Selmer Group Chabauty

Michael Stoll
Universität Bayreuth

Winter Workshop Chabauty-Kim
Heidelberg

February 14, 2024

Classical (Linear) Chabauty

Setting:

- C: a (nice) curve of genus $g \geq 2$ over $\mathbb{Q}$, with Jacobian J
- $P_0 \in C(\mathbb{Q})$ ($\rightsquigarrow$ get embedding $i\colon C \hookrightarrow J$ over $\mathbb{Q}$)
- $Q_1, \ldots, Q_r \in J(\mathbb{Q})$ generators of a finite-index subgroup of $J(\mathbb{Q})$
  need: $r < g$ ("Chabauty condition")

Goal: Determine $C(\mathbb{Q})$!

$$\begin{array}{ccccccc}
C(\mathbb{Q}) & \xhookrightarrow{\;i\;} & J(\mathbb{Q}) & & \xrightarrow{\qquad\qquad 0 \qquad\qquad} & & \mathbb{Q}_p \\
\downarrow & & \downarrow & & & & \| \\
C(\mathbb{Q}_p) & \xhookrightarrow{\;i\;} & J(\mathbb{Q}_p) & \xrightarrow{\log} & H^0(J_{\mathbb{Q}_p}, \Omega^1)^* & \xrightarrow{\mathrm{ev}_\omega} & \mathbb{Q}_p
\end{array}$$

- For $P \in C(\mathbb{Q}_p)$, $\mathrm{ev}_\omega \log i(P) = \displaystyle\int_{P_0}^{P} i^*\omega$.

Potential Problems

We need $r = \operatorname{rank} J(\mathbb{Q})$ independent points $Q_1, \dots, Q_r \in J(\mathbb{Q})$.
In particular, we need to know $\operatorname{rank} J(\mathbb{Q})$.

Usual approach:

1. Compute a Selmer group $\operatorname{Sel}_p J$.

Global Part: Class groups and units of number fields

- Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

- Can get painful even for $p = 2$ and moderate g.

2. Find $Q_1, \dots, Q_r \in J(\mathbb{Q})$ such that $\langle Q_1, \dots, Q_r \rangle + J(\mathbb{Q})_{\text{tors}} \twoheadrightarrow \operatorname{Sel}_p J$.

Problems: rank bound not tight, large generators,
high-dimensional search space.

- The most serious stumbling block in many cases.

Example

Say, we would like to solve the Generalized Fermat Equation

$$x^5 + y^5 = z^{17}.$$

Proposition (Dahmen & Siksek 2014).
Let p be an odd prime. If the only rational points on the curve

$$C_p \colon 5y^2 = 4x^p + 1$$

are the obvious ones (namely, ∞ and $(1, \pm 1)$),
then the only primitive integral solutions of $x^5 + y^5 = z^p$
are the trivial ones.

(Dahmen and Siksek show this for $p = 7$ and $p = 19$
and deal with $p = 11$ and $p = 13$ in another way, assuming GRH.)

Why the Usual Approach Does Not Work Here

So we would like to show that $C_{17}(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$.

The first step is to compute the 2-Selmer group $\mathrm{Sel}_2\, J_{17} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
Since $J_{17}(\mathbb{Q})[2] = 0$, this gives rank $J_{17}(\mathbb{Q}) \leq 2$.
We know the point $[(1, 1) - \infty]$ of infinite order, so rank $J_{17}(\mathbb{Q}) \geq 1$,
and (assuming finiteness of Sha) therefore rank $J_{17}(\mathbb{Q}) = 2$.

But we are unable to find another independent point,
so we cannot proceed with Chabauty's method.

The Idea

Use the p-Selmer group as a proxy for the Mordell-Weil group $J(\mathbb{Q})$!

Let $X \subset C(\mathbb{Q}_p)$ be a p-adic disk.

❶ If $C(\mathbb{Q}) \cap X = \emptyset$, we want to prove that.

❷ If $P_0 \in C(\mathbb{Q}) \cap X$, we want to show that $C(\mathbb{Q}) \cap X = \{P_0\}$.

$$\begin{array}{ccccccccc}
C(\mathbb{Q}) \cap X & \hookrightarrow & C(\mathbb{Q}) & \overset{i}{\hookrightarrow} & J(\mathbb{Q}) & \overset{\pi}{\twoheadrightarrow} & \dfrac{J(\mathbb{Q})}{pJ(\mathbb{Q})} & \overset{\delta}{\hookrightarrow} & \mathrm{Sel}_p J \\
\downarrow & & \downarrow & & \downarrow & & \downarrow r & \overset{\sigma}{\swarrow} & \\
X & \hookrightarrow & C(\mathbb{Q}_p) & \overset{i}{\hookrightarrow} & J(\mathbb{Q}_p) & \overset{\pi_p}{\twoheadrightarrow} & \dfrac{J(\mathbb{Q}_p)}{pJ(\mathbb{Q}_p)} & &
\end{array}$$

❶ $\pi_p i(X) \cap \mathrm{im}(\sigma) = \emptyset$ implies that $C(\mathbb{Q}) \cap X = \emptyset$.
Weaker condition $\pi_p i(X) \cap \sigma(\mathrm{Sel}_p C) = \emptyset$; $\mathrm{Sel}_p C$ is the p-Selmer set of C.

❷ is more involved $\rightsquigarrow$ next slide.

One Point in the Disk

We now assume that $P_0 \in C(\mathbb{Q}) \cap X$.

For simplicity, assume that $J(\mathbb{Q})[p] = \{0\}$. We also need:

- σ is injective $\rightsquigarrow$ $r = \sigma\delta$ is injective $\rightsquigarrow$ $J(\mathbb{Q}) \cap pJ(\mathbb{Q}_p) = pJ(\mathbb{Q})$

Consider $P \in C(\mathbb{Q}) \cap X$. We want to show that $P = P_0$.

- If $i(P) \in J(\mathbb{Q})$ is infinitely p-divisible, then $i(P) \in J(\mathbb{Q})_{\text{tors}}$ $\rightsquigarrow$ $P = P_0$.

So we can assume that $i(P) = p^n Q$ with $n \geq 0$ and $Q \in J(\mathbb{Q}) \setminus pJ(\mathbb{Q})$.
(Note that n and Q are uniquely determined since $J(\mathbb{Q})[p] = \{0\}$.)

Definition. For $Z \subset J(\mathbb{Q}_p)$, set

$$q(Z) = \left\{\pi_p(R) \;\middle|\; R \in J(\mathbb{Q}_p),\ \exists n \geq 0\colon p^n R \in Z\right\} \subset \frac{J(\mathbb{Q}_p)}{pJ(\mathbb{Q}_p)}$$

Then $\pi_p(Q) \in q(i(X)) \setminus \{0\}$ and $\pi_p(Q) = \sigma\delta\pi(Q) \in \mathrm{im}(\sigma)$.
So $q(i(X)) \cap \mathrm{im}(\sigma) \subset \{0\}$ implies that $C(\mathbb{Q}) \cap X = \{P_0\}$.

Remarks

❶ The function $P \mapsto q(\{i(P)\})$ is (explicitly) locally constant
$\rightsquigarrow$ we can compute $q(i(X))$.

❷ There is a more general statement in terms of a subgroup $\Gamma \subset J(\mathbb{Q})$
that shows $C(\mathbb{Q}) \cap X \subset i^{-1}(\bar{\Gamma})$ ($\bar{\Gamma}$ is the saturation of Γ)
under potententially weaker assumptions.

❸ **Pro:** No need to find many independent points in $J(\mathbb{Q})$
or to determine rank $J(\mathbb{Q})$.

❹ **Pro:** Necessary conditions are likely satisfied when g is not very small.

❺ **Con:** Does not always work, even when Selmer rank $< g$.
(E.g., when two rational points are p-adically sufficiently close.)

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

- q is locally constant in an explicit way.
- To compute q, need to halve points in $J(\mathbb{Q}_2)$.
  This can be done explicitly (in principle).
- If C is given as $y^2 = f(x)$ and $L = \mathbb{Q}[x]/\langle f \rangle$, then have compatible maps
  $$\mu\colon J(\mathbb{Q}) \to \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \hookrightarrow L^{\square}, \qquad \mu_2\colon J(\mathbb{Q}_2) \to \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \hookrightarrow L_2^{\square}, \qquad \rho\colon L^{\square} \to L_2^{\square},$$
  where $L_2 = L \otimes_{\mathbb{Q}} \mathbb{Q}_2$ and $R^{\square} = R^{\times}/(R^{\times})^2$.
- Can compute $\mathrm{Sel}_2\, C$ and $\mathrm{Sel}_2\, J$ as a subset and subgroup of $L^{\square}$.
- So work with $L^{\square}$ and $L_2^{\square}$ instead of $J(\mathbb{Q})/2J(\mathbb{Q})$ and $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(\rho) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\text{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:
   a. If $X \cap C(\mathbb{Q})_{\text{known}} = \emptyset$:
      if $\mu_2(X) \cap \rho(\mathrm{Sel}_2 C) \neq \emptyset$ then return FAIL, else continue with next X.
   b. Pick $P_0 \in X \cap C(\mathbb{Q})_{\text{known}}$ and compute $Y = \mu_2(q(i_{P_0}(X) + J(\mathbb{Q})[2^\infty]))$
   c. If $Y \cap \rho(\mathrm{Sel}_2 J) \not\subset R$ then return FAIL.
7. Return $C(\mathbb{Q})_{\text{known}}$.

Remark. Can leave out 2-adic condition for $\mathrm{Sel}_2 J$.

Applications

(1) $5y^2 = 4x^p + 1$:

Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $\rho(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $\rho|_{\mathrm{Sel}_2 J_p}$ is injective. This gives

Theorem (via work of Dahmen and Siksek).
$x^5 + y^5 = z^p$ has only trivial solutions for $p \leq 53$ (under GRH for $p \geq 23$).

(2) Similar application to FLT (via $y^2 = 4x^p + 1$).

(3) For $C\colon y^2 = x^{15} + (x^7 + (x^3 + (x+1)^2)^2)^2$ we can show that

$$C(\mathbb{Q}) = \{\infty, (0,1), (0,-1)\}.$$

(4) Elliptic curve Chabauty variant proves that the only rational points on
$y^2 = 81x^{10} + 420x^9 + 1380x^8 + 1860x^7 + 3060x^6 - 66x^5 + 3240x^4 - 1740x^3 + 1320x^2 - 480x + 69$
are the two points at infinity.
(Note: $g = \mathrm{rank}\, J(\mathbb{Q}) = 4$.)

(5) Elliptic curve Selmer Chabauty was also used to determine the primitive integral solutions of the GFE $x^2 + y^3 = z^{11}$.

Reference

Michael Stoll, *Chabauty without the Mordell-Weil group*
In G. Böckle, W. Decker, G. Malle (Eds.):
Algorithmic and Experimental Methods in Algebra,
Geometry, and Number Theory,
Springer Verlag (2018).
DOI: 10.1007/978-3-319-70566-8_28.
arXiv:1506.04286 [math.NT]

Thank You!