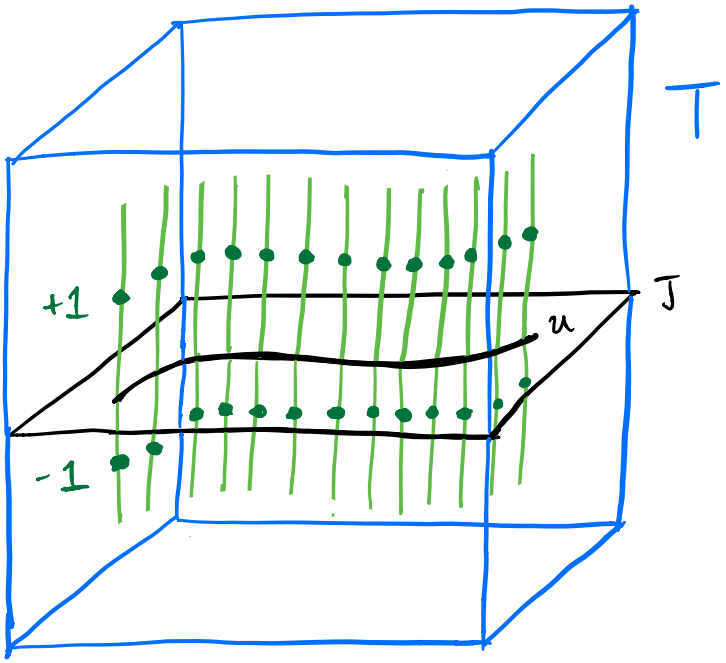
A CARTOON GUIDE to FINDING $\mathbb{Q}$-PTS WITH GEOMETRIC QUADRATIC CHABAUTY:

Making quadratic Chabauty friendly again.™

Sachi Hashimoto



Section I: Introduction

This note aims to make (geometric) quadratic Chabauty friendly again by describing it only in terms of "simple cartoons." Section I describes the set-up. Section II describes the geometric method in less than 10 cartoons. Appendix A describes the parameters on the Jacobian.

Acknowledgements

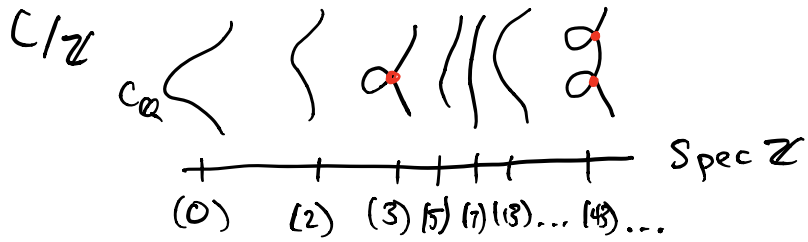
These notes grew out of a project with Hannah Larson to read Edixhoven and Lido's "Geometric Quadratic Chabauty." Much of the original illustration and exposition is joint work with Hannah.

The cartoon in Section II.v on parameters for $U(\tilde{X})^{\wedge p}$ is a modified version of a cartoon originally drawn by Bas Edixhoven at the 2020 Arizona Winter School.

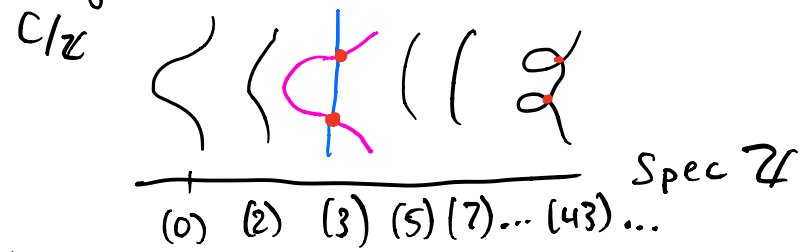
I. i. The Curve (Surface?)

This is a curve: or so you thought!

If your curve were defined over $\mathbb{Z}$, the pretty thing you drew is just $C_{\mathbb{Q}}$. To study arithmetic properties of the curve, we actually study a "surface":

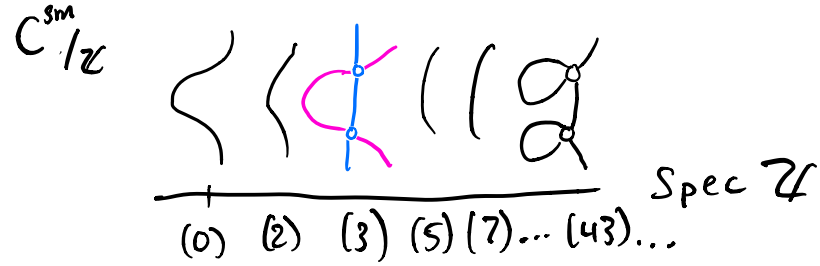


For each p, we can reduce mod p to get $C_{\mathbb{F}_p}$. Most fibres are smooth, a few are singular. If a point is singular on the surface, we blow it up:

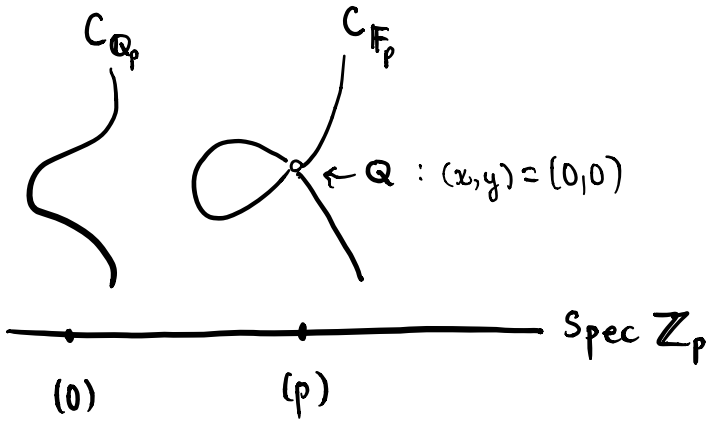


From now on, assume that C is regular.

When we write C^{sm}, we mean C minus any points that are singular in the fibers over Spec $\mathbb{Z}$, so:



An important fact is that $C_{\mathbb{Q}}(\mathbb{Q}) = C^{sm}(\mathbb{Z})$. It suffices to argue locally near any point we removed

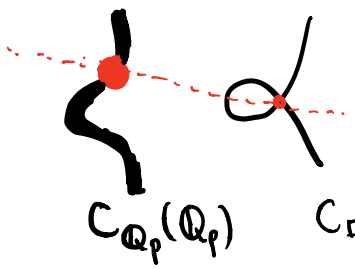


Because C is regular, $\dim \mathfrak{m}_Q/\mathfrak{m}_Q^2 = 2$

But Q is singular in the fiber over (p) so the tangent space at Q to the fiber also has dim 2. Since the fiber is cut out by the vanishing of p, the tangent space to the fiber is also cut out by p (inside $\mathfrak{m}_Q/\mathfrak{m}_Q^2$), ie

$$\dim \left(\mathfrak{m}_Q/\mathfrak{m}_Q^2\right)/(p) = 2 = \dim \mathfrak{m}_Q/\mathfrak{m}_Q^2 \Rightarrow p \in \mathfrak{m}_Q^2.$$

Suppose we have a $\mathbb{Q}_p$ point whose reduction mod p is Q



(ie a $\mathbb{Z}_p$ point)

This all takes place inside some affine chart say $\frac{\operatorname{Spec} \mathbb{Z}_p[x,y]}{(f(x,y))} \subset C_{\mathbb{Z}_p}$ w/ coords s.t. $m_Q = (p, x, y)$ and our $\mathbb{Z}_p$ point is some $(X, Y) = (0,0) \bmod p$.

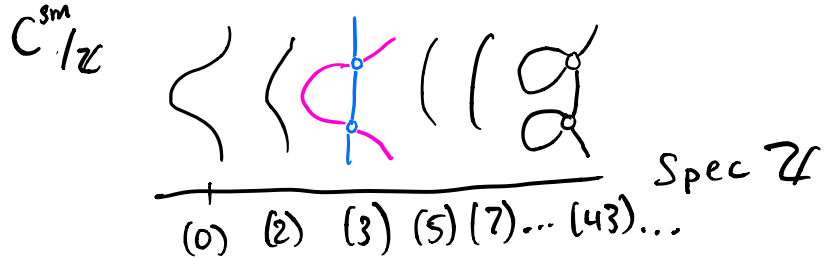
From before, $p \in m_Q^2$. This means we can write $p = \lambda f(x,y) + (p, x, y)^2$ in $\mathbb{Z}_p[x,y]$

Hence,

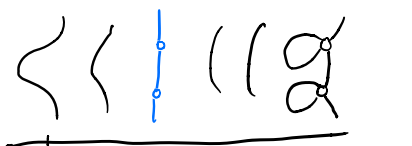
$$\underbrace{\lambda f(X,Y)}_{=0} + \text{stuff with valuation} \geq 2 = \underbrace{p}_{\text{valuation } 1}$$

This is a contradiction so there are no $\mathbb{Z}_p$-points reducing to Q mod p. □

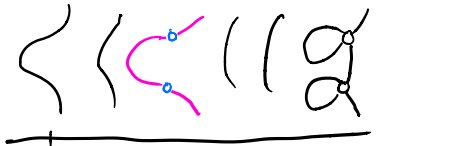
After blowing up so that C is regular, some fibers $C_{\mathbb{F}_p}$ may have multiple components:



We define $U_i \subset C^{sm}$ to be open sets obtained by removing all but one irreducible component over $C_{\mathbb{F}_p}$:



U_0

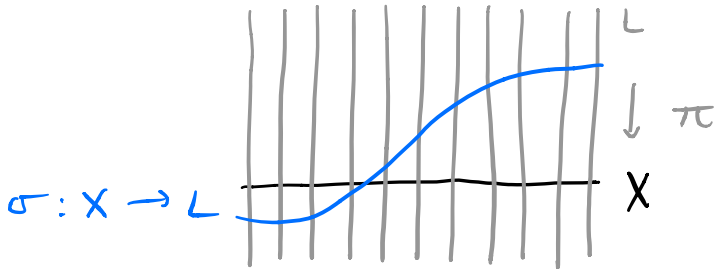


U_1

Section II: From Torsors to Finiteness

II.i How to stop worrying and work with $\mathbb{G}_m$-torsors

This the total space of a line bundle:

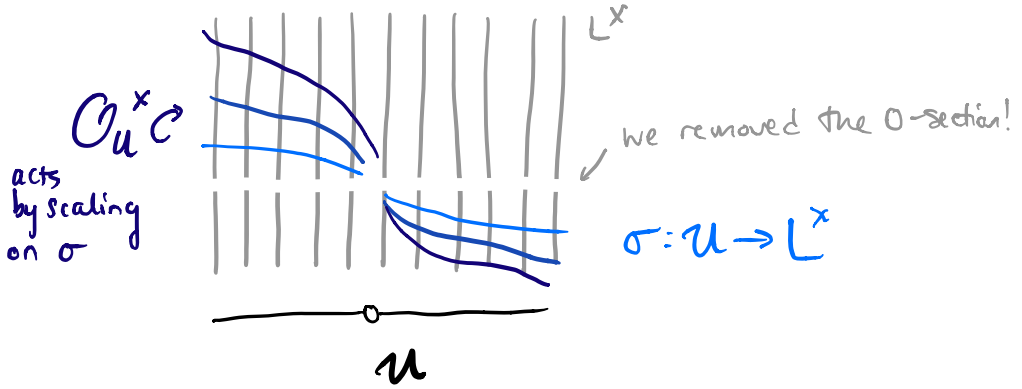


as a sheaf, $\mathcal{L}(U) = \{\sigma : U \to L : \pi \circ \sigma = id\}$.

The associated $\mathbb{G}_m$-torsor $\mathcal{L}^\times$ is the sheaf

$\mathcal{L}^\times(U) = \{\sigma : U \to L : \pi \circ \sigma = id$ and $\sigma(p) \neq 0 \ \forall p \in U\}$.

Thus we picture it like so:



This respects pullback, so for any scheme S over X,

$$\mathcal{L}^\times(S) = \left\{ \begin{array}{ccc} \sigma : S & \to & L^\times \\ & \searrow & \swarrow \\ & X & \end{array} \text{ commutes} \right\}.$$

We will apply the above constructions to the Poincaré line bundle to get the Poincaré torsor.

II.ii Why is everything named after Poincaré?

Let J be the (Néron model) of the Jacobian of C over $\mathbb{Z}$, and $J^\vee$ the dual so that J parametrizes deg 0 line bundles over C and $J^\vee$ parametrizes deg 0 line bundles on J. (Yo dawg I heard you liked line bundles so I put some line bundles on your line bundles...)

On $J \times J^\vee$, there is a master line bunde P_Q, the Poincaré line bundle. It is determined by 2 properties:

Each $c \in J^\vee$ corresponds to a line bundle L_c on J.

① $P|_{J \times \{c\}} \cong L_c$.

(so as a special case $P|_{J \times \{0\}}$ is trivial)

There are many line bundles with property ①. If P satisfies ① and M is any line bundle on $J^\vee$, then

$$(P \otimes \pi_2^* M)|_{J \times \{c\}} \cong P|_{J \times \{c\}} \otimes \underbrace{(\pi_2^* M)|_{J \times \{c\}}}_{\text{trivial}} \cong L_c$$

② So we additionally require $P|_{J^\vee \times \{0\}}$ is trivial

This uniquely identifies P.

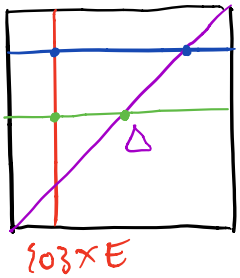
Example

Let E be an elliptic curve. Then $J = E = J^\vee$.

The Poincaré bundle P on $E \times E$ has a nice description as $P = \mathcal{O}_{E\times E}(\Delta - \{0\}\times E - E \times \{0\})$, where Δ is the diagonal.

(1) For $c \in E$, $P|_{\{c\}\times E} = \mathcal{O}_E(c - 0)$

(2) $P|_{E\times\{0\}} = \mathcal{O}_E$



$E \times \{0\} \simeq \mathcal{O}_E$

$P|_{\{c\}\times E} \simeq \mathcal{O}_C(c-0)$

Remarks

- P is symmetric: $[-1]^* P = P$
- Exchanging J and $J^\vee$ identifies $J \simeq J^\vee$ and leaves P unchanged

Let Θ be the Theta divisor on J, which induces the principal polarization $\lambda : J \to J^\vee$ in the following way:

$$\begin{array}{ccc} \lambda : J & \longrightarrow & J^\vee \\ a & \mapsto & [t_a^* \Theta - \Theta] \end{array}$$

where $t_a : J \to J$ is translation by a.

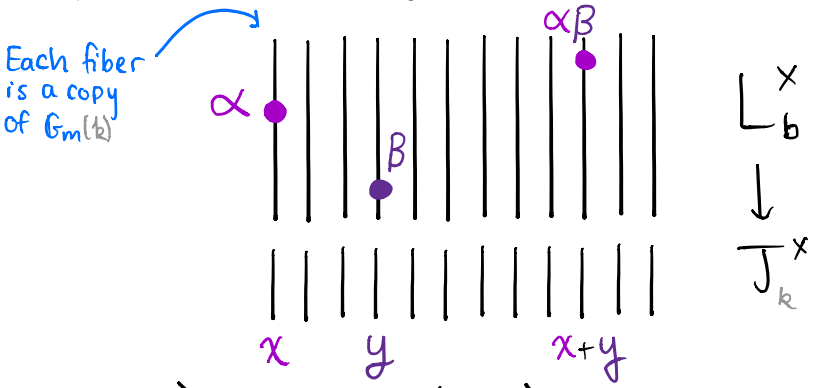
The Poincaré torsor is a biextension of $J_k \times J_k^\vee$ by $\mathbb{G}_m(k)$ meaning the following: there is a map (*)

$$P_k^\times \xrightarrow{\pi} J_k \times J_k^\vee$$

making $J_k \times J_k^\vee$ into the quotient of $P_k^\times$ by $\mathbb{G}_m(k)$.

(*) one should be careful about the "field" of definition. We take $k = \mathbb{Q}$ first, but we will need to work over $\mathbb{Z}$ later. To do so, we must instead take π mapping into $J \times J^{\vee 0}$ where $J^{\vee 0}$ is the fiberwise connected component of 0 in $J^\vee$.

For every fiber $J_k \times \{b\}$, $\pi^{-1}(J_k \times \{b\})$ is a line bundle $L_b^\times$ in $P_k^\times$ and for any $x, y \in J_k \times J_k^\vee$



with $x = (\alpha, b)$ and $y = (\beta, b)$, we can define "$x +_1 y$" to be $\alpha\beta$ in $(L_b)_{x+y} = (t_{x+y}^* L_b)_0$. This makes sense by applying the Theorem of the Square:

$$(t_x^* L_b)_0 \otimes (t_y^* L_b)_0 \simeq (t_{y+x}^* L_b)_0 \otimes (L_b)_0$$

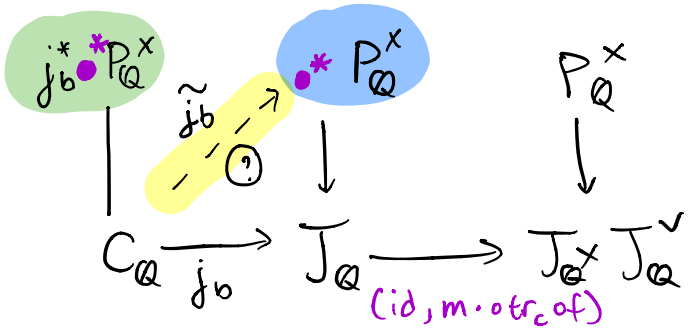
Similarly, if $x = (b, \alpha)$ and $y = (b, \beta)$, we can define "$x +_2 y$". These operations are compatible: if $x = (a_1, b_1)$, $y = (a_1, c_1)$, $u = (d_1, b_1)$, $v = (d_1, c_1)$, then

$$(x +_1 y) +_2 (u +_1 v) = (x +_2 u) +_1 (y +_2 v).$$

II.iii Chabauty's Theorem

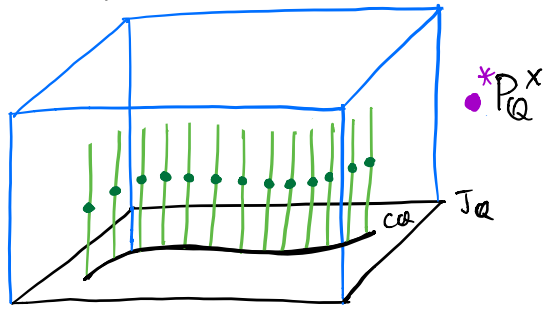
Let $b \in C(\mathbb{Z})$ be a basepoint. This gives a morphism $j_b: C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ which extends uniquely to $j_b: C^{sm} \to J$. We want to lift j_b on the open $U \subset C^{sm}$ to a morphism to a $\mathbb{G}_m^{\rho-1}$-torsor T over J, where $\rho \overset{\circledast}{=} \operatorname{rank} \operatorname{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)^+$, the free $\mathbb{Z}$-module of self-dual homomorphisms. Let $m_\bullet$ denote multiplication by m on J, tr_c translation by c in $J^\vee(\mathbb{Z})$, and $f \in \operatorname{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)^+$. $\circledast$ ρ is also $\operatorname{rk} NS(J_{\mathbb{Q}})$.

Then



j_b lifts to $\tilde{j}_b$ iff $j_b^* P_{\mathbb{Q}}^X$ is trivial on $C_{\mathbb{Q}}$.

"Proof" (sketch)



A nonzero section trivializes the line bundle over $C_{\mathbb{Q}}$.

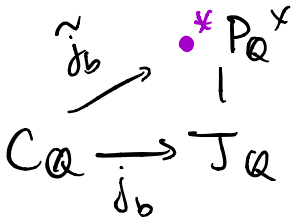
□

Given a fixed f, for what c is $j_b^*(\mathrm{id}, \operatorname{tr}_c \circ f)^* P_{\mathbb{Q}}^X$ trivial? (and therefore $j_b^* P_{\mathbb{Q}}^X$ trivial). Well, tr_c has the effect of tensoring with the inverse of the line bundle corresponding to $c \in J_{\mathbb{Q}}^\vee$, so $j_b^* P_{\mathbb{Q}}^X$ is trivial exactly when c corresponds to the line bundle $(\mathrm{id}, f)^* P_{\mathbb{Q}}^X$. For this to make sense, $(\mathrm{id}, f)^* P_{\mathbb{Q}}^X$ should have degree 0.

$\deg L_c \in J_{\mathbb{Q}}^\vee$.

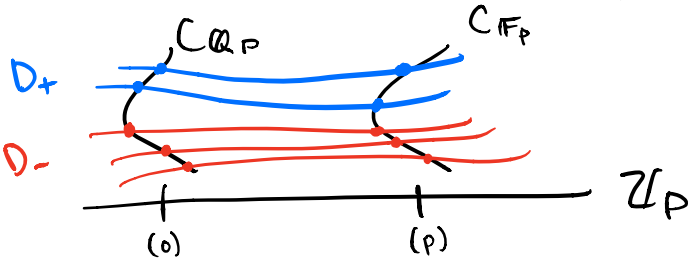
Let $f_1, \dots, f_{p-1}$ be a basis for $\mathrm{Hom}(J_{\mathbb{Q}}, J_{\mathbb{Q}}^\vee)^+$ with $(\mathrm{id}, f_i)^* P_{\mathbb{Q}}^\times$ degree 0. Then let c_i be the associated translation making $j_b^* P_{\mathbb{Q}}^\times$ trivial. By construction, we have, for each f_i

Lifts are unique up to an element of $\mathbb{Q}^\times$



But, we want to spread this out over $\mathbb{Z}$. For each $\mathcal{U} = \mathcal{U}_i$ discussed in Section I, $\mathrm{Pic}(\mathcal{U}) \to \mathrm{Pic}(C_{\mathbb{Q}})$ given by restricting to the generic fiber is an isomorphism:

- given $L \in \mathrm{Pic}(C_{\mathbb{Q}})$ write $L = \mathcal{O}(D_+ - D_-)$ ($V(f) = V(\lambda f)$, $V(g) = V(\lambda g)$)
- for each p prime, we can normalize
$$p^n f \in \mathbb{Z}_p \setminus p\mathbb{Z}_p, \quad p^m g \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$$
- then locally we have $L \in \mathrm{Pic}(C_{\mathbb{Q}_p})$

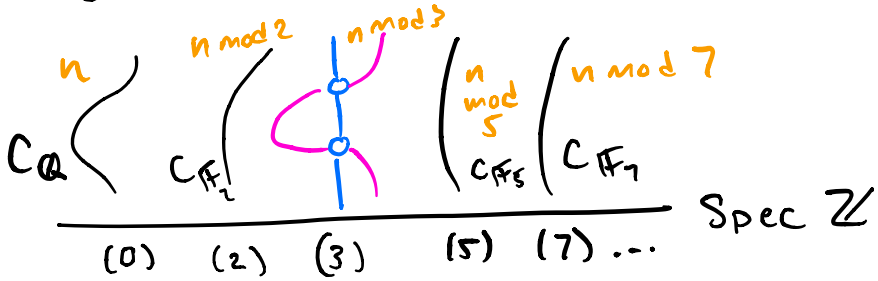


so then

$$D_+ = V(p^n f) \subseteq C_{\mathbb{Q}_p} \text{ and also } \subseteq C_{\mathbb{F}_p}$$
$$D_- = V(p^m g) \subseteq C_{\mathbb{Q}_p} \text{ also } \subseteq C_{\mathbb{F}_p}$$
$$\Rightarrow D_+ \text{ and } D_- \text{ are defined over } \mathbb{Z}_p$$

$\Rightarrow L$ is defined over $\mathcal{U}$.

Furthermore, $\mathcal{O}_C(\mathcal{U}) = \mathbb{Z}$, since for $n \in \mathcal{O}_C(\mathcal{U})$



we have the following commuting diagram

$$\begin{array}{ccc} n \in \mathcal{O}_C(\mathcal{U}) & \xrightarrow{\text{res}} & \mathcal{O}_{C_{\mathbb{Q}}}(C_{\mathbb{Q}}) = \mathbb{Q} \\ & \searrow^{\text{res}} & \uparrow \text{mod } p \\ & & \mathcal{O}_{C_{\mathbb{F}_p}}(C_{\mathbb{F}_p}) \\ & & \| \\ & & \mathbb{F}_p \end{array}$$

Because this map is well-defined, we can't have any denominators.

□

Since $\mathrm{Pic}(\mathcal{U}) \simeq \mathrm{Pic}(C_{\mathbb{Q}})$, we can lift j_b to $\tilde{j}_b$ for each $\mathcal{U}$, and $j_b^* \cdot^* P^X$ is trivial by construction

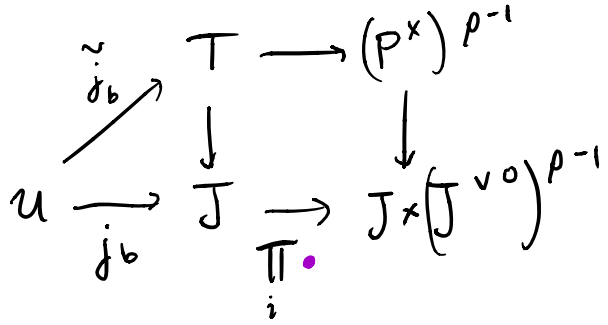
$\{\pm 1\} = \mathbb{Z}^\times = \mathcal{O}_C^\times(\mathcal{U}) \circlearrowright$ $j_b^* \cdot^* P^X$ $\cdot^* P^X$

$$\begin{array}{ccc} \downarrow & \overset{\tilde{j}_b}{\nearrow} & \downarrow \\ \mathcal{U} & \xrightarrow[j_b^*]{} & J \end{array}$$

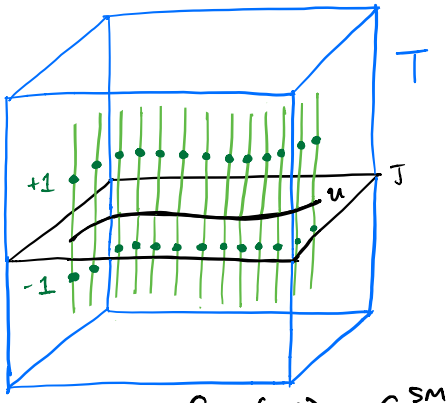
and unique up to a choice of $\mathbb{Z}^\times = \{\pm 1\}$. We let

$$T := \prod_{i=1}^{p-1} \cdot^* P^X$$ be the $\mathbb{G}^{p-1}$-torsor over J.

Then we have the diagram:



upon which we compute "heuristic dimensions".



For each rational point $x \in C_{\mathbb{Q}}(\mathbb{Q}) = C^{sm}(\mathbb{Z})$, x lies in one of the (finitely many) $\mathcal{U}(\mathbb{Z})$'s. For each open $\mathcal{U}(\mathbb{Z})$, the lift $\tilde{j}_b(\mathcal{U}(\mathbb{Z}))$ is contained in the p-adic closure of $T(\mathbb{Z})$ in $T(\mathbb{Z}_p)$.

$$\begin{array}{ccccccc} & & \overset{\text{like } (\mathbb{Z}^x)^{p-1} \times \mathbb{Z}^r}{T(\mathbb{Z})} & \subset & \overset{\dim \le r}{\overline{T(\mathbb{Z})}} & \subset & \underset{\dim g+p-1}{T(\mathbb{Z}_p)} \\ & \overset{\tilde{j}_b}{\nearrow} & \downarrow & & & & \downarrow \\ \mathcal{U}(\mathbb{Z}) & \xrightarrow[j_b]{} & J(\mathbb{Z}) & \subset & \underset{\dim \le r}{\overline{J(\mathbb{Z})}} & \subset & \underset{\dim\ g}{J(\mathbb{Z}_p)} \end{array}$$

Considering $\underbrace{\tilde{j}_b(\mathcal{U}(\mathbb{Z}))}_{1-\dim 1} \cap \underbrace{\overline{T(\mathbb{Z})}}_{\dim \le r}$ we expect to get a finite set when $r < g+p-1$. Hence we expect C has finitely many rational points, and studying this intersection gives a potential method of finding them all. (This is an analogue of Chabauty's Theorem.)

II.iv Biextensions for fun and profit

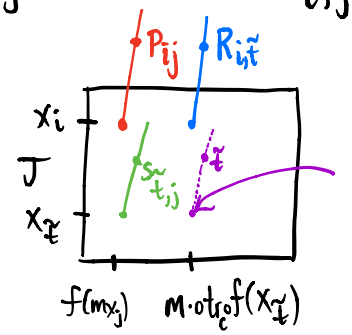
To prove $U(\mathbb{Z})$ is finite, it suffices to fix some good prime p and prove that for each $u \in U(\mathbb{F}_p)$, there are finitely many $\mathbb{Z}$ points reducing to u mod p. We call the set of all such points the <u>residue disk</u> $U(\mathbb{Z})_u$. Let $t = j_b(u)$ and choose any $\tilde{t} \in T(\mathbb{Z})_t$

$$\begin{array}{ccccc} & & t & & \\ & \nearrow^{\tilde{j}_b} & \uparrow & & \\ u \in U(\mathbb{F}_p) & \xrightarrow{j_b} & T(\mathbb{F}_p) & \xleftarrow{\text{red mod } p} & T(\mathbb{Z}) \ni \tilde{t} \\ & & & & \downarrow \\ & & J(\mathbb{F}_p) \ni j_b(u) & \longleftarrow & J(\mathbb{Z}) \ni x_{\tilde{t}} \end{array} \quad \leftarrow \text{image of } \tilde{t}.$$

Let $x_1, \dots, x_r$ be a basis for $\ker\left(J(\mathbb{Z}) \longrightarrow J(\mathbb{F}_p)\right)$. Since it is a free $\mathbb{Z}$-module,

$$\left\{ x_{\tilde{t}} + \textstyle\sum_i n_i x_i : (n_1, \dots, n_r) \in \mathbb{Z}^r \right\} = J(\mathbb{Z})_{j_b(u)}$$

We will now use the biextension structure on P^x (and so $P^{x,p-1}$) to produce a parametrization of $T(\mathbb{Z})_t := \{\mathbb{Z} \text{ points reducing to } t \text{ mod } p\}$. We start by producing a bunch of points in $P^{x,p-1}$ which we smoosh together to get something that actually lives in $T(\mathbb{Z})$. Choose points P_{ij}, $R_{i\tilde{t}}$ and $S_{\tilde{t},j}$ in $P^{x,p-1}$ as pictured below:



Notice: this corner of the rectangle is $\bullet(x_{\tilde{t}})$.

The biextension allows us to add things on the same horizontal or vertical fibers, denoted $+_2$ (resp. $+_1$).

$$\begin{array}{c} (J^{\vee 0})^{p-1} \\ \uparrow f = (f_1, \dots, f_{p-1}) \\ J \end{array}$$

We want to make things in $P^{x,p-1}$ that live over

- $(x_{\tilde{t}} + \sum_1 n_i x_i)$ and reduce to t mod p.

that reduces to

- $(x_{\tilde{t}})$ mod p

Observe that for $X \in T(\mathbb{F}_p)$, we have $(p-1) \cdot_1 X$ and $(p-1) \cdot_2 X$ are both the identity element of the fiber $(\mathbb{F}_p^x)^{p-1}$ they live in. Therefore, anything of the form

$$\left(\left(\sum_1 n_i \cdot_1 \sum_2 n_j \cdot_2 P_{ij} \right) +_2 \left(\sum_1 n_i \cdot_1 R_{i,\tilde{t}} \right) \right) +_1 \left(\left(\sum_1 n_j \cdot_2 S_{\tilde{t},j} \right) +_2 \tilde{t} \right) := D_{\tilde{t}}(n)$$

where $n = (n_1, \dots, n_r) \in \mathbb{N}^r$

where $(p-1) \mid n_i \ \forall i$ will reduce to t mod p, and thus gives an element of $T(\mathbb{Z})_t$.

This gives the map

$$K_{\mathcal{Z}}: \mathcal{Z}^r \longrightarrow T(\mathcal{Z})_t, \quad n \mapsto D_t^{\sim}((p-1)n).$$

Theorem 4.10

The map $K_{\mathcal{Z}}$ extends uniquely to a continuous map

$$K: \mathbb{Z}_p^r \xrightarrow[\text{choosing parameters}]{\sim} \overline{T(\mathcal{Z})}_t \xrightarrow{\dim r} T(\mathbb{Z}_p) \xrightarrow[\text{choosing parameters}]{\sim} \mathbb{Z}_p^{g+p-1}$$

whose image is $\overline{T(\mathcal{Z})}_t$, $K = (K_1, \dots, K_{g+p-1})$ in $\mathbb{Z}_p\langle z_1, \dots, z_r \rangle$.*

* A note about degrees: the degree of K_i, $1 \le i \le g+p-1$ in $\mathbb{F}_p[z_1, \dots, z_r]$ is 1 for $i \le g$ and 2 for $i > g$.

II. v Finiteness, finally

The time has come (the Walrus said) to talk of many things: of systems of parameters — and finiteness of points.

First, we set-up some notation: we work with overconvergent power series on our residue disks. We denote

$$\mathcal{O}(\tilde{X}_x)^{\wedge p} = \left\{ \sum_{I \in \mathbb{N}^d} a_I \tilde{t}^I \in \mathbb{Z}_p[[\tilde{t}_1, \dots, \tilde{t}_d]] : \forall n \ge 0 \text{ for almost all } I, v_p(a_I) > 0 \right\}$$

where X_x is a smooth scheme of relative dimension d over $\mathbb{Z}_p$ and $p, t_1, \dots, t_d$ are a system of parameters for X at $x \in X$.

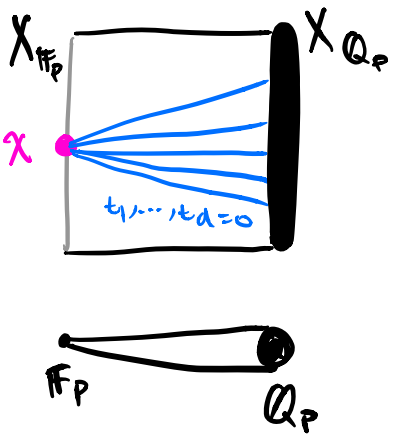
These parameters give an isomorphism of the residue disk to affine space:

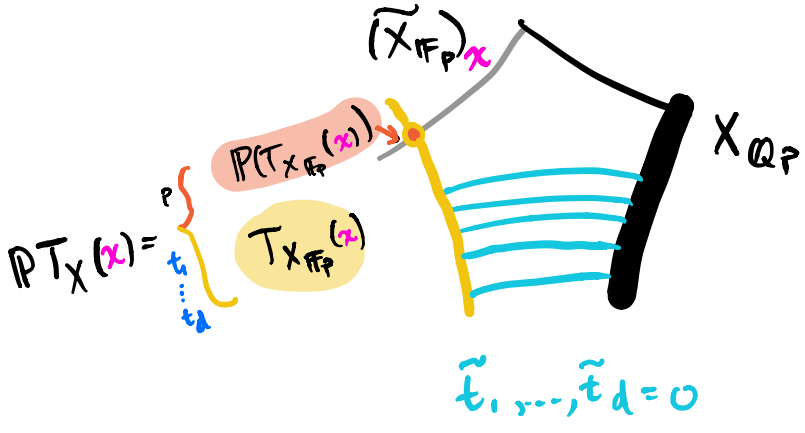
$$X(\mathbb{Z}_p)_x \xrightarrow[\sim]{t_1,\dots,t_d} p\mathbb{Z}_p^d \xrightarrow[\sim]{\frac{1}{p}} \mathbb{Z}_p^d$$

$$\tilde{t} = (\tilde{t}_1, \dots, \tilde{t}_d)$$

which geometrically we can picture as a blow-up. Shrinking X so that X is affine and t_i are regular, $t_i : X \to \mathbb{A}^d_{\mathbb{Z}_p}$ étale, $t^{-1}(0_{\mathbb{F}_p}) = \{x\}$ we have

$$X \leftarrow \tilde{X}_x$$





and p-adically completing along $T_{X_{\mathbb{F}_p}}(x)$ gives

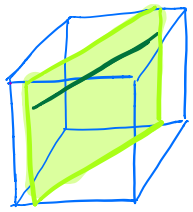
$$\mathcal{O}(\tilde{X}_x)^{\wedge_p} = \mathbb{Z}_p\langle \tilde{t}_1,\dots,\tilde{t}_d \rangle = \mathbb{Z}_p[\tilde{t}_1,\dots,\tilde{t}_d]^{\wedge_p}.$$

We want to understand $\tilde{j}_b(U(\mathbb{Z}_p)_u) \cap \overline{T(\mathcal{Z})}_t \subset T(\mathbb{Z}_p)_t$.

This is a complete intersection in $T(\mathbb{Z}_p)_t$, cut out by equations (*) $g_1, \dots, g_{g+p-2} \in \mathbb{Z}\langle z_1, \dots, z_{g+p-1}\rangle$. Composing $K^*: \mathcal{O}(\tilde{T}_t)^{\wedge p} \to \mathcal{O}(\mathbb{A}^r)^{\wedge p}_{\mathbb{Z}_p}$ with the parametrization of $\overline{T(\mathcal{Z})}_t \subset T(\mathbb{Z}_p)_t$, we obtain

$K^*g_1, \dots, K^*g_{g+p-2} \in \mathbb{Z}_p\langle z_1, \dots, z_r\rangle$.

(*) We use g_i for these equations, which Edixhoven-Lido call f_i, to avoid confusion with the other f_i.



$$\begin{array}{ccccc} & & \overline{T(\mathcal{Z})}_t & \xrightarrow{\sim} & \mathbb{Z}_p^r \\ & & \downarrow & & \downarrow K \\ \mathbb{Z}_p & \xrightarrow{\sim} U(\mathbb{Z}_p)_u & \xrightarrow{\tilde{j}_b} T(\mathbb{Z}_p)_t & \xrightarrow{\sim} & \mathbb{Z}_p^{g+p-1} \end{array}$$

Then morphisms $\left(\dfrac{\mathbb{Z}_p\langle z_1, \dots, z_r\rangle}{(K^*g_1, \dots, K^*g_{g+p-2})}\right)_{red} \to \mathbb{Z}_p$ are in bijection with points of $j_b(U(\mathbb{Z}_p)_u) \cap \overline{T(\mathcal{Z})}_t$.

Rmk: Geometric quadratic Chabauty, unlike its "non-geometric" counterpart, works locally in each residue disk of the biextension. This local strategy does not readily provide any global bound, but provides some flexibility in the choice of $\tilde{j}_b$ for each u.

Let $A = \left(\frac{\mathbb{Z}_p\langle z_1, \dots, z_r \rangle}{(K^* g_1, \dots, K^* g_{g+r^2})} \right)$.

Thm (4.12) Assume $\bar{A} := A/pA$ is finite. Then

$$\sum_{\substack{\mathfrak{m} \text{ maximal} \\ \text{ideal of } A}} \dim_{\mathbb{F}_p} \bar{A}_{\mathfrak{m}}$$

is an upper bound for the number of elements of $\mathcal{U}(\mathbb{Z})$ with with image u in $\mathcal{U}(\mathbb{F}_p)$.*

*A note about degrees: $\deg \bar{g}_i = 1$, so we can write $K^* \bar{g}_i$ as an $\mathbb{F}_p$-linear combination of the K_i. Then $g_1, \dots, g_{g-1} \in \mathcal{O}(J_{b(u)})^{\eta_p}$, and by 4.10 for $i < g$, $\deg K^* \bar{g}_i = 1$, for $i \geq g$ $\deg K^* \bar{g}_i = 2$. Hence "quadratic".

Proof Sketch: A is p-adically complete so $\bar{A}$ finite $\Rightarrow$ A finitely generated as a $\mathbb{Z}_p$-module.

Then we can write A as a product of its localizations

$$A = \prod_{\substack{\mathfrak{m} \\ \text{maximal}}} A_{\mathfrak{m}}, \quad \text{so} \quad \operatorname{Hom}(A, \mathbb{Z}_p) = \prod_{\substack{\mathfrak{m} \\ \text{maximal}}} \operatorname{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p).$$

Then $\#\operatorname{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p) \leq \operatorname{rank}_{\mathbb{Z}_p}(A_{\mathfrak{m}}) \leq \dim_{\mathbb{F}_p}(\bar{A}_{\mathfrak{m}})$.*

*Note $\operatorname{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p) = \emptyset$ if $A/\mathfrak{m} \neq \mathbb{F}_p$, so it suffices to consider $A_{\mathfrak{m}}$ with the correct residue field. □

The goal, then, is to apply theorem 4.12 to establish upper bounds which are sharp in each residue disk, for some fixed prime p. To do so, one must establish finiteness of $\bar{A}$ for every $\mathcal{U}_i$ and every $u \in \mathcal{U}_i(\mathbb{F}_p)$.

Appendix A: Why 2?

When applying Theorem 4.12, we work with p-adic power series $K^* g_i$. The amazing fact of geometric quadratic Chabauty is that the necessary "precision"⊛ for computing $K^* g_i$ is only 2. We explain this in this appendix by showing that for $(D,E) \in (J \times J)(\mathbb{F}_p)$ we can parametrize $(J \times J)(\mathbb{Z}/p^2)_{(D,E)}$ and hence, for an avatar of the Poincaré torsor $\mathcal{M}$ (over $J \times J$), we obtain a parametrization of $\mathcal{M}^\times(\mathbb{Z}/p^2)_{(D,E)}$

$$\begin{array}{ccc} P & \longrightarrow & \mathcal{M} \\ \downarrow & & \downarrow \\ J \times_S J & \xleftarrow{\text{id} \times j_b^{*,-1}} & J \times_S J \end{array}$$

(M is for Mumford)

Let $C/\mathbb{Z}/p^2$ and fix $b = (b_1, \dots, b_g)$ in $C(\mathbb{Z}/p^2)^g$.

Let $\begin{cases} D = D^+ - D^- \\ E = E^+ - E^- \end{cases}$ relative Cartier divisors of deg 0 on C.

Parameters on J are inherited from parameters on C_1 via the maps

$$C_b^g \twoheadrightarrow \mathrm{Sym}^g C_b \twoheadrightarrow \mathrm{Pic}^g C_b \xrightarrow{\sim} J_D$$

at each step $\twoheadrightarrow$ we check the map is étale at the basepoint

$\twoheadrightarrow$ is étale if $\bar{b}_i \neq \bar{b}_j$ for $i \neq j$ where $\bar{b}_i$ is the reduction mod p

$\twoheadrightarrow$ is étale if $h^0(C_{\mathbb{F}_p}, \bar{b}_1 + \dots + \bar{b}_g) = 1$

⊛ This is neither a "precision" nor necessary: one can compute to higher powers of p, and may need to: the point is we could work with $\mathcal{U}(\mathbb{Z}/p^2)_u$, etc.

Thus we have maps for $b=(b_1,\dots,b_g)$, $b'=(b_{g+1},\dots,b_{2g})$

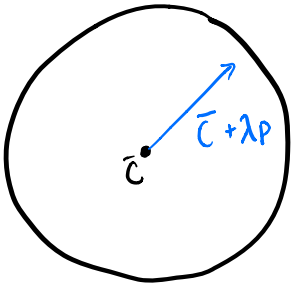
$$f_1: C^g \longrightarrow J$$
$$(c_1,\dots,c_g) \mapsto [\mathcal{O}_C(c_1+\dots+c_g-(b_1+\dots+b_g)+D)]$$

$$f_2: C^g \longrightarrow J$$
$$(c_1,\dots,c_g) \mapsto [\mathcal{O}_C(c_1+\dots+c_g-(b_{g+1}+\dots+b_{2g})+E)]$$

which are étale at the basepoints b, b'. So they induce isomorphisms

$$C^g(\mathbb{Z}/p^2)_b \xrightarrow{\sim} J(\mathbb{Z}/p^2)_D$$
$$C^g(\mathbb{Z}/p^2)_{b'} \xrightarrow{\sim} J(\mathbb{Z}/p^2)_E$$

For $c\in C(\mathbb{Z}/p^2)$, $C(\mathbb{Z}/p^2)_c = \{\bar{c}+\lambda p \mid \lambda\in\mathbb{F}_p\}$, are "points with a tangent direction"



$c_\lambda \in C(\mathbb{Z}/p^2)$

The parameter λ gives an isomorphism $\lambda: C(\mathbb{Z}/p^2)_c \to \mathbb{F}_p$.
For $c=\bar{b}_i$ can do this: so

$$\mathbb{F}_p^g \xrightarrow{\sim} C^g(\mathbb{Z}/p^2)_b \xrightarrow{\sim} J(\mathbb{Z}/p^2)_D$$
$$\lambda=(\lambda_1,\dots,\lambda_g) \mapsto (\underbrace{b_{1,\lambda_1}}_{\bar{b}_1+\lambda_1 p},\dots,b_{g,\lambda_g}) \mapsto \underbrace{D+(b_{1,\lambda_1}+\dots+b_{g,\lambda_g})-b_1+\dots+b_g}_{D_\lambda}$$

and similarly for f_2.

So $\mathcal{M}^X(\mathbb{Z}/p^2)_{(D,E)} = \bigcup_{(\lambda,\mu)\in(\mathbb{F}_p^g)^2} \mathcal{M}^X(D_\lambda, E_\mu)$. While this is not yet a parametrization of a residue disk of $\mathcal{M}^X$, we can see the beginnings, and why $\mathbb{Z}/p^2$ is enough!