Fundamental groups and Diophantine geometry

Minhyong Kim

September 12, 2006

$X/\mathbb{Q}$ compact smooth hyperbolic curve.

$\mathrm{Cov}(\bar{X})$ category of finite étale coverings of $\bar{X}$.

$b \in X(\mathbb{Q})$ rational point. Determines a fiber functor

$F_b : \mathrm{Cov}(X) \rightarrow$ Finite Sets

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

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

For any other point $x \in X(\mathbb{Q})$, have the *torsor of paths*

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

All carry actions of $\Gamma := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, i.e. are Γ-equivariant torsors. Classified by continuous non-abelian cohomology set:

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

Thus, we have a map

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

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

Grothendieck's section conjecture:

$\hat{\kappa}$ is a bijection.

Remark: Injectivity known. Surjectivity appears very difficult.

Grothendieck and Deligne expected the conjecture to be relevant to Diophantine geometry, especially the theorem of Faltings. Initial expectation appears to have been erroneous.

Question: Why should such a statement be relevant to Diophantine finiteness?

Two separate problems:

(1) Section conjecture itself;

(2) Relevance to Diophantine finiteness.

1/2-answer:

Analogy to Birch and Swinnerton-Dyer:

$$\hat{\kappa} : \widehat{E(\mathbb{Q})} \rightarrow H^1_f(\Gamma, \hat{\pi}_1(\bar{E}, e))$$

is a bijection.

Grothendieck's conjecture is a *higher-genus non-abelian* analogue.

The target is a *Selmer group* that can be

(a) computed (in principle) $\leftarrow$ Cremona's algorithms;

(b) controlled (occasionally) $\leftarrow$ method of Kolyvagin and Kato;

(a) involves descent and searching for points in order of height.

(b) involves critically technology of *motives*: L-functions, Iwasawa theory, duality, Hodge theory, ...

Non-abelian analogues?

Some beginnings...

We have

Non-abelian Selmer varieties

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

and

Unipotent Kummer maps

$$\kappa_n^u : X(\mathbb{Q}) \rightarrow H^1_f(\Gamma, U_n^{et})$$

where U^{et} is the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of X with basepoint b.

That is,

$$U_n^{et} = Aut^{\otimes}(F_b^u)$$

where

$$F_b^u : \mathrm{Un}^{et}(\bar{X}, \mathbb{Q}_p) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p}$$

$$\mathcal{L} \mapsto \mathcal{L}_b$$

and

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

is the category of unipotent $\mathbb{Q}_p$-lisse sheaves on $\bar{X}_{et}$.

$$U_n^{et} = (U^{et})^n \backslash U^{et}$$

where the descending central series on U is given by $U^1 = U$, $U^{n+1} = [U, U^n]$.

For another $x \in X(\mathbb{Q})$, define the *torsor of unipotent paths*:

$$P^{et}(x) := \mathrm{Isom}^{\otimes}(F_b^u, F_x^u)$$

These also carry compatible Γ-actions making them into Γ-equivariant U^{et}-torsors. Classified by a Selmer pro-variety

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

with finite-dimensional quotients

$$H^1_f(\Gamma, U^{et}_n)$$

The Kummer map is defined in the natural way:

$$\kappa^u : X(\mathbb{Q}) \rightarrow H^1_f(\Gamma, U^{et})$$

$$x \mapsto [P^{et}(x)]$$

and the ones κ^u_n at finite level by composing:

$$\begin{array}{ccc} X & \xrightarrow{\kappa^u} & H^1_f(\Gamma, U^{et}) \\ & \searrow^{\kappa^u_n} & \downarrow \\ & & H^1_f(\Gamma, U^{et}_n) \end{array}$$

Remark: In contrast to the pro-finite case, we have *local conditions.*

If S is the set of primes of bad reduction for X, we take $p \notin S$. The torsors in $H^1_f(\Gamma, U^{et})$ are required to be unramified at all primes $l \notin \{p\} \cup S$ and crystalline at p.

The last condition is already suggestive of the motivic technology that makes κ^u more accessible than $\hat{\kappa}$.

In fact, hope of controlling Selmer variety comes from the diagram:

$$
\begin{array}{ccccc}
X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\
\downarrow \kappa_n^u & & \downarrow \kappa_{n,loc}^u & \searrow \kappa_{dr,n}^u & \\
H^1_f(\Gamma, U_n^{et}) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n^{et}) & \xrightarrow{\log} & U_n^{DR}/F^0
\end{array}
$$

As in Kato, loc_p should capture most of the content of the Selmer variety. Can analyze image using non-abelian p-adic Hodge theory, i.e., the log map.

Remarks: (1) Target is a classifying space for *De Rham torsors*, i.e., torsors for the De Rham fundamental group U^{dr} with basepoint b, classifying unipotent flat connections on $X \otimes \mathbb{Q}_p$. For points $x \in X(\mathbb{Q}_p)$ we also have De Rham path spaces $P^{dr}(x)$ defined in the obvious manner. They carry compatible Hodge filtrations, and Frobenius actions coming from comparisons with U^{cr} and $P^{cr}(\bar{x})$ defined using convergent iso-crystals on the special fiber. Such torsors have a canonical Frobenius invariant element $p^{cr} \in P^{dr}$ and we can choose an element $p^H \in F^0 P^{dr}$. Comparison between the two turns

$$U^{dr}/F^0$$

into a classifying space for such torsors. Then the map

$$k^u_{dr} : X(\mathbb{Q}_p) \rightarrow U^{dr}/F^0$$

sends x to $[P^{dr}(x)]$.

(2) The space $H^1_f(G_p, U^{et})$ classifies G_p- equivariant torsors for U^{et} which are crystalline, i.e., trivialized when base-changed to B_{cr}. The maps κ^u_{loc} and loc_p are the evident ones.

(3) The map log associates to a crystalline U^{et}-torsor

$$P^{et} = \mathrm{Spec}(\mathcal{P}^{et})$$

the U^{dr}-torsor

$$\log(P^{et}) := \mathrm{Spec}((\mathcal{P}^{et} \otimes B_{cr})^{G_p})$$

(4) The fact that $\kappa^u_{loc}(x)$ is a crystalline torsor and that the diagram commutes is due to many people Shiho, Vologodsky, Olsson, Faltings, ...

(5) Maps between classifying spaces are all algebraic. But maps from points are highly transcendental. In fact, image of $X(\mathbb{Q}_p)$ via κ^u_{dr} is Zariski dense. Coordinates are described by Coleman functions, i.e., iterated integrals of rigid analytic functions.

(6) There is an affine analogue related to local and global integral points. In fact, will incorporate that version into the discussion without introducing additional notation. For $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ the coordinates of κ^u_{dr} are p-adic multiple polylogarithms.

(7) All the U's are components of the *motivic fundamental group* U^M. Underlying idea is

$$X(\mathbb{Q}) \rightarrow \text{classifying space for motivic torsors}$$

$$x \mapsto P^M(x)$$

Goal: Control the image

$$\mathrm{Im}_n[H^1_f(\Gamma, U_n^{et})]$$

of global Selmer variety inside U_n^{dr}/F^0.

In fact, would like to show that

$$(*) \qquad \mathrm{Im}_n[H^1_f(\Gamma, U^{et}_n)] \text{ is } \textit{not} \text{ Zariski dense for some } n.$$

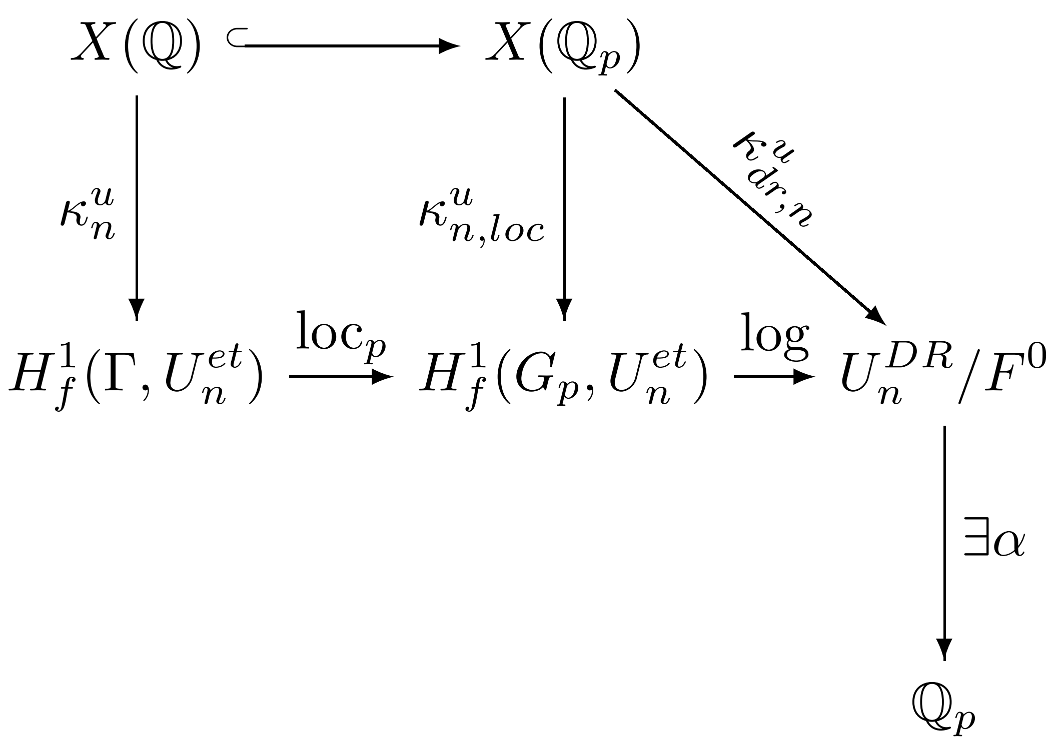
This statement (*) implies that

$$\mathrm{Im}_n[H^1_f(\Gamma, U^{et}_n)] \cap \mathrm{Im}_n[X(\mathbb{Q}_p)]$$

is finite, and hence, that

$$X(\mathbb{Q})$$

is finite.



$$\alpha|\mathrm{Im}_n[H_f^1(\Gamma, U_n^{et})] = 0$$

$$\alpha|\mathrm{Im}_n[X(\mathbb{Q}_p)] \neq 0$$

We see thus the relevance of non-abelian torsor spaces, i.e, *constructions* that occure in the section conjecture, to Diophantine finiteness.

Note the usefulness of a 'BSD(=motivic)' viewpoint.

For motivic *statements* of the section conjecture variety, recall:

(Bloch-Kato) If $V/\mathbb{Q}$ is a smooth projective variety. Then

$$ch_{n,r} : K^{(r)}_{2r-n-1}(V) \otimes \mathbb{Q}_p \rightarrow H^1_g(\Gamma, H^n(\bar{V}, \mathbb{Q}_p(r)))$$

is surjective.

(Fontaine-Mazur) If $V/\mathbb{Q}$ is a smooth projective variety. Then

$$\text{Mixed Motives} \rightarrow H^1_g(\Gamma, H^n(\bar{V}, \mathbb{Q}_p(r)))$$

is surjective.

Apply to $H^n(\bar{X}^n, \mathbb{Q}_p(n+1))$.

Then either of these implies (*), and hence, finiteness.

Can prove (*) for

-curves of genus zero (minus at least three points).

-$X = E \setminus \{e\}$ where $E/\mathbb{Q}$ is an elliptic curve of rank one, with a naturally modified Selmer variety. (Appropriate for finiteness.)

-special Galois-theoretic circumstances, e.g. if $\mathbb{Q}(J_X[p])$ has trivial p-ideal class group.

Outline of genus one, rank one case. (Joint with A. Tamagawa)

Inductive structure:

$$0 \rightarrow U^3 \backslash U^2 \rightarrow U_3 \rightarrow U_2 \rightarrow 0$$

In the étale realization, get

$$0 \rightarrow H^1_f(\Gamma, (U^{et})^3 \backslash (U^{et})^2) \rightarrow H^1_f(\Gamma, U^{et}_3) \rightarrow H^1_f(\Gamma, U^{et}_2) \rightarrow$$

But the image $\kappa_3^u(X(\mathbb{Z}))$ lies inside a subvariety

$$H^1_{0,\Sigma} \subset H^1_f(\Gamma, U^3 \backslash U)$$

defined by the intersection of

(a) $\mathrm{loc}_l^{-1}(0)$ for all $l \notin \{p\} \cup S$.

(b) $(\prod_{l \in S} \mathrm{loc}_l)^{-1}(\Sigma)$ for a finite subset

$$\Sigma \subset \prod_{l \in S} H^1(G_l, U_3)$$

This follows from a general fact: Let $l \neq p$ and

$$\mathcal{Y} \rightarrow \mathrm{Spec}(\mathbb{Z}_l)$$

a flat regular curve with smooth generic fiber Y. Then for any n, the image of

$$\mathcal{Y}(\mathbb{Z}_l) \rightarrow H^1(G_l, U_n^{et})$$

is finite. This is an analogue of the vanishing of this map when $n = 2$.

Thus, we actually have an exact sequence

$$0 \to H^1_{0,\Sigma}(\Gamma, (U^{et})^3 \backslash (U^{et})^2) \to H^1_{0,\Sigma}(\Gamma, U_3^{et}) \to H^1_f(\Gamma, U_2^{et})$$

(in naive sense) and the fibers of the second map have form

$$H^1_{0,\Sigma+v}((U^{et})^3 \backslash (U^{et})^2)$$

for some $v \in H^1_{0,\Sigma}(\Gamma, U_3^{et})$.

Because $U^3 \backslash U^2 \simeq \mathbb{Q}_p(1)$ for $E \setminus \{0\}$, The fibers are finite.

So the Zariski closure of $\kappa_3^u(X(\mathbb{Z}))$ is quasi-finite over the closure of $\kappa_2^u(X(\mathbb{Z})) \subset \kappa_2^u(X(\mathbb{Q}))$ which has dimension ≤ 1. Therefore,

$$\dim \overline{\kappa_3^u(X(\mathbb{Z}))} \leq 1$$

One the other hand, the dimension of U_3^{dr}/F^0 can be computed with a recursive formula for

$$d_n = \dim(U^{n+1} \backslash U^n)$$

$$\Sigma_{i \leq n} i d_i = \left(\begin{array}{cc} (2g)^n & \text{(affine case)} \\ (g+\sqrt{g^2-1})^n + (g-\sqrt{g^2-1})^n & \text{(compact case)} \end{array} \right.$$

From this, one computes $\dim U_3^{dr}/F^0 = 2$. Thus,

$$\mathrm{Im}_3(\kappa_3^u(\mathbb{Z}))$$

is not Zariski-dense.

Remark: If we assume analytic rank 1, then $\mathrm{Im}_3[H^1_{0,\Sigma}(\Gamma, U_3^{et})]$ is itself not dense.

The implications mentioned above all follow a similar pattern, except B-K or F-M is used to show that

$$\dim H^1_f(\Gamma, U_n^{et}) < U_n^{dr}/F^0$$

for n sufficiently large (effectively computable).

Computation of dimension uses Euler characteristic formula

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

and control of H^2 provided by B-K or F-M.

Direct bound for H^2 in genus zero case.

All such methods (would) show *existence* of a function that vanishes on the image of $H^1_f(\Gamma, U_n^{et})$ (or a modification). Can perhaps hope to find one by *computation* of the map

$$H^1_f(\Gamma, U_n^{et}) \rightarrow U_n^{dr}/F^0$$

Theoretical alternative: Geometrically *produce* a function that vanishes on $\mathrm{Im}_n(H^1_f(\Gamma, U_n^{et}))$?

Requires a more serious development of non-abelian BSD program.

Some speculative comments on duality.

-There is a pairing:

$$< \cdot, \cdot >_l : H^1(G_l, U_n^{et}) \times Ext^1_{G_l}(U_n^{et}, \mathbb{Q}_p(1)) \rightarrow \mathbb{Q}_p$$

for all l.

-Points in $X(\mathbb{Q}_l)$ give rise to classes in both sets that annihilate each other.

-If $a \in H^1(\Gamma_T, U_n^{et})$ and $b \in Ext^1_{\Gamma_T}(U_n^{et}, \mathbb{Q}_p(1))$ are global classes, then

$$\Sigma_l < \mathrm{loc}_l(a), \mathrm{loc}_l(b) >= 0$$

Note that if a is the class of a point, this corresponds to a finite set of equations at p, one of which is satisfied by $\mathrm{loc}_p(a)$.

Unfortunately, all classes in

$$Ext^1_\Gamma(U_n^{et}, \mathbb{Q}_p(1))$$

come from

$$Ext^1_\Gamma(U_2^{et}, \mathbb{Q}_p(1))$$

Need a much more non-linear construction.

$$\text{60's Grothendieck} \overset{vs}{\leftrightarrow} \text{80's Grothendieck}$$

60's: Motives.

80's: Disdains motives and favors π_1. Possibly observing the failure of the motivic theory to describe *non-abelian Diophantine sets* (letter to Faltings). That is, it almost never says anything about $X(\mathbb{Q})$.

$$\text{motives} \overset{vs}{\leftrightarrow} \text{anabelian geometry}$$

Moral: Importance of *the middle way*.