Lecture 1: Descent & Chabauty–Coleman

Diophantine Geometry is the study of rational points on varieties over $\mathbb{Q}$ (or any number field)

Theorem Let $X/\mathbb{Q}$ be a smooth projective curve of genus g.

- If $g=0$, then either $X(\mathbb{Q})=\emptyset$ or $\#X(\mathbb{Q})=\infty$.
- If $g=1$, then either $X(\mathbb{Q})=\emptyset$ or $X(\mathbb{Q})$ is a finitely generated abelian group (MORDELL-WEIL)
- If $g\geq 2$, then $\#X(\mathbb{Q})<\infty$ (FALTINGS).

In genus 0, $X(\mathbb{Q})\neq\emptyset$ iff $X(\mathbb{R})\neq\emptyset$ and $X(\mathbb{Q}_p)\neq\emptyset$ for all p (HASSE-MINKOWSKI).

In higher genus this fails (LIND, REICHARDT, SELMER, ...) but we can still ask

$$\boxed{\text{Where does } X(\mathbb{Q}) \text{ lie inside } X(\mathbb{A}^f_{\mathbb{Q}})=\prod_p X(\mathbb{Q}_p)?}$$

This is the subject of obstruction theory

Descent on elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve.

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^{rk(E(\mathbb{Q}))}$$

MAZUR BIRCH—SWINNERTON-DYER

For $n \in \mathbb{N}$ we have the KUMMER sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0$$

Galois cohomology $\rightsquigarrow$ KUMMER map

$$E(\mathbb{Q}) \xrightarrow{[n]} E(\mathbb{Q}) \xrightarrow{\kappa_n} H^1(G_{\mathbb{Q}}, E[n])$$

For ℓ prime (or ∞) also have local Kummer map

$$\kappa_{n,\ell} : E(\mathbb{Q}_\ell) \longrightarrow H^1(G_\ell, E[n])$$

decomposition group @ℓ.

Gives the <u>descent square</u>

$$\begin{tikzcd}
E(\mathbb{Q}) \arrow[r, hook] \arrow[d, "\kappa_n"] & \prod_\ell E(\mathbb{Q}_\ell) \arrow[d, "\prod \kappa_{n,\ell}"] \\
H^1(G_{\mathbb{Q}}, E[n]) \arrow[r, "\prod loc_\ell"] & \prod_\ell H^1(G_\ell, E[n])
\end{tikzcd}$$

localization/restriction map

So $E(\mathbb{Q})$ lies in the "intersection" of $H^1(G_{\mathbb{Q}}, E[n])$ and $E(\mathbb{A}_{\mathbb{Q}}) = \prod_\ell E(\mathbb{Q}_\ell)$.

<u>Definition</u>

1) The <u>n-SELMER group</u> is

$$\mathrm{Sel}^{(n)}(E/\mathbb{Q}) := \{ \xi \in H^1(G_{\mathbb{Q}}, E[n]) : \mathrm{loc}_\ell(\xi) \in \mathrm{im}(K_{n,\ell}) \ \forall \ell \}$$

2) The <u>n-descent locus</u> is

$$E(\mathbb{A}_{\mathbb{Q}})^{(n)} = \{ (x_\ell)_\ell \in \prod_\ell E(\mathbb{Q}_\ell) : \exists \xi \in H^1(G_{\mathbb{Q}}, E[n]) \text{ with } \mathrm{loc}_\ell(\xi) = K_{n,\ell}(x_\ell) \ \forall \ell \}$$

Note: $E(\mathbb{Q}) \subseteq E(\mathbb{A}_{\mathbb{Q}})^{(n)} \subseteq E(\mathbb{A}_{\mathbb{Q}})$

so $E(\mathbb{A}_{\mathbb{Q}})^{(n)}$ constrains where $E(\mathbb{Q})$ can lie in $E(\mathbb{A}_{\mathbb{Q}})$

<u>Theorem</u> (STOLL) If $Ш(E/\mathbb{Q})$ is finite, then $\bigcap_n E(\mathbb{A}_{\mathbb{Q}})^{(n)}$ is the intersection of all clopen subsets of $E(\mathbb{A}_{\mathbb{Q}})$ containing $E(\mathbb{Q})$

CHABAUTY's method

Another way to constrain rational points was developed by Claude CHABAUTY in 1941, using p-adic integration on Abelian varieties.

Let $A/\mathbb{Q}_p$ be an abelian variety, $\omega \in H^0(A, \Omega^1)$, $t_1, \dots, t_g$ local parameters at $O \in A(\mathbb{Q}_p)$.

Working in the complete local ring at O, we can write

$$\omega = \sum_{i=1}^{g} f_i \, dt_i \quad , \quad f_i \in \mathbb{Q}_p[[t_1, \dots, t_g]]$$

As ω is closed, $\frac{\partial f_i}{\partial t_j} = \frac{\partial f_j}{\partial t_i}$ so $\exists F_0 \in \mathbb{Q}_p[[t_1, \dots, t_g]]$ with $dF_0 = \omega$. F_0 converges on a neighbourhood $O \in U \subseteq A(\mathbb{Q}_p)$

<u>Definition</u>: If $P \in U$, define

$$\int_O^P \omega := F_0(t_1(P), \dots, t_g(P)).$$

In general $\int_O^P \omega := \frac{1}{n} F_0(t_1(nP), \dots, t_g(nP))$ for $nP \in U$.

<u>Fact</u>: the map
$$
\begin{aligned}
F : A(\mathbb{Q}_p) &\longrightarrow \mathbb{Q}_p \\
P &\longmapsto \int_0^P \omega
\end{aligned}
$$
is locally analytic and $dF = \omega$.

The pairing
$$
\begin{aligned}
A(\mathbb{Q}_p) \times H^0(A, \Omega^1) &\longrightarrow \mathbb{Q}_p \\
(P, \omega) &\longmapsto \int_0^P \omega
\end{aligned}
$$
is bilinear.

Can pull this back to integration theory on curves. Let $X/\mathbb{Q}_p$ be a curve, $J = \mathrm{Jac}(X)$, so $H^1(X, \Omega^1) = H^1(J, \Omega^1)$.

<u>Definition</u>: For $x, y \in X(\mathbb{Q}_p)$, $\omega \in H^0(X, \Omega^1)$
$$
\int_x^y \omega := \underbrace{\int_0^{[y]-[x]} \omega}_{\text{integral on } J}
$$

For fixed $b \in X(\mathbb{Q}_p)$, the map
$$
\begin{aligned}
F : X(\mathbb{Q}_p) &\longrightarrow \mathbb{Q}_p \\
x &\longmapsto \int_b^x \omega
\end{aligned}
$$
is locally analytic and $dF = \omega$.

Theorem (CHABAUTY) Let $X/\mathbb{Q}$ be a curve. Suppose $rk(J(\mathbb{Q})) < g = g(X)$. $(*)$
Then $\# X(\mathbb{Q}) < \infty$.

Proof: $(*) \Rightarrow$ the map

$$\Phi : H^0(X_{\mathbb{Q}_p}, \Omega^1) = H^0(J_{\mathbb{Q}_p}, \Omega^1) \to \mathrm{Hom}(J(\mathbb{Q}), \mathbb{Q}_p)$$
$$\omega \longmapsto \left(P \longmapsto \int_0^P \omega\right)$$

is not injective. If $0 \neq \omega \in \ker(\Phi)$, then for fixed $b \in X(\mathbb{Q})$ we have that the map

$$F : X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$
$$x \longmapsto \int_b^x \omega$$

vanishes on $X(\mathbb{Q})$. F is locally analytic, and F doesn't vanish uniformly on any disc, as $dF = \omega \neq 0$. So F has only finitely many zeroes. $\square$

Rmk: If we define $X(\mathbb{Q}_p)_{Chab} = \{x \in X(\mathbb{Q}_p) : \int_b^x \omega = 0 \ \forall \omega \in \ker(\Phi)\}$

then $X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_{Chab} \subseteq X(\mathbb{Q}_p)$.

Rmk: COLEMAN observed that one can often compute a basis of $\ker(\Phi)$ up to any desired p-adic precision, and use this to explicitly compute $X(\mathbb{Q})$ in some cases.

Thm (COLEMAN) Suppose $\mathrm{rk}(J(\mathbb{Q})) < g$ and X has good reduction at $p > 2g$. Then $\#X(\mathbb{Q}) < \#X(\mathbb{F}_p) + 2g - 2$.

CHABAUTY–COLEMAN as $\mathbb{Q}_p$-linear descent

Although CHABAUTY's method and descent seem very different, they are actually closely related.

Let $A/\mathbb{Q}$ be an abelian variety, p prime. $g = \dim A$

<u>Definition</u>: • The <u>$\mathbb{Z}_p$-linear Tate module</u> is

$$T_p A := \varprojlim_n A[p^n] = \varprojlim \left(\dots \to A[p^3] \xrightarrow{[p]} A[p^2] \to A[p] \right)$$
$$\simeq \mathbb{Z}_p^{2g}$$

• The <u>$\mathbb{Q}_p$-linear Tate module</u> is

$$V_p A := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p A \simeq \mathbb{Q}_p^{2g}$$

Taking the inverse limit of the level p^n KUMMER maps gives a <u>$\mathbb{Q}_p$-linear KUMMER map</u>

$$K : A(\mathbb{Q}) \longrightarrow H^1(G_\mathbb{Q}, V_p A)$$

and local versions

$$K_\ell : A(\mathbb{Q}_\ell) \longrightarrow H^1(G_\ell, V_p A).$$

Definition: the $\mathbb{Q}_p$-linear Selmer group

$$\mathrm{Sel}_1(A/\mathbb{Q}) := \{ \xi \in H^1(G_{\mathbb{Q}}, V_pA) : \mathrm{loc}_\ell(\xi) \in \mathbb{Q}_p\text{-span of } \mathrm{im}(\kappa_\ell) \ \forall \ell \}$$

Understood thanks to

Theorem (BLOCH–KATO)

1) If $\ell \neq p$ then $H^1(G_\ell, V_pA) = 0$ (so $\mathrm{loc}_\ell(\xi) \in \mathrm{im}(\kappa_\ell)$ automatically)

2) If $\ell = p$, then

defined using p-adic Hodge theory, see later.

$$\mathbb{Q}_p\text{-span of } \mathrm{im}(\kappa_p) = H^1_f(G_p, V_pA) \cong H^0(A_{\mathbb{Q}_p}, \Omega^1)^*$$

and

$$\begin{array}{ccc} A(\mathbb{Q}_p) & \xrightarrow{\kappa_p} & H^1_f(G_p, V_pA) \cong H^0(A_{\mathbb{Q}_p}, \Omega^1)^* \end{array}$$

is

$$P \longmapsto \left(\omega \longmapsto \int_0^P \omega\right)$$

3) Have exact sequence

$$0 \to \mathbb{Q}_p \underset{\mathbb{Z}}{\otimes} A(\mathbb{Q}) \xrightarrow{\kappa} \mathrm{Sel}_1(A/\mathbb{Q}) \to V_p Ш(A/\mathbb{Q}) \to 0$$

$$V_p Ш(A/\mathbb{Q}) = \mathbb{Q}_p \underset{\mathbb{Z}_p}{\otimes} \varprojlim_n Ш(A/\mathbb{Q})[p^n]$$

$= 0$ if $Ш(A/\mathbb{Q})[p^\infty]$ finite.

Now let $X/\mathbb{Q}$ be a curve, $b \in X(\mathbb{Q})$,
$J = \mathrm{Jac}(X)$, $AJ : X \longrightarrow J$ ABEL-JACOBI map.

Definition / Notation:

- $\mathrm{Sel}_1(X/\mathbb{Q}) := \mathrm{Sel}_1(J/\mathbb{Q})$.
- $j_1 : X(\mathbb{Q}) \longrightarrow \mathrm{Sel}_1(X/\mathbb{Q})$ is the composite
$$X(\mathbb{Q}) \xrightarrow{AJ} J(\mathbb{Q}) \xrightarrow{\kappa} \mathrm{Sel}_1(J/\mathbb{Q})$$
- $j_{1,p} : X(\mathbb{Q}_p) \longrightarrow H^1_f(G_p, V_pJ)$ similarly.

Get a $\mathbb{Q}_p$-linear descent square

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook] \arrow[d, "j_1"] & X(\mathbb{Q}_p) \arrow[d, "j_{1,p}"] \\
\mathrm{Sel}_1(X/\mathbb{Q}) \arrow[r, "\mathrm{loc}_p"] & H^1_f(G_p, V_pJ)
\end{tikzcd}$$

- The $\mathbb{Q}_p$-linear descent locus is
$$X(\mathbb{Q}_p)_1 = \{x \in X(\mathbb{Q}_p) : j_{1,p}(x) \in \mathrm{im}(\mathrm{loc}_p)\}$$

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_1 \subseteq X(\mathbb{Q}_p).$$

The relationship between $\mathbb{Q}_p$-linear descent and CHABAUTY's method is as follows.

<u>Proposition</u>: $X(\mathbb{Q}_p)_{Chab} \subseteq X(\mathbb{Q}_p)_1$, with equality if $Ш(J/\mathbb{Q})[p^\infty]$ finite.

<u>Proof</u>: Write Φ' for the composite

$$H^0(X_{\mathbb{Q}_p}, \Omega^1) \cong H^1_f(G_p, V_pJ)^* \xrightarrow{loc_p^*} Sel_1(X/\mathbb{Q})^*$$

so by definition

$$X(\mathbb{Q}_p)_1 = \{x \in X(\mathbb{Q}_p) : \int_b^x \omega = 0 \ \forall \omega \in \ker(\Phi')\}$$

The composite

$$H^0(J_{\mathbb{Q}_p}, \Omega^1) \xrightarrow{\Phi'} Sel_1(J/\mathbb{Q})^* \xrightarrow{\kappa_p^*} Hom(J(\mathbb{Q}), \mathbb{Q}_p)$$

is the map Φ from earlier, so

$$\ker(\Phi') \subseteq \ker(\Phi).$$

This gives $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_{Chab}$.

If $Ш(J/\mathbb{Q})[p^\infty]$ is finite, then κ_p^* is an isomorphism, so equality holds. $\square$.

A sketch of non-abelian Chabauty

The non-abelian CHABAUTY method is a descent obstruction which is both $\mathbb{Q}_p$-linear and non-abelian.

Observation (KIM)

$$V_p J = H_1^{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) := H^1_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$$

$$\text{"} = \pi_1^{ab} \text{"}.$$

Is there a non-abelian lift of the CHABAUTY method?

Let $X/\mathbb{Q}$ be a curve, p a prime of good reductio

Key players: For $n \in \mathbb{N}$
- U_n = "n-step $\mathbb{Q}_p$-unipotent étale fundamental group of $X_{\overline{\mathbb{Q}}}$"
- "Selmer schemes" $Sel_n(X/\mathbb{Q})$, $H^1_f(G_{\mathbb{Q}_p}, U_n)$ (affine schemes of finite type over $\mathbb{Q}_p$)
- "localization map" $loc_p : Sel_n(X/\mathbb{Q}) \to H^1_f(G_{\mathbb{Q}_p}, U_n)$ (algebraic)

- "unipotent KUMMER maps"

$$j_n : X(\mathbb{Q}) \longrightarrow \mathrm{Sel}_n(X/\mathbb{Q})(\mathbb{Q}_p)$$

$$j_{n,p} : X(\mathbb{Q}_p) \longrightarrow H^1_f(G_p, U_n)(\mathbb{Q}_p)$$

in a "unipotent descent square"

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook] \arrow[d, "j_n"] & X(\mathbb{Q}_p) \arrow[d, "j_{p,n}"] \\
\mathrm{Sel}_n(X/\mathbb{Q}) \arrow[r, "\mathrm{loc}_p"] & H^1_f(G_{\mathbb{Q}_p}, U_n)
\end{tikzcd}$$

<u>Definition:</u> The n^{th} CHABAUTY-KIM locus is

$$X(\mathbb{Q}_p)_n = \{ x \in X(\mathbb{Q}_p) : j_{p,n}(x) \in \mathrm{im}(\mathrm{loc}_p) \}$$

scheme-theoretic image

$$X(\mathbb{Q}) \subseteq \dots \subseteq X(\mathbb{Q}_p)_3 \subseteq X(\mathbb{Q}_p)_2 \subseteq X(\mathbb{Q}_p)_1 \subseteq X(\mathbb{Q}_p)$$

$\mathbb{Q}_p$-linear descent locus.

Generalising CHABAUTY's theorem, we have

<u>Theorem</u> (KIM)

Suppose $\dim_{\mathbb{Q}_p} \mathrm{Sel}_n(X/\mathbb{Q}) < \dim_{\mathbb{Q}_p} H^1_f(G_p, U_n)$. $(*_n)$

Then $X(\mathbb{Q}_p)_n$ is finite ($\Rightarrow X(\mathbb{Q})$ is finite)

<u>Remarks</u>:

1) The conjectures of BLOCH–KATO or MAZUR–TATE imply $(*_n)$ holds for $n \gg 0$

2) KIM conjectured that
$$X(\mathbb{Q}_p)_n = X(\mathbb{Q}) \text{ for } n \gg 0.$$

3) Like CHABAUTY's original method, non-abelian CHABAUTY can be made explizit in some cases, especially for small n.

Example 1:

Theorem (BALAKRISHNAN–DOGRA–MÜLLER–TUITMAN–VONK)

Suppose $E/\mathbb{Q}$ is an elliptic curve and $E[13] \simeq \mathbb{F}_{13}^2$ is a trivialisation such that the image of the Galois representation

$$\rho : G_{\mathbb{Q}} \longrightarrow GL(E[13]) \simeq GL_2(\mathbb{F}_{13})$$

is contained in $\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$.

Then there are exactly 6 possibilities for E, all with complex multiplication.

Idea: Use quadratic Chabauty$^{(n=2)}$ to compute rational points on a modular curve $X_s(13)$.

The "cursed curve" of BILU–PARENT–REBOLLEDO

<u>Example 2</u>: There is a version of non-abelian Chabauty for S-integral points on hyperbolic curves (S = finite set of primes).

different methods

<u>Theorem</u> (SIEGEL, KIM) Let $\mathfrak{X} = \mathbb{P}^1_{\mathbb{Z}} \setminus \{0,1,\infty\}$. Then $\mathfrak{X}(\mathbb{Z}_S)$ is finite for all S.

Recently, a number of authors have begun using Chabauty and non-abelian Chabauty to study uniformity questions (COLEMAN, STOLL, KATZ–RABINOFF–ZUREICK-BROWN, BALAKRISHNAN–DOGRA, B.). For example

different methods.

<u>Theorem</u> (EVERTSE, B.) Let $\mathfrak{X} = \mathbb{P}^1_{\mathbb{Z}} \setminus \{0,1,\infty\}$. Then for all $s \geq 0$ there is a bound $B(s)$ such that $\#\mathfrak{X}(\mathbb{Z}_S) \leq B(s)$ for all S of size s.