O-minimality and Diophantine Geometry

Jonathan Pila

University of Oxford

ICM 2014, Seoul

Themes

- Rational points on **definable sets in o-minimal structures** and applications to some Diophantine problems comprehended within the **Zilber-Pink conjecture**.
- **Model theory of** (complex and real) **exponentiation**.
- **Schanuel's conjecture** in transcendental number theory.

Plan

- Diophantine geometry: **Mordell conjecture to Zilber-Pink**
- Transcendental number theory: **Schanuel and Ax-Schanuel**
- Model theory of exponentiation, **o-minimal structures**
- **Counting rational points**
- Diophantine applications: ingredients and problems

Diophantine geometry: Mordell's conjecture

Diophantine problems: solving systems of algebraic equations

$$F_i(x_1, \ldots, x_n) = 0, i = 1, \ldots, m, \quad F_i \in \mathbb{Z}[x_1, \ldots, x_n]$$

for x_i in integers, rational numbers,...

When does a system have only **finitely many** solutions?

Conjecture (Mordell,1922; proved by Faltings, 1983)

A plane algebraic curve $F(x, y) = 0$ of genus ≥ 2 defined over $\mathbb{Q}$ has only finitely many rational points.

E.g. any (projectively) non-singular curve of degree 4 or greater. Likewise over a number field K, $[K, \mathbb{Q}] < \infty$.

L.J. Mordell, *Proc. Cam. Phil. Soc.* **21** (1922), 179–192;
S. Lang, *Ann. Mat. Pura. Appl.* (4) **70** (1965), 229–234.

On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees. By L. J. MORDELL, Manchester College of Technology.

[*Received* 1 May, *read* 22 May, 1922.]

§ 1. Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results*, as that of finding the rational solutions†, or say for shortness, the solutions of indeterminate equations of genus unity of the forms

$$\left.\begin{aligned} \zeta^2 &= a\xi^4 + b\xi^3\eta + c\xi^2\eta^2 + d\xi\eta^3 + e\eta^4 \\ y^2 &= ax^4 + bx^3 + cx^2 + dx + e \end{aligned}\right\} \quad \ldots\ldots\ldots(1),$$

$$0 = f(x, y, z) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2),$$

where f is a ternary homogeneous cubic in x, y, z, including as a particular case

$$y^2 = 4x^3 - g_2x - g_3 \quad \ldots\ldots\ldots\ldots\ldots\ldots(3);$$

and there is no loss of generality in assuming that the coefficients of all equations in this paper are integers. Our present knowledge is based on three types of results, of which the first enables us in general to find an infinite number of solutions when a finite number have already been found, e.g. by trial, and has been known in principle for some centuries. For a value of x, y, z, satisfying equation (2) defines a rational point P on the cubic curve (2); and the tangent at P will meet the cubic in another rational point P_1 different in general from P. Not only can this process be repeated with P_1, but if another rational point Q is known, then the intersection of the chord PQ with the cubic gives also a rational point. This process can in general be continued indefinitely.

The analytical interpretation is obvious from equation (3). For if we know several solutions, say $x_1, y_1; x_2, y_2, \ldots$, we define arguments $u_1, u_2 \ldots$ by writing

$$x_1 = \wp(u_1), \quad y_1 = \wp'(u_1), \quad \text{etc.}$$

in the usual notation of elliptic functions. The addition formula then shows that the formulae

$$x = \wp(m_1u_1 + m_2u_2 \ldots), \quad y = \wp'(m_1u_1 + m_2u_2 \ldots) \quad \ldots(4)$$

* See, for example, vol. II. of Dickson's *History of the Theory of Numbers*.

† We may suppose that ξ, η, ζ in equation (1), and x, y, z in equation (2) are all integers.

Division points on curves.

by SERGE LANG (a New York)

In memory of Guido Castelnuovo in the recurrence of the first centenary of his birth.

Summary. - *A curve contained in a product of multiplicative groups passing through the origin, and containing infinitely many torsion points is a subgroup. The analogous statement on abelian varieties is discussed and reduced to an analogue of the irreducibility of the cyclotomic equation.*

Let A be an abelian variety, or a product of multiplicative groups (or a group extension of these), defined over the complex numbers, say. Let Γ_0 be a finitely generated subgroup of A, and let V be a curve (subvariety of dimension 1) in A, passing through the origin, say. When A is an abelian variety, the MORDELL conjecture has been expressed as asserting that *if the intersection of V with Γ_0 is infinite, then V is a group subvariety* (cf. [2], [3]). When A is a product of multiplicative groups, then I proved the analogous statement in [2], [3].

A few years ago, MUMFORD asked me the following question:

If a curve in its Jacobian contains infinitely many points of finite period, is the curve of genus 1? The same question arose in MANIN'S investigations of the PICARD–FUCHS equations [4]. At the time I did not see how to make a conjecture which would include all the above statements, but now it seems to me that one can formulate such a conjecture as follows: *Let Γ be the division group of Γ_0, i.e. the group of points P on A such that there exists some integer $n \geqq 1$ (depending on P) such that nP lies in Γ_0. If the intersection of V with Γ is infinite, then V is a group subvariety.* In other words, from a diophantine point of view, when one considered previously a finitely generated group, one may as well consider its division group. Taking Γ_0 to be the unit element of A yields the special case when Γ consists of all points of finite period on A.

When A is a product of multiplicative groups, then the conjecture admits a particularly elementary formulation:

Let Γ_0 be a finitely generated multiplicative group of complex numbers, and let Γ be the group of complex numbers z such that z^n lies in Γ_0 for some n (depending on z).

Step 1: From Mordell to Mordell-Lang

Curve $C \subset (\mathbb{C}^\times)^2$ defined by $F(x, y) = 0, F \in \mathbb{C}[X, Y]$.

Theorem (Ihara-Serre-Tate; Lang 1965)

If infinitely many $(\xi, \eta) \in C$ with ξ, η roots of unity then F is of form

$$x^n y^m = \zeta,$$

with $n, m \in \mathbb{Z}$, not both zero, ζ a root of unity.

...so C is a coset of a subgroup by a torsion point: "torsion coset".

Consider $V \subset (\mathbb{C}^\times)^n$. If $\dim V \geq 2$ it may contain positive dimensional torsion-cosets:

Theorem ("Multiplicative Manin-Mumford"; Mann/Laurent)

V contains only finitely many **maximal** *torsion cosets.*

Manin-Mumford and Mordell-Lang

If $(\mathbb{C}^\times)^n$ is replaced by an Abelian variety $X = \Lambda\backslash\mathbb{C}^n$:

Conjecture (Manin-Mumford, 1960's; proved by Raynaud, 1983)

A subvariety V of an abelian variety X contains only finitely many maximal torsion cosets.

Now we replace torsion points by the **division group** Γ of a finitely generated group, torsion cosets by Γ-cosets of abelian subvarieties.

Theorem (Mordell-Lang conjecture; Faltings, Vojta, McQuillan et al 1983-1995)

A subvariety V of an abelian variety X contains only finitely many maximal Γ-torsion cosets.

Implies Mordell's conjecture, as a curve embeds in its Jacobian and group of rational points is finitely generated (**Mordell, 1922**-Weil).

Step 2: ...to André-Oort...

We consider $V \subset X$ where X is a **Shimura variety**.

.. certain arithmetic quotients, e.g. moduli spaces; example below

Such X has a collection $\{T\}$ of "**special subvarieties**", including "**special points**".

Conjecture (André-Oort)

Let X be a Shimura variety and $V \subset X$ a subvariety. Then V contains only finitely many maximal special subvarieties.

- André (1998): $X = \mathbb{C}^2$, unconditional
- Edixhoven, Klingler, Ullmo, Yafaev (1998–2014): on GRH
- O-minimality and point-counting (2011–): unconditional cases

$\mathbb{C}$ as a Shimura variety

Background: elliptic curves and their moduli:

Lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\tau \in \mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\tau > 0\}$
Elliptic curve: $E_\tau = \Lambda \backslash \mathbb{C}$, has structure of an algebraic curve.
$j(E)$ determines E up to isomorphism over $\mathbb{C}$.

Key for us is the **modular function** a.k.a. j-invariant, j-function:

$$j : \mathbb{H} \to \mathbb{C}, \quad j(\tau) = j(E_\tau).$$

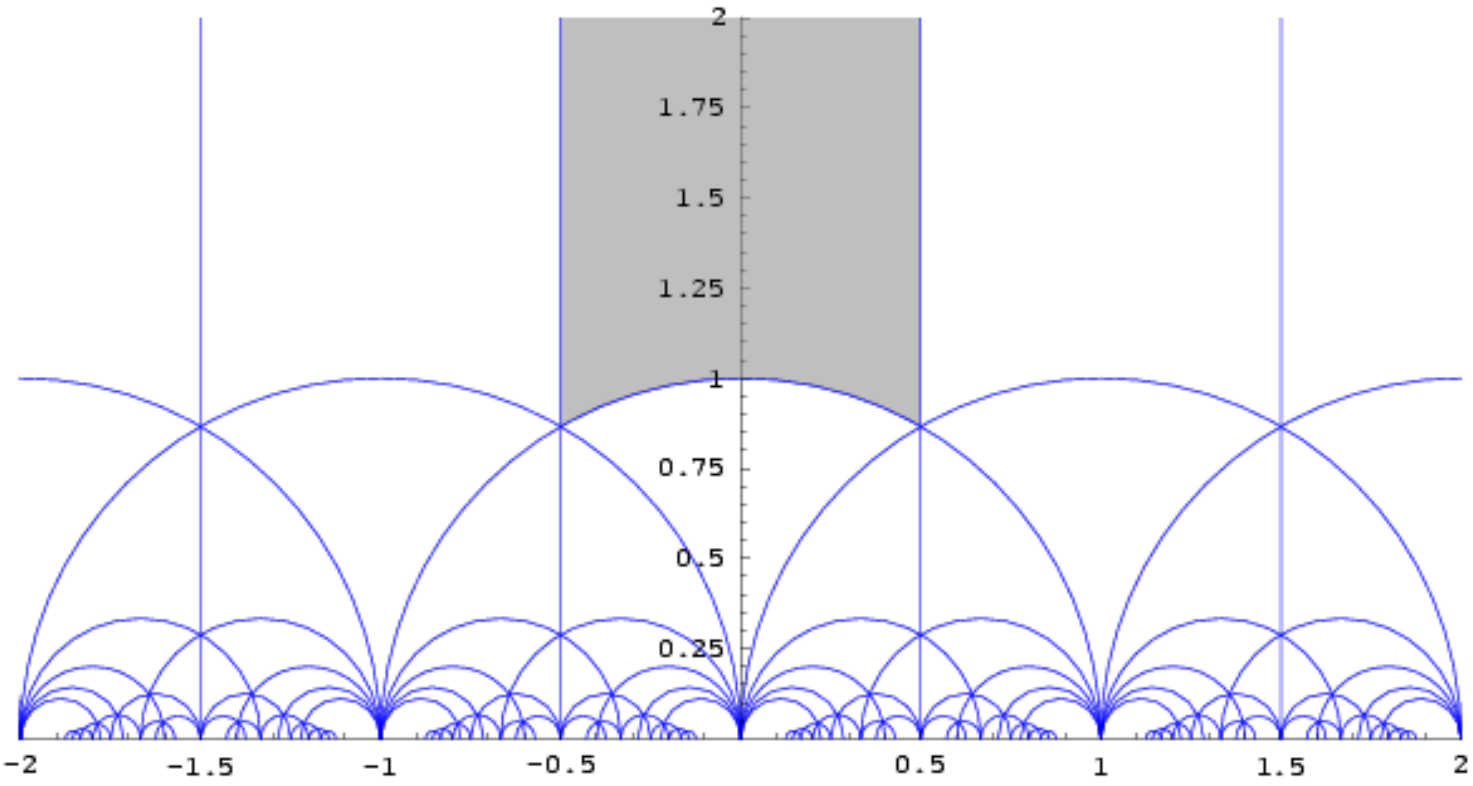
Basic arithmetic properties: $\mathrm{SL}_2(\mathbb{Z})$ **invariance**:

$$j(g\tau) = j(\tau), \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

For $g \in \mathrm{GL}_2^+(\mathbb{Q})$, $\Phi_N(j(\tau), j(g\tau)) = 0$, **modular polynomial** Φ_N.

Special points: $j(\tau)$ where $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$, "CM points"

Fundamental domains for the modular function



$X = \mathbb{C}^2$ as a Shimura variety

Special subvarieties of $X = \mathbb{C}^2$:

- Dimension 2: X.
- Dimension 1: $\{(x, y) : x = j_0\}$ and $\{(x, y) : y = j_0\}$ where j_0 is "special", and modular curves $\Phi_N(x, y) = 0$.
- Dimension 0: special points (j_0, j_1) with j_0, j_1 special.

Theorem (André, 1998)

A curve $C \subset \mathbb{C}^2$ containing infinitely many special points is special.

- Edixhoven 1998: proof on GRH.
- Kühne, Bilu-Masser-Zannier, 2012/13: **effective**.

Some further examples

- $X = \mathbb{C}^n$
  Special subvarieties: irreducible components of algebraic sets defined by some equations $\Phi_N(x_k, x_\ell) = 0$ with various N and $x_h = \sigma$ with various special σ.
  Special points: n-tuples of special points in $\mathbb{C}$.
  Weakly special subvarieties: allow $x_h = c$, any $c \in \mathbb{C}$.
- $X = \mathcal{A}_g$
  Moduli space of pp abelian varieties of dimension g.

Step 3: ...to Zilber-Pink

Let X be a mixed Shimura variety, $V \subset X$ a subvariety

Definition

A subvariety $A \subset V$ is **atypical** if there is a special subvariety $T \subset X$ such that $A \subset V \cap T$ and

$$\dim A > \dim V + \dim T - \dim X.$$

Conjecture (Zilber-Pink)

$V \subset X$ contains only finitely many maximal atypical subvarieties.

Sources: Zilber, Bombieri-Masser-Zannier, Pink.

Open even for $X = (\mathbb{C}^\times)^n$. Implies MM, ML, AO, and much more: "A Mordell conjecture for the 21st century."

ZP for curves

An "atypical component" of a curve $C \subset (\mathbb{C}^\times)^n$ is either:

- A point $P \in C$ satisfying two (or more) independent multiplicative conditions or
- The curve C itself if it satisfies a nontrivial multiplicative condition $x_1^{k_1} \dots x_n^{k_n} = 1$.

Theorem (Maurin, BMZ, 2009)

If $C \subset (\mathbb{C}^\times)^n$, defined over $\mathbb{C}$, is not atypical then there are only finitely many atypical $P \in C$.

Theorem (Habegger-P, 201?)

Let $C \subset A$ be a curve in an abelian variety, both over $\overline{\mathbb{Q}}$. If C is not atypical then there are only finitely many atypical $P \in C$.

Habegger-P, 2012: a partial result for modular setting $C \subset \mathbb{C}^n$.

Transcendence theory: Schanuel's conjecture

Theorem (Lindemann (-Weierstrass) Theorem, 1873/5)

If $z_i \in \overline{\mathbb{Q}}$ are l.i. over $\mathbb{Q}$ then $e^{z_1}, \ldots, e^{z_n}$ are algebraically independent over $\mathbb{Q}$.

Conjecture (Schanuel, circa 1966)

If $z_1, \ldots, z_n \in \mathbb{C}$ are l.i. over $\mathbb{Q}$ then

$$\mathrm{tr.deg.}_{\mathbb{Q}}\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}) \geq n.$$

Implies:

- Baker's theorem
- Four exponentials conjecture
- Algebraic independence of logarithms of multiplicatively independent algebraic numbers
- And much more, but open for $n \geq 2$

Schanuel's Conjecture in Lang, *Intro. Trans. Nbrs.* (1966); J. Ax, *Annals of Mathematics* **93** (1971), 252–268.

INTRODUCTION TO TRANSCENDENTAL NUMBERS

SERGE LANG
Columbia University, New York, New York

For the ordinary exponential function, Schanuel has made a very general conjecture, to the effect that *if* $\alpha_1, \ldots, \alpha_m$ *are complex numbers, linearly independent over* $\mathbf{Q}$, *then the transcendence degree of*

$$\alpha_1, \ldots, \alpha_m, \; e^{\alpha_1}, \ldots, e^{\alpha_m}$$

is at least m. From this statement, one would get most statements about algebraic independence of values of e^t and $\log t$ which one feels to be true.

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts · Palo Alto · London · Don Mills, Ontario

On Schanuel's conjectures

By James Ax*

In this paper proofs are given of conjectures of Schanuel on the algebraic relations satisfied by exponentiation in a differential-algebraic setting. The methods and results are then used to give new proofs and generalizations of the theorems of Chabauty, Kolchin, and Skolem.

1. Introduction

(i) *Statement of the conjectures and our main results.* S. Schanuel has made a conjecture [1, p. 30–31] concerning the exponential function which embodies all its known transcendentality properties such as the theorems of Lindemann [2, p. 225 or 1, Ch. VII, § 2, Th. 1], Baker [3, Cor. 1, 2, and 4, Th. 1, 2], and other results (e.g. [1, Ch. II, Th. 1; Ch. V, Th. 1]) and implies a whole collection of special conjectures (e.g. [1, p. 11, Remark], [5, p. 138, Problems 1, 7, 8] and the algebraic independence of π and e over $\mathbf{Q}$).

The conjecture runs as follows:

(S) Let $y_1, \cdots, y_n \in \mathbf{C}$ be $\mathbf{Q}$-linearly independent. Then

$$\dim_{\mathbf{Q}} \mathbf{Q}(y_1, \cdots, y_n, e^{y_1}, \cdots, e^{y_n}) \geqq n \, .$$

Here $\dim_E F$, for any extension of fields F/E, denotes the cardinality of a maximally E-algebraically independent subset of F.

Schanuel also made the analogous power series conjecture.

(SP) Let $y_1, \cdots, y_n \in t\mathbf{C}[[t]]$ be $\mathbf{Q}$-linearly independent. Then

$$\dim_{\mathbf{C}(t)} \mathbf{C}(t)(y_1, \cdots, y_n, \exp y_1, \cdots, \exp y_n) \geqq n \, .$$

In this paper we prove (SP) and obtain certain generalizations and related results.

Let us consider the hypothesis

(Σ) Let $y_1, \cdots, y_n \in \mathbf{C}[[t_1, \cdots, t_m]]$ be $\mathbf{Q}$-linearly independent. Then

$$\dim_{\mathbf{Q}} \mathbf{Q}(y_1, \cdots, y_n, \exp y_1, \cdots, \exp y_n) \geqq n + \operatorname{rank}\left(\frac{\partial y_\nu}{\partial t_\mu}\right)_{\substack{\nu=1,\cdots,n \\ \mu=1,\cdots,m}} \, .$$

Then (S) is the special case of (Σ) when $m = 0$ (or when each $y_\nu \in \mathbf{C}$). (SP)

* This research was performed while the author was partially supported by NSF Grant GP-12814 and partially while the author was an IBM summer faculty employee at the T. J. Watson Research Center, Yorktown Heights, New York.

Ax-Schanuel

K a field of locally meromorphic functions with derivations D_i, $\mathbb{C} = \bigcap \ker D_i$, containing functions $x_1, \ldots, x_n$ and $e^{x_1}, \ldots, e^{x_n}$.

Definition

The $x_1, \ldots, x_n$ are called **linearly independent over $\mathbb{Q}$ mod $\mathbb{C}$** if there are no non-trivial equations $\sum q_i x_i = c, \ q_i \in \mathbb{Q}, \ c \in \mathbb{C}$.

Theorem ("Ax-Schanuel", Ax, 1971)

If $x_1, \ldots, x_n$ are linearly independent over $\mathbb{Q}$ mod $\mathbb{C}$, then

$$\mathrm{tr.deg.}_{\mathbb{C}} \mathbb{C}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}) \geq n + \mathrm{rank}_K(D_k x_\ell).$$

"Ax-Lindemann"

Consider algebraic $W \subset \mathbb{C}^n$ with $z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n} \in K$ the field of functions meromorphic on $U \subset W$.

Then $z_1, \ldots, z_n$ fail to be "linearly independent over $\mathbb{Q}$ mod $\mathbb{C}$" iff W is contained in a proper "weakly special subvariety".

Theorem ("Ax-Lindemann")

If W is not contained in a proper weakly special subvariety then $\exp(W)$ is Zariski-dense in $(\mathbb{C}^\times)^n$.

Else $\exp(W) \subset V$ for some proper $V \subset (\mathbb{C}^\times)^n$. Another form:

Theorem ("Ax-Lindemann")

For algebraic $V \subset (\mathbb{C}^\times)^n$, a **maximal** *algebraic $W \subset \exp^{-1}(V)$ is weakly special.*

Model theory: complex exponentiation

First-order theory of $\mathbb{C}$ is very well behaved: complete, decidable,...

$\mathrm{Th}(\mathbb{C}_{\exp})$ is complicated, as $\mathbb{Z}$ is definable:

$$\mathbb{Z} = \{z \in \mathbb{C} : \forall w \big(\exp(w) = 1 \to \exp(zw) = 1 \big) \}.$$

Zilber showed: an "infinitary" formulation of the theory $\mathbb{C}$ with an exponential satisfying SC and "exponential algebraic closedness" is well-behaved.
See work of: D'Aquino, Macintyre, Terzo, Shkop, Kirby, Onshuus,..

Zilber formulated "CIT" = ZP for $(\mathbb{C}^{\times})^n$ (and semiabelian vars).

CIT and the Uniform Schanuel Conjecture

Conjecture (Uniform Schanuel Conjecture, Zilber 2002)

Let $V \subset \mathbb{C}^{2n}$ be an algebraic set defined over $\mathbb{Q}$ with $\dim V < n$. There exists a finite set $\mu(V)$ of proper $\mathbb{Q}$-linear subspaces of $\mathbb{C}^n$ such that if $(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}) \in V$ then there is $M \in \mu(V)$ and $k = (k_1, \ldots, k_n) \in \mathbb{Z}^n$ such that $z + 2\pi i k \in M$. Moreover if M has codimension one then $k = 0$.

Theorem (Zilber, 2002)

SC plus CIT implies USC.

Also USC implies CIT (and SC).

Model theory: real exponentiation

Question (Tarski)

Is $\mathrm{Th}(\mathbb{R}_{\exp})$ *decidable?*

Led to development of "o-minimality" by van den Dries and Pillay-Steinhorn.

Theorem (Wilkie, 1993)

$\mathrm{Th}(\mathbb{R}_{\exp})$ *is (model-complete and) o-minimal.*

Theorem (Macintyre-Wilkie, 1996)

Assume SC. Then $\mathrm{Th}(\mathbb{R}_{\exp})$ *is decidable.*

O-minimality

$\mathbb{R}$ with some relations and functions e.g. $<, \times, +, f_1, \ldots, R_j, \ldots$, and consider **definable sets** in this "language", i.e. sets $Z \subset \mathbb{R}^n, n = 1, 2, \ldots$ with a definition

$$Z = \{z \in \mathbb{R}^n : \phi(z) \text{ holds } \}$$

with $\phi(z)$ a formula built using $<, +, \times, f_i, R_j,$ constants, $\neg, \wedge$ and quantifiers $\forall, \exists$ ranging over $\mathbb{R}$. E.g.

$$Z = \{(x, y, z) \in \mathbb{R}^3 : \exists u \exists v \big(u = \exp v\big) \wedge \big(xu^2 + yu + z = v\big)\big\}.$$

Definition

Such a structure $(\mathbb{R}, <, \times, +, f_i, R_j, \ldots)$ is **o-minimal** if every definable subset of $\mathbb{R}$ is a finite union of points and intervals.

E.g. fails with $\sin x$. Key points:

- This condition is **very strong**; such a structure is "tame".
- **Examples**: $\mathbb{R}_{\exp}$, $\mathbb{R}_{\text{an exp}}$ are o-minimal.

Counting rational points on algebraic varieties

Example: Expect there are no non-trivial integer solutions to

$$x^5 + y^5 = w^5 + z^5.$$

"Trivial" solutions: $\{x, y\} = \{w, z\}$.

Known that trivial solutions "out-number" non-trivial ones: $\text{height} = \max(|w|, |x|, |y|, |z|)$. Hooley (1964) proved

$$\#\{\text{nontrivial solutions up to height } \leq T\} \ll_\epsilon T^{5/3+\epsilon},$$

while $\#\{\text{trivial solutions up to height } \leq T\} \sim 2T^2$.

Conjectures of Bombieri, Lang and the philosophy of "Geometry governs arithmetic".

Counting rational points in definable sets

- Bombieri-P, 1989 : results for integer points on plane curves
- Heath-Brown 2002: p-adic method for rational points on vars
- What about higher-dimensional "real analytic" sets $Z \subset \mathbb{R}^n$?

Definition

Let $Z \subset \mathbb{R}^n$. The **algebraic part** Z^{alg} of Z is the union of connected positive dimensional semi-algebraic sets contained in Z. The **transcendental part** of Z is $Z^{\mathrm{trans}} = Z - Z^{\mathrm{alg}}$

Semi-algebraic = finite boolean combinations of sets defined by algebraic equations and inequations.

Height: $H(a/b) = \max(|a|, |b|)$ for $a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1$. For $q \in \mathbb{Q}^n$, $H(q) = \max(H(q_1), \ldots, H(q_n))$.

Counting: For $Z \subset \mathbb{R}^n$ set $Z(\mathbb{Q}, T) = \{z \in Z \cap \mathbb{Q}^n : H(z) \leq T\}$.

The Counting Theorem

Theorem (P-Wilkie, 2006)

If $Z \subset \mathbb{R}^n$ is definable in some o-minimal structure and $\epsilon > 0$ then there exists $c(Z, \epsilon)$ such that

$$\#Z^{\mathrm{trans}}(\mathbb{Q}, T) \leq c(Z, \epsilon) T^{\epsilon}.$$

Method: elementary analysis; o-minimal Yomdin-Gromov paramaterizations of definable sets.

Algebraic points of bounded degree:
$Z(k, T) = \{z \in Z : [\mathbb{Q}(z_i) : \mathbb{Q}] \leq k, H(z_i) \leq T, i = 1, \ldots, n\}$.
Under same conditions:

$$\#Z^{\mathrm{trans}}(k, H) \leq c(Z, k, \epsilon) H^{\epsilon}.$$

"Special point" problems

Setting: $\pi : U \to X$, $V \subset X$, say V defined over $\mathbb{Q}$. Examples:

- $$\mathbf{e} : \mathbb{C}^n \to (\mathbb{C}^\times)^n, \quad \mathbf{e}(z) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n})$$
  Invariance: $\mathbb{Z}^n$ translations; Fundamental domain:
  $$F = F_e^n, \quad F_e = \{z : 0 \leq \mathrm{Re}(z) \leq 1\}.$$
  Ingredient 1: $\pi|F$ is definable in $\mathbb{R}_{\mathrm{an\ exp}}$
  Pre-image of torsion points are rational points in $\mathbb{C}^n$
  Count rational points in $Z = \pi^{-1}(V) \cap F$, definable

- $$\mathbf{j} : \mathbb{H}^n \to \mathbb{C}^n, \quad \mathbf{j}(z) = (j(z_1), \ldots, j(z_n))$$
  Invariance: $\mathrm{SL}_2(\mathbb{Z})^n$ action; Fundamental domain:
  $$F = F_j^n, \quad F_j = \{z : |\mathrm{Re}(z)| \leq 1/2, |z| \geq 1\}$$
  Ingredient 1: $\pi|F$ is definable in $\mathbb{R}_{\mathrm{an\ exp}}$
  Pre-image of special points: quadratic points in $\mathbb{H}^n$
  Count quadratic points in $Z = \pi^{-1}(V) \cap F$, definable

$\mathbf{e} : \mathbb{C}^n \to (\mathbb{C}^\times)^n$, ctd

- Ingredient 1: $\pi|F$ is definable
  Count rational points in definable $Z = \pi^{-1}(V) \cap F$
- Ingredients 2 and 3: Lower (Galois) and upper (height) bounds
  $[\mathbb{Q}(\exp(2\pi i/N)) : \mathbb{Q}] = \phi(N) \approx N$
  If $\zeta \in V$ has order N get $\approx N$ preimages in $Z(\mathbb{Q}, N)$
- Ingredient 4:
  Ax-Lindemann: maximal algebraic subvarieties of $\pi^{-1}(V)$ are weakly special: A special case of "Ax-Schanuel"
- Final inductive argument completes proof of:

Theorem

$V \subset (\mathbb{C}^\times)^n$ contains only finitely many maximal torsion cosets.

L.Kronecker, *Zur theorie der elliptischen functionen*, 1883-; C.-L. Siegel, *Acta Arithmetica* **1** (1935), 83–86

ZUR THEORIE DER ELLIPTISCHEN FUNCTIONEN.[1])

[Gelesen in der Akademie der Wissenschaften am 19. April 1883 (I—III), am 26. April 1883 (IV—V), am 30. Juli 1885 (VI—X), am 27. Mai und 29. Juli 1886 (XI), am 31. Januar 1889 (XII), am 21. Februar 1889 (XIII).]

Die hier folgenden Entwickelungen sollen zur Vorbereitung und Begründung von Resultaten dienen, welche ich einerseits bei meinen Untersuchungen über die allgemeinen Invarianten (vgl. die Sitzung vom 20. April v. J.)[2]) und andererseits bei denen über die elliptischen Functionen mit singulären Moduln erlangt habe, und welche ich in weiteren Mittheilungen auseinandersetzen werde.

I.

Ich behalte die Bezeichnungen bei, welche ich in meinen früheren auf die Theorie der elliptischen Functionen bezüglichen Aufsätzen, namentlich in den Monatsberichten vom Januar 1863[3]), vom Juli 1880[4]), vom October 1880[5]) und vom December 1881[6]) angewendet habe und setze demgemäss[7]):

$$\vartheta(\zeta, \omega) = \sum_{\nu} e^{\frac{1}{4}(\nu^2 w + 4\nu\zeta - 2\nu)\pi i} \qquad (\nu = \pm 1, \pm 3, \pm 5, \ldots).$$

Hiernach ist auch (vgl. Monatsbericht vom October 1880)[5]):

$$\vartheta(\zeta, w) = 2e^{\frac{1}{4} w \pi i} \sin \zeta\pi \prod_{n} (1 - e^{2nw\pi i}) \prod_{n,\,\varepsilon} (1 - e^{2(nw + \varepsilon\zeta)\pi i}),$$

$$(\varepsilon = +1, -1;\ n = 1, 2, 3, \ldots)$$

[1]) Vgl. Zusatz 82 am Endes dieses Bandes. H
[2]) Vgl. Zusatz 83 am Ende dieses Bandes. H
[3]) Bd. IV, S. 222 dieser Ausgabe von *L. Kronecker*'s Werken. H
[4]) Bd. IV, S. 287 dieser Ausgabe von *L. Kronecker*'s Werken. H
[5]) Bd. IV, S. 291 dieser Ausgabe von *L. Kronecker*'s Werken. H
[6]) Bd. IV, S. 314 dieser Ausgabe von *L. Kronecker*'s Werken. H
[7]) Vgl. Zusatz 84 am Ende dieses Bandes. H

Über die Classenzahl quadratischer Zahlkörper.

Von

Carl Ludwig Siegel (Frankfurt a/M.).

Durch eine scharfsinnige Combination zweier Ansätze von Hecke und Deuring ist es Heilbronn gelungen, den lange vermuteten Satz zu beweisen, dass die Classenzahl $h(d)$ des imaginären quadratischen Zahlkörpers der Discriminante d mit $|d|$ unendlich wird. Es ist naheliegend, nach einer genaueren unteren Abschätzung von $h(d)$ zu fragen. Im folgenden soll die asymptotische Formel

$$\log h(d) \sim \log \sqrt{|d|} \tag{1}$$

bewiesen werden. Da nach Dirichlet

$$\pi |d|^{-\frac{1}{2}} h(d) = L_d(1) \qquad (d < -4)$$

gilt, wo

$$L_d(s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-s}$$

gesetzt ist, so ist (1) mit der Aussage

$$\log L_d(1) = o(\log |d|) \tag{2}$$

gleichbedeutend. Man wird vermuten, dass (2) auch für positive Discriminanten d richtig ist; und dies wird ebenfalls bewiesen werden. Bedeutet ε_d die Grundeinheit, so ist nach Dirichlet

$$2 d^{-\frac{1}{2}} h(d) \log \varepsilon_d = L_d(1) \qquad (d > 0)$$

und folglich die Beziehung

$$\log (h(d) \log \varepsilon_d) \sim \log \sqrt{d}$$

das Analogon zu (1) für reelle quadratische Körper.

$\mathbf{j} : \mathbb{H}^n \to \mathbb{C}^n$, ctd

Ingredient 1: $\pi|F$ is definable
Count quadratic points in definable $Z = \pi^{-1}(V) \cap F$

Ingredients 2 and 3:

- Quadratic point $\tau \in \mathbb{H}$ has discriminant $\Delta(\tau) = b^2 - 4ac$ where $ax^2 + bx + c$ is the minimal polynomial for τ over $\mathbb{Z}$.
- Classical CM theory: $[\mathbb{Q}(j(\tau) : \mathbb{Q}] = h(\mathcal{O}_\Delta)$, **class number** of the corresponding quadratic order, is "large" (Landau-Siegel):
$$h(\mathcal{O}_\Delta) \approx |\Delta(\tau)|^{1/2}.$$
- Preimage in F has height $\approx |\Delta(\tau)|$.
- So a special point of large discriminant in V gives "many" quadratic points in Z, most must lie in Z^{alg}.

$\mathbf{j} : \mathbb{H}^n \to \mathbb{C}^n$, ctd

Last: characterise maximal (complex) algebraic subsets of $j^{-1}(V)$.

Ingredient 4: "Modular Ax-Lindemann"

Theorem (P, 2011)

A maximal algebraic $W \subset \mathbf{j}^{-1}(V)$ is weakly special.

Method: If $W \subset \mathbf{j}^{-1}(V)$ then so are "many" of its $\mathrm{SL}_2(\mathbb{Z})^n$-translates.

Apply the Counting Theorem to certain definable subsets of $\mathrm{SL}_2(\mathbb{R})^n$ with "many" points from $\mathrm{SL}_2(\mathbb{Z})^n$.

Inductive argument concludes (using more o-minimality):

Theorem (P, 2011)

AO for $\mathbb{C}^n$.

Further applications to AO

Setting: $\pi : U \to X$, $V \subset X$. Always have:

* $U \subset \mathbb{C}^N$: hermitian symmetric domain
* π is invariant under Γ
* Pre-images of special pts are algebraic pts of bounded degree.

Ingredients to prove AO:

- **Ing. 1. Definability**: Peterzil-Starchenko for $\mathcal{A}_g$ (and $\mathcal{X}_g$), Klingler-Ullmo-Yafaev and Gao in general (mixed Shimuras)
- **Ing. 2. Galois lower bound**: Tsimerman for $\mathcal{A}_g, g \leq 6$
- **Ing. 3. Height upper bound**: P-Tsimerman for $\mathcal{A}_g$, all g
- **Ing. 4. Ax-Lindemann**: Ullmo-Yafaev for compact cases, P-Tsimerman for $\mathcal{A}_g$ and Klingler-U-Y and Gao in general, all using o-minimality and point-counting.

AO known: for all $\mathcal{A}_g^n$, $g \leq 6$ (and corresponding mixed cases).

O-minimality and atypical intersections

Turning to broader ZP problems (AO is very special):

O-minimality and point-counting are applicable to other cases:

- "Relative MM problems" of Masser-Zannier$\pm$ Bertrand-Pillay
- Results by (combinations of) Bays, Habegger, Orr, P

Special subvarieties correspond to rational points on certain Grassmanian-type varieties (e.g. parameterising subavarieties of $\mathbb{H}^n$ defined by real Mobius transformations).

Given $V \subset X = \mathbb{C}^n$, say, the set of subvarieties defined by Mobius transformations which intersect the definable set Z in a set of some given (atypical) dimension is definable, and we can apply the counting theorem.

Conditional Modular ZP

- LGO: "Large Galois Orbit" conjecture for suitable atypical intersection points
- WCA: "Weak Complex Ax" conjecture for the j-function

Theorem (Habegger-P, 201?)

Assume LGO and WCA. Then ZP holds for $\mathbb{C}^n$,

WCA follows from a "Modular Ax-Schanuel" conjecture.
Result announced by P-Tsimerman 2014.