Rational points of definable sets and Diophantine problems

Jonathan Pila

University of Bristol

MODNET

Barcelona, 4 November 2008

Key points

* Upper bounds for the number of rational points of height $\leq T$ on certain **non-algebraic** sets $X \subset \mathbb{R}^n$.

* Guiding idea: A "transcendental" set has "few" rational points "in a suitable sense".

* Connection with transcendence theory.

* Connection with Manin-Mumford conjecture and other results in diophantine geometry.

Plan

I Curves

II Higher dimensions – Main result

III Wilkie's conjecture

IV Manin-Mumford conjecture

V Andre-Oort-Manin-Mumford type results

Notation

$$X(\mathbb{Q}, T) = \{x \in X : x \in \mathbb{Q}^n, H(x) \le T\}$$

where $X \subset \mathbb{R}^n$ and **height** $H(x)$ is defined by

$$H(a_1/b_1, \ldots, a_n/b_n) = \max(|a_i|, |b_i|)$$

for

$$a_i, b_i \in \mathbb{Z}, b_i \ne 0, \gcd(a_i, b_i) = 1, i = 1, \ldots, n.$$

(Not projective height.)

The **counting** or **density function** of X, for $T \ge e$ to avoid trivialities:

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

Seek upper bound estimates for $N(X, T)$.

Constants $c(\ldots)$ may differ at each occurence.

I. Curves

Bombieri+JP (1989): results for **integer points** on the **homothetic dilation**

$$tX = \{(tx_1, \ldots, tx_n) : (x_1, \ldots, x_n) \in X\}.$$

(where $t \geq 1$) of a graph

$$X : y = f(x), x \in I = [a, b].$$

Upper bounds for $\#\left(tX \cap \mathbb{Z}^2\right)$, as $t \to \infty$, for

* f smooth and convex (won't discuss)

* f real analytic

* upper bounds for

$$\#\left(X(\mathbb{Z}) \cap [0, T]^2\right)$$

when f is algebraic (mention briefly)

Transcendental analytic curves

Consider $X : y = f(x), x \in I = [a, b]$ where function f is real-analytic and non-algebraic.

Theorem. *We have, for every* $\epsilon > 0$*,*

$$\#\left(tX \cap \mathbb{Z}^2\right) \leq c(f, \epsilon)t^\epsilon$$

Note: $t \geq 1$ need not be an integer.

Theorem. (JP, 1991) *For every* $\epsilon > 0$*,*

$$N(X, T) \leq c(f, \epsilon)T^\epsilon$$

If e.g. $f(x) = e^x$ then (Hermite-Lindemann) the only **algebraic** point of X is $(0, 1)$.

At other extreme, constructions going back to Weierstrass give: entire transcendental f with $f(\mathbb{Q}) \subset \mathbb{Q}$. (van der Poorten...)

Little control of height in such constructions.

Key to method

$X(\mathbb{Q}, T)$ is contained in **few** (i.e. $\leq c(X, \epsilon)T^\epsilon$) **intersections** of X with plane algebraic curves of suitable degree.

Lemma. *Let* $X : y = f(x)$ *be* C^∞ *on* $[0, 1]$ *and* $\epsilon > 0$*. There is a* $d = d(\epsilon)$*: for every* $T \geq 1$*,*

$$X(\mathbb{Q}, T) \subset \bigcup_V X \cap V$$

with the union over $O_{f,\epsilon}(T^\epsilon)$ *plane algebraic curves* V *of degree* d *(possibly reducible).*

Proof of Lemma. Consider points

$$P_i = (x_i, y_i) \in X, i = 1, \dots, E.$$

They lie on a plane algebraic curve of degree d iff the matrix

$$(1 \quad x_i \quad y_i \quad x_i^2 \quad x_i y_i \quad y_i^2 \quad \dots \quad x_i^d \quad \dots \quad y_i^d),$$

$i = 1, \dots, E$, has rank $< D = (d+1)(d+2)/2$.

If not, have D points with

$$\Delta = \det(\phi_j(x_i)) \neq 0$$

where the $\phi_j(x)$ are the D functions of the form $x^\mu f(x)^\nu, 0 \leq \mu, \nu \leq d$.

If $P_i \in X(\mathbb{Q}, T)$, the entries in a row have a common denominator $\leq T^{2d}$. So

$$T^{2dD} |\Delta| \geq 1.$$

Mean value statement: if ϕ_j are functions with $D-1$ continuous derivatives on an interval containing x_i then

$$\frac{\Delta}{V(x_i)} = \frac{1}{0!1!\dots(D-1)!}\,\mathrm{det}\,(\phi_j^{(i-1)}(\zeta_{ij})).$$

for some suitable intermediate points $\zeta_{ij} \in [0,1]$, $V(x_i)$ the Vandermonde determinant.

In our case: $\phi_j(x) = x^\mu f(x)^\nu, 0 \le \mu, \nu \le d$.

If the $x_i \in I, \ell(I) \le r$,

$$T^{-dD} \le |\Delta| \le C(f,d) r^{D(D-1)/2}.$$

Conclusion: if

$$\ell(I) \leq C'(f,d)T^{-2dD/(D(D-1))},$$

the points of $X(\mathbb{Q},T)$ in I all lie on **one** curve of degree d. The interval $[0,1]$ is covered by

$$C''(f,d)T^{2dD/(D(D-1))}$$

such intervals, and since $D = (d+1)(d+2)/2$, the exponent

$$\frac{2dD}{D(D-1)}$$

goes to zero as $d \to \infty$. $\square$

Remark. For given ϵ do not need C^∞: need C^D, $D <<>> 1/\epsilon^2$, and $c(X,\epsilon)$ depends on the size of the derivatives of f up to order $D-1$.

(**Theorem.** *For* $\epsilon > 0$, $X(\mathbb{Q}, T) \leq c(f, \epsilon)T^{\epsilon}$.)

Proof of Theorem.

Choose $d = d(\epsilon)$: $X(\mathbb{Q}, T)$ is contained in $c(f, \epsilon)T^{\epsilon}$ algebraic curves V of degree d.

X is transcendental: $X \cap V$ is *finite* for any V of degree d. Uniform bound

$$\#X \cap V \leq C(d)$$

for any curve V of degree d by **compactness**. Then

$$N(X, T) \leq C(d)c(f, \epsilon)T^{\epsilon}. \square$$

Cannot be much improved.

If $\epsilon(t) : [1, \infty) \to \mathbb{R}$ is positive, monotonically decreasing to 0, have $X : y = f(x), x \in [0, 1]$ transcendental real-analytic, and a (lacunary) sequence T_j such that

$$N(X, T_j) \geq T_j^{\epsilon(T_j)}.$$

E.g. with $\epsilon(t) = (\log t)^{-1/2}$, gives an example

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

satisfying no estimate

$$N(X, T) \leq C(\log T)^c.$$

Cf. results of Surroca: better estimates do hold on a sequence of $T_i \to \infty$.

Algebraic curves

Theorem. (EB+JP 1989, JP 1996) *Suppose* $f \in \mathbb{Z}[x,y]$ *is absolutely irreducible of degree* d, $X = \{(x,y) : f(x,y) = 0\}$. *Then*

$$\#\left(X(\mathbb{Z}) \cap [0,T]^2\right) \leq c(d) T^{1/d} (\log T)^{2d+3}.$$

Exponent $1/d$ is best possible : $y = x^d$.

Improvements: JP, Walkowiak (by Heath-Brown method) – application to Hilbert irreducibility.

Heath-Brown (2002): a p-adic version of method for rational points on projective varieties in all dimensions, in particular

Theorem. (Heath-Brown, 2002) *For* $X \subset \mathbb{P}^2$ *irreducible, degree* d

$$X(\mathbb{Q}, T) \leq c(d,\epsilon) T^{2/d+\epsilon}.$$

Exponent $2/d$ best possible: $y = x^d$.

Point of estimate: **uniformity**

Siegel/Faltings: finiteness of $X(\mathbb{Z})$ (or $X(\mathbb{Q})$) for $g > 0$ but not good uniformity as curve varies with fixed degree.

These uniform bounds are crude but useful, especially in higher dimensional problems, e.g. Waring type problems (e.g. Browning, Greaves, Hooley, Skinner-Wooley, Vaughan-Wooley), and Hilbert irreducibility (e.g. work of Schinzel-Zannier, Walkowiak). Heath-Brown's results have also been useful in further work (HB, Browning, Salberger,...)

Breaking $1/d, 2/d$ **uniformly** when genus $g > 0$: Helfgott-Venkatesh, Ellenberg-Venkatesh.

Bombieri-Zannier: $E(\mathbb{Q})$.

Schmidt conjecture: $c(d, \epsilon)T^{\epsilon}$ for $g > 0$.

II. Higher dimensions

Seek to generalize

$$N(X,T) \le c(X,\epsilon)T^{\epsilon}$$

to suitable "transcendental analytic" $X \subset \mathbb{R}^n$.

Consider e.g. surface $X \subset \mathbb{R}^3$

$$X : z = f(x,y), (x,y) \in [0,1]^2.$$

Straightforward: $X(\mathbb{Q},T)$ contained in

$$O_{X,\epsilon}(T^{\epsilon})$$

intersections of X with algebraic hypersurfaces V of degree $d(\epsilon)$, where the implied constant depends on sizes of derivatives of $f(x,y)$ up to order $D << >> d^n$.

(Determinant Δ, expand entries in Taylor srs.)

Repeat the argument for these intersections: semi-analytic curves $X \cap V$?

Leads to: **(bounded) semi-analytic sets** in $\mathbb{R}^n$.

Then projections: **(bounded) subanalytic sets** in $\mathbb{R}^n$.

These are contained in the **globally sub-analytic sets** in $\mathbb{R}^n$.

This class has "good" properties: dimension theory, stratification, cell decomposition, and strong **finiteness properties** —sets have just finitely many connected components — (get e.g. uniform bounds for intersections with an algebraic curve)

Globally subanalytic sets: an example of an **o-minimal structure over** $\mathbb{R}$.

O-minimal structures over $\mathbb{R}$

Definition. A **pre-structure** is a sequence $S = (S_n : n \geq 1)$, each S_n is a collection of subsets of $\mathbb{R}^n$.

A pre-structure S is called a **structure** (over $\mathbb{R}$) if, for all $n, m \geq 1$,
(1) S_n is a boolean algebra
(2) S_n contains every semialgebraic subset
(3) if $A \in S_n$ and $B \in S_m$, then $A \times B \in S_{n+m}$
(4) if $m \geq n, A \in S_m$ then $\pi(A) \in S_n$, where $\pi : \mathbb{R}^m \to \mathbb{R}^n$ is projection on first n coords

A structure is called **o-minimal** if

(5) The boundary of every set in S_1 is finite.

First 4 axioms: S admits various constructions, condition 5 is the "minimality" condition.

$X \subset \mathbb{R}^n$ is **definable** in S if $X \in S_n$.

Examples.

Semi-algebraic sets: Tarski-Seidenberg

$\mathbb{R}_{\text{an}}$, the globally subanalytic sets: Gabrielov

$\mathbb{R}_{\text{exp}}$: the sets definable using $y = e^x$: Wilkie

$\mathbb{R}_{\text{an,exp}}$: generated by $\mathbb{R}_{\text{an}}$ and $\mathbb{R}_{\text{exp}}$ **together**: van den Dries-Macintyre-Marker

Richer examples. No "largest" o-minimal structure: Rolin, Speissegger, Wilkie

Some problems:

* Curves $X \cap V$ are not presented as graphs with uniformly bounded derivatives (indeed they may be singular).

(The hypersurfaces V that occur vary with T.)

This can be fixed.

* Surface X may contain semi-algebraic sets of positive dimension, e.g. lines. These may contain $>> T^\delta$ rational points up to height T for some $\delta > 0$.

This cannot be fixed!

The "algebraic part"

Definition. The **algebraic part** X^{alg} of a set X is the union of all **connected** semialgebraic subsets of **positive dimension**.

Seek: for suitably "nice" $X \subset \mathbb{R}^n$, and $\epsilon > 0$,

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

Crude analogue of the **special set** V^{special} of V in diophantine geometry .

V^{special} =Zariski closure of $\bigcup$ of images in V of non-constant rational maps of $\mathbb{P}^m$, Abelian varieties.

Bombieri-Lang Conjecture: $(V - V^{\mathsf{sp}})(\mathbb{Q})$ is finite. Curves: Mordell Conjecture (Faltings's Theorem). In higher dimensions, it is open.

"Geometry governs arithmetic"

X^{alg} can be complicated

Example 1. For $1 \leq w, x, y, z \leq 2$ say

$$X_1 : \log w \log x = \log y \log z,$$

For $r \in \mathbb{Q}^\times$ have surfaces $w = y^r, z = x^r$, and $w = z^r, y = x^r$. These are dense in the 3-fold. X_1^{alg} is not definable.

Example 2. For $2 < x, y < 3$ say

$$X_2 : z = x^y$$

Each rational y gives a rational curve in X_2, X_2^{alg} is not definable.

Example 3. For $2 < x, y < 3$ say

$$X_3 : z = 2^{x+y}$$

Here $X_3^{\mathrm{alg}} = X_3$.

Theorem v1. (Wilkie+JP, 2006) *Let X be a set definable in an o-minimal structure over $\mathbb{R}$. Let $\epsilon > 0$. Then*

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

The o-minimal setting: general and natural. Controlled oscillation and compactness bounds for intersections are both consequences of the o-minimality.

Estimate cannot be much improved in general: already in $\mathbb{R}_{\mathsf{an}}$ when $n = 1$.

Later: Wilkie conjectures a substantial improvement for X definable in $\mathbb{R}_{\mathsf{exp}}$.

Strategy

Given $X \subset \mathbb{R}^n$ of dimension k and ϵ:

* can assume $X \subset (0,1)^n$ using $x \mapsto \pm 1/x$.

* by a **parameterization** realize X as union of images of cubes $(0,1)^k$ with bounded derivatives up to order $b(\epsilon/k)$

(For bounded subanalytic sets: uniformization theorem)

* then for suitable degree d, $X(\mathbb{Q}, T)$ contained in $<< T^{\epsilon/k}$ intersections $X \cap V$, with $\deg(V) = d$

* repeat for these $X \cap V$ so

* need **uniform parameterization** of these $X \cap V$ to get a uniform estimate, i.e.

Need a version of Theorem for families

Definable families of sets

A **definable family** means the collection of **fibres** of a projection of a definable set $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ to $\mathbb{R}^m$, considered as sets in $\mathbb{R}^n$.

Theorem v2. *Let $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ be a definable family. Let $\epsilon > 0$. Then there is a constant $c(Z, \epsilon)$ such that, for any fibre X of Z,*

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

In general X^{alg} is not semi-algebraic (or even definable). But perhaps: given $\epsilon > 0$, there is a **semialgebraic** $X_\epsilon \subset X^{\text{alg}}$ such that

$$N(X - X_\epsilon, T) \leq c(X, \epsilon)T^\epsilon?$$

No. Example: $\{(x, y) : 0 < x < 1, 0 < y < e^x\}$.

But one can find a **definable** X_ϵ.

Theorem v3. *Let Z be a definable family, $\epsilon > 0$. There is a definable family $W = W(Z, \epsilon)$ and a constant $c(Z, \epsilon)$ with the following property. Let X be a fibre of Z. Then the corresponding fibre X_ϵ of W has $X_\epsilon \subset X^{\text{alg}}$ and*

$$N(X - X_\epsilon, T) \leq c(Z, \epsilon)T^\epsilon.$$

This version: can make a non-trivial statement in certain cases where $(X - X^{\text{alg}})(\mathbb{Q}) = \emptyset$, e.g. $X_2 : z = x^y$.

Parameterization

What we need:

Let $Z \subset (0,1)^n \times \mathbb{R}^m$ be a definable family of fibre dimension k, and $b \in \mathbb{N}$.

There exists $J \in \mathbb{Z}$ such that, for every fibre X of Z, there exist maps

$$\theta_i : (0,1)^k \to (0,1)^n, i = 1, \ldots, J,$$

$$\bigcup_{i=1}^{J} \theta_i \left((0,1)^k \right) = X$$

and

$$\sup_{z \in (0,1)^k} |\partial_\mu \theta(z)| \leq 1$$

for every partial derivative ∂_μ, $\mu = (\mu_1, \ldots, \mu_k) \in \mathbb{N}^k$ with $|\mu| = \sum \mu_i \leq b$.

Just such a result existed for semialgebraic sets.

Theorem. (Yomdin 1987, Gromov 1987) *Let* $Y = V \cap [0,1]^n$ *where* V *is closed algebraic set of degree* d *and dimension* k*. For each* b*, there is an integer* $N(n,b,d)$ *such that* Y *can be parameterized by at most* N *maps* $\psi : [0,1]^k \to Y$*, all of whose partial derivatives up to order* b *have absolute value bounded by 1.*

Gromov's is a refined version of Yomdin's.

Analogous result can be proved in the o-minimal setting, uniform parameterization for families of definable sets.

(Maps $\theta : (0,1)^k \to (0,1)^n$ will also come in families.)

Key to parameterization

Proposition. *Suppose* $b \geq 2$ *and* $f : (0,1) \to \mathbb{R}$ *is a* C^b*, definable function. Suppose*

$$|f^{(j)}(x)| \leq 1, x \in (0,1), j = 0, \ldots, b-1.$$

Suppose further that $|f^{(b)}|$ *is weakly decreasing. Put* $g(x) = f(x^2)$*. Then, for suitable* C*,*

$$|g^{(j)}(x)| \leq C, x \in (0,1), j = 0, \ldots, b.$$

Proof. For g: clear for $j = 0, \ldots, b-1$, by chain rule.

For bth derivative: Observe: $|f^{(b)}(x)| \leq 4/x$ (otherwise $|f^{(b-1)}(x/2)| > (x/2)(4/x) - 1 = 1$).

Then by chain rule:

$$g^{(b)}(x) = \sum_{i=0}^{b-1} \rho_{ib}(x) f^{(i)}(x^2) + 2^b x^b f^{(b)}(x^2)$$

is bounded as $b \geq 2$. □

Sketch proof of Theorem

Given Z of fibre dimension k and ϵ.

Can assume $k < n$.

Obtain a b-parameterization with b so large that, for every fibre X, $X(\mathbb{Q}, T)$ is contained in $\leq c(Z, \epsilon)T^{\epsilon/k}$ algebraic sets in $\mathbb{R}^n$ of dimension k.

(Intersection of cylinders on hypersurfaces in each choice of $k+1$ coordinates.)

Consider intersections $X \cap V$. Any point that is regular of dimension k in X and V and $X \cap V$ is in a semi-algebraic disk, so in X^{alg}.

So proceed with: the points not regular of dimension k in those intersections. These form a family of fibre dimension $\leq k-1$.

Finally: 0-dimensional family of intersections, bounded number of connected components. □

Extension of result to: algebraic points of bounded degree

Definition. Let $k \geq 1$ For $X \subset \mathbb{R}^n$, $x = (x_1, \ldots, x_n)$ define

$$N_k(X, T) =$$

$$\#\{x \in X : \max_i [\mathbb{Q}(x_i) : \mathbb{Q}] \leq k, \max_i H(x_i) \leq T\}$$

where $H(x_i)$ is the absolute height.

Definition. Let $k \geq 1$. Define $H_k^{\text{poly}}(\alpha) = \infty$ if $[\mathbb{Q}(\alpha) : \mathbb{Q}] > k$. Otherwise

$$H_k^{\text{poly}}(\alpha) = \min\{(H(\xi), \xi = (\xi_0, \ldots, \xi_k) \in \mathbb{Q}^{k+1} - \{0\} :$$

$$\sum \xi_j \alpha^j = 0\}.$$

If $[\mathbb{Q}(\alpha) : \mathbb{Q}] = k$ then $H_k^{\text{poly}}(\alpha) \leq 2^k H(\alpha)^k$.

Theorem. (JP 2008) *Let $X \subset \mathbb{R}^n$ be definable, $k \geq 1$, $\epsilon > 0$. Then*

$$N_k(X,T) = O_{X,k,\epsilon}(T^\epsilon).$$

In fact prove this: using H_k^{poly} instead of H, stronger, and for families of X.

Sketch: have projection

$$Y = \{(x,\xi) \in \mathbb{R}^n \times \mathbb{R}^{n(k+1)} : \ldots\} \to X$$

so Y is definable and also Z where

$$Z = \{\xi \in \mathbb{R}^{n(k+1)} : \ldots\} \leftarrow Y$$

is a semi-algebraic **finite** map. Has semi-algebraic inverse, so get **semialgebraic** map

$$Z \to X.$$

Problem: Y, Z are completely fibred by semi-algebraic subsets, so $Z^{\mathrm{alg}} = Z$ and existing Theorem is trivial.

III. Wilkie's conjecture

In general (in $\mathbb{R}_{\text{an}}$) cannot much improve

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

Conjecture. (Wilkie) Supopose X is definable in $\mathbb{R}_{\text{exp}}$. Then

$$N(X - X^{\text{alg}}, T) \leq c(X)(\log T)^{C}.$$

Should get "version 2" over a number field F, with **exponent of** $\log T$ **independent of** F, and also (version 3)

$$N_k(X - X^{\text{alg}}, T) \leq c(X)(\log T)^{C}.$$

Theorem. (JP 2007) *Wilkie's conjecture holds for a pfaff curve. v2: JP 200?*

"Pfaff curve" = graph of a *pfaffian function* of one variable on a connected (possibly non-compact) subset of its domain.

Example. For $W : y = x^\alpha$, α real irrational, $x \in (0, \infty)$ and $[F : \mathbb{Q}] < \infty$,

$$N_F(W, T) <<_F (\log T)^{20}.$$

Implies: "Forty-Two exponentials". Cannot have 21 algebraic points (x_i, y_i) with x_i multiplicatively independent. ("Six exponentials": same is true with $21 \to 3$).

Point: Wilkie v2 entails estimates of the same quality to ones yielding transcendence results.

Theorem. (JP 2008) *Wilkie's conjecture v2 for*

$$X = \{(x, y, z) \in (0, \infty)^3 : \log z = \log x \log y\},$$

more precisely,

$$N(X - X^{\mathrm{alg}}, T) <<_{F,\epsilon} (\log T)^{44+\epsilon}.$$

I.e. bound for points $(x, y) \in (0, \infty)^2$ where

$$x, \quad y, \quad \exp(\log x \log y)$$

simultaneously in a given F with height $\leq T$, not in X^{alg}.

$X^{\mathrm{alg}} = \{(x, 1, 1)\} \cup \{(1, y, 1)\} \cup \{(x, e^q, x^q)\} \cup \{(e^q, y, y^q)\}, \quad q \in \mathbb{Q}$

Both results use: Gabrielov-Vorobjov bounds for # connected components of pfaffian sets.

Transcendence methods?

IV. The Manin-Mumford conjecture

Analogue for subvarieties of Abelian varieties of Lang conjecture for $V \subset \mathbb{G}_m^n = (\mathbb{C}^*)^n$ and points whose coordinates are roots of unity (torsion points).

Let A be an Abelian variety of dimension g. For $n \in \mathbb{Z}$, n^{2g} n-torsion points, denoted $A[n]$. Their union is the torsion subgroup A_{tor} of A.

Thm: Manin-Mumford conjecture (over $\overline{\mathbb{Q}}$). *Let $V \subset A$, both $/\overline{\mathbb{Q}}$. Then $V \cap A_{\text{tor}}$ is contained in a finite union of cosets of abelian subvarieties of A contained in V.*

Originally proved by Raynaud, 1983 (and $/\mathbb{C}$)

Several proofs exist of MM or combinations (with Mordell (Mordell-Lang), Bogomolov) and quantitative versions.

New proof, with Umberto Zannier (2008).

An abelian variety A of dimension g is complex-analyticially isomorphic to a complex torus

$$\mathbb{C}^g/\Lambda,$$

with Λ a lattice. Have uniformization

$$\pi : \mathbb{C}^g \to A.$$

Take real coordinates on $\mathbb{C}^g$ using a basis of Λ. Then **torsion points** of A correspond to **rational points** in $\mathbb{R}^{2g}$ (order=denominator). Have

$$X = \pi^{-1}(V)$$

semi-analytic and $\mathbb{Z}^g$-periodic.

Apply PW to $X \cap [0,1)^{2g} = \mathcal{X}$ to conclude:

$$N(\mathcal{X} - \mathcal{X}^{\mathrm{alg}}, T) <<_{\mathcal{X},\epsilon} T^{\epsilon}.$$

Since X is periodic show: $\mathcal{X}^{\mathrm{alg}}$ is a union of hyperplanes – indeed subtori corresponding to abelian subvarieties.

So in this situation $X^{\mathrm{alg}} \leftrightarrow V^{\mathrm{special}}$.

Key ingredient: **lower bound** for degree of a torsion point.

Masser: if A, V are defined over a numberfield, and P is a torsion point of order T then

$$d(P) >>_A T^{\delta}$$

for some $\delta > 0$ (depends only on g).

Combine with

$$N(\mathcal{X} - \mathcal{X}^{\mathsf{alg}}, T) <<_{\mathcal{X},\epsilon} T^{\epsilon}$$

for some $\epsilon < \delta$.

MM for A, V over numberfield follows. □

Should also prove $\mathbb{G}_m$ case.

Relative Manin-Mumford conjecture

Conjecture. (Pink) Let X be an irreducible variety over $\mathbb{C}$ and $B \to X$ an algebraic family of semiabelian varieties. Let $Y \subset B$ be an irreducible closed subvariety, not contained in any proper closed subgroup scheme of $B \to X$. If Y contains a zariski dense subset of torsion points then $\dim Y \geq \dim(B/X)$.

Theorem. (Masser-Zannier 2008) *There are only finitely many* $\lambda \in \mathbb{C}, \lambda \neq 0, 1$ *such that*

$P_\lambda = (2, \sqrt{2(2-\lambda)})$, and $Q_\lambda = (3, \sqrt{6(3-\lambda)})$

are **both** *of finite order on*

$$E_\lambda : y^2 = x(x-1)(x-\lambda).$$

So $X = \mathbb{C}$, $B_\lambda = E_\lambda \times E_\lambda$, $Y = \{(P_\lambda, Q_\lambda)\}$.

For P_λ alone: infinitely many λ, but sparse.

The "unlikely intersection" of the two sparse sets is finite.

V. Andre-Oort conjecture

Analogue of MM.

Manin-Mumford conjecture:

$A_{\text{tor}} \subset A \supset V \supset$ torsion coset of ab. subv. ?

Andre-Oort conjecture:

special points $\subset S \supset V \supset$ special subvariety?

AO is now Theorem of Yafaev-Klingler-Ullmo under GRH for CM fields

Example: $\mathbb{C}$ is a Shimura variety, as j-line. Special points = j invariants of CM elliptic curve. No interesting subvarieties.

Another example: $\mathbb{C}^2$ is a Shimura variety parameterizing pairs of elliptic curves.

Special points: (j, j'), j, j' both CM points.

Special subvarieties: "vertical" , "horizontal" copies of $\mathbb{C}$ with the fixed coordinate a CM point, $\mathbb{C}^2$ itself, and **modular curves**.

Recall: $j : \mathbb{H} \to \mathbb{C}$, invariant under $\mathrm{SL}_2(\mathbb{Z})$. If $\tau' = N\tau$ then $F_N(j(\tau), j(\tau')) = 0$. More generally if $\tau' = \gamma\tau$ for $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$ acting as fractional linear transformation on $\mathbb{H}$.

CM values of $j \in \mathbb{C} \leftrightarrow$ imag. quadratic $\tau \in \mathbb{H}$, preserved by $\tau' = \gamma\tau$ for $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$. So modular curves $V \subset \mathbb{C}^2 : F_N(x, y) = 0$ have lots of special points.

Early case of AO:

Theorem. (André, Edixhoven 1998) *Let V be an irreducible curve in $\mathbb{C}^2$. Then V contains only finitely many special points unless V is a special subvariety.*

Edixhoven: **conditional** on GRHIQ, **uniform** for curves of given degree and degree of definition, and **effective** (Breuer 2001).

Andre: **unconditional**, but **not uniform**.

New proof (JP, 2008). **Unconditional** and also **uniform** (but **ineffective** without GRHIQ)

Sketch proof. Can assume V defined over $\overline{\mathbb{Q}}$.

Have $\mathrm{SL}_2(\mathbb{Z})^2$ invariant map

$$\pi : \mathbb{H}^2 \to \mathbb{C}^2, \quad \pi(\tau_1, \tau_2) = (j(\tau_1), j(\tau_2)).$$

Let F be the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. Have

$$\{(j, j') \text{ CM points}\} \subset \mathbb{C}^2 \supset V,$$

pull back under π to get

$$\{(\tau, \tau') \text{ quadratic points}\} \subset \mathbb{H}^2 \supset X$$

and X is an $\mathrm{SL}_2(\mathbb{Z})^2$ invariant **analytic** set.

Show: X contains no **semialgebraic curves** except possibly of form $z = \gamma z'$ for $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$, vertical or horizontal lines i.e. (almost) just if V has no special subvarieties as components.

Definability.

$j : \mathbb{H} \to \mathbb{C}$ is not definable in any o-minimal structure, as it is periodic under $\mathsf{SL}_2(\mathbb{Z})$, so j^{-1}(point) is an infinite discrete set.

But $j : F \to \mathbb{C}$ is.

The Weierstrass $\wp$ function $\wp(\tau, z)$. For $\tau \in \mathbb{H}$, doubly periodic meromorphic function in z with fundamental parallelogram

$$\mathbb{L}_\tau = \{t_1 + t_2\tau : 0 \le t_1, t_2 < 1\}.$$

Peterzil-Starchenko: $\wp(\tau, z)$ is definable on

$$\{(\tau, z) : \tau \in F, z \in \mathbb{L}_\tau\}$$

in the o-minimal structure $\mathbb{R}_{\text{an,exp}}$. And the "exp" is necessary.

Definability of $j : F \to \mathbb{C}$ follows.

Continue sketch proof of André-Oort for $\mathbb{C}^2$.

We view X as a real surface in $\mathbb{R}^4$, and $\mathcal{X} = X \cap F^2$ is definable.

Suppose V contains no special subvarieties then *essentially* X contains no algebraic curves. Then , if $\epsilon > 0$,

$$N_2(\mathcal{X}, T) \leq c(X, \epsilon) T^{\epsilon}$$

For discriminant D of an imag. quad. order,

$$h(D) >>_{\delta} |D|^{1/2-\delta}$$

by Siegel (ineffective; effective under GRHIQ).

$$H(\text{Im}(\tau)), H(\text{Re }(\tau)) << H(\tau) << |D|^{1/2},$$

and $j(\tau)$ has $h(D)$ conjugates.

Suppose $(\tau_1, \tau_2) \in \mathcal{X}$ with τ_1, τ_2 imag. quadratic.

Put $\tau_1 = u + iv, \tau_2 = x + iy$.

Put $\Delta = \max(|D(\tau_1)|, |D(\tau_2)|)$.

$H(u, v, x, y) \le 16\sqrt{\Delta}$

Conjugates of $(j(\tau_1), j(\tau_2))$ come from points $(\tau_1', \tau_2') \in F^2$ with same discriminant, so same bound on height. A positive fraction $c(V)$ of the conjugates also lie on V. So

$$c(\delta)c(V)\Delta^{1/2-\delta} \le N_2(\mathcal{X}, 16\sqrt{\Delta}) \le c(X, \epsilon)(16\sqrt{\Delta})^{\epsilon}$$

Choose $\delta = 1/4, \epsilon = 1/3$ say. Estimates are untenable once Δ is sufficiently large. □

Two further “André-Oort-Manin-Mumford” type results.

Elliptic curve in Legendre form (rational 2-torsion):

$$E_\lambda: \quad y^2 = x(x-1)(x-\lambda), \quad \lambda \neq 0, 1$$

Surface $A \subset \mathbb{A}^1 \times \mathbb{P}^2$

$$Y^2 Z = X(X-Z)(X-\lambda Z), \quad \lambda \neq 0, 1$$

Special points: (λ, P) where E_λ is CM and $P \in E_\lambda$ torsion.

Special subvarieties: “vertical” some $\{\lambda\} \times E_\lambda$, CM, “horizontal”: a torsion section, A itself.

Theorem. (JP 2008) *Let V be an irreducible curve in A. Then the number of special points of V is finite unless V is special.*

A variant of a result of André ($\leq$ 2001):

Finiteness for special points on a non-torsion section of a non-isotrivial elliptic pencil.

Our A is a particular non-isotrivial pencil as j is a non-constant function of λ, but our V need not be a section.

Again: unconditional and uniform (for V) but ineffective.

Modular elliptic curve $X_0(N) \to E$.

Can ask: when is the image of a special point (=CM point) of $X_0(N)$ torsion on E?

= special points on the graph Γ of $X_0(N) \to E$, $\Gamma \subset X_0(N) \times E$.

The map is non-constant and surjective, so not special.

Heegner points. Nekovar-Schappacher (1999): for the CM points with Heegner conditions, only finitely many map to torsion in E. (and for abelian variety A instead of E)

Let $A = X_0(N) \times E$, any elliptic curve over $\overline{\mathbb{Q}}$.

Special points: (CM, torsion).

Special subvarieties: "vertical" $\{P\} \times E$, where P is CM, "horizontal" constant maps to $Q \in E$ torsion, A.

Theorem. (JP 2008) *Let V be an irreducible curve in A. Then V has only finitely many special points unless V is special.*

Remark. Definability in all these results is in $\mathbb{R}_{\mathrm{an,exp}}$ by Peterzil-Starchenko. Subanalytic sets are not enough. The o-minimal generality is necessary.

***

"'Tame" geometry governs arithmetic"