Distribution of points in varieties : various aspects and their interaction

Ziyang Gao

CNRS, IMJ–PRG

Paris
28/06/2021

Part 0. 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 the equation $f(X, Y) = 0$?
(Diophantine problem)

- $f(X, Y) = X^2 + Y^2 - 1$. We wish to find rational numbers (x, y) such that $x^2 + y^2 = 1$. Pythagorian triples $(3/5, 4/5)$, $(5/13, 12/13)$, *etc*.
- $f(X, Y) = Y^3 - X^3 - 2$. We wish to find rational numbers (x, y) such that $y^3 = x^3 + 2$. There are solutions like $(-1, \pm 1)$, $(34/8, \pm 71/8)$, $(2667/9261, 13175/9261)$, *etc*.
- $f(X, Y) = X^3 + Y^3 - 1$. We wish to find rational numbers (x, y) such that $x^3 + y^3 = 1$. The only such solutions are $(1, 0)$ and $(0, 1)$.

Part 0. Motivation

The last example from the previous slide, $x^3 + y^3 = 1$, is a particular case of the so-called *Fermat's Last Theorem*.

Theorem (Wiles, Taylor–Wiles, 1995)

Let $n \geq 3$ be an integer. 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.

This suggests that it can be extremely hard to find all $\mathbb{Q}$-solutions to an arbitrary polynomial $f(X, Y) = 0$!

Part 0. Motivation

Instead, here is a more achievable but still fundamental question.

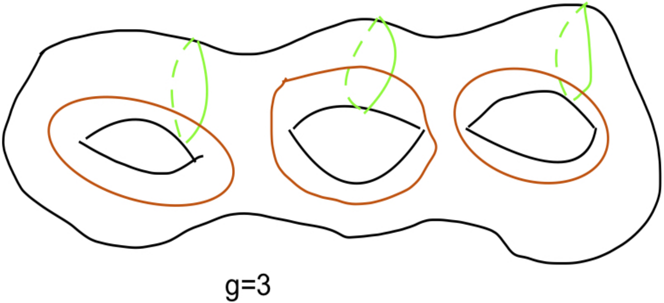
Question (Mordell, Weil, Manin, Mumford, Faltings, *etc.*)

Is there an "easy" upper bound for the number of the $\mathbb{Q}$-solutions?
How do these $\mathbb{Q}$-solutions "distribute"?

Modern Language: the $\mathbb{Q}$-solutions become rational points on algebraic varieties.

Part 0. Motivation

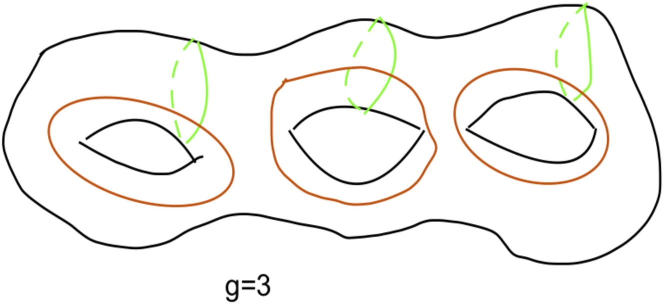
More precisely, the modern treatment is as follows.
The complex solutions to $f(X, Y) = 0$ define an (affine) curve in $\mathbb{C}^2$, and all curves in $\mathbb{C}^2$ defined over $\mathbb{Q}$ arise in this way.



Thus the question becomes: how many $\mathbb{Q}$-points are there on a curve in $\mathbb{C}^2$ defined over $\mathbb{Q}$? How do these $\mathbb{Q}$-points distribute?

Part 0. Classification of curves (topological invariant)

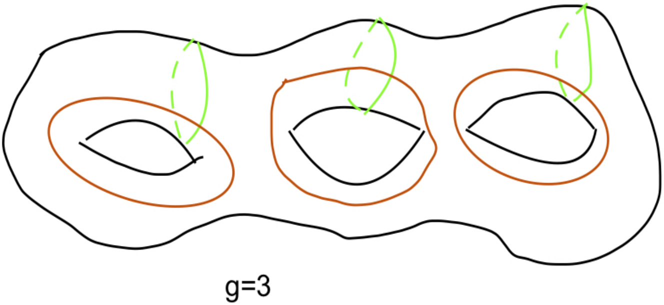
Next, associated to each projective curve, there is an intrinsic integer $g \geq 0$, called the genus.



$g = \frac{(\deg F - 1)(\deg F - 2)}{2} - \delta$ if the curve has only nodes as singular points; in general can be reduced to this case by Cremona transformations.

Part 0. Faltings's Theorem

In what follows, $g \geq 0$ and $d \geq 1$ will be two integers, and K *is a number field with* $[K : \mathbb{Q}] = d$. Let $C =$ irreducible smooth projective curve of genus g defined over K.



In 1983, Faltings proved the famous Mordell Conjecture (since 1922).

Theorem (Faltings 1983)

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

C is the set of zeros of some polynomials;
C is defined over K $\leftrightsquigarrow$ these polynomials have coefficients in K;
$C(K)$:= the set of K-solutions.

However Faltings's 1983 proof does not give a good upper bound on $\#C(K)$.

Part 0. In search of an upper bound on $\#C(K)$

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

Example

The hyperelliptic curve defined by

$$y^2 = x(x-1)\cdots(x-2021)$$

has at least 2022 *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.*

Part 0. In search of an upper bound 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 Lang's conjecture (Caporaso–Harris–Mazur, Pacelli).

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

Part 0. Classical result on $\#C(K)$

In early 90s, Vojta gave a second proof to Faltings's Theorem. The proof was simplified and generalized by Faltings, and further simplified by Bombieri. This new proof (BFV) gives an upper bound, which was later on made explicit by de Diego, David–Philippon, and Rémond.

Theorem (Vojta, Faltings, Bombieri, de Diego, David–Philippon, Rémond)

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

where $J =$Jacobian of C, and $h_{\mathrm{Fal}}(J) = \max\{$Faltings height of $J, 1\}$.

Roughly speaking, the number $h_{\mathrm{Fal}}(J)$ measures the "complexity" of the coefficients of the equations defining the curve C.

Table of contents

Part 1. Bound on $\#C(K)$

Theorem (Dimitrov-G'-Habegger, Ann. Math. 2021)

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 J. Moreover, $c(g, [K:\mathbb{Q}])$ grows at most polynomially in $[K:\mathbb{Q}]$.

- This proves a conjecture of Mazur (1986, 2000).
- Compared to the classical result, the *height of J* is no longer involved in the bound.
- Heuristic for $\mathrm{rk} J(K)$ by Poonen.
- We showed that the dependence of c on $[K:\mathbb{Q}]$ can be removed assuming the Relative Bogomolov Conjecture. More recently, this is achieved unconditionally by Kühne.

Part 1. Previously known results on this bound

- By Diophantine method, based on BFV,
  - David–Philippon 2007: when $J \subset E^n$.
  - David–Nakamaye–Philippon 2007: for some particular families of curves.
  - Alpoge 2018: average number of $\#C(K)$ when $g = 2$.
- By the Chabauty–Coleman method,
  - Stoll 2015: hyperelliptic curves when $\mathrm{rk} J(K) \leq g - 3$.
  - Katz–Rabinoff–Zureick-Brown 2016: when $\mathrm{rk} J(K) \leq g - 3$.

Part 1. Example of a 1-parameter family

Example (DGH 2019, IMRN)

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 $\epsilon > 0$,

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

Part 1. Uniform Mordell–Lang for curves

The following theorem is a question posed by Mazur 1986.

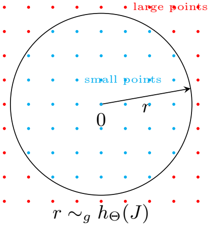
Theorem (Dimitrov-G'-Habegger, Ann. Math. 2021)

Let $P_0 \in C(\overline{\mathbb{Q}})$ and $J =$Jacobian of C. Let $C - P_0$ be the image of the Abel–Jacobi embedding of C in J based at P_0. Let Γ be a finite rank subgroup of $J(\overline{\mathbb{Q}})$. If $h_{\mathrm{Fal}}(J) \geq \delta(g)$, then

$$\#(C(\overline{\mathbb{Q}}) - P_0) \cap \Gamma \leq c(g)^{1+\mathrm{rk}\Gamma}.$$

- Upshot: $\#(C(\overline{\mathbb{Q}}) - P_0) \cap \Gamma \leq c(g, [K : \mathbb{Q}])^{1+\mathrm{rk}\Gamma}$ if C is defined over a number field K and $P_0 \in C(K)$.
- Kühne proved the this result for curves with $h_{\mathrm{Fal}}(J) < \delta(g)$.
- Uniform Manin–Mumford: $\Gamma = J(\overline{\mathbb{Q}})_{\mathrm{tor}}$. In this case, Katz–Rabinoff–Zureick-Brown 2016: assuming some good reduction behavior. DeMarco–Krieger–Ye 2018: $g = 2$ bi-elliptic.

Part 1. Review of the BFV method



On $J(\overline{\mathbb{Q}})$, there is a function $\hat{h}_L\colon J(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ vanishing precisely on $J(\overline{\mathbb{Q}})_{\mathrm{tor}}$.

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

$\rightsquigarrow$ "Normed Euclidean space" $(J(K)\otimes_{\mathbb{Z}}\mathbb{R}, \hat{h}_L)$, and $J(K)$ becomes a lattice in it.

Theorem (Bombieri, de Diego, Alpoge)

$\#$large points $\leq c(g)1.872^{\mathrm{rk}J(K)}$.

Part 1. A New Gap Principle

Our new contribution is the following New Gap Principle.

Theorem (Dimitrov–G'–Habegger 2021, uses G' 2020 Compositio Math.)

Set $m = 3g - 2$. Then if $P, P_1, \ldots, P_m$ are points of $C(\overline{\mathbb{Q}})$ in general position, then

$$\hat{h}_L(P_1 - P) + \cdots + \hat{h}_L(P_m - P) \geq c h_{\mathrm{Fal}}(J) - c',$$

where $c > 0$ and c' are constants which depend only on g.

As an upshot, we have:

Theorem (New Gap Principle for large curves)

There exists a constant $\delta = \delta(g) > 0$ with the following property. If $h_{\mathrm{Fal}}(J) > \delta$, then 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 constants c_1 and c_2 depending only on g.

Part 1. A New Gap Principle

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

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 constants $c_1 > 0$ and $c_2 > 0$ depending only on g.

- This theorem says (roughly) that algebraic points in $C(\overline{\mathbb{Q}})$ are in general far from each other in a quantitative way. In particular, this holds true for rational points in C. $\rightsquigarrow$ Distribution of algebraic points in C.
- The proof of this New Gap Principle uses deep results on functional transcendence (the mixed Ax–Schanuel theorem) (G', Compositio Math. 2020) and is highly related to unlikely intersection theory (see G', Compositio Math. 2020).

Part 1. Setup for the proof

$$\begin{tikzcd} \mathfrak{C}_g \arrow[d] \\ \mathbb{M}_g \end{tikzcd}$$

$\mathfrak{C}_g$: universal curve

$\mathbb{M}_g$: moduli space of curves of genus g with level-3-structure

We are interested $Q - P$, for $P, Q \in C(\overline{\mathbb{Q}})$, viewed as a point in J. This can be realized in families.

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

$(P, Q) \mapsto Q - P$ fiberwise

Part 1. Setup for the proof

On step further, one can put everything in the universal abelian variety $\pi\colon \mathfrak{A}_g \to \mathbb{A}_g$.

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

where τ is given by the Torelli morphism. Thus one can see the image of $\mathcal{D}_1$ as a subvariety of $\mathfrak{A}_g$. Hence we are required to study certain subvarieties of $\mathfrak{A}_g$.

The proof uses Betti map/form and Betti rank (Corvaja, Masser, Zannier, Bertrand, André; Mok). A key point is to prove that $X := \mathcal{D}_M(\mathfrak{C}_g^{M+1})$ is non-degenerate (as introduced by Habegger 2013), *i.e.* X has Betti rank $2\dim X$. This is done in G' 2020 Compositio Math.

- Part 1. Bound on $\#C(K)$ and distribution of algebraic points in curves.
- Part 2. Small points in abelian varieties.
- Part 3. Special points in moduli spaces, especially in mixed Shimura varieties.
- Part 4. Interactions: functional transcendence and unlikely intersections.

Part 2. Small points on abelian varieties

In Part 1, we have seen a height bound, if $h_{\mathrm{Fal}}(J) > \delta(g)$ for some fixed $\delta(g)$,

$$\hat{h}_L(P_1 - P) + \cdots + \hat{h}_L(P_m - P) \geq c h_{\mathrm{Fal}}(J) - c'$$

for $(P, P_1, \ldots, P_m) \in C(\overline{\mathbb{Q}})$ in general position.

Another way to understand this height bound is as follows. Consider the following morphism

$$D_m \colon C^{m+1} \to J^m, \quad (P_0, P_1, \ldots, P_m) \mapsto (P_1 - P_0, \ldots, P_m - P_0).$$

Then the point $(P_1 - P, P_2 - P, \ldots, P_m - P)$ is precisely $D_m(P, P_1, \ldots, P_m)$.

In other words, the height bound can be translated to: If $h_{\mathrm{Fal}}(J) > \delta(g)$, then $\hat{h}_L(x) \geq c h_{\mathrm{Fal}}(J) - c'$ for a generic point $x \in X(\overline{\mathbb{Q}})$, where $X = D_m(C^{m+1})$.

Part 2. Small points on abelian varieties

This is a (quantative) refinement of the following theorem of Ullmo and S. Zhang, which is known as the *Bogomolov conjecture* over number fields.

Theorem (Ullmo, S. Zhang 1998)

Let A be an abelian variety and X be a subvariety, both defined over $\overline{\mathbb{Q}}$. Let L be a symmetric ample line bundle on A. Then there exists a number $\epsilon = \epsilon(A, L, X) > 0$ such that

$$\hat{h}_L(x) \geq \epsilon$$

for a generic $x \in X(\overline{\mathbb{Q}})$, unless X is a torsion coset.

However, it was not shown how ϵ depends on A, L, X.

Part 2. Small points on abelian varieties

However, the analogue over function fields, known as the Geometric Bogomlov Conjecture, remained open in its full generality, both over characteristic 0 and $p > 0$.
With Serge Cantat, Philipp Habegger and Junyi Xie, we proved this conjecture in its full generality over characteristic 0.

Theorem (Cantat–G'-Habegger–Xie, Duke Math. J. 2021)

Let K be a function field over characteristic 0. Let A be an abelian variety and X be a subvariety, both defined over K. Let L be a symmetric ample line bundle on A. Then there exists a number $\epsilon = \epsilon(A, L, X) > 0$ such that

$$\hat{h}_L(x) \geq \epsilon$$

for a generic $x \in X(\overline{\mathbb{Q}})$, unless X is a torsion coset translated by a subvariety from the trace of A.

Part 2. Small points on abelian varieties

- Classical proof by Arakelov geometry. Gubler 2006 proved GBC for A totally degenerate at some place. In a series of work, Yamaki reduced GBC to A traceless and has good reduction everywhere. As a consequence, he could prove GBC if X is a curve or has codimension 1.
- There is a serious obstacle for the classical approach: If A has good reduction everywhere, then we do not have a place which could possibly give a "good" metric with which we can work. This phenomenon does not show up in the number field case (because of the archimedean place, at which an abelian variety becomes a complex torus).
- Our approach is different. No Arakelov geometry is used. We use the Betti map / foliation (Corvaja, Masser, Zannier, Bertrand, André), and either the Pila–Wilkie counting theorem from o-minimality or arithmetic dynamics.
- Compared with the classical approach, although very different, there is one surprisingly common aspect. The Betti map / foliation in some way constructs a "*totally degenerate place*", over which we have a real torus.

- Part 1. Bound on $\#C(K)$ and distribution of algebraic points in curves.
- Part 2. Small points in abelian varieties.
- Part 3. Special points in moduli spaces, especially in mixed Shimura varieties.
- Part 4. Interactions: functional transcendence and unlikely intersections.

Part 3. Special points on moduli spaces

There is an analogue between abelian varieties and moduli spaces of mixed Hodge structures (mixed Shimura varieties). We also take the universal abelian variety $\mathfrak{A}_g \to \mathbb{A}_g$ as an illustrating example.

Abelian varieties	mixed Shimura varieties	$\mathfrak{A}_g \to \mathbb{A}_g$
torsion / small points	special points	torsion points on CM fibers
torsion cosets	Shimura subvarieties	"sub-"moduli spaces

The analogue of the Manin–Mumford conjecture or the Bogomolov conjecture becomes the André–Oort conjecture.

Part 3. Special points on moduli spaces

Theorem (G' 2016 and 2017, André–Oort conjecture)

Let S be a connected mixed Shimura variety and X be a subvariety. Suppose X contains a Zariski dense subset of special points. Then X is a Shimura subvariety, if a lower bound for the size of Galois orbit of special points holds true.
In particular, combined with the lower bound proved by Tsimerman 2018, the result holds unconditionally for $\mathfrak{A}_g$.

This theorem is based on and extends many other works. The proof follows the Pila–Zannier method. For pure Shimura varieties, it is proved in a serious of work by Pila, Daw, Klingler, Tsimerman, Ullmo, Yafaev...

- Part 1. Bound on $\#C(K)$ and distribution of algebraic points in curves.
- Part 2. Small points in abelian varieties.
- Part 3. Special points in moduli spaces, especially in mixed Shimura varieties.
- Part 4. Interactions: functional transcendence and unlikely intersections.

Part 4. Interaction: functional transcendence

In the proof of the three kinds of distribution of points explained before, a key idea / tool is the functional transcendence in the spirit of Ax–Schanuel.

Question ((weak) Ax-Schanuel)

Let $q\colon \Omega \to S$ be a surjective holomorphic morphism between algebraic varieties. Let $Z \subseteq \Omega$ be complex analytic. Then

$$\dim \overline{Z}^{\mathrm{Zar}} + \dim \overline{q(Z)}^{\mathrm{Zar}} \geq \dim Z + \dim \overline{q(Z)}^{\mathrm{biZar}}.$$

Here $\overline{q(Z)}^{\mathrm{biZar}}$ means the smallest bi-algebraic subvariety of S containing $q(Z)$, where bi-algebraic means "both algebraic in Ω and in S".

Theorem (Ax, 1971, 1973)

Ax-Schanuel holds for semi-abelian varieties.

Part 4. Interaction: functional transcendence

Theorem (G' 2017, 2020)

Let S be a mixed Shimura variety. Then Ax–Schanuel holds if

- *if Z is algebraic (Ax–Lindemann);*
- *if $q(Z)$ is algebraic (logarithmic Ax);*
- *if $S = \mathfrak{A}_g$, or more generally S is of Kuga type.*

The theorem extends and is based on the following previously known results.

- Various particular cases of Ax–Lindemann were proved by Pila, Tsimerman, Ullmo, Yafaev, before it was proved for all pure Shimura varieties by Klingler–Ullmo–Yafaev.
- Ax–Schanuel was proved for pure Shimura varieties by Mok–Pila–Tsimerman.

O-minimality is extensively used in the proofs!

Part 4. Interaction: unlikely intersections

Another aspect of the interactions of the three kinds of distribution presented before is the unlikely intersection behavior. More precisely, the Geometric Bogomlov Conjecture and the André–Oort conjecture are particular cases of unlikely intersections, and one uses ideas and results from unlikely intersections to prove the bound for $\#C(K)$.

In particular, an important result to study unlikely intersections is the generalization of the following theorem of Bogomolov.

Theorem (Bogomolov, '81)

Let A be an abelian variety and let X be a subvariety. There are only finitely many abelian subvarieties B of A satisfying:
(1) $\dim B > 0$ *and* $a + B \subsetneq X$ *for some* $a \in A$*;*
(2) B is maximal for the property described in (1).

Part 4. Interaction: unlikely intersections

Generalization of this theorem, all by using o-minimality.

- Ullmo (2014) proved the corresponding result for pure Shimura varieties, for the purpose of studying the André-Oort conjecture.
- Inspired by some work of Rémond, Habegger–Pila (2016) introduced the notion of *weakly optimal* subvarieties when studying the more general Zilber-Pink conjecture. They also proved the corresponding finiteness result for the case $Y(1)^N$.
- Daw–Ren (2018) proved the finiteness result for pure Shimura varieties.
- G' 2020 (Compositio Math.) extended and simplified Daw–Ren's result to $\mathfrak{A}_g$ (mixed Shimura varieties).

Part 5. After this memoire was submitted

- There is more general Ax–Schanuel conjecture for variations of Hodge structures proposed by Klingler in 2016. Proved for VPHS by Bakker–Tsimerman 2019; for VMHS independently by Chiu and G'–Klingler (preprint 2021).

Part 5. After this memoire was submitted

✎
- A abelian variety;
- L an ample line bundle;
- X irreducible subvariety;
- Γ a finite rank subgroup of $A(\overline{\mathbb{Q}})$.

Theorem (Mordell–Lang Conjecture, Falting 1991 + Hindry 1988)

Each irreducible component of $(X(\overline{\mathbb{Q}}) \cap \Gamma)^{\mathrm{Zar}}$ is a coset of A.

Rémond (2000) proved a bound on the number of irreducible components, $\leq c(g, \deg_L X, \deg_L A, h_{\mathrm{Fal}}(A))^{1+\mathrm{rk}\Gamma}$.
Uniform Mordell–Lang, conjectured by David–Philippon:

Theorem (G'–Ge–Kühne, 2021 preprint)

The number of irreducible components $\leq c(g, \deg_L X)^{1+\mathrm{rk}\Gamma}$.

Thanks!