Unlikely Intersections and applications to Diophantine Geometry

Laura Capuano
Giornata INdAM 2022

10 Maggio 2022

Diophantine Geometry

Diophantine Geometry is the study of polynomial equations

$$F(X_1, X_2, \ldots, X_n) = 0,$$

where F is usually a polynomial with rational coefficients.

Diophantine Geometry

Diophantine Geometry is the study of polynomial equations

$$F(X_1, X_2, \ldots, X_n) = 0,$$

where F is usually a polynomial with rational coefficients.

Theorem (Fermat's Conjecture, Wiles '95)

There are no positive integer solutions to the equation

$$a^n + b^n = c^n \quad \textit{with } n \geq 3.$$

Diophantine Geometry

Diophantine Geometry is the study of polynomial equations

$$F(X_1, X_2, \dots, X_n) = 0,$$

where F is usually a polynomial with rational coefficients.

Theorem (Fermat's Conjecture, Wiles '95)

There are no positive integer solutions to the equation

$$a^n + b^n = c^n \quad \textit{with } n \geq 3.$$

Problems:

- Decide when a polynomial equation has or has not rational or integer solutions;

Diophantine Geometry

Diophantine Geometry is the study of polynomial equations

$$F(X_1, X_2, \ldots, X_n) = 0,$$

where F is usually a polynomial with rational coefficients.

Theorem (Fermat's Conjecture, Wiles '95)

There are no positive integer solutions to the equation

$$a^n + b^n = c^n \quad \text{with } n \geq 3.$$

Problems:

- Decide when a polynomial equation has or has not rational or integer solutions;
- Decide if the number of solutions is finite;

Diophantine Geometry

Diophantine Geometry is the study of polynomial equations

$$F(X_1, X_2, \ldots, X_n) = 0,$$

where F is usually a polynomial with rational coefficients.

Theorem (Fermat's Conjecture, Wiles '95)

There are no positive integer solutions to the equation

$$a^n + b^n = c^n \quad \textit{with } n \geq 3.$$

Problems:

- Decide when a polynomial equation has or has not rational or integer solutions;
- Decide if the number of solutions is finite;
- In case of an infinite number of solutions, determine their "distribution";

Diophantine Geometry

Diophantine Geometry is the study of polynomial equations

$$F(X_1, X_2, \ldots, X_n) = 0,$$

where F is usually a polynomial with rational coefficients.

Theorem (Fermat's Conjecture, Wiles '95)

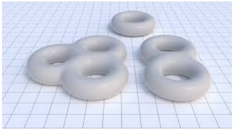
There are no positive integer solutions to the equation

$$a^n + b^n = c^n \quad \text{with } n \geq 3.$$

Problems:

- Decide when a polynomial equation has or has not rational or integer solutions;
- Decide if the number of solutions is finite;
- In case of an infinite number of solutions, determine their "distribution";
- Find all the solutions.

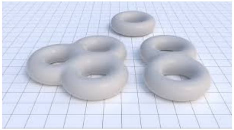
Diophantine Geometry



Geometrically, a system of polynomials defines an **algebraic variety**.

$\rightarrow$ Study of rational/integral points on a variety

Diophantine Geometry



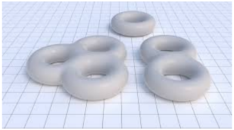
Geometrically, a system of polynomials defines an **algebraic variety**.

$\rightarrow$ Study of rational/integral points on a variety

Curves: The behaviour is totally determined by the *genus* of the curve:

- $g = 0$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}(\mathbb{Q})$ is *infinite*;

Diophantine Geometry



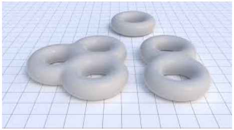
Geometrically, a system of polynomials defines an **algebraic variety**.

$\rightarrow$ Study of rational/integral points on a variety

Curves: The behaviour is totally determined by the *genus* of the curve:

- $g = 0$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}(\mathbb{Q})$ is *infinite*;
- $g = 1$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}$ is an elliptic curve and $\mathcal{C}(\mathbb{Q})$ is a *finitely generated* group (*Mordell-Weil*);

Diophantine Geometry



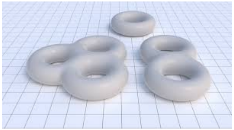
Geometrically, a system of polynomials defines an **algebraic variety**.

$\rightarrow$ Study of rational/integral points on a variety

Curves: The behaviour is totally determined by the *genus* of the curve:

- $g = 0$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}(\mathbb{Q})$ is *infinite*;
- $g = 1$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}$ is an elliptic curve and $\mathcal{C}(\mathbb{Q})$ is a *finitely generated* group (*Mordell-Weil*);
- $g \geq 2$: **Mordell conjecture (Faltings '83)**: $|\mathcal{C}(\mathbb{Q})| < +\infty$.

Diophantine Geometry



Geometrically, a system of polynomials defines an **algebraic variety**.

$\rightarrow$ Study of rational/integral points on a variety

Curves: The behaviour is totally determined by the *genus* of the curve:

- $g = 0$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}(\mathbb{Q})$ is *infinite*;
- $g = 1$: either $\mathcal{C}(\mathbb{Q}) = \varnothing$ or $\mathcal{C}$ is an elliptic curve and $\mathcal{C}(\mathbb{Q})$ is a *finitely generated* group (*Mordell-Weil*);
- $g \geq 2$: **Mordell conjecture (Faltings '83)**: $|\mathcal{C}(\mathbb{Q})| < +\infty$.

"geometry determines arithmetic"

A possible strategy:

- If $\mathcal{C}(\mathbb{Q}) \neq \varnothing$, we can embed $\mathcal{C}$ in an abelian variety $\mathcal{J}_{\mathcal{C}}$ (Jacobian variety);

Unlikely intersections and Zilber-Pink conjecture

A possible strategy:

- If $\mathcal{C}(\mathbb{Q}) \neq \emptyset$, we can embed $\mathcal{C}$ in an abelian variety $\mathcal{J}_{\mathcal{C}}$ (Jacobian variety);
- $\mathcal{J}_{\mathcal{C}}(\mathbb{Q})$ is a finitely generated subgroup (Mordell-Weil);

Unlikely intersections and Zilber-Pink conjecture

A possible strategy:

- If $\mathcal{C}(\mathbb{Q}) \neq \varnothing$, we can embed $\mathcal{C}$ in an abelian variety $\mathcal{J}_{\mathcal{C}}$ (Jacobian variety);
- $\mathcal{J}_{\mathcal{C}}(\mathbb{Q})$ is a finitely generated subgroup (Mordell-Weil);
- We have to show that $\mathcal{C}(\mathbb{Q}) = \mathcal{C} \cap \mathcal{J}_{\mathcal{C}}(\mathbb{Q})$ is finite.

Unlikely intersections and Zilber-Pink conjecture

A possible strategy:

- If $\mathcal{C}(\mathbb{Q}) \neq \emptyset$, we can embed $\mathcal{C}$ in an abelian variety $\mathcal{J}_{\mathcal{C}}$ (Jacobian variety);
- $\mathcal{J}_{\mathcal{C}}(\mathbb{Q})$ is a finitely generated subgroup (Mordell-Weil);
- We have to show that $\mathcal{C}(\mathbb{Q}) = \mathcal{C} \cap \mathcal{J}_{\mathcal{C}}(\mathbb{Q})$ is finite.

This strategy inspired the formulation of several conjectures, as

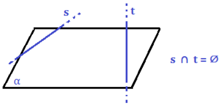
- Manin-Mumford conjecture (Laurent, Raynaud, Hindry, Hurshowski, Szpiro-Ullmo-Zhang, Pila-Zannier),
- Mordell-Lang conjecture (Laurent, Faltings, Hindry, Vojta, McQuillan),

recently generalized by Zilber, Bombieri-Masser-Zannier in the case of tori and more generally by Pink in the setting of mixed Shimura varieties.

Unlikely Intersections - General philosophy

$X, Y \subset T$ subvarieties of an ambient variety of dimension n.

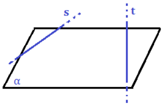
General expectation:
$\dim(X \cap Y) \leq \dim X + \dim Y - n$; in particular
$X \cap Y = \varnothing$ if $\dim X + \dim Y < n$
unless there is some *geometric reason* for this.



Unlikely Intersections - General philosophy

$X, Y \subset T$ subvarieties of an ambient variety of dimension n.

Aspettativa: $\dim(X \cap Y) \leq \dim X + \dim Y - n$;
in particular $X \cap Y = \varnothing$ se $\dim X + \dim Y < n$
unless there are some *special reasons*.

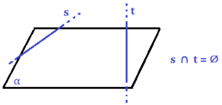


"*Unlikely intersections*"

Unlikely Intersections - General philosophy

$X, Y \subset T$ subvarieties of an ambient variety of dimension n.

Aspettativa: $\dim(X \cap Y) \leq \dim X + \dim Y - n$;
in particular $X \cap Y = \varnothing$ se $\dim X + \dim Y < n$
unless there are some *special reasons*.



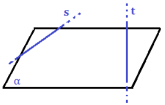
"Unlikely intersections"

More generally, let us fix $X \subset T$ and let us consider $\mathcal{Y}$ a family of subvarieties of T of codimension $> \dim X$.

Unlikely Intersections - General philosophy

$X, Y \subset T$ subvarieties of an ambient variety of dimension n.

Aspettativa: $\dim(X \cap Y) \leq \dim X + \dim Y - n$;
in particular $X \cap Y = \emptyset$ se $\dim X + \dim Y < n$
unless there are some *special reasons*.



"*Unlikely intersections*"

More generally, let us fix $X \subset T$ and let us consider $\mathcal{Y}$ a family of subvarieties of T of codimension $> \dim X$.

General expectation: $X \cap Y = \emptyset$ in "most of" the cases;
in particular, $\bigcup_{Y \in \mathcal{Y}} X \cap Y$ is "small" with respect to X.

Zilber-Pink Conjecture for semiabelian varieties

Conjecture (Zilber-Pink)

Let A be a complex semiabelian variety and let X be an irreducible subvariety of A of dimension d. Let

$$A^{[d+1]} := \bigcup_{codim\ H \geq d+1} H.$$

Then, if X is not contained in any proper algebraic subgroup of A, the intersection $X \cap A^{[d+1]}$ is not Zariski-dense in X.

Zilber-Pink Conjecture for semiabelian varieties

Conjecture (Zilber-Pink)

Let A be a complex semiabelian variety and let X be an irreducible subvariety of A of dimension d. Let

$$A^{[d+1]} := \bigcup_{\mathrm{codim}\ H \geq d+1} H.$$

Then, if X is not contained in any proper algebraic subgroup of A, the intersection $X \cap A^{[d+1]}$ is not Zariski-dense in X.

- few known cases – if X is a curve or $\dim X = n - 2$ (Maurin, Bombieri-Masser-Zannier, Viada, Rémond, Habegger-Pila, Barroero-Kühne-Schmidt ...).

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Example:

There exist only finitely many $x \in \mathbb{C}$ satisfying

$$\begin{cases} x^{a_1}(1-x)^{a_2}(1+x)^{a_3} = 1 \\ x^{b_1}(1-x)^{b_2}(1+x)^{b_3} = 1 \end{cases}$$

with $(a_1, a_2, a_3), (b_1, b_2, b_3) \in \mathbb{Z}^3$ linearly independent.

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Proof of BMZ:
bound on the height,
diophantine approximation.

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Proof of BMZ:
bound on the height,
diophantine approximation.

Height of an algebraic number:
measure of the *"complexity"* of the number.
Ex: if $\alpha = \frac{a}{b} \in \mathbb{Q}$, then:

$$H(\alpha) = \max\{|a|, |b|\}.$$

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Proof of BMZ:
bound on the height,
diophantine approximation.

New proof (C., 2014): Pila-Zannier method: combination of techniques from model theory (o-minimality), functional transcendence.

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Proof of BMZ:
bound on the height,
diophantine approximation.

New proof (C., 2014): Pila-Zannier method: combination of techniques from model theory (o-minimality), functional transcendence.

↓

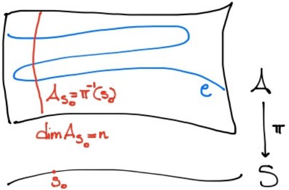
generalizable to other contexts

Unlikely intersections in a torus

Theorem (Bombieri-Masser-Zannier 1999)

Let $\mathcal{C} \subset (\mathbb{C}^*)^n$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ such that it is not contained in a translate of a proper algebraic subgroup of $(\mathbb{C}^*)^n$. Then, $\mathcal{C} \cap (\mathbb{C}^*)^{[2]}$ is finite.

Analogous results for curves in families of abelian varieties (Barroero-C.)



Application to Pell equation in polinomials

Let $D \in \mathbb{C}[t]$ be a polynomial without multiple roots; we ask whether there exist $A, B \in \mathbb{C}[t]$ with $B \neq 0$ such that

$$A^2 - DB^2 = 1.$$

In this case D is said to be "Pellian".

Application to Pell equation in polinomials

Let $D \in \mathbb{C}[t]$ be a polynomial without multiple roots; we ask whether there exist $A, B \in \mathbb{C}[t]$ with $B \neq 0$ such that

$$A^2 - DB^2 = 1.$$

In this case D is said to be "Pellian".

- D Pellian $\rightarrow \deg D = 2d$ and $D \neq \square$ in $\mathbb{C}[t]$;

Application to Pell equation in polinomials

Let $D \in \mathbb{C}[t]$ be a polynomial without multiple roots; we ask whether there exist $A, B \in \mathbb{C}[t]$ with $B \neq 0$ such that

$$A^2 - DB^2 = 1.$$

In this case D is said to be "Pellian".

- D Pellian $\rightarrow \deg D = 2d$ and $D \neq \square$ in $\mathbb{C}[t]$;
- The converse is not always true:

Example:

$$D(t) = t^4 + t + 1 \text{ is not Pellian.}$$

Application to Pell equation in polinomials

Let $D \in \mathbb{C}[t]$ be a polynomial without multiple roots; we ask whether there exist $A, B \in \mathbb{C}[t]$ with $B \neq 0$ such that

$$A^2 - DB^2 = 1.$$

In this case D is said to be "Pellian".

- D Pellian $\rightarrow \deg D = 2d$ and $D \neq \square$ in $\mathbb{C}[t]$;
- The converse is not always true:

Example:

$$D(t) = t^4 + t + 1 \text{ is not Pellian.}$$

Question: How many Pellian polynomials do we have?

Application to Pell equation in polinomials

Results of unlikely intersections → solvability of

$$A^2 - DB^2 = 1$$

for families of polynomials $D_\lambda(t)$ in function of a parameter λ.

Application to Pell equation in polinomials

Results of unlikely intersections → solvability of

$$A^2 - DB^2 = 1$$

for families of polynomials $D_\lambda(t)$ in function of a parameter λ.

Example:

Let $D_\lambda(t) = t^6 + t + \lambda$. There are only finitely many $\lambda_0 \in \mathbb{C}$ such that $t^6 + t + \lambda_0$ is Pellian.

Application to Pell equation in polinomials

Results of unlikely intersections → solvability of

$$A^2 - DB^2 = 1$$

for families of polynomials $D_\lambda(t)$ in function of a parameter λ.

Example:

Let $D_\lambda(t) = t^6 + t + \lambda$. There are only finitely many $\lambda_0 \in \mathbb{C}$ such that $t^6 + t + \lambda_0$ is Pellian.

One can study the same questions for families of "generalized" Pell equations

$$A^2 - DB^2 = F$$

with $D, F \in \mathbb{C}[\lambda, t]$.

Application to Pell equation in polinomials

Theorem (Barroero-C. 2020)

Let $D_\lambda(t) \in \overline{\mathbb{Q}}(\lambda)[t]$ some "nice" polynomial. Let $F_\lambda(t) \in \overline{\mathbb{Q}}[t, \lambda] \setminus \{0\}$. Then, either the generalized Pell equation has an identical solution, or there exist at most finitely many $\lambda_0 \in \mathbb{C}$ such that the specialized equation

$$A^2 - D_{\lambda_0} B^2 = F_{\lambda_0}$$

has a solution $A, B \in \mathbb{C}[t]$ with $B \neq 0$.

Application to Pell equation in polinomials

Theorem (Barroero-C. 2020)

Let $D_\lambda(t) \in \overline{\mathbb{Q}}(\lambda)[t]$ some "nice" polynomial. Let $F_\lambda(t) \in \overline{\mathbb{Q}}[t,\lambda] \smallsetminus \{0\}$. Then, either the generalized Pell equation has an identical solution, or there exist at most finitely many $\lambda_0 \in \mathbb{C}$ such that the specialized equation

$$A^2 - D_{\lambda_0} B^2 = F_{\lambda_0}$$

has a solution $A, B \in \mathbb{C}[t]$ with $B \neq 0$.

Example:

Let $D_\lambda(t) = (t-\lambda)(t^7 - t^3 - 1)$ and $F(X) = 4t + 1$. Then there exist only finitely many $\lambda_0 \in \mathbb{C}$ such that the equation

$$A^2 - (t-\lambda_0)(t^7 - t^3 - 1)B^2 = 4t + 1$$

has a non trivial solution $A, B \in \mathbb{C}[t]$ with $B \neq 0$.