Chabauty–Coleman's Method

Matthew Hase-Liu

1 09/10 (Matthew): Overview of seminar and introduction to Chabauty–Coleman

Mostly everything will be over $\mathbb{Q}$, but there are generalizations to number fields. When we say "curve", we mean smooth, projective, and geometrically integral of dimension 1.

Let X be a curve over $\mathbb{Q}$ of genus $g \geq 2$. Mordell famously conjectured that $X(\mathbb{Q})$ is finite, and this was proved by Faltings in 1983. This leads to the following problem:

Problem 1. For X with $g \geq 2$ as above, compute the finite set $X(\mathbb{Q})$.

Parshin showed that Faltings' approach can be adapted to get an upper bound on the size of $X(\mathbb{Q})$, but does not give an algorithm to find the rational points. We'll discuss a different strategy introduced by Chabauty that can be modified in a way to be effective.

Suppose $X(\mathbb{Q}) \neq \varnothing$. Let J be the Jacobian of X. Recall that:

- J is an abelian variety.
- Its T-points are $\{\mathcal{L} \in \operatorname{Pic}(C \times T) : \deg(\mathcal{L}_t) = 0 \forall t\} / q^* \operatorname{Pic}(T)$.
- Fix $O \in X(\mathbb{Q})$. Then, we have an embedding $\iota : X \hookrightarrow J$ given by $P \mapsto [P - O]$.

One basic approach to computing $X(\mathbb{Q})$ is as follows:

(i) Find $J(\mathbb{Q})$.

(ii) Determine which points of $J(\mathbb{Q})$ are actually on $X(\mathbb{Q})$.

For the first step, the Mordell–Weil theorem ensures that $J(\mathbb{Q})$ is a finitely-generated abelian group. To find its generators and relations, there are algorithms based on descent.

If $J(\mathbb{Q})$ is moreover finite, one can determine $X(\mathbb{Q})$ by trying to find $P \in X(\mathbb{Q})$ satisfying $\iota(P) = [P - O] = [D]$ for each degree-0 divisor $[D] \in J(\mathbb{Q})$. This amounts to $P = D + O + (f)$ for f a non-zero rational function in $L(D + O)$, and Riemann–Roch spaces can be computed efficiently.

Another strategy is as follows:

(i) Embed $J(\mathbb{Q})$ in the Lie group $J(\mathbb{R})$, which is a compact commutative Lie group isomorphic to $\mathbb{R}^g/\mathbb{Z}^g \times F$ for some finite abelian group F.

(ii) Let $\overline{J(\mathbb{Q})}$ be the closure of $J(\mathbb{Q})$ in $J(\mathbb{R})$, which is a Lie subgroup.

(iii) It would be nice if $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{R})$ is finite, since this would imply that $X(\mathbb{Q})$ is finite.

Unfortunately, when $J(\mathbb{Q})$ is dense in J, this is expected to not be the case.

Chabauty's strategy was to use $\mathbb{Q}_p$ instead of $\mathbb{R}$.

Let us recall a bit about the structure of the p-adic Lie group $J(\mathbb{Q}_p)$:

- Let $H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)$ be the g-dimensional $\mathbb{Q}_p$-vector space of regular 1-forms. For $\omega_J \in H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)$, it turns out there is an antiderivative, which is a homomorphism:

$$\eta_j \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p, Q \mapsto \int_0^Q \omega_J.$$

- This induces a bilinear pairing

$$J(\mathbb{Q}_p) \times H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right) \to \mathbb{Q}_p,$$

which when written as

$$\log \colon J(\mathbb{Q}_p) \to H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)^\vee$$

is a local diffeomorphism (the tangent spaces at 0 of both are $H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)^\vee$).

(i) Embed $J(\mathbb{Q})$ in the p-adic Lie group $J(\mathbb{Q}_p)$.

(ii) Let $\overline{J(\mathbb{Q})}$ be the closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$, which is a p-adic Lie subgroup. The hope is that this is smaller than when taking the closure in $J(\mathbb{R})$.

(iii) It would be nice if $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ is finite, since this would imply that $X(\mathbb{Q})$ is finite.

To make this work, let $r' = \dim \overline{J(\mathbb{Q})}$ and $r = \operatorname{rk} J(\mathbb{Q})$. It turns out that $r' \leq r$ and g always.

Theorem 2 (Chabauty)**.** *Let X be a curve of genus $g \geq 2$ over $\mathbb{Q}$. Let p be a prime and r, r' be as above. Suppose $r' < g$ (which is automatic e.g. if $r < g$). Then, $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$, hence $X(\mathbb{Q})$, is finite.*

Although this is weaker than Faltings' theorem in that it requires $r' < g$, it has the advantage that it gives an explicit upper bound on $\#X(\mathbb{Q})$ that is often sharp.

Suppose X has good reduction, i.e. is the generic fiber of a smooth proper curve over $\mathbb{Z}_p$. Let $X(\mathbb{F}_p)$ denote the $\mathbb{F}_p$-points of the reduction of X. By using a function on $J(\mathbb{Q}_p)$ that vanishes on $\overline{J(\mathbb{Q})}$, Coleman proves the following bound:

Theorem 3 (Coleman)**.** *For $p > 2g$ and p a prime of good reduction for X,*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2).$$