THE METHOD OF CHABAUTY AND COLEMAN

GAL PORAT

Abstract. These are notes for a talk which introduces the method of Chabauty and Coleman, a $p$-adic method that sometimes bounds the set of rational points on a curve of genus $g \geq 2$. We present the method and give an example. We loosely follow the presentation given in [McPo].

1. The Jacobian Variety

Let $X/\mathbb{Q}$ be a smooth and projective curve of genus $g \geq 2$. The Jacobian variety $J(X) = J$ is an abelian variety of dimension $g$, satisfying

$$J(F) \cong \text{Pic}^0(X(F))$$

for each field $\mathbb{Q} \subset F$. The group $J(\mathbb{Q})$ is finitely generated.

Fixing some $O \in X(\mathbb{Q})$, there is an embedding $X \hookrightarrow J$ given by

$$P \mapsto [P - O].$$

In this talk, we are interested in bounding $\#X(\mathbb{Q})$. The idea will be to use the embedding

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$$

and to bound $\#X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ instead.

2. The Statement of the Main Theorem

Let $r = \text{rank}_\mathbb{Z} J(\mathbb{Q})$, and let $p$ be a prime.

Theorem 2.1. (Chabauty-Coleman) Suppose $r < g$, $p > 2g$ and that $X$ has good reduction at $p$. Then

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

Remark 2.1. Chabauty ([Cha]) proved a noneffective version of the theorem in 1941. This was one of the pieces of evidence for the Mordell conjecture.

Remark 2.2. Coleman ([Col]) proved the effective version presented here in 1985.
3. An Example

Let \( X \) be the genus 2 hyperelliptic curve given by
\[
y^2 = x(x - 1)(x - 2)(x - 5)(x - 6).
\]
This curve has good reduction at \( p = 7 \), and
\[
X(\mathbb{F}_7) = \{(0, 0), (1, 0), (2, 0), (5, 0), (6, 0), (3, \pm 6), \infty\}.
\]
A descent calculation shows that \( r = 1 \). By the theorem,
\[
\# X(\mathbb{Q}) \leq 8 + 2 = 10.
\]
It turns out that we have an equality, since
\[
\{(0, 0), (1, 0), (2, 0), (5, 0), (6, 0), (3, \pm 6), (10, \pm 120), \infty\} \subset X(\mathbb{Q}).
\]

4. The Structure of \( J(\mathbb{Q}_p) \)

Recall that our idea was to bound \( X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \). As \( J(\mathbb{Q}_p) \) is \( g \)-dimensional and \( X(\mathbb{Q}_p) \) is 1-dimensional, one hopes that \( X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \) is finite if \( \dim J(\mathbb{Q}) < g \).

With in mind, let us first bound \( \dim \overline{J(\mathbb{Q})} \). Since \( \overline{J(\mathbb{Q})} \) is a \( p \)-adic Lie group, its dimension is equal to the dimension of its Lie algebra as a \( \mathbb{Q}_p \) vector space. More precisely, there is a homomorphism
\[
\log : J(\mathbb{Q}_p) \to \text{Lie} J(\mathbb{Q}_p)
\]
which is a diffeomorphism near the origin. This gives us
\[
\dim \overline{J(\mathbb{Q})} = \dim \log J(\mathbb{Q}) = \dim \log J(\mathbb{Q}) \leq \dim_{\mathbb{Q}_p} \mathbb{Z}_p J(\mathbb{Q}) \leq \text{rank} J(\mathbb{Q}) = r.
\]

5. \( p \)-adic Differentials

We may think of differentials as being functionals on the tangent space at each point. Since \( J(\mathbb{Q}_p) \) is a Lie group, a functional on the tangent space at the origin gives rise to a functional at any tangent space, by translation. By dimension counting, any global differential is obtained in this way. This gives the canonical isomorphism
\[
\text{Lie} J(\mathbb{Q}_p) \cong H^0(J_{\mathbb{Q}_p}, \Omega^1)^\vee,
\]
so the map \( \log : J(\mathbb{Q}_p) \to \text{Lie} J(\mathbb{Q}_p) \) gives rise to a pairing
\[
J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) \to \mathbb{Q}_p,
\]
\[
Q, \omega \mapsto \int_0^Q \omega.
\]
It turns out that the embedding \( X \hookrightarrow J \) induces an isomorphism \( H^0(J_{\mathbb{Q}_p}, \Omega^1) \isom H^0(X_{\mathbb{Q}_p}, \Omega^1) \) by pullback. Hence, we have an induced pairing
\[
X(\mathbb{Q}_p) \times H^0(X_{\mathbb{Q}_p}, \Omega^1) \to \mathbb{Q}_p,
\]
\[
P, \omega \mapsto \int_0^P \omega.
\]
If $X$ has good reduction, we can locally give a parametrization by a uniformizer $t$, which gives an identification with $p\mathbb{Z}_p$. Then $\omega$ is of the form $w(t)dt$ for $w \in \mathbb{Q}_p[[t]]$. If $X$ has good reduction, one can normalize $\omega$ so that $w \in \mathbb{Z}_p[[t]]$ and $w$ is nonzero mod $p$. Thus $\tilde{\omega} = \tilde{w}(t)dt$ is a nonzero differential for the reduction of $X$.

6. A proof of the Main Theorem

Suppose now that $r < g$. Then $\dim J(\mathbb{Q}) \leq r < g$, which implies there is a differential $\omega$ of $J_{\mathbb{Q}_p}$ vanishing on $J(\mathbb{Q})$.

Lemma 6.1. Let $\tilde{Q} \in X(\mathbb{F}_p)$, and let $m = m_{\tilde{Q}} = \text{ord}_{\tilde{Q}}\tilde{\omega}$. If $m < p - 2$, then there are at most $m + 1$ points $Q'$ of $X(\mathbb{Q}_p)$ reducing to $\tilde{Q}$ with $\int_{Q'}^Q \omega = 0$.

Proof. Points $Q'$ which reduce to $\tilde{Q}$ lie close to $Q$ in $X(\mathbb{F}_p)$; indeed, they are congruent mod $p$. On each such small neighborhood we can pick a uniformizing parameter $t$ so that $\omega$ is of the form $w(t)dt$ for $w \in \mathbb{Z}_p[[t]]$, with $t = 0$ corresponding to $Q$. Then $\int_{Q}^{Q'} \omega$ is the formal antiderivative of $w$ in terms of $t$. If we write

$$w(t) = a_0 + a_1 t + a_2 t^2 + ..., a_i \in \mathbb{Z}_p,$$

then for $Q' = Q'(t)$, we have

$$\int_{Q}^{Q'} \omega = a_0 t + a_1 \frac{t^2}{2} + ... + a_{i-1} \frac{t^i}{i} + ...$$

We have $v(a_m) = 0$ and $v(a_{i-1}/i) > m + 1 - i$ for $i > m + 1$. This means that the Newton polygon of $\int_{Q}^{Q'} \omega$ has a point at $(m + 1, 0)$, and lies above the line with slope -1 starting at this point. Thus the Newton polygon can only lie in the blue-shaded region in the following picture.
This implies that $\int_{Q}^{Q'} \omega$ has at most $m + 1$ segments of slope $-1$, hence at most $m + 1$ zeros in $p\mathbb{Z}_p$, by the theory of Newton polygons. \qed

We may now prove the main theorem.

Proof of Theorem 2.1. By the Riemann Roch theorem, the total number of zeros of $\tilde{\omega}$ in $X(\overline{\mathbb{F}_p})$ is $\deg \tilde{\omega} = 2g - 2$. Therefore,

$$\sum_{\tilde{Q} \in X(\overline{\mathbb{F}_p})} m_{\tilde{Q}} \leq 2g - 2.$$ 

Hence, by the previous lemma,

$$\# X(\mathbb{Q}) \leq \# X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \leq \sum_{\tilde{Q} \in X(\overline{\mathbb{F}_p})} (m_{\tilde{Q}} + 1) \leq \# X(\mathbb{F}_p) + (2g - 2).$$
7. A picture of the idea in the proof

8. The Example Revisited

We illustrate the argument for the curve $y^2 = x(x - 1)(x - 2)(x - 5)(x - 6)$. In this case, $X(\mathbb{F}_7) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3,\pm 6), \infty \}$. Let $\omega$ be as in the theorem; we know that it has exactly $2g - 2 = 2$ zeros. Notice that there are two points in $X(\mathbb{Q})$ lying over $(3,6)$: these are $(3,6)$ and $(10,-120)$. So by the lemma, $(3,6)$ must be a zero of $\tilde{\omega}$.

On the other hand, as $X$ is a genus 2 curve given by $y^2 = f(x)$, we know $\tilde{\omega}$ is a linear combination of $\frac{dx}{y}$, $\frac{xdx}{y}$. This implies (up to a normalization) that $\tilde{\omega} = \frac{(x-3)dx}{y}$.

Thus, by the lemma, there is at most 1 point above $(0,0), (1,0), (2,0), (5,0), (6,0), \infty$ (which are not zeros of $\tilde{\omega}$) and at most 2 points above $(3,\pm 6)$ (which are simple zeros of $\tilde{\omega}$).

References

