Introduction to Chabauty's method and Kim's nonabelian generalization

Bjorn Poonen March 7, 2020

Rational points

<u>Faltings's theorem</u> (originally the Mordell conjecture)

$[K:\mathbb{Q}] < \infty$

X nice curve of genus g over K

smooth, projective, geom. integral

If $g > 1$, then $X(K)$ is finite.

Proofs by
- Faltings 1983 (Arakelov methods)
- Vojta 1991 (variant by Bombieri) (dioph. approx.)
- Lawrence-Venkatesh 2018+ (p-adic period maps)

Integral points

Siegel's theorem

$[K:\mathbb{Q}] < \infty$

$\mathcal{O} = \mathcal{O}_{K,S} := \{x \in K : v(x) \geq 0 \text{ for all } v \notin S\}$

S: f. set of places of K, including all the arch. places

$U := X - Z$ over K

X: nice curve of genus g

Z: nonempty 0-dim subscheme

$\chi(U) := (2-2g) - r$, where $r := \# Z(\overline{K})$

$\mathcal{U}$ f.type $\mathcal{O}$-scheme with $\mathcal{U}_K \simeq U$

If $\underbrace{\chi(U) < 0}_{U \text{ is hyperbolic}}$, then $\mathcal{U}(\mathcal{O})$ is finite.

[over $\mathbb{C}$, $\widetilde{U} \simeq \mathfrak{h}$]

Proofs by
- Siegel 1929

* Baker - Coates 1970 when $g \leq 1$ or U is $y^2 = f(x)$ in $\mathbb{A}^2$

- Lawrence - Venkatesh 2018+ when $U = \mathbb{P}^1 - \{0, 1, \infty\}$.

Example: $U = \mathbb{P}^1 - \{0,1,\infty\}$

$$\mathcal{U} = \operatorname{Spec} \mathcal{O}\left[x, \frac{1}{x}, \frac{1}{1-x}\right]$$

$$\mathcal{U}(\mathcal{O}) = \left\{ \text{solutions to } x+y=1 \text{ with } x,y \in \mathcal{O}^\times \right\}$$

Remark: Faltings $\Longrightarrow$ Siegel

(Key: If $\chi(U) < 0$, then some f. étale cover of U is open in a nice curve of genus > 1.)

In Siegel-Faltings,

$\chi(U) < 0$ means
- $g = 0$, $r \geq 3$
- $g = 1$, $r \geq 1$
- $g \geq 2$, r arbitrary

Chabauty's method

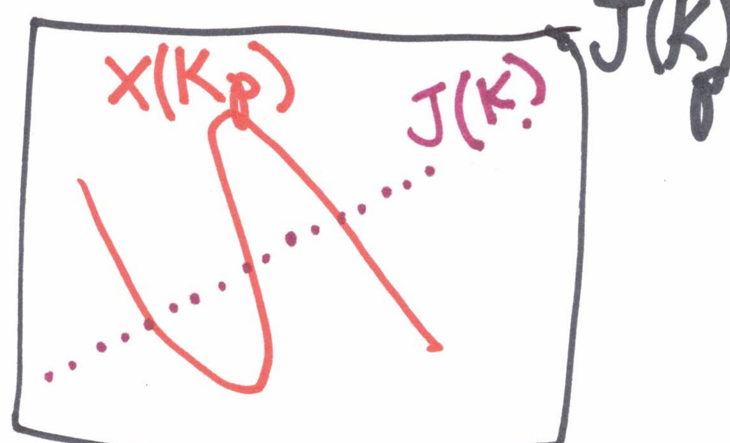
$$\begin{array}{ccc} K & & \mathfrak{p} \\ | & & \\ \mathbb{Q} & & p \end{array}$$

X nice curve of genus g over K ~~with good reduction at $\mathfrak{p}$~~

$J := \operatorname{Jac} X$ g-dim abelian variety

$r := \operatorname{rk} J(K)$

Choose $x \in X(K)$ to get $X \hookrightarrow J$.



$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(K_{\mathfrak p}) \arrow[d] & & \\ J(K) \arrow[r] & J(K_{\mathfrak p}) \arrow[r, "\log"] & \operatorname{Lie} J_{K_{\mathfrak p}} \simeq K_{\mathfrak p}^g \end{tikzcd}$$

$\ker(\log)$ is finite

$\operatorname{im}(\log)$ is compact open subgp.

$\operatorname{image}(J(K) \to K_{\mathfrak p}^g)$ is generated by r elts.

$\dim_{K_{\mathfrak p}} (K_{\mathfrak p}\text{-span of image}(\cdots)) \le r$

If $r < g$,

$\exists$ nonzero linear $\lambda : \operatorname{Lie} J_{K_p} \to K_p$

vanishing on $\operatorname{im} J(K)$,

and λ pulls back to a nonzero locally analytic function on $X(K_p)$

vanishing on $X(K)$,

so $X(K)$ is finite.

Goal: Get rid of J

in order to generalize.

Rewriting

Bad

Good

$$
\begin{tikzcd}
X(K) \arrow[rr] \arrow[d] & & X(K_p) \arrow[d] & \\
J(K) \arrow[rr] \arrow[d] & & J(K_p) \arrow[r, "\log"] \arrow[d] & \mathrm{Lie}\, J_{K_p} \\
\widehat{J(K)}\left[\frac{1}{p}\right] \arrow[rr] \arrow[d] & & \widehat{J(K_p)}\left[\frac{1}{p}\right] \arrow[ur, "\sim"'] \arrow[d] & \\
\mathrm{Sel}_{\mathbb{Q}_p} J \arrow[r, phantom, "\simeq"] \arrow[d] & H^1_f(K,V) \arrow[r] & H^1_f(K_p,V) \arrow[r, "\log_{BK}", "\sim"'] \arrow[d] & H^{dR}_1(X_{K_p})/\mathrm{Fil}^0 \\
H^1(K,V) \arrow[rr] & & H^1(K_p,V) &
\end{tikzcd}
$$

Given M abelian group

define $\hat{M} := \varprojlim M/p^n M$ $\mathbb{Z}_p$-module

$\hat{M}[\frac{1}{p}] \cong \hat{M} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ $\mathbb{Q}_p$-v.space

V is étale homology

Motivation:

X over $\mathbb{C}$

J

Then $J(\mathbb{C}) \overset{\text{analytically}}{\simeq} \mathbb{C}^g / \Lambda$

where $\Lambda = H_1(J(\mathbb{C}), \mathbb{Z})$

and $J[p] \simeq \frac{1}{p}\Lambda / \Lambda \xrightarrow[\sim]{p} \Lambda / p\Lambda$

$= H_1(J(\mathbb{C}), \mathbb{Z}/p\mathbb{Z})$

$= H_1(X(\mathbb{C}), \mathbb{Z}/p\mathbb{Z}).$

For X over K,

$$J[p] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z}) := \mathbb{Z}/p\mathbb{Z}\text{-dual of } H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$$

Likewise,

$$J[p^n] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z})$$

$\varprojlim$

$\mathbb{Z}_p$ Tate module

$$T := \varprojlim J[p^n] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$$

$\mathbb{Q}_p$ Tate module

$$V := T[\tfrac{1}{p}] = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$$

$\mathbb{Q}_p$-v. space of dim $2g$

$$\|$$

$\mathcal{V}(\mathbb{Q}_p)$ for a group variety $\mathcal{V} \simeq \mathbb{G}_a^{2g}$ over $\mathbb{Q}_p$

($\mathbb{A}^{2g}$ with additive group law)

$G_K := \mathrm{Gal}(\overline{K}/K)$ acts continuously on all of these

e.g. $G_K \longrightarrow \mathrm{Aut}_{\text{gp. var.}} \mathcal{V} \simeq GL_n(\mathbb{Q}_p)$

Selmer groups

$$0 \to J[p] \longrightarrow J \xrightarrow{p} J \longrightarrow 0$$

$$J(K) \xrightarrow{p} J(K) \to H^1(K, J[p])$$

$$\begin{tikzcd}
\dfrac{J(K)}{pJ(K)} \arrow[r, hook] \arrow[d] & \mathrm{Sel}_p J \subset H^1(K, J[p]) \arrow[d, "\beta"'] \\
\prod_v \dfrac{J(K_v)}{pJ(K_v)} \arrow[r, hook, "\alpha"] & \prod_v H^1(K_v, J[p])
\end{tikzcd}$$

infinite-dim $\mathbb{F}_p$-v. space (if $\dim J > 0$)

$\cancel{\mathrm{Sel}_p V}$: $\mathrm{Sel}_p J := \{ \xi \in H^1(K, J[p]) : \beta(\xi) \in \mathrm{im}(\alpha) \}$

Similarly,

$$\frac{J(K)}{p^n J(K)} \hookrightarrow \mathrm{Sel}_{p^n} J \subset H^1(K, J[p^n])$$

finite and computable!

lim

$$\widehat{J(K)} \hookrightarrow \mathrm{Sel}_{\mathbb{Z}_p} J \subset H^1(K, T)$$

invert p

$$\widehat{J(K)}\left[\tfrac{1}{p}\right] \hookrightarrow \mathrm{Sel}_{\mathbb{Q}_p} J \subset H^1(K, V)$$

Have

$$0 \to \frac{J(K)}{pJ(K)} \to \mathrm{Sel}_p J \to Ш[p] \to 0$$

Shafarevich-Tate gp.

$$0 \to \widehat{J(K)}\left[\tfrac{1}{p}\right] \to \mathrm{Sel}_{\mathbb{Q}_p} J \to \underbrace{\left(\varprojlim Ш[p^n]\right)\left[\tfrac{1}{p}\right]}_{0 \text{ if } Ш[p^\infty] \text{ is finite}} \to 0$$

Bloch–Kato Selmer group (in terms of V, not J)

General setting (local Galois repr.):

V f.dim $\mathbb{Q}_p$-v.space with conts. action G_{K_v}-action

$$D_{cris}(V) := \left(B_{cris} \otimes_{\mathbb{Q}_p} V\right)^{G_{K_v}}$$

a certain ring equipped w. a G_{K_v}-action

Fact: $\dim_{K_v} D_{cris}(V) \leq \dim_{\mathbb{Q}_p} V$

Call V crystalline if equality holds.

Fact: Fix v and an ab. var. J/K_v.
Then J has good reduction
$\iff$ its $\mathbb{Q}_p$ Tate module V
is $\begin{cases} \text{unram. if } v \nmid p \\ \text{crystalline if } v \mid p \end{cases}$

Now suppose $\xi \in H^1(K_v, V)$

Let
$$0 \to V \to E \to \underset{\text{trivial action}}{\mathbb{Q}_p} \to 0$$
be the corresponding extension.

Call ξ <u>crystalline</u> if E is crystalline.

$$H^1_f(K_v, V) := \{\text{crystalline classes in } H^1(K_v, V)\}$$

<u>Fact.</u> $\mathfrak{p} \mid p$

J ab. var. w. good red. at $\mathfrak{p}$

V $\mathbb{Q}_p$ Tate module

Then the image of

$$J(K_\mathfrak{p})[\tfrac{1}{p}] \longrightarrow H^1(K_\mathfrak{p}, V)$$

equals $H^1_f(K_\mathfrak{p}, V)$.

(If $\mathfrak{p} \nmid p$, then $H^1(K_\mathfrak{p}, V) = 0$)

General setting (global Galois repr.)

V f. dim $\mathbb{Q}_p$-v. space with conts G_K-action

Given $\xi \in H^1(K,V)$, let ξ_v be its image in $H^1(K_v,V)$.

Bloch-Kato Selmer gp:

$$H^1_f(K,V) := \{\xi \in H^1(K,V) : \xi_v \text{ is crystalline for all } v \mid p\}.$$

Fact: J ab. var. $/K$ w. good red. above p

V $\mathbb{Q}_p$ Tate module

Then $H^1_f(K,V) = \mathrm{Sel}_{\mathbb{Q}_p} J$.

algebraic de Rham cohom. $H^1_{dR}(X) := \mathbb{H}^1(X, \Omega^\bullet)$

hypercohomology

with Hodge filtration Fil

$H_1^{dR}(X) :=$ dual of H^1_{dR} with dual filtration

$\boxed{\text{Upshot}}$ Assume X has good red. above p, from now on.

Get

$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(K_p) \arrow[d] \arrow[dr, bend left, "p\text{-adic integrals}"] & \\ H^1_f(K,V) \arrow[r] & H^1_f(K_p,V) \arrow[r, "\sim"] & H_1^{dR}(X_{K_p})/\mathrm{Fil}^0 \end{tikzcd}$$

Lower central series

G (~~top.~~) group

For $A, B \leq G$, let $(A,B) := \langle aba^{-1}b^{-1} : a \in A, b \in B \rangle$

Lower central series

$$C^1G := G$$
$$\mathrel{\rotatebox{90}{$\leq$}}$$
$$C^2G := (G, C^1G) = (G,G)$$
$$\mathrel{\rotatebox{90}{$\leq$}}$$
$$C^3G := (G, C^2G)$$
$$\mathrel{\rotatebox{90}{$\leq$}}$$
$$\vdots$$

$$G_n := G / C^{n+1}G$$

~~n~~-step nilpotent gp.

Example:

$$G_1 = G/(G,G) =: G^{ab}$$

<u>abelianization</u> of G

(largest abelian quotient)

Abelianized fundamental group

Motivation:

Given M connected real manifold, $m \in M$

get

$$\underbrace{\pi_1(M, m)}_{\text{fund. gp.}}{}^{ab} \simeq H_1(M, \mathbb{Z})$$

Algebraic version:

Given X nice genus g curve$/K$, $x \in X(K)$

$$\begin{tikzcd}
 & \pi_1^{\text{ét}}(X_{\overline{K}}, x)^{ab} \arrow[r, phantom, "\simeq"] & H_1^{\text{ét}}(X_{\overline{K}}, \hat{\mathbb{Z}}) \arrow[d, two heads] \\
\pi_1^{\text{ét}}(X_{\overline{K}}, x)_1 \arrow[ur, phantom, "\wr"] & & H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \arrow[d, phantom, "\cap"] \\
 & & H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) =: V \arrow[d, phantom, "\parallel"] \\
 & & \mathcal{V}(\mathbb{Q}_p)
\end{tikzcd}$$

compatible with G_K-actions

Deeper quotients

Kim obtains a generalization

$$\pi_1^{\text{ét}}(X_{\bar{K}}, x) \longrightarrow V_n = \mathcal{V}_n(\mathbb{Q}_p)$$

some unipotent algebraic gp

and

$$\begin{tikzcd}
X(K) \arrow[r] \arrow[d] & X(K_p) \arrow[d] \arrow[dr, "p\text{-adic iterated integrals (Zar. dense image)}"] & \\
H^1_f(K, V_n) \arrow[r] & H^1_f(K_p, V_n) \arrow[r, "\simeq"] & \pi_1^{dR}(X_{K_p}, x)_n / \mathrm{Fil}^0
\end{tikzcd}$$

and morphisms of $\mathbb{Q}_p$-varieties

$$\mathrm{Sel}^{[n]} \longrightarrow J^{[n]} \longrightarrow L^{[n]}$$

$\mathbb{Q}_p$-pts

__Thm.__ (Kim) If for some $n \geq 1$, $\dim \mathrm{Sel}^{[n]} < \dim J^{[n]}$ then $X(K)$ is contained in the set of zeros of some nonzero loc. analytic functions on $X(K_p)$, so $X(K)$ is finite.