

- Q: Let  $X$  be a smooth, projective, geometrically integral curve with genus  $g \geq 2$  defined over  $\mathbb{Q}$  describe  $X(\mathbb{Q})$ ?

↳ This has many answers.....

- Theorem: (Faltings)  $\#X(\mathbb{Q}) < \infty$ .

↳ This proof does not give a "workable" bound nor does it actually compute  $X(\mathbb{Q})$ .....

- The goal of Chabauty and Coleman is to do better than this....
- If we are going to succeed we probably need something to put some additional structure on  $X(\mathbb{Q})$ .....

- Def: Let  $X$  be a nice curve s.t.  $X(k) \neq \emptyset$  then the Jacobian of  $X$  is an algebraic variety  $J$  s.t. there are functorial isomorphisms

$$J(k') \xrightarrow{\cong} \text{Pic}^0(X(k'))$$

for all extensions  $k'/k$ .

- Recall +  $\text{Pic}(X) = \text{Div}(X) / \text{linearly equivalence}$

$$= \mathbb{Z} \{ \text{closed points} \} / \text{linearly equivalence}$$

$$+ \deg(D) = \sum_i n_i$$

$$+ \text{Pic}^0(X) = \text{degree 0 divisors} \dots$$

• Whatever this  $J$  is all we need is that.....

• Fact:  $J$  is a group, that is finitely generated, and abelian.

+ There is a natural embedding:

$$\begin{aligned} X &\xhookrightarrow{i} J \\ P &\longmapsto [P - O] \end{aligned}$$

where  $O \in X(\mathbb{Q})$ .

• Strategy to answer our question:

1) Understand  $J(\mathbb{Q})$ .

2) Determine which points of  $J(\mathbb{Q}) \in X$ .

• Doing #1 is hard, but "maybe" possible.

• The goal now becomes to get to a place where  $J(\mathbb{Q})$  is finite....

If  $J(\mathbb{Q})$  is finite and  $D \in J(\mathbb{Q})$  then if  $i(P) = D$  then

$$P = D + O + (F)$$

For some  $F \in L(D + O)$ .

↑ This we can understand.

• KEY IDEA: Find some finite subset of  $J(\mathbb{Q})$  containing  $X(\mathbb{Q})$ .

↳ Then we could try and count things.

• Now  $J(\mathbb{R})$  is a  $g$ -dimensional real Lie group. Now  $J(\mathbb{Q}) \subseteq J(\mathbb{R})$

So we could take its closure making  $\overline{J(\mathbb{Q})}$  a real Lie group. Now is

$$\overline{J(\mathbb{Q})} \cap X(\mathbb{R}) \subseteq J(\mathbb{R}) \text{ finite?}$$

well....

$$\dim(\overline{J(\mathbb{Q})} \cap X(\mathbb{R})) = \underset{-2-}{\dim(J(\mathbb{Q}))} + \underset{\uparrow 1}{\dim X(\mathbb{R})} - \underset{\uparrow g}{\dim J(\mathbb{R})}$$

• So if  $\dim \overline{J(\mathbb{Q})} < g$  we are in business.....

↳ Sadly this is not the case and  $\dim \overline{J(\mathbb{Q})} = g$  "most of the time"

↳ when  $J(\mathbb{Q})$  is dense in  $J$  we expect  $\overline{J(\mathbb{Q})}$  to be open in  $J(\mathbb{R})$ .

• Game change.....  $p$ -adic manifolds &  $p$ -adic Lie group.

↳ why? who knows.....

• Def: A function  $f: U \rightarrow \mathbb{Q}_p^m$  where  $U \subseteq \mathbb{Q}_p^n$  is open is locally analytic iff  $\forall p \in U$  there is a neighborhood  $V \subseteq U$  s.t.  $\pi_i \circ f|_V$  is analytic i.e. is a convergent power series.

• Def: A  $p$ -adic manifold is a topological space  $X$  together with an atlas  $\{(\phi_i, U_i)\}$  where  $\phi_i: U_i \rightarrow \mathbb{Q}_p^n$  is a homeomorphism s.t.

$$\phi_i^{-1} \circ \phi_j: U_j \rightarrow U_i$$

is locally analytic.

• Def: A  $p$ -adic Lie group is a  $p$ -adic manifold together with a group structure s.t. the multiplication is locally analytic.

• Facts: 1)  $X(\mathbb{Q}_p)$  is a  $p$ -adic manifold (assuming  $X$  is smooth)  
2)  $J(\mathbb{Q}_p)$  is a  $p$ -adic Lie group...

• Now we play the same game  $\overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p)$  be the  $p$ -adic closure

$$\dim [X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}] = \dim X(\mathbb{Q}_p) + \dim \overline{J(\mathbb{Q})} - \dim J(\mathbb{Q}_p)$$

$\uparrow$   $\uparrow$   $\uparrow$   
 $= 0$  hopefully.  $1$   $g$



- So if  $\dim \overline{J(\mathbb{Q})} < g$  we are in game.... (maybe)  
 $\hookrightarrow$  some place as before.

• Lemma:  $\dim \overline{J(\mathbb{Q})} \leq \text{rank}(J(\mathbb{Q}))$

• Thus if  $\text{rank}(J(\mathbb{Q})) < g$  we are good to go.

• Coleman-Chabauty-Hypothesis:  $\dim \overline{J(\mathbb{Q})} < g$ .

• We now suspect  $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$  is finite, but how could we count any of this.... USE THE LIE GROUP STRUCTURE.

• Since  $\overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p)$  and  $\dim \overline{J(\mathbb{Q})} \leq \dim(J(\mathbb{Q}_p))$  we know

$$T \overline{J(\mathbb{Q})} \subsetneq T J(\mathbb{Q}_p)$$

moreover there is a map

$$\lambda: T J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

That vanishes on  $T \overline{J(\mathbb{Q})}$ .

• Moreover since  $J(\mathbb{Q}_p)$  is a lie group we have the log map

$$\log: J(\mathbb{Q}_p) \longrightarrow T J(\mathbb{Q}_p)$$

So by composing these we get an locally analytic map

$$\eta_J: J(\mathbb{Q}_p) \xrightarrow{\log} T J(\mathbb{Q}_p) \xrightarrow{\lambda} \mathbb{Q}_p$$

That vanishes on  $\overline{J(\mathbb{Q})}!!$  So we get an analytic map

$$\eta: X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

that vanishes exactly on  $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}!!$

- So to bound  $X(\mathbb{Q})$  we just need to bound the # of zeros of  $\eta$  !!

{  $\rightarrow$  So what this seems untrackable...  
 $\rightarrow$  Again harness the power of Lie groups?

- In particular, we use the fact that  $\eta$  is related to integration.

- Fact: The functional  $\lambda: T\mathcal{J}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$  corresponds to a non-zero differential  $\omega_{\mathcal{J}} \in H^0(\mathcal{J}_{\mathbb{Q}_p}, \Omega^1)$ . Then the map  $\eta$  is given by

$$\eta_{\mathcal{J}}^*: \overline{\mathcal{J}}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

$$\mathbb{Q} \longmapsto \underbrace{\int_0^{\theta} \omega_{\mathcal{J}}}_{\text{What exactly this is} \dots \text{is somewhat mysterious.}}$$

- Prop:  $\eta_{\mathcal{J}}$  is characterized as

1) Being a group homomorphism.

2) There is an open neighborhood  $\mathcal{U} \subseteq \mathcal{J}(\mathbb{Q}_p)$  s.t

$\forall \theta \in \mathcal{U}$ , we may compute  $\eta_{\mathcal{J}}(\theta)$  by formally expanding  $\omega_{\mathcal{J}}$  in local coordinates & formally anti-differentiating.

- So now we may think about  $\eta$  as an integral, and it seems like we might be able to actually count zeros.

- Doing exactly this - in a clever way - we get the following theorem of Coleman.

• Theorem: (Coleman '85): Let  $X$  be a smooth <sup>curve</sup> of genus  $g \geq 2$  and  $p$  be a prime of good reduction for  $X$  s.t.

$$\dim \overline{J(\mathbb{Q})} \leq g \quad (\text{CCH}).$$

If  $p > 2g$  then

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

• Ex:  $X: y^2 = x(x-1)(x-2)(x-5)(x-6)$

$$\left. \begin{array}{l} \bullet \text{Smooth} \\ \bullet \text{genus 2 curve} \\ \bullet J(\mathbb{Q}) \text{ has rank one} \end{array} \right\} \dim \overline{J(\mathbb{Q})} \leq \text{rank } J(\mathbb{Q}) < g \quad (\text{CCH})$$

Moreover this curve has good reduction at  $p=7$ .

$$\# X(\mathbb{F}_7) = 8$$

So Coleman implies

$$\# X(\mathbb{Q}) \leq \# X(\mathbb{F}_7) + 2g - 2 = 8 + 2 \cdot 2 - 2 = 10$$

$$X(\mathbb{Q}) = \left\{ (0,0), (1,0), (2,0), (5,0), (6,0), (3, \pm 6), (10, \pm 20), \infty \right\}$$

## Sketch of Proof : 3 Steps:

### 1) Properties of $\eta$ :

A) If  $\theta_i, \theta_i' \in X(\mathbb{Q}_p)$  st  $\text{div}(f) = \sum [\theta_i' - \theta_i]$  then

$$\sum_i \int_{\theta_i}^{\theta_i'} \omega \equiv 0$$

B) If  $\theta, \theta' \in X(\mathbb{Q}_p)$  have the same image under the map  $X(\mathbb{Q}_p) \longrightarrow X(\mathbb{F}_p)$  then

$$\int_{\theta}^{\theta'} \omega$$

may be computed by expanding  $\omega$  as a power series.

C) If  $\theta_i, \theta_i' \in X(\mathbb{Q}_p)$  st  $\sum [\theta_i - \theta_i'] \in \overline{J}(\mathbb{Q})$  then

$$\sum \int_{\theta_i'}^{\theta_i} \omega \equiv 0.$$

i.e.  $\omega \in \mathbb{Q}_p[[t]]$  for some neighborhood.

$$\hookrightarrow \text{Here } \int_{\theta_i}^{\theta_i'} \omega = \int_0^{[a_i - a_i']} \omega_j$$

where  $\omega_j \mapsto \omega$  under the isomorphism  $H^0(J_{\mathbb{Q}_p}) \longrightarrow H^0(X_p)$ .

2)  $p$ -adic zero count: If  $f(t) \in \mathbb{Q}_p[[t]]$  st  $f'(t) \in \mathbb{Z}_p[[t]]$

$\S \text{ord}_{t=0} [f'(t) \bmod p] < p-2 \Rightarrow f(t)$  has at most  $m+1$  zeros in  $\mathbb{P}^1_p$

$\hookrightarrow$  Newton polygon

• 3: Put it together...