Using abelian varieties for diophantine definitions of rings of integers

Bjorn Poonen

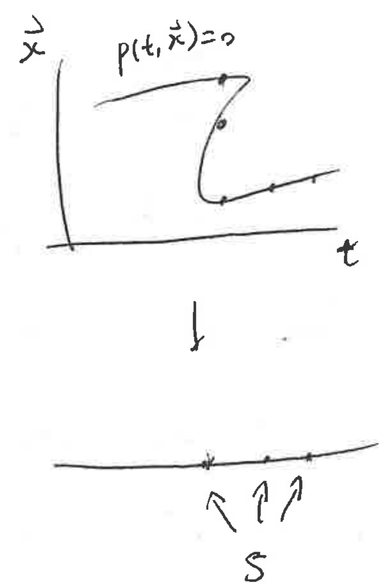
Diophantine sets

$$\begin{tikzcd} K \arrow[r, phantom, "\supset"] \arrow[d, dash] & \mathcal{O} = \mathcal{O}_K = \text{ring of integers of } K \arrow[d, dash] \\ \mathbb{Q} \arrow[r, phantom, "\supset"] & \mathbb{Z} \end{tikzcd}$$

<u>Def</u> $S \subset \mathcal{O}$ is <u>$\mathcal{O}$-diophantine</u> if $\exists\ p(t, \vec{x}) \in \mathcal{O}[t, \vec{x}]$ s.t.

$$S = \{ a \in \mathcal{O} : \exists\, \vec{x} \in \mathcal{O}^n,\ p(a, \vec{x}) = 0 \}$$

$=$ projection of $\{$zeroes of p in $\mathcal{O}^{n+1}\}$ onto the 1^{st} coordinate.



More generally, X finite type $\mathcal{O}$-scheme

$S \subset X(\mathcal{O})$ is <u>$\mathcal{O}$-diophantine</u> if $S = f(Y(\mathcal{O}))$ for some $Y \xrightarrow{f} X$ finite type

<u>Goal</u>. $K \subset L$ no. field. A abelian variety $/K$ s.t. $0 < \operatorname{rank} A(K) = \operatorname{rank} A(L)$

Then $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine.

<u>Preliminaries</u> <u>Prop</u>. $\mathcal{O} - \{0\}$ is $\mathcal{O}$-diophantine.

For simplicity, assume $\mathcal{O} = \mathbb{Z}$.

Lemma. For any nonzero $N \in \mathbb{Z}$, $\exists\, x \in \mathbb{Z}$ w/ $(2x-1)(3x-1) \equiv 0 \pmod N$

Proof. Case 1. $N = p^n$ for some $p \neq 2$. Chose x s.t. $N \mid 2x-1$.

Case 2. $N = p^n$ for some $p \neq 3$ Chose x s.t. $N \mid 3x-1$.

General case: Chinese Reminder theorem.

Proof that $\mathbb{Z}-\{0\}$ is $\mathbb{Z}$-diophantine.

$N \neq 0 \iff \exists\, x, y \in \mathbb{Z}$ s.t. $(2x-1)(3x-1) = yN$.

Elts of K can be represented as $\frac{a}{b}$ ← elts of $\mathcal{O}$

$b \neq 0$.

So we may

- use K-valued vars in $\mathcal{O}$-dioph. defs
- talk about $\mathcal{O}$-dioph. subsets of $X(K)$ for any f.type K-scheme X

Each $I \subset \mathcal{O}$ can be encoded as (i_1, i_2) for some $i_1, i_2 \in \mathcal{O}$

- $a \in I \iff \exists\, x, y \in \mathcal{O}$, $a = x i_1 + y i_2$
- $J \mid I \iff i_1, i_2 \in J$
- $I = J \iff I \mid J$ & $J \mid I$
- I, J coprime
- For $s = \frac{a}{b} \in K$, $(s) = \frac{I}{J} \iff bI = aJ$.
- $I = \mathrm{num}(s) \iff \exists J$ s.t. $(s) = \frac{I}{J}$ and I, J coprime.
- $a \equiv b \pmod I \iff a - b \in I$
- Def: $a \equiv' b \pmod I \iff I \mid \mathrm{num}(a-b)$

  ↖ elts of K

<u>Example for $\mathbb{Z} \subset \mathbb{Z}[i]$</u>

If $\alpha \in \mathbb{Z}[i]$, $|\alpha| < 5$, $\alpha \equiv k \pmod{10\mathbb{Z}[i]}$ for some $k \in \mathbb{Z}$.

then $\alpha \in \mathbb{Z}$

<u>Lemma 1.</u> Fix $K \subset L$. There exists $n \geq 1$ s.t. for all $\alpha \in \mathcal{O}_L$, all nonzero ideals $I \subset \mathcal{O}_K$, all $k \in K$, $(\alpha-1)\cdots(\alpha-n) \mid I\mathcal{O}_L$ and $\alpha \equiv' k \pmod{I\mathcal{O}_L} \Rightarrow \alpha \in \mathcal{O}_K$.

K no field. $\mathfrak{p} \subset \mathcal{O}$ prime ideal, $K_\mathfrak{p}$ = completion.

<u>Def</u> $S \subset K$

S <u>weakly approximate $\mathbb{Z}$</u> $\Leftrightarrow$ $\mathbb{Z} \subset$ closure of S in $\prod_\mathfrak{p} K_\mathfrak{p}$

$\Leftrightarrow$ $\forall k \in \mathbb{Z}$, $\forall$ primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$, $\exists$ sequence in S converging to k in $K_{\mathfrak{p}_i}$ simultaneously.

$\Leftrightarrow$ $\forall k \in \mathbb{Z}$, $\forall$ nonzero ideal $I \subset \mathcal{O}_K$, the congruence $x \equiv' k \pmod I$ has a solution x in S.

<u>Lemma 2.</u> If S weakly approximate $\mathbb{Z}$ and $\beta \in \mathcal{O} - \{0\}$, then $\exists\, s \in S$ w/ $\beta \mid \mathrm{num}(s)$.

<u>Proof.</u> The congruence $x \equiv' 0 \pmod \beta$ has a solution in S.

For this talk, suppose that A is an elliptic curve: $y^2 = x^3 + ax + b$ (a, b elt of K)

$A(K) < A(L)$ are f.g. abelian groups of the same rank.

($A(K)$ finite index, say r)

Then $A(K)$ is a finite union of cosets of $rA(L)$ in $A(L)$.

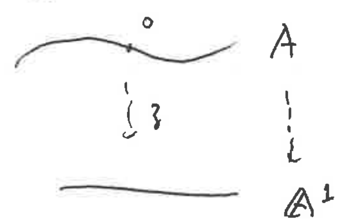
So $A(K)$ is $\mathcal{O}_L$- diophantine.

<u>Step 1</u>. $\exists$ infinite $\mathcal{O}_L$- dioph. subset $T \subset K$.

<u>Proof</u>. Let $T = x\left(A(K)\right)$.

<u>Step 2</u>. $\exists$ $\mathcal{O}_L$- dioph. subset $S \subset K$ that weakly approx. $\mathbb{Z}$.

<u>Pf</u>. Let $S = \left\{ \frac{z(Q)}{z(P)} : P, Q \in A(K) \right\} \subset K$



By defn, S is $\mathcal{O}_L$- dioph.

Suppose $k \in \mathbb{Z}$, For any $p \in \mathcal{O}_K$, $\lim\limits_{\substack{R \to 0 \\ \text{in } A(K_p)}} \frac{z(kR)}{z(R)} = k$.

Let $a \in A(K)$ be a point of infinite order. Then as $N \to \infty$, $N!a \to 0$ in $A(K_p)$ since $A(K_p)$ is a profinite group. Thus $\frac{z(k\,N!a)}{z(N!a)} \to k$ in K_p for every p

<u>Step 3</u>. $\exists$ $\mathcal{O}_L$ -dioph. U w/ $\mathbb{Z} \subset U \subset \mathcal{O}_K$.

<u>Pf</u>. Let $V = \left\{ \alpha \in \mathcal{O}_L : \begin{array}{l} \exists\, k \in S,\ \exists\, s \in S \text{ s.t. } I = \mathrm{num}(s) \text{ satisfies} \\ (\alpha-1)\cdots(\alpha-n) \mid I\mathcal{O}_L \text{ and } \alpha \equiv' k \pmod{I} \end{array} \right\}$

<u>Claim</u>. $\mathbb{Z} - \{1, 2, \cdots, n\} \subset V \subset \mathcal{O}_K$
$\uparrow$ Lemma 1.

If $\alpha \in \mathbb{Z} - \{1, 2, \cdots, n\}$, — By Lemma 2. $\exists s \in S$ s.t. $(\alpha-1)\cdots(\alpha-n) \mid I\mathcal{O}_L = \mathrm{num}(s)$

- By weak approximation, $\exists\, k \in S$ s.t. $k \equiv' \alpha \pmod{I}$

Thus $\alpha \in V$. Let $U = V \cup \{1, 2, \cdots, n\}$.

<u>Step 4.</u> $\mathcal{O}_K$ is $\mathcal{O}_L$- diophantine.

<u>Pf.</u> Let $b_1, \cdots, b_{[K:\mathbb{Q}]}$ be a $\mathbb{Z}$- basis of $\mathcal{O}_K$.

$$\mathcal{O}_K = \sum \mathbb{Z} b_i \subset \underbrace{\sum U b_i}_{\mathcal{O}_L\text{- dioph.}} \subset \mathcal{O}_K$$

$\Leftarrow$ equality everywhere.

$\mathcal{O}_K = \sum U b_i$ is $\mathcal{O}_L$- dioph.