On the Torsion and rational Points of some Curves

Evelina Viada
Georg-August University Göttingen

The Mordell conjecture 100 years later
MIT, July 8-12, 2024

Let C be an algebraic curve over $\mathbb{Q}$ embedded in its Jacobian J_C (in an abelian variety A).

- Task 1 : find C_{Tor} the torsion points of J_C (of A) that lie on C.
  Explicit Manin Mumford Conjecture
- Task 2 : find $C(\mathbb{Q})$ the set of rational points of C.
  Explicit Mordell Conjecture

QUESTION: Can we do that?

ANSWER TO TASK 2: NO

OPTIMISTIC ANSWER: NOT YET, SOMETIMES

ANSWER TO TASK 1: YES

REALISTIC ANSWER: AT LEAST IN PRINCIPLE

Example to Task 1: Find the torsion (with R. Pengo)

Example

Consider $\mathbb{A}^2 \times \mathbb{A}^2$ with coordinates $(x_1, y_1) \times (x_2, y_2)$, and the family of curves (or their projective closures):

$$\mathcal{C}_1(a,b): \begin{cases} y_1^2 &= x_1^3 - 16x_1 + 16 \\ y_2^2 &= x_2^3 - 16x_2 + 16 \\ ay_2 &= bx_1 \end{cases}$$

for every two non-zero integer numbers a, b. Then $\mathcal{C}_1(a,b)$ is the affine part of a curve embedded in E^2, where $E\colon\ y^2z = x^3 - 16xz^2 + 16z^3$.

The torsion subset $\mathcal{C}_1(a,b)_{Tor}$ is exactly

$$\mathcal{C}_1(a,b)_{Tor} = \{(0_E, P) : P \in E[2](\overline{\mathbb{Q}})\} \subset ExE$$

If $\alpha = \sqrt[3]{\frac{8}{9}\sqrt{-111} - 8}$, then $x_P = -\frac{1}{2}\alpha(1+\sqrt{-3}) - \frac{8(1-\sqrt{-3})}{3\alpha}, -\frac{1}{2}\alpha(1-\sqrt{-3}) - \frac{8(1+\sqrt{-3})}{3\alpha}, \alpha + \frac{16}{3\alpha}$.

Example to Task 2: find the rational points with R. Pengo, relying on a method with F. Veneziano

Example

Consider in $\mathbb{A}^2 \times \mathbb{A}^2$ with coordinates $(x_1, y_1) \times (x_2, y_2)$, the family of curves

$$\mathcal{C}_n = \begin{cases} y_1^2 & = x_1^3 - 3x_1 - 1 \\ y_2^2 & = x_2^3 - 3x_2 - 1 \\ y_2 & = x_1^n + x_1 + 1 \end{cases}$$

The rational points are exactly

$$\mathcal{C}_n(\mathbb{Q}) = \begin{cases} \{(-1, \pm 1, -1, 1), (-1, \pm 1, 2, 1)\}, & \text{if } 2 \mid n \\ \{(-1, \pm 1, -1, -1), (-1, \pm 1, 2, -1)\}, & \text{if } 2 \nmid n \end{cases}$$

Beyond task 2: (with F. Veneziano)
Find the $\mathbb{Q}(\sqrt{-3})$-rational points

Example

Consider in $\mathbb{A}^2 \times \mathbb{A}^2$ with coordinates $(x_1, y_1) \times (x_2, y_2)$, the curve

$$C_6' = \begin{cases} y_1^2 & = x_1^3 + 2 \\ y_2^2 & = x_2^3 + 2 \\ x_1^6 & = y_2 \end{cases}$$

The $\mathbb{Q}(\sqrt{-3})$-rational points on C_6'.

Let $\zeta = \frac{-1+\sqrt{-3}}{2}$. Then $C_6'(\mathbb{Q}(\sqrt{-3}))$ is given by:

$$\begin{aligned}\{&(-1,1,-1,1),(-1,-1,-1,1),(-1,1,-\zeta,1),(-1,-1,-\zeta,1),\\ &(-1,1,\zeta+1,1),(-1,-1,\zeta+1,1),(-\zeta,1,-1,1),(-\zeta,-1,-1,1),\\ &(-\zeta,1,-\zeta,1),(-\zeta,-1,-\zeta,1),(-\zeta,1,\zeta+1,1),(-\zeta,-1,\zeta+1,1),\\ &(\zeta+1,1,-1,1),(\zeta+1,-1,-1,1),(\zeta+1,1,-\zeta,1),\\ &(\zeta+1,-1,-\zeta,1),(\zeta+1,1,\zeta+1,1),(\zeta+1,-1,\zeta+1,1)\}\end{aligned}$$

The $\mathbb{Q}(\sqrt{-3})$-rational points on the C'_n

Example

Consider in $\mathbb{P}^2 \times \mathbb{P}^2$ with coordinates $(x_1 : y_1 : z_1) \times (x_2 : y_2 : z_2)$, the projective closure of

$$C'_n = \begin{cases} y_1^2 &= x_1^3 + 2 \quad \text{elliptic curve} \quad E \quad \text{with CM} \\ y_2^2 &= x_2^3 + 2 \\ x_1^n &= y_2 \end{cases}$$

Let $g = (-1 : 1 : 1)$ and $\mathrm{End(E)} = \mathbb{Z}[\zeta]$ for $\zeta = \frac{-1+\sqrt{-3}}{2}$. Then $C'_n(\mathbb{Q}(\sqrt{-3}))$ is given by:

$$\begin{aligned} &C'_n(\mathbb{Q}(\sqrt{-3})) \setminus (0_E, 0_E) = \\ &= \{([a]g, [b]g) \mid a = \pm 1, \pm\zeta, \pm\zeta^2 \text{ and } b = 1, \zeta, \zeta^2\} && \text{if } n \equiv 0 \pmod 6 \\ &= \{([a]g, [b]g) \mid a = \pm 1 \text{ and } b = -1, -\zeta, -\zeta^2\} && \text{if } n \equiv \pm 1 \pmod 6 \\ &= \{([a]g, [b]g) \mid a = \pm 1 \text{ and } b = 1, \zeta, \zeta^2\} && \text{if } n \equiv \pm 2 \pmod 6 \\ &= \{([a]g, [b]g) \mid a = \pm 1, \pm\zeta, \pm\zeta^2, b = -1, -\zeta, -\zeta^2\} && \text{if } n \equiv 3 \pmod 6, \end{aligned}$$

Why is task 1 easier? Quantitative aspects

Question 1 Is C_{Tor} a finite set? (Manin-Mumford Conjecture).

Answer 1 YES, if the genus of C is at least 2
(C non-torsion in A, i.e. not the translate of an elliptic curve by a torsion point.)
(Raynaud's Theorem).

- If we can bound the cardinality of C_{Tor}, then we can find C_{Tor} (in principle)
- The height of the torsion is 0

Question 2 Is $C(\mathbb{Q})$ a finite set? (Mordell Conjecture)

Answer 2 YES, if the genus of C is at least 2.
(Faltings' Theorem).

- If we can bound the cardinality of $C(\mathbb{Q})$ then we CANNOT find $C(\mathbb{Q})$
- There is no known bound for the height of $C(\mathbb{Q})$ in general.

Northcott's Theorem: there exists a procedure to find the points of bounded height and bounded degree in $\mathbb{P}^n$.

Can we say how many?

- Quantitative/Explicit Manin Mumford (Galateau & Martínez's Theorem):

$$|C_{Tor}| \leq 4^{(2c(A)+2)g} \deg(C)^2$$

  where g is the dimension of A and $c(A)$ is a constant introduced by Serre (to be defined later).
  Serre's constant is explicitly bounded for product of elliptic curves, CM abelian varieties and Jacobians.

- Quantitative Mordell Conjecture: how explicit should the constants be? What should they depend on?
  - explicit dependence on the degree of C, the dimension and height of A, and the rank of $A(\mathbb{Q})$.

$$|C(\mathbb{Q})| \leq (2^{34} \max(1, h_\theta(A)) \cdot \deg(C))^{(\mathrm{rk}(A(\mathbb{Q}))+1)\dim(A)^{20}}.$$

(Rémond + David-Philippon)

  - for smooth C, dependence on the genus of C and rank of $J_C(\mathbb{Q})$, not explicit.

$$|C(\mathbb{Q})| \leq c(\dim(J_C))^{1+\mathrm{rk}(J_C(\mathbb{Q}))}$$

(Dimitrov, Gao, Habegger)

Let k be a field and $A \subseteq \mathbb{P}^n$ an abelian variety over k.

For $G_k := \mathrm{Gal}(\overline{k}/k)$ and $\rho_A \colon G_k \to \mathrm{Aut}_{\mathbb{Z}}(A_{\mathrm{tors}}) \cong \mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$, define Serre's constant as

$$c(A) := [\mathcal{H}_A(\widehat{\mathbb{Z}}) \colon (\rho_A(G_k) \cap \mathcal{H}_A(\widehat{\mathbb{Z}}))]$$

where with $\mathcal{H}_A(\widehat{\mathbb{Z}}) \cong \widehat{\mathbb{Z}}^\times$ we mean the homotheties.

Let V be an algebraic subvariety A and let $\delta(V)$ be the smallest d such that V is the intersection of hypersurfaces of degree at most d.
Define V^j_{tor} to be the equidimensional component of dimension j in V_{tor}. So

$$V_{\mathrm{tor}} := \overline{V \cap A_{\mathrm{tor}}} = \bigcup_{j=0}^{\dim V} V^j_{\mathrm{tor}}.$$

Manin-Mumford for Varieties: The V^j_{tor} are torsion varieties, i.e. union of components of algebraic subgroups.

Work of **Galateau & Martìnez (2017)** shows that:

$$deg(V^j_{\mathrm{tor}}) \leq ((2g+4)^3 16^{g(c(A)+2)})^{(g-j)\dim(V)} \cdot \deg(A) \cdot \delta(V)^{g-j},$$

where $c(A)$ is Serre's constant.

Estimates for $c(A)$:

- If E has CM and $j(E) \neq 0, 1728$, work of **Campagna & Pengo (2022)** gives explicit bounds. In particular, if E is defined over $\mathbb{Q}$ then $c(E) = 2$.
- if E non-CM then work of **Lombardo (2015)** gives an explicit bound. If E is defined over $\mathbb{Q}$, then $c(E) \leq e^{1.910^{10}} \max\{1, h(E)\}^{12395}$.
- If A is a CM abelian variety then work of **Eckstein (2005)** gives $c(A) \leq [k : \mathbb{Q}]3^{5g^2}$.
- For any Jacobian $A = J_C$, work of **Buium (1996)** gives a method to find an explicit bound.
- $c(A_1 \times \cdots \times A_r) = \max\{c(A_1), \ldots, c(A_r)\}$.

Our example

- Choose a *Serre curve* E, that means an elliptic curve with $c(E) = 1$. (Example $E\colon\ y^2 = x^3 - 16x + 16$)
- Compute $\delta(\mathcal{C}_1(a,b))) \leq \deg(\mathcal{C}_1(a,b)) = \deg(\mathcal{C}_1) = 15$ and $g(\mathcal{C}_1(a,b)) = 6$.
- Go through Galateau-Martìnez's proof to keep constants as small as possible.
- Find that $|\mathcal{C}_1(a,b)_{Tor}| \leq 17775$.

  Note that the general bound is independent of $h(C)$ thus this bound holds for all curves $\mathcal{C}_1(a,b)$
- Use the fact that if P lies on $\mathcal{C}_1(a,b)$ then all its conjugates do, to find that $\mathrm{ord}(P) \leq 241$.
- Use the division polynomials to find all the torsion points of order at most 241.
- Check if they are on any of our curves, that is if the ratio x_1/y_2 can be rational.

In conclusion:

- in many cases (such as CM abelian varieties, Jacobians and products of elliptic curves), Serre's constant $c(A)$ can be bounded explicitly;
- for any variety V embedded in an abelian variety A for which Serre's constant $c(A)$ is bounded explicitly, we have an algorithm to find V_{tor}.

PROBLEM: This algorithm might not be implementable, given the current computational constraints.

Irreducible curve C in an abelian variety A of dimension N

Given a set $S \subseteq A$ with some properties, when is $S \cap C$ finite ?

$\boxed{S_0 = \bigcup_{dimB=0} B}$

$\boxed{S_1 = \bigcup_{dimB\leq 1} B}$

$\vdots$

$\boxed{S_{N-2} = \bigcup_{dimB\leq N-2} B}$

$\boxed{S_{N-1} = \bigcup_{dimB\leq N-1} B}$

Manin-Mumford
C non-torsion $\Rightarrow S_0 \cap C$ finite

$\xLeftarrow{\mathrm{rk}(S_0)=0}$

Mordell-Lang
$S \leq A$, $\mathrm{rk}(S)$ finite, C non-translate $\Rightarrow S \cap C$ finite

explicit Manin-Mumford (see previous discussion) $\Longleftarrow$ effective/explicit Mordell-Lang

$\Big\Downarrow$ Mordell-Weil

Mordell
$g(C) \geq 2 \Rightarrow C(\mathbb{Q})$ finite

effective/explicitly bounded height

Torsion Anomalous Conjecture (TAC)
C weak-transverse $\Rightarrow S_{N-2} \cap C$ finite

explicit Mordell for transverse $C \subseteq A$, when $\mathrm{rk}(A(\mathbb{Q})) < \dim(A)$

C transverse $\Rightarrow S_{N-1} \cap C$ has explicitly bounded height

Example: $C \subseteq E^N$ transverse, $\mathrm{rk}(E(K)) < N \Rightarrow h(C(K)) \leq$ an explicit constant.
If this constant is small, one can find $C(K)$ (see previous examples).

Recall: Weak-transverse: irreducible $V \not\subseteq B$ for any proper algebraic subgroup $B \subsetneq A$.
Transverse: irreducible $V \not\subseteq B + q$ for any translate of B by a point $q \in A$.

The result of Faltings is not effective, in the sense that it does not give any method for finding the rational points on C.
This is due to the non existence of an effective bound for the height of the points in $C(\mathbb{Q})$ in general.

Effective Methods

- The method of **Chabauty-Coleman** and the **quadratic Chabauty and Kim** program.
  A significant number of examples of curves in general of small genus and restricted to the condition that the $\mathbb{Q}$-rank of the Jacobian is strictly smaller than the genus of the curve (Bruin, Flynn, Poonen, Stoll, ...). Exception for the split Cartan modular curve of level 13, and other modular curves whose rank is equal to the genus of the curve (Balakrishnan, Dogra, Müller, Tuitman, Vonk, ...).
- The **Manin-Dem'janenko** method (our method relies on the same starting principle).
  Families of examples of genus 2 or 3 and $\mathbb{Q}$-rank 1 or 2 and some other condition for instance a factor of the Jacobian given by $y^2 = x^3 + a^2x$, with a square-free integer. (Kulesz, Girard, Matera, Silverman, Schost...)

Explicit TAC $\Rightarrow$ method for Example 2

Theorem (Torsion Anomalous Conjecture for Curves)

Let C be weak-transverse in E^N. Then the set

$$C \cap S_{N-2} = C \cap \cup_{\dim B \leq N-2} B \quad \text{is finite.}$$

Let C be transverse in E^N. Then the set

$$C \cap S_{N-1} = C \cap \cup_{\dim B \leq N-1} B \quad \text{has} \quad \text{explicitly} \quad \text{bounded height.}$$

Remark

The original proof of **Bombieri-Masser-Zannier (1999)** *in $\mathbb{G}_m^n$ for transverse curves can be adapted to E^N for E with CM, due to the use of a Lehmer Type bound. For E without CM one can use a Bogomolov Type bound and Vojta's inequality in a non effective way. To get the examples we make explicit the second part with a different approximation method that keeps the constants small. This implies the effective Mordell Conjecture for C transverse in E^N and $\mathrm{rk} E(\mathbb{Q}) \leq N-1$. Thus we can in principle find the rational points of such curves.*
For C weak-transverse in A, the finiteness of $C \cap S_{N-2}$ is proven by **Habegger-Pila (2016)** *using O-minimality.*

Algebraic subgroups of E^N

- Let $\phi_B \in \mathrm{Mat}_{r,n}(\mathrm{End}(E))$ be a matrix of rank r

$$\phi_B = \begin{pmatrix} b_{11} & \dots & b_{1N} \\ \vdots & \vdots & \vdots \\ b_{r1} & \dots & b_{rN} \end{pmatrix} : E^N \to E^r$$

$$\begin{aligned} \phi_B : (x_1, \dots, x_N) \mapsto (b_{11}x_1 +_E \dots +_E\ & b_{1N}x_N, \\ \vdots \qquad\qquad & \quad \vdots \\ b_{r1}x_1 +_E \dots +_E\ & b_{rN}x_N) \end{aligned}$$

- $B = \ker \phi_B$ is an algebraic subgroup of $\mathrm{codim} B = r$
  Minkowski reduction of ϕ_B gives $\deg B \approx ||b_1||^2 \dots ||b_r||^2$.

An algebraic subgroup of E^2 of dimension 1 is given, up to some torsion, by

$$B : \{b_1 X_1 + b_2 X_2 = 0$$

Consider an algebraic curve $\mathcal{C} \subset E^2$, and suppose that $\mathrm{rk}(E(\mathbb{Q})) = 1$, i.e. $E(\mathbb{Q}) = \langle g_1 \rangle$
Then a point $P = (P_1, P_2) \in \mathcal{C}(\mathbb{Q}) \subset E(\mathbb{Q})^2$ has the form

$$P = (a_1 g_1, a_2 g_1)$$

and therefore P is a point in

$$P \in B_P : \{a_2 X_1 - a_1 X_2 = 0$$

So

$$\forall P \in \mathcal{C}(\mathbb{Q}) \text{ then } P \in \mathcal{C} \cap B_P \Rightarrow \mathcal{C}(\mathbb{Q}) \subset \mathcal{C} \cap \bigcup_{dim B = 1} B.$$

The Theorem tells us that the set

$$\mathcal{C} \cap \bigcup_{dim B = 1} B \quad \text{has height explicitly bounded.}$$

Thus if $E(\mathbb{Q})$ has rank 1 and $\mathcal{C} \in E^2$ has genus ≥ 2 then $\mathcal{C}(\mathbb{Q})$ has explicitly bounded height.

The constraint on the rank is unavoidable with this method.

If $\mathcal{C} \subset E^2$ and E has rank 2 with $E(\mathbb{Q}) = \langle g_1, g_2 \rangle_{\mathbb{Z}}$ and $P \in \mathcal{C}(\mathbb{Q})$ then $P = (a_1 g_1 + a_2 g_2, b_1 g_1 + b_2 g_2)$ but you do not have any subgroup B_P that contains P.

$$\frownie$$

To remove the hypothesis on the rank is equivalent to prove that for weak-transverse curves C the set $C \cap (\cup_{\dim B \leq N-2} B)$ has explicitly bounded height (Explicit TAC implies Explicit Mordell).
If $\mathcal{C}_0$ is transverse in E^2 and $E(\mathbb{Q}) = \langle g_1, \ldots, g_r \rangle$ then $P = (P_1, P_2) \in \mathcal{C}(\mathbb{Q})$ is given by $(P_1, P_2) = (a_1 g_1 + \cdots + a_r g_r, b_1 g_1 + \cdots + b_r g_r)$. Consider the curves $C = \mathcal{C}_0 \times g_1 \times \cdots \times g_r$ weak-transverse in E^{2+r}. Thus $(P_1, P_2, g_1, \ldots, g_r)$ is a point in C and in

$$B_P = \begin{cases} X_1 & = a_1 Y_1 + \cdots + a_r Y_r \\ X_2 & = b_1 Y_1 + \cdots + b_r Y_r \end{cases}$$

Let E be an elliptic curve given in the form

$$y^2 = x^3 + Ax + B.$$

with A, B algebraic integers.
Let $C(E) = \frac{h_W(\Delta)+3h_W(j)}{4} + \frac{h_W(A)+h_W(B)}{2} + 4$.
Let $\hat{h}$ be the Néron-Tate height on E^N.
For a curve $\mathcal{C}$ let $h(\mathcal{C})$ be the normalised height of $\mathcal{C}$.

Theorem (Arithmetic Bézout Theorem, explicit version of Philippon)

Let V and W be irreducible subvarieties of $\mathbb{P}^m$. Let $Z_1, \ldots, Z_n$ be the irreducible components of $V \cap W$. Then

$$\sum_{i=1}^{n} h(Z_i) \leq \deg V \; h(W) + h(V) \; \deg W + c(m) \deg V \deg W.$$

Essential Minimum

Definition:
$h : V(\overline{\mathbb{Q}}) \to \mathbb{R}^+$

$$0 \underbrace{\qquad\qquad\qquad}_{h^{-1}\ \mathrm{non-dense}} \mu(V) \underbrace{\qquad\qquad\qquad}_{h^{-1}\ \mathrm{dense}} \longrightarrow$$

Essential Minimum

$$\mu(V) = \sup\{\varepsilon : h^{-1}[0,\varepsilon)\ \mathrm{non-dense\ in}\ \ V\}$$

Theorem (Zhang Inequality)

Let V be an irreducible subvariety of $\mathbb{P}^m$, then

$$\frac{1}{(1+\dim V)}\frac{h(V)}{\deg V} \leq \mu(V) \leq \frac{h(V)}{\deg V}.$$

Theorem (Minkowski Convex Body Theorem)

Let Λ be a lattice of volume Δ in $\mathbb{R}^n$ and $S \subset \mathbb{R}^n$ a convex body, symmetric with respect to the origin. If the volume of S is $> 2^n\Delta$ then S contains at least one lattice point other than the origin.

Theorem (Veneziano, V. 2022 (generalization of N=2 Checcoli, Veneziano, V. 2018))

Let E be a non-CM elliptic curve and let $\mathcal{C}$ be a curve transverse in E^N. Then all the points P in $\mathcal{C} \cap S_{N-1}$ have Néron-Tate height explicitely bounded as follows:

$$\hat{h}(P) \leq D_1(N) \cdot h(\mathcal{C})(\deg \mathcal{C})^{N-1} + D_2(N,E)(\deg \mathcal{C})^N + D_3(N,E).$$

The constants are given by:

$$D_1(N) = 4N! \left(\frac{N^2(N-1)^2 3^N}{4^{N-3}} N!(N-1)!^4 \right)^{N-1},$$
$$D_2(N,E) = D_1(N) \left(N^2 C(E) + 3^N \log 2 \right),$$
$$D_3(N,E) = (N+1)C(E) + 1, C(E)$$

Theorem (Veneziano, V. 2022)

Let E be an elliptic curve with Complex Multiplication by the field K and let $\mathcal{C}$ be a curve transverse in E^N. Then all the points P in $\mathcal{C} \cap S_{N-1}$ have Néron-Tate height explicitely bounded as follows:

$$\hat{h}(P) \leq C_1(N,E) \cdot h(\mathcal{C})(\deg \mathcal{C})^{N-1} + C_2(N,E)(\deg \mathcal{C})^N + C_3(N,E).$$

The constants are given by:

$$\begin{aligned} c(N) &= N! \left(N \cdot N! \cdot (2N)!^2\right)^{N-1}, \\ C_1(N,E) &= c(N) f^N |D_K|^{N^2 - \frac{3}{2}N+1} + 1, \\ C_2(N,E) &= c(N) f^N |D_K|^{N^2 - \frac{3}{2}N+1} \left(N^2 C(E) + 3^N \log 2 + 1\right), \\ C_3(N,E) &= N(N+1)C(E) + 3^N \log 2 + 1. \end{aligned}$$

where D_K is the discriminant of the field of complex multiplication and f is the conductor of $\mathrm{End(E)}$.

Estimates for the height of curves

Proposition (with Riccardo Pengo)

Let $\mathcal{C} \subseteq \mathbb{P}^2 \times \mathbb{P}^2$ *be the curve*

$$\mathcal{C}\colon \begin{cases} y_1^2 z_1 & = x_1^3 + Ax_1 z_1^2 + Bz_1^3 \\ y_2^2 z_2 & = x_2^3 + Ax_2 z_2^2 + Bz_2^3 \\ f(x_1 : y_1 : z_1, x_2 : y_2 : z_2) & = 0, \end{cases}$$

where $f \in \mathbb{Z}[x_1 : y_1 : z_1, x_2 : y_2 : z_2]$ *is a bi-homogeneous polynomial of bi-degree* $(\delta_1(f), \delta_2(f))$*. Then*

$$h(\mathcal{C}) \leq 9 \cdot \left((\delta_1(f) + \delta_2(f)) \left(\frac{1}{2} \log\left(\frac{|A|^2 + 3|B|^2 + 4}{3} \right) + \frac{15}{4} \right) + \frac{1}{2} \log\left(\sum_{v,w} \frac{|a_{v,w}(f)|^2}{(v)(w)} \right) \right)$$

where

$$f = \sum_{\substack{v_1+v_2+v_3=\delta_1(f) \\ w_1+w_2+w_3=\delta_2(f)}} a_{v,w}(f) \cdot x_1^{v_1} y_1^{v_2} z_1^{v_3} x_2^{w_1} y_2^{w_2} z_2^{w_3} \in \mathbb{Z}[x_1 : y_1 : z_1, x_2 : y_2 : z_2]$$

and we denote by $(b) := \frac{(b_1+\cdots+b_k)!}{b_1!\cdots b_k!}$ *for* $b \in \mathbb{N}^k$.

Producing Families of Curves of increasing Genus s.t. we can find $C(\mathbb{Q})$

Choose an elliptic curve E such that $\operatorname{rk} E(\mathbb{Q}) = 1$.

For example

$$\begin{aligned}
&E_1: y^2 = x^3 - x + 1 && E_4: y^2 = x^3 + 3x + 1\\
&E_2: y^2 = x^3 + x - 1 && E_5: y^2 = x^3 - 3x - 1\\
&E_3: y^2 = x^3 + 2x + 1 && E_6: y^2 = x^3 + 4x + 1:
\end{aligned}$$

Remark

The method works for any number field K such that $\operatorname{rk} E(K) = 1$.
We do not need to have the generator of $E(K)$ even if this speeds up the implementation.

The Family $\mathcal{C}_n$

Cut in *ExE* a (family) of curves with an extra polynomial.

For example

$$\mathcal{C}_{n,1} = \begin{cases} y_1^2 &= x_1^3 - x_1 + 1 \\ y_2^2 &= x_2^3 - x_2 + 1 \\ y_2 &= x_1^n + x_1 + 1 \end{cases}$$

For other E_i, we can define $\mathcal{C}_{n,i}$ to be the curve in $E_i \times E_i$ cut by $y_2 = x_1^n + x_1 + 1$.

Compute the invariants $h(C)$ and $\deg C$

The $\mathcal{C}_n$ have genus $n+5$, degree $\deg \mathcal{C}_n = 6n+9$ and height:

$$h((\mathcal{C}_n)) \leq 9\left((n+1)\left(\frac{1}{2}\log\left(\frac{|A|^2+3|B|^2+4}{3}\right)+\frac{15}{4}\right)+\frac{1}{2}\log\left(3+\frac{1}{n}\right)\right).$$

Plug the invariants in our non-CM Theorem to get $h(P) \leq$ Number

For every point $P \in \mathcal{C}_n(\mathbb{Q})$ we have

$$\hat{h}(P) \leq 81193n^2 + 238012n + 174343.$$

For a family we need a result of Stoll

This shows that it suffices to check the curves for $n \leq$ Number and the integral points.
For our family only the curves with $n \leq 19$ need to be checked.

Use Belabas Altgorithm to make a computer search and obtain $C(\mathbb{Q})$

The affine rational points on the families $\mathcal{C}_{n,i}(\mathbb{Q})$ are

$$\mathcal{C}_{n,i}(\mathbb{Q}) = \begin{cases} \left\{ \begin{array}{l} ((-1,\pm 1),(0,-1)),((-1,\pm 1), \\ (\pm 1,-1)),((0,\pm 1),(0,1)),((0,\pm 1),(\pm 1,1)), \\ ((5,11),(5,11)) \end{array} \right\}, & \text{if } i=1 \text{ and } n=1 \\ \left\{ \begin{array}{l} ((0,\pm 1),(0,1)),((0,\pm 1),(\pm 1,1)), \\ ((-1,\pm 1),(0,1)),((-1,\pm 1),(\pm 1,1)) \end{array} \right\}, & \text{if } i=1 \text{ and } 2 \mid n \\ \left\{ \begin{array}{l} ((0,\pm 1),(0,1)),((0,\pm 1),(\pm 1,1)), \\ ((-1,\pm 1),(0,-1)),((-1,\pm 1),(\pm 1,-1)) \end{array} \right\}, & \text{if } i=1,\ n \geq 3 \text{ and } 2 \nmid n \\ \{((1,\pm 1),(2,3))\}, & \text{if } i=2 \\ \{((0,\pm 1),(0,1))\}, & \text{if } i=3,4 \\ \{((-1,\pm 1),(-1,1)),((-1,\pm 1),(2,1))\}, & \text{if } i=5 \text{ and } 2 \mid n \\ \{((-1,\pm 1),(-1,-1)),((-1,\pm 1),(2,-1))\}, & \text{if } i=5 \text{ and } 2 \nmid n \\ \{((0,\pm 1),(0,1)),((4,\pm 9),(4,9))\}, & \text{if } i=6 \text{ and } n=1 \\ \{((0,\pm 1),(0,1))\}, & \text{if } i=6 \text{ and } n \neq 1 \end{cases}$$

The CM case (with Veneziano)

Choose an elliptic curve E with CM by K such that $\mathrm{rk}_{\mathbb{Q}} \mathrm{E(K)} = 2$.

For example

$$E : y^2 = x^3 + 2.$$

$E(\mathbb{Q}(\sqrt{-3})) = \langle(-1:1:1),(-\zeta:1:1)\rangle_{\mathbb{Z}}$ has rank 2 as an abelian group.

- But E has CM by $K = \mathbb{Q}(\sqrt{-3})$.
- $\mathrm{End(E)} = \mathbb{Z}[\zeta]$ for $\zeta = \frac{-1+\sqrt{-3}}{2}$ a primitive cube root of 1
- $E(\mathbb{Q}(\sqrt{-3})) = \langle(-1:1:1)\rangle_{\mathbb{Z}[\zeta]}$ has $\mathbb{Z}[\zeta]$-rank 1 with generator $g = (-1:1:1)$.
- The discriminant $D_K = -3$, $O_K = \mathbb{Z}[\zeta]$ and the conductor $f = 1$.

Define a Family in E^2

Example

Consider the family

$$C'_n = \begin{cases} y_1^2 & = x_1^3 + 2 \\ y_2^2 & = x_2^3 + 2 \\ x_1^n & = y_2 \end{cases}$$

- Compute the invariants: the C'_n have genus $4n+2$ and

$$\deg C'_n = 6n+9,$$
$$h(C'_n) \leq 6(2n+3)\log(3+|A|+|B|).$$

- Plug all invariants in our CM theorem to get that for $P \in C'_n(\mathbb{Q}(\sqrt{-3}))$ the height

$$\hat{h}(P) \leq 644391 \cdot (2n+3)^2 + 28$$

- Generalize Stoll's result to number fields to obtain that for $n \geq 21$ then $C'_n(K) = C'_n(\mathcal{O}_K)$.
- Let the search althgorithm of Allombert run to find the points on $C'_n(K)$ for $n \leq 20$.

The $\mathbb{Q}(\sqrt{-3})$-rational points on the C'_n

$$C'_n = \begin{cases} y_1^2 & = x_1^3 + 2 \\ y_2^2 & = x_2^3 + 2 \\ x_1^n & = y_2 \end{cases}$$

Let $g = (-1 : 1 : 1)$. Our explicit bound on the height of $C'_n(\mathbb{Q}(\sqrt{-3}))$ implies:

$$\begin{aligned} & C'_n(\mathbb{Q}(\sqrt{-3})) \setminus \{(O,O)\} = \\ & = \{(ag, bg) \mid a = \pm 1, \pm\zeta, \pm\zeta^2 \text{ and } b = 1, \zeta, \zeta^2\} && \text{if } n \equiv 0 \pmod 6 \\ & = \{(ag, bg) \mid a = \pm 1 \text{ and } b = -1, -\zeta, -\zeta^2\} && \text{if } n \equiv \pm 1 \pmod 6 \\ & = \{(ag, bg) \mid a = \pm 1 \text{ and } b = 1, \zeta, \zeta^2\} && \text{if } n \equiv \pm 2 \pmod 6 \\ & = \{(ag, bg) \mid a = \pm 1, \pm\zeta, \pm\zeta^2, b = -1, -\zeta, -\zeta^2\} && \text{if } n \equiv 3 \pmod 6, \end{aligned}$$

Examples in E^3: find $C(\mathbb{Q})$ for $C \subset E^3$

- Choose E such that $\mathrm{rk}\,\mathrm{E}(\mathbb{Q}) = 2$ and cut C on E^3 with two extra polynomials.
- Choose two polynomials that cut a transverse $C \subset E^N$ and so that $\deg C$ and $h(C)$ are small.
- Estimate $h(C)$ and $\deg C$
- Plug the estimates in our theorem to obtain $\hat{h}(P) \leq$ Number

In general the bound is not implementable

Try to improve the bound choosing a special E, for instance such that the generators of $E(\mathbb{Q})$ are almost orthogonal, sharp comparison of $h(P)$ and $\hat{h}(P)$, some new ideas .... to improve the bound to

$$\hat{h}(P) \leq 10^{15}$$

Then it is implementable.
This gives infinitely many possible master/PhD projects ☺

Irreducible variety V embedded in A

Manin-Mumford
V non-torsion $\Rightarrow S_0 \cap V$ non-dense

$\Uparrow$

Mordell-Lang
$S \leq A$, $\mathrm{rk}(S)$ finite, V non-translate
$\Rightarrow S \cap V$ non-dense

$\Uparrow$

Torsion Anomalous Conjecture (TAC)
V weak-transverse
$\Rightarrow \bigcup V$-anomalous varieties is non-dense in V

(only known for curves, hypersufaces
and for $V \subseteq E^N$ of codimension 2.)

$\Downarrow$

weak TAC, V weak-transverse
$\Rightarrow V \cap S_{N-\dim(V)-1}$ non-dense

Remark: $\mathrm{codim}(V \cap B)$ is expected to be $\mathrm{codim}(V) + \mathrm{codim}(B)$.
If C is a weak-transverse curve, then $C \not\subseteq B$

$\dim(B) = N - 1 \Rightarrow$ expect points in $C \cap B$

$$\dim(B) < N-1 \Rightarrow \begin{cases} \text{expect } C \cap B = \emptyset \\ \text{otherwise } C - \text{anomalous} \end{cases}$$

If V is a weak-transvese variety, we expect that for every component Y of $V \cap B$

$$\mathrm{codim}(Y) = \mathrm{codim}(V) + \mathrm{codim}(B),$$

otherwise Y is anomalous.

Toto Point = Point pools

Exercise

Define a curve C of genus ≥ 2 in E^2 with E an elliptic curve of rank 1 such that C has a rational point of large height. Large height means for instance $\geq 10(h(C)+\deg C)$, or $\gg (h(C)+\deg C)^{\alpha}$ with $1 < \alpha < 2$.

THANK YOU