Southwest Center
for Arithmetic Geometry

ARIZONA WINTER SCHOOL 2020

Department of Mathematics
The University of Arizona®

Deadline to apply for funding:
November 8, 2019

http://swc.math.arizona.edu

NONABELIAN CHABAUTY

Jennifer Balakrishnan
Computational tools for quadratic Chabauty

Bas Edixhoven
Geometric quadratic Chabauty

Minhyong Kim
Foundations of nonabelian Chabauty

David Zureick-Brown
Classical Chabauty

with **Bjorn Poonen**, Clay Lecturer

TUCSON, MARCH 7-11, 2020

Funded by the National Science Foundation
Supported by the National Security Agency
Organized in partnership
with the Clay Mathematics Institute

University of Arizona

Arizona Winter School 2020
Nonabelian Chabauty

Notes By: Caleb McWhorter

March 2020

Contents

Part I
Talk Notes

1 Bjorn Poonen: Introduction to Chabauty's method and Kim's non-abelian generalization

1.1 Lecture 1

1.1.1 Rational points on Curves

The starting point is Falting's Theorem, which was originally known as Mordell's conjecture.

Theorem 1.1 (Falting's, 1983)**.** *Suppose* $[K\colon \mathbb{Q}] < \infty$*, and let* X *be a 'nice'*[1] *curve of genus* g *over* K*. If* $g > 1$*, then* $X(K)$ *is finite.*

There are several proofs now. The first was Falting's proof in 1983 based on Arakelov methods. The next was by Vojta 1991 and its variant (phrased in more elementary terms via Diophantine approximation) by Bomberi. But now there is a proof by Lawrence-Venkatesh in 2018 via p-adic period maps.

For integral points, the parallel to Falting's Theorem is Siegel's Theorem. Let $[K\colon \mathbb{Q}] < \infty$. Let $\mathcal{O} = \mathcal{O}_{K,S} = \{x \in K\colon v(x) \geq 0 \text{ for all } v \in S\}$, where S is a finite set of places, including all the archimedean places. Let $U := X \setminus Z$, where X is a nice curve of genus g and Z is a nonempty 0-dimensional subscheme. Now $\chi(U) := (2-2g) - r$, where $r = \#Z(\overline{K})$ and χ is the Euler characteristic. Suppose $\mathcal{U}$ is a finite type $\mathcal{O}$-scheme with $\mathcal{U}_K = U$. If $\chi(U) < 0$. The condition that $\chi(U) < 0$ is sometimes phrased as that U is hyperbolic [over $\mathbb{C}$, $\widetilde{U} \simeq b$].

Theorem 1.2 (Siegel's Theorem)**.** *If* $\chi(U) < 0$*, then* $\mathcal{U}(\mathcal{O})$ *is finite.*

There is a proof, obviously, by Siegel. But there are also proofs by Baker-Coates (1970) when either $g \leq 1$ or when U is $y^2 = f(x)$ in $\mathbb{A}^2$, and Lawrence-Venkatesh (2018) when $U = \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Example 1.1. If $U = \mathbb{P} \setminus \{0, 1, \infty\}$, then $\mathcal{U} = \operatorname{Spec} \mathcal{O}[x, \frac{1}{x}, \frac{1}{1-x}]$ and $\mathcal{U}(\mathcal{O})$ is the set of solutions to $x + y = 1$ with $x, y \in \mathcal{O}^\times$.

Remark. Falting's Theorem is strictly harder than Siegel's Theorem in that Falting's Theorem implies Siegel's Theorem. The key idea is that if $\chi(U) < 0$, then there is some finite étale cover of U is open in a nice curve of genus greater than 1.

In Siegel-Falting, $\chi(U) < 0$ means that

- $g = 0$, then $r \geq 3$
- $g = 1$, then $r \geq 1$
- $g \geq 2$, r arbitrary

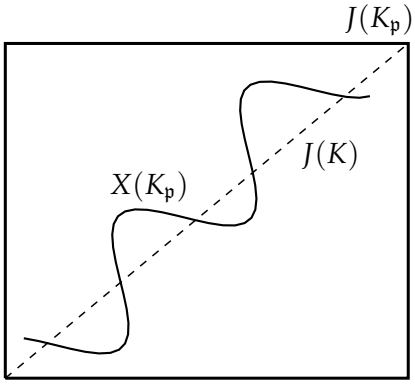
The problem with nearly all of these methods is that they are not effective. The goal is then to try to make them effective. This was exactly the hope of Chabauty.

[1] smooth, projective, geometrically integral

1.1.2 Chabauty's Method

$$\begin{array}{ccc} K & & \mathfrak{p} \\ {\scriptstyle [K:\mathbb{Q}]=\dim_{\mathbb{Q}} K}\Big| & & \Big| \\ \mathbb{Q} & & p \end{array}$$

Let X be a nice curve of genus g over K. Then X is a g-dimensional abelian variety. Let $J = \operatorname{Jac} X$ and let $r = \operatorname{rank} J(K)$. Choose $x \in X(K)$ to get $X \hookrightarrow J$.



$$\begin{array}{ccccc} X(K) & \longrightarrow & X(K_\mathfrak{p}) & & \\ \downarrow & & \downarrow & & \\ J(K) & \longrightarrow & J(K_\mathfrak{p}) & \xrightarrow{\log} & \operatorname{Lie} J_{K_\mathfrak{p}} \simeq K_\mathfrak{p}^g \end{array}$$

The kernel of the log map is finite and is a local diffeomorphism so the image will be open and compact (J is a compact group). Therefore, the image of log is an open compact subgroup of the Lie group $\operatorname{Lie} J_{K_\mathfrak{p}}$. Moreover, the image of $J(K) \to K_\mathfrak{p}^g$ is generated by r elements. Then the dimension of $K_\mathfrak{p}$-span of the image is at most r. If $r < g$, there exists a nonzero linear $\lambda : \operatorname{Lie} J_{K_\mathfrak{p}} \to K_\mathfrak{p}$ vanishing in $J(K)$, and λ pulls back to a nonzero locally analytic function on $X(K_\mathfrak{p})$ vanishing on $X(K)$, so $X(K)$ is finite. But of course, this all requires what might be called Chabauty's condition: $r < g$.

How do we limit the role of the Jacobian in this to generalize? Rewriting

$$\begin{array}{ccccc} X(K) & \longrightarrow & X(K_\mathfrak{p}) & & \\ \downarrow & & \downarrow & & \\ J(K) & \longrightarrow & J(K_\mathfrak{p}) & \xrightarrow{\log} & \operatorname{Lie} J_{K_\mathfrak{p}} \\ \downarrow & & \downarrow & \nearrow \wr & \\ \widehat{J(K)}[\tfrac{1}{p}] & \longrightarrow & \widehat{J(K_\mathfrak{p})}[\tfrac{1}{p}] & & \end{array}$$

Given M, an abelian group, define $\widehat{M} := \varprojlim M/p^n M$, which is a $\mathcal{Z}_p$-module. Then $\widehat{M}[\frac{1}{p}] \simeq \widehat{M} \otimes_{\mathcal{Z}_p} \mathbb{Q}_p$, which is a $\mathbb{Q}_p$ vector space.

V is étale homology. As a motivation, if X is a curve over $\mathbb{C}$ and J is its Jacobian. Then analytically, $J(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$, where $\Lambda = H_1(J(\mathbb{C}), \mathcal{Z})$. Using the right hand side, it is easy to see that

$$J[p] \simeq \frac{1}{p}\Lambda/\Lambda \xrightarrow{p} \Lambda/p\Lambda = H_1(J(\mathbb{C}), \mathcal{Z}/p\mathcal{Z}) = H_1(X(\mathbb{C}), \mathcal{Z}/p\mathcal{Z})$$

If we are not using $\mathbb{C}$, we are going to have to switch to Étale (co)homology.

For X over K, $J[p] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathcal{Z}/p\mathcal{Z}) := \mathcal{Z}/p\mathcal{Z}$-dual of $H^1_{\text{ét}}(X_{\overline{K}}, \mathcal{Z}/p\mathcal{Z})$. Likewise, $J[p^n] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathcal{Z}/p^n\mathcal{Z})$. Now $\mathcal{Z}_p$ is the Tate module, where $T := \varprojlim J[p^n] \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathcal{Z}_p)$. Tensoring with $\mathbb{Q}_p$, we obtain the $\mathbb{Q}_p$-Tate module $V := T[\frac{1}{p}] = T \otimes_{\mathcal{Z}_p} \mathbb{Q}_p \simeq H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$, which is a $\mathbb{Q}_p$-vector space of dimension $2g$.

Now write $\mathcal{V}(\mathbb{Q}_p)$ for a group variety $\mathcal{V} \simeq \mathbb{G}_a^{2g}$ over $\mathbb{Q}_p$. Note that $\mathcal{V}$ is $\mathbb{A}^{2g}$ with an additive group law. The group $G_K := \text{Gal}(\overline{K}/K)$ acts continuously on all of these, e.g. $G_K \to \text{Aut}\,\mathcal{V} \simeq \text{GL}_n(\mathbb{Q}_p)$, as a group variety.

1.2 Lecture 2

1.2.1 Selmer Groups

$$0 \longrightarrow J[p] \longrightarrow J \xrightarrow{p} J \longrightarrow 0$$

$$J(K) \xrightarrow{p} J(K) \longrightarrow H^1(K, J[p])$$

$$\frac{J(K)}{pJ(K)} \hookrightarrow H^1(K, J[p])$$

But the right side is an infinite dimensional $\mathbb{F}_p$-vector space if $\dim J \geq 0$.

$$\begin{array}{ccccc} \dfrac{J(K)}{pJ(K)} & \hookrightarrow & \mathrm{Sel}_p J & \subseteq & H^1(K, J[p]) \\ & & & & \downarrow \beta \\ \prod_\nu \dfrac{J(K_\nu)}{pJ(K_\nu)} & & \xhookrightarrow{\alpha} & & \prod_\nu H^1(K_\nu, J[p]) \end{array}$$

$\mathrm{Sel}_p J := \{\xi \in H^1(K, J[p]) \colon \beta(\xi) \in \operatorname{im} \alpha\}$. This group is conjecturally finite and computable.

Similarly,

$$\frac{J(K)}{p^n J(K)} \hookrightarrow \mathrm{Sel}_{p^n} J \subset H^1(K, J[p^n])$$

By taking inverse limits

$$\widehat{J(K)} \hookrightarrow \mathrm{Sel}_{\mathcal{Z}_p} J \subset H^1(K, T)$$

then by inverting p

$$\widehat{J(K)}\left[\frac{1}{p}\right] \hookrightarrow \mathrm{Sel}_{\mathbb{Q}_p} J \subset H^1(K, V)$$

Then we have

$$0 \longrightarrow \frac{J(K)}{pJ(K)} \longrightarrow \mathrm{Sel}_p J \longrightarrow Ш[p] \longrightarrow 0$$

$$0 \longrightarrow \widehat{J(K)}\left[\frac{1}{p}\right] \longrightarrow \mathrm{Sel}_{\mathbb{Q}_p} J \longrightarrow \left(\varprojlim Ш[p^n]\right)\left[\frac{1}{p}\right] \longrightarrow 0$$

$$\begin{array}{ccccc} X(K) & \longrightarrow & X(K_\mathfrak{p}) & & \\ \downarrow & & \downarrow & & \\ J(K) & \longrightarrow & J(K_\mathfrak{p}) & \xrightarrow{\log} & \mathrm{Lie}\, J_{K_\mathfrak{p}} \\ \downarrow & & \downarrow & \nearrow \wr & \\ \widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_\mathfrak{p})}[\frac{1}{p}] & & \\ \downarrow & & & & \\ \mathrm{Sel}_{\mathbb{Q}_p} J & & & & \\ \downarrow & & & & \\ H^1(K, V) & \longrightarrow & H^1(K_\mathfrak{p}, V) & & \end{array}$$

1.2.2 Bloch-Kato Selmer Group

We examine the Block-Kato Selmer group in terms of V and not J. In the general setting (local Galois representations), let V be a finite dimensional $\mathbb{Q}_p$-vector space with continuous action—G_{K_ν}-action.

$$D_{\text{cris}}(V) := (B_{\text{cris}} \otimes_{\mathbb{Q}_p} V)^{G_{K_\nu}}$$

where B_{cris} is a certain ring equipped with a G_{K_ν}-action.

Remark. $\dim_{K_\nu} D_{\text{cris}}(V) \leq \dim_{\mathbb{Q}_p} V$

Definition (Crystalline)**.** We call V crystalline if equality holds.

Remark. For ν and an abelian variety J/K_ν, then J has good reduction if and only if its $\mathbb{Q}_p$ Tate module V is unramified if $\nu \nmid p$ and crystalline if $\nu \mid p$.

Now suppose $\xi \in H^1(K, V)$. Let

$$0 \longrightarrow V \longrightarrow E \longrightarrow \mathbb{Q}_p \longrightarrow 0$$

be the corresponding extension. Call ξ crystalline if E is crystalline.

$$H^1_f(K_\nu, V) := \{\text{crystalline classes in } H^1(K_\nu, V)\}$$

Remark. $\mathfrak{p} \mid p$. If J is an abelian variety with good reduction at $\mathfrak{p}$, and V is a $\mathbb{Q}_p$ Tate module, then the iamge of

$$\widehat{J(K_\mathfrak{p})}[\frac{1}{p}] \to H^1(K_\mathfrak{p}, V)$$

equals $H^1_f(K_\mathfrak{p}, V)$. If $\mathfrak{p} \nmid p$, then $H^1(K_\mathfrak{p}, V = 0$.

1.2.3 Global Galois Representations

Let V be a finite dimensional $\mathbb{Q}_p$-vector space with continuous G_K-action. Given $\xi \in H^1(K, V)$. Let ξ_ν be its image in $H^1(K_\ni, V)$. The Bloch-Kato Selmer group of v is the group

$$H^1_f(K, V) := \{\xi \in H^1(K, V) \colon \xi_\nu \text{ is crystalline for all } \nu \mid p\}$$

Remark. If J is an abelian variety over K and V is a $\mathbb{Q}_p$ Tate module, then $H^1_f(K, V) = \text{Sel}_{\mathbb{Q}_p} J$.

$$\begin{array}{ccccc}
X(K) & \longrightarrow & X(K_\mathfrak{p}) & & \\
\downarrow & & \downarrow & & \\
J(K) & \longrightarrow & J(K_\mathfrak{p}) & \xrightarrow{\log} & \text{Lie } J_{K_\mathfrak{p}} \\
\downarrow & & \downarrow & \nearrow & \\
\widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_\mathfrak{p})}[\frac{1}{p}] & & \\
\downarrow & & \downarrow & & \\
\text{Sel}_{\mathbb{Q}_p} J = H^1_f(K, V) & \longrightarrow & H^1_f(K_\mathfrak{p}, V) & & \\
\downarrow & & \downarrow & & \\
H^1(K, V) & \longrightarrow & H^1(K_\mathfrak{p}, V) & &
\end{array}$$

Algebraic de Rham Cohomology: $H^1_{\mathrm{dR}}(X) := \mathbb{H}^1(X, \Omega^0)$ with Hodge filtration Fil^0, where $\mathbb{H}$ is hypercohomology. Define also $H_1^{\mathrm{dR}}(X) :=$ dual of H^1_{dR} with dual filtration.

$$\begin{array}{ccccc}
X(K) & \longrightarrow & X(K_\mathfrak{p}) & & \\
\downarrow & & \downarrow & & \\
J(K) & \longrightarrow & J(K_\mathfrak{p}) & \xrightarrow{\log} & \mathrm{Lie}\, J_{K_\mathfrak{p}} \\
\downarrow & & \downarrow & \nearrow & \\
\widehat{J(K)}[\frac{1}{p}] & \longrightarrow & \widehat{J(K_\mathfrak{p})}[\frac{1}{p}] & & \\
\downarrow & & \downarrow & & \\
\mathrm{Sel}_{\mathbb{Q}_p} J = H^1_f(K, V) & \longrightarrow & H^1_f(K_\mathfrak{p}, V) & \xrightarrow{\log,\sim} & H_1^{\mathrm{dR}}(K_{K_\mathfrak{p}})/\,\mathrm{Fil}^0 \\
\downarrow & & \downarrow & & \\
H^1(K, V) & \longrightarrow & H^1(K_\mathfrak{p}, V) & &
\end{array}$$

We get

$$\begin{array}{ccccc}
X(K) & \longrightarrow & X(K_\mathfrak{p}) & & \\
\downarrow & & \downarrow & \searrow^{p\text{-adic integrals}} & \\
H^1_f(K, V) & \longrightarrow & H^1_f(K_\mathfrak{p}, V) & \xrightarrow{\sim} & H_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})/\,\mathrm{Fil}^0
\end{array}$$

1.2.4 Lower Central Series

Let G be a (topological) group. For $A, B \leq g$, define $(A, B) := \overline{\langle aba^{-1}b^{-1} \colon a \in A, b \in B\rangle}$. Now define the lower central series by

$$\begin{aligned}
C^1G &:= G \\
C^2G &:= (G, C^1G) = (G, G) \\
C^3G &:= (G, C^2G) \\
&\vdots
\end{aligned}$$

Finally, define $G_n := G/C^{n+1}G$. This is a n-step nilpotent group.

Example 1.2. $G_1 = G/(G, G) =: G^{ab}$, the abelianization of G, i.e. the largest abelian quotient.

This was just Group Theory. Now let's apply this to the fundamental group of the curve.

1.2.5 Abelianized Fundamental Group

Given M a connected real manifold, $m \in M$, we get $\pi_1(M, m)^a b \simeq H_1(M, \mathcal{Z})$, where π_1 is the fundamental group. What is the algebraic version? Given X, a 'nice' curve of genus g curve over K, $x \in X(K)$, we obtain

$$\pi_1^{\text{ét}}(X_{\overline{K}}, x)^a b \simeq H_1^{\text{ét}}(X_{\overline{K}}, \widehat{\mathcal{Z}})$$

But we have maps

$$\pi_1^{\text{ét}}(X_{\overline{K}}, x)_1 \xrightarrow{\sim} \pi_1^{\text{ét}}(X_{\overline{K}}, x)^a b \simeq H_1^{\text{ét}}(X_{\overline{K}}, \widehat{\mathcal{Z}}) \twoheadrightarrow H_1^{\text{ét}}(X_{\overline{K}}, \mathcal{Z}_p) \subset H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) =: V = \mathcal{V}(\mathbb{Q}_p)$$

Kim obtains a generalization

$$\pi_1^{\text{ét}}(X_{\overline{K}}, x) \longrightarrow V_n = \mathcal{V}_n(\mathbb{Q}_p)$$

where $\mathcal{V}_n$ is some unipotent algebraic group, and

$$\begin{array}{ccccc} X(K) & \longrightarrow & X(K_{\mathfrak{p}}) & & \\ \downarrow & & \downarrow & \searrow^{p\text{-adic iterated integrals}} & \\ H_f^1(K, V_n) & \longrightarrow & H_f^1(K_{\mathfrak{p}}, V_n) & \xrightarrow{\sim} & \pi_1^{\text{dR}}(X_{K_{\mathfrak{p}}}, x)_n / \operatorname{Fil}^0 \end{array}$$

and morphisms of $\mathbb{Q}_p$-varieties

$$\text{Sel}^{[n]} \longrightarrow J^{[n]} \longrightarrow L^{[n]}$$

which gives you the $\mathbb{Q}_p$ points of $\pi_1^{\text{dR}}(X_{K_{\mathfrak{p}}}, x)_n / \operatorname{Fil}^0$.

Theorem 1.3 (Kim). *If for some $n \geq 1$, $\dim \text{Sel}^{[n]} < \dim J^{[n]}$, then $X(K)$ is contained in the set of zeros of some nonzero locally analytic functions on the local points of the curve, which are given by some iterated integrals. Therefore, $X(K)$ is finite.*

2 David Zureick-Brown: Effective Chabauty

2.1 Lecture 1

Lorenzini-Tucker
McCollem-Poonen
Stoll
Katz-ZB

Theorem 2.1 (K-ZB). *Let $X/\mathbb{Q}$ be a 'nice' curve with $r = \operatorname{rank} J(\mathbb{Q})$, and $p > 2r+2$ a prime. Let $\mathfrak{X}$ be a regular proper minimal model of X. Let $r < g$, then*

$$\#(X(\mathbb{Q})) \leq \#\mathfrak{X}^{?}_{\mathbb{F}_p}(\mathbb{F}_p) + 2r$$

Theorem 2.2 (Coleman, "rank favorable bound"). *In the situation above,*

$$\#(X(\mathbb{Q})) \leq \#\mathfrak{X}^{?}_{\mathbb{F}_p}(\mathbb{F}_p) + (2g-2)$$

A question of Mazur is can we bound $\#X(K)$ using the rank of $J(K)$ and g?

Conjecture 2.1 (Uniformity Conjecture). *There exists $B(K,g)$ such that for all nice X/K of genus g with*

$$\#X(K) \leq B(K,g)$$

Work of Poonen et al gives heuristics that, in the case of X an elliptic curve, imply r is bounded.

The Weak Lang Conjecture states that if X/K is a variety of general type, then there is $Z \subseteq X$ closed such that $Z(K) \subseteq X(K)$.

Theorem 2.3 (Caparso,Harris,Mazur). *The Weak Lang Conjecture implies the Uniformity Conjecture*

Example 2.1 (Gordon-Grant, '93). Let $X : y^2 = x(x-1)(x-2)(x-5)(x-6)$. This is a hyperelliptic curve with $g = 2$ and rank 1. But $r = 1 < 2$ so Coleman applies. Then $\#X(\mathbb{Q}) = 10$ GWP, 3 IG and IQ ± 120. But mod 7, we have $\#X(\mathbb{F}_7) = 8$ gWP, $(3, \pm 6)$.

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

Theorem 2.4 (Stoll). *Suppose that X is hyperelliptic, and suppose that $r \leq g-3$. Then $\#X(\mathbb{Q}) \leq 3(r+4)(g-1) + \max\{1, 4r\} \cdot g$.*

Theorem 2.5 (Katz-Rabinoff-ZB). *Suppose $r \leq g-3$. Then $\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28$.*

2.1.1 Effective Manin-Mumford

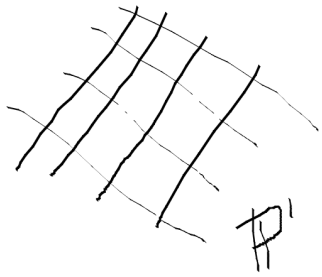
Let X be a curve and $X \overset{i}{\hookrightarrow} J$. Then $\#i(X) \cap J_{\text{tor}} < \infty$, proven by Raynaud, Buildum, Coleman.

$$X \hookrightarrow J \xrightarrow{\log} \operatorname{Lie} J$$

Then the integrals vanish on $X \cap J_{\text{tors}}$. The nice thing here is that there is no necessary rank condition.

Theorem 2.6 (KRZB).

- $(X \cap J_{tors})(\mathbb{Q}) \leq (?)$



- *I and X is very degenerate, e.g. totally degenerate*
  then we can bound $\# \cap J_{tors} \leq ---$

$$\begin{array}{ccccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\ & & \downarrow & \searrow & \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & \text{Lie } J_{\mathbb{Q}_p} \end{array}$$

where the log map is $D \mapsto (\omega \mapsto \int_Q^D \omega)$

'Black box Chabauty'.

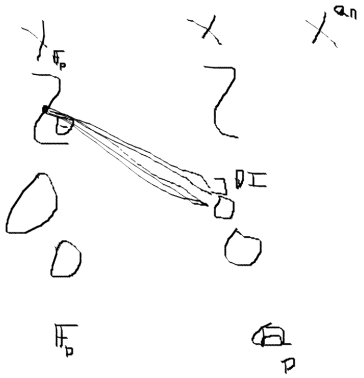
- Setup
- local analysis
- global coordination

Setup

Let $r < g$. There exists $V \subseteq H^0(X_{\mathbb{Q}_p}, \Omega^1)$ such that for all $P, Q \in X(\mathbb{Q})$, $\int_P^Q \omega = 0$ for all $\omega \in V$ and $\dim V \geq g - r > 0$.

Local Analysis:

We can compute $\int_P^Q \omega$ locally and analyze with a Newton Polygon.



[$QI := \{P \in X(\mathbb{Q}_p) \text{ such that } P \equiv Q \mod p\} \simeq p\mathcal{Z}_p$, the p-adic disc. Where the map is $p \mapsto u(P)$, where u is a uniformizer at $\tilde{Q}$, a lift of Q.

Example 2.2 (HP survey)**.** $X : y^2 = f(x) = x^6 + 8x^5 + \cdots + 1 = xg(x) + 1$.

$(0,1) \in X(\mathbb{F}_3)$.

$[(0,1)] \xrightarrow{\sim} p\mathcal{Z}_p$ with map $p \mapsto X(P)$ forward and $t \mapsto (t, \sqrt{tg(t)+1})$, which converges because t is small, $\nu_p(t) > 0$.

To compute $\int_P^Q \omega$, only compute "tiny" integrals, i.e. $P = Q \mod p$. If $Q \in [P] \simeq p\mathcal{Z}_p \ni t$ with $\omega|_{[P]} = f(t)\,dt$ for some $f(t) \in \mathcal{Z}_p[1+1]$.

$$\int_P^Q \omega = \int_Q^t f(t)\,dt = I(t)$$

integrating formally.

2.2 Lecture 2

$\int$'s are locally analytic.

$P \in X(\mathbb{F}_p)$, $Q_1, Q_2 \in [P] \xrightarrow{\sim} P\widehat{i}P$, given by $Q \mapsto t(Q)$, t with respect to P.

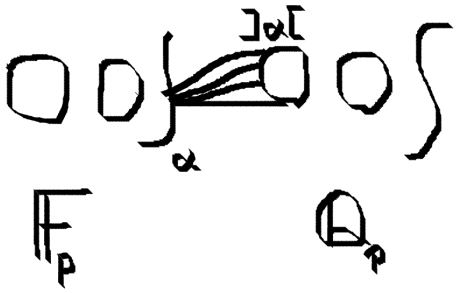
$$\int_{Q_1}^{Q_2} \omega = \int_{t_1}^{t_2} f(t)\, dt = \sum \frac{d_i t^{i+1}}{i+1}\Big|_{t_1}^{t_2} = I_i(t)$$

by the Fundamental Theorem of Calculus.

$$\omega\Big|_{[P]} = f(t)\, dt = \sum a_i t^i, \quad a_i \in \mathcal{Z}_p$$

Theorem 2.7 (Coleman). *If $X/\mathbb{Q}$ is nice, $r < g$, and p is a good prime with $p > 2g$, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2$.*

Proof. Let $Q \in X(\mathbb{F}_p)$ and let $\omega \in V$ be a fixed annihilating differential. Let $n_{\mathbb{Q}} = \deg(\operatorname{Div}\omega \cap [Q])$, then $\#\{z \in p\mathcal{Z}_p \colon I_i(z) = 0\} \leq 1 + n_{\mathbb{Q}}$. Then $\#X(\mathbb{Q}) \leq \#X(\mathbb{Q}_p)_1$ (the $\mathbb{Q}_p$ solutions to these integrals, i.e. the $\mathbb{Q}_p$ points that vanish under the abelian integral). But this is at most $\sum_{Q \in X(\mathbb{F}_p)}(1 + n_{\mathbb{Q}})$



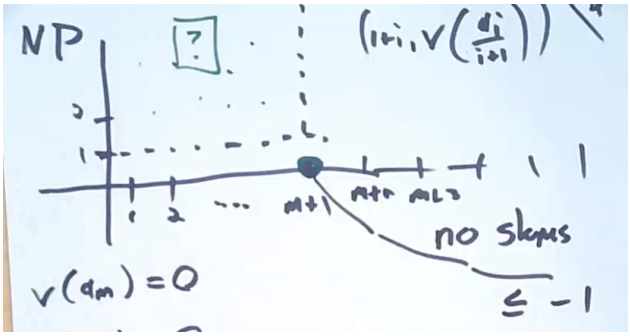
But then we have

$$\begin{aligned}
\#X(\mathbb{Q}) &\leq \#X(\mathbb{Q}_p)_1 \\
&\leq \sum_{Q \in X(\mathbb{F}_p)} (1 + n_{\mathbb{Q}}) \\
&= \sum_{\alpha \in X(\mathbb{F}_p)} + \sum_{\alpha \in X(\mathbb{F}_p)} n_{\mathbb{Q}} \\
&\leq \#X(\mathbb{F}_p) + \underbrace{2g - 2}_{\deg \omega}
\end{aligned}$$

□

Remark. We did not really compute an upper bound on $\#X(\mathbb{Q})$, but rather $\#X(\mathbb{Q}_p)_1$, which is strictly larger.

Lemma 2.1 (Coleman). *Let $f(t) = \sum \frac{a_i}{i+1} \in \mathbb{Q}_p[i+1]$ such that $f'(t) = \sum a_i t^i \in \mathcal{Z}_p[i+1]$. Let $m = \operatorname{ord}_{t=0}(f'(t) \mod p)$.[2] Suppose that $m < p - 2$.[3] Then f has at most $m + 1$ zeros in $p\mathcal{Z}_p$.*



Proof. Newton polygons.

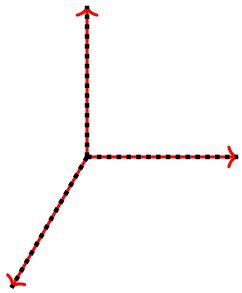
Note that $v(a_m) = 0$. Because of the bound on p. Then $v(m+1) = 0$. Then $v(a_i) > 0$ for $i < m$ and $v(i+1) = 0$ for $i < m$. But

$$v\left(\frac{a_i}{i+1}\right) \geq v_p(i+1) > m+1-(i+1)$$

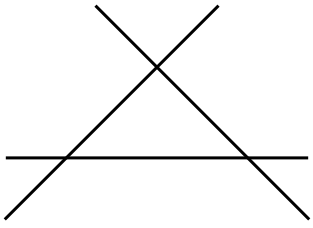
Segments of slope α correspond to roots with valuation $-\alpha$. The length of the segment corresponds to the number of roots. □

If $X/\mathbb{Q}_p$ is any variety, then Trep $X := \overline{v(X(\overline{\mathbb{Q}_p}))}$.

Example 2.3. $x + y = 1$, then



Example 2.4. $xyz = p(x^3 + y^3 + z^3)$



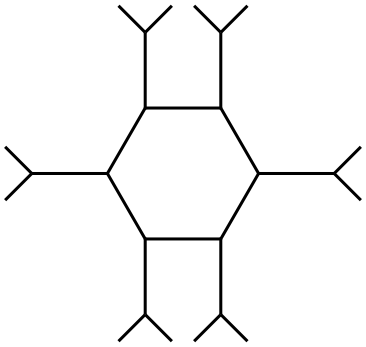
2.2.1 Stoll's Idea

Choose the 'best' ω for each $Q \in X(\mathbb{F}_p)$. Let $n_Q(\omega) = \deg(\operatorname{Div} w(J \otimes L))$, $n_Q = \min_{W \in V} n_Q(\omega)$.

$$\#X(\mathbb{Q}) \leq \sum_{Q \in X(\mathbb{F}_p)} (1 + n_Q) \leq \#X(\mathbb{F}_p) + \sum_{Q \in X(\mathbb{F}_p)} n_Q$$

[2] Note, $m = n_{\mathbb{Q}}$)

[3] By the previous footnote, $p > m + 2$ implies that $m \leq 2g - 2$ by Riemann-Roch.



Now define $D := \sum_{Q \in X(\mathbb{F}_p)} n_q[Q]$. We claim that $\deg D \leq 2r$. Now $\dim V \geq g - r$. Observe that D is special. If K_D is a canonical divisor, then D is special if $\dim H^0(X, K \setminus D) \geq 1$. Then there exists same canonical divisor $K^1 \geq 0$ such that $D \leq K^1$. Now $\dim H^0(X, \Omega^1(-D)) > 0$ containing ω if and only if $\operatorname{Div} \omega \geq D$.

Theorem 2.8 (Clifford)**.** *If D is special, then* $\dim H^0(X, D) \leq \dfrac{\deg D}{\alpha} + 1$.

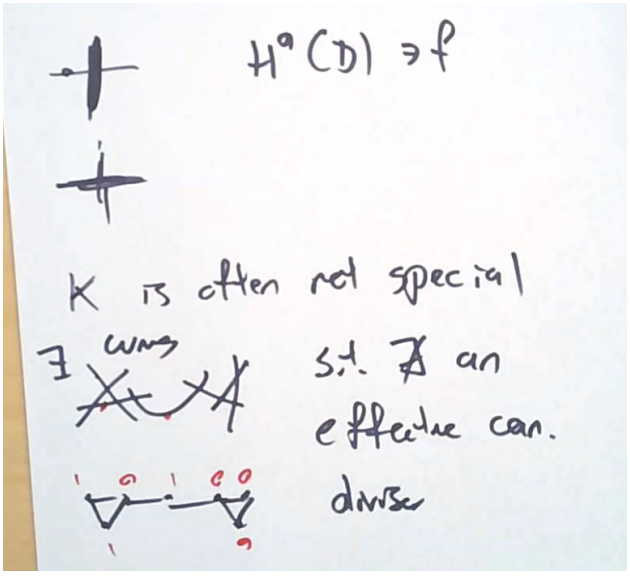
Context (Riemann-Roch). $h^0(D) - h^0(K - D) = \deg D + 1 - g$.

Proof. $D = \sum n_q[Q]$.

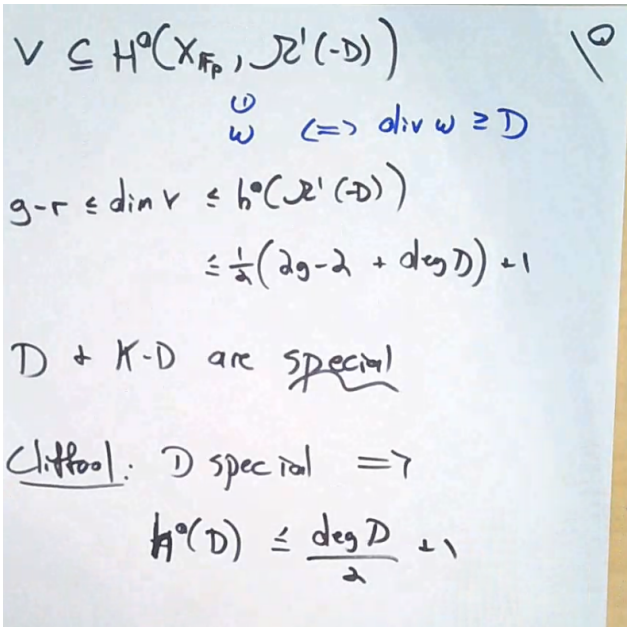
$$V \subseteq H^0(X_{\mathbb{F}_p}, \Omega^1(-D))$$

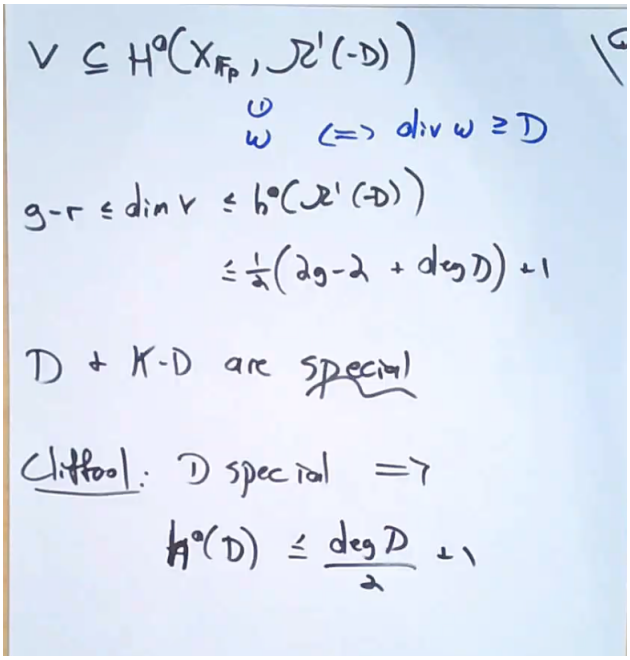
Then $g - r \leq \dim H^0(\Omega^1(-D)) \leq \frac{1}{2}(2g - 2 - \deg D) + 1$. But then $\deg D \leq 2r$. □

The notion of special is not good for singular curves. $H^0(D) \in P$. K is not often special, there exist curves such that there does not exist an effective canonical divisor.



2.3 Lecture 3



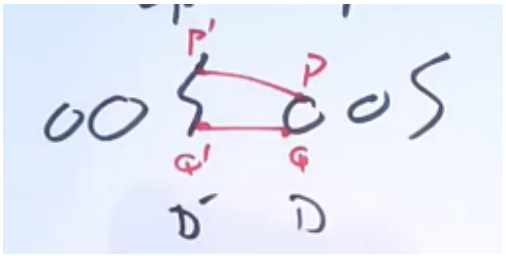


$|D| = \{E \geq 0 \colon E \cap D\} \simeq \mathbb{P}^r$.

$$
\begin{aligned}
r(D) &= -1 \quad \text{if } |D| = \emptyset \\
r(D) &= 0 \quad \text{if } |D| \neq \emptyset \\
r(D) &= 1 \quad \text{if } \forall P \in X, |D - P| \neq \emptyset \\
r(D) &\geq i \quad \text{if } \forall E \geq 0 \text{ of deg } E \leq i, |D - E| \neq \emptyset
\end{aligned}
$$

Then X sm, then $r(D) = \dim H^0(X, D) - 1$. If X is singular, then $r(D) \neq \dim H^0(D)$

The rank of D is semicontinuous, i.e. if $\mathfrak{X}/E_P$, then $\mathfrak{X}_{\mathbb{Q}_p} \to \mathfrak{X}_{\mathbb{F}_p}$ then $r(D) \geq r(D')$ [Hartshorne III.12].



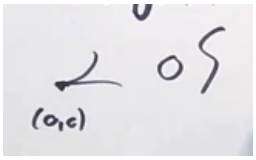
Remark. This inequality can be strict. If $P, Q \in X$ are not hyperelliptic, then reduces to $P', Q' = i(P), h^0(P+Q) = 1$ and $h^0(P' + i(P)) = 2$.

Definition (Regular)**.** Let X be a scheme. We say that X is regular if for all $P \in X$ corresponding to $\mathfrak{p}$, we have $\dim_{k(\mathfrak{p})} \mathfrak{p}/\mathfrak{p}^2 = \dim X$.

Example 2.5. $y^2 - x^3 - p / \mathcal{Z}_p$.

$$\begin{array}{c} \mathfrak{X} \\ \big\downarrow \text{not sm} \\ \operatorname{Spec} \mathcal{Z}_p \end{array}$$

$\mathfrak{X}$ is regular, $\mathfrak{m} = (x, y, p)$, $\mathfrak{m}/\mathfrak{m}^2 = \langle x, y, p \rangle = \langle x, y \rangle$ PGM



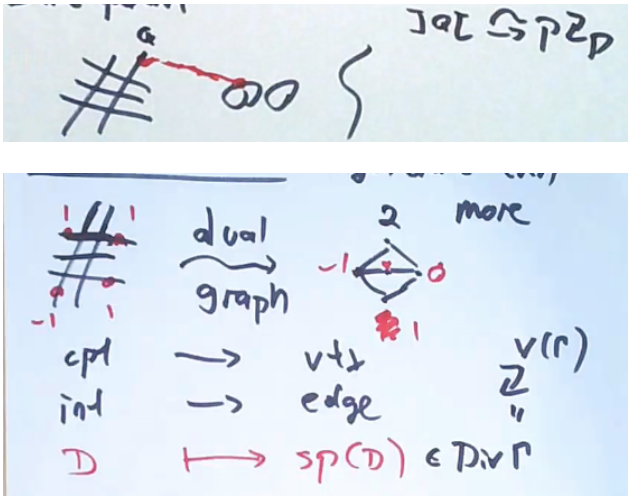
If $\mathfrak{X}/\mathcal{Z}_p$ is a regular proper model of a sm curve

$$\operatorname{im}(\mathfrak{X}(\mathbb{Q}_p) \xrightarrow{\text{red}} \mathfrak{X}(\mathbb{F}_p)) \subseteq \mathfrak{X}^{\text{sm}}(\mathbb{F}_p)$$

Example 2.6. $y^2 - x^3 - p$, $[0,0] = \emptyset$, $y^2 - x^3 - p^2$, $[0,0]$? lop
Lorenzini-Tucker, Mc Poonen
regular, etc, $\mathfrak{X}$ r.p. model

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

The idea is the same proof:



2.3.1 Matt Baker's Idea: Degenerate Even More

Baker, Baker-Norine

Notion of linear system, equivalence of divisors, and notion of rank, i.e. $|D|, r(D)$, $r(D) \leq r(\mathrm{sp}(D))$

$$K_P = \sum (\deg v - 2)[v]$$

Notion of special RR and Clifford

For Riemann-Roch, we have $r(D) - r(K_P - D) = \deg D + 1 - g$. Clifford gives if D is special, then $r(D) \leq \frac{\deg D}{2}$.

Theorem 2.9 (Katz,ZB). *Suppose $\mathfrak{X}$ is a regular proper model and $\mathfrak{X}_{\mathbb{F}_p}$ is totally degenerated. Then $\mathrm{sp}(D_{ch})$ is special*

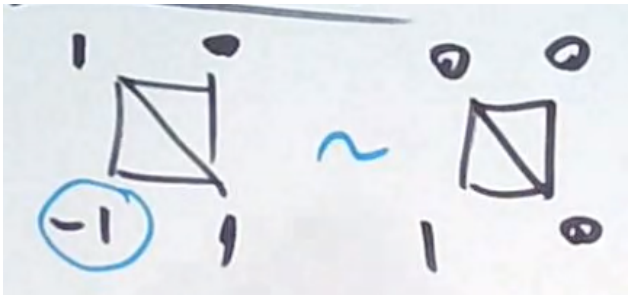
$$D_{ch} = \sum n_{\mathbb{Q}}[\mathbb{Q}]$$

Actually, $r(K_P - D) \geq g - r - 1$.

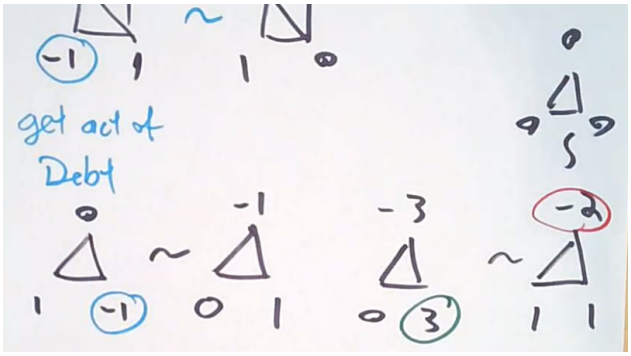
Proof. (of rank favorability) $g - r - 1 \leq r(K_r - \mathrm{sp}(D)) \leq \frac{\deg(K_r - \deg D)}{2} = \frac{1}{2}(2g - 2 + \deg D)$. □

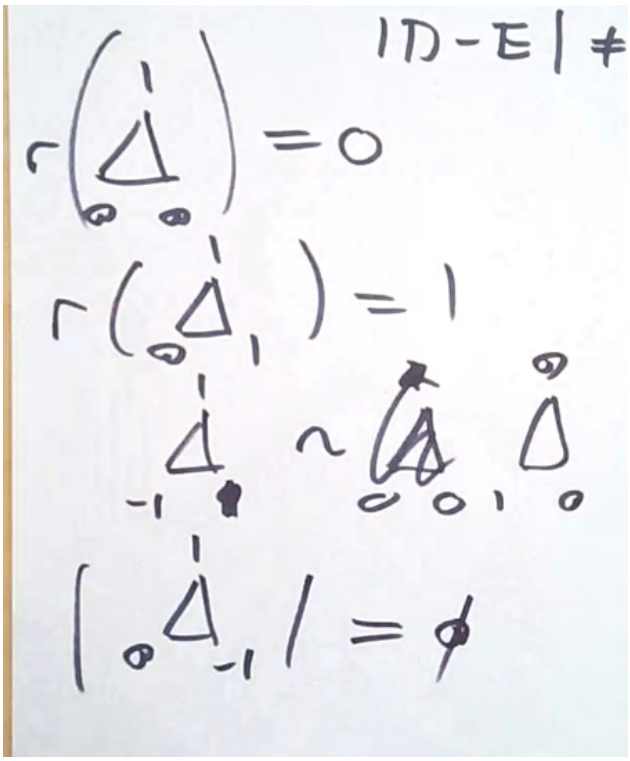
2.3.2 Chip Firing

Goal: Get (everybody) out of debt.



We say that $D \sim D^1$ if they differ by some sequence of loans and borrows. component group of special fiber of $\mathrm{Pic}^0 \Gamma \subseteq \mathrm{Pic}\,\Gamma = \mathrm{Div}\,\Gamma / \sim$.





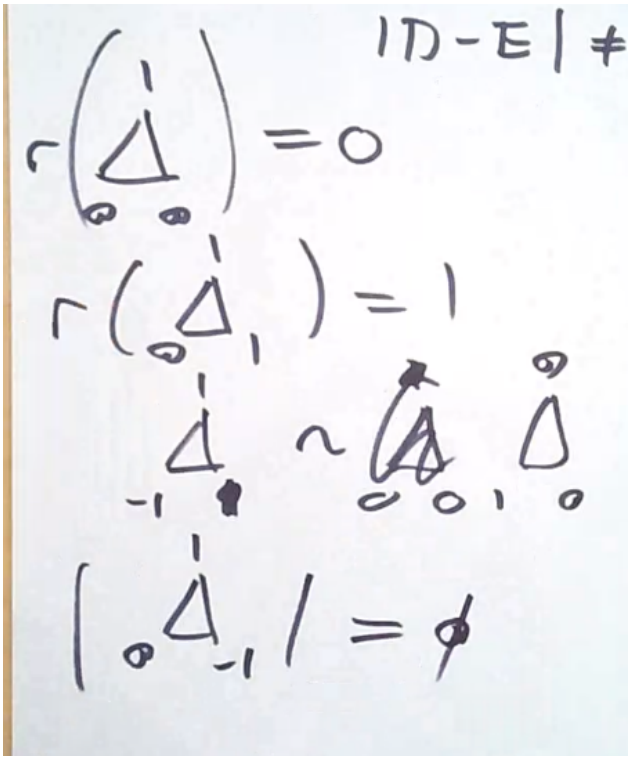
$|D| = \{D' \geq 0 \colon D' \sim D\}$. $r(D) \geq i$ if for all $E \geq 0$ with $\deg E \leq i$, $|D - E| \neq \emptyset$.
$\mathfrak{X}/\mathcal{Z}_p$, $\mathfrak{X}_{\mathbb{F}_p} = \cup C_i$, $\operatorname{Pic}\mathfrak{X} \xrightarrow{\text{sp}} \operatorname{Div}\Gamma'$ given by $L \mapsto \operatorname{sp}(L) := \sum(\deg L\big|_{C_i})[v_i]$.

Example 2.7. $L = \mathcal{O}(C_i)$

$$\deg \mathcal{O}(C_i)\big|_{C_j} = \begin{cases} \#\text{ int points of } C_i \cap C_j \\ \#\text{ self int of } C_i \end{cases}$$

$\mathfrak{X}_{\mathbb{F}_p} = (P)$ then $C_i \sim -\sum_{j \neq i} C_j$
$\operatorname{sp}(\mathcal{O}(C_i))$ if and only if firing at vertex i.

Example 2.8. $L = \omega_Z$.

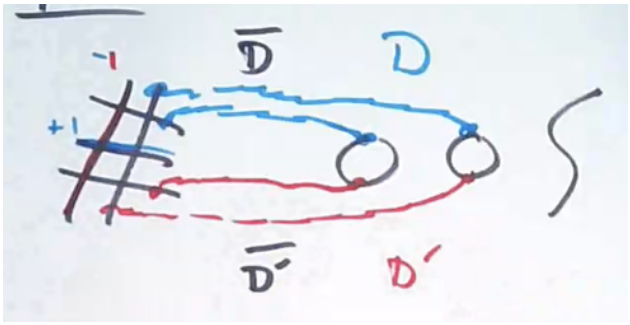


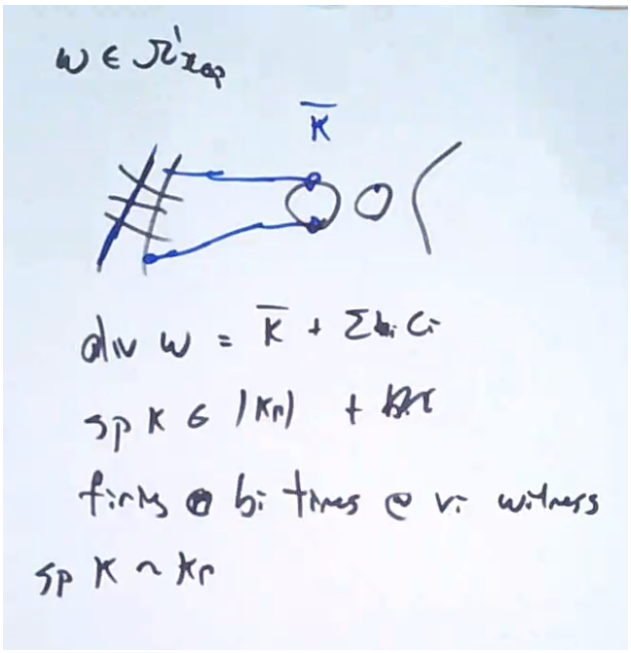
Adjunction: $(\omega_{\mathfrak{X}} \otimes \mathcal{O}(C_i))\big|_{C_i} \simeq \Omega^1_{C_i}$

$$\begin{aligned}\deg \omega_{\mathfrak{X}}\big|_{C_i} &= \deg \Omega^1_{\mathbb{P}^1} - \deg \mathcal{O}(C_i)\big|_C \\ &= -2 + \#\text{ int points of } C_i \text{ with rest } \mathfrak{X} \\ &= K_p\end{aligned}$$

As an upshot,

$D \sim D'$ on $\mathfrak{X}_{\text{sp}}$, $\operatorname{Div} f = D - D'$, $f : \mathfrak{X}_{\text{sp}} \to \mathbb{P}^1$, extend f to $\mathfrak{X} \leftrightarrow F$. Then $\operatorname{Div} F = \overline{D} - \overline{D}' + \sum \alpha_i C_i$. The equivalence $\text{sp}(\overline{D})$ with $\text{sp}(\overline{D}')$ is witnessed by lending at $C_i(v_i)$ α_i many times.





2.4 Lecture 4

Problem: $\mathfrak{X}^{\mathrm{sm}}(\mathbb{F}_p)$ is unbounded. $xyz = p(x^3 + y^3 + z^3)$.
Stoll

- Work of non-regular model
- cont. chains of $\mathbb{P}^1$'s
- then $\mathfrak{X}(\mathbb{F}_p)$ is bounded via p and g

Problem: Setup and local analysis is hard.
Main Tool: (KRZB)
Systematic use of Berkovich and tropical geometry
Setup, 2 types of $\int$'s

$$\int_{\text{abelian}} + \int_{\text{Berk.-Coleman}}$$

The abelian integral comes from Lie J and ????. The Berk.-Coleman integral is more computable and not equal to $\int_{\mathrm{Ab}}$. The difference between the two is linear in ω. The difference factors through

RECALL

$p > 2g+2$
$r < g$

L-T, McP $\#X(\mathbb{Q}) \leq \#\mathcal{X}^{sm}(\mathbb{F}_p) + 2g - 2$

Stoll: Sps X hyperelliptic & $r \leq g-3$.
Then $\#X(\mathbb{Q}) \leq 3(r+4)(g-1) + \max\{1, 4r\} \cdot g$

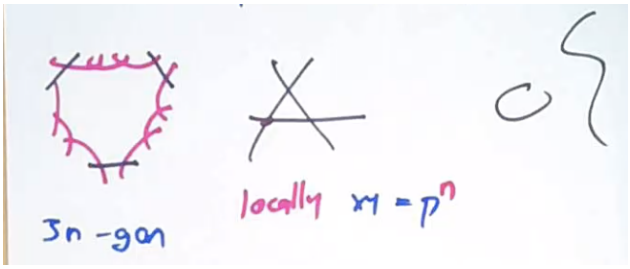
Katz-Rabinoff-Zb Sps $r \leq g-3$.
then $\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28$

RECALL

X regular if $\forall p \in X$,

$$\dim_{\kappa(p)} \mathfrak{p}/\mathfrak{p}^2 = \dim_p X$$

Regular $\Rightarrow$ $\mathrm{im}\left(\mathcal{X}(\mathbb{Q}_p) \to \mathcal{X}(\mathbb{F}_p)\right) \leq \mathcal{X}^{sm}(\mathbb{F}_p) = {}_{HL}$



Trop T, where T is

$$T \subseteq$$

$$A \qquad \subseteq \tilde{J} \longrightarrow J^?$$

$$\downarrow$$

A good red

3 Minhyong Kim

3.1 Lectures 1–4

Minhyong Kim's lectures were from his lecture note slides, please see those sections in Part II.

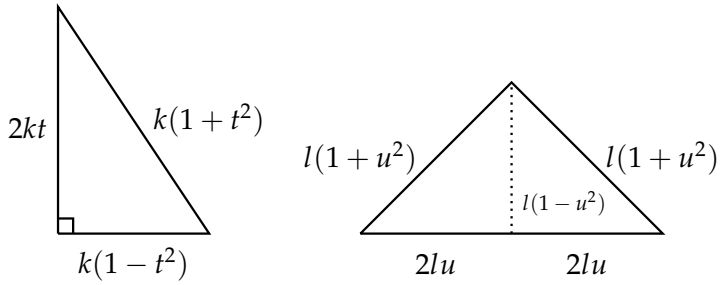
4 Jennifer Balakrishnan: Computational tools for quadratic Chabauty

4.1 Lecture 1

4.1.1 An Example

Question 1. Does there exist a pair of rational right triangles and a rational isosceles triangle that have the same area and the same perimeter?

If the answer to the question was a yes, we could draw triangles of the following form:



We rescale so that we can assume $l = 1$. Now suppose $k, t, u \in \mathbb{Q}$, $0 < t, u < 1$, and $k > 0$. Equating areas and perimeters, we find the simultaneous system of equations

$$\begin{cases} k^2 t(1-t^2) = 2u(1-u^2) \\ k + kt = 1 + 2u + u^2 \end{cases}$$

After some algebra, we see there exists $x \in \mathbb{Q}$, $1 < x < 2$, such that $2xk^2 + (-3x^2 - 2x^2 + 6x - 4)k + x^5 = 0$. The discriminant of this polynomial in k is a rational square. But then for some y, we have

$$y^2 = (-3x^2 - 2x^2 + 6x - 4)^2 - 4(2x)x^5 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16$$

We can then define a curve X by

$$X: \quad y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16$$

Now X is a genus 2 curve, and we would like to determine $X(\mathbb{Q})$. The Jacobian, J, of X has rank rank $J(\mathbb{Q}) = 1$. Also, the Chabauty-Coleman bound gives $\#X(\mathbb{Q}) \leq 10$. However, we have yet to actually find any rational points! In fact, we can find

$$\{\infty^{\pm}, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3)\} \subseteq X(\mathbb{Q})$$

Therefore, we have completely determined $X(\mathbb{Q})$, and the rational point $(12/11, 868/11^3)$ gives us a unique pair of triangles. It was Hirakawa and Matsumura in 2018 that answered this discriminant question, and hence the triangle question, that yes, there are exactly one pair of such triangles.

Theorem 4.1 (Hirakawa-Matsumura, 2018)**.** *Up to similitude, there exists a unique pair of rational right triangles and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with side* $(377, 135, 352)$*. and isosceles triangle with sides* $(366, 366, 132)$*.*

4.1.2 Coleman's Effective Chabauty

Let $X/\mathbb{Q}$ be a 'nice' curve with genus $g \geq 2$. Suppose that $r = \operatorname{rank} J(\mathbb{Q}) < g$. If $p > 2g$ is good reduction for X, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2$. This bound comes from bounding the number of zeros of a p-adic (Coleman) integral. Coleman gave this theory of p-adic line integration in the 1980s. In particular, he proved

Theorem 4.2 (Coleman)**.** *Let $X/\mathbb{Q}_p$ be a nice curve with good reduction at p. The p-adic integral $\int_P^Q \omega \in \overline{\mathbb{Q}}_p$, defined for $P, Q \in X(\overline{\mathbb{Q}}_p)$ and regular differential $\omega \in H^0(X, \Omega^1)$, satisfies the following:*

(i) the integral is $\overline{\mathbb{Q}}_p$-linear in ω.

(ii) if P, Q reduce to the same point $\overline{P} \in X(\overline{\mathbb{F}}_p)$, then we call the integral a 'tiny' integral. It can be evaluated by writing $\omega = \omega(t)\, dt$, with t is a uniformizer at $\overline{P}$ and ω a power series, then integrating formally and obtaining a power series ℓ such that $d\ell(t) = \omega(t)\, dt$, and finally evaluating $\ell(t(Q))$, which converges. This implies $\int_P^P \omega = 0$.

(iii) We have

$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega$$

Then it makes sense to define $\int_D \omega$ for

$$D = \sum_{j=1}^{n} \big((Q_j) - (P_j) \big) \in \operatorname{Div}_X^0(\overline{\mathbb{Q}}_p)$$

as

$$\int_D \omega = \sum_{j=1}^{n} \int_{Q_j}^{P_j} \omega.$$

(iv) if D is principal, then $\int_D \omega = 0$.

(v) The integral is compatible with the action of $\operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

(vi) Fix $P_0 \in X(\overline{\mathbb{Q}}_p)$. If $0 \neq \omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$, then the set of points $P \in X(\overline{\mathbb{Q}}_p)$ reducing to a fixed point on $X(\mathbb{F}_p)$ such that $\int_{P_0}^{P_1} \omega = 0$ is finite.

The integral above is known as the Coleman integral. Now given the hypotheses of the previous theorem, let $b \in X(\mathbb{Q}_p)$, and J be the Jacobian of X with Abel-Jacobi imbedding $i : X \hookrightarrow J$ given by $P \mapsto [P - b]$. There is a map $J(\mathbb{Q}_p) \times H^0(X_{\mathbb{Q}_p}, \Omega^1) \to \mathbb{Q}_p$ given by $(Q, \omega) \mapsto \langle Q, \omega \rangle$ that is additive in Q, $\mathbb{Q}_p$-linear in ω, and given by

$$\langle [D], \omega \rangle = \int_D \omega \text{ for } D \in \operatorname{Div}_X^0 .$$

But then for $P \in X(\mathbb{Q}_p)$, we have the Abel-Jacobi morphism AJ_b that takes P to the linear functional

$$\langle i(P), \omega \rangle = \int_b^P \omega =: \mathrm{AJ}_b(P).$$

The Chabauty-Coleman method uses a certain subspace of the space of regular 1-forms. We will assume that $b \in X(\mathbb{Q})$, and use this to embed $X \hookrightarrow J$.

Definition (Annihilating Differentials)**.** Let $A = \{\omega \in H^0(X, \Omega^1) \colon \text{ for all } P \in J(\mathbb{Q}), \langle P, \omega \rangle = 0\}$ is the subspace of annihilating differentials.

The embedding $i : X \hookrightarrow J$ induces an isomorphism of vector spaces $H^0(J_{\mathbb{Q}_p}, \Omega^1) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)$. Similarly, we have a pairing $J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) \longrightarrow \mathbb{Q}_p$ given by $(Q, \omega_J) \mapsto \int_0^Q \omega_J$. This induces a homomorphism $\log : J(\mathbb{Q}_p) \to H^0(J_{\mathbb{Q}_p}, \Omega^1)^*$. Thus, we have the following diagram

$$\begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & & \\ \downarrow & & \downarrow & \overset{\mathrm{AJ}_b}{\searrow} & \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & H^0(J_{\mathbb{Q}_p}, \Omega^1)^* \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \end{array}$$

By "computing rational points via the Chabauty-Coleman method", we mean that we compute the finite set of p-adic points

$$X(\mathbb{Q}_p)_1 := \{z \in X(\mathbb{Q}_p) \colon \int_b^z \omega = 0 \text{ for all } \omega \in A\}.$$

By construction, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$. Of course, it might be that $X(\mathbb{Q}_p)_1$ is strictly larger than a known set of rational points in $X(\mathbb{Q})$, so that extra work needs to be done in order to provably compute $X(\mathbb{Q})$ entirely. One approach to this problem is the Mordell-Weil sieve. But how do we compute the annihilating differential?

Example 4.1. Let $X : y^2 = x^5 - 2x^3 + x + \frac{1}{4}$, which has LMFBD label 971.a.971.1. Here are some facts about X:

(i) $X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$.

(ii) J is simple, $J(\mathbb{Q}) \simeq \mathcal{Z}$, and the point $[(-1, -1/2) - (0, 1/2)] \in J(\mathbb{Q})$ has infinite order (this can be seen by computing the Coleman integrals on regular 1-forms).

(iii) The conductor N is 971, which is prime. Therefore, X has good reduction at $p = 3$, and we can compute $\#X(\mathbb{F}_3) = 7$. Using Stoll's refinement of the Chabauty-Coleman bound for $p = 3$, we find

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_3) + 2r + \left\lfloor \frac{2 \cdot 1}{3 - 2} \right\rfloor = 11$$

This bound is then now sharp enough to prove that we have all the $\mathbb{Q}$-points. [In fact, we do not even know that we have all the $\mathbb{Q}$-points, though we suspect this is the case, and it is. We would like to prove this.]

We will use $p = 3$ to construct a 3-adic annihilating differential η. A basis of $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ is

$$\left\{\omega_i = \frac{x^i \, dx}{2y}\right\}_{i=0,1}.$$

So η is a $\mathbb{Q}_3$-linear combination of ω_0, ω_1. We will compute the values of

$$\alpha := \int_{(0,1/2)}^{(-1,-1/2)} \omega_0$$

and

$$\beta := \int_{(0,1/2)}^{(-1,-1/2)} \omega_1$$

to compute η. SageMath can compute α, β

$$\alpha = 3 + 3^2 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{10} + O(3^{11})$$
$$\beta = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 3^4 + 3^6 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10}).$$

Taking a slightly different basis (see the notes), we can take $\eta = \beta\omega_0 - \alpha\omega_1$ as our annihilating differential and run Chabauty-Coleman.[4]

4.1.3 Explicit Coleman Integration

But where do all these numbers come from? They come from using the action of Frobenius on p-adic cohomology. Let X^{an} denote the rigid analytic space over $\mathbb{Q}_p$ associated to $X/\mathbb{Q}_p$.

Definition (Wide Open Subspace)**.** A wide open subspace of X^{an} is the complement in X^{an} of the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$.

Before continuing, we will give a few more properties of the Coleman integral that we will need.

Theorem 4.3 (Coleman)**.** *Let η, ξ be 1-forms on a wide open subspace V of X^{an}, and let $P, Q, R \in V(\overline{\mathbb{Q}_p})$. Let $a, b \in \overline{\mathbb{Q}_p}$. Then we have*

(i) Linearity in the integrand:

$$\int_P^Q (a\eta + b\xi) = a\int_P^Q \eta + b\int_P^Q \xi$$

(ii) Additivity in the endpoints:

$$\int_P^R \eta + \int_R^Q \eta = \int_P^Q \eta$$

(iii) Change of variables under rigid analytic maps (Frobenius): if $V' \subset X'$ is a wide open subspace of the rigid analytic space X', ω', a 1-form on V' and $\phi : V \to V'$ a rigid analytic map, then

$$\int_P^Q \phi^*\omega' = \int_{\phi(P)}^{\phi(Q)} \omega'.$$

(iv) Fundamental Theorem of Calculus:

$$\int_P^Q df = f(P) - f(Q)$$

for a rigid analytic function on V.

[4] Note, use Sage for hyperelliptic curves and Magma for plane curves.

(v) Galois compatibility: if $P, Q \in V(\mathbb{Q}_p)$ and ω is defined over $\mathbb{Q}_p$, then $\int_P^Q \omega \in \mathbb{Q}_p$.

We first integrate $\int_P^Q \omega$ for ω a 1-form of the second kind, where $P, Q \in V(\mathbb{Q}_p)$. We will discuss this in the case where X is a hyperelliptic curve by examining the method of explicit Coleman integration due to Balakrishnan-Bradshaw-Kedlaya. The method is the following:

1. Take a lift, ϕ, of p-power Frobenius from the special fiber.
2. Compute a basis, $\{\omega_i\}$, of 1-forms of the second kind.
3. Compute $\phi^*\omega_i$ via Kedlaya's zeta function algorithm, and use properties of Coleman integrals to relate $\int_P^Q \phi^*\omega_i$ to $\int_P^Q \omega_i$ and other terms.
4. Solve for $\int_P^Q \omega_i$ using linear algebra.

We sketch Kedlaya's algorithm. Let X be the curve $y^2 = p(x)$. We work in an affine $Y \subset X$ given by defining Weierstrass points. Take ϕ to be $x \mapsto x^p$ and $y \mapsto y^p \sum_{j=0}^{\infty} \binom{1/2}{1} \left(\frac{p(x^p - p(x)^p}{y^{2p}}\right)^j$. Then we compute the action of ϕ on

$$\begin{aligned}\phi^*\left(\frac{x^i\,dx}{y}\right) &= \frac{x^{pi}\,d(x^p)}{\phi(y)} \\ &= \frac{x^{pi}px^{p-1}\,dx}{\phi(y)} \\ &= px^{pi+p-1}y^{-p}\sum_{j=0}^{\infty}\binom{1/2}{1}\left(\frac{p(x^p-p(x)^p}{y^{2p}}\right)^j\end{aligned}$$

and reduce pole order of each resulting differential using relations in H^1. Denote the basis by $\{\omega_i\}_{i=0,\ldots,2g-1}$. Then Kedlaya's algorithm gives

$$\phi^*\omega_i = dh_i + \sum_{j=0}^{2g-1} \mu_{ji}\omega_j$$

If we can compute h_i and M, then

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i \\ \vdots \end{pmatrix} = (M^t - I)^{-1} \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i \\ \vdots \end{pmatrix} \qquad (*)$$

Finishing the 3-adic integrals on $y^2 = x^5 - 2x^3 + x + 1/4$, we constructed $\eta = \beta\omega_0 - \alpha\omega_1$, where α, β are computed using (*). We want to compute $X(\mathbb{Q}_3)_1$. Note that $X(\mathbb{F}_3) = \{\infty, (0, \pm 1), (1, \pm 1), (2 \pm 1)\}$. We need to compute power series expansions of

$$\left\{\int_{(0,1/2)}^{P_t} \eta\right\}$$

where P_t ranges over all residue disks, and then solve for $z \in X(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^{z} \eta = 0$. To compute these integrals, we can take P_0 to be a lift of some $\mathbb{F}_3$-point in the same residue disk as P_t. Then

$$\int_{(0,1/2)}^{P_t} \eta = \underbrace{\int_{(0,1/2)}^{P_0} \eta}_{\text{Gives 3-adic}} + \underbrace{\int_{P_0}^{P_t} \eta}_{\text{Coleman 3-adic series}}$$

Note the first integral on the right side is some 3-adic constant, and the second is a tiny integral which was computed using a local coordinate at P_0. As a lucky fact, for each residue disk, there exists a rational point $P_0 \in X(\mathbb{Q})$ such that the 3-adic number is 0. This forces the constant of integration to be 0 in each residue disk by the construction of the annihilating differential. Then any further computation is solely local. Computing the tiny integral in each residue disk, we find each just has a simple zero at a known rational point, and no others. But then we have

$$X(\mathbb{Q}_3)_1 = X(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/20\}$$

which proves that $\#X(\mathbb{Q}) = 7$.

4.2 Lecture 2

Last time we gave an algorithm to compute Coleman integrals between points in different residue disks on hyperelliptic curves, i.e. the curves "analytic continuation along Frobenius." To do this, we wrote down an action of Frobenius ω on differentials ω_i, reduced to pole orders, and obtained $\phi^* w_i = dh_i + \sum M_{ji}\omega_j$, then wrote a system to produce

$$\left\{ \begin{pmatrix} \vdots \\ \int_Q^P \omega_i \\ \vdots \end{pmatrix} \right\}_{i=0,\ldots,2g-1}$$

How do we do this for more general curves? We use Tuitman's algorithm, showing how it can be used to compute Coleman integrals for place curves. Let $X/\mathbb{Q}$ be a 'nice' curve of genus g with a plane model $Q(x,y) = y^{d_x} + Q_{d_x-1}y^{d_x-1} + \cdots + Q_0 = 0$ such that $Q(x,y)$ is irreducible, $Q_i(x) \in \mathcal{Z}[x]$. Let p be a good prime for X.

1. Consider the map $x : X \to \mathbb{P}^1$ and remove the ramification locus $r(x)$, analogous to removing Weierstrass points in Kedlaya's algorithm.

2. Choose a lift of Frobenius with $x \mapsto x^p$. Compute the image of y through Hensel lifting.

3. Compute a basis of $H^1_{\mathrm{dR}}(X)$ using an integral basis of $\mathbb{Q}(X)$ over $\mathbb{Q}[X]$, $\mathbb{Q}[\frac{1}{x}]$.

4. Compute the action of Frobenius on differentials and reduce pole orders using relations in cohomology via Louder's fibration algorithm—Tuitman uses an integral basis of $\mathbb{Q}(X)$.

Then $\phi^*\omega_i = dh_i + \sum M_{ji}\omega_j$. Use this to give a lih system to produce values

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i \\ \vdots \end{pmatrix}$$

Example 4.2 (B-Tuitman)**.** Can compute Coleman integrals on a non-hyperelliptic genus 55 curve to show its Jacobian has rank ≥ 1.

Let $X/\mathbb{Q}$ be a 'nice' curve of genus g. By work of Coleman (1982) and Coleman-deShali (1988), we have a theory of iterated p-adic integrals on X. What are these? There are iterated path integrals:

$$\int_P^Q \eta_n \cdots \eta_1 := \int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \ \cdots \ dt_1$$

We will often suppress writing the iterated integral and instead write a single integral. In our computations, we will focus on the case $n = 2$ (double Coleman integrals):

$$\int_P^Q \eta_2\eta_1 := \int_P^Q \eta_2 \int_P^R \eta_1$$

These integrals play an important role in nonabelian Chabauty.

How do we compute these integrals? We want to apply an algorithm for computing the action of Frobenius on p-adic cohomology, e.g. Kedlaya or Tuitman, to produce

$$\phi^* \omega_i = dh_i + \sum M_{ji} \omega_j$$

Observe that the algorithm of $M^{\otimes n}$ are not 1, and reduce the computation of n-fold iterated integrals to $(n-1)$-fold iterated integrals.

Here are some useful properties of iterated Coleman integrals:

Proposition 4.1. *Let $\omega_{i_1}, \dots, \omega_{i_n}$ be forms of the second kind, holomorphic at $P, Q \in X(\mathbb{Q}_p)$. Then*

(i) $\int_P^Q \omega_{i_1} \cdots \omega_{i_n} = 0$

(ii)

$$\sum_{all\ perm} \int_P^Q \omega_{\sigma(t_1)} \cdots \omega_{\sigma(t_n)} = \prod_{j=1}^n \int_P^Q \omega_j$$

(iii) $\int_P^Q \omega_{i_1} \cdots \omega_{i_n} = (-1)^n \int_Q^P \omega_{i_n} \cdots \omega_{i_1}$

(iv) If $P, P', Q \in X(\mathbb{Q}_p)$, then

$$\int_P^Q \omega_{i_1} \cdots \omega_{i_n} = \sum_{j=0}^n \int_P^Q \omega_i \cdots \omega_j \int_P^{P'} \omega_{i_{j+1}} \cdots \omega_{i_n}$$

This let's us break up a path.

So this gives the analogue of additivity in endpoints for double integrals (have $P, P', Q \in X(\mathbb{Q}_p)$).

$$\int_P^Q \omega_i \omega_k = \int_P^{P'} \omega_i \omega_k + \int_{P'}^Q \omega_i \omega_k + \int_{Q'}^Q \omega_i \omega_k + \int_P^{P'} \omega_k \int_{P'}^Q \omega_i + \int_{P'}^{Q'} \omega_k + \int_{Q'}^Q \omega_i$$

Let $P' = \phi(P)$, $Q' = \phi(Q)$, here is how we compute double Coleman integrals.

$$\begin{aligned} \int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k &= \int_P^Q \phi^*(\omega_i) \phi^*(\omega_k) \\ &= \int_P^Q (df_1 + \sum M_{ji} \omega_j X\ df_k \sum M_{jk} \omega_j) \\ &= c_{ik} + \int_P^Q \sum M_{ji} \omega_j \sum M_{jk} \omega_j \end{aligned}$$

This gives us

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i \omega_k \\ \vdots \end{pmatrix} = (I - M^{t \otimes ?})^{-1} \left(c_{ik} - \int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k - \int_P^Q \omega_i \int_{\phi(P)}^P \omega_i - \int_Q^{\phi(Q)} \omega_i - \int_{\phi(P)}^{\phi(Q)} \omega_k + \int_{\phi(Q)}^Q \omega_i \omega_k \right)$$

As an application (preview), let $E/\mathcal{Z}$ be the minimal regular model of an elliptic curve. Let $X = \mathcal{E} \setminus \mathcal{O}$. Let $\omega_0 = \dfrac{dx}{2y + a_1 x + a_3}$, $\omega_1 = x\omega_0$. Let v be a tangential base point of $\mathcal{O}$ at an integral 2-torsion point. Let p be a prime of good reduction. Suppose that $\mathcal{E}$ has analytic rank 1 and Tamagawa product 1. Let $\log(z) = \int_b^t \omega_0$, $D_2(z) = \int_b^t \omega_0 \omega_1$.

Theorem 4.4 (Kim,B-Kedlaya-Kim)**.** *Suppose P is a point of infinite order in $\mathcal{E}(\mathcal{Z})$. Then $X(\mathbb{Q}) \subseteq \mathcal{E}(\mathcal{Z})$ is in the zero set of*

$$f(z) = (\log P)^2 D_2(z) - (\log z)^2 D_2(P)$$

Kim shows that this D_2 is related to p-adic heights on Z.

4.2.1 p-adic heights on Jacobians of curves

p-adic heights are a natural source of bilinear forms on global points. They allow us to generate some of our linear techniques from Chabauty-Coleman.

Remark. Some p-adic heights are in p-adic BSD/p-adic Gross-Zagier.

Let $X/\mathbb{Q}$ be a 'nice' curve of genus $g > 1$. Let p be a good prime. Fix a branch of $\log_p : \mathbb{Q}_p^\times \to \mathbb{Q}_p$. Also fix an idelic class character $\chi : A_{\mathbb{Q}}^*/\mathbb{Q}^* \to \mathbb{Q}_p$. A splitting of the Hodge filtration on $H^1_{\mathrm{dR}}(X/\mathbb{Q}_p)$ such that the basis is isotropic with respect to the cup product. Fixing a splitting of the Hodge filtration corresponds to fixing a subspace $W = \ker s$ of $H^1_{\mathrm{dR}}(X)$ corresponding to the space $H^0(X, \Omega^1)$, i.e. $H^1_{\mathrm{dR}}(X, \mathbb{Q}_p) \simeq H^0(X, \Omega^1) \oplus W$

Definition (Coleman-Gross, 1989)**.** The cyclotomic p-adic height pairing is a symmetric bi-additive pairing

$$\mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \to \mathbb{Q}_p$$

given by $(D_1, D_2) \mapsto h(D_1, D_2)$ for $D_1, D_2 \in \mathrm{Div}^0(X)$ with divergent support such that

(i) $k(D_1, D_2) = \sum_{\text{height}} h_v(D_1, D_2) = h_P(D_1, D_2) + \sum_{\text{supp}} h_i(D_1, D_2)$. $\int_{D_2} \omega_{D_1} + \sum m_l \log_P(l)$, where $m_l \in \mathbb{Q}$ is an intersection multiplicity.

(ii) For $\beta \in \mathbb{Q}(X)^*$, we have $h(D, \mathrm{Div}(\beta)) = 0$, so this gives a symmetric, bilinear pairing $\sigma(\mathbb{Q}) \times J(Q) \to \mathbb{Q}_p$.

4.2.2 Local height at P

We need to construct a normalized differential ω_D with respect to choice of ω. Let $T(\mathbb{Q}_p)$ be the differential of the third kind: simple poles and integer residues. We have a residue divisor homomorphism

$$\mathrm{Res} : T(\mathbb{Q}_p) \to \mathrm{Div}^0(X)$$

given by $\omega \mapsto \mathrm{Res}(\omega) = \sum_P (\mathrm{Res}_P \omega) P$. This induces

$$0 \longrightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1) \longrightarrow T(\mathbb{Q}_p) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(X) \longrightarrow 0$$

Want ω_0 will be a certain 3rd kind of differential with $\mathrm{Res}(\omega_{D_i}) = D_i$.

Example 4.3. Let X be a hyperelliptic curve $y^2 = f(x)$, and $D_1 = (P) - (Q)$, with P, Q nonsingular Weierstrass points. Then

$$\omega = \frac{dx}{2y}\left(\frac{y + y(P)}{x - x(P)} - \frac{y + y(Q)}{x - x(Q)}\right)$$

has $\mathrm{Res}\,\mathrm{Div}\, D_1$ a simple pole at P, Q residues $+1, -1$, respectively. However, adding any holomorphic η to ω and taking $\mathrm{Res}(\eta + \omega) = D_1$. So we must take care of this. Let $T_l(\mathbb{Q}_p)$ be the log differentials $\dfrac{df}{P}$, $f \in \mathbb{Q}_p(X)^*$. We have

$$0 \longrightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1) \longrightarrow T(\mathbb{Q}_p)/T_l(\mathbb{Q}_p) \longrightarrow J(\mathbb{Q}_p) \longrightarrow 0$$

Proposition 4.2. *There is a canonical homomorphism* $\Psi : T(\mathbb{Q}_p)/T_l(\mathbb{Q}_p) \to H^1_{dR}(X)$ *such that*

(i) Ψ *is the identity on holomorphic differentials.*

(ii) Ψ *sends third kind with* $\mathrm{Res}(v_0) = D$ *and* $\psi(\omega_0) \in W$.

Remark. If p is ordinary, we can take W to be the unit root subspace for Frobenius.

4.3 Lecture 3

$$\begin{aligned} h(D_1, D_2) &= \sum_v h_v(D_1, D_2) \\ &= \underbrace{\int_{D_2} \omega_{D_1}}_{=h_P(D_1,D_2)} + \sum_{v \neq P} h_v(D_1, D_2) \end{aligned}$$

We constructed ω_{D_1} (3rd kind differentials). How do we compute Coleman integrals of differentials of the 3rd kind: $\int_S^R \omega$, $\mathrm{Res}(\omega) = (P) - (Q)$.

1. Compute $\Psi(\omega) \in H^1_{\mathrm{dR}}(X)$ by computing cup products.

$$\Psi(\omega) = \sum \underbrace{b_i \omega_i}_{\text{solve for } b_i}$$

   for $\{\omega_i\}$ a basis of H^1_{dR}, by computing $\Psi(\omega) \smile [\omega_j]$.

2. Let $\alpha := \phi^* \omega - p\omega$. Use Frobenius equivariance to compute $\Psi(\alpha) = \phi^* \Psi(\omega) - p\Psi(\omega)$.

3. Let β be such that $\mathrm{Res}(\beta) = (R) - (S)$. Compute $\Psi(\beta)$.

4. Using Coleman reciprocity

$$\int_S^R \omega = \frac{1}{1-p} \left(\Psi(\alpha) \smile \Psi(\beta) + \sum_{A \in X(\overline{\mathbb{Q}_p})} \mathrm{Res}_A \left(\alpha \int \beta - \int_{\phi(S)}^{S} \omega - \int_R^{\phi(R)} \omega \right) \right)$$

This lets us compute $h_P(D_1, D_2)$ because $h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$. What about the self-pairing of a divisor? $h_P(D, D)$? It turns out that if we consider the case of $X/\mathbb{Q}$ a hyperelliptic curve of odd degree model

$$h_P(D, D) = -2 \sum_{i=0}^{g-1} \int_b^z \omega_i \overline{\omega}_i$$

where g is the genus, $\omega_i = \dfrac{x^i \, dx}{2y}$, $\overline{\omega}_i$ is the dual under U, and $D = (\alpha) - (\infty)$.

Can we use this to study integral points on hyperelliptic curves?

4.3.1 Quadratic Chabauty for Integral Points on Hyperelliptic Curves

This is work of B.-Besser-Müller. Let $f \in \mathcal{Z}[x]$ be monic, separable, and have degree $2g + 1 \geq 3$. Let $U = \mathrm{Spec}(\mathcal{Z}[x, y]/(y^2 - f(x))$. Let X be the normalization of projective closure of generic fiber of U. Let J be the Jacobian of X. Assume $\mathrm{rank}\, J(\mathbb{Q}) = g$. Suppose $\log : J(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ is an isomorphism. Let p be a good prime. Then there exists $\alpha_{ij} \in \mathbb{Q}_p$ such that

$$p(z) = -2 \sum_{i=0}^{g-1} \int_b^z \omega_i \overline{\omega}_i - \sum_{i,j<g} \alpha_{ij} \int_\infty^z \omega_i \int_\infty^z \omega_j,$$

where $\omega_i = \dfrac{x^i \, dx}{2y}$. This takes values in an explicitly computable finite set $S \subset \mathbb{Q}_p$ for all $z \in U(\mathcal{Z})$.

The idea is that the global height $h = h_p + \sum_{l \neq p} h_l$, then $h - h_p = \sum_{l \neq p} h_l$ on integral points, finitely many values, and we can compute these ahead of time. Now $h = \sum \alpha_{ij} \int \omega_i \int \omega_j$, allows us to solve for α_{ij}.

What goes wrong for rational points? We do not know how to control $\sum_{l \neq p} h_l$ on all rational points. Our goal is to extend QC from integral points to rational points. The problem is that we need to control local heights away from p. The solution is to use heights that factor through Kim's unipotent Kummer map. Can control local heights in this setting. For this, we need "non-abelian" height (instead of heights via the Jacobian). Use heights on Block-Kato Selmer groups.

Let $X/\mathbb{Q}$ be a 'nice' curve $g > 1$, and p a good prime. Let $V = H^1_{\mathrm{dR}}(X_{\mathbb{Q}})^*$. By Nakorar (1993), we have a bilinear symmetric pairing

$$h : H^1_f(G_{\mathbb{Q}}, V) \times H^1_f(G_{\mathbb{Q}}, V^*(1)) \to \mathbb{Q}_p$$

where $h = \sum_v h_v$. This is equivalent to the Coleman-Gross height via an étale Abel-Jacobi map (Besser). This height is also dependent on choices like the C-G height.

1. the choice of an idele class character

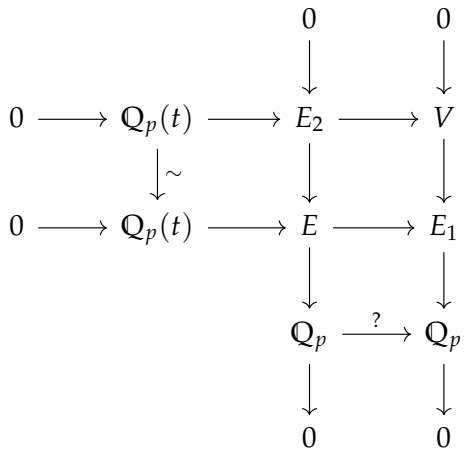
$$\chi : \mathbb{A}^*_{\mathbb{Q}}/\mathbb{Q}^\times \to \mathbb{Q}_p$$

2. a splitting s of the Hodge filtration on $V_{\mathrm{dR}} = D_{\mathrm{cris}}(V) = H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})^*$

Recall that in the Coleman-Gross height, to pair points on the Jacobian, we needed to a choice of divisors. Here ??? depends on ?? extensions: given a pair of extension classes $(c_1, c_2) \in H^1_f(G_{\mathbb{Q}}, V) \times H^1_f(G_{\mathbb{Q}}, V^*(1))$. Take representations E_1, E_2,

$$\begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ ?? & \longrightarrow & E_2 & \longrightarrow & V & \longrightarrow & 0 \\ & & & & \downarrow & & \\ & & & & E_1 & & \\ & & & & \downarrow & & \\ & & & & \mathbb{Q}_p & & \\ & & & & \downarrow & & \\ & & & & 0 & & \end{array}$$

Filling in the diagram.



E is a mixed extension ($G_{\mathbb{Q}}$-representations) of E_1, E_2 with graded pieces $\mathbb{Q}_p$, V, $\mathbb{Q}_p(1)$ with a weighted filtration $0 = w_3ESw_{-2}ESw_{-1}ESw_0E = 0$ such that $w_{-1}E \simeq E_2$, $w_0E/w_{-2}E = E_{-1}$.

Now let $M_{\mathbb{Q}}$ be the set of such extensions. If v is prime, then M_v is the set of mixed extensions of G_v-representations. $M_{\mathbb{Q},f}$ f subscript crystalline.

For $E \in M_{\mathbb{Q},f}$, define $h_v(E) = \overline{h_v(\text{loc}E)} = h_v(\overline{E_v})$ and then define $h(e_1, e_2) = \sum_v h_v(E)$. From this point forward, we will assume that $h_l(E_l) = 0$ for all $l \neq p$, eg.. when X has potential good reduction at l, local height $h_l = 0$.

Definition: A filtered ϕ-module (over $\mathbb{Q}_p$) is a finite dimensional $\mathbb{Q}_p$-vector space W, with an exhaustive and separated decreasing filtration Fil^1 and an automorphism ϕ:

- exhaustive $W = \cup_i \text{Fil}^i$
- separated $\cap_i \text{Fil}^i = 0$
- decreasing $\text{Fil}^{i+1} \subseteq \text{Fil}^i$

Example 4.4. (i) $\mathbb{Q}_p$ with $\text{Fil}^0 = \mathbb{Q}_p$, $\text{Fil}^n = 0$ for all $n > 0$, $\phi = \text{id}$.

(ii) By Falting's Comparison Theorem, we have $H^1_{\text{dR}}(X_{\mathbb{Q}_p}) = D_{\text{cris}}(H^1_{\text{dR}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ and $H^1_{\text{ét}}(X_{\overline{Q}}, \mathbb{Q}_p)$ is crystallline, take Frobenius ϕ on crystalline cohomology and Hodge filtration, then $H^1_{\text{dR}}(X_{\mathbb{Q}_p})$ has the strucutre of a filtered ϕ-module.

(iii) $V_{\text{dR}} = H^1_{\text{dR}}(X_{\mathbb{Q}_p})^* =$??? with dual filtration and action.

(iv) The direct sum $\mathbb{Q}_p \oplus V \oplus \mathbb{Q}_p(1)$ has the structure of a filtered ϕ-module as well. Let $E_p \in M_{p,f}$. Then $E_{\text{dR}} = D_{\text{cris}}(E_p)$ is a mixed extension filtered ϕ-modules with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$. To construct the local heights h_p of E_p, need an explicit description of

- Frobenius ϕ
- filtration on E_{dR}

Want to comute $h(E) = \sum h_v(E_v) = h_p(E_p) + /\sum_{l \neq p} h_v(E_R)$.
From Kim to Nakovar:
Want maps $X(\mathbb{Q}) \to M_{\mathbb{Q},f}$, $X(\mathbb{Q}_p) \to M_{p,f}$, and $X(\mathbb{Q}_l) \to M_l$, factor through ?? Kummer map.

Assume in addition to $X/\mathbb{Q}$ with $g \geq 2$, $\operatorname{rank} J(\mathbb{Q}) = g$, $\operatorname{rank} NS(J) > 1$, then there exists $z \in \operatorname{Pic}(X \times X)$ that allows us to construct a nice quotient $U = U_z$ of U_z. By Kim, U_n is the n-unipotent quotient of $?_1^{\text{ét}}(X_{\mathbb{Q}})$.

By work of Kim, have local unipotent Kummer maps $j_{u,v} : X(\mathbb{Q}_v) \to H^i(G_v, U)$. We will assume that $j_{i,l}$ is trivial for all $l \neq p$. In general, by Kim-Tamagawa know that $j_{u,l}$ has finite image. * this assumption is satisfied in the case of X having everywhere potentially good reduction.

So we have the following diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow ? & & \downarrow j_{i,p}:=j_p \\ H^i_f(G_p, U) & \longrightarrow & H^1_f(G_p, U) \end{array}$$

Lemma 4.1. *The set $X(\mathbb{Q})_U = j_p^{-1}(loc_p(H^1_f(G_p, U)))$ is finite. More generally, this result is holds for $r < g + \operatorname{rank} Ns(T) - 1$ We have $X(\mathbb{Q}) \subset X(\mathbb{Q})_u$ and the goal is to compute $X(\mathbb{Q}_p)_U$ using p-adic heights This is "quadratic Chabauty" for rational points.*

4.4 Lecture 4

5 Bas Edixhoven: Geometric Quadratic Chabauty

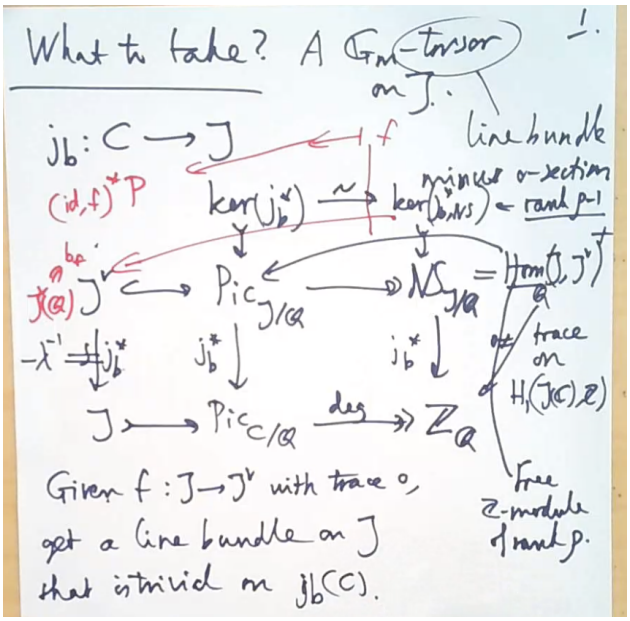
5.1 Lecture 1

This is joint work with Guido Lido. Let $C/\mathbb{Q}$ be a 'nice' curve with genus $g > 1$, and assume that we have a rational point $b \in C(\mathbb{Q})$. We have a map $j_b : C \to J$ given by $P \mapsto O_C(P - b)$. The Chabauty method has a problem if $r \not< g$:

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ \downarrow & & \cap \\ & & \overline{J(\mathbb{Q})} \\ & & \cap \\ C(\mathbb{Q}_p) & \longrightarrow & J(\mathbb{Q}_p) \end{array}$$

Our idea is to replace J be something bigger, of higher dimension, and then play the Chabauty 'game'.

The question is, what object to take? A $\mathbb{G}_m$-torsor (line bundle minus 0-section). Given the map $j_b : C \to J$, we have a diagram



5.1.1 Poincaré Bundle

For all abelian varieties A, we can view $A^\vee$ as $\mathrm{Ext}^1(A, \mathbb{G}_m)$, where

$$\mathbb{G}_m \longrightarrow E \overset{\mathbb{G}_m \text{ torsor}}{\longrightarrow} A$$

The maps $\mathbb{G}_m \to E$ are rigid: they have no non-trivial automorphisms that induce id_A and $\mathrm{id}_{\mathbb{G}_m}$. So over $A^\vee$, we have a universal extension

$$\begin{array}{ccccc} \mathbb{G}_{m,A} & \hookrightarrow & P^\times & \twoheadrightarrow & A \times A^\vee \\ & \searrow & \downarrow & \swarrow & \\ & & A^\vee & & \end{array}$$

$P^\times$ is also the universal extension of $A^\vee$ by $\mathbb{G}_m$ over A. So we have

$$\begin{array}{ccccc} j_b^* T_f & \longrightarrow & T_{f\,r} & \longrightarrow & P^\times \\ \updownarrow & \nearrow^{j_b} & & & \downarrow \\ C & \xrightarrow{j_b} & J & \xrightarrow{(\mathrm{id}, \mathrm{tr}_{b_f} \circ f)} & J \times J^\vee \end{array}$$

We know J has dimension g and T_{fr} has dimension $g+1$. Take a $\mathcal{Z}$-basis $f_1, \ldots, f_{j-1}$ of $\ker(j_{b??}^*)$, gives

$$\begin{array}{ccccc} & & T & \longrightarrow & (P^\times)^{j-1} \\ & \nearrow^{\tilde{j}_b} & \downarrow & & \downarrow \\ C & \xrightarrow{j_b} & J & \xrightarrow{(\mathrm{id}, \mathrm{tr}_{b_{f_1}} \circ f_1, \ldots, \mathrm{tr}_{b_{f_1}})} & J \times (J^\vee)^{p-1} \end{array}$$

Now $(P^\times)^{j-1}$ is a $\mathbb{G}_m^{p-1}$ torsor and T has dimension $g+p-1$. We play the Chabauty game in T. We hope that if it works that $r < g+p-1$. (most wanted example have $p = g$). Now $T(\mathbb{Q})$ is a $\mathbb{Q}^{\times, p-1}$-torsor.

$$\begin{array}{c} T(\mathbb{Q}) \\ \downarrow \\ J(\mathbb{Q}) \end{array}$$

Now $\mathbb{Q}^\times = \{\pm 1\} \times \mathcal{Z}$ (set of primes). There is a big problem: there are too many $\mathbb{Q}$-points in T. As a solution, we extend the geometry over $\mathcal{Z}$, $\mathcal{Z}^\times = \{\pm 1\}$.

Remark. From now on, everything is over $\mathcal{Z}$

Let C be a proper, regular model of $C_{\mathbb{Q}}$, and let J be the Néron model of $J_{\mathbb{Q}}$. Let $J^\vee$ be the Néron model of $J_{\mathbb{Q}}^\vee$, $J^{\vee,0} \subset J^\vee$, is the fiberwise connected component of α. Now $P^\times$ is the unique extension of $P_{\mathbb{Q}}^\times$ to $J \times J^{\vee,0}$ as a bi-extension.

Now $P^\times$ is a $\mathbb{G}_m$-biextension of $A \times A^\vee$. Then there are two partial group laws, given by what we have already seen. For example, one of them is: if $x_1, x_2 \in A$, and $y \in A^\times$, i.e. $(x_1, y), (x_2, y) \in A \times A^\vee$, $z_1 \in P^\times(x_1, y)$, $z_2 \in P^\times(x_2, y)$, then we obtain $z_1 +_1 z_2 \in P^\times(x_1 + x_2, y)$.

We use the biextension structure of $P^\times$ over $J \times J^{\vee,0}$ to parametrize

$$\begin{array}{c} T(\mathcal{Z}) \\ \vdots \downarrow \\ J(\mathcal{Z}) \end{array}$$

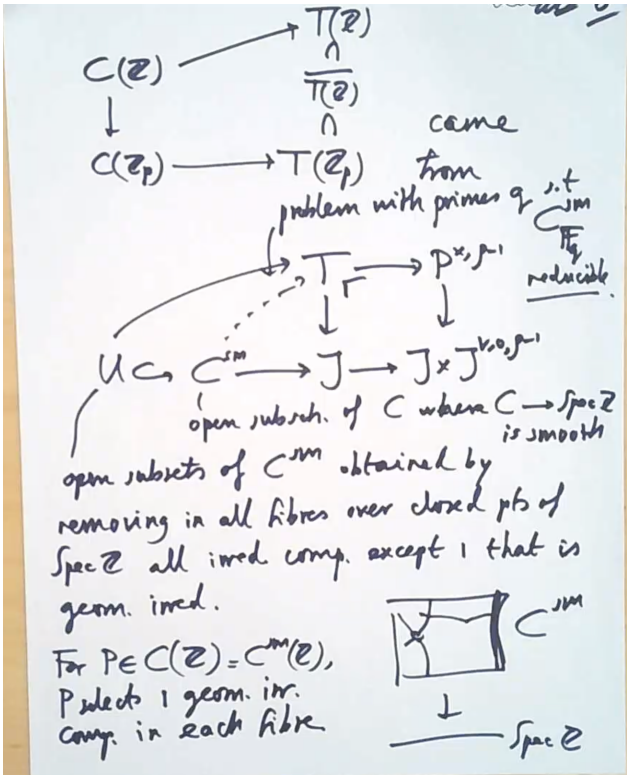
noting that $T(\mathcal{Z})$ is a $(\pm 1)^{p-1}$-torsor.

$$\begin{array}{ccc} C(\mathcal{Z}) & \longrightarrow & T(\mathcal{Z}) \\ \downarrow & & \cap \\ & & \overline{T(\mathcal{Z})} \\ & & \cap \\ C(\mathcal{Z}_p) & \longrightarrow & T(\mathcal{Z}_p) \end{array}$$

Now $C(\mathcal{Z}_p)$ is 1-dimensional, $g + p - 1$-dimensional, and $\overline{T(\mathcal{Z})}$ is at most r-dimensional.

5.2 Lecture 2

Excuse the laziness, typesetting will come later for this lecture...



Say n is the product of primes q of bad reduction of $C/\mathcal{Z}$. Then $C \to \operatorname{Spec} \mathcal{Z}$ is smooth over $\mathcal{Z}[1/n]$. These are finitely many of smooth U's and $C_{\mathbb{Q}} = C^{\mathrm{sm}}(\mathcal{Z}) = \sqcup_{\text{all } U\text{'s}} U(\mathcal{Z})$.

Example 5.1. $y^2 + y = x^6 + \cdots$ (see section 8 of the notes). $n = 3.43$, $C^{\mathrm{sm}}_{\mathbb{F}_{49}}$ ind $C^{\mathrm{sm}}_{\mathbb{F}_j}$. There are exactly 2 U's.

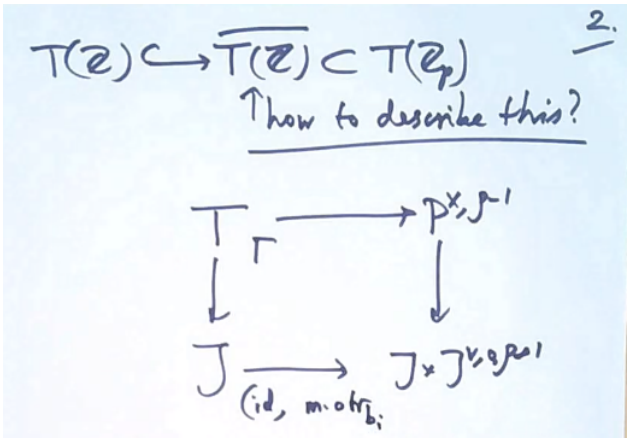
$J^{\vee,0} \hookrightarrow J^{\vee} \twoheadrightarrow \Phi^{\vee}$, the group scheme of components of $J^{\vee}$. $\Phi^{\vee}$ trivial over $\mathcal{Z}[1/n]$. Finite étfibers over $\mathcal{Z}/n\mathcal{Z}$. $m :=$ least common multiple of exponents of $\Phi^{\vee}(\tilde{\mathbb{F}}_q), q \mid n$.

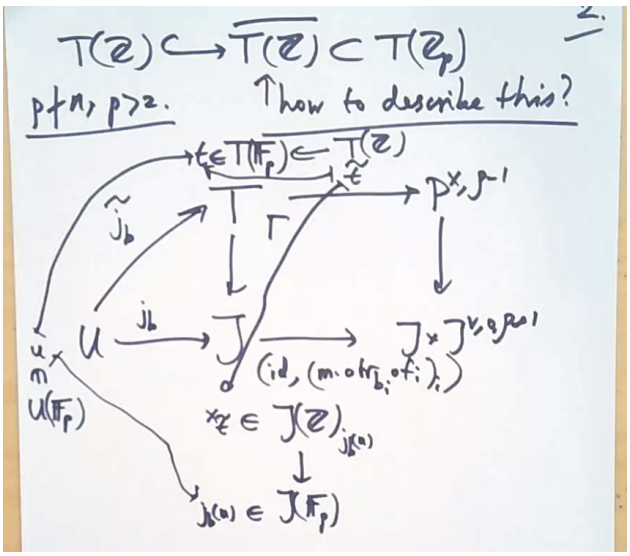
We want to create a map $J(\mathcal{Z}) \to T(\mathcal{Z})$ but this is difficult because no such map comes from geometry. $J(\mathcal{Z})_0 \cong \mathcal{Z}^r$, $x_1, \ldots, x_r$. We get a map $k_{\mathcal{Z}} : \mathcal{Z}^r \to T(\mathcal{Z})_t$, not really surjective.

Theorem 5.1 (4.10)**.**

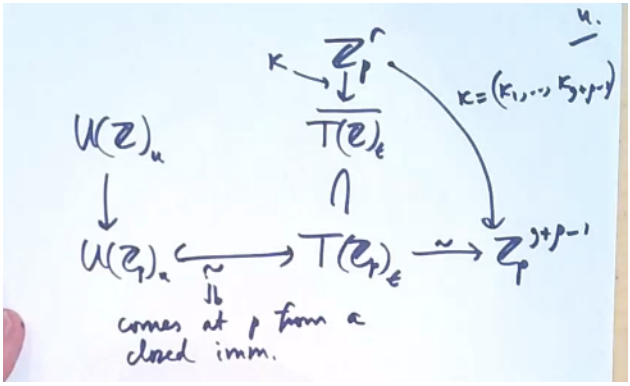
$$\mathcal{Z}^r \xrightarrow{k_{\mathcal{Z}}} T(\mathcal{Z}_p)_t \xrightarrow{\sim} \mathcal{Z}_p^{g+\rho-1}$$

where the bijection is given by evaluation at $1/p$ in the parametrization of $\mathcal{O}_{T,t}$. Note that $\mathcal{Z}^r \subset \mathcal{Z}_p^r$ is dense. There exists a unique $k = (k_1, \ldots, k_{g+\rho-1})$, $k_i \in \mathcal{Z}_p\langle z_1, \ldots, z_r\rangle = \mathcal{Z}_p[z_1, \ldots, z_r]^{\wedge p}$ and $\overline{T(\mathcal{Z})}_t$ is the image of k.





Proof. All of section 5, three and a half pages and lots of representations, $n \mapsto nP = \exp(n \log P)$. □



1. We want to pull back expressions fro the complete intersection $U \hookrightarrow T$ and at u get $g + \rho - 2$ equations to $\mathcal{Z}_p^r$.

2. We want to do this in terms of formal geometry, e.g. rings like $\mathcal{Z}_p\langle z_1, \ldots, z_r\rangle$, and then reduce mod p, so we get polynomials in $\mathbb{F}_p[z_1, \ldots, z_r]$.

5.3 Lecture 3

Let p be any prime number. Let X be a smooth, $\mathcal{Z}_p$-scheme of relative dimension d. Let $x \in X(\mathbb{F}_p)$.

$$\begin{array}{ccc} X(\mathcal{Z}_p) & \longrightarrow & X(\mathbb{F}_p) \\ \cap & & \cap \\ X(\mathcal{Z}_p)_n & \longrightarrow & \{n\} \end{array}$$

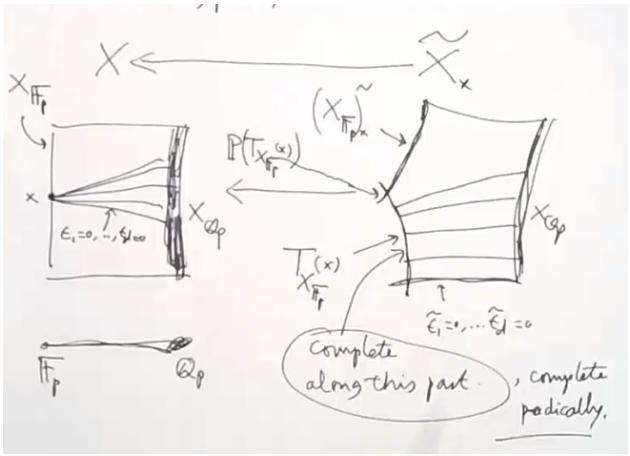
Let $p, t_1, \ldots, t_d$ be generators of the maximal ideal in $\mathcal{O}_{X,n}$.

$$X(\mathcal{Z}_p) \xrightarrow{??} p\mathcal{Z}_p^d \xrightarrow{\phi,\sim} \mathcal{Z}_p^d$$
$$\mathcal{Z} := (\mathcal{Z}_1, \ldots, \mathcal{Z}_d) = (t_1, p, t_2/p, \ldots, t_d/p)$$

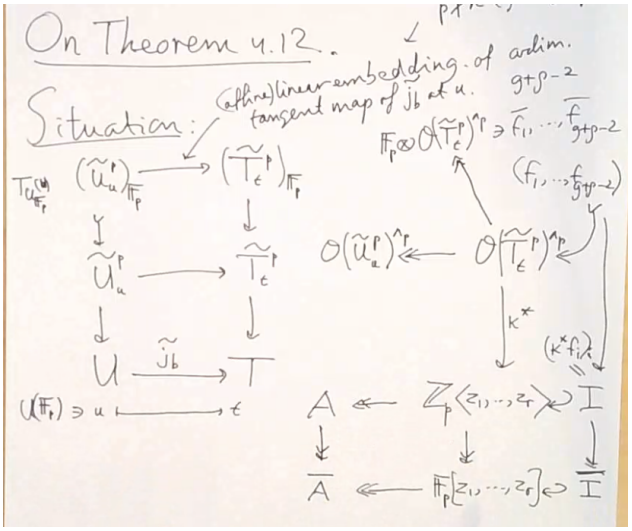
Geometrically, shrink X such that it is affine, t regular, and

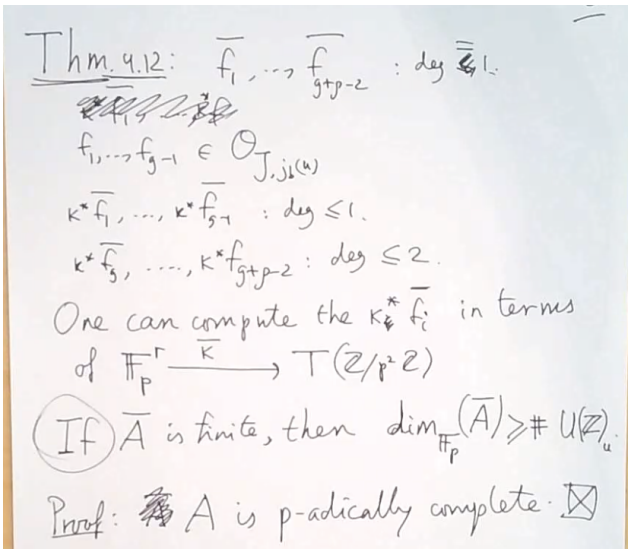
$$\begin{array}{ccccc} t^{\text{ét}} : X & \longrightarrow & \mathbb{A}^d_{\mathcal{Z}_p} & \longrightarrow & \mathcal{Z}_p[t_1, \ldots, t_d] \\ \pi \uparrow & & \uparrow & & \\ \tilde{X}^L_x & \longrightarrow & \mathbb{A}^d_{\mathcal{Z}_p^n} & p & \downarrow t_i \to p\tilde{t}_i \\ \cap & & \uparrow & & \\ \tilde{X}^p_x & \longrightarrow & \mathbb{A}^d_{\mathcal{Z}_p} & & \mathcal{Z}_p[\tilde{t}_1, \ldots, \tilde{t}_n] \end{array}$$

is the blow up in x. Note $t^{-1}(\mathbb{F}_p) = \{x\}$ and $\tilde{t}_i = t_i/p$. Now a picture for the case $d = 1$ and $p = 5$.



This gives $\mathcal{Z}_p\langle \tilde{t}_1, \ldots, \tilde{t}_d \rangle = \mathcal{Z}_p[\tilde{t}_1, \ldots, \tilde{t}_d]^{\vee p}$ is p-adically complete.
$\overline{\mathbb{F}}_p \otimes_{\mathcal{Z}_p} (\mathcal{O}(\tilde{X}^p_x)^{\vee p}) = \mathbb{F}_p[\tilde{t}_1, \ldots, \tilde{t}_d]$ germ $T_{X_{\mathbb{F}_p}}(x)$.
On Theorem 4.12


On Theorem 4.12.
Situation:
(affine)tangent map of $\tilde{j}_b$ at u.
embedding of ordim. $g+p-2$
$\mathbb{F}_p \otimes \mathcal{O}(\tilde{T}_\epsilon^p)^\wedge_p \ni \overline{f}_1, \cdots, \overline{f}_{g+p-2}$
$(f_1, \cdots, f_{g+p-2})$
$T_{U_{\mathbb{F}_p}^{(u)}}$
$(\tilde{U}_u^p)_{\mathbb{F}_p}$
$(\tilde{T}_\epsilon^p)_{\mathbb{F}_p}$
$\tilde{U}_u^p$
$\tilde{T}_\epsilon^p$
U
$\tilde{j}_b$
T
$(\mathbb{F}_p) \ni u \longmapsto \epsilon$
$\mathcal{O}(\tilde{U}_u^p)^\wedge_p \leftarrow \mathcal{O}(\tilde{T}_\epsilon^p)^\wedge_p$
k^*
$(k^* f_i)_i$
$A \leftarrow \mathbb{Z}_p\langle z_1, \cdots, z_r \rangle \twoheadleftarrow I$
$\overline{A} \leftarrow \mathbb{F}_p[z_1, \cdots, z_r] \twoheadleftarrow \overline{I}$


Thm. 4.12: $\overline{f}_1, \cdots, \overline{f}_{g+p-2}$: deg ≤ 1.
$f_1, \cdots, f_{g-1} \in \mathcal{O}_{J, j_b(u)}$
$k^* \overline{f}_1, \cdots, k^* \overline{f}_{g-1}$: deg ≤ 1.
$k^* \overline{f}_g, \cdots, k^* f_{g+p-2}$: deg ≤ 2.
One can compute the $k_\ell^* \overline{f}_i$ in terms of $\mathbb{F}_p^r \xrightarrow{\overline{\kappa}} T(\mathbb{Z}/p^2\mathbb{Z})$
If $\overline{A}$ is finite, then $\dim_{\mathbb{F}_p}(\overline{A}) \geq \#\, U(\mathbb{Z})_u$.
Proof: A is p-adically complete. $\boxtimes$

5.4 Lecture 4