The principle of Birch and Swinnerton-dyer for certain hyperbolic curves

Minhyong Kim

November 12, 2007

London-Paris Number Theory Seminar

I. Preliminary remarks

II. Arithmetic fundamental groups

III. Selmer varieties

IV. Elliptic curves with complex multiplication

V. Preliminary remarks

I. Preliminary remarks

(i) Path torsors

M reasonable connected topological space. $b \in M$, point.
Determines a fundamental group:

$$\pi_1(M, b).$$

More generally, consider $b, x \in M$, and the set

$$\pi_1(M; b, x)$$

of homotopy classes of paths from b to x.

Wish to study dependence on variable x.

Somewhat more structure:

Each

$$\pi_1(M; b, x)$$

has an action of

$$\pi_1(M, b)$$

on the right

$$\pi_1(M; b, x) \times \pi_1(M, b) \to \pi_1(M; b, x)$$

$$(p, \gamma) \mapsto p \circ \gamma$$

turning it into a *torsor* for $\pi_1(M, b)$.

We have a *variation of torsors*.

In set-theoretic setting, problem trivial. Whenever we choose an element $p \in \pi_1(M; b, x)$, action induces a bijection

$$\pi_1(M, b) \simeq \pi_1(M; b, x)$$

$$\gamma \mapsto p \circ \gamma$$

That is to say, the choice of any element determines a trivialization.

But such isomorphisms are not canonical, as is often emphasized in elementary topology. That is, any two torsors $\pi_1(M; b, x_1)$ and $\pi_1(M; b, x_2)$ are isomorphic, but not canonically. Usually, this distinction is not important.

However, geometrically, these torsors form a *natural family*.

(ii) Covering spaces

Recall another interpretation of the fundamental group. Let

$$\tilde{M} \to M$$

be a universal covering. Fix a point $\tilde{b} \in \tilde{M}$ so that we get a map

$$(\tilde{M}, \tilde{b}) \to (M, b)$$

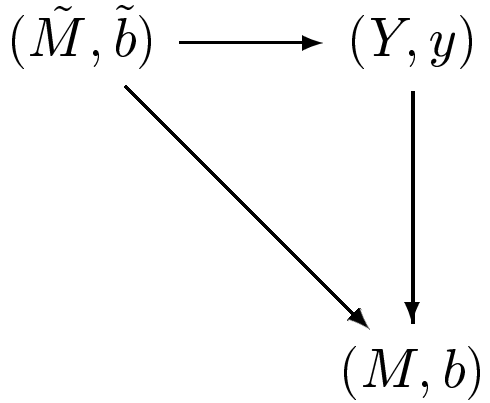
of pointed spaces.

This map is universal among pointed covering spaces.

That is, given any pointed covering space

$$(Y, y) \to (M, b)$$

there is a unique commutative diagram



Using $(\tilde{M}, \tilde{b})$, we get an isomorphism

$$\pi_1(M; b, x) \simeq \tilde{M}_x$$

by lifting paths. Thus, the study of the variation of $\pi_1(M; b, x)$ in x, becomes that of studying the fibers of

$$\tilde{M} \to M$$

This fiber bundle is of course not trivial in general, i.e., the universal $\pi_1(M, b)$-torsor is not trivial.

[One *construction* of $\tilde{M}$ consists in

$$\tilde{M} := \cup_x \pi(M; b, x)]$$

Of course we are interested in the situation where

$$X/\mathbb{Q}$$

is a variety,

$$M = X(\mathbb{C})$$

and

$$b, x \in X(\mathbb{Q}) \subset M$$

That is, in $\pi_1(X(\mathbb{C}); b, x)$ for *special points* x.

But in this form, can't distinguish such special points from generic ones.

II. Arithmetic fundamental groups

(i) Galois Actions

Consider the profinite completion

$$\pi_1(X(\mathbb{C}), b)^\wedge$$

and the pushout torsor

$$\pi_1(X(\mathbb{C}); b, x)^\wedge = \pi_1(X(\mathbb{C}); b, x) \times_{\pi_1(X(\mathbb{C}), b)} \pi_1(X(\mathbb{C}), b)^\wedge$$

Then $\pi_1(X(\mathbb{C}), b)^\wedge$ and $\pi_1(X(\mathbb{C}); b, x)^\wedge$ end up with compatible actions of

$$\Gamma := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

Compatibility means that for $g \in \Gamma$, $l \in \pi_1(X(\mathbb{C}), b)^\wedge$ and $p \in \pi_1(X(\mathbb{C}); b, x)^\wedge$, then

$$g(p)g(l) = g(pl)$$

Thus, $\pi_1(X(\mathbb{C}); b, x)^\wedge$ becomes a Γ-equivariant torsor for $\hat{\pi}_1(X(\mathbb{C}), b)$.

[Or a torsor on the étale site of $\mathrm{Spec}(\mathbb{Q})$.]

Underlying this action are the isomorphisms

$$\pi_1(X(\mathbb{C}), b)^\wedge \simeq \hat{\pi}_1(\bar{X}, b)$$

and

$$\pi_1(X(\mathbb{C}); b, x)^\wedge \simeq \hat{\pi}_1(\bar{X}; b, x)$$

involving the profinite étale fundamental group and the étale torsor of paths for

$$\bar{X} := X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\bar{\mathbb{Q}})$$

Defined using $\mathrm{Cov}(\bar{X})$, the category of finite étale covering spaces of $\bar{X}$ and the fiber functors

$$F_b : \mathrm{Cov}(\bar{X}) \to \text{finite sets}$$

$$\begin{array}{ccc} Y & & Y_b \\ \downarrow & \mapsto & \downarrow \\ \bar{X} & & b \end{array}$$

Functorial definition:

$$\hat{\pi}_1(\bar{X}, b) := \mathrm{Aut}(F_b)$$

$$\hat{\pi}_1(\bar{X}; b, x) := \mathrm{Isom}(F_b, F_x)$$

Then Γ acts on the category preserving the fiber functors (when $b, x \in X(\mathbb{Q})$) and hence acts on the group and torsor.

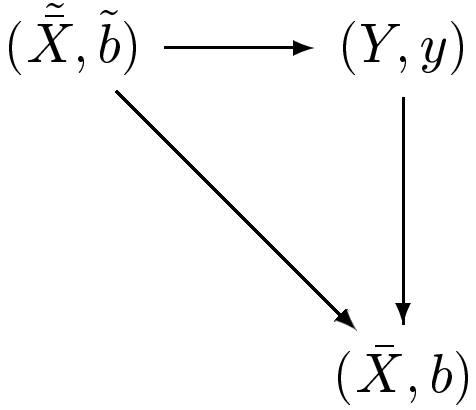
[It is this definition that allows us to study flexibly the base-point dependence.]

(ii) Universal pro-covering spaces

To compute this action, again use a universal pointed covering space

$$(\tilde{\bar{X}}, \tilde{b}) \to (\bar{X}, b)$$

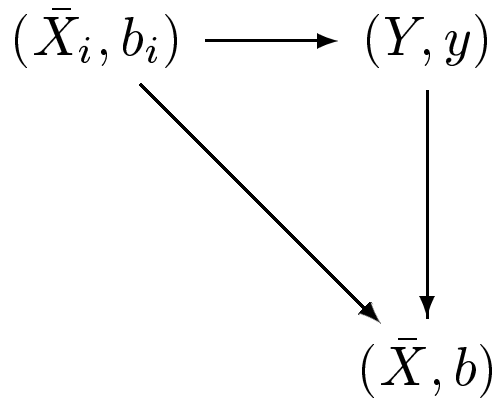
constructed, for example, using Galois theory, with the universal property that given any finite algebraic covering space $(Y, y) \to (\bar{X}, b)$ there is a unique commutative diagram



$(\tilde{\bar{X}}, \tilde{b})$ is actually a projective system

$$\{(\bar{X}_i, b_i)\}$$

and the diagram means that there is some index i and a commutative diagram



In this situation, once again, we have

$$\hat{\pi}_1(\bar{X}, b) \simeq \tilde{\bar{X}}_b$$

and the path space

$$\hat{\pi}_1(\bar{X}; b, x) \simeq \tilde{\bar{X}}_x$$

As the notation suggests, can take the whole system $\tilde{\bar{X}}$, i.e., each

$$\bar{X}_i \to X,$$

the transition maps between them, and the base point $\tilde{b} = \{b_i\}$ to be defined over $\mathbb{Q}$. And then the Galois action just becomes the naive action on the fibers of

$$\tilde{\bar{X}} \to \bar{X}$$

over rational points.

Example:

$(\bar{E}, 0)$ elliptic curve with origin over $\mathbb{Q}$. Let

$$E_n \to E$$

be the covering space given by E itself with the multiplication map

$$[n] : E \to E$$

Then the system

$$(\tilde{\bar{E}}, \tilde{0}) := \{(\bar{E}_n, 0)\}_n \longrightarrow (\bar{E}, 0)$$

is a universal pointed covering space.

Thus, for $(E, 0)$,

$$\hat{\pi}_1(\bar{E}, 0) \simeq \hat{T}(E)$$

and an element of the fundamental group is just a compatible collection of torsion points of E.

Similarly,

$$\hat{\pi}_1(\bar{E}; 0, x) \simeq \hat{\bar{E}}_x$$

consists of compatible systems of division points of x.

This example illustrates that if we take into account the Galois action, it is no longer possible to trivialize the torsor in general, even point-wise.

That is, there will usually be no isomorphism between $\hat{\pi}_1(\bar{X}, b)$ and $\hat{\pi}_1(\bar{X}; b, x)$ in the category of Γ-equivariant torsors. [Or as sheaves on $\mathrm{Spec}(\mathbb{Q})$.]

In the case of $(E, 0)$, if there were an isomorphism

$$\hat{\pi}_1(\bar{E}, 0) \simeq \hat{\pi}_1(\bar{E}; 0, x)$$

then there would be a Galois invariant element of

$$\hat{\pi}_1(\bar{E}; 0, x) \simeq \tilde{\bar{E}}_x.$$

In particular, for any n, there would be a rational point x_n such that $nx_n = x$. Not possible by Mordell's theorem.

[In general, a Γ-equivariant torsor can be trivialized if and only if it has a Γ-invariant element.]

(iii) The general formalism of arithmetic period maps

Given a Γ-equivariant torsor T for $\hat{\pi}_1(\bar{X}, b)$ choose any element $t \in T$. Then for each $g \in \Gamma$, $g(t)$ is related to t by the $\hat{\pi}_1(\bar{X}, b)$-action, i.e.,

$$g(t) = t\gamma_g$$

for some $\gamma_g \in \hat{\pi}_1(\bar{X}, b)$. The map $g \mapsto \gamma_g$ obtained thereby determines a non-abelian (continuous) cocycle

$$c : \Gamma \to \hat{\pi}_1(\bar{X}; b, x),$$

that is, satisfying the relation

$$c(g_1 g_2) = c(g_1) g_1(c(g_2))$$

The set of such cocycles is denoted by

$$Z^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

$\hat{\pi}_1(\bar{X}, b)$ itself acts on the set of cocycles via

$$(\gamma c)(g) = g(\gamma^{-1})c(g)\gamma$$

giving rise to the set of orbits

$$H^1(\Gamma, \hat{\pi}_1(\bar{X}, b)) := \hat{\pi}_1(\bar{X}, b) \backslash Z^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

This is a non-abelian cohomology set classifying the Γ-equivariant torsors for $\hat{\pi}_1(\bar{X}, b)$.

Thus, the previous discussion of varying torsors of paths can be summarized as a 'period' map

$$X(\mathbb{Q}) \to H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

$$x \mapsto [\hat{\pi}_1(\bar{X}; b, x)]$$

Suppose X is a compact smooth curve of genus ≥ 2. Then this map is injective by the Mordell-Weil theorem.

Grothendieck's section conjecture

proposes that this map is surjective as well, i.e., torsors of paths coming from rational points are the only natural torsors for $\hat{\pi}_1(\bar{X}, b)$. Part of his *anabelian* program.

(iv) The Diophantine connection

Grothendieck expected section conjecture to lead to another proof of Diophantine finiteness for hyperbolic curves. Somewhat explains his disapproval of motives? Theory of motives, involving *abelianization*, rarely gives information on $X(\mathbb{Q})$. Serious deficiency indicating need to move beyond abelian motives.

However, correctness of expectation unclear. Perhaps $\hat{\pi}_1(\bar{X}, b)$ is too non-abelian. Need to find middle ground between anabelian and motivic language, or between hyperbolic and elliptic curves.

For elliptic curves, the corresponding map

$$E(\mathbb{Q}) \to H^1(\Gamma, \hat{T}(E))$$

is classical, and its study is *Kummer theory*. In the theory of elliptic curves, one constructs a natural subspace

$$H^1_f(\Gamma, \hat{T}(E)) \subset H^1(\Gamma, \hat{T}(E))$$

using local conditions and conjectures that

$$\widehat{E(\mathbb{Q})} \simeq H^1_f(\Gamma, \hat{T}(E))$$

(Birch and Swinnerton-Dyer)

From this perspective, the section conjecture is a natural non-abelian generalization of BSD.

Parallel picture:

$$E(\mathbb{Q}) \longrightarrow H^1(\Gamma, \hat{T}(E))$$

$$X(\mathbb{Q}) \longrightarrow H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

$$x \longmapsto [\hat{\pi}_1(\cdot; b, x)]$$

Finiteness then should follow from a kind of non-abelian BSD principle:

Non-vanishing of L-values $\Rightarrow$ Diophantine finiteness.

Mostly speculative...

III. Selmer varieties

(i) Summary

This idea can be implemented for

-hyperbolic curves of genus zero;

-the 'Coates-Wiles' situation:

$$X = E \setminus \{0\}$$

where $E/\mathbb{Q}$ is an elliptic curves with complex multiplication;

-a few more scattered cases

using *Selmer varieties*.

Also, finiteness for a general hyperbolic curve follows from a 'higher BSD conjecture' such as the Bloch-Kato conjecture, or the Fontaine-Mazur conjecture. Both of these are assertions of surjectivity of [e.g. regulator] maps from motives to some $H^1_f(\Gamma, \cdot)$.

That is to say, so far, general finiteness for curves accounted for by

abelian surjectivity + mildly non-abelian construction

(ii) Motivic fundamental groups

Focus now on a hyperbolic curve X and the $\mathbb{Q}_p$-*pro-unipotent completion* of its fundamental group.

$$\hat{\pi}_1(\bar{X}, b) \longrightarrow U^{\mathbb{Q}_p} = \pi_1^{et,\mathbb{Q}_p}(\bar{X}, b)$$

where $U^{\mathbb{Q}_p}$ is defined using

$$\mathrm{Un}(\bar{X})^{\mathbb{Q}_p}$$

category of unipotent $\mathbb{Q}_p$-lisse sheaves of $\bar{X}$.

[A sheaf is unipotent if it corresponds to a unipotent representation of $\hat{\pi}_1(\bar{X}, b)$.]

Point $b \in X(\mathbb{Q})$ again determines a linear fiber functor

$$F_b : \mathrm{Un}(\bar{X})^{\mathbb{Q}_p} \to \mathrm{Vect}_{\mathbb{Q}_p}$$

and

$$U^{\mathbb{Q}_p} := \mathrm{Aut}^{\otimes}(F_b)$$

For $x \in X(\mathbb{Q})$ there is a torsor of unipotent paths

$$\pi_1^{et,\mathbb{Q}_p}(\bar{X}; b, x) := \mathrm{Isom}^{\otimes}(F_b, F_x) \quad (\simeq \hat{\pi}_1(\bar{X}; b, x) \times_{\hat{\pi}_1(\bar{X}, b)} U^{\mathbb{Q}_p})$$

These objects also carry compatible Γ-actions.

The previous period map is replaced by

$$X(\mathbb{Q}) \longrightarrow H^1(\Gamma, U^{\mathbb{Q}_p})$$

$$x \longmapsto [\pi_1^{et,\mathbb{Q}_p}(\bar{X}; b, x)]$$

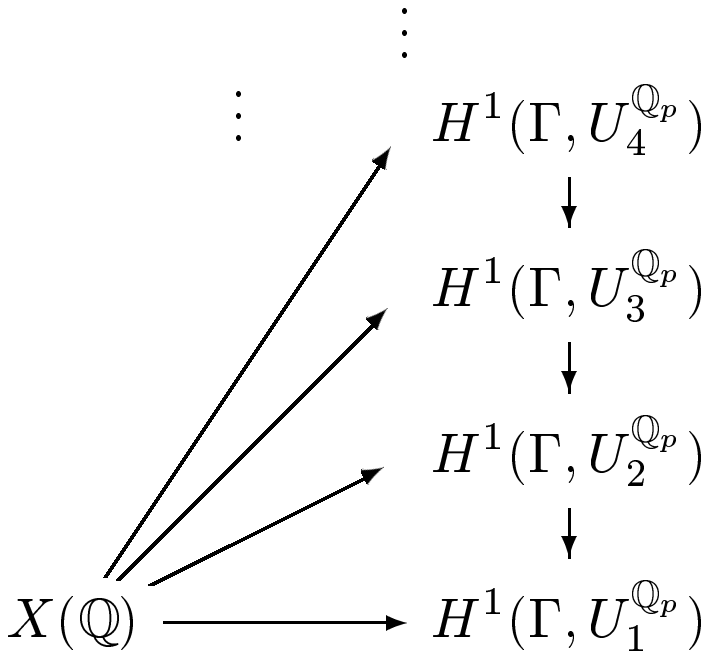
Can study this inductively using the descending central series

$$Z^1 := U^{\mathbb{Q}_p} \supset Z^2 := [U^{\mathbb{Q}_p}, U^{\mathbb{Q}_p}] \supset Z^3 := [U^{\mathbb{Q}_p}, [U^{\mathbb{Q}_p}, U^{\mathbb{Q}_p}]] \supset \cdots$$

and the associated quotients $U_n^{\mathbb{Q}_p} := U^{\mathbb{Q}_p}/Z^{n+1}$ that fit into exact sequences

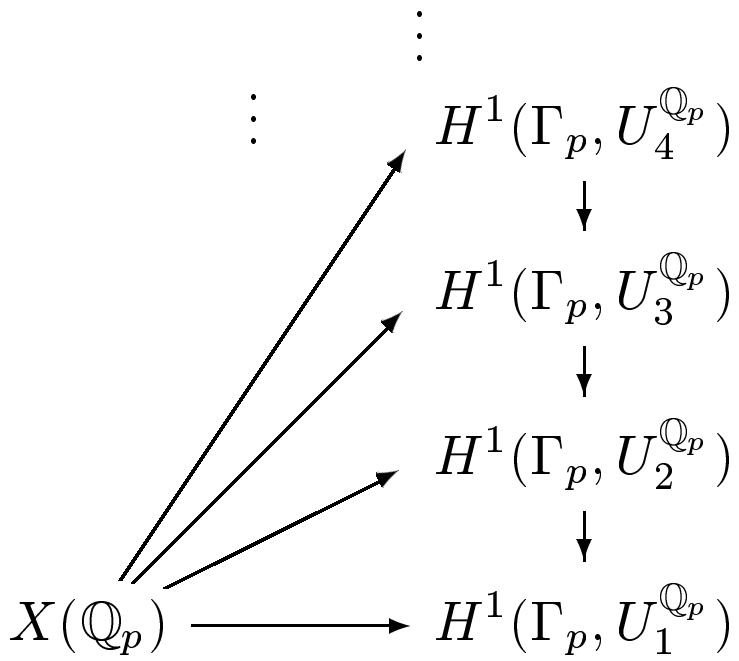
$$0 \to [Z^{n+1} \backslash Z^n] \to U_n^{\mathbb{Q}_p} \to U_{n-1}^{\mathbb{Q}_p} \to 0$$

and induce a tower:



lifting classical Kummer theory.

Can also consider the local action of $\Gamma_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and a local version of the tower



leading to a sequence of commutative diagrams

$$\begin{array}{ccc} X(\mathbb{Q}) & \to & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ H^1(\Gamma, U_n^{et}) & \to & H^1(\Gamma_p, U_n^{et}) \end{array}$$

(iii) Selmer varieties

We will utilize this diagram by way of a bit more geometric information. Let S be a finite set of primes, $\mathbb{Z}_S$ the ring of S-integers, and

$$\mathcal{X} \to \mathrm{Spec}(\mathbb{Z}_S)$$

a good model of X. [A smooth model with a smooth compactification having an étale compactification divisor (possibly empty).]

Choose $p \notin S$ and put $T = S \cup \{p\}$.

Then we get an induced diagram:

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_S) & \to & \mathcal{X}(\mathbb{Z}_p) \\ \downarrow \kappa_n^{glob} & & \downarrow \kappa_n^{loc} \\ H^1_f(\Gamma, U_n^{et}) & \stackrel{loc}{\to} & H^1_f(\Gamma_p, U_n^{et}) \end{array}$$

where

$$H^1_f(\Gamma_p, U_n^{et}) \subset H^1(\Gamma_p, U_n^{et})$$

classifies torsors that are crystalline, i.e., have a Γ_p-invariant B_{cr}-point, and

$$H^1_f(\Gamma, U_n^{et}) \subset H^1(\Gamma, U_n^{et})$$

classifies torsors that are unramified outside T and crystalline at p:

These notions allow us to focus the general formalism.

Two key points:

I. The localizations

$$H^1_f(\Gamma, U_n^{et}) \longrightarrow H^1_f(\Gamma_p, U_n^{et})$$

are maps of algebraic varieties over $\mathbb{Q}_p$.

In particular,

-$H^1_f(\Gamma, U_n^{et})$ and $H^1_f(\Gamma_p, U_n^{et})$ are natural geometric families into which the points fit:

global and local *Selmer varieties*;

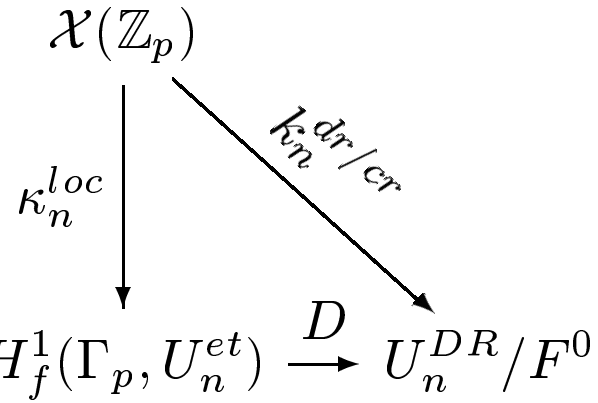
-and the difficult inclusion $\mathcal{X}(\mathbb{Z}_S) \subset \mathcal{X}(\mathbb{Z}_p)$ is replaced by an algebraic map.

II. The map

$$\kappa_n^{loc} : \mathcal{X}(\mathbb{Z}_p) \to H^1_f(\Gamma_p, U_n^{\mathbb{Q}_p})$$

can be computed using *non-abelian p-adic Hodge theory.*

In fact, Hodge theory provides a commutative diagram:



and the map $\kappa_n^{dr/cr}$ can be explicitly computed using *p-adic iterated integrals.*

(iv) The local map

Here

$$U^{DR} = \pi_1^{DR}(X \otimes \mathbb{Q}_p, b)$$

is the De Rham/crystalline fundamental group of $X \otimes \mathbb{Q}_p$ and F^i refers to the Hodge filtration.

Then U^{DR}/F^0 becomes a classifying space for De Rham/crystalline torsors, and the map

$$\mathcal{X}(\mathbb{Z}_p) \to U^{DR}/F^0$$

again associates to a point x the torsor

$$\pi_1^{DR}(X \otimes \mathbb{Q}_p; b, x)$$

of De Rham/crystalline paths.

Example:

$X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$. Then the coordinate ring of U^{DR} is the $\mathbb{Q}_p$-vector space

$$\mathbb{Q}_p[\alpha_w]$$

where w runs over words on two letters A, B. Also, $F^0 = 0$, and for

$$w = A^{m_1} B A^{m_2} B \cdots A^{m_l} B$$

we get

$$\alpha_w \circ \kappa^{dr/cr}(x)$$

$$= \int_b^x (dz/z)^{m_1} (dz/(1-z))(dz/z)^{m_2} \cdots (dz/z)^{m_l} (dz/(1-z))$$

a $p-$adic multiple polylogarithm.

The map

$$D : H^1_f(\Gamma_p, U_n^{\mathbb{Q}_p}) \to U_n^{DR}/F^0$$

is given by

$$D(P) = \mathrm{Spec}([\mathcal{P} \otimes B_{cr}]^{G_p})$$

if $P = \mathrm{Spec}(\mathcal{P})$. Commutativity of the diagram is the assertion

$$\pi_1^{et,\mathbb{Q}_p}(\bar{X}; b, x) \otimes B_{cr} \simeq \pi_1^{DR}(X \otimes \mathbb{Q}_p; b, x) \otimes B_{cr}$$

proved by Shiho, Vologodsky, Faltings, Olsson.

A corollary of this description is that

Theorem 0.1 *The image of each*

$$\mathcal{X}(\mathbb{Z}_p) \to H^1_f(\Gamma_p, U_n^{\mathbb{Q}_p})$$

is Zariski dense. In fact, the image of each residue disk is Zariski-dense.

A poor man's local substitute for the section conjecture.

(v) Finiteness

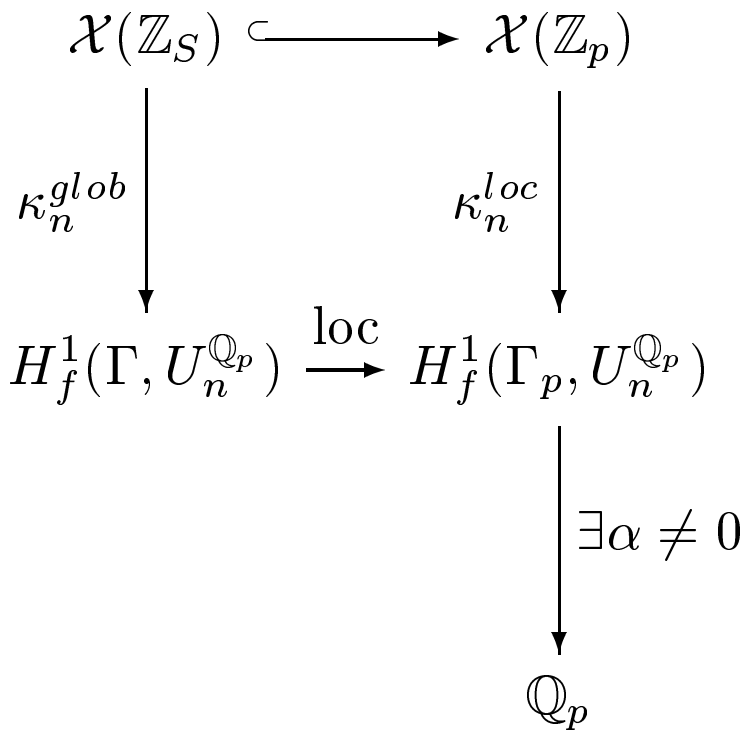
Another corollary:

Theorem 0.2 *Suppose*

$$Im[H^1_f(\Gamma, U_n^{\mathbb{Q}_p})] \subset H^1_f(\Gamma_p, U_n^{\mathbb{Q}_p})$$

is not *Zariski dense. Then* $\mathcal{X}(\mathbb{Z}_S)$ *is finite.*

Idea of proof:



such that α vanishes on $Im[H^1_f(\Gamma, U_n^{\mathbb{Q}_p})]$. Hence, $\alpha \circ \kappa_n^{loc}$ vanishes on $\mathcal{X}(\mathbb{Z}_S)$. But this function is a non-vanishing convergent power series on each residue disk. $\square$

(vi) Connection to Iwasawa theory

In all cases so far, prove non-denseness by showing

$$\dim H^1_f(\Gamma, U_n^{\mathbb{Q}_p}) < \dim H^1_f(\Gamma_p, U_n^{\mathbb{Q}_p})$$

for $n >> 0$. Implied by standard motivic conjectures.

That is, *controlling the Selmer variety leads to finiteness of points.*

Nature of the inequality suggests that proofs should go through *Iwasawa theory.*

Preliminary outline:

$$H^1_f(\Gamma, U_n^{\mathbb{Q}_p}) \subset H^1(\Gamma_T, U_n^{\mathbb{Q}_p})$$

and

$$0 \to H^1(\Gamma_T, Z^{n+1} \backslash Z^n) \to H^1(\Gamma_T, U_n^{\mathbb{Q}_p}) \to H^1(\Gamma_T, U_{n-1}^{\mathbb{Q}_p})$$

is an exact sequence.

Euler characteristic formula:

$$\dim H^1(\Gamma_T, Z^{n+1} \backslash Z^n) - \dim H^2(\Gamma_T, Z^{n+1} \backslash Z^n) = \dim(Z^{n+1} \backslash Z^n)^-$$

Therefore, controlling

$$H^2(\Gamma_T, Z^{n+1} \backslash Z^n)$$

gives a bound on the dimensions of global Selmer varieties. Meanwhile, dimension of local Selmer varieties given by precise combinatorial formula.

For $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$,

$$Z^{n+1} \backslash Z^n \simeq \mathbb{Q}_p(n)^{r_n}$$

and

$$H^2(\Gamma_T, Z^{n+1} \backslash Z^n) = 0$$

for $n >> 0$ follows from the finiteness of zeros of p-adic L-function for cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\mu_p)$.

[Can also use Soulé's map from K-theory.]

IV. Elliptic curves with complex multiplication

For $X = E \setminus \{0\}$, E elliptic curve with CM by an imaginary quadratic field K, need to choose p to be split as $p = \pi\bar{\pi}$ in K and replace $U^{\mathbb{Q}_p}$ by a natural quotient W with property that

$$U_2^{\mathbb{Q}_p} \simeq W_2$$

and (for $n \geq 3$)

$$W^n/W^{n+1} \simeq \mathbb{Q}_p(\psi^{n-2})(1) \oplus \mathbb{Q}_p(\bar{\psi}^{n-2})(1)$$

viewed as a representation of Γ in the natural way, where ψ and $\bar{\psi}$ are characters of $N := \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ corresponding to $T_\pi E := \varprojlim E[\pi^n]$ and $T_{\bar{\pi}} E := \varprojlim E[\bar{\pi}^n]$ respectively.

Notation:

$s = |S| - 1$

$r = \dim H^1_f(\Gamma, U_1^{\mathbb{Q}_p})$

$M = K(E[\pi^\infty]), \quad \bar{M} = K(E[\bar{\pi}^\infty])$

$G = \mathrm{Gal}(M/K), \quad \bar{G} = \mathrm{Gal}(\bar{M}/K)$

$\Lambda = \mathbb{Z}_p[[G]], \quad \bar{\Lambda} = \mathbb{Z}_p[[\bar{G}]]$

$\psi : \Lambda \to \mathbb{Q}_p$ defined by action of G on $T_\pi(E)$

$\bar{\psi} : \bar{\Lambda} \to \mathbb{Q}_p$ defined by action of $\bar{G}$ on $T_{\bar{\pi}}(E)$

$V_p = T_p(E) \otimes \mathbb{Q}$, V_π, etc.

Have corresponding p-adic L-functions:

$$\mathcal{L}_p \in \Lambda, \quad \bar{\mathcal{L}}_p \in \bar{\Lambda}$$

Construction of W:

$\Gamma = N < \sigma >$, where σ is complex conjugation.

Choose a $\mathbb{Q}_p$-basis e of $T_\pi(E) \otimes \mathbb{Q}_p$ so that $f := \sigma(e)$ is a $\mathbb{Q}_p$-basis of $T_{\bar{\pi}}(E) \otimes \mathbb{Q}_p$.

Recall that

$$\mathcal{U} := \mathrm{Lie}U$$

can be realized as the primitive elements in

$$T(U_1) = T(V_p)$$

where $T(\cdots)$ refers to the tensor algebra (but with a different Galois action).

For example, if $\gamma \in N$, then

$$\gamma[e,[e,f]] = \psi(\gamma)^2\bar{\psi}(\gamma)[e,[e,f]] + \text{Lie monomials of higher degree}$$

and

$$\sigma[e,[e,f]] = [f,[f,e]] + \text{Lie monomials of higher degree}$$

That is, $\mathcal{U}$ has a bi-grading

$$\mathcal{U} = \overline{\oplus_{i,j\geq 1}\mathcal{U}_{i,j}}$$

corresponding to e and f degrees, but which is not preserved by the Galois action.

However, easy to check that the filtration

$$\mathcal{U}_{\geq n,\geq m} := \overline{\oplus_{i\geq n,j\geq m}\mathcal{U}_{i,j}}$$

is preserved by N, while

$$\sigma(\mathcal{U}_{\geq n,\geq m}) = \mathcal{U}_{\geq m,\geq n}$$

So

$$\mathcal{U}_{\geq n,\geq n}$$

is Galois invariant for each n.

Furthermore, it is a Lie ideal.

Hence, there is a well-defined quotient W of U corresponding to

$$\mathcal{U}/\mathcal{U}_{\geq 2,\geq 2}$$

We then see that

$$W^n/W^{n+1}$$

$$\simeq < \mathrm{ad}(e)^{n-1}(f) > \oplus < \mathrm{ad}(f)^{n-1}(e) > \pmod{W^{n+1}}$$

$$\simeq \psi^{n-2}(1) \oplus \bar{\psi}^{n-2}(1)$$

Extended diagram:

$$\begin{array}{ccc}
\mathcal{X}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{X}(\mathbb{Z}_p) \\
\downarrow & & \downarrow \\
H^1_f(\Gamma, U_n) & \to & H^1_f(\Gamma_p, U_n^{\mathbb{Q}_p}) \\
\downarrow & & \downarrow \\
H^1_f(\Gamma, W_n) & \to & H^1_f(\Gamma_p, W_n)
\end{array}$$

Theorem 0.3

$$dim H^1_f(\Gamma, W_n) < dim H^1_f(\Gamma_p, W_n)$$

for $n >> 0$.

Theorem 0.4 *Assume*

(*) $\psi^{-k}(\mathcal{L}_p) \neq 0$ and $\bar{\psi}^{-k}(\bar{\mathcal{L}}_p) \neq 0$ for all $k > 0$.

Then

$$dim H^1_f(\Gamma, W_n) < dim H^1_f(\Gamma_p, W_n)$$

for $n = r + s$.

Finiteness follows from the previous argument applied to these modified Selmer varieties.

Proof of theorems

Uses main conjecture for K. We will concentrate on (0.4).

We need the exact sequence

$$0 \to W^n/W^{n+1} \to W_n \to W_{n-1} \to 0$$

As for the Hodge filtration,

$$\dim W_1^{DR}/F^0 = 1$$

and

$$F^0[(W^{DR})^n/(W^{DR})^{n+1}] = 0$$

for $n \geq 2$, so that

$$\dim H^1_f(\Gamma_p, W_n) = 2 + 2(n-2) = 2n - 2$$

for $n \geq 2$.

Meanwhile,

$$\dim H^1_f(\Gamma, W_1) = r$$

$$\dim H^1_f(\Gamma, W^1/W^2) = \dim H^1_f(\Gamma, \mathbb{Q}_p(1)) = s - 1$$

so that

$$\dim H^1_f(\Gamma, W_2) \leq r + s - 1$$

As we go down the lower central series, we have, in any case, the Euler characteristic formula

$$\dim H^1(\Gamma_T, W^n/W^{n+1}) - \dim H^2(\Gamma_T, W^n/W^{n+1})$$

$$= \dim(W^n/W^{n+1})^{\sigma=-1} = 1$$

and

$$H^1_f(\Gamma, W^n/W^{n+1}) = H^1(\Gamma_T, W^n/W^{n+1})$$

for $n \geq 2$, so we need to compute the H^2 term.

Claim (still assuming (*)):

$$H^2(\Gamma_T, W^n/W^{n+1}) = 0$$

for $n \geq 3$.

Clearly, it suffices to prove this after restricting to $N_T \subset \Gamma_T$ (with obvious notation). Then we have

$$W^n/W^{n+1} \simeq \psi^{n-2}(1) \oplus \bar{\psi}^{n-2}(1)$$

We will show

$$H^2(N_T, \psi^{n-2}(1)) = 0$$

for $n \geq 3$.

Consider the localization sequence

$$0 \to Sha^2_T(\psi^{n-2}(1)) \hookrightarrow H^2(N_T, \psi^{n-2}(1)) \to \oplus_{v|T} H^2(N_v, \psi^{n-2}(1))$$

that defines the vector space $Sha^2(\psi^{n-2}(1))$. By local duality,

$$H^2(N_v, \psi^{n-2}(1)) \simeq H^0(N_v, \psi^{2-n})^* = 0$$

since the representation ψ^{2-n} is potentially unramified or potentially crystalline.

So we have

$$H^2(N_T, \psi^{n-2}(1)) \simeq Sha^2_T(\psi^{n-2}(1)) \simeq Sha^1_T(\psi^{2-n})^*$$

by Poitou-Tate duality. But

$$Sha^1_T(\psi^{2-n}) \simeq \mathrm{Hom}_\Lambda(A, \psi^{2-n})$$

where A is the Galois group of the maximal abelian unramified pro-p extension of $M(= K(E[\pi^\infty]))$ split above the primes dividing T.

In particular, A is annihilated by $\mathcal{L}_p$.

Since we are assuming $\psi^{2-n}(\mathcal{L}_p) \neq 0$ for $n \geq 3$, we get the desired vanishing:

$$H^2(N_T, \psi^{n-2}(1)) = 0$$

Similarly,

$$H^2(N_T, \bar{\psi}^{n-2}(1)) = 0$$

Finally, we conclude that

$$\dim H^1_f(\Gamma, W^n/W^{n+1}) = 1$$

for $n \geq 3$ so that

$$\dim H^1_f(\Gamma, W_n) \leq r + s + n - 3$$

for $n \geq 2$.

Thus,

$$H^1_f(\Gamma_p, W_n) = 2n - 2 > r + s + n - 3 = \dim H^1_f(\Gamma, W_n)$$

as soon as $n \geq r + s$.

Note that even without (*), we have

$$\psi^{2-n}(\mathcal{L}_p) \neq 0 \quad \bar{\psi}^{2-n}(\bar{\mathcal{L}}_p) \neq 0$$

and hence,

$$H^2(\Gamma_T, W^n/W^{n+1}) = 0$$

for n sufficiently large.

Therefore,

$$\dim H^1_f(\Gamma, W_n) \sim n < \dim H^1_f(\Gamma_p, W_n) \sim 2n$$

for n sufficiently large, yielding finiteness of

$$\mathcal{X}(\mathbb{Z}_S)$$

in any case.

However, the effectivity in n that appears in (0.4) should eventually apply to the problem of finding points.

V. Preliminary remarks

Non-abelian principle of Birch and Swinnerton-Dyer:

> non-vanishing of (most) L-values $\Rightarrow$ control of Selmer varieties $\Rightarrow$ finiteness of integral points

in parallel to the case of elliptic curves, with just the substitution of Selmer varieties for Selmer groups. But the cases studied so far should just be a shadow of the true picture, where, for example, the non-vanishing of L should be a non-abelian statment.

Also, both implications should eventually be *direct*.

Relevance of section conjecture: complete computation of points and *non-abelian descent*.