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

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

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 $r = \mathrm{rank}_{\mathbb{Z}} J(\mathbb{Q})$, 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 $\dim \overline{J(\mathbb{Q})} < g$.

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

$$\log : J(\mathbb{Q}_p) \to \mathrm{Lie} J(\mathbb{Q}_p)$$

which is a diffeomorphism near the origin. This gives us

$$\dim \overline{J(\mathbb{Q})} = \dim \log \overline{J(\mathbb{Q})} = \dim \overline{\log J(\mathbb{Q})} \leq \dim_{\mathbb{Z}_p} \mathbb{Z}_p J(\mathbb{Q}) \leq \mathrm{rank} J(\mathbb{Q}) = r.$$

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

$$\mathrm{Lie} J(\mathbb{Q}_p) \cong \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1)^\vee,$$

so the map $\log : J(\mathbb{Q}_p) \to \mathrm{Lie} J(\mathbb{Q}_p)$ gives rise to a pairing

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

$$Q \quad , \quad \omega \mapsto \int_0^Q \omega.$$

It turns out that the embedding $X \hookrightarrow J$ induces an isomorphism $\mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1) \xrightarrow{\sim} \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$ by pullback. Hence, we have an induced pairing

$$X(\mathbb{Q}_p) \times \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \to \mathbb{Q}_p,$$

$$P \quad , \quad \omega \mapsto \int_O^P \omega.$$

If X has good reduction, we can locally give a parametrization by a uniformizer t, which gives an identifcation with $p\mathbb{Z}_p$. Then ω is of the form $w(t)dt$ for $w \in \mathbb{Q}_p[[t]]$. If X has good reduction, one can normalize ω so that $w \in \mathbb{Z}_p[[t]]$ and w is nonzero mod p. Thus $\widetilde{\omega} = \widetilde{w}(t)dt$ is a nonzero differential for the reduction of X.

6. A proof of the Main Theorem

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

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

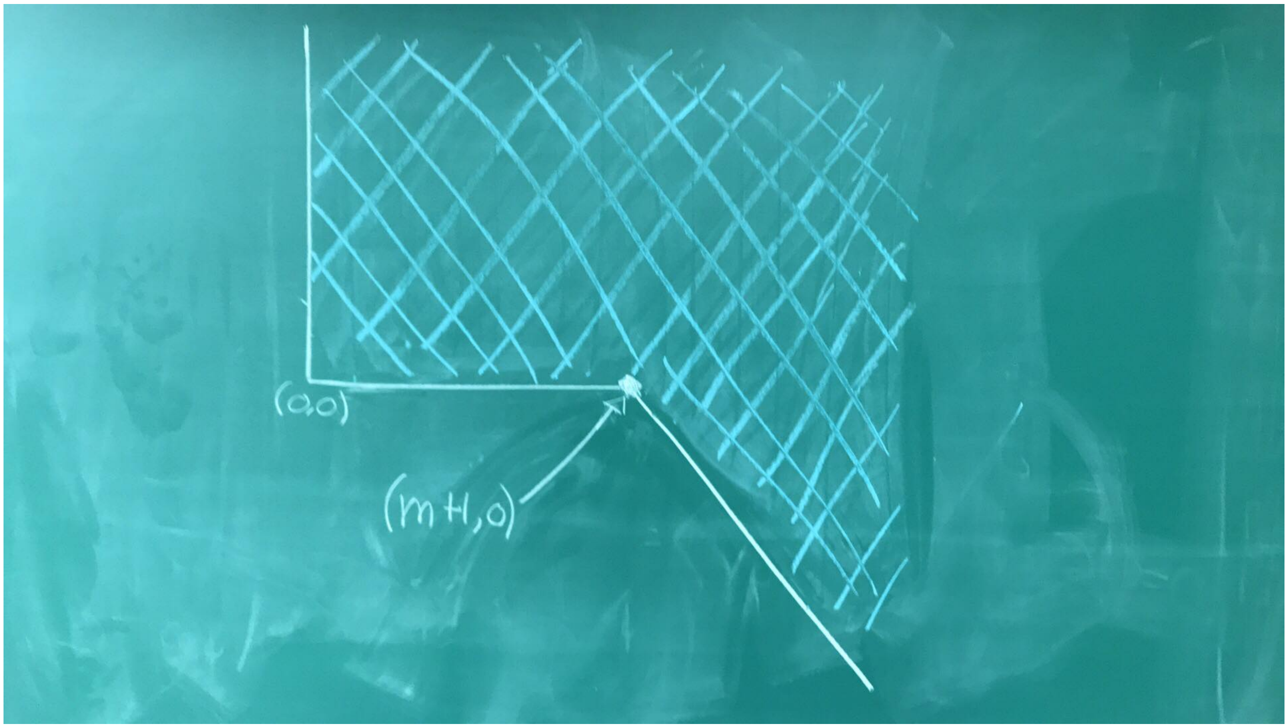
Proof. Points Q' which reduce to $\widetilde{Q}$ lie close to Q in $X(\mathbb{F}_p)$; indeed, they are congruent mod p. On each such small neighborhood we can pick a uniformizing parameter t so that ω is of the form $w(t)dt$ for $w \in \mathbb{Z}_p[[t]]$, with $t = 0$ corresponding to Q. Then $\int_Q^{Q'}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

We may now prove the main theorem.

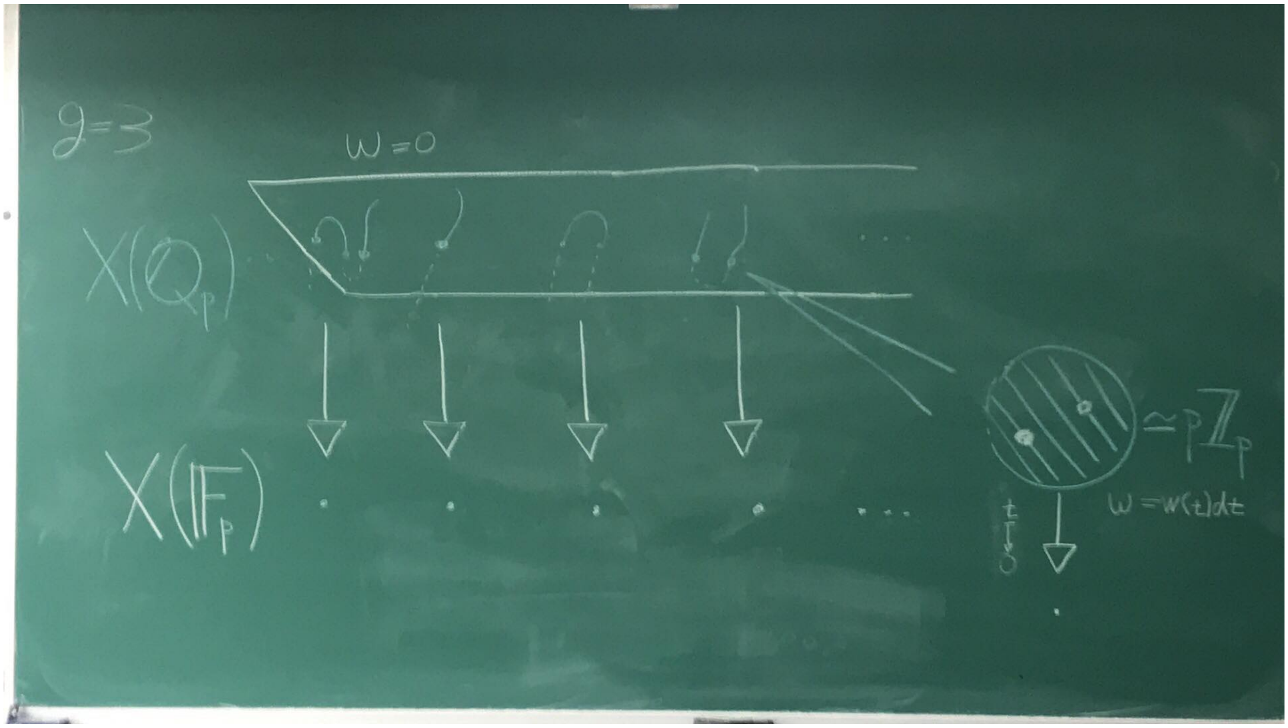
Proof of Theorem 2.1. By the Riemann Roch theorem, the total number of zeros of $\widetilde{\omega}$ in $X(\overline{\mathbb{F}_p})$ is $\deg \widetilde{\omega} = 2g-2$. Therefore,

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

Hence, by the previous lemma,

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \leq \sum_{\widetilde{Q} \in X(\mathbb{F}_p)} (m_{\widetilde{Q}} + 1) \leq \#X(\mathbb{F}_p) + (2g-2).$$

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 ω 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 $\widetilde{\omega}$.

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

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 $\widetilde{\omega}$) and at most 2 points above $(3,\pm 6)$ (which are simple zeros of $\widetilde{\omega}$).

References

[Cha] Claude Chabauty, Sur les points rationnels des courbes alg´ebriques de genre sup´erieur 'a l'unit´e, C. R. Acad. Sci. Paris 212 (1941), 882–885 (French). MR0004484 (3,14d) ↑4, 4.4

[Col] Robert F. Coleman, Effective Chabauty, Duke Math. J. 52 (1985), no. 3, 765–770. MR808103 (87f:11043) ↑4.3, 5.3, 5.4

[McPo] McCallum, W & Poonen, B. (2012). The method of Chabauty and Coleman, Explicit Methods in Number Theory, Panor. Synthèses. Soc. Math. France, Paris. 36. 99-117.