Lecture 11: The non-abelian Chabauty method, I

We're now ready to set up the non-abelian Chabauty method. For this section, we drop down somewhat in generality and consider a smooth projective curve X over $k=\mathbb{Q}$ of genus ≥ 2. More generally, we consider a smooth hyperbolic curve Y over $\mathbb{Q}$. We write $Y=X\setminus D$ for X a smooth projective curve and $D\subset X$ a reduced divisor, and write g for the genus of X and r for the degree of D. We explicitly allow the possibility that $D=\emptyset$, i.e. that $Y=X$ is projective of genus ≥ 2.

For any two rational points $x,y\in Y(\mathbb{Q})$ (resp. $\mathbb{Q}_\ell$-rational points $x,y\in Y(\mathbb{Q}_\ell)$), we have the $\mathbb{Q}_p$-pro-unipotent étale torsor of paths

$$\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}};x,y) \quad \left(\text{resp. } \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell};x,y)\right),$$

where p is some auxiliary prime we fix once and for all. These are affine schemes over $\mathbb{Q}_p$, coming with composition maps $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}};y,z)\times\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}};x,y)\to\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}};x,$ etc. making them into a groupoid in affine $\mathbb{Q}_p$-schemes.

The natural action of $G_{\mathbb{Q}}$ on $Y_{\bar{\mathbb{Q}}}$ (resp. action of the decomposition group G_ℓ on $Y_{\bar{\mathbb{Q}}_\ell}$) induces an action on $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x, y)$ (resp. $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; x, y)$) for all x, y. We recall several facts we have proven about this setup.

Proposition:

1. When $x = y$, $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x)$ is a finitely generated pro-unipotent group over $\mathbb{Q}_p$, isomorphic to the $\mathbb{Q}_p$-Malčev completion of the discrete surface group

$$\Sigma_{g,r} = \left\langle a_1, \dots, a_g, b_1, \dots, b_g, c_1, \dots, c_r \;\middle|\; \prod_{i=1}^{g} [a_i, b_i] \cdot \prod_{j=1}^{r} c_j = 1 \right\rangle$$

1a. For all $x, y \in Y(\mathbb{Q})$ (resp. $x, y \in Y(\mathbb{Q}_\ell)$), we have that $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x, y) \neq \emptyset$ is non-empty (resp. $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; x, y) \neq \emptyset$ is non-empty). In fact, both schemes even have a $\mathbb{Q}_p$-point.

2. The action of $G_{\mathbb{Q}}$ on $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; x, y)$ (resp. G_ℓ on $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}_\ell}; x, y)$) is continuous (on $\mathbb{Q}_p$-points).

To state the next two properties, let us say that Y has <u>good reduction</u> at ℓ just when there exists a smooth proper $\mathbb{Z}_\ell$-scheme $\mathcal{X}_{\mathbb{Z}_\ell}$ and a horizontal divisor $\mathcal{D}_{\mathbb{Z}_\ell} \subset \mathcal{X}_{\mathbb{Z}_\ell}$, étale over $\mathbb{Z}_\ell$, such that $(X_{\mathbb{Q}_\ell}, D_{\mathbb{Q}_\ell})$ is isomorphic to the generic fibre of $(\mathcal{X}_{\mathbb{Z}_\ell}, \mathcal{D}_{\mathbb{Z}_\ell})$. (Such an $(\mathcal{X}_{\mathbb{Z}_\ell}, \mathcal{D}_{\mathbb{Z}_\ell})$ is unique up to unique isomorphism if we remember the isomorphism of the generic fibre with $(X_{\mathbb{Q}_\ell}, D_{\mathbb{Q}_\ell})$.) We write $\mathcal{Y}_{\mathbb{Z}_\ell} = \mathcal{X}_{\mathbb{Z}_\ell} \setminus \mathcal{D}_{\mathbb{Z}_\ell}$, so that $Y_{\mathbb{Q}_\ell}$ is the generic fibre of $\mathcal{Y}_{\mathbb{Z}_\ell}$.

<u>Proposition</u> (ct'd)

3. If $\ell \neq p$ is a prime of good reduction and if $x, y \in \mathcal{Y}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$ are ℓ-integral, then the action of G_ℓ on $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; x, y)$ is unramified.

(N.B. If $Y = X$ is projective, then $\mathcal{Y}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell) = \mathcal{X}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell) = X(\mathbb{Q}_\ell)$. So the action on $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}_\ell}; x, y)$ is unramified for all $x, y \in X(\mathbb{Q}_\ell)$.)

4. If $\ell = p$, then the action of G_p on $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_p}; x, y)$ is de Rham (meaning that $\mathbb{Q}_p[\![\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_p}; x, y)]\!]$ is a pro-de Rham representation) for all $x, y \in Y(\mathbb{Q}_p)$. If moreover p is a prime of good reduction, then $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_p}; x, y)$ is crystalline at p for all $x, y \in \mathcal{Y}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$.

(N.B. We haven't actually proved this yet.)

5. $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x)$ is mixed with negative weights: if $W_\bullet \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x)$ denotes the weight filtration constructed in Lecture 7, then

$$\frac{W_{-n}\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x)}{W_{-n-1}\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; x)}$$

is pure of weight $-n$ at all primes ℓ, for all $n \geq 1$. Moreover, it is a semisimple representation of $G_{\mathbb{Q}}$ for all $n \geq 1$. (We didn't mention this in Lecture 7, but it's a consequence of the Tate Conjecture for abelian varieties, as proven by Faltings.)

= descending central series with reversed indexing if $Y = X$.

Remark: j and j_ℓ are sometimes called non-abelian Kummer maps or higher Albanese maps in the literature.

Variant: Suppose that U is some $G_{\mathbb{Q}}$-equivariant quotient of $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)$, e.g. the quotient by W_{-n-1} for some n. Then we denote by j_U and $j_{\ell,U}$ the composite maps

$$Y(\mathbb{Q}) \xrightarrow{j} H^1(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p)) \to H^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p)$$

$$Y(\mathbb{Q}_\ell) \xrightarrow{j_\ell} H^1(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p)) \to H^1(G_\ell, U(\mathbb{Q}_p)$$

When $U = \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)/W_{-n-1}$, we often abbreviate j_U and $j_{\ell,U}$ to j_n and $j_{\ell,n}$.

Remark: We will always endow U with the natural filtration induced from the weight filtration on $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)$. This enjoys all of the usual properties: unramifiedness, de Rhamness, mixedness etc. The only thing which is not obvious here is why U is mixed: this is because $V_n = W_{-n}U/W_{-n-1}U$ is a quotient of the semisimple $W_{-n}\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)/W_{-n-1}$, so is a direct summa and so remains pure of weight $-n$. This is the only time

Lemma: Suppose that Y has good reduction at $\ell \neq p$ and that $b \in Y_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$ is $\mathbb{Z}_\ell$-integral. Then $j_\ell(x) = *$ for all $x \in Y_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$.

Proof: We know that the G_ℓ-action on $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b, x)$ is unramified. This means that the cohomology class $j_\ell(x) = [\xi]$ lies in $H^1_{nr}(G_\ell, \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b)(\mathbb{Q}_p)) = \{*\}$. □

The global Selmer scheme

Now let's explain how to attach a global Selmer scheme to this setup. We fix:

- a finite set S of primes
- a proper, flat, integral $\mathbb{Z}_S$-scheme $\mathcal{X}/\mathbb{Z}_S$ whose generic fibre is X. We let $\mathcal{D} \subset \mathcal{X}$ denote the closure of $D \subset X$, and set $\mathcal{Y} := \mathcal{X} \setminus \mathcal{D}$.

We also fix a choice of $G_{\mathbb{Q}}$-equivariant quotient U of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$.

3. Historically, several different definitions of the Selmer scheme have been used in the literature. In Minhyong Kim's original papers, he used the Selmer scheme

$$H^1_{f,S}(G_{\mathbb{Q}}, U)$$

and always assumed that $p \notin S$ and S contained all bad primes for (Y, b).

Later, in the paper "A non-abelian conjecture of Tate–Shafarevich type for hyperbolic curves" (BALAKRISHNAN–DAN-COHEN–KIM–WEW[illegible] they introduced the smaller Selmer scheme

$$Sel_U(Y/\mathbb{Z}_S)^{BDCKW}$$ (our notation)

associated to the Selmer structure

$$\mathcal{G}_\ell = \begin{cases} j_{\ell,U}(Y(\mathbb{Z}_\ell))^{Zar} & \text{if } \ell \notin S \\ [illegible] H^1(G_\ell, U) & \text{if } \ell \in S \end{cases}$$

where now $p \notin S$ is assumed to be [illegible] good for (Y, b).

The Selmer scheme we've defined above is from my paper with Netan DOGRA. We have containments

$$Sel_U(Y/\mathbb{Z}_S) \subseteq Sel_U(Y/\mathbb{Z}_S)^{BDCKW} \subseteq H^1_{f,S}(G_{\mathbb{Q}}, U)$$

where the first inclusion is an equality when $S=\emptyset$ (e.g. if $Y=X$ is projective).

This means that, of the three, $Sel_U(Y/\mathbb{Z}_S)$ will afford the strongest constraints on rational or S-integral points.

Localisation maps

For every prime ℓ (especially $\ell=p$), restriction to the decomposition group G_ℓ at ℓ provides a natural transformation

$$loc_\ell : H^1(G_{\mathbb{Q}}, U) \longrightarrow H^1(G_\ell, U)$$

of functors, which restricts then (by Voevodal) to a morphism

$$loc_\ell : Sel_U(Y/\mathbb{Z}_S) \longrightarrow H^1(G_\ell, U)$$

of affine $\mathbb{Q}_p$-schemes. We call loc_ℓ the localisation map.

The local and global pro-unipotent Kummer maps are compatible, in that they fit into a commuting square

$$\begin{array}{ccc} Y(\mathbb{Q}) & \longrightarrow & Y(\mathbb{Q}_\ell) \\ \downarrow j_U & & \downarrow j_{\ell,U} \\ H^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p)) & \xrightarrow{\mathrm{loc}_\ell} & H^1(G_\ell, U(\mathbb{Q}_p)). \end{array} \qquad (*)$$

Lemma: The image of $Y(\mathbb{Z}_S)$ under j_U is contained in the Selmer scheme

$$\mathrm{Sel}_U(Y/\mathbb{Z}_S).$$

Proof: For $x \in Y(\mathbb{Z}_S)$, the commutativity of $(*)$ shows that

$$\mathrm{loc}_\ell(j_U(x)) = j_{\ell,U}(x) \in \widetilde{S}_\ell$$

by definition of $\widetilde{S}_\ell$. So $j_U(x) \in \mathrm{Sel}_U(Y/\mathbb{Z}_S)(\mathbb{Q}_p)$

$\square$

This brings us to the main definition of the whole course.

Definition: Let $p \notin S$. The **Chabauty–Kim locus** associated to the quotient U is the subset

$$Y(\mathbb{Z}_p)_U \subseteq Y(\mathbb{Z}_p)$$

consisting of those points $x \in Y(\mathbb{Z}_p)$ for which $j_{p,U}(x)$ lies in the scheme-theoretic image of the localisation map

$$loc_p : Sel_U(Y/\mathbb{Z}_S) \longrightarrow H^1(G_p, U).$$

As usual for obstruction loci, the Chabauty-Kim locus contains the set of S-integral points.

Proposition: For $p \notin S$, we have

$$Y(\mathbb{Z}_S) \subseteq Y(\mathbb{Z}_p)_U.$$

Proof: If $x \in Y(\mathbb{Z}_S)$, then $j_{p,U}(x) = loc_p(j_U(x))$ lies in the image of the localisation map (as $j_U(x)$ lies in $Sel_U(Y/\mathbb{Z}_S)$.).

Remark: When $Y = X$ is projective, we usually write $X(\mathbb{Q}_p)_U$ instead of $Y(\mathbb{Z}_p)_U$. This contains $X(\mathbb{Q})$.

In order to say more, we need to specialize our setup further.

Assumptions: From now on, assume that $p \notin S$, that p is good for $\mathcal{Y}$, and that $b \in \mathcal{Y}(\mathbb{Z}_p)$ is p-integral.

The reason we make these assumptions is to get a good handle on the local Kummer map

$$j_{p,U} : \mathcal{Y}(\mathbb{Z}_p) \longrightarrow H^1(G_p, U(\mathbb{Q}_p)).$$

In the next part of the course, we will prove the following.

Theorem: Under the above assumptions, U is crystalline at p, and the Zariski-closure of ~~[illegible]~~ $j_{p,U}(\mathcal{Y}(\mathbb{Z}_p))$ is $H^1_f(G_p, U)$.

More strongly, if $x_0 \in \mathcal{Y}(\mathbb{F}_p)$ is a point in the mod-p special fibre and $\mathbb{D}_{x_0} =]x_0[\subset Y^{an}_{\mathbb{Q}_p}$ is the corresponding residue disc (the points reducing to x_0), then:

1. $j_{p,U}(\mathbb{D}_{x_0}(\mathbb{Q}_p))^{Zar} = H^1_f(G_p, U)$
2. the restriction of $j_{p,U}$ to $\mathbb{D}_{x_0}$ is $\mathbb{Q}_p$-analytic.

We can summarise the picture in the following Chabauty–Kim square.

$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \longhookrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\ \downarrow j_U & & \downarrow j_{p,U} \\ Sel_U(\mathcal{Y}/\mathbb{Z}_S)(\mathbb{Q}_p) & \xrightarrow{loc_p} & H^1_f(G_p, U(\mathbb{Q}_p)). \end{array}$$

The commutativity of this square gives us the main theorem of Chabauty–Kim theory, generalising Chabauty's criterion.

Theorem: (Chabauty–Kim criterion) Suppose that U is unipotent, and that the dimension inequality

$$(*) \quad \dim_{\mathbb{Q}_p} Sel_U(\mathcal{Y}/\mathbb{Z}_S) < \dim_{\mathbb{Q}_p} H^1_f(G_p, U)$$

holds. Then $\mathcal{Y}(\mathbb{Z}_p)_U$ is finite. In particular, $\mathcal{Y}(\mathbb{Z}_S) \subseteq \mathcal{Y}(\mathbb{Z}_p)_U$ is finite.

Proof: the dimension inequality implies that the localisation map $\mathrm{loc}_p: Sel_u(\mathcal{Y}/\mathbb{Z}_S) \to H^1_f(G_p, U)$ cannot be scheme-theoretically dense. So there is a non-zero $\alpha: H^1_f(G_p, U) \to \mathbb{A}^1_{\mathbb{Q}_p}$ which vanishes on the scheme-theoretic image of loc_p. We thus have the following picture

$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\ \downarrow j_u & & \downarrow j_{p,u} \\ Sel_u(\mathcal{Y}/\mathbb{Z}_S)(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U(\mathbb{Q}_p)) \xrightarrow{\alpha} \mathbb{Q}_p \\ & & \searrow \quad \vdots \quad \swarrow \\ & & 0 \end{array}$$

Consider the function

$$\alpha \circ j_{p,u}: \mathcal{Y}(\mathbb{Z}_p) \to \mathbb{Q}_p.$$

This satisfies the following properties:

1. $\alpha \circ j_{p,u}$ vanishes on $\mathcal{Y}(\mathbb{Z}_p)_u$ (by definition)
2. $\alpha \circ j_{p,u}$ is $\mathbb{Q}_p$-analytic on any residue disc (as the same is true of $j_{p,u}$ and α is algebraic).
3. $\alpha \circ j_{p,u}$ does not vanish uniformly on any residue disc (as the image of such a disc under $j_{p,u}$ is Zariski-dense in $H^1_f(G_p, U)$ and $\alpha \neq 0$).

Properties 2. + 3. ensure that $\alpha \circ j_{p,U}$ has only finitely many zeroes on each residue disc. Since $Y(\mathbb{Z}_p)$ is covered by finitely many residue discs (since $Y(\mathbb{F}_p)$ is finite, or by compactness), it follows that $\alpha \circ j_{p,U}$ has only finitely many zeroes on $Y(\mathbb{Z}_p)$. So $Y(\mathbb{Z}_p)_U$ is finite by 1. □

To actually use this criterion in practice, we need to control the dimensions of the global Selmer scheme $\mathrm{Sel}_U(Y/\mathbb{Z}_S)$ and the local Selmer scheme $H^1_f(G_p, U)$. The latter is quite easy: indeed we have already shown that

$$\dim_{\mathbb{Q}_p} H^1_f(G_p, U) = \sum_{n \geq 1} \dim_{\mathbb{Q}_p} H^1_f(G_p, V_n),$$

where $V_n = W_{-n}U / W_{-n-1}$, and the summands on the right are usually easy to compute. For the former, we have

$$\dim_{\mathbb{Q}_p} \mathrm{Sel}_U(Y/\mathbb{Z}_S) \leq \sum_{\ell \neq p} \dim_{\mathbb{Q}_p} \mathbb{G}_\ell + \sum_{n \geq 1} \dim_{\mathbb{Q}_p} H^1_f(G_{\mathbb{Q}}, V$$

The right-hand sum is usually quite subtle, especially the terms for $n \geq 3$, but the left-hand sum we can be completely explicit about.

Proposition: Let $\ell \neq p$. Then

i. The image of $Y(\mathbb{Z}_\ell)$ under the pro-unipotent Kummer map is finite.

ii. The Zariski-closure of the image of $Y(\mathbb{Q}_\ell)$ has dimension ≤ 1.

Before we get to the proof, we note that this proposition gives us a weaker but more user-friendly version of the main theorem.

Theorem: Suppose that

$$(**) \quad \#S + \sum_{n \geq 1} \dim_{\mathbb{Q}_p} H^1_f(G_{\mathbb{Q}}, V_n) < \sum_{n \geq 1} \dim_{\mathbb{Q}_p} H^1_f(G_p, V_n).$$

Then $Y(\mathbb{Z}_p)_n$ is finite.

Proof: According to the Proposition,

$$\dim_{\mathbb{Q}_p} \mathcal{G}_\ell = \begin{cases} 0 & \text{if } \ell \notin S \cup \{p\} \\ \leq 1 & \text{if } \ell \in S. \end{cases}$$

So $\dim_{\mathbb{Q}_p} Sel_n(Y/\mathbb{Z}_S) \leq \#S + \sum_{n \geq 1} \dim_{\mathbb{Q}_p} H^1_f(G_{\mathbb{Q}}, V_n)$

and hence $(**)$ implies inequality $(*)$. $\square$

To prove the proposition, we need a little analytic geometry. Let $\mathbb{C}_\ell$ denote the completion of $\overline{\mathbb{Q}}_\ell$, and let $Z_{\mathbb{C}_\ell}$ be a Berkovich analytic space over $\mathbb{C}_\ell$. In practice, we will only be interested in the case that $Z_{\mathbb{C}_\ell}$ is an open disc, or an open disc minus a single puncture. In the paper *Étale fundamental groups of non-archimedean analytic spaces*, de Jong defines what it means for a morphism $Z'_{\mathbb{C}_\ell} \to Z_{\mathbb{C}_\ell}$ of Berkovich spaces to be a finite étale covering. The category $F\acute{E}t(Z_{\mathbb{C}_\ell})$ of finite étale coverings comes with a fibre functor

$$\omega_x^{\acute{e}t} : F\acute{E}t(Z_{\mathbb{C}_\ell}) \longrightarrow \underline{Set}_{fin}$$

for each $\mathbb{C}_\ell$-point $x \in Z_{\mathbb{C}_\ell}(\mathbb{C}_\ell)$, and one can again define a profinite fundamental groupoid, called the <u>algebraic fundamental groupoid</u> $\pi_1^{alg}(Z_{\mathbb{C}_\ell}; -, -)$ by

$$\pi_1^{alg}(Z_{\mathbb{C}_\ell}; x, y) := Iso(\omega_x^{\acute{e}t}, \omega_y^{\acute{e}t}).$$

This fundamental groupoid is connected when $Z_{\mathbb{C}_\ell} \neq 3$, see [Theorem 2.9].

Lemma:

1. Suppose that $Z = \mathbb{D}_{\mathbb{Q}_\ell}$ is the open disc of radius 1. Then $\pi_1^{alg}(\mathbb{D}_{\mathbb{Q}_\ell}; x)^{(\ell')} = 1$.

2. Suppose that $Z = \mathbb{D}^\times_{\mathbb{Q}_\ell}$ is the open disc of radius 1 minus the origin. Then

$$\pi_1^{alg}(\mathbb{D}^\times_{\mathbb{Q}_\ell}; x)^{(\ell')} \cong \hat{\mathbb{Z}}(1)^{(\ell')}.$$

Proof: As in the theory of profinite étale fundamental groups of schemes, there is an equivalence of categories

$$F\acute{E}t(Z_{\mathbb{Q}_\ell}) \simeq \{\text{finite continuous } \pi_1^{alg}(Z_{\mathbb{Q}_\ell}; x)\text{-sets}\}$$

(for $Z_{\mathbb{Q}_\ell}$ connected). On the right-hand side one has the objects $\pi_1^{alg}(Z_{\mathbb{Q}_\ell}; x)/N$ for N an open normal subgroup; on the left-hand side these correspond to the Galois coverings: coverings $Z'_{\mathbb{Q}_\ell} \to Z_{\mathbb{Q}_\ell}$ with $Z'_{\mathbb{Q}_\ell}$ connected for which $Aut_{Z_{\mathbb{Q}_\ell}}(Z'_{\mathbb{Q}_\ell})$ acts transitively on the fibre over x (or any other point). If N is the normal subgroup corresponding to $Z'_{\mathbb{Q}_\ell} \to Z_{\mathbb{Q}_\ell}$ then

$$\pi_1^{alg}(Z_{\mathbb{Q}_\ell}; x)/N \cong Aut_{Z_{\mathbb{Q}_\ell}}(Z'_{\mathbb{Q}_\ell})^{op}.$$

In particular, the open normal subgroups N such that $\pi_1^{alg}(Z_{\mathbb{Q}_\ell};x)/N$ is a prime-to-ℓ group correspond to Galois coverings $Z'_{\mathbb{Q}_\ell} \longrightarrow Z_{\mathbb{Q}_\ell}$ of degree prime to ℓ.

Now in the case $Z_{\mathbb{Q}_\ell} = \mathring{\mathbb{D}}_{\mathbb{Q}_\ell}$, a result of Berkovich gives that the only Galois covering of $\mathring{\mathbb{D}}_{\mathbb{Q}_\ell}$ of degree prime to ℓ is the identity map $\mathring{\mathbb{D}}_{\mathbb{Q}_\ell} \longrightarrow \mathring{\mathbb{D}}_{\mathbb{Q}_\ell}$. So $\pi_1^{alg}(\mathring{\mathbb{D}}_{\mathbb{Q}_\ell};x)$ has only one open normal subgroup of index prime to ℓ, namely $\pi_1^{alg}(\mathring{\mathbb{D}}_{\mathbb{Q}_\ell};x)$ itself. So

$$\pi_1^{alg}(\mathring{\mathbb{D}}_{\mathbb{Q}_\ell};x)^{(\ell')} = 1.$$

In the case $Z_{\mathbb{Q}_\ell} = \mathring{\mathbb{D}}^\times_{\mathbb{Q}_\ell}$, for a positive integer q prime to ℓ, let $[q]: \mathring{\mathbb{D}}^\times_{\mathbb{Q}_\ell} \longrightarrow \mathring{\mathbb{D}}^\times_{\mathbb{Q}_\ell}$ denote the q^{th} power map. This is a Galois covering with group μ_q. Another result of Berkovich shows that these are the only Galois coverings of $\mathring{\mathbb{D}}^\times_{\mathbb{Q}_\ell}$ of degree prime to ℓ. So $\pi_1^{alg}(\mathring{\mathbb{D}}^\times_{\mathbb{Q}_\ell};x)$ has exactly one quotient of each degree q prime to ℓ, namely μ_q. So

$$\pi_1^{alg}(\mathring{\mathbb{D}}^\times_{\mathbb{Q}_\ell};x)^{(\ell')} \cong \varprojlim_q \mu_q = \hat{\mathbb{Z}}(1)^{(\ell')}$$

Remark: Explicitly, the isomorphism

$$\pi_1^{alg}(\mathbb{D}_{q_i}^{\times}; x)^{(\ell')} \xrightarrow{\sim} \hat{\mathbb{Z}}(1)^{(\ell')}$$

is given as follows. For q prime to ℓ, ~~the action of~~ an element $\gamma \in \pi_1^{alg}(\mathbb{D}_{q_i}^{\times}; x)$ acts on the fibres of the covering $[q]: \mathbb{D}_{q_i}^{\times} \longrightarrow \mathbb{D}_{q_i}^{\times}$ — i.e. the set of q^{th} roots of x — by $x^{1/q} \longmapsto \chi_q(\gamma) x^{1/q}$ for some $\chi_q(\gamma) \in \mu_q$. This defines a character

$$\chi_q : \pi_1^{alg}(\mathbb{D}_{q_i}^{\times}; x)^{(\ell')} \longrightarrow \mu_q$$

and the above isomorphism is the inverse limit of these characters.

Now let's prove part (i) of the proposition. Specifically, we will prove

Lemma: let $\mathbb{D} \subset Y^{an}$ be an analytic disc defined over $\mathbb{Q}_\ell$. Then $j_\ell(x) = j_\ell(y)$ for all $x, y \in \mathbb{D}(\mathbb{Q}_\ell) \subset Y(\mathbb{Q}_\ell)$.

Since $Y(\mathbb{Z}_\ell)$ can be covered by the $\mathbb{Q}_\ell$-points of finitely many discs by compactness, the lemma implies that $j_\ell(Y(\mathbb{Z}_\ell))$ is finite as desired.

To prove the lemma, there is a functor

$$F\acute{E}t(Y_{\bar{\mathbb{Q}}_\ell}) \longrightarrow F\acute{E}t(\mathbb{D}_{\mathbb{C}_\ell})$$

given by sending a finite étale covering $Y' \longrightarrow Y_{\bar{\mathbb{Q}}_\ell}$ to $Y'^{an}_{\mathbb{C}_\ell}|_{\mathbb{D}_{\mathbb{C}_\ell}}$. This induces a map

$$\pi_1^{alg}(\mathbb{D}_{\mathbb{C}_\ell}; x, y) \longrightarrow \pi_1^{\acute{e}t}(Y_{\bar{\mathbb{Q}}_\ell}; x, y) \quad \circledast$$

The map $\circledast$ automatically factors through the maximal pro-prime-to-ℓ quotient, and moreover is equivariant for the natural action of G_ℓ on both sides (induced from the actions on $\bar{\mathbb{Q}}_\ell$ and $\mathbb{C}_\ell$). Since $\pi_1^{alg}(\mathbb{D}_{\mathbb{C}_\ell}; x, y)^{(\ell')}$ is a single point with trivial G_ℓ-action, this implies that

$$\left[\pi_1^{\acute{e}t}(Y_{\bar{\mathbb{Q}}_\ell}; x, y)^{(\ell')}\right]^{G_\ell} \neq \emptyset,$$

in words, that there is a G_ℓ-invariant pro-prime-to-ℓ path from x to y. In particular, we have

$$\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; x, y)^{G_\ell} \neq \emptyset \quad \text{since } p \neq \ell;$$

more strongly we have $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; x, y)(\mathbb{Q}_p)^{G_\ell} \neq \emptyset$.

We now compare the image of x and y under the ~~non-ab~~ unipotent Kummer map j_ℓ. Pick any path $\gamma_{b,x} \in \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; b, x)(\mathbb{Q}_p)$ and let

$$\gamma_{b,y} = \gamma_{x,y} \cdot \gamma_{b,x} \in \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; b, y)(\mathbb{Q}_p)$$

where $\gamma_{x,y} \in \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}_\ell}; x, y)(\mathbb{Q}_p)$ is G_ℓ-invariant.

Then $j_\ell(y)$ is the class of the cocycle

$$\sigma \longmapsto \gamma_{b,y}^{-1}\, \sigma(\gamma_{b,y}) = \gamma_{b,x}^{-1} \cdot \gamma_{x,y}^{-1} \cdot \sigma(\gamma_{x,y}) \cdot \sigma(\gamma_{b,x})$$

$$= \gamma_{b,x}^{-1} \cdot \sigma(\gamma_{b,x}),$$

which is also the cocycle representing $j_\ell(x)$. So $j_\ell(x) = j_\ell(y)$ and we have proved the lemma. □

The second part of the proposition follows by a more elaborate version of the same argument.

Lemma: Let $\mathbb{D}^\times \subset Y^{an}$ be a punctured analytic disc defined over $\mathbb{Q}_\ell$. Then the image of $\mathbb{D}^\times(\mathbb{Q}_\ell)$ under the unipotent Kummer map j_ℓ is contained in a subscheme of $H^1(G_\ell, U)$ of dimension ≤ 1.

Proof To simplify the notation, we assume that our chosen basepoint b lies in $\mathbb{D}^\times$. Again, pulling back and analytifying coverings defines morphisms

$$\pi_1^{alg}(\mathbb{D}^\times_{\mathbb{Q}_\ell}; b)^{(\ell')} \longrightarrow \pi_1^{\acute{e}t}(\mathbb{D}, Y_{\bar{\mathbb{Q}}_\ell}; b)^{(\ell')}$$

and

$$\pi_1^{alg}(\mathbb{D}^\times_{\mathbb{Q}_\ell}; b, y)^{(\ell')} \longrightarrow \pi_1^{\acute{e}t}(Y_{\bar{\mathbb{Q}}_\ell}; b, y)^{(\ell')}$$

for all $y \in \mathbb{D}^\times(\mathbb{Q}_\ell)$. These morphisms are compatible with composition and are equivariant for the natural actions of G_ℓ.

The first of the above maps induces a map

$$\mathbb{Q}_p(1) \longrightarrow \pi_1^{\Phi_p}(Y_{\bar{\mathbb{Q}}_\ell}; b)$$

and hence a map

$$H^1(G_{\mathbb{Q}_\ell}, \mathbb{Q}_p(1)) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b)) \quad (\dagger).$$

We will show that $j_\ell(\mathbb{D}^\times(\mathbb{Q}_\ell))$ is contained inside the image of $(\dagger)$ — this completes the proof of the lemma since $H^1(G_{\mathbb{Q}_\ell}, \mathbb{Q}_p(1)) \cong \mathbb{Q}_p$ is one-dimensional.

But this is now straightforward: for $y \in \mathbb{D}^\times(\mathbb{Q}_\ell)$, let $\gamma_{b,y} \in \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b, y)(\mathbb{Q}_p)$ be a path which lies in the image of $\pi_1^{alg}(\mathbb{D}^\times_{\overline{\mathbb{Q}}_\ell}; b, y)^{(\ell')}$. Then the cocycle

$$\sigma \longmapsto \gamma_{b,y}^{-1} \cdot \sigma(\gamma_{b,y})$$

representing $j_\ell(y)$ takes values in $\mathbb{Q}_\ell(1)$, and so $j_\ell(y) \in \mathrm{im}((\dagger))$ as claimed. □

This concludes the proof of the Proposition.

Pro-unipotent Kummer maps

Let's now fix a basepoint $b \in Y(\mathbb{Q})$. For any rational point $x \in Y(\mathbb{Q})$, we may choose a path

$$\gamma \in \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b, x)(\mathbb{Q}_p)$$

from b to x. For $\sigma \in G_{\mathbb{Q}}$, $\sigma(\gamma)$ is also a path from b to x, so we may form the element

$$\xi(\sigma) := \gamma^{-1}\sigma(\gamma) \in \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p).$$

The function $\xi : G_{\mathbb{Q}} \longrightarrow \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p)$ this defines is a continuous 1-cocycle, and its class in $H^1(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p))$ is independent of the choice of path γ.

Definition: The map

$$\begin{aligned} j : Y(\mathbb{Q}) &\longrightarrow H^1(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p)) \\ x &\longmapsto [\xi] \end{aligned}$$

is called the (global) **pro-unipotent Kummer map**.

Exactly the same construction defines a local pro-unipotent Kummer map

$$j_\ell : Y(\mathbb{Q}_\ell) \longrightarrow H^1(G_\ell, \pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)(\mathbb{Q}_p))$$

for all primes ℓ.

Examples:

Let us now illustrate how to use the Chabauty-Kim criterion by giving three examples of finiteness results proved using this method.

Siegel's Theorem

First, we indicate how to use the criterion to re-prove a finiteness theorem due to Siegel.

Theorem (Siegel) Let S be a finite set of prime numbers. Then there are only finitely many triples (a,b,c) of coprime integers, each only divisible by primes in S, such that

$$a + b = c.$$

(E.g. if $S = \{2,3\}$, then the only solutions, up to signed permutation of (a,b,c), are

$$1+1=2\,, \quad 1+2=3\,, \quad 1+3=4\,, \quad 1+8=9\,.)$$

Put another way, Siegel's Theorem asserts that there are only finitely many solutions to the equation

$$x + y = 1 \qquad \text{for } x, y \in \mathbb{Z}_S^\times$$

(take $x = \frac{a}{c}$, $y = \frac{b}{c}$).

Now an element $x \in \mathbb{Z}_S^\times$ such that $1-x \in \mathbb{Z}_S^\times$ also is the same thing as a $\mathbb{Z}_S$-integral point on

$$Y = \mathbb{P}^1_{\mathbb{Z}} \setminus \{0,1,\infty\} = \operatorname{Spec} \mathbb{Z}\left[t, \frac{1}{t(1-t)}\right].$$

So Siegel's Theorem is equivalent to saying that

$Y(\mathbb{Z}_S)$ is finite for all S — it is in this guise that we shall prove the result.

Let $Y = Y_{\mathbb{Q}} = \mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\}$ denote the generic fibre. So $Y(\mathbb{C}) = \mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}$ is homeomorphic to a sphere with three points removed, which means that the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $Y_{\bar{\mathbb{Q}}}$ (at your favourite basepoint) is pro-unipotent free on two generators. We can even be explicit about the Galois action on the graded pieces.

Proposition: Let U denote the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $Y_{\bar{\mathbb{Q}}}$, and

$$V_n := \operatorname{gr}^W_{-n} U$$

as usual. Then $V_n = 0$ if n is odd, and otherwise we have $V_{2n} = \mathbb{Q}_p(n)^{r_n}$ for some positive integer r_n.

Proof: Since the completion $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ of $Y_{\bar{\mathbb{Q}}}$ has trivial fundamental group, we know that

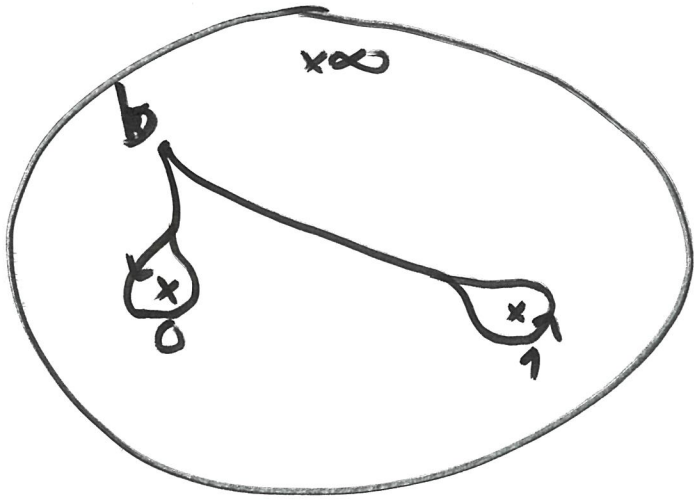
$$W_{1-2n}U = W_{-2n}U = \Gamma^n U$$

for all $n \geq 1$, where $\Gamma^\bullet U$ is the descending central series so $V_n = 0$ for odd n.

Now $V_2 = U^{ab}$ is the abelianisation of U. We can describe this geometrically. Let

$$f: Y \longrightarrow \mathbb{G}^2_{m,\mathbb{Q}}$$

be the map $t \longmapsto (t, 1-t)$. I claim that the induced map on fundamental groups is the abelianisation of U. On the level of topological fundamental groups, this is easy to see: $\pi_1(Y(\mathbb{C}); x)^{\wedge F_2}$ is freely generated by the classes of two loops



and these two loops are taken to
$(1,0)$ and $(0,1)$ $\in \mathbb{Z}^2 = \pi_1((\mathbb{G}_m^*)^2; f(b))$

Since abelianisation commutes with Malčev completion, it follows that the map

$$f_*: U \longrightarrow \pi_1^{\mathbb{Q}_p}(\mathbb{G}_{m,\mathbb{Q}}^2; f(b)) \cong \mathbb{Q}_p(1)^2$$

is the abelianisation map for U. Since it is $G_{\mathbb{Q}}$-equivariant this gives that $V_2 \cong \mathbb{Q}_p(1)^2$ as claimed.

For $n \geq 2$, we have the iterated commutator map

$$V_2^{\otimes n} \longrightarrow\!\!\!\!\rightarrow V_{2n}$$

which is surjective, so $G_{\mathbb{Q}}$ acts on V_{2n} via the n^{th} power of the cyclotomic character, as claimed. □

Remark: The r_n are the dimensions of the graded pieces of the descending central series on the free Lie algebra on two generators, and these are known to be given by the values of the Moiregan necklace polynomial, i.e.

$$r_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d$$

where μ is the Möbius function.

To compute the local and global Selmer dimensions appearing in the Chabauty–Kim criterion, we use the following calculation.

Lemma: For $n \geq 1$, we have

$$\dim_{\mathbb{Q}_p} H^1_f(G_p, \mathbb{Q}_p(n)) = 1$$

$$\dim_{\mathbb{Q}_p} H^1_f(G_p, \mathbb{Q}_p(n)) = \begin{cases} 0 & \text{if } n=1 \text{ or } n \text{ even} \\ 1 & \text{if } n \geq 3 \text{ odd.} \end{cases}$$

Proof: For the local dimensions,

$$D_{dR}(\mathbb{Q}_p(n)) = \mathbb{Q}_p$$

is one-dimensional, with Hodge filtration given by

$$F^i D_{dR}(\mathbb{Q}_p(n)) = \begin{cases} \mathbb{Q}_p & i \leq -n \\ 0 & i > -n. \end{cases}$$

In our case, since $n \geq 1$, we have

$$D^+_{dR}(\mathbb{Q}_p(n)) = F^0 D_{dR}(\mathbb{Q}_p(n)) = 0.$$

So $\dim H^1_f(G_p, \mathbb{Q}_p(n)) = \dim D_{dR}(\mathbb{Q}_p(n)) - \dim D^+_{dR}(\mathbb{Q}_p(n))$

$$= 1 - 0 = 1.$$

For the global dimensions, these are much harder, and were proven by Soulé for p odd and Shiriti for $p=2$ (Sharifi's work is unpublished).

So we omit the proof, save to remark that the case $n=1$ follows from Kummer theory. □.

Now let's try to apply the Chabauty–Kim criterion to the quotient $U_{2N} = U/W_{-2N-1}U$ for some (large N). On the local side, we have

$$\sum_{n=1}^{N} \dim_{\mathbb{Q}_p} H^1_f(G_p, V_{2n}) = \sum_{n=1}^{N} \dim H^1_f(G_p, \mathbb{Q}_p(n)^{\oplus r_n})$$
$$= \sum_{n=1}^{N} r_n,$$

while on the global side, we have

$$\sum_{n=1}^{N} \dim H^1_f(G_{\mathbb{Q}}, V_{2n}) = \sum_{n=1}^{N} \dim H^1_f(G_{\mathbb{Q}}, \mathbb{Q}_p(n)^{\oplus r_n})$$
$$= \sum_{\substack{3 \le n \le N \\ \text{odd.}}} r_n$$

Now since the r_n are all positive integers, we have that

$$\#S + \sum_{\substack{3 \le n \le N \\ \text{odd}}} r_n < \sum_{1 \le n \le N} r_n$$

for N sufficiently large (for fixed S). So the Chabauty–Kim criterion for $N \gg 0$ shows finiteness of $Y(\mathbb{Z}_S)$, as claimed. □

Quadratic Chabauty

The next example we will discuss is that of quadratic Chabauty, which is concerned with controlling rational or integral points on curves using the weight ≥ -2 part of the fundamental group.

To state the result, recall that the Néron–Severi group $NS(X)$ of a variety X over a field k is the group of divisors modulo algebraic equivalence.

So $$NS(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$$

The theorem of the base says that $NS(X)$ is finitely generated.

Example: If X is a smooth projective curve, then $NS(X) \cong \mathbb{Z}$ via the degree map.

Example: If $X = A$ is principally polarised abelian variety, with polarisation $\lambda: A \xrightarrow{\sim} \hat{A}$. Then there is an involution of $\mathrm{End}(A)$, called the Rosati involution, given by $\psi \longmapsto \lambda^{-1} \circ \hat{\psi} \circ \lambda$

$\psi \in \mathrm{End}(A)$

If we write $\mathrm{End}(A)^+$ for the subspace fixed by the Rosati involution, then there is an isomorphism

$$\mathbb{Q} \underset{\mathbb{Z}}{\otimes} NS(A) \cong \mathbb{Q} \underset{\mathbb{Z}}{\otimes} \mathrm{End}(A)^+. \quad (*)$$

Explicitly, if $D \subseteq A$ is a divisor, then D determines a morphism $\lambda_D : A \longrightarrow \hat{A}$ by

$$\lambda_D(x) = [\tau_x^* D - D]$$

↑ translation by x.

The map $\mathrm{Div}(A) \longrightarrow \mathrm{End}(A)$ given by $D \longmapsto \lambda^{-1}\lambda_D$ induces the isomorphism $(*)$.

⚠ Warning: As for Picard groups, there is also a Néron-Severi group-scheme $\underline{NS}(X)$, defined as the quotient $\underline{\mathrm{Pic}}(X)/\underline{\mathrm{Pic}}^\circ(X)$ where $\underline{\mathrm{Pic}}(X)$ is the Picard scheme of X. $\underline{NS}(X)$ is a discrete group-scheme over k, but it is not generally true that

$$NS(X) = \underline{NS}(X)(k)$$

in general. Instead, there is an inclusion

$$NS(X) \subseteq \underline{NS}(X)(k)$$

whose cokernel is torsion.

The (k-rational) Picard number $\rho_k(X)$ is by definition the rank of the group $NS(X)$.

Theorem: (Quadratic Chabauty) Let $X/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 2$, with Jacobian J. Suppose that

$$\mathrm{rk}(J(\mathbb{Q})) < g + \rho_{\mathbb{Q}}(J) - 1. \qquad (**)$$

Then $X(\mathbb{Q})$ is finite.

Remark: We always have $\rho_{\mathbb{Q}}(J) \geq 1$, so $(**)$ is always a weaker condition than the Chabauty condition

$\mathrm{rk}(J(\mathbb{Q})) < g$. So Quadratic Chabauty can be applied in more cases.

—

Let's now discuss the proof of quadratic Chabauty. For this, we want to identify a relevant quotient of the fundamental group. We will do this via a careful study of the fundamental groups of $\mathbb{G}_m$-torsors over abelian varieties.

Proposition: Let A be an abelian variety over a characteristic 0 field, let L be a line bundle over A, and let $L^\times$ be the associated $\mathbb{G}_m$-torsor, i.e. the complement of the zero-section in the total space of A. Let $\tilde{O} \in L^\times(K)$ be any preimage of $O \in A(K)$. Then the maps

$$\mathbb{G}_m \hookrightarrow L^\times \twoheadrightarrow A$$

induce a G_K-equivariant central extension

$$\circledast \quad 1 \to \underbrace{\pi_1^{\mathbb{Q}_p}(\mathbb{G}_{m,\bar{K}}; 1)}_{\| \; \mathbb{Q}_p(1)} \to \pi_1^{\mathbb{Q}_p}(L^\times_{\bar{K}}; \tilde{O}) \to \underbrace{\pi_1^{\mathbb{Q}_p}(A_{\bar{K}}; O)}_{\| \; V_p A} \to 1$$

on étale fundamental groups. Moreover, the commutator pairing in $\circledast$ is equal to

$$\bullet \quad c_1^{\text{ét}}(L) \in H^2_{\text{ét}}(A_{\bar{K}}; \mathbb{Q}_p)(1) = \left(\textstyle\bigwedge^2 H^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Q}_p)\right)(1)$$

$$= \mathrm{Hom}\left(\textstyle\bigwedge^2 V_p A, \mathbb{Q}_p(1)\right)$$

where $c_1^{\text{ét}}(L)$ is the first étale Chern class.

Proof: We'll prove the result by comparing with Betti fundamental groups. That is, after embedding K inside $\mathbb{C}$ (and maybe using a Lefschetz argument), it suffices to show that for every A and L defined over $\mathbb{C}$, the maps

$$G_m \longrightarrow L^\times_* \longrightarrow A$$

induce a central extension

$$(*)\quad 1 \longrightarrow \pi_1(\mathbb{C}^\times; 1) \longrightarrow \pi_1(L^\times(\mathbb{C}); \check{0}) \longrightarrow \pi_1(A(\mathbb{C}); 0) \longrightarrow 1$$

$$\pi_1(\mathbb{C}^\times; 1) = \mathbb{Z}(1) = 2\pi i\mathbb{Z} \qquad \pi_1(A(\mathbb{C}); 0) = H_1(A(\mathbb{C}), \mathbb{Z})$$

on fundamental groups, whose commutator pairing is the first Chern class $c_1(\mathcal{L}) \in H^2(A(\mathbb{C}), \mathbb{Z})(1)$

$$= \mathrm{Hom}(\Lambda^2 H_1(A(\mathbb{C}), \mathbb{Z}), \mathbb{Z}(1))$$

The first part is straightforward: since

$$\mathbb{C}^\times \longrightarrow L^\times(\mathbb{C}) \longrightarrow A(\mathbb{C})$$

is a fibre bundle, we have the homotopy exact sequence

$$\pi_2(A(\mathbb{C}); 0) \to \pi_1(\mathbb{C}^\times; 1) \to \pi_1(L^\times(\mathbb{C}); \check{0}) \to \pi_1(A(\mathbb{C}); 0) \to \pi_0(\mathbb{C}^\times; 1)$$

$$= 1 \qquad\qquad = 1$$

and so $(*)$ is exact.

Moreover, the action of $\pi_1(A(\mathcal{L});0)$ on $\pi_1(\mathbb{C}^\times;1)$ by conjugation in the extension $\oplus$ is identified with the monodromy action on $H_1(\mathbb{C}^\times,\mathbb{Z})$ coming from the locally trivial fibration $L^\times(\mathcal{L})\to A(\mathcal{L})$. Since $L^\times(\mathcal{L})$ is an <u>oriented</u> $\mathbb{C}^\times$-bundle, this monodromy action is trivial, and so $\oplus$ is a central extension.

It remains to prove the assertion regarding Chern classes, which we will prove via a more explicit calculation (which also re-proves the first part).

Let us write $A(\mathcal{L}) = V/\Lambda$ where V is a complex vector space of dimension $g = \dim A$ and Λ is a lattice of rank $2g$ in V. So we can identify $\Lambda = \pi_1(A;0)$ canonically.

The APPELL-HUMBERT Theorem gives us a complete description of the $\mathbb{C}^\times$-torsors over $A(\mathcal{L})$ (in the complex analytic category).

Let $H(-,-)$ be a Hermitian form on V and $\alpha : \Lambda \longrightarrow U(1)$ (the unit circle) be a map such that:

- $E(-,-) := \operatorname{Im} H(-,-)$ is a $\mathbb{Z}$-valued antisymmetric pairing on Λ; and
- $\alpha(u_1+u_2) = e^{\pi i E(u_1,u_2)} \cdot \alpha(u_1) \cdot \alpha(u_2)$.

There is then a right action of Λ on $\mathbb{C}^\times \times V$ given by

$$(\lambda, v) \cdot u := (\alpha(u) \cdot e^{\pi H(v,u) + \frac{1}{2}\pi H(u,u)} \cdot \lambda, v+u),$$

and the quotient $\mathbb{C}^\times \times V / \Lambda$ is a $\mathbb{C}^\times$-bundle on $A(\Gamma) = V/\Lambda$. The Appell-Humbert Theorem says that every $\mathbb{C}^\times$-bundle arises in this way, for a unique H and α satisfying the above conditions. Moreover, $E \in \operatorname{Hom}(\Lambda^2\Lambda, \mathbb{Z}(1)) = H^2(A(\Gamma), \mathbb{Z}(1))$ is the Chern class of L.

Now given such an H and α, let Π be the set

$$\Pi = \{ (\gamma, u) \in i\mathbb{R} \times \Lambda : e^\gamma = \alpha(u) \}.$$

There is a natural group law on Π given by

$$(\gamma_1, u_1) \cdot (\gamma_2, u_2) := (\gamma_1 + \gamma_2 + \pi i E(u_1, u_2), u_1 + u_2),$$

making Π into a central extension of Λ by $\mathbb{Z}(1)$. There is a natural right action of Π on $\mathbb{C}\times V$ given by

$$(\tilde{\lambda}, v)\cdot(\gamma, u) = (\gamma + \pi H(v,u) + \tfrac{1}{2}\pi H(u,u) + \tilde{\lambda}, v+u),$$

and the quotient is (quotienting out first by $\mathbb{Z}(1)$ using $\mathbb{C}/\mathbb{Z}(1) = \mathbb{C}^\times$)

$$\mathbb{C}\times V/\Pi = \mathbb{C}^\times \times V/\Lambda = L^\times(\mathbb{C}).$$

Since $\mathbb{C}\times V$ is simply connected, this shows that $\pi_1(L^\times(\mathbb{C}); \tilde{0}) \cong \Pi$. It is easy to check that this identification is compatible with the structures as central extensions of Λ by $\mathbb{Z}(1)$. So the commutator pairing in $\pi_1(L^\times(\mathbb{C}); \tilde{0})$ is equal to the commutator pairing in Π, which by direct calculation is $2\pi i E(-,-)$. We know that this pairing is the one corresponding to $c_1(L)$, so we are done. $\square$

Now we return to the setting of quadratic Chabauty: $X/\mathbb{Q}$ is a smooth projective curve with Jacobian J such that

$$rk(J(\mathbb{Q})) < g + \rho_{\mathbb{Q}}(J) - 1.$$

We suppose moreover that $X(\mathbb{Q}) \neq \emptyset$, otherwise there is nothing to prove. The Abel-Jacobi embedding $X \hookrightarrow J$ induces on pullback an isomorphism $Pic^0(J) \xrightarrow{\sim} Pic^0(X)$, and so ~~induces~~ there is an isomorphism

$$\ker(NS(J) \to \underset{\rotatebox{90}{$=$}}{\mathbb{Z}} NS(X)) \cong \ker(Pic(J) \to Pic(X)) =: \mathcal{K}.$$

The group $\mathcal{K}$ is a ~~lattice~~ free abelian group of rank $\rho_{\mathbb{Q}}(J) - 1$ (since the map $NS(J) \to NS(X)$ is non-zero, as ample ~~divi~~ line bundles pull back to ample line bundles).

Suppose we are given a non-zero element of $\mathcal{K}$, i.e. a line bundle L on J s.t. $L|_X = \mathcal{O}_X$ is trivial. If $L^\times$ is the corresponding $\mathbb{G}_m$-torsor, then the Abel-Jacobi embedding lifts to an embedding

$\widetilde{AJ}: X \hookrightarrow L^\times$.

In particular, after choosing the point $\tilde{O} \in L^\times(\mathbb{Q})$ appropriately, there is an induced map

$$\widetilde{AJ}_* : \pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; b) \longrightarrow \pi_1^{\mathbb{Q}_p}(L^\times_{\bar{\mathbb{Q}}}; \tilde{O})$$

on fundamental groups.

Claim: $\widetilde{AJ}_*$ is surjective.

Proof: Since $[L] \notin \mathrm{Pic}^0(X)$, its Chern class $c_1^{\text{ét}}(L)$ is non-zero, so the commutator pairing

$$\wedge^2 V_p X \longrightarrow \mathbb{Q}_p(1)$$ coming from $\pi_1^{\mathbb{Q}_p}(L^\times_{\bar{\mathbb{Q}}}; \tilde{O})$

is surjective. This, combined with the fact that the composite map

$$\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; b) \longrightarrow \pi_1^{\mathbb{Q}_p}(L^\times_{\bar{\mathbb{Q}}}; 0) \longrightarrow V_p J$$

is surjective, implies that $\widetilde{AJ}_*$ is surjective. ✓claim

Since $\widetilde{AJ}_*$ is surjective, it determines a $G_{\mathbb{Q}}$-equivariant quotient of $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; b)$ which is a central extension of $V_p J$ by $\mathbb{Q}_p(1)$.

More generally, let $L_1, \ldots, L_{p-1}$ be independent elements of $\mathcal{K}$, for $p = p_{\mathbb{Q}}(J)$. If we write

$$M = L_1 \underset{J}{\times} L_2 \underset{J}{\times} \cdots \underset{J}{\times} L_{p-1}$$

for the common fibre product, then M is a $\mathbb{G}_m^{p-1}$-torsor over J, and its fundamental group is a central extension of $V_p J$ by $\mathbb{Q}_p(1)^{p-1}$ in which the commutator pairings is given by the Chern classes $c_1^{\text{ét}}(L_1), \ldots, c_1^{\text{ét}}(L_{p-1})$. The lifted Abel–Jacobi embeddings lift to a common embedding $X \hookrightarrow M$, whose induced map on fundamental groups is surjective since the $c_1^{\text{ét}}(L_i)$ are linearly independent. Thus we have shown:

Lemma: there is a quotient U of $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; b)$ which is a central extension of $V_p J$ by $\mathbb{Q}_p(1)^{p-1}$!

Let's feed this Lemma into the Chabauty–Kim criterion. We've discussed the Bloch–Kato Selmer groups for $\mathbb{Q}_p(1)$ already. For $V_p J$ we have

Lemma: Let $A/\mathbb{Q}$ be an abelian variety of dimension g. Then:

- $\dim H^1_f(G_p, V_pA) = g$
- if $Ш(A/\mathbb{Q})[p^\infty]$ is finite, then $\dim H^1_f(G_{\mathbb{Q}}, V_pA) = rk(A(\mathbb{Q}))$.

Proof: For the first part, $V_pA = H^1_{\text{ét}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$, so the comparison isomorphism between étale and de Rham cohomology shows that

$$D_{dR}(V_pA) = H^1_{dR}(A_{\mathbb{Q}_p}/\mathbb{Q}_p)^*.$$

We know from the usual description of de Rham cohomology that

$$\dim F^i H^1_{dR}(A_{\mathbb{Q}_p}/\mathbb{Q}_p) = \begin{cases} 2g & i \leq 0 \\ g & i = 1 \\ 0 & i \geq 0 \end{cases}$$

So $\dim H^1_f(G_p, V_pA) = \dim\left(\frac{H^1_{dR}(A_{\mathbb{Q}_p}/\mathbb{Q}_p)^*}{F^0}\right) = g$.

For the second, $H^1_f(G_{\mathbb{Q}}, V_pA)$ is the $\mathbb{Q}_p$-linear Selmer group attached to A, which sits in an exact sequence

$$0 \to \mathbb{Q}_p \underset{\mathbb{Z}}{\otimes} A(\mathbb{Q}) \to H^1_f(G_{\mathbb{Q}}, V_pA) \to V_p Ш(A/\mathbb{Q}) \to 0.$$

If $Ш(A/\mathbb{Q})[p^\infty]$ is finite, then

$$V_p Ш(A/\mathbb{Q}) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim Ш(A/\mathbb{Q})[p^n] = 0$$

so $\dim H^1_f(G_\mathbb{Q}, V_p A) = rk(A(\mathbb{Q}))$ as claimed. □

Back in the setting of quadratic Chabauty, the graded pieces of our quotient are $V_p J$, $\mathbb{Q}_p(1)^{p-1}$, so assuming that $Ш(J/\mathbb{Q})[p^\infty]$ is finite, we have

$$\dim H^1_f(G_\mathbb{Q}, V_p J) + \dim H^1_f(G_\mathbb{Q}, \mathbb{Q}_p(1)^{p-1}) = rk\, J(\mathbb{Q})$$

while

$$\dim H^1_f(G_p, V_p J) + \dim H^1_f(G_p, \mathbb{Q}_p(1)^{p-1}) = g + p - 1.$$

So if $rk\, J(\mathbb{Q}) < g + p - 1$, then the Chabauty–Kim criterion proves finiteness of $X(\mathbb{Q})$, proving the Theorem on Quadratic Chabauty.

It remains to explain how we can remove the assumption that $Ш(J/\mathbb{Q})[p^\infty]$ is finite. We do this by "defining away" the problem using a construction of Jennifer Balakrishnan and Netan Dogra.

Definition Let $X/\mathbb{Q}$ be a smooth projective curve, $b \in X(\mathbb{Q})$ a rational basepoint, and suppose U is a $G_{\mathbb{Q}}$-equivariant quotient of $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; b)$ which dominates the abelianisation $\pi_1^{\mathbb{Q}_p}(X_{\bar{\mathbb{Q}}}; b)^{ab} = V_p J$. Let V be the image of the abelian Kummer map

$$\mathbb{Q}_p \otimes_{\mathbb{Z}} J(\mathbb{Q}) \hookrightarrow H^1_f(G_{\mathbb{Q}}, V_p J).$$

The Balakrishnan–Dogra Selmer scheme $\mathrm{Sel}_U(X/\mathbb{Q})^{BD}$ is by definition the closed subscheme of $\mathrm{Sel}_U(X/\mathbb{Q})$ which is the preimage of V under the map $\mathrm{Sel}_U(X/\mathbb{Q}) \to H^1_f(G_{\mathbb{Q}}, V_p J)$.

The Balakrishnan–Dogra–Chabauty–Kim locus $X(\mathbb{Q}_p)_U^{BD}$ is the set of points $x \in X(\mathbb{Q}_p)$ such that $j_{p,U}(x)$ lies in the scheme-theoretic image of

$$\mathrm{loc}_p : \mathrm{Sel}_U(X/\mathbb{Q})^{BD} \to H^1_f(G_p, U).$$

The same arguments as before establish

- $X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_U^{BD} \subseteq X(\mathbb{Q}_p)_U$
- if $\dim Sel_U(X/\mathbb{Q})^{BD} < \dim H^1_f(G_p, U)$, then $X(\mathbb{Q}_p)_U^{BD}$ is finite.
- We have

$$\dim Sel_U(X/\mathbb{Q})^{BD} \leq \dim(V) + \sum_{n \geq 2} \dim H^1_f(G_{\mathbb{Q}}, V_n)$$

$$\leq g + \sum_{n \geq 2} \dim H^1_f(G_{\mathbb{Q}}, V_n).$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \ rk\, J(\mathbb{Q})$

Applying this to our quotient U used in quadratic Chabauty, we see that

$$\dim Sel_U(X/\mathbb{Q})^{BD} \leq g \ rk J(\mathbb{Q})$$

and so we get $X(\mathbb{Q}_p)_U^{BD}$ is finite — and hence so is $X(\mathbb{Q})$ — once $rk\, J(\mathbb{Q}) < g + \rho - 1$.

This concludes the proof of the quadratic Chabauty theorem.

Remark: A more sophisticated version of the same argument shows that $X(\mathbb{Q})$ is finite as soon as

$$rk\, J(\mathbb{Q}) < g + \rho + \dim rk\left(NS(J_{\bar{\mathbb{Q}}})^{c=-1}\right) - 1$$ where c is complex conjugation. (For this, one must consider torsors under tori other than $\mathbb{G}_m^{\rho-1}$.)

Conditional results

The Chabauty–Kim criterion can be used to prove finiteness of rational or S-integral points on curves in a wide range of situations, including:

- S-integral points on the thrice-punctured line (Kim)
- Quadratic Chabauty (Besser, Balakrishnan, Müller, Dogra, ...)
- S-integral points on once-punctured elliptic curves with CM (Kim)
- Rational points on curves with CM Jacobians (Kim, Coates)
- Rational points on projective hyperbolic curves which are solvable covers of $\mathbb{P}^1$, e.g. superelliptic curves (Ellenberg, Hast).

However, at the time of writing, the criterion falls short of being able to prove such finiteness results for <u>all</u> hyperbolic curves, due to the difficulty in controlling the global Bloch–Kato Selmer groups $H^1_f(G_{\mathbb{Q}}, V_n)$.

What I want to explain in the final part of this section is why one should expect the Chabauty–Kim criterion

$$\#S + \sum_n \dim H^1_f(G_{\mathbb{Q}}, V_n) < \sum_n \dim H^1_f(G_{\mathbb{Q}_p}, V_n)$$

to hold when the quotient U is sufficiently large, assuming some standard conjectures in Galois representations. Specifically, we will use the Fontaine–Mazur conjecture

Conjecture (Fontaine–Mazur) Let k be a number field. Let V be a finitely ramified irreducible representation of G_k, de Rham at all places above p. Then V is a subquotient of

$$H^i_{\text{ét}}(X_{\bar{k}}, \mathbb{Q}_p)(j)$$

for some smooth projective X/k and i and j. In particular, V is pure of some weight k outside a finite set of places.

The same holds for reducible V, except that X may not be smooth or proper. (and we need to consider relative cohomology.)

Consequence: Assume Fontaine–Mazur. Then for any finitely ramified representation V of G_K, de Rham at all places above p and pure of weight $k>0$ at all but finitely many places. Then

$$H^1_g(G_K, V) = 0.$$

Proof: An element of $H^1_g(G_K, V)$ is represented by a G_K-equivariant extension

$$0 \longrightarrow V \longrightarrow E \longrightarrow \mathbb{Q}_p(0) \longrightarrow 0 \qquad (\ast)$$

where E is de Rham at all places above p.
F–M implies that E is mixed: it has a G_K-invariant weight filtration $W_\bullet E$ such that $\mathrm{gr}^W_k E$ is pure of weight k at all but finitely many places.
(This is a weaker notion of "mixed" than we've been using.)
This weight filtration is unique, and functorial with respect to morphisms of representations. In particular, in $(\ast)$, $W_0 E$ maps isomorphically to $\mathbb{Q}_p(0)$ (since V has positive weight), so defines a splitting.
$\therefore$ $[E]=0$ is the trivial extension $\square$

This allows us to get a handle on the Bloch-Kato Selmer groups appearing in the Chabauty-Kim criterion, by an Euler-characteristic-style formula due to Fontaine and Perrin-Rion.

Proposition: Let V be a finitely ramified representation of G_K, de Rham at all places over p.

Then

$$\dim H^1_f(G_K, V) = \dim V^{G_K} + \dim H^1_f(G_K, V^*(1)) - \dim V^*(1)^{G_K} + \sum_{v|p} \dim H^1_f(G_v, V) - \sum_{v|\infty} \dim V^{G_v}.$$

In particular, assuming Fontaine-Mazur, when V is pure of weight $k \leq -3$ we have

$$\dim H^1_f(G_K, V) = \sum_{v|p} \dim H^1_f(G_v, V) - \sum_{v|\infty} \dim V^{G_v}$$

Consequently, we get a conditional proof of Siegel–Faltings using the Chabauty–Kim criterion.

Theorem: Assume the Fontaine–Mazur Conjecture. Then for any hyperbolic curve $Y/\mathbb{Q}$ with S-integral model $\mathcal{Y}/\mathbb{Z}_S$, basepoint $b \in Y(\mathbb{Q})$ etc., the inequality

$$\#S + \sum_{n=1}^{N} \dim H^1_f(G_{\mathbb{Q}}, V_n) < \sum_{n=1}^{N} \dim H^1_f(G_{\mathbb{Q}_p}, V_n)$$

holds for $N \gg 0$, where V_n is the n^{th} weight-graded piece of $\pi_1^{\mathbb{Q}_p}(Y_{\bar{\mathbb{Q}}}; b)$. In particular, $\mathcal{Y}(\mathbb{Z}_S)$ is finite.

Proof: Under Fontaine–Mazur, the left- and right-hand sides are equal to

$$\text{const.} + \sum_{n=3}^{N} \dim H^1_f(G_{\mathbb{Q}_p}, V_n) - \sum_{n=3}^{N} \dim V_n^{\sigma}$$

and

$$\text{const.} + \sum_{n=3}^{N} \dim H^1_f(G_p, V_n)$$

respectively, where σ is complex conjugation. It thus suffices to prove that $\dim V_n^{\sigma} > 0$ for infinitely many n.

If not, then there is some n_0 such that σ acts by -1 on V_n for all $n \geq n_0$. In particular, for $n_1, n_2 \geq n_0$, the commutator of any elements in V_{n_1} and V_{n_2} must vanish in $V_{n_1+n_2}$.