n) \in \mathbb{C}^n : 0 \leq \text{Re}(z_i) < 1 \text{ for each } i\}. \]
The main idea

- We have an analytic surjection

\[ e: \mathbb{C}^n \to (\mathbb{C}^\times)^n, \quad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}). \]

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

- \( e \) has a fundamental domain:

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

Then with \( \bar{e} := e \upharpoonright D \), we still have

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

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

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

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

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

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

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

(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 $\mathbb{C}^n$  

- J. PILA and A. J. WILKIE, The rational points of a definable set  

- Y. PETERZIL and S. STARCHENKO, Uniform definability of the Weierstrass $\wp$-functions and generalized tori of dimension one  

- , Definability of restricted theta functions and families of abelian varieties  

. . . plus four more papers!
The method of PILA-ZANNIER

Split

\[ \widetilde{X} = \widetilde{X}^{\text{alg}} \cup \widetilde{X}^{\text{trans}} \]

(algebraic part \quad transcendental part)

(to be defined).
The method of Pilà-Zannier

Split

\[ \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \]

(to be defined).

Strategy

1. The upper bound: \textit{Prove that } \tilde{X}^{\text{trans}}(\mathbb{Q}) \textit{ is "small."}
The method of PILA-ZANNIER

Split

\[ \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \]

\begin{itemize}
  \item \textbf{The upper bound:} Prove that \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) is “small.”
  \item \textbf{The lower bound:} Suppose that \( X \) contains a dense set of special points (here: that \( X(\mathbb{U}) \) is dense in \( X \)). \textit{Show that this implies that} \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) \textit{actually is finite.}
\end{itemize}
The method of PilA-Zannier

Split
\[ \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \]
(algebraic part \hspace{1cm} transcendental part
(to be defined).

Strategy

1. **The upper bound:** Prove that \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) 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 \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) actually is finite.

3. **Analyze \( \tilde{X}^{\text{alg}}(\mathbb{Q}) \):** 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 \( \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \) (to be defined).

Strategy

1. The upper bound: *Prove that \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) is “small.”*  
   [Follows from definability of \( \tilde{X} \) 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 \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) actually is finite.*

3. Analyze \( \tilde{X}^{\text{alg}}(\mathbb{Q}) \): 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 \( \mathbb{Q} \).*
Split

\[ \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \]

(to be defined).

Strategy

1. **The upper bound**: Prove that \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) is “small.”
   [Follows from definability of \( \tilde{X} \) 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 \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) actually is finite.
   [Involves an automorphism argument and some number theory; here, only simple properties of Euler’s \( \varphi \)-function.]

3. **Analyze \( \tilde{X}^{\text{alg}}(\mathbb{Q}) \)**: 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 \( \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \) (to be defined).

Strategy

1. **The upper bound**: Prove that \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) is “small.”
   [Follows from definability of \( \tilde{X} \) 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 \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) actually is finite.
   [Involves an automorphism argument and some number theory; here, only simple properties of Euler’s \( \varphi \)-function.]

3. **Analyze \( \tilde{X}^{\text{alg}}(\mathbb{Q}) \)**: 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.]
The method of PILA-ZANNIER

Split

\[ \tilde{X} = \tilde{X}^{\text{alg}} \cup \tilde{X}^{\text{trans}} \]

(algebraic part  transcendental part) (to be defined).

Strategy

1. **The upper bound:** Prove that \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) is “small.”
   [Follows from definability of \( \tilde{X} \) 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 \( \tilde{X}^{\text{trans}}(\mathbb{Q}) \) actually is finite.
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER’s \( \varphi \)-function.]

3. **Analyze** \( \tilde{X}^{\text{alg}}(\mathbb{Q}) \): 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 $\mathbb{R} = (\mathbb{R}; <, \ldots)$ 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 $R = (\mathbb{R}; <, \ldots)$ 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 $\mathbb{R} = (\mathbb{R}; <, \ldots)$ 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 $\mathbb{R}$, possibly with parameters.” A map $f : S \to \mathbb{R}^n$, where $S \subseteq \mathbb{R}^m$, is called definable if its graph $\Gamma(f) \subseteq \mathbb{R}^{m+n}$ is.
Definition

\( R \) is **o-minimal** : \( \iff \) all definable subsets of \( \mathbb{R} \) are finite unions of singletons and (open) intervals

\( \iff \) all definable subsets of \( \mathbb{R} \) have finitely many connected components

\( \iff \) the definable subsets of \( \mathbb{R} \) are those that are already definable in the reduct \( (\mathbb{R};<) \) of \( R \)
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 $n \geq 1$. 

- Cell Decomposition Theorem: 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.
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 $n \geq 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only \textit{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 $n \geq 1$.

Some points in case

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

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 $n \geq 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only \textit{finitely many connected components}.
- Definable maps $S \to \mathbb{R}^n$ ($S \subseteq \mathbb{R}^m$) are very regular, e.g.,
  - \textit{piecewise differentiable} up to some fixed finite order;
  - the \textit{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 $n \geq 1$.

Some points in case

- Cell Decomposition Theorem $\Rightarrow$ definable subsets of $\mathbb{R}^n$ have only finitely many connected components.
- Definable maps $S \rightarrow \mathbb{R}^n$ ($S \subseteq \mathbb{R}^m$) 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

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

(Here we assume that $R$ 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

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

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

Each o-minimal structure $R$ gives rise to a self-contained universe for a kind of “tame topology” (no pathologies) as envisaged by Grothendieck (1980s).
\[ \mathbb{R}_{\text{alg}} = (\mathbb{R}; <, 0, 1, +, \times) \]

Tarski, 1940s
$\mathbb{R}_{an} = (\mathbb{R}_{alg}, \{f: [-1,1]^n \to \mathbb{R} \text{ restricted analytic, } n \in \mathbb{N}\geq1\})$

VAN DEN DRIES, 1986
VAN DEN DRIES-DENEF, 1988

$\mathbb{R}_{alg} = (\mathbb{R}; <, 0, 1, +, \times)$
TARKSI, 1940s
O-minimal structures: examples

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

\text{VAN DEN DRIES, 1986}

\text{VAN DEN DRIES-DENEF, 1988}

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

\text{WILKIE, 1991}

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

\text{TARKSI, 1940s}
O-minimal structures: examples

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

\text{VAN DEN DRIES-MILLER, 1992}

\text{MACINTYRE-MARKER-VAN DEN DRIES, 1994}

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

\text{VAN DEN DRIES, 1986}

\text{VAN DEN DRIES-DENEF, 1988}

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

\text{WILKIE, 1991}

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

\text{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**

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

**Van den Dries, 1986**
**Van den Dries-Denef, 1988**

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

**Wilkie, 1991**

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

**Tarski, 1940s**

**Semialgebraic sets**
The citation for the Karp Prize 2014 mentions . . .

- J. Pila, O-minimality and the André-Oort conjecture for $\mathbb{C}^n$

- J. Pila and A. J. Wilkie, The rational points of a definable set

- Y. Peterzil and S. Starchenko, Uniform definability of the
  Weierstrass $\wp$-functions and generalized tori of dimension one

- , Definability of restricted theta functions and families of
  abelian varieties

. . . plus four more papers!
Fix an o-minimal expansion $\mathbf{R} = (\mathbb{R}; <, 0, 1, +, \times, \ldots )$ of $\mathbb{R}_{\text{alg}}$. 
Fix an o-minimal expansion $\mathcal{R} = (\mathbb{R}; <, 0, 1, +, \times, \ldots)$ of $\mathbb{R}_{\text{alg}}$.

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

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

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 $\mathbb{R}_{\text{an}}$.

These developments culminated in the theorem of Pila-Wilkie (2006):

*Definable sets which are sufficiently “transcendental” contain few rational points.*
Given non-zero coprime \( a, b \in \mathbb{Z} \) define the **height** of \( x = \frac{a}{b} \) by

\[
H(x) := \max\{|a|, |b|\}, \quad \text{and set} \quad H(0) := 0.
\]
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 $H$:

$$H(x_1, \ldots, x_n) := \max \{H(x_1), \ldots, H(x_n)\}.$$
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 \(H\):
\[
H(x_1, \ldots, x_n) := \max \{H(x_1), \ldots, H(x_n)\}.
\]

Given \(X \subseteq \mathbb{R}^n\) and \(t \in \mathbb{R}\), put
\[
X(\mathbb{Q}, t) := \{x \in X \cap \mathbb{Q}^n : H(x) \leq t\} \quad \text{(a finite set)}.
\]
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 $H$:

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

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

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

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


Example

\[
\begin{aligned}
X &= \Gamma(P) \text{ where } P : \mathbb{R}^{n-1} \to \mathbb{R} \\
\text{is a polynomial function with integer coefficients of degree } d
\end{aligned}
\]

\[
\Rightarrow |X(\mathbb{Q}, t)| \sim C t^{2(n-1)/d}
\]
O-minimal structures: diophantine properties

Example

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

Question

When does \(|X(\mathbb{Q}, t)|\) grow sub-polynomially as \(t \to \infty\)?
O-minimal structures: diophantine properties

Example

\[
\begin{aligned}
&X = \Gamma(P) \text{ where } P : \mathbb{R}^{n-1} \to \mathbb{R} \\
is \text{ a polynomial function with integer coefficients of degree } d
\end{aligned}
\] 
\[
\implies |X(\mathbb{Q}, t)| \sim Ct^{2(n-1)/d}
\]

Question

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

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

\[
X^{\text{alg}} := \left\{ \text{union of all infinite connected semialgebraic subsets of } X \right\}
\]

\[
X^{\text{trans}} := X \setminus X^{\text{alg}}
\]

(A caveat: even if \(X\) is definable, then \(X^{\text{alg}}\) 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

$$|X^{\text{trans}}(\mathbb{Q}, t)| \leq t^\varepsilon \quad \text{for all } t \geq t_0.$$
Theorem (PILÁ-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

$$|X^{\text{trans}}(\mathbb{Q}, t)| \leq t^\varepsilon \quad \text{for all } t \geq t_0.$$

Remark

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

  $\mathbb{Q} \rightsquigarrow$ set of algebraic numbers of degree $\leq d$

  $H \rightsquigarrow$ a suitable height function on $\mathbb{Q}^{\text{alg}}$.

(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).
Theorem I (parametrization)

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

- the union of the images of the \( \phi \in \Phi \) equals \( X \);
- each \( \phi \in \Phi \) is \( C^p \) with \( ||\phi(\alpha)|| \leq 1 \) for \( |\alpha| \leq p \).
Theorem I (parametrization)

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

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

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 \( \phi: (0, 1)^m \to \mathbb{R}^n \) is \( C^p \) with image \( X \) such that \( \|\phi^{(\alpha)}\| \leq 1 \) for \( |\alpha| \leq p \), then for each \( t, X(\mathbb{Q}, t) \) is contained in the union of \( Ct^\varepsilon \) hypersurfaces of degree \( d \);
- \( \varepsilon = \varepsilon(m, n, d) \to 0 \) as \( d \to \infty \).
Toy case of the PILA-WILKIE Theorem:

\[ X = \Gamma(f) \text{ where } f : (0, 1) \to (0, 1) \text{ is definable.} \]
Toy case of the Pila-Wilkie Theorem:

\[ X = \Gamma(f) \text{ where } f : (0, 1) \to (0, 1) \text{ is definable.} \]

Let \( \varepsilon > 0 \) be given. Choose \( d \) so that \( \varepsilon(1, 2, d) \leq \varepsilon \), and then choose \( C, p \) as in Theorem II. Let \( \Phi \) 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 \( C_1 := C \cdot |\Phi| \).
Toy case of the PILA-WILKIE Theorem:

\[ X = \Gamma(f) \text{ where } f : (0, 1) \to (0, 1) \text{ is definable.} \]

Let \( \varepsilon > 0 \) be given. Choose \( d \) so that \( \varepsilon(1, 2, d) \leq \varepsilon \), and then choose \( C, p \) as in Theorem II. Let \( \Phi \) 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 \( X \cap H \subseteq X^{\text{alg}} \)) or finite of uniformly bounded size (by o-minimality). This allows us to count \( X^{\text{trans}}(\mathbb{Q}, t) \). \( \square \)
Pila's Theorem deals with *elliptic curves*:

\[ y^2 = x^3 + ax + b \quad \text{where} \quad a, b \in \mathbb{C}, \ 4a^3 \neq -27b^2. \]
**Elliptic curves: viewed algebraically**

Pila’s Theorem deals with *elliptic curves*:

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

- 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*:

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

- 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”:

\[
E = \{(x, y) \in \mathbb{C}^2 : y^2 = x^3 + ax + b\} \cup \{0\}
\]
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 $p, q, r \in E$,

$$p + q + r = 0 \iff p, q, r \text{ lie on a line.}$$
Let $E$ be an elliptic curve. Then $E$ can be made into an abelian group with 0 as its identity element. For $p, q, r \in E$,

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

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

$$\Lambda = \mathbb{Z} + \mathbb{Z}\tau \quad \text{where} \quad \tau \in \mathbb{H} := \{ z \in \mathbb{C} : \text{Im} \ z > 0 \}.$$
Let $E$ be an elliptic curve. Then there is a complex analytic surjective group morphism $\pi: \mathbb{C} \to E$ whose kernel is a lattice, which (after a change of coordinates) we may express as

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

Conversely, for every $\tau \in \mathbb{H}$ there is an elliptic curve $E = E_\tau$ and an analytic group morphism $\mathbb{C} \to E$ with kernel $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. 
Let $E$ be an elliptic curve. Then there is a complex analytic surjective group morphism $\pi : \mathbb{C} \to E$ whose kernel is a lattice, which (after a change of coordinates) we may express as

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

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

![Diagram of elliptic curve and lattice](image)
Thus \( \mathbb{H} \) is a parameter space for elliptic curves.
Thus $\mathbb{H}$ is a parameter space for elliptic curves. But the map

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

is not one-to-one:

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

acts on $\mathbb{H}$ via

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

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

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

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

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

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

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

$$j(\sigma) = j(\tau) \iff E_\sigma \cong E_\tau.$$
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:

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

acts on $\mathbb{H}$ via

$$(a \ b \\ c \ d) \cdot \tau = \frac{a\tau + b}{c\tau + d},$$

and for $\sigma, \tau \in \mathbb{H}$:

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

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

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

$$j(\sigma) = j(\tau) \iff E_\sigma \cong E_\tau.$$ (So the “correct” parameter space is $\mathbb{C} \cong \text{SL}(2, \mathbb{Z})\backslash \mathbb{H}$.)
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 \( z \mapsto e^{2\pi i z} : \mathbb{C} \to \mathbb{C}^\times \).
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 $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

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

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

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

$$\text{End}(E) \neq \mathbb{Z} \iff \tau \text{ satisfies a quadratic equation over } \mathbb{Q}.$$
Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

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

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

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

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 $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \in \mathbb{H}$).

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

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

$\text{End}(E) \neq \mathbb{Z} \iff \tau$ 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 $\iff K \subseteq \mathbb{Q}(\zeta)$ for some $\zeta \in \mathbb{U}$. (KRONECKER-WEBER)
- If $E_\tau$ has CM, all abelian extensions of $\mathbb{Q}(\tau)$ can similarly be constructed from $\mathbb{U}$, $j(\tau)$, and torsion points of $E_\tau$. 
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 $n$th classical modular polynomial ($n \in \mathbb{N}_{\geq 1}$)

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 $\Phi_n$ are symmetric in $X$ and $Y$. 

**Pila’s Theorem**
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 $n$th classical modular polynomial ($n \in \mathbb{N}_{\geq 1}$)

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 $\Phi_n$ are symmetric in $X$ and $Y$.

For example,

$$\Phi_2 = X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY + 8748000000X + Y^3 - 162000Y^2 + 8748000000Y - 157464000000000.$$
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.
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

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

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

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 $\mathbb{R}_{\text{an,exp}}$. 
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

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

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 $\mathbb{R}_{\text{an,exp}}$.

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

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

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

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 \( j \).
Many recent results employ and further develop ingredients from this circle of ideas:

- in number theory: Ullmo-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, ...
SCANLON’s excellent surveys:

