Rational Points on Curves

- $\overline{\mathbb{Q}}$ algebraic closure of $\mathbb{Q}$.
- k a number field.

Ambient variety:

- Elliptic curve
  E an elliptic curve defined over $\overline{\mathbb{Q}}$.
  $E^N = E \times \cdots \times E$.
- In general
  A an abelian variety defined over $\overline{\mathbb{Q}}$.

For A defined over k, we denote by $A(k)$ the k-rational points of A, (all coordinates in k).
We identify $A = A(\overline{\mathbb{Q}})$.

Tori

$\mathbb{G}_m = \overline{\mathbb{Q}}^*$ the multiplicative group of $\overline{\mathbb{Q}}$
$\mathbb{G}_m^n = \overline{\mathbb{Q}}^* \times \cdots \times \overline{\mathbb{Q}}^*$,

Torsion subgroup of $\mathbb{G}_m^n$

$$\mathrm{Tor}_{\mathbb{G}_m} = \text{Roots of unity} = \{\zeta \in \mathbb{G}_m : \exists N \in \mathbb{N}^*, \zeta^N = 1\}$$
$$\mathrm{Tor}_{\mathbb{G}_m^n} = \{(\zeta_1, \cdots, \zeta_n) \in \mathbb{G}_m^n : \zeta_i \in \mathrm{Tor}_{\mathbb{G}_m}\}$$

Finitely generated subgroup Γ of $\mathbb{G}_m^n$

Algebraic subgroups of $\mathbb{G}_m^n$

- An algebraic subgroup B of dimension $n-s$ is the kernel of a matrix $\phi_B \in \mathrm{Mat}_{s,n}(\mathbb{Z})$ of rank s

$$\phi_B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \vdots & \vdots \\ b_{s1} & \dots & b_{sn} \end{pmatrix} : \mathbb{G}_m^n \to \mathbb{G}_m^s$$

$$\phi_B : (x_1, \dots, x_n) \to (x_1^{b_{11}} \cdot \dots \cdot x_n^{b_{1n}}, \dots, x_1^{b_{s1}} \cdot \dots \cdot x_n^{b_{sn}}).$$

- Up to constants, $\deg B$ is the maximal Minor of ϕ_B.
- Choosing ϕ_B appropriately, $\deg B$ is up to constant $||b_1|| \dots ||b_s||$.

Remark

- There are only finitely many algebraic subgroups of bounded degree.
- $\mathrm{Tor}_{\mathbb{G}_m^n} = \cup_{\dim B=0} B$.
- $\cup_{\dim B=0} B \subset \cup_{\dim B\leq 1} B \cdots \subset \cup_{\dim B\leq n-1} B$.

Cuves in Tori

Let C be an algebraic curve embedded in $\mathbb{G}_m^n$.

Questions

- When is $C \cap \mathrm{Tor}_{\mathbb{G}_m^n}$ finite?
- When is $C \cap \Gamma$ finite?
- When is $C \cap \cup_{\dim B \leq r} B$ finite?

Note that if $C = \mathbb{G}_m \times \zeta_2 \times \cdots \times \zeta_n$ then none of the above sets is finite!!
These are special cases of the toric Manin-Mumford Conjecture, Mordell-Lang Conjecture, Torsion Anomalous Conjecture

Elliptic Case

Let E be an elliptic curve. Consider E^N for some integer N.

Torsion subgroups

$$\mathrm{Tor}_E = \{P \in E : \exists m \in \mathbb{N}^+ \text{ with } mP = 0\}$$
$$\mathrm{Tor}_{E^N} = (\mathrm{Tor}_E)^N$$

Finitely generated subgroup Γ of E^N

Theorem (Mordell-Weil Theorem)

Let k be a number field and let E be defined over k. Then $E(k)$ is finitely generated.
Let A be an abelian variety defined over k. Then $A(k)$ is finitely generated.

Algebraic subgroups of E^N

- An algebraic subgroup B of dimension $n-s$ is the kernel of a matrix $\phi_B \in \mathrm{Mat}_{s,n}(\mathrm{End}(E))$ of rank s

$$\phi_B = \begin{pmatrix} b_{11} & \dots & b_{1,n} \\ \vdots & \vdots & \vdots \\ b_{s,1} & \dots & b_{s,n} \end{pmatrix} : E^N \to E^s$$

$$\phi_B : (x_1, \dots, x_N) \to (b_{11}x_1 + \dots + b_{1N}x_N, \dots, b_{s1}x_1 + \dots + b_{sN}x_N).$$

- Up to constants, $\deg B$ is the square of the maximal Minor of ϕ_B.
- Choosing ϕ_B appropriately, $\deg B$ is up to constants $||b_1||^2 \dots ||b_s||^2$.

Remark

- There are only finitely many algebraic subgroups of bounded degree.
- $\mathrm{Tor}_{E^N} = \cup_{\dim B=0} B$.
- $\cup_{\dim B=0} B \subset \cup_{\dim B\leq 1} B \cdots \subset \cup_{\dim B\leq n-1} B$.

Cuves in E^N

Let C be an algebraic curve embedded in E^N.

Questions

- When is $C \cap \mathrm{Tor}_{E^N}$ finite?
- When is $C(k)$ finite?
- When is $C \cap \cup_{\dim B \leq r} B$ finite?

Note that if $C = E + t$ with t a torsion point, then none of the above sets is finite!!
These are special cases of the Manin-Mumford Conjecture, Mordell-Lang Conjecture, Torsion Anomalous Conjecture

Some Classical results on Curves

Let $C \subset \mathbb{P}^2$ be a curve defined by a homogeneous polynomial

$$P(x, y, z) = 0$$

with coefficients in k.

Geometry	Arithmetic	$C(k)$
Quadrics $g(C) = 0$	$\deg P \leq 2$	$C(k) = \emptyset$ or $C(k)$ infinite
Elliptic curves $g(C) = 1$	$\deg P = 3$ non-singular	$C(k) \cong$ $\mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ (*Mordell-Weil 1922*)
$g(C) \geq 2$	$\deg P \geq 4$ non-singular	$C(k)$ finite (*Faltings 1983*)

Effectivity

The result of Faltings is not effective, in the sense that it does not give any method for finding the points in $C(k)$.

This is due to the non existence of an effective bound for the height of the points in $C(k)$.

Height Function is a measure of the complexity of the coordinates of a point.

$$h : E^N(\overline{\mathbb{Q}}) \to \mathbb{R}^+$$

- On $\mathbb{P}^N(\overline{\mathbb{Q}})$ we consider the logarithmic Weil height.
- On an abelian variety we consider the canonical Néron-Tate height. This is the square of a norm.

Theorem (Northcott Theorem)

A set of bounded (Néron-Tate) height and bounded degree is finite.

Effective Methods

The method of Chabauty-Coleman provides a bound on the number of rational points on curves with Jacobian of $\mathbb{Q}$-rank strictly smaller than the genus.

Example

Flynn gives **explicit** examples: he finds the rational points for a selection of curves of genus 2 with Jacobian of $\mathbb{Q}$-rank 1.

The Manin-Dem'janenko method applies to curves that admit many $\mathbb{Q}$-independent morphisms towards an abelian variety.

Example

Kulesz, Girard, Matera, Schost and others find all rational points on some families of curves: these curves have genus 2 (resp. 3) and elliptic Jacobian of $\mathbb{Q}$-rank 1 (resp. 2) with some special properties. For instance with factors given by a Weierstrass equation $y^2 = x^3 + a^2x$, with a square-free integer and such that the Mordell-Weil group has rank 1.

No explicit height's bound

The bounds for the height must be worked out with *ad hoc* methods case by case and for the technique to be successful the equations of the curve must be of a special shape and small genus.

Joint work with S. Checcoli and F. Veneziano

Let E be an elliptic curve given in the form

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

with A, B algebraic integers.
Let $\hat{h}$ be the Néron-Tate height on E^N.
Let $h(\mathcal{C})$ be the normalised height of $\mathcal{C}$.

Theorem

Let E be an elliptic curve of $\mathbb{Q}$-rank 1. Let $C \subset E^N$ be a curve of genus at least 2. Then $P \in C(\mathbb{Q})$ has height bounded as

$$\hat{h}(P) \leq 4 \cdot 3^{N-2} N! \deg C \left(C_1 h(C) (\deg C) + 4 C_1 c_1 (\deg C)^2 + 2 c_1 \right).$$

Moreover if $N = 2$

$$\hat{h}(P) \leq C_1 \cdot h(C) \deg C + 4 C_1 c_1 (\deg C)^2 + 4 c_1$$

$$C_1 = 145$$

$$c_1 = c_1(E) = 2h_W(A) + 2h_W(B) + 4,$$

Compared with previous bounds

In a previous work, for C not contained in any translate of a subgroup of E^N with $N \geq 3$ then

$$\hat{h}(P) \leq B_1(N)4(N-1)C_1 \cdot h(C)(\deg C)^{N-1} + B_2(N)(N-1)C_2(\deg C)^N + \\ + N^2 C_3$$

where $B_1(N) \geq B_2(N) \geq 10^{27} N^{N^2} (N!)^N$.
While here

$$\hat{h}(P) \leq 4(N-1)C_1 h(C) \deg C + (N-1)C_2(\deg C)^2 + N^2 C_3,$$

Explicit Bounds

Assume that E is without CM, defined over a number field k and that $E(k)$ has rank 1.

Let $(x_1, y_1) \times (x_2, y_2)$ be the affine coordinates of E^2

Corollary

Let $\mathcal{C}$ be the curve given in E^2 cut by the additional equation

$$p(x_1) = y_2,$$

with $p(X) \in k[X]$ a non-constant polynomial of degree n. Then for $P \in \mathcal{C}(k)$ we have

$$\hat{h}(P) \leq 2595\,(h_W(p) + \log n + 4c_1(E))\,(2n+3)^2 + 4c_1(E)$$

where $h_W(p) = h_W(1 : p_0 : \ldots : p_n)$ is the height of the coefficients of $p(X)$ and $c_1 = 2\log(3 + |A| + |B|) + 4$.

$\mathcal{C}$ is transverse. Moreover

$$\deg \mathcal{C} = 6n+9$$

and

$$h(\mathcal{C}) \leq 6(2n+3)\left(h_W(p)+\log n+2c_1(E)\right)$$

For almost all E, the $\mathcal{C}_n$ have genus $4n+2$ and
the $\mathcal{D}_n$ have increasing genus.

Explicit Examples

Definition

Let $\{\mathcal{C}_n\}_n$ be the family of curves $\mathcal{C}_n \subseteq E^2$ defined for $n \geq 1$ via the additional equation

$$x_1^n = y_2.$$

Let $\{\mathcal{D}_n\}_n$ be the family of curves $\mathcal{D}_n \subseteq E^2$ defined for $n \geq 1$ via the additional equation

$$\Phi_n(x_1) = y_2,$$

where $\Phi_n(x)$ is the n-th cyclotomic polynomial.

Choice of the ambient variety:

$$E_1 : y^2 = x^3 + x - 1,$$
$$E_2 : y^2 = x^3 - 26811x - 7320618,$$
$$E_3 : y^2 = x^3 - 675243x - 213578586,$$
$$E_4 : y^2 = x^3 - 110038419x + 12067837188462,$$
$$E_5 : y^2 = x^3 - 2581990371x - 50433763600098.$$

These are five elliptic curves without CM and of rank 1 over $\mathbb{Q}$.

$$\mathcal{C}_n = \begin{cases} y_1^2 & = x_1^3 + x_1 - 1 \quad E_1 \\ y_2^2 & = x_2^3 + x_2 - 1 \quad E_1 \\ {x_1}^n & = y_2 \end{cases}$$

$$\mathcal{D}_n = \begin{cases} y_1^2 & = x_1^3 + x_1 - 1 \quad E_1 \\ y_2^2 & = x_2^3 + x_2 - 1 \quad E_1 \\ \Phi_n(x_1) & = y_2 \end{cases}$$

The $\mathcal{C}_n$ have genus $4n+2$ and the $\mathcal{D}_n$ have increasing genus.

$$\deg \mathcal{C}_n = 6n+9,$$
$$h(\mathcal{C}_n) \le 6(2n+3)\log(3+|A|+|B|).$$

$$\deg \mathcal{D}_n = 6\varphi(n)+9,$$
$$h(\mathcal{D}_n) \le 6(2\varphi(n)+3)\left(2^{\omega_2(n)}\log 2 + 2\log(3+|A|+|B|)\right),$$

where $\varphi(n)$ is the Euler function, $\omega_2(n)$ is the number of distinct odd prime factors of n.

For every $n \geq 1$ and every point $P \in \mathcal{C}_n(\mathbb{Q})$ we have

$$\hat{h}(P) \leq 1301\,(4c_6(E))\,(2n+3)^2 + 4c_6(E).$$

For every $n \geq 2$ and every point $P \in \mathcal{D}_n(\mathbb{Q})$ we have

$$\hat{h}(P) \leq 1302\left(2^{\omega_2(n)}\log 2 + 4c_6(E)\right)(2\varphi(n)+3)^2 + 4c_6(E)$$

were $c_6(E) = \log(3+|A|+|B|)$.

Explit Examples

Example

For the curves $\mathcal{C}_n \subseteq E_1 \times E_1$ we have

$$\mathcal{C}_n(\mathbb{Q}) = \{(1, \pm 1) \times (1, 1)\}.$$

For the curves $\mathcal{C}_n \subseteq E_i \times E_i$ with $i = 2, 3, 4, 5$, we have

$$\mathcal{C}_n(\mathbb{Q}) = \varnothing.$$

Example

For $i = 2, 3, 4, 5$, the curves $\mathcal{D}_n \subseteq E_i \times E_i$ have

$$\mathcal{D}_n(\mathbb{Q}) = \varnothing.$$

For the curves $\mathcal{D}_n \subseteq E_1 \times E_1$ we have

$$\begin{aligned}
\mathcal{D}_1(\mathbb{Q}) &= (2, \pm 3) \times (1, 1) \\
\mathcal{D}_2(\mathbb{Q}) &= (2, \pm 3) \times (2, 3) \\
\mathcal{D}_{3^k}(\mathbb{Q}) &= (1, \pm 1) \times (2, 3) \\
\mathcal{D}_{47^k}(\mathbb{Q}) &= (1, \pm 1) \times (13, 47) \\
\mathcal{D}_{p^k}(\mathbb{Q}) &= \varnothing \text{ if } p \neq 3, 47 \text{ or } p = 2 \text{ and } k > 1 \\
\mathcal{D}_6(\mathbb{Q}) &= (1, \pm 1) \times (1, 1) \text{ and } (2, \pm 3) \times (2, 3) \\
\mathcal{D}_n(\mathbb{Q}) &= (1, \pm 1) \times (1, 1) \text{ if } n \neq 6 \text{ has at least two distinct prime factors.}
\end{aligned}$$

Theorem (Manin-Mumford Conjecture)

Raynaud 1983

Let A be an abelian variety and $\mathrm{Tor_A}$ *its torsion. Let* $C \subset A$ *be a curve of genus* ≥ 2*. Then,*

$$C \cap \mathrm{Tor_A} \text{ is finite.}$$

Theorem (Mordell-Lang Conjecture)

Faltings 1983, Vojta 1996, Hindry 1988

Let $C \subset A$ *of genus at least* 2*. Let* Γ *be a subgroup of A of finite rank. Then*

$$C \cap \Gamma \text{ is finite.}$$

- Mordell-Lang Conjecture implies Manin-Mumford Conjecture
- Mordell-Lang Conjecture + Mordell-Weil Theorem imply $C(k)$ is non dense.

Theorem (Torsion Anomalous Conjecture)

Let C be weak-transverse in A. Then the set

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

Here B ranges over all algebraic subgroups of dimension $\leq N-2$.

Show that

- $C \cap \cup_{\dim B \leq N-2} B$ has bounded height.
- $C \cap \cup_{\dim B \leq N-2} B$ has bounded degree.

Remark

This theorem implies the Mordell-Lang conjecture for curves.

Effective/Explicit Methods For Curves

The proof of the theorem is effective only if

- C is transverse in E^N (i.e. not contained in any translate of an algebraic subgroup of E^N)
  (Use the geometry of numbers and properties of the height)
- **In principle effective** For $N \geq 3$ and C weak-transverse in E^N, E with CM and $C \cap \cup_{\dim B=1} B$.
  (Use a Lehmer type bound)
- **explicit** For $N \geq 2$ and C in E^N of genus at least 2, E without CM and $C \cap \cup_{\dim B=1} B$.
  IMPLEMENTABLE FOR $N = 2$
- **explicit** (preprint 2016) For $N \geq 2$ and C transverse in E^N and $C \cap \cup_{\dim B \leq N-1} B$.

This explicit result implies new cases of the Effective Mordell Conjecture.

- Let C be transverse in E^N and rank of $E(k) \leq N-1$.
  Then $C(k)$ has height bounded by an explicit constant.

Normalized Height

- The height of a subvariety V of A is its normalized height.

The normalized height of an algebraic subgroup is 0.

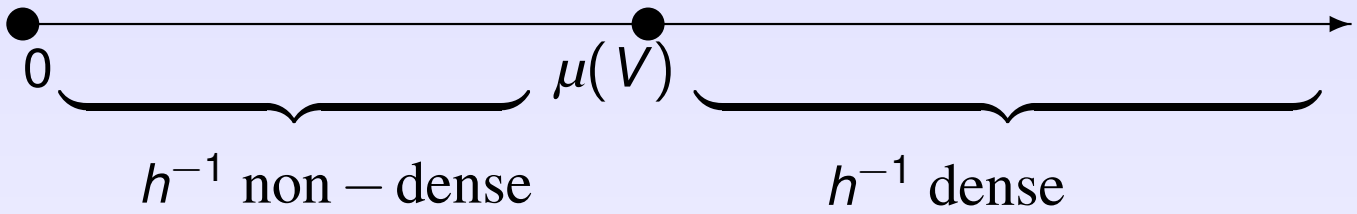
Theorem (Arithmetic Bézout Theorem)

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

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

Essential Minimum

Definition:
$h : V \to \mathbb{R}^+$



Essential Minimum

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

Theorem (Zhang Inequality)

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

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