Rational Points on Curves

Lectures by: Steffel Müller
Notes by: Ross Paterson

These notes were taken live during lectures at the CMI-HIMR Computational Number Theory summer school held at the University of Bristol in June 2019. In particular, any mistakes are the fault of the transcriber and not of the lecturer. Remarks in red were not written on the board, and were often added later by the transcriber.

Lecture List

Contents

Lecture 1: Canonical Heights

1 Introduction

Throughout this course, $X/\mathbb{Q}$ is a nice curve of genus g. Our goal will be to compute the rational points on X, i.e. $X(\mathbb{Q})$. But what do we mean by this? How does one "compute" a potentially

infinite set? Well firstly, $X(\mathbb{Q}) = \emptyset$ is one possibility, and we will always need to decide if this is the case. Else we are in one of the following cases:

Genus g	**Structure of X**$(\mathbb{Q})$	**"Computing" X**$(\mathbb{Q})$
$(g = 0)$	$X(\mathbb{Q}) \cong_{\mathbb{Q}} \mathbb{P}^1_{\mathbb{Q}}$	Find the isomorphism $X \to \mathbb{P}^1$
$(g = 1)$	$X(\mathbb{Q})$ is a finitely generated abelian group (Mordell)	Find generators of $X(\mathbb{Q})$
$(g = 0)$	$\#X(\mathbb{Q}) < \infty$ (Faltings)	List the elements $X(\mathbb{Q})$

Today we focus on methods of deciding if $X(\mathbb{Q}) = \emptyset$, then in the later lectures we will consider the other cases. Note that there is a trivial obstruction that is worth mentioning, namely if $K/\mathbb{Q}$ is a field extension then $X(K) = \emptyset \Rightarrow X(\mathbb{Q}) = \emptyset$. So if it is easy to prove that there are no K rational points then we get the result for $\mathbb{Q}$ for free.

Definition 1.1. *Our variety X is **everywhere locally soluble (ELS)** if*

- $X(\mathbb{R}) \neq \emptyset$,
- $X(\mathbb{Q}_p) \neq \emptyset$ *for all primes p.*

So by what we've said, X must be everywhere locally soluble if it has any $\mathbb{Q}$-rational points. How do we check if X is ELS? Well $X(\mathbb{R})$ is relatively easy, we just need to find one point and we can usually expect to be able to do this by hand. For $\mathbb{Q}_p$ we have a useful lemma.

Lemma 1.2. *If there is a smooth point $\overline{P} \in X(\mathbb{F}_p)$, then $\overline{P}$ lifts to a point in $X(\mathbb{Q}_p)$.*

Proof. This is essentially just Hensels lemma, and is an exercise in John Cremona's course. □

Corollary 1.3. *If $p \in \{p > 4g^2 \mid X \text{ has good reduction at } p\}$ then $X(\mathbb{Q}_p) \neq \emptyset$ for $g \geq 1$.*

Proof. Just use Lemma 1.2 and the Hasse-Weil bound. □

What about the remaining primes? Well:

$(g = 0)$ Without loss of generality we can assume that X is a smooth conic and we can check if X is ELS via finitely many congruence conditions (this is an exercise!).

$(g \geq 1)$ Say $\overline{X}(\mathbb{F}_p) \neq \emptyset$ but all $\overline{P} \in \overline{X}(\mathbb{F}_p)$ are singular. Then we choose a model $\mathscr{X}/\mathbb{Z}_p$ for $X_{\mathbb{Q}_p}$, and for all $\overline{P} \in \overline{X}(\mathbb{F}_p)$:

- "zoom in" (blow up) at $\overline{P}$ to get a new model $\mathscr{X}'$,
- Check if $\mathscr{X}'(\mathbb{F}_p) = \emptyset$ or $\mathscr{X}'(\mathbb{F}_p)$ has smooth points. In either of these cases we are done,
- Else repeat with $\mathscr{X}$ replaced by $\mathscr{X}'$.

This is a finite process and checks if X is everywhere locally soluble.

Question 1. *Is this sufficient to decide if $X(\mathbb{Q}) = \emptyset$?*

Theorem 1.4 (Legendre)**.** *If $g = 0$ then*

$$X \text{ ELS} \iff X(\mathbb{Q}) \neq \emptyset$$

Note that this is a special case, and the answer to our question is in general no. In fact, we should expect for higher genus that there are no global points but ELS is very common.

2 Descent and Covering Collections

Example 1. *$X : y^2 = f(x)$ a hyperelliptic curve such that $f = f_1 f_2$ for $f_1, f_2 \in \mathbb{Z}[x]$ which are nonconstant and not both of odd degree (and coprime, but this is assured by defining a hyperelliptic curve). We have an obvious unramified double cover:*

$$\mathbb{P}^3 \supset Y : \begin{cases} y_1^2 = f_1(x) \\ y_2^2 = f_2(x) \end{cases} \to X$$
$$\pi : (x, y_1, y_2) \mapsto (x, y_1 y_2)$$

as well as several "twists" of this, for $d \in \mathbb{Z}$ squarefree:

$$\mathbb{P}^3 \supset Y_d : \begin{cases} d y_1^2 = f_1(x) \\ d y_2^2 = f_2(x) \end{cases} \to X$$
$$\pi_d : (x, y_1, y_2) \mapsto (x, d y_1 y_2)$$

Which give us commutative diagrams:

$$\begin{array}{ccc} Y_d & \xrightarrow[\overline{\mathbb{Q}}]{\sim} & Y \\ & {\scriptstyle \pi_d} \searrow \quad \swarrow {\scriptstyle \pi} & \\ & X & \end{array}$$

We aim to use these kinds of twists to study rational points.

Lemma 2.1. *$X(\mathbb{Q}) = \bigcup_{d \in S} \pi_d(Y_d(\mathbb{Q}))$ where S is a finite set and is (theoretically) explicitly computable.*

Proof. If $(x, y) \in X(\mathbb{Q})$ then there is a unique $d \in \mathbb{Z}_{\geq 0}$ squarefree such that

$$\begin{cases} f_1(x) = d y_1^2 \\ f_2(x) = d y_2 \end{cases}$$

with $y_1, y_2 \in \mathbb{Q}$. The remainder is an exercise. □

This extends more generally to nice curves X as follows,

Theorem 2.2. *Let $\pi : Y \to X$ be an unramified geometrically Galois covering. Then there is a set*

$$\mathrm{Sel}(\pi) \subset H^1(G_{\mathbb{Q}}, \mathrm{Aut}_{\overline{\mathbb{Q}}}(\pi))$$

which is finite and (in principle) explicitly computable such that

$$X(\mathbb{Q}) = \bigcup_{\alpha \in \mathrm{Sel}(\pi)} \pi_\alpha(Y_\alpha(\mathbb{Q}))$$

In fact,

Definition 2.3. *The **Selmer set of** π is*

$$\mathrm{Sel}(\pi) = \left\{ \alpha \in H^1(G_{\mathbb{Q}}, \mathrm{Aut}_{\overline{\mathbb{Q}}}) \mid Y_\alpha \text{ is ELS} \right\}.$$

Corollary 2.4. *If $\mathrm{Sel}^{(n)}(\pi) = \emptyset$ then $X(\mathbb{Q}) = \emptyset$.*

Note that in the example, $\mathrm{Aut}_{\overline{\mathbb{Q}}}(\pi) = \mathbb{Z}/2\mathbb{Z}$ so that

$$H^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$$

for which squarefree $d \in \mathbb{Z}$ form a system of representatives.

2.1 n-coverings

Definition 2.5. *Suppose we are given $\iota : X \to E = \operatorname{Jac} X$ which is defined over $\mathbb{Q}$, for example there are the Abel-Jacobi maps $P \mapsto [P] - c$ for some $c \in \operatorname{Pic}^1(X)$. Then for any $\pi : Y \to X$ such that*

$$\begin{array}{ccc} Y & \xrightarrow[\overline{\mathbb{Q}}]{\sim} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle[n]} \\ X & \xrightarrow{\iota} & E \end{array}$$

*commutes, we call $\pi : Y \to X$ an n-**covering**. For genus $g \geq 1$ let $\iota : X \to J = \operatorname{Jac} X$ be a $\mathbb{Q}$ morphism. Then more generally for*

$$\begin{array}{ccccc} Y & \longrightarrow & V & \xrightarrow[\overline{\mathbb{Q}}]{\sim} & J \\ {\scriptstyle\pi}\downarrow & & \downarrow & \swarrow{\scriptstyle[n]} & \\ X & \xrightarrow{\iota} & J & & \end{array}$$

We see that V is an n-covering of J and we call $\pi : Y \to X$ an n-covering of X.

Now, we have the definition of the n-Selmer set:

Definition 2.6. *The n-Selmer set is*

$$\operatorname{Sel}^{(n)}(X) = \{\text{ELS } n\text{-coverings of } X\}$$

Theorem 2.7. $\operatorname{Sel}^{(n)}(X)$ *is finite and explicitly computable (In principle).*

In practice, we can often compute $\operatorname{Sel}^{(n)}(X)$ when:

- $(g = 1)$, $X \in \operatorname{Sel}^{(m)}(\operatorname{Jac}(X)/\mathbb{Q})$ and
  - $m = n = 2$ (Cassels, Merriman-Siksek-Smart)
  - $m = n = 3$ (Creatz)
  - $m = 4, n = 2$ (Stamminger)
  - $mn \in \{6, 12\}$ (Fisher)
- $(g \geq 2)$ of X is hyperelliptic (Bruin-Stoll)

Lecture 2: Curves of Small Genus

3 Curves of Small Genus

Let $X/\mathbb{Q}$ be a nice curve, $g \leq 1$ and $X(\mathbb{Q}) \neq \emptyset$.

3.1 Genus 0

Say $g = 0$, WLOG $X : Q = 0$ is a conic with $Q \in \mathbb{Z}[X, Y, Z]$ quadric and $\operatorname{disc}(Q) \neq 0$. Given $P_0 \in X(\mathbb{Q})$ we have an isomorphism $X \cong_{\mathbb{Q}} \mathbb{P}^1_{\mathbb{Q}}$ via projection from P_0. (See Figure 1)

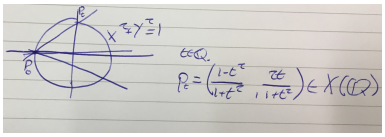


Figure 1: The special fibre with multiplicative reduction.

3.1.1 Finding a Rational Point

We want to find $P_0 \in X(\mathbb{Q})$.

Idea: Replace Q by a "simpler" quadratic form Q', then deduce rational solution from Q from rational solution of Q'.

Theorem 3.1 (Simon's Algorithm, (some goes back to Gauss))**.** *Need everywhere locally soluble.*

- *Minimization: for all prime $P \mid \operatorname{disc}(Q)$, find Q' such that $P \nmid \operatorname{disc}(Q')$. WLOG $|\operatorname{disc}(Q)| = 1$.*
- *Reduction to the unit circle via indefinite quadratic form LLL.*

Remark 3.2. *There are alternatives to this due to Cremona-Rusin.*

3.2 Genus 1

Say $g = 1$.

Example 2. *Below are some examples:*

- *$X : y^2 = f(x)$ where $f \in \mathbb{Z}[x]$ with $\deg(f) = 4$ and f squarefree.*
- *$X \subset \mathbb{P}^2$ a plane cubic,*
- *$X = S_1 \cap S_2 \subset \mathbb{P}^3$ for S_i quadratic surfaces.*

e.g. via n-descent on $\operatorname{Jac} X$ for $n = 2, 3, 4$.

To find $P_0 \in X(\mathbb{Q})$ search on X or on a cover of X. Covers hace "smaller" rational points (this will be due to functoriality of heights, we will see this a little later). Given $P_0 \in X(\mathbb{Q})$, can construct

$$X \cong_{\mathbb{Q}} E : y^2 = x^3 + ax + b$$

such that $P_0 \mapsto O = [0 : 1 : 0]$, e.g. via Riemann-Roch.

Goal: Find generators of $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$ for $r \geq 0$ and $\#T < \infty$.

3.2.1 Generators of Torsion

Lemma 3.3. *For p a good prime for E, we have that $E(\mathbb{Q}_p)_{\text{tors}} \subset \widetilde{E}(\mathbb{F}_p)$. Combining this for several primes p we get an upper bound for $\#E(\mathbb{Q})_{\text{tors}}$. This extends to general number fields*

For a lower bound: can just search, or use the theorem of Nagell-Lutz which says that rational torsion which is not 2-torsion satisfies some division relations. Namely:

Theorem 3.4 (Nagell-Lutz)**.** *If $(x, y) \in E(\mathbb{Q})_{\text{tors}} \backslash E[2]$, then $x, y \in \mathbb{Z}$ and $y \mid \Delta_E$.*

Remark 3.5. *These in no way guarantee that the upper and lower bounds agree, there is still some searching and trickery to do.*

3.2.2 Rank

n-descent will give us an upper bound on r, but it might not be sharp because we do not know Ш very well. A lower bound can be obtained via searching on E or via points on the n-covering. See online notes for more detail.

Problem 1. *Given $Q_1, \dots, Q_r \in E(\mathbb{Q})$ independent modulo torsion, compute $P_1, \dots, P_r \in E(\mathbb{Q})$ such that $[P_1], \dots, [P_r] \in E(\mathbb{Q})/\text{tors}$ are linearly independent generators.*

How do we even begin to answer such a question? Heights!

3.2.3 Heights

For $P = (x_0 : \cdots : x_N) \in \mathbb{P}^N(\mathbb{Q})$, $x_0, \dots, x_N \in \mathbb{Z}$ and $\gcd(x_i)_i = 1$ then we define the height

$$h(P) = \log \max \{|x_i|_\infty\}.$$

This definition does not extend in an obvious way to a number field, there is a whole theory behind defining a height on general number fields, which specialises to this for $\mathbb{Q}$.

The **Naive height function** on $E(\mathbb{Q})$ is

$$\begin{aligned} h : E(\mathbb{Q}) &\to \mathbb{R}_{\geq 0} \\ (x, y) &\mapsto h(x) \\ O &\mapsto 0 \end{aligned}$$

Theorem 3.6. *The naive height has some properties.*

(1) $\#\{P \in E(\mathbb{Q}) \mid h(P) \leq B\} < \infty$ *for any* $B \in \mathbb{R}$,

(2) There is some $C \in \mathbb{R}$ *such that* $h(2P) - 4h(P) \leq C$ *for all* $P \in E(\mathbb{Q})$. *i.e. it is almost a quadratic form,*

(3) For $P \in E(\mathbb{Q})$, *the* ***canonical height***

$$\widehat{h}(P) := \lim_{n \to \infty} 4^{-n} h(2^n P)$$

exists,

(4) $\widehat{h}$ *is a quadratic form,*

(5) $h - \widehat{h}$ *is bounded.*

(6) $\widehat{h}(p) = 0$ *if and only if* P *is torsion.*

(7) $\#\left\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq B\right\} < \infty$ *for any* $B \in \mathbb{R}$ *(follows from ((1)) and ((5)))*,

(8) $\widehat{h}$ *extends to a positive definite quadratic form on* $E(\mathbb{Q}) \otimes \mathbb{R} \cong \mathbb{R}^r$.

For $P, Q \in E(\mathbb{Q})$ set the **height pairing**:

$$\langle P, Q \rangle = \frac{\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)}{2}.$$

If $P_1, \dots, P_r$ generate $E(\mathbb{Q})/\text{tors}$ then set

$$\text{Reg}(E/\mathbb{Q}) := \det\left(\langle P_i, P_j \rangle\right)_{i,j}$$

to be the **Regulator of** $E/\mathbb{Q}$

All known algorithms to solve Problem 1 require essentially 2 ingredients, algorithms to:

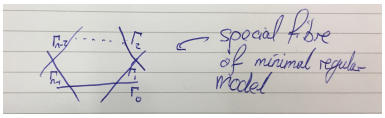


Figure 2: The special fibre with multiplicative reduction.

1. Compute $\widehat{h}(P)$ for a given $P \in E(\mathbb{Q})$.
2. enumerate $\left\{P \in E(\mathbb{Q}) : \widehat{h}(P) \leq B\right\}$ for a given $B \in \mathbb{R}$.

Remark 3.7. *We know that*

$$\left\{P \in E(\mathbb{Q}) : \widehat{h}(P) \leq B\right\} \subseteq \{P \in E(\mathbb{Q}) : h(P) \leq B + \beta\}$$

where $\left|h - \widehat{h}\right| \leq \beta$ *and the naive height* h *is somewhat easier to compute.*

For (1) and (2) use

Theorem 3.8 (Néron)**.** $h - \widehat{h} = \sum_{p \text{ prime}} \psi_p + \psi_\infty$ *such that*

$$\psi_v : E(\mathbb{Q}_v) \to \mathbb{R}$$

satisfy

1. ψ_v *is* v*-adically continuous and bounded,*
2. *For* p *prime,* ψ_p *factors through* $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$*.*
3. $\psi_p(Q)/\log p \in \mathbb{Q}_{\geq 0}$ *for* $Q \in E(\mathbb{Q}_p)$*.*

and ψ_∞ *is related to the Weierstrass sigma function, but we won't write it down for lack of time.*

Example 3. *Suppose that* $E/\mathbb{Q}_p$ *has multiplicative reduction, and* $v_p(\Delta_E) = n \geq 3$*. You saw last week that the Néron model has special fibre an* n*-gon (see Figure 2).*

Let $\Gamma_0(\mathbb{F}_p) = \overline{E_0(\mathbb{Q}_p)}$*, the identity component. Then*

$$\psi_p(\Gamma_i) = \frac{i(n-i)}{n} \log p$$

Lecture 3: Chabauty's Method

We begin with some leftovers from yesterday. The state of the art with heights means that we can in fact do the following:

- Compute and bound $h(P) - \widehat{h}(P) = \sum_v \psi_v(P) = \sum_{n \geq 0} 4^{-n-1} \Phi_v(2^n P)$. We can do this particularly well through an interpretation via Néron models.
- Compute $\widehat{h}(P)$ without integer factorisation, so we don't actually need to know which ψ_v contribute to the sum!
- Extend the definitions of $\widehat{h}, h$ and Reg to abelian varieties.
  - Compute $\widehat{h}$ for jacobians.
  - Bound $h - \widehat{h}$ for jacobians of hyperelliptic curves.

4 Chabauty's Method

Here we leave the familiar relm of low genus curves, let $X/\mathbb{Q}$ be a nice curve of genus $g \geq 2$ and $X(\mathbb{Q}) \neq \emptyset$. let p be a prime of good reduction for X.

Searching gives $X(\mathbb{Q})_{\text{known}} \subseteq X(\mathbb{Q})$ a set of known points, our goal is to be able to show that in fact $X(\mathbb{Q})_{\text{known}} = X(\mathbb{Q})$. Fix a rational base point $b \in X(\mathbb{Q})$, and recall the familiar map

$$\begin{aligned} X &\to J := \operatorname{Jac} X \\ P &\mapsto [P - b] \end{aligned}$$

Idea: Cut out $X(\mathbb{Q})$ in $X(\mathbb{Q}_p)$.

We know that $J(\mathbb{Q}_p)$ is a p-adic Lie group, there exists a continuous homomorphism

$$\log : J(\mathbb{Q}_p) \to H^0(J_{\mathbb{Q}_p}, \Omega^1)^* \cong H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$$

such that $\ker \log = J(\mathbb{Q}_p)_{\text{tors}}$.

Lemma 4.1 (Chabauty)**.** *If $r = \operatorname{rk}(J(\mathbb{Q})) < g$ then there exists a nonzero holomorphic differential*

$$\omega_0 \in H^0(X_{\mathbb{Q}_p}, \Omega^1) \backslash \{0\}$$

such that

$$\log(J(\mathbb{Q}))(\omega_0) = 0.$$

*call ω_0 an **annihilating differential**.*

Sketch proof: $\dim_{\mathbb{Q}_p} \overline{\log J(\mathbb{Q})} = \operatorname{rk}(\mathbb{Z}_p \cdot \log J(\mathbb{Q})) \leq r < g = \dim_{\mathbb{Q}_p} H^0(X_{\mathbb{Q}_p}, \Omega^1)$ □

Corollary 4.2. *Let $P, Q \in X(\mathbb{Q})$, then*

$$\log([P - Q])(\omega_0) = 0$$

Definition 4.3. *For $P, Q \in X(\mathbb{Q}_p)$, and $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ then define*

$$\int_Q^P \omega := \log([P - Q])(\omega)$$

Definition 4.4. *The **residue disk** of $\overline{P} \in \overline{X}(\mathbb{F}_p)$ is*

$$D_{\overline{P}} := \left\{ Q \in X(\mathbb{Q}_p) \mid \overline{Q} = \overline{P} \right\}$$

Lemma 4.5. *Let $P \in X(\mathbb{Q}_p)$, and $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ such that $\overline{\omega} \in H^0(\overline{X}, \Omega^1) \backslash \{0\}$. Let t be a uniformiser at P such that $\overline{t}$ is a uniformiser at $\overline{P}$. Then*

1. *$t : D_{\overline{P}} \cong p\mathbb{Z}_p$ where $t \mapsto p$ defines the map.*
2. *There is an expansion $\omega = \omega(t)dt$ convergent on $D_{\overline{P}}$ such that $\omega(t) \in \mathbb{Z}_p[[t]]$.*
3. *For $Q \in D_{\overline{P}}$,*

$$\int_P^Q \omega = \int_0^{t(Q)} \omega(t)dt$$

Lemma 4.6. *Let $\ell \in \mathbb{Q}_p[[t]]$ such that the derivative $w := \ell' \in \mathbb{Z}_p[[t]]$. Let $\nu := \operatorname{ord}_{\overline{t}=0} \overline{w}$. Then if $\nu \leq p - 2$ we have*

$$\#\left\{ t \in p\mathbb{Z}_p : \ell(t) = 0 \right\} \leq \nu + 1$$

We prove this using Newton polygons, but we do not have the time to spend on this.

From now on we will assume that:

- $r < g$
- ω_0 is an annihilating differential which is scaled so that $\overline{\omega_0} \in H^0(\overline{X}, \Omega^1) \setminus \{0\}$

Corollary 4.7. *Let $\overline{P} \in \overline{X}(\mathbb{F}_p)$. If $\nu_{\overline{P}} := \operatorname{ord}_{\overline{t}=0} \overline{\omega_0} \leq p-2$ then*

$$\#D_{\overline{P}} \cap X(\mathbb{Q}) \leq \nu_{\overline{P}} + 1$$

Note that this actually proves Faltings/Mordells theorem/conjecture in this case, since there are finitely many points over the residue field so finitely many residue disks and then the corollary tells us that there are finitely many points in each residue disk.

Proof. WLOG there is a point $P \in D_{\overline{P}} \cap X(\mathbb{Q})$. Fix a uniformiser t at P as above. For all $Q \in D_{\overline{P}} \cap X(\mathbb{Q})$:

$$\begin{aligned} 0 &= \int_P^Q \omega_0 \\ &= \int_0^{t(Q)} w(t)dt && w \in \mathbb{Z}_p[[t]] \\ &= \ell(t(Q)) \end{aligned}$$

where $\ell \in \mathbb{Q}_p[[t]]$ satisfies the conditions of the lemma. □

Theorem 4.8 (Coleman)**.** *Let $r < g$ and $p > 2g$. Then*

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

Proof. For $\overline{P} \in \overline{X}(\mathbb{F}_p)$,

$$\begin{aligned} \nu_{\overline{P}} &\leq \sum_{\overline{Q} \in \overline{X}(\mathbb{F}_p)} \nu_{\overline{Q}} \\ &= \deg \operatorname{Div} \overline{\omega_0} \\ &= 2g - 2 && \text{(Reimann Roch)} \\ &< p - 2 \end{aligned}$$

Now sum over all $\overline{P} \in \overline{X}(\mathbb{F}_p)$ and apply the corollary above. □

Remark 4.9. *There are improvements, in practice this bound is almost never sharp.*

Corollary 4.10. *If* Reg *and $\nu_{\overline{P}} \leq p-2$ for all $\overline{P}$ and $\#X(\mathbb{Q})_{\text{known}} \cap D_{\overline{P}} = 1 + \nu_{\overline{P}}$ then*

$$X(\mathbb{Q}) = X(\mathbb{Q})_{\text{known}}$$

Example 4.

$$X : X : y^2 = x^6 - 4x^4 + 8x^2 - 4$$

- $r = 1 < 2 = g$
- $p = 3 \nmid \operatorname{disc}(X)$

staring at the equation for a little bit we see eight points:

$$X(\mathbb{Q})_{\text{known}} = \{\infty_\pm, (\pm 1, \pm 1)\}\,.$$

Compute (will say more on Friday)

$$\int_{(-1,-1)}^{(1,1)} \frac{dx}{y} = 0 \neq \int_{(-1,-1)}^{(1,1)} x\frac{dx}{y}$$

where the nonequality on the right tells us that $[(1,1)-(-1,-1)]$ *is not torsion. Can thus take an annihilating differential* $\omega_0 = \frac{dx}{y}$.

For $P = (1,1)$*, take uniformizer* $t = x - 1$ *(works because* P *is not a Weierstass point), on* $D_{\overline{P}}$*,*

$$\begin{aligned}\frac{dx}{y} &= (1 + 6t - t^2 + 4t^3 + 11t^4 + 6t^5 + t^6)^{-1/2}dt \\ &= (1 - 3t + 14t^2 + \dots)dt \\ &\Rightarrow \nu_{\overline{P}} = 0 \\ &\Rightarrow D_{\overline{P}} \cap X(\mathbb{Q})_{\text{known}} = \{(1,1)\}\end{aligned}$$

The same holds for all $(\pm 1, \pm 1)$*. But* $\nu_{\infty_\pm} = 1$

We thus know that $X(\mathbb{Q})\backslash X(\mathbb{Q})_{\text{known}} \subset D_{\infty_+} \cup D_{\infty_+}$*. Can compute the zeroes of*

$$Q \mapsto \int_{\infty_\pm}^{Q} \omega_0$$

on $D_{\infty_\pm}$*. Show that zeroes* $\neq \infty_\pm$ *are not rational.*

Lecture 4: Mordell-Weil Sieve

Today we talk about yet another method for rational points, which rather than working with complicated p-adic analysis we will work with information $\mod p$. Given $X/\mathbb{Q}$ a nice curve with genus $g \geq 2$, let $J = \operatorname{Jac} X$ and let $X \xhookrightarrow{\iota} J/\mathbb{Q}$ be an Abel-Jacobi map. Assume that generators of $J(\mathbb{Q})$ are given. We have a commutative diagram for p a prime of good reduction.

$$\begin{array}{ccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle \nu_p} \\ \overline{X}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \overline{J}(\mathbb{F}_p) \end{array} \tag{1}$$

$\iota(X(\mathbb{Q})) \subset \nu_p^{-1}\iota_p(\overline{X}(\mathbb{F}_p)) =: V_p$. Let S be some set of good primes, then

Theorem 4.11 (Scharaschkin)**.** *If* $\bigcap_{p\in S} V_p = \emptyset$ *then* $X(\mathbb{Q}) = \emptyset$.

Is there any hope of this being true? Well there is a heuristic due to Poonen

Heuristic 1 (Poonen)**.** *If* $X(\mathbb{Q}) = \emptyset$ *then there exists some* S *finite such that*

$$\bigcap_{p\in S} V_p = \emptyset$$

In fact this is related to the Brauer Manin obstruction, as was shown by Scharaschkin under assumption that Ш is finite.

Remark 4.12. *Can also:*

- *Work mod p^n for $n > 1$,*
- *Use bad primes*

Suppose that $X(\mathbb{Q}) \neq \emptyset$, and we have $X(\mathbb{Q})_{\text{known}} \subset X(\mathbb{Q})$ we want to show equality. Fix $b \in X(\mathbb{Q})_{\text{known}}$ and let $\iota(P) = [P - b]$ be our fixed Abel-Jacobi map. Let $p \in S$ and $\overline{P} \in \overline{X}(\mathbb{F}_p) \backslash X(\mathbb{Q})_{\text{known}}$. If

$$\nu_p^{-1}(\iota_p(\overline{P})) \not\subset \bigcap_{q \in S} V_q$$

then $\overline{P} \notin \overline{X(\mathbb{Q})}$.

Note that, compared to the version of Chabauty we saw yesterday, this can actually detect when the set of rational points is empty which Chabauty (as we saw it) cannot. More generally, Chabauty uses $\rho : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ where $P \mapsto \int_0^P \omega_0$ for ω_0 an annihilating differential, so that $\rho(X(\mathbb{Q})) = 0$. This means that the zeroes of ρ are precisely $X(\mathbb{Q}) \cup Z \subset X(\mathbb{Q}_p)$, and one can show that $Z \cap X(\mathbb{Q}) = \emptyset$ using congruence conditions and Mordell-Weil Sieve. We adapt the commutative diagram (1) to the set of primes S to look at:

$$\begin{array}{ccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle \nu_S} \\ \prod_{p \in S} \overline{X}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \prod_{p \in S} \overline{J}(\mathbb{F}_p) \end{array} \tag{2}$$

Consider $C : Q + NJ(\mathbb{Q})$ for $N \geq 2$ and $Q \in J(\mathbb{Q})$. If $\nu_S(C) \cap \text{im}(\iota_S)$ then there are no rational points on the curve mapping into C, i.e. $\iota(X(\mathbb{Q})) \cap C = \emptyset$. Extending (2) we look now at

$$\begin{array}{ccccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle \nu_S} & & \downarrow{\scriptstyle \beta_{S,N}} \\ \prod_{p \in S} \overline{X}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \prod_{p \in S} \overline{J}(\mathbb{F}_p) & \longrightarrow & \prod_{p \in S} \overline{J}(\mathbb{F}_p)/N\overline{J}(\mathbb{F}_p) \end{array} \tag{3}$$

we label the composition along the bottom row as $\alpha_{S,N}$. We want $\gcd(N, \#\overline{J}(\mathbb{F}_p))$ to be big for many $p \in S$.

Suppose for some reason you know that $X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})/NJ(\mathbb{Q})$. This gives rise to a method where we try to compute $X(\mathbb{Q})$ as follows:

1. Select suitable S,
2. For all $c \in J(\mathbb{Q})/NJ(\mathbb{Q})$, such that no $P \in X(\mathbb{Q})_{\text{known}}$ maps to c.
   - *By day*, try to show that $\beta_{S,N}(c) \notin \text{im}(\alpha_{S,N})$
   - *By night*, search for rational points $P \in X(\mathbb{Q})$ mapping to C.

Lemma 4.13. *Let $r < g$ and p a good prime, $\omega_0 \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ an annihilating differential such that $\overline{\omega_0} \in H^0(\overline{X}, \Omega^1)\setminus\{0\}$. Assume that $\overline{\omega_0}(\overline{P}) \neq 0$ for all $\overline{P} \in \overline{X}(\mathbb{F}_p)$. Let $N \geq 2$ be such that N is divisible by the exponent of $\#\overline{J}(\mathbb{F}_p)$. Then*

$$X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})/NJ(\mathbb{Q})$$

is an injection.

Proof. Let $P, Q \in X(\mathbb{Q})$ be such that $\iota(P) - \iota(Q) \in NJ(\mathbb{Q})$. Then $\overline{\iota(P)} = \overline{\iota(Q)}$ since N is divisible by the exponent. But $\bar{\iota}$ is an injection so $\overline{P} = \overline{Q}$. However, $\overline{\omega_0}(\overline{P}) \neq 0$ then $\#D_{\overline{P}} \cap X(\mathbb{Q}) \leq 1$ so $P = Q$. □

We get a practical method to compute $X(\mathbb{Q})$ if $r < g$ and if we can

- Compute $\int_P^Q \omega$ for $\overline{P} \neq \overline{Q}$. There is $n \mid \#\overline{J}(\mathbb{F}_p)$ such that $n[Q - P] = \sum_i [Q_i - P_i]$ where $\overline{Q_i} = \overline{P_i}$ for all i. Then
$$\int_P^Q \omega = \frac{1}{n} \sum_i \int_{P_i}^{Q_i} \omega$$
however $P_i, Q_i \in X(\overline{\mathbb{Q}_p})$, so this may be difficult.
- Use Coleman integration, for which you need a lift of Frobenius to a certain p-adic cohomology group. (See Balakrishnan-Bradshaw-Ketlaya for more details, or Balakrishnan-Tuitman for an extension to greater generality)
- Show $r < g$ (r is rank!) and find r independent points in $J(\mathbb{Q})$ mod $J(\mathbb{Q})_{\text{tors}}$ to find ω_0. We can often work entirely in $\text{Sel}^{(2)}(J/\mathbb{Q})$ (See Poonen-Stoll or Stoll).

Example 5. *This will not use anything we said so far, but do something much simpler.*

$$X : y^2 = x^6 - 4x^4 + 8x^2 - 4$$

Chabauty did not work for this. Consider the quotient elliptic curve obtained via $\varphi : (x, y) \mapsto (x^2, y)$:

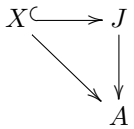
$$E : y^2 = x^3 - 4x^2 + 8x - 4$$

$X(\mathbb{Q}) \subset \varphi^{-1}E(\mathbb{Q})$. But $\text{rk}(E(\mathbb{Q})) = 1$, so no use. However, the Jacobian of X is an abelian variety of dimension 2 which will contain E, so there is another elliptic curve in this. Consider

$$E' : y^2 = -4x^3 + 8x^2 - 4x + 1$$

obtained by $(x, y) \mapsto (x^{-2}, yx^{-3})$. Show that $E'(\mathbb{Q}) = \{\infty, (0, \pm 1), (1, \pm 1)\}$. Thus $X(\mathbb{Q}) = \{\infty_\pm, (\pm 1, \pm 1)\}$.

Example 6. *If $J \sim A \times \dots$ such that $\text{rk}(A/\mathbb{Q}) = 0$ we can use*



If $r = g$ and $\text{rk}(NS(J)) > 1$ (NS here means the Neŕon-Severi group) we can sometimes use non-abelian Chabauty (Kim, Balakrishnan-Dogra,...). Arizona winter school 2020 will be about precisely this, and you are all heartily encouraged to attend.