I

Point-counting *and* diophantine applications

Jonathan Pila

UNIVERSITY OF OXFORD

Hermann Weyl Lecture, IAS, 23 October 2018

Overview

General topic: diophantine problems

- But: some will involve *non-algebraic sets*
- With: applications to classical diophantine problems around the *André-Oort conjecture*
- Leads to: *functional transcendence* questions

“Geometry governs arithmetic”

Conjecture (Mordell 1922; Faltings 1983)

A curve of genus at least 2 has only finitely many rational points.

E.g. A non-singular plane quartic (or higher) curve.

Conjecture (Lang's General Conjecture)

An algebraic variety V is “mordellic” outside its “special set”.

E.g. Expect no non-trivial solutions in positive integers to

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

Browning–Heath-Brown: trivial solutions ($\asymp T^2$ up to height T) outnumber non-trivial $\ll_\epsilon T^{13/8+\epsilon}$ (improving Hooley $5/3+\epsilon$).

Rational points on non-algebraic sets

Non-algebraic function f, analytic on $U \supset [0, 1]$, graph

$$Z : y = f(x), \quad x \in [0, 1]$$

Possible (Weierstrass... van der Poorten): $f(\mathbb{Q}) \subset \mathbb{Q}$.

But (Bombieri-P, 1989):
In a height density sense there are "few" rational points.

With Alex Wilkie (2005): Extension to higher dimensional sets $Z \subset \mathbb{R}^n$ "definable in an o-minimal structure".

Umberto Zannier: Strategy to reprove Manin-Mumford conjecture (Raynaud's theorem),

The non-algebraic/algebraic connection

Via: **the arithmetic properties of classical special functions.**

Under the **exponential function**

$$e : \mathbb{C} \to \mathbb{C}^{\times}, \quad e(z) = \exp(2\pi i z),$$

rational numbers map to **roots of unity**.

Studying **rational points** on

$$\mathcal{Z} = \{(z, w) \in \mathbb{C}^2 : F\big(e(z), e(w)\big) = 0\}, \quad F \in \mathbb{C}[X, Y]$$

a possible route to study **torsion points** (root-of-unity coords) on

$$V : F(x, y) = 0.$$

The non-algebraic/algebraic connection: André-Oort

The **modular function** (a.k.a. the j function)

$$j : \mathbb{H} \to \mathbb{C}, \quad \mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

maps **quadratic points** (over $\mathbb{Q}$) to **singular moduli**, algebraic numbers with rich arithmetic properties.

Studying **quadratic points** on

$$\mathcal{Z} = \{(z, w) \in \mathbb{H}^2 : F\big(j(z), j(w)\big) = 0\}, \quad F \in \mathbb{C}[X, Y]$$

a possible route to **"special points"** (singular moduli coords) on

$$V : F(x, y) = 0.$$

The counting function

Let $Z \subset \mathbb{R}^n$, $T \geq 1$ set

$$Z(\mathbb{Q}, T) = \{z \in Z : z_i \in \mathbb{Q}, H(z_i) \leq T, i = 1, \ldots, n\},$$

where **height** $H(a/b) = \max(|a|, b), \gcd(a, b) = 1, b \geq 1$, and

$$N(Z, T) = \#Z(\mathbb{Q}, T).$$

Extend H to number fields (Weil height); then count points of degree (up to) $d \geq 1$:

$$Z(d, T) = \{z \in Z : [\mathbb{Q}(z_i) : \mathbb{Q}] \leq d, H(z_i) \leq T, i = 1, \ldots, n\}$$

$$N(Z, d, T) = \#Z(d, T).$$

Analytic curves

Consider $f : [0,1] \to \mathbb{R}$, f real analytic on a nbd, graph Z.

Methods of Bombieri-P 1989 yield: Z has "few" rational points.

Theorem

For $\epsilon > 0$, $$N(Z,T) \le c(f,\epsilon)T^{\epsilon}.$$

Lemma (H. A. Schwarz, 1880)

Let $\phi_1, \ldots, \phi_D \in C^{D-1}(I)$, $x_1, \ldots, x_D \in I$, $\Delta = \det\big(\phi_i(x_j)\big)$. *Then*

$$\Delta = V(x_1, \ldots, x_D) \det\left(\phi_i^{(j-1}(\xi_{ij})\right)$$

where V *is Vandermonde and* ξ_{ij} *suitable points. Hence*

$$|\Delta| \le c(\max_{k<D}\{|\phi_i^k|\})\,|I|^{D(D-1)/2}.$$

Proof of Theorem

Combines: The "fundamental theorem of transcendence theory" ($\mathbb{Z} \cap (0,1) = \emptyset$) with a "zero-estimate".

Proof. Fix d, let $D = (d+1)(d+2)/2$ and apply Lemma with the D monomial functions $\phi_{ij} = x^i f(x)^j, i + j \le d$.
Suppose $x_k \in J$ with $(x_k, f(x_k)) \in Z(\mathbb{Q}, T)$, J subinterval.

Then Δ has denominator $\le T^{dD/3}$ but $|\Delta| \ll_{f,d} |J|^{D(D-1)/2}$.

Now $dD \asymp d^3$ but $D(D-1)/2) \asymp d^4$.
So if $|J|^{D(D-1)/2} \ll_{f,d} T^{-dD/3}$ then $\Delta = 0$.
So **all** $(x_k, y_k) \in Z, x_k \in J$ lie on **one** algebraic curve $\deg(Y) \le d$.

Now $[0,1]$ can be covered by $\ll_{f,d} T^{\frac{3}{d+3}}$ such subintervals.

(So: Given ϵ, choose d: $3/(d+3) \le \epsilon$.)

But $\# Z \cap Y, \deg Y \le d$, **uniformly bounded**. $\square$

Observe: we did not really need f to be analytic.

Higher dimensional sets

Try to count rational points on $Z \subset \mathbb{R}^n$.

- Z should be "tame": "**definable in an o-minimal structure**" e.g. image Z of $\phi : [0,1]^k \to [0,1]^n$ real analytic on nbd.
- A non-algebraic, Z might still contain positive-dimensional semi-algebraic subsets, which could have "many" rational points. E.g. $Z : z = x^y, x, y \in [2,3]$.

Definition

The *algebraic part* $Z^{\mathrm{alg}} \subset Z$ is the union of all connected positive-dimensional semi-algebraic sets $A \subset Z$.

The Counting Theorem

Theorem (P-Wilkie, 2006)

Let $Z \subset \mathbb{R}^n$ be "definable in an o-minimal structure", $\epsilon > 0$. Then

$$N(Z - Z^{\mathrm{alg}}, T) \leq c(Z, \epsilon) T^{\epsilon}.$$

Remarks

- A crude analogue of Lang's General Conjecture.
- (But can do better than just exclude all of Z^{alg}.)
- Implies one-dimensional result for more curves.
- Similarly, $N(Z - Z^{\mathrm{alg}}, d, T) \leq c(Z, d, \epsilon) T^{\epsilon}$.
- Result is uniform in "definable families" $Z \subset \mathbb{R}^n \times \mathbb{R}^m$.

Multiplicative Manin-Mumford (MMM)

Theorem (Lang 1965: Ihara, Serre, Tate)

Let $V \subset \left(\mathbb{C}^{\times}\right)^2$ be a curve defined by $F(x,y) = 0$. Then V has only **finitely many** *torsion points unless F is of form $X^n Y^m = \zeta$ where $n, m \in \mathbb{Z}$ not both zero and ζ root of unity.*

Torsion coset: the translate of a subtorus by a torion point. Eqvtly, a component of an algebraic subgroup, i.e. cpt of some system of multiplicative equations:

$$x^a = x_1^{a_1} \dots x_n^{a_n} = 1 \quad , x^b = 1, \dots.$$

Theorem (Laurent, Mann, Sarnak)

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

Classical MM (Raynaud, 1983): replace $\left(\mathbb{C}^{\times}\right)^n$ by an abelian vty.

Sketch proof of MMM. First step: Opposing bounds

Let $e : \mathbb{C}^n \to \left(\mathbb{C}^\times\right)^n$. Identify $\mathbb{C} = \mathbb{R}^2$. Let $F = [0,1) \times i\mathbb{R}$ fundamental domain for $\mathbb{Z}^n$ action.

Theorem

Let $V \subset \left(\mathbb{C}^\times\right)^n$. Then $e^{-1}(V) \cap \mathbb{Q}^n$ consists of the $\mathbb{Z}^n$ translates of **finitely many** *rational linear subvarieties contained in $e^{-1}(V)$.*

Sketch proof. Can assume V is defined over a number field. Let

$$Z = e^{-1}(V) \cap F^n.$$

Then Z is a "definable set" in $\mathbb{R}^{2n}$ (full $e^{-1}(V)$ isn't).

A torsion point $\zeta \in V$ of order N has nearly N conjugates, so get:
$\gg N^{1/2}$ rational points on Z of height $\ll N$ on Z.

So (CT with e.g. $\epsilon = 1/4$) large N gives: semi-algebraic $A \subset Z$.

Second step: Functional transcendence

Have positive dimensional semi-algebraic $A \subset Z$, by analytic continuation get positive dimensional **complex algebraic**

$$W \subset e^{-1}(V).$$

Theorem (Ax, 1971; "Ax-Schanuel"; implies "Ax-Lindemann")

Functional version of Schanuel's Conjecture (next lecture). Implies: $e(W)$ is Zariski-dense in $(\mathbb{C}^\times)^n$ unless $W \subset L$ a translate of a proper $\mathbb{Q}$ subspace

Translate of $\mathbb{Q}$-subspace L a **weakly special subvariety**.

If now $e(W)$ is Zariski dense in $e(L)$ we get $e(L) \subset V$. Else W is contained in a further proper $L' \subset L$.

Theorem ("Ax-Lindemann")

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

Conclusion

Weakly special $L \subset e^{-1}(V)$ give cosets of subtori $T \subset V$, which is essentially the exceptional case: only torsion cosets $\ni$ torsion pts.

Need: the maximal weakly special subvarieties in $e^{-1}(V)$ are translates of **finitely many** $\mathbb{Q}$ subspaces.

This can be proved in (at least) 3 ways:

- Explicit, effective argument of Bombieri-Masser-Zannier
- O-minimality (the set of such $\mathbb{Q}$ subspaces is "definable"; L2)
- Model-theoretic compactness on Ax-Schanuel theorem.

For each such $\mathbb{Q}$-subspace, the torsion cosets of it contained in V gives a lower dimensional MMM problem.

Conclude by induction. $\square$

Modular André-Oort

The André-Oort conjecture is an analogue of Manin-Mumford.
The simplest cases are obtained by replacing:
the (cartesian product of the) **exponential function**

$$e : \mathbb{C}^n \to \left(\mathbb{C}^\times\right)^n$$

by the (cartesian product of the) **modular function**

$$j : \mathbb{H}^n \to \mathbb{C}^n.$$

$$j : \mathbb{H} \to \mathbb{C}, \quad j(z) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n, \quad q = e(z),$$

holomorphic in $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

The j function

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.
The j-invariant $j(E)$ determines E up to isomorphism over $\mathbb{C}$.

The **modular function** a.k.a. j-invariant, j-function:

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

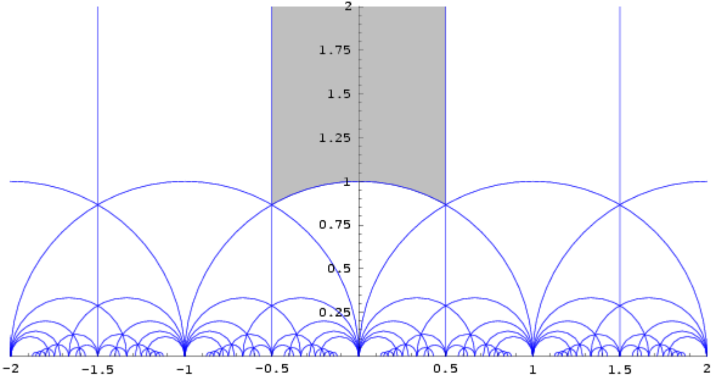
Basic arithmetic properties: $\mathrm{SL}_2(\mathbb{Z})$ **invariance**:

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

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

Fundamental domain for the j-function

The classical fundamental domain F for the $\mathrm{SL}_2(\mathbb{Z})$ action.



E.g. $X = j(z)$ and $Y = j(2z) = j(\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} z)$ are related by

$$0 = \Phi_2(X, Y) = -X^2Y^2 + 1488(X^2Y + XY^2) + Y^3$$
$$-162.10^3(X^2+Y^2)+40773375XY+8748.10^3(X+Y)-157464.10^9.$$

Singular Moduli

Singular moduli are the "special values" of the j-function.

Definition

A **singular modulus** is a complex number $j(\tau)$ where $j : \mathbb{H} \to \mathbb{C}$ is the modular function, and $\tau \in \mathbb{H}$ is quadratic ($[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$).

$$\Sigma = \{\sigma = j(\tau) : \tau \in \mathbb{H}, [\mathbb{Q}(\tau) : \mathbb{Q}] = 2\}$$

Schneider: These are precisely the points with $\tau, j(\tau) \in \overline{\mathbb{Q}}$.

These are the elliptic curves with "complex multiplication" (CM): there are non-integer $\mu : \mu\Lambda_\tau \subset \Lambda_\tau$.

They are algebraic integers.

E.g. $j(\frac{1+\sqrt{-163}}{2}) = -2^{18}3^3 5^3 23^3 29^3$, $\quad j(\sqrt{-5}) = (50 + 26\sqrt{5})^3$.

Theorem of André

Theorem (André 1998)

Let $V \subset \mathbb{C}^2$. Then V contains only finitely many **special points** *unless V is a* **special subvariety**, *that is*

- *A modular curve*
- *a vertical or horizontal line on a singular modulus*

Also proved by Edixhoven 1998 under GRH, which led to further cases of AO under GRH, such as $\mathbb{C}^n$, 2005, and full proof of AO under GRH by Klingler-Ullmo-Yafaev.

André's thm is the analogue of the Lang/Ihara/Serre/Tate thm:

Theorem

Let $V \subset \left(\mathbb{C}^\times\right)^2$. Then V contains only finitely many **torsion points** *unless V is a* **torsion coset**.

Special subvarieties and AO in $\mathbb{C}^n$

Special points in $\mathbb{C}^n$: *n*-tuples of singular moduli.

Special subvarieties of $\mathbb{C}^n$:

1. The hypersurface $\Phi_N(x_i, x_j) = 0$ is special;
2. Also hypersurfaces $x_k = \sigma$, where σ a singular modulus;
3. Irreducible cmpnnts of intersections of special subvts are special.

Equivalently: the images of maps of the form

$$\mathbb{H} \ni z \mapsto (g_1 z, \ldots, g_k z) \in \mathbb{C}^k, \quad g_i \in \mathrm{GL}_2^+(\mathbb{Q}),$$

and cartesian products of such images and special points.

Weakly special subvs: same but any point is weakly special.

Theorem (P 2011; Edixhoven 2005 on GRH)

A subvariety $V \subset \mathbb{C}^n$ contains only **finitely many** *maximal special subvarieties.*

Sketch proof

Since special points are algebraic we can assume V defined over a number field. We consider

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

and take the "definable set" (the full $j^{-1}(V)$ isn't)

$$Z = j^{-1}(V) \cap F^n \subset \mathbb{R}^{2n}.$$

A special point $\sigma \in V$ has a pre-image $\tau \in Z$ which is a quadratic point. We will apply the Counting Theorem to quadratic points. A quadratic point $\tau_i \in \mathbb{H}$ has a minimal polynomial

$$a\tau_i^2 + b\tau_i + c = 0, \quad a, b, c \in \mathbb{Z}, \quad \gcd(a, b, c) = 1,$$

and discriminant

$$D(\tau_i) = b^2 - 4ac < 0, \quad D(\tau) = \max\left(D(\tau_i)\right)$$

First step: Opposing bounds

The discriminant measures "complexity" of the special point.
For $j(\tau) = \sigma$ with $\tau \in F$ have:

$$H(\tau) \ll |D(\tau)|.$$

The theory of CM gives that

$$[\mathbb{Q}(\sigma_i) : \mathbb{Q}] = h\big(D(\tau_i)\big),$$

the **class number** of the corresponding quadratic order. One has

$$h(D) \geq c(\epsilon)|D|^{1/2-\epsilon},$$

for $\epsilon > 0$, by a classical (ineffective) theorem of Siegel.

A positive proportion (depending on field of definition of V) of the conjugates land back on V and by Counting (with some $\epsilon < 1/2$) we see that **one** special point of large complexity gives **too many** quadratic points in Z, unless we have "algebraic" $W \subset j^{-1}(V)$.

Second step: "Ax-Lindemann" for the modular function

Theorem (Modular "Ax-Lindemann"; P 2011)

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

- Equivalently: $j(W)$ is Zariski dense in $\mathbb{C}^n$ unless some coordinate on W is constant, or $z_i = gz_k$ on W for some $g \in \mathrm{GL}_2^+(\mathbb{Q})$.
- Implies: The "bi-algebraic" varieties are precisely the weakly specials subvarieties.
- Observe: If $j(W)$ is not Zariski dense, i.e. the $j(z_i)$ restricted to $z \in W$ are algebraically dependent over $\mathbb{C}$, then already either one of them is (i.e. constant) or two are (modular relation).

Sketch proof of Modular Ax-Lindemann

Sketch proof. Say $W \subset j^{-1}(V)$ with $W \cap F^n \neq \emptyset$.
Each "translate" gW of W by $g \in \mathrm{SL}_2(\mathbb{Z})$ has $gW \subset j^{-1}(V)$, and "many" of these also intersect F^n and so Z.

The full space of $\mathrm{SL}_2(\mathbb{R})$ translates is definable, as is its intersections with Z, and we get a definable set which intersects Z locally in its full dimension, with "many" rational $(\mathrm{SL}_2(\mathbb{Z}))$ points.

Counting: get a positive-dimensional semi-algebraic set of such translates, hence complex algebraic family.

Try to enlarge W by taking a union over the family. If W is maximal, it must be stable under a lot of translations, and prove it is weakly special. $\square$

Conclusion of proof of Modular AO

Show: the maximal weakly special subvarieties of V come in finitely many families i.e the $\mathrm{GL}_2^+(\mathbb{Q})$ relations (the "translates" are the constant coordinates).

Proof: By o-minimality, as the set of them is "definable". □

Conclude by induction. □

Ineffective due to: (1) Siegel lower bound and (2) The counting and (3) this finiteness step (now effective).

Kühne, Bilu-Masser-Zannier: Effective proof of André's theorem ($\mathbb{C}^2$), and Bilu-Kühne: effective AO for linear subvarieties of $\mathbb{C}^n$.

A lot of progress towards effective counting (or better bounds: Wilkie's conjecture) by Butler, Jones-(Miller-)Thomas, Binyamini-Novikov, Cluckers-P-Wilkie.

The André-Oort conjecture

André (1989), Oort (1994): the "same" statement for a Shimura variety X, certain kind of arithmetic quotient

$$u : \Omega \to X, \quad \Gamma\backslash\Omega = X$$

for a suitable Hermitian symmetric domain Ω, and arithmetic group Γ. E.g. Siegel modular varieties $\mathcal{A}_g$.

Such X has **special subvarieties**, which are "Shimura subvarieties" in a compatible way, the zero-dimensional ones being the **special points**. Also **weakly special subvarieties**, which are precisely the "bi-algebraic" varieties (Ullmo-Yafaev).

Conjecture (André-Oort)

Let $V \subset X$. Then V contains only finitely many maximal special subvarieties.

Ingredients for AO via point-counting

Ullmo showed: point-counting proves AO given:

1. **Definability** of $u : \Omega \to X$ on a fundamental domain F. This holds by Peterzil-Starchenko ($\mathcal{A}_g$), Klingler-Ullmo-Yafaev for arithmetic quotients.
   Also: Klingler, Bakker-Tsimerman: period mappings and new proof of Cattani-Deligne-Kaplan.
2. **Height bound** for pre-image in F of a special point. Tsimerman ($\mathcal{A}_g$); Daw-Orr in general.
3. **Ax-Lindemann**: P, UY, P-Tsimerman ($\mathcal{A}_g$), KUY in general. All use point-counting (also monodromy, Hwang-To, ...)
4. **Lower bound for Galois orbits of special points.** Tsimerman, for $\mathcal{A}_g$, required the "Averaged Colmez conjecture" (Andreatta-Goren- Howard- Madapusi Pera; Yuan-Zhang, 2015) and isogeny estimates (Masser-Wustholz).

The André-Oort Conjecture

Theorem

The André-Oort conjecture holds...

1. *unconditionally for* $\mathbb{C}^2$ *(André,1998)*
2. *under GRH (Edixhoven, Klingler-Ullmo-Yafaev, 1998-2014)*
3. *unconditionally* $\mathbb{C}^n, \ldots, \mathcal{A}_g$ *(P ... Tsimerman 2015; ineffctive)*
4. *in general assuming lower bounds for Galois orbits (see prev)*
5. *for the corresponding mixed Shimura varieties (Gao)*
6. *effectively for* $\mathbb{C}^2$ *(Kühne, Bilu-Masser-Zannier)*
7. *effectively for linear subvars of* $\mathbb{C}^n$ *(Bilu-Kühne)*
8. *"nearly effective" for* $\mathbb{C}^n$ *(Binyamini)*

With items 3, 4, 5, 8 via point-counting.
Item 6: Linear forms in logarithms, item 7, 8. Class field theory.
Item 8: also, Duke+Siegel-Tatuzawa (Kowalski)

Next lectures

Next lectures

- L2: O-minimality and point-counting; Ax-Schanuel properties
- L3: The Zilber-Pink conjecture

THANK YOU!