Sparsity of rational points on curves: What is known and what is expected

Ziyang Gao

Leibniz University Hannover, Germany

VaNTAGe seminar
Feb. 20, 2024

Motivation

It is a fundamental question in mathematics to solve equations.

For example:
$f(X, Y)$= polynomial in X and Y with coefficients in $\mathbb{Q}$.
What can we say about the $\mathbb{Q}$-solutions to $f(X, Y) = 0$?

$\rightsquigarrow$
Diophantine problem. Rational points on algebraic curves.

Some examples:

$f(X, Y)$	$X^2 + Y^2 - 1$	$Y^2 - X^3 - X$	$Y^2 - X^3 - 2$	$Y^2 - X^6 - X^2 - 1$
$\mathbb{Q}$-solutions	$(3/5, 4/5)$, $(5/13, 12/13)$, $(8/17, 15/17)$, *etc.* infinitely many	$(0, 0)$, $(\pm 1, 0)$. finitely many	$(-1, 1)$, $(34/8, 71/8)$, $(2667/9261, 13175/9261)$, *etc.* infinitely many	$(0, \pm 1)$, $(\pm 1/2, \pm 9/8)$. finitely many
genus of the associated curve	0	1	1	2

Motivation

It is a fundamental question in mathematics to solve equations.

For example:
$f(X, Y)$= polynomial in X and Y with coefficients in $\mathbb{Q}$.
What can we say about the $\mathbb{Q}$-solutions to $f(X, Y) = 0$?

$\rightsquigarrow$

Diophantine problem. Rational points on algebraic curves.

Some examples:

$f(X, Y)$	$X^2 + Y^2 - 1$	$Y^2 - X^3 - X$	$Y^2 - X^3 - 2$	$Y^2 - X^6 - X^2 - 1$
$\mathbb{Q}$-solutions	$(3/5, 4/5)$, $(5/13, 12/13)$, $(8/17, 15/17)$, *etc.* infinitely many	$(0, 0)$, $(\pm 1, 0)$. finitely many	$(-1, 1)$, $(34/8, 71/8)$, $(2667/9261, 13175/9261)$, *etc.* infinitely many	$(0, \pm 1)$, $(\pm 1/2, \pm 9/8)$. finitely many
genus of the associated curve	0	1	1	2

Setup and Genus 0

In what follows,

- $g \geq 0$ and $d \geq 1$ integers;
- K= number field of degree d;
- $C =$ irreducible smooth projective curve of genus g defined over K.

As usual, we use $C(K)$ to denote the set of K-points on C.

✎ If $g = 0$, then either $C(K) = \emptyset$ or $C \cong \mathbb{P}^1$ over K.

Setup and Genus 0

In what follows,

- $g \geq 0$ and $d \geq 1$ integers;
- K= number field of degree d;
- $C =$ irreducible smooth projective curve of genus g defined over K.

As usual, we use $C(K)$ to denote the set of K-points on C.

✎ If $g = 0$, then either $C(K) = \varnothing$ or $C \cong \mathbb{P}^1$ over K.

Genus 1

Assume $g = 1$.
If $C(K) \neq \emptyset$, then $C(K)$ has a structure of abelian groups with an identity element $O \in C(K)$. $\rightsquigarrow$ Elliptic curve $E/K := (C, O)$.

Theorem (Mordell–Weil)

$E(K)$ is a finitely generated abelian group. Namely,

$$E(K) \cong \mathbb{Z}^{\rho} \oplus E(K)_{\mathrm{tor}}$$

with $\rho < \infty$ and $E(K)_{\mathrm{tor}}$ finite.

Genus 1: infinite part

✎ In general, no effective method to calculate ρ.

Conjecture (Birch and Swinnerton–Dyer)

$\rho = \mathrm{ord}_{s=1} L(E, s)$.

Coates–Wiles, Gross–Zagier, Kolyvagin, Rubin, Breuil–Conrad–Diamond–Taylor, Darmon, Bhargava–Shankar, Nevokar, Dokchitser–Dokchitser, Skinner–Urban...

✎ Upper bound:

- Ooe–Top '89: $\rho \leq c_1 \log |N_{K/\mathbb{Q}} \mathcal{N}_{E/K}| + c_2$, where $\mathcal{N}_{E/K}$ is the conductor of E, and c_1 and c_2 depend on K in an explicit way.
- Is ρ bounded for fixed K? Divergent opinions, already for $K = \mathbb{Q}$!
  * Park–Poonen–Voight–Wood ('19): heuristic which suggests that $\rho \leq 21$ except for at most finitely many $E/\mathbb{Q}$.
  * Elkies (2006): $E/\mathbb{Q}$ with $\rho \geq 28$ (= under GRH).

Genus 1: infinite part

✎ In general, no effective method to calculate ρ.

Conjecture (Birch and Swinnerton–Dyer)

$\rho = \mathrm{ord}_{s=1} L(E, s)$.

Coates–Wiles, Gross–Zagier, Kolyvagin, Rubin, Breuil–Conrad–Diamond–Taylor, Darmon, Bhargava–Shankar, Nevokar, Dokchitser–Dokchitser, Skinner–Urban...

✎ Upper bound:

- ➢ Ooe–Top '89: $\rho \leq c_1 \log |N_{K/\mathbb{Q}} \mathcal{N}_{E/K}| + c_2$, where $\mathcal{N}_{E/K}$ is the conductor of E, and c_1 and c_2 depend on K in an explicit way.
- ➢ Is ρ bounded for fixed K? Divergent opinions, already for $K = \mathbb{Q}$!
  * Park–Poonen–Voight–Wood ('19): heuristic which suggests that $\rho \leq 21$ except for at most finitely many $E/\mathbb{Q}$.
  * Elkies (2006): $E/\mathbb{Q}$ with $\rho \geq 28$ ($=$ under GRH).

Genus 1: infinite part

✎ In general, no effective method to calculate ρ.

Conjecture (Birch and Swinnerton–Dyer)

$\rho = \mathrm{ord}_{s=1} L(E, s)$.

Coates–Wiles, Gross–Zagier, Kolyvagin, Rubin, Breuil–Conrad–Diamond–Taylor, Darmon, Bhargava–Shankar, Nevokar, Dokchitser–Dokchitser, Skinner–Urban...

✎ Upper bound:

- Ooe–Top '89: $\rho \leq c_1 \log |N_{K/\mathbb{Q}} \mathcal{N}_{E/K}| + c_2$, where $\mathcal{N}_{E/K}$ is the conductor of E, and c_1 and c_2 depend on K in an explicit way.
- Is ρ bounded for fixed K? Divergent opinions, already for $K = \mathbb{Q}$!
  * Park–Poonen–Voight–Wood ('19): heuristic which suggests that $\rho \leq 21$ except for at most finitely many $E/\mathbb{Q}$.
  * Elkies (2006): $E/\mathbb{Q}$ with $\rho \geq 28$ ($=$ under GRH).

Genus 1: finite part

Theorem (Mazur '77 for $K = \mathbb{Q}$, Merel '96)

$\#E(K)_{\mathrm{tor}}$ is uniformly bounded above in terms of $[K : \mathbb{Q}]$.

Mazur proved this result by establishing the following theorem:

Theorem (Mazur '77)

If $N = 11$ or $N \geq 13$, then the only $\mathbb{Q}$-points of the modular curve $X_1(N)$ are the rational cusps.

The genus of $X_1(N)$ is ≥ 2 if $N = 13$ or $N \geq 16$.

$\rightsquigarrow$ results of rational points on curves of genus ≥ 2.

Genus ≥ 2: Mordell Conjecture

Mordell made the following conjecture about 100 years ago (1922), known as the Mordell Conjecture. It became a theorem in 1983, proved by Faltings.

Theorem (Faltings '83; known as Mordell Conjecture)

If $g \geq 2$, then the set $C(K)$ is finite.

Feature of this theorem	When applied to Mazur's result on $X_1(N)$
➢ weak topological hypothesis, very strong arithmetic conclusion!	✎ $X_1(N)$ has only finitely many $\mathbb{Q}$-points if $N \geq 16$.
➢ not constructive yet.	✎ $X_1(N)(\mathbb{Q})$ cannot be determined by Faltings's Theorem.

Genus ≥ 2: Fermat's Last Theorem

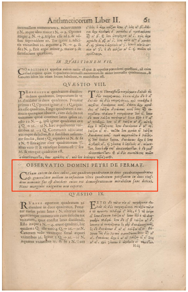
Fix $n \geq 4$ integer.

$$F_n : X^n + Y^n - 1 = 0.$$

Then $g(F_n) \geq 2$.

$$\Big\Downarrow \text{Faltings}$$

$\exists$ only finitely many $(x, y) \in \mathbb{Q}^2$ with $x^n + y^n = 1$.



For this example, more is expected.

Theorem (Wiles, Taylor–Wiles, '95; known as Fermat's Last Theorem)

If x and y are rational numbers such that $x^n + y^n = 1$, then $(x, y) = (0, \pm 1)$ or $(x, y) = (\pm 1, 0)$.

Of course if n is furthermore assumed to be odd, then -1 cannot be attained.

Genus ≥ 2

From now on, we always assume that $g \geq 2$.
The example of Fermat's Last Theorem suggests that it can be extremely hard to compute $C(\mathbb{Q})$ for an arbitrary C!
Instead, here is a more achievable but still fundamental question.

Question (Mordell, Weil, Manin, Mumford, Faltings, *etc.*)

Is there an "easy" upper bound for $\#C(K)$? How does $C(K)$ "distribute"?

Different grades of the question:

- Finiteness of $C(K)$
- Upper bound of $\#C(K)$
- Uniformity of bounds of $\#C(K)$
- Effective Mordell

Heights

Use height to measure the "size" of the rational and algebraic points.

- ✎ On $\mathbb{Q}$: $h(a/b) = \log\max\{|a|,|b|\}$, for $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$.
- ✎ On $\mathbb{P}^n(\mathbb{Q})$: $h([x_0 : \cdots : x_n]) = \log\max\{|x_0|, \ldots, |x_n|\}$, for $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$.
- ✎ Arbitrary number field K: For $[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ with each $x_j \in K$, $h([x_0 : \cdots : x_n]) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \Sigma_K} \log\max\{\|x_0\|_v, \ldots, \|x_n\|_v\}$.

⇝ (logarithmic) Weil height on $\mathbb{P}^n(\overline{\mathbb{Q}})$, and on any subvariety $X \subseteq \mathbb{P}^n$.

Two important properties →
↓

Northcott Property

For all B and $d \geq 1$,

$$\{\mathbf{x} \in \mathbb{P}^n(\overline{\mathbb{Q}}) : h(\mathbf{x}) \leq B, [\mathbb{Q}(\mathbf{x}) : \mathbb{Q}] \leq d\}$$

is finite.

Bounded from below

$h(\mathbf{x}) \geq 0$ *for all* $\mathbf{x} \in \mathbb{P}^n(\overline{\mathbb{Q}})$.

Heights

Use height to measure the "size" of the rational and algebraic points.

- ✎ On $\mathbb{Q}$: $h(a/b) = \log\max\{|a|, |b|\}$, for $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$.
- ✎ On $\mathbb{P}^n(\mathbb{Q})$: $h([x_0 : \cdots : x_n]) = \log\max\{|x_0|, \ldots, |x_n|\}$, for $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$.
- ✎ Arbitrary number field K: For $[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ with each $x_j \in K$, $h([x_0 : \cdots : x_n]) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \Sigma_K} \log\max\{\|x_0\|_v, \ldots, \|x_n\|_v\}$.

$\rightsquigarrow$ (logarithmic) Weil height on $\mathbb{P}^n(\overline{\mathbb{Q}})$, and on any subvariety $X \subseteq \mathbb{P}^n$.

Two important properties $\rightarrow$ $\downarrow$

Bounded from below

$h(\mathbf{x}) \geq 0$ *for all* $\mathbf{x} \in \mathbb{P}^n(\overline{\mathbb{Q}})$.

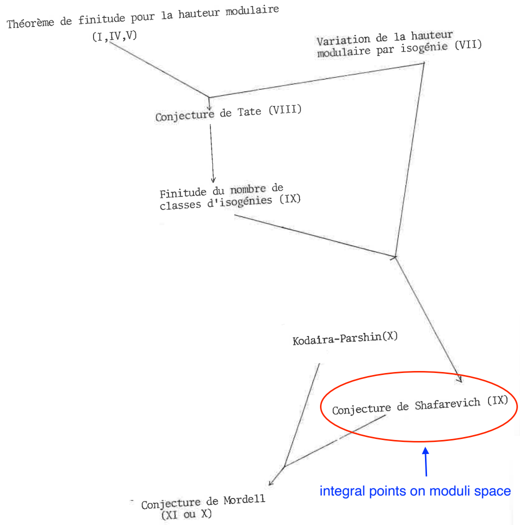
Northcott Property

For all B and $d \geq 1$,

$$\{\mathbf{x} \in \mathbb{P}^n(\overline{\mathbb{Q}}) : h(\mathbf{x}) \leq B, [\mathbb{Q}(\mathbf{x}) : \mathbb{Q}] \leq d\}$$

is finite.

Genus $\geq$ 2: Faltings's proof of the Mordell Conjecture



Extracted from « Séminaire sur les pinceaux arithmétiques, La conjecture de Mordell » (Astérisque 127), Lucien Szpiro.

- $\mathbb{A}_g$ = moduli space of pp abelian varieties

New approach to treat integral points on moduli spaces: Lawrence–Venkatesh.

Faltings height

- $A/\overline{\mathbb{Q}}$ = pp abelian variety.

Faltings defined an intrinsic number $h_{\mathrm{Fal}}(A)$ associated with A (cf. Astérisque 127, or Call–Silverman).

$\rightsquigarrow h_{\mathrm{Fal}} \colon \mathbb{A}_g(\overline{\mathbb{Q}}) \to \mathbb{R}$.

Why is it called a height?

Fix an embedding $\mathbb{A}_g \subseteq \mathbb{P}^N$ over $\overline{\mathbb{Q}}$. $\rightsquigarrow$ Weil height $h \colon \mathbb{A}_g(\overline{\mathbb{Q}}) \to \mathbb{R}$.

Theorem (Faltings, improved constants by Bost, David, Pazuki)

$|\frac{1}{2}h_{\mathrm{Fal}}(A) - h([A])| \leq c_g \log(h([A]) + 2)$.

Upshots:

- $h_{\mathrm{Fal}}(A)$ bounded from below solely in terms of g.
- Northcott property for h_{Fal}.

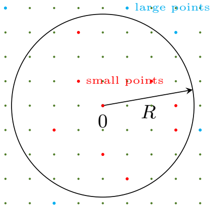
Genus ≥ 2: a new proof by Vojta

In early 90s, Vojta gave a second proof to Faltings's Theorem with Diophantine method.

- In this proof, one sees some descriptions of distribution of algebraic points on C. They lead to an upper bound on $\#C(K)$.
- The proof was simplified by Bombieri. And generalized by Faltings to some high dimensional cases.

Starting Point: Take $P_0 \in C(K)$, and see C as a curve in $J = \mathrm{Jac}(C)$ via the Abel–Jacobi embedding $C \to J$ based at P_0. Then $C(K) \subseteq J(K)$.

Vojta's proof of the Mordell Conjecture: Setup



Normalized height function $\hat{h}\colon J(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ vanishing precisely on $J(\overline{\mathbb{Q}})_{\mathrm{tor}}$.

$\rightsquigarrow$ $\hat{h}\colon J(K) \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}_{\geq 0}$ quadratic, positive definite.

$\rightsquigarrow$ Normed Euclidean space $(J(K) \otimes_{\mathbb{Z}} \mathbb{R}, |\cdot| := \hat{h}^{1/2})$, with $J(K)$ a lattice.

$\rightsquigarrow$ Inner product $\langle \cdot, \cdot \rangle$ on $J(K) \otimes_{\mathbb{Z}} \mathbb{R}$, and the angle of each two points in $J(K) \otimes_{\mathbb{Z}} \mathbb{R}$.

Vojta's proof of Mordell Conjecture: Mumford's work

A starting point is the following (consequence of) Mumford's Formula: For $P, Q \in C(\overline{\mathbb{Q}})$ with $P \neq Q$, we have

$$\frac{1}{g}\left(|P|^2 + |Q|^2 - 2g\langle P, Q\rangle\right) + O(|P| + |Q| + 1) \geq 0$$

As $g \geq 2$, the leading term is an indefinite quadratic form, which a priori could take any value. This gives a strong constraint on the pair (P, Q)!
$\rightsquigarrow$ Algebraic points are "sparse" in C!

Vojta's proof of Mordell Conjecture: Both inequalities

Theorem

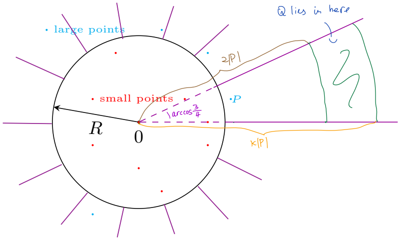
There exist $R = R(C)$ and $\kappa = \kappa(g)$ satisfying the following property. If two distinct points $P, Q \in C(\overline{\mathbb{Q}})$ satisfy $|Q| \geq |P| \geq R$ and

$$\langle P, Q\rangle \leq (3/4)|P||Q|,$$

then

- *(Mumford, '65)* $|Q| \geq 2|P|$;
- *(Vojta, '91)* $|Q| \leq \kappa|P|$.

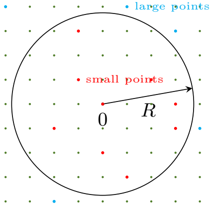
This finishes the proof of the Mordell Conjecture, with #large points$\leq (\log_2 \kappa + 1)7^{\mathrm{rk} J(K)}$.



If $P_1, \ldots, P_n$ are in the cone where P lies, then $\kappa|P| \geq |P_n| \geq 2|P_{n-1}| \geq \cdots \geq 2^n|P|$.
So in each cone there are $\leq \log_2 \kappa + 1$ large points!

$7^{\mathrm{rk} J(K)}$ such cones, according to the angle condition.

Genus ≥ 2: Classical bound



Theorem (Bombieri '91, de Diego '97, Alpoge 2018)

- *One can take* $R^2 = c_0(g)h_{\mathrm{Fal}}(J)$.
- $\#$*large points* $\leq c(g)1.872^{\mathrm{rk}_{\mathbb{Z}} J(K)}$. $\rightsquigarrow$ *A nice bound for #large points!*

For a bound of $\#C(K)$, we have:

Theorem (David–Philippon, Rémond 2000)

$$\#C(K) \leq c(g, [K : \mathbb{Q}], h_{\mathrm{Fal}}(J))^{1+\mathrm{rk}_{\mathbb{Z}} J(K)}.$$

Genus ≥ 2

Different grades of the question:

- Finiteness of $C(K)$ ✓
- Upper bound of $\#C(K)$ ✓
- Uniformity of bounds of $\#C(K)$
- Effective Mordell

Sparsity of algebraic points:

"sparsity" of large points

- Mumford's Inequality '65
- Vojta's Inequality '91
- ?✎
- ???

And about the distribution / sparsity of points:

✎ Are there other descriptions of the "sparsity" of algebraic points on C? Or at least can we say something about "small" points?

Genus ≥ 2: Towards uniform bounds on $\#C(K)$

The cardinality $\#C(K)$ must depend on g.

Example

The hyperelliptic curve defined by

$$y^2 = x(x-1)\cdots(x-2024)$$

has genus 1012 *and has at least* 2026 *different rational points.*

The cardinality $\#C(K)$ must depend on $[K : \mathbb{Q}]$.

Example

The hyperelliptic curve

$$y^2 = x^6 - 1$$

has points $(1,0)$, $(2, \pm\sqrt{63})$, $(3, \pm\sqrt{728})$, *etc.*

Genus ≥ 2: Towards uniform bounds on $\#C(K)$

Here is a very ambitious bound.

Question

Is it possible to find a number $B(g, [K : \mathbb{Q}]) > 0$ *such that*

$$\#C(K) \leq B?$$

This question has an affirmative answer if one assumes a widely open conjecture of Bombieri–Lang on rational points on varieties of general type (Caporaso–Harris–Mazur, Pacelli, '97).

- ✎ Two divergent opinions towards this conditional result: either this ambitious bound is true, or one could use this to disprove this conjecture of Bombieri–Lang.

Genus ≥ 2: Mazur's Conjecture B

Theorem (Dimitrov-G'-Habegger, 2021; Mazur's Conjecture B ('86, 2000))

If $g \geq 2$, then

$$\#C(K) \leq c(g, [K:\mathbb{Q}])^{1+\mathrm{rk}_{\mathbb{Z}} J(K)}$$

where J is the Jacobian of C. Moreover, $c(g,[K:\mathbb{Q}])$ grows at most polynomially in $[K:\mathbb{Q}]$.

- Compared to the classical result, the *height of C* is no longer involved.
- We showed that c does not depend on $[K:\mathbb{Q}]$ assuming the relative Bogomolov conjecture. Kühne (2021) removed this dependence on $[K:\mathbb{Q}]$ unconditionally.
- Previous results:
  - When $J \subseteq E^n$ and some particular family of curves (David, Philippon, Nakamaye 2007). Average number of $\#C(\mathbb{Q})$ when $g=2$ (Alpoge 2018).
  - When $\mathrm{rk} J(K) \leq g-3$ (hyperelliptic by Stoll 2015, then Katz–Rabinoff–Zureick-Brown 2016).

✎ If you believe that the Mordell–Weil rank $\mathrm{rk}_{\mathbb{Z}} J(K)$ is bounded for fixed g and K, then the ambitious bound on last page is true. If you do not believe the ambitious bound on the last page, then the Mordell–Weil rank is unbounded.

Example of a 1-parameter family

Example (DGH 2019)

Let $s \geq 5$ be an integer and let C_s be the genus 2 hyperelliptic curve defined by

$$C_s : y^2 = x(x-1)(x-2)(x-3)(x-4)(x-s).$$

Then

$$\begin{aligned}\mathrm{rk}(J_s)(\mathbb{Q}) &\leq 2g\#\{p : \ p = 2 \text{ or } C_s \text{ has bad reduction at } p\} \\ &\leq 2g\#\{p : p | 2 \cdot 3 \cdot 5 \cdot s(s-1)(s-2)(s-3)(s-4)\} \\ &\ll_g \frac{\log s}{\log\log s}.\end{aligned}$$

This yields, for any $\epsilon > 0$,

$$\#C_s(\mathbb{Q}) \ll_\epsilon s^\epsilon.$$

Genus ≥ 2: New Gap Principle

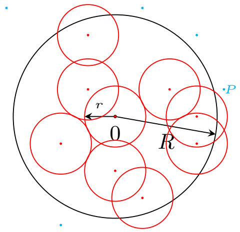
Our new contribution is a New Gap Principle.

Theorem (New Gap Principle, Dimitrov–G'–Habegger + Kühne, 2021)

Assume $g \geq 2$. Each $P \in C(\overline{\mathbb{Q}})$ satisfies

$$\#\{Q \in C(\overline{\mathbb{Q}}) : \hat{h}_L(Q-P) \leq c_1 h_{\mathrm{Fal}}(J)\} \leq c_2$$

for some positive constants c_1 and c_2 depending only on g.



$R^2 = c_0(g) h_{\mathrm{Fal}}(C)$
$r^2 = c_1(g) h_{\mathrm{Fal}}(C)$
small balls to cover all small points $\leq (R/r)^{\mathrm{rk} J(K)}$
of points in each ball $\leq c_2$

- The Bogomolov Conjecture, proved by Ullmo and S.Zhang ('98), gives this result with c_1 and c_2 depending on C (but don't know how).
- The New Gap Principle is another phenomenon of the "sparsity" of algebraic points in C of genus ≥ 2. It says that algebraic points in $C(\overline{\mathbb{Q}})$ are in general far from each other in a quantitative way.
- It implies that #small rational points $\leq c'(g)^{1+\mathrm{rk} J(K)}$ by a simple packing argument.

Genus ≥ 2

Different grades of the question:

- Finiteness of $C(K)$ ✓
- Upper bound of $\#C(K)$ ✓
- Uniformity of bounds of $\#C(K)$
  ✓"subject" to the Mordell–Weil rank
- Effective Mordell

Sparsity of algebraic points:

- Mumford's Inequality -'65
- Vojta's Inequality -'91
- New Gap Principle -2021 (Dimitrov–G'–Habegger + Kühne)
- ???✎

And:

✎ Mumford's and Vojta's Inequalities to describe that large algebraic points are "sparse" in C.

✎ New Gap Principle gives another description on how all algebraic points are "sparse" in C.

✎ Effective Mordell is a conjectural statement which describes where to find the rational points ("no large rational points").

Genus ≥ 2

Different grades of the question:

- Finiteness of $C(K)$ ✓
- Upper bound of $\#C(K)$ ✓
- Uniformity of bounds of $\#C(K)$ ✓"subject" to the Mordell–Weil rank
- Effective Mordell

Sparsity of algebraic points:

- Mumford's Inequality -'65
- Vojta's Inequality -'91
- New Gap Principle -2021 (Dimitrov–G'–Habegger + Kühne)
- ???✎

And:

✎ Mumford's and Vojta's Inequalities to describe that large algebraic points are "sparse" in C.

✎ New Gap Principle gives another description on how all algebraic points are "sparse" in C.

✎ Effective Mordell is a conjectural statement which describes where to find the rational points ("no large rational points").

Genus ≥ 2: Effective Mordell

Conjecture (Effective Mordell, made by Szpiro)

There exists an effectively computable $c = c(g, [K:\mathbb{Q}], \mathrm{disc}(K/\mathbb{Q})) > 0$ *such that* $\hat{h}(P) \leq c h_{\mathrm{Fal}}(J)$ *for all* C/K *and* $P \in C(K)$*.*

- Effective Mordell tells us where to find all the rational points on C ("no large rational points")!
- Little is known about Effective Mordell.
- Checcoli, Veneziano, and Viada proved results in this direction when $C \subsetneq E^n$ for some elliptic curve E with $\mathrm{rk}E(K) < n$ (modification if E has CM) and C is *transverse*, following the method of Manin–Demjanenko.

Genus ≥ 2: Chabauty–Coleman–Kim method

✎ Another approach to compute $C(K)$ is the Chabauty–Coleman–Kim method, by obtaining sharp bounds on $\#C(K)$ when $\mathrm{rk}J(K)$ is small. Currently:

- ➢ Chabauty–Coleman: $K = \mathbb{Q}$, $\mathrm{rk}J(\mathbb{Q}) < g$.

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r, hook] \arrow[d, hook] & J(\mathbb{Q}) \arrow[d, hook] \\ C(\mathbb{Q}_p) \arrow[r, hook] & J(\mathbb{Q}_p) \end{tikzcd}$$

$\dim \overline{J(\mathbb{Q})} \leq \mathrm{rk}J(\mathbb{Q}) < g \Rightarrow C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ finite.

- ➢ Quadratic Chabauty: $\mathrm{rk}J(\mathbb{Q}) = g$, in various publications of Jennifer Balakrishnan in collaboration with Besser, Müller, Dogra *et al*.

A geometric point of view by Edixhoven–Lido:

$$\begin{tikzcd} & (1,f)^* P^x \arrow[r] \arrow[d] & P^x \arrow[d] \\ C \arrow[ur, dashed] \arrow[r] & J \arrow[r, "{(1,f)}"] & J \times J^\vee \end{tikzcd}$$

the lifting exists $\Leftrightarrow \deg(1,f)^* P^x = 0$.

$\Rightarrow C \hookrightarrow T$ with $T \to J$ a $\mathbb{G}_\mathrm{m}^{\rho-1}$-torsor, with $\rho = \mathrm{rkNS}(J)$.

Hence need $\mathrm{rk}J(\mathbb{Q}) < g + \rho - 1$.

Proof of DGH: a tale of two heights

Theorem (New Gap Principle, Dimitrov–G'–Habegger + Kühne, 2021)

Assume $g \geq 2$. Each $P \in C(\overline{\mathbb{Q}})$ satisfies

$$\#\{Q \in C(\overline{\mathbb{Q}}) : \hat{h}_L(Q-P) \leq c_1 h_{\mathrm{Fal}}(J)\} \leq c_2$$

for some positive constants c_1 and c_2 depending only on g.

- $Q - P \in C - C \subseteq J$
- We are comparing:
  - $\hat{h}_L|_{C-C}$ height on J, and
  - $h_{\mathrm{Fal}}(J)$ height of J

Put all curves "together":

$$\begin{array}{cl} \mathcal{C}_g & \text{universal curve} \\ \downarrow & \\ \mathbb{M}_g & \text{moduli space of curves of genus } g \text{ with level-4-structure} \end{array}$$

Proof of DGH: a tale of two heights

Theorem (New Gap Principle, Dimitrov–G'–Habegger + Kühne, 2021)

Assume $g \geq 2$. Each $P \in C(\overline{\mathbb{Q}})$ satisfies

$$\#\{Q \in C(\overline{\mathbb{Q}}) : \hat{h}_L(Q-P) \leq c_1 h_{\mathrm{Fal}}(J)\} \leq c_2$$

for some positive constants c_1 and c_2 depending only on g.

- $Q - P \in C - C \subseteq J$
- We are comparing:
  - $\hat{h}_L|_{C-C}$ height on J, and
  - $h_{\mathrm{Fal}}(J)$ height of J

$$\begin{tikzcd} \mathcal{C}_g \times_{\mathbb{M}_g} \mathcal{C}_g \arrow[r, "\mathcal{D}_1"] \arrow[dr] & \mathrm{Jac}(\mathcal{C}_g/\mathbb{M}_g) \arrow[d, "\pi"] \\ & \mathbb{M}_g \end{tikzcd}$$

$$\begin{tikzcd} X \subseteq \mathcal{A}_g \arrow[d, "\pi"] \\ \mathbb{A}_g \end{tikzcd}$$

- $\hat{h}$ fiberwise, and
- $h_{\mathrm{Fal}}(J)$ height on the base $\mathbb{M}_g$.
- Want to find the correct condition for X such that $\hat{h} \geq c h_{\mathrm{Fal}}$ when restricted on X for some constant c.

Proof of DGH: a tale of two heights

Theorem (GH 2019, DGH 2021)

The followings are equivalent:

(i) *There exists a Zariski open dense subset U of X, and a constant $c = c(X) > 0$ such that for all $x \in U(\overline{\mathbb{Q}})$,*

$$\hat{h}(x) \geq c h_{\mathrm{Fal}}(A_x) - c.$$

(ii) *X satisfies a linear algebra property, called non-degenerate.*

In the terminology of Yuan–Zhang 2021, (ii) is equivalent to: the tautological adelic line bundle $\widetilde{\mathcal{L}}_g$ is big when restricted to X (DGH + YZ).

An immediate observation by definition: If $\dim X > g$, then X is degenerate! $\rightsquigarrow$ naive degenerate.

For example, $\mathcal{C}_g - \mathcal{C}_g = \mathcal{D}_1(\mathcal{C}_g \times_{\mathbb{M}_g} \mathcal{C}_g)$ is degenerate!

Proof of DGH: a tool (degeneracy loci) and bigness

✎ (G' 2020) For each $t \in \mathbb{Z}$, one can define the t-th degeneracy locus $X^{\deg}(t)$ of X. ⇝ Important tool to study these uniformity results.

Theorem (G' 2020, example of application of $X^{\deg}(0)$)

TFAE:

- *X is degenerate, i.e. $\widetilde{\mathcal{L}}_g|_X$ is NOT big.*
- *$\exists$ abelian subscheme $\mathcal{B}$ of $\mathcal{A} \to S$ such that "a generic fiber of $\iota \circ p|_X$ is naive degenerate", i.e.* $\dim X - \dim(\iota \circ p)(X) > \dim \mathcal{B} - \dim S$.

$$\begin{tikzcd} \mathcal{A} \arrow[r, "p"] \arrow[d] & \mathcal{A}/\mathcal{B} \arrow[r, "\iota"] \arrow[d] \arrow[dr, phantom, "\lrcorner"] & \mathcal{A}_{g'} \arrow[d] \\ S \arrow[r, "="] & S \arrow[r] & \mathbb{A}_{g'}. \end{tikzcd}$$

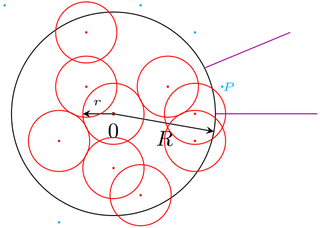
✎ Applications of this theorem and beyond:

- $X := \mathcal{D}_M(\mathcal{C}_g^{[M+1]})$ is non-degenerate if $M \geq 3g-2$ (for DGH and K).
- the full Uniform Mordell–Lang Conjecture (G'–Ge–Kühne 2021).
- $X^{\deg}(1)$ for the Relative Manin–Mumford Conjecture (G'–Habegger 2023).

Genus ≥ 2: Some further questions related to the rather uniform bound of DGH+K

$\#C(K) \leq c_2(g)c(g)^{\mathrm{rk}J(K)}$

- How does $c_2(g)$ grow as $g \to \infty$?
  - $c_2(g) \to \infty$ $(y^2 = x(x-1)\cdots(x-2024))$.
  - Over function fields: $\sim g^2$ by Looper–Silverman–Wilms 2022.
  - Over number fields: no explicit formula.
- What if we confine ourselves to rational torsion points $\mathrm{TP}(C, P) := (C - P)(K) \cap J_{\mathrm{tor}}$?
  - Baker–Poonen 2001: $\#\mathrm{TP}(C, P) \leq 2$ for all but $B = B(C)$ points $P \in C(K)$.
  - Is it possible to make $B(C)$ uniform in g up to replacing 2 by 6?

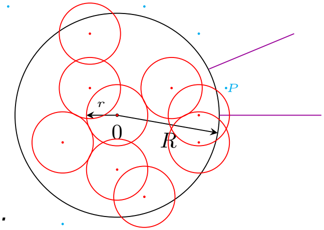


$$R^2 = c_0(g)h_{\mathrm{Fal}}(C)$$
$$r^2 = c_1(g)h_{\mathrm{Fal}}(C)$$
$$\#\text{ small balls to cover all small points} \leq (R/r)^{\mathrm{rk}J(K)}$$
$$\#\text{ of points in each ball} \leq c_2$$

Genus ≥ 2: Some further questions related to the rather uniform bound of DGH+K

$\#C(K) \leq c_2(g)c(g)^{\mathrm{rk}J(K)}$

- ✎ Is it true that $c(g) \to 1$ when $g \to \infty$, or at least give an absolute upper bound of $c(g)$?
  - ➢ In view of Mumford's Formula
    $$\frac{1}{g}\left(|P|^2 + |Q|^2 - 2g\langle P, Q\rangle\right) + O(|P| + |Q| + 1) \geq 0.$$
  - ➢ The angle condition in both inequalities can be improved.
  - ➢ A more precise version of Mumford's formula.



$R^2 = c_0(g)h_{\mathrm{Fal}}(C)$
$r^2 = c_1(g)h_{\mathrm{Fal}}(C)$
$\#$ small balls to cover all small points $\leq (R/r)^{\mathrm{rk}J(K)}$
$\#$ of points in each ball $\leq c_2$

- ✎ Arithmetic Statistics: Average number of rational points.
  - ➢ Alpoge ('18): $K = \mathbb{Q}$ and $g = 2$, before the result of DGH.
  - ➢ Bhargava–Gross ('13): $K = \mathbb{Q}$, the average of $2^{\mathrm{rk}J(\mathbb{Q})}$ is a finite number for hyperelliptic curves having a rational Weierstrass point.

Genus 1: integral points

Another interesting subject is the integral points on elliptic curves.
For simplicity we only discuss $\mathbb{Q}$ and $\mathbb{Z}$.
Every elliptic curve $E/\mathbb{Q}$ defined over $\mathbb{Q}$ has a Weierstrass model of the following form:

$$\boxed{E: \ Y^2 = X^3 + aX + b \text{ with } a, b \in \mathbb{Z} \text{ and } 4a^3 + 27b^2 \neq 0}$$

Use $E(\mathbb{Z})$ to denote the integer solutions to the equation, *i.e.* $(x, y) \in \mathbb{Z}^2$ such that $y^2 = x^3 + ax + b$.

- Finiteness:

  Theorem (Siegel '29)

  $E(\mathbb{Z})$ is a finite set.

- (Uniform) Bound;
- Effectiveness.

Genus 1: integral points

- Finiteness; ✓
- (Uniform) Bound: Assume the model is minimal, *i.e.* $|4a^3 + 27b^2|$ is minimal for $a, b \in \mathbb{Z}$.

Conjecture (Lang)

$\#E(\mathbb{Z}) \leq c^{1+\mathrm{rk}E(\mathbb{Q})}$ *for some absolute constant c.*

Silverman ('87) proved $\#E(\mathbb{Z}) \leq c^{1+\mathrm{rk}E(\mathbb{Q})+\#\{\text{bad reduction places}\}}$.

Theorem (Hindry–Silverman '88)

$\#E(\mathbb{Z}) \leq c^{(1+\mathrm{rk}E(\mathbb{Q}))\sigma}$, *where σ is the Szpiro quotient.*
In particular, Lang's conjecture above holds true if the abc conjecture holds true.

Unconditional results in Arithmetic Statistics (average number of integral points on elliptic curves in certain families) by Alpoge, Chan, Ho, *etc.*

- Effectiveness: Little is known.

Genus 1: Growth of integral and rational points

Conjecture

For any $\varepsilon > 0$, there exists $c = c(\varepsilon) > 0$ such that

- ✎ *(Integral Points)* $\# E(\mathbb{Z}) \leq c \cdot \exp(\varepsilon h_{\mathrm{Fal}}(E))$.
- ✎ *(Rational Points)* $\# \{ P \in E(\mathbb{Q}) : \hat{h}(P) \leq B \} \leq c \exp(\varepsilon \cdot \max\{ h_{\mathrm{Fal}}(E), B \})$.

➢ Bombieri–Zannier (2004) and Naccarato (2021) proved the “Rational Points Part” of this conjecture if E has non-trivial rational 2-torsion points. In their proof it is important to work with the number field $\mathbb{Q}$, and the proof uses Hindry–Silverman ’88 (height bound on non-torsion rational points).

Lang–Silverman and UBC

Conjecture (Lang–Silverman)

Let $g \geq 1$ be an integer. For all number field K, there exist constants $c_1 = c_1(g, K)$, $c_2 = c_2(g, K)$, $c_3 = c_3(g, K)$ with the following property. For each abelian variety A of dimension g defined over K and each $P \in A(K)$, we have

(i) *Either P is contained in a proper abelian subvariety B of A with $\deg B \leq c_2 \deg A$ and $\mathrm{ord}(P)$ is $\leq c_3$ modulo B;*

(ii) *Or $\mathrm{End}(A) \cdot P$ is Zariski dense in A and*

$$\hat{h}(P) \geq c_1 \max\{h_{\mathrm{Fal}}(A), 1\}.$$

An immediate corollary of the Lang–Silverman Conjecture is the following widely open Uniform Boundedness Conjecture.

Conjecture (Uniform Boundedness Conjecture)

For each abelian variety A of dimension $g \geq 1$ defined over $\mathbb{Q}$, we have

$$\#A(\mathbb{Q})_{\mathrm{tor}} \leq B(g).$$

Thanks!