Diophantine geometry and non-abelian duality

Minhyong Kim

Kavli Centre, May, 2011

▲□▶ ▲圖▶ ▲臣▶ ★臣▶ ―臣 …の�?

Diophantine geometry and abelian cohomology

E: elliptic curve over a number field F.

Kummer theory:

$$E(F) \otimes \mathbb{Z}_p \longrightarrow H^1_f(G, T_p(E))$$

conjectured to be an isomorphism.

Should allow us, in principle, to compute E(F).

Furthermore, size of $H_f^1(G, T_p(E))$ should be controlled by an *L*-function.

In the theorem

$$L(E/\mathbb{Q},1) \neq 0 \Rightarrow |E(\mathbb{Q})| < \infty,$$

key point is that the image of

$$\operatorname{loc}_{p}: H^{1}_{f}(G, T_{p}(E)) \longrightarrow H^{1}_{f}(G_{p}, T_{p}(E))$$

is annihilated using Poitou-Tate duality by a class

$$c \in H^1(G, T_p(E))$$

whose image in

$$H^1(G_p, T_p(E))/H^1_f(G_p, T_p(E))$$

is non-torsion.

An explicit local reciprocity law then translates this into an analytic function on $E(\mathbb{Q}_p)$ that annihilates $E(\mathbb{Q})$.

Wish to investigate an extension of this phenomenon to hyperbolic curves. That is, curves of

-genus zero minus at least three points;

-genus one minus at least one point;

-genus at least two.

Notation

- F: Number field.
- S_0 : finite set of primes of F.

 $R := \mathcal{O}_F[1/S_0]$, the ring of S integers in F.

 $p{:}$ odd prime not divisible by primes in $S_0;$ $v{:}$ a prime of F above p with $F_v=\mathbb{Q}_p{.}.$

 $G := \operatorname{Gal}(\overline{F}/F).$

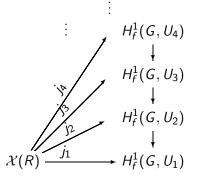
 $G_S := \text{Gal}(F_S/F)$, where F_S is the maximal extension of F unramified outside $S = S_0 \cup \{v|p\}$. \mathcal{X} : smooth curve over Spec(R) with good compactification.

(Might be compact itself.)

X: generic fiber of \mathcal{X} , assumed to be hyperbolic.

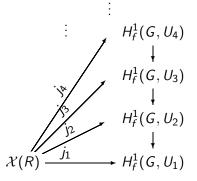
 $b \in \mathcal{X}(R)$, possibly tangential.

Unipotent descent tower



◆□▶ ◆□▶ ◆臣▶ ◆臣▶ ─臣 ─の�@

Unipotent descent tower



Here,

$$j: x \in \mathcal{X}(R) \mapsto [P(x)] \in H^1_f(G, U),$$

(日) (四) (日) (日)

э

is the \mathbb{Q}_p -unipotent étale period map.

U is the \mathbb{Q}_p -pro-unipotent étale fundamental group of

$$ar{X} = X imes_{\operatorname{\mathsf{Spec}}(F)} \operatorname{\mathsf{Spec}}(ar{F})$$

with base-point b.

A linearization of the profinite étale fundamental group $\hat{\pi}_1(\bar{X}, b)$:

$$U = ``\hat{\pi}_1(\bar{X}, b) \otimes \mathbb{Q}_p".$$

Unipotent descent tower

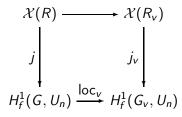
 $U_n := U^{n+1} \setminus U$, where U^n is the lower central series with $U^1 = U$. So $U_1 = U^{ab} = T_p J_X \otimes \mathbb{Q}_p$.

 $P(x) := \hat{\pi}_1(\bar{X}; b, x) \times_{\hat{\pi}_1(\bar{X}, b)} U$, is the *U*-torsor of \mathbb{Q}_p -unipotent étale paths from *b* to *x*, viewed as a function of *x*.

All these objects have natural actions of G.

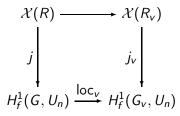
 H_f^1 refers to continuous non-abelian cohomology of G with coefficients in U satisfying local 'Selmer conditions'.

Localization



◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

Localization



Goal: Compute the image of loc_{ν} .

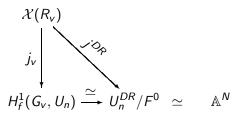
・ロト ・ 日 ・ モート ・ 日 ・ うへつ

Local period map

One essential fact is that the local map

$$\mathcal{X}(R_v) \xrightarrow{j_v} H^1_f(G_v, U_n)$$

can be computed via a diagram



where U_n^{DR}/F^0 is a homogeneous space for the *De Rham-crystalline fundamental group*, and the map j^{DR} can be described explicitly using *p*-adic iterated integrals.

Non-abelian method of Chabauty

Meanwhile, the localization map is an algebraic map of varieties over \mathbb{Q}_p making it feasible, in principle, to discuss its computation.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Non-abelian method of Chabauty

Meanwhile, the localization map is an algebraic map of varieties over \mathbb{Q}_p making it feasible, in principle, to discuss its computation. Knowledge of

$$\mathit{Im}(\mathsf{loc}_v) \subset H^1_f(G_v, U_n)$$

will lead to knowledge of

$$\mathcal{X}(R) \subset [j_{v}]^{-1}(\mathit{Im}(\mathsf{loc}_{v})) \subset \mathcal{X}(R_{v}).$$

For example, when $Im(loc_v)$ is not Zariski dense, immediately deduce finiteness of $\mathcal{X}(R)$.

Non-abelian method of Chabauty

This deduction is captured by the diagram

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

such that $\psi \circ j_{\nu}^{et}$ kills $\mathcal{X}(R)$.

Some cases of Diophantine finiteness

Can use this to give a new proof of finiteness of points in some cases:

 $F = \mathbb{Q}$ and the Jacobian of X has potential CM. (joint with John Coates)

 $F = \mathbb{Q}$ and X, elliptic curve minus one point.

F totally real and X of genus zero.

Some cases of Diophantine finiteness

Can use this to give a new proof of finiteness of points in some cases:

 $F = \mathbb{Q}$ and the Jacobian of X has potential CM. (joint with John Coates)

 $F = \mathbb{Q}$ and X, elliptic curve minus one point.

F totally real and X of genus zero.

But would like to *construct* ψ in some canonical fashion.

Non-abelian duality?

◆□▶
◆□▶
●□▶
●□▶
●□▶
●□▶
●□▶
●□▶
●□▶

Non-abelian duality?

Alternatively, $Im(loc_v)$ should be computed using a sort of *non-abelian Poitou-Tate duality.*

▲□▶ ▲圖▶ ▲臣▶ ★臣▶ ―臣 …の�?

Alternatively, $Im(loc_v)$ should be computed using a sort of *non-abelian Poitou-Tate duality.*

In the elliptic curve case, we know that Poitou-Tate duality is the basic tool for computing the global image inside local cohomology. Would like a non-abelian analogue.

ション ふゆ くりょう しょう くうく

Alternatively, $Im(loc_v)$ should be computed using a sort of *non-abelian Poitou-Tate duality.*

In the elliptic curve case, we know that Poitou-Tate duality is the basic tool for computing the global image inside local cohomology. Would like a non-abelian analogue.

ション ふゆ くりょう しょう くうく

Duality for Galois cohomology with coefficients in various non-abelian groups should also be interpreted as a sort of *non-abelian class field theory.*

 E/\mathbb{Q} : elliptic curve with

 $\mathsf{rank}E(\mathbb{Q}) = 1,$

trivial Tamagawa numbers, and

 $|\mathrm{III}(E)[p^\infty]|<\infty$

for a prime p of good reduction.

 $X =: E \setminus \{0\}$ given as a minimal Weierstrass model:

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 x$$

So

$$X(\mathbb{Z}) \subset E(\mathbb{Z}) = E(\mathbb{Q}).$$

Let

$$\alpha = dx/(2y + a_1x + a_3), \ \beta = xdx/(2y + a_1x + a_3).$$

Get analytic functions on $X(\mathbb{Q}_p)$,

$$\log_{lpha}(z) = \int_{b}^{z} lpha; \quad \log_{eta}(z) = \int_{b}^{z} eta;$$
 $D_{2}(z) = \int_{b}^{z} lpha eta.$

Here, *b* is a tangential base-point at 0, and the integral is (iterated) *Coleman integration*.

Locally, the integrals are just anti-derivatives of the forms, while for the iteration,

$$dD_2 = \left(\int_b^2 \beta\right) \alpha.$$

Theorem

Suppose there is a point $y \in X(\mathbb{Z})$ of infinite order in $E(\mathbb{Q})$. Then the subset

 $X(\mathbb{Z}) \subset X(\mathbb{Q}_p)$

lies in the zero set of the analytic function

$$\psi(z) := D_2(z) - \frac{D_2(y)}{(\int_b^y \alpha)^2} (\int_b^z \alpha)^2.$$

◆□▶ ◆□▶ ★□▶ ★□▶ □ のQ@

Theorem

Suppose there is a point $y \in X(\mathbb{Z})$ of infinite order in $E(\mathbb{Q})$. Then the subset

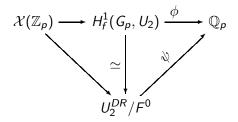
 $X(\mathbb{Z}) \subset X(\mathbb{Q}_p)$

lies in the zero set of the analytic function

$$\psi(z) := D_2(z) - \frac{D_2(y)}{(\int_b^y \alpha)^2} (\int_b^z \alpha)^2.$$

A fragment of non-abelian duality and explicit reciprocity.

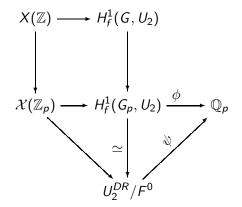
Function ψ is actually a composition



where ϕ is constructed using secondary cohomology products and has the property that

$$\phi(\mathsf{loc}_p(H^1_f(G, U_2))) = 0.$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●



《曰》 《圖》 《臣》 《臣》

3

 $U_2 \simeq V \times \mathbb{Q}_p(1)$

where $V = T_p(E) \otimes \mathbb{Q}_p$, with group law

$$(X, a)(Y, b) = (X + Y, a + b + (1/2) < X, Y >).$$

A function

$$\mathsf{a}=(\mathsf{a}_1,\mathsf{a}_2)$$
 : $\mathsf{G}_{\mathsf{p}}{
ightarrow} U_2$

is a cocycle if and only if

$$da_1 = 0; \quad da_2 = -(1/2)[a_1, a_1].$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

For $a = (a_1, a_2) \in H^1_f(G_p, U_2)$, we define

 $\phi(a_1,a_2) := [b,a_1] + \log \chi_p \cup (-2a_2) \in H^2(\mathcal{G}_p,\mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

For
$$a = (a_1, a_2) \in H^1_f(G_p, U_2)$$
, we define

$$\phi(\mathsf{a}_1,\mathsf{a}_2) := [b,\mathsf{a}_1] + \log \chi_p \cup (-2\mathsf{a}_2) \in H^2(\mathcal{G}_p,\mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

where

$$\log \chi_p : G_p \to \mathbb{Q}_p$$

is the logarithm of the *p*-adic cyclotomic character and

$$b: G \rightarrow V$$

is a solution to the equation

$$db = \log \chi_p \cup a_1.$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

The annihilation comes from the standard exact sequence

$$0{\rightarrow} H^2(G,\mathbb{Q}_p(1)){\rightarrow} \sum_{v} H^2(G_v,\mathbb{Q}_p(1)){\rightarrow} \mathbb{Q}_p{\rightarrow} 0.$$

That is, our assumptions imply that the class

 $[\pi_1(\bar{X};b,x)]_2$

for $x \in X(\mathbb{Z})$ is trivial at all places $l \neq p$. On the other hand

 $\phi(\mathsf{loc}_p([\pi_1(\bar{X}; b, x)]_2)) = \mathsf{loc}_p(\phi^{glob}([\pi_1(\bar{X}; b, x)]_2)).$

With respect to the coordinates

$$H^1_f(G_p, U_2) \simeq U_2^{DR}/F^0 \simeq \mathbb{A}^2 = \{(s, t)\}$$

the image

$$\mathsf{loc}_p(H^1_f(G, U_2)) \subset H^1_f(G_p, U_2)$$

is described by the equation

$$t - \frac{D_2(y)}{(\int_b^y \alpha)^2} s^2 = 0.$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Let

$$L = \oplus_{n \in (n)} L_n$$

graded Lie algebra over field k. The map $D: L \rightarrow L$ such that

 $D|L_n = n$

is a derivation, i.e., an element of $H^1(L, L)$. Can be viewed as an element of $H^2(L^* \rtimes L, k)$, that is, a central extension of $L^* \rtimes L$:

$$0 \longrightarrow k \longrightarrow E' \longrightarrow L^* \rtimes L \longrightarrow 0.$$

Explicitly described as follows:

 $[(a, \alpha, X), (b, \beta, Y)] = (\alpha(D(Y)) - \beta(D(X)), ad_X(\beta) - ad_Y(\alpha), [X, Y]).$

When $L = L_1$ and D = I, then this gives a standard Heisenberg extension.

Explicitly described as follows:

 $[(a, \alpha, X), (b, \beta, Y)] = (\alpha(D(Y)) - \beta(D(X)), ad_X(\beta) - ad_Y(\alpha), [X, Y]).$

When $L = L_1$ and D = I, then this gives a standard Heisenberg extension.

When $k = \mathbb{Q}_p$ and we are given an action of G or G_v , can twist to

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow E \longrightarrow L^*(1) \rtimes L \longrightarrow 0.$$

Also have a corresponding group extension

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow \mathcal{E} \longrightarrow L^*(1) \rtimes U \rightarrow 0.$$

(L = Lie(U))

From this, we get a boundary map

$$H^1(G_v, L^*(1) \rtimes U) \xrightarrow{\delta} H^2(G_v, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p.$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

This boundary map should form the basis of (unipotent) non-abelian duality.

Non-abelian duality: abstract framework

From this, we get a boundary map

$$H^1(G_v, L^*(1) \rtimes U) \xrightarrow{\delta} H^2(G_v, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p.$$

This boundary map should form the basis of (unipotent) non-abelian duality.

$$H^{1}(G_{\nu}, L^{*}(1)) \longrightarrow H^{1}(G_{\nu}, L^{*}(1) \rtimes U) \xrightarrow{\delta} \mathbb{Q}_{p}$$

$$\downarrow$$

$$H^{1}(G_{\nu}, U)$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Non-abelian duality: difficulties

1. We would like a function on

 $H^1_f(G_v, U),$

depending on a class in $H^1(G_v, L^*(1))$. Hence, need some splitting of

$$H^1(G_v, L^*(1) \rtimes U) \longrightarrow H^1(G_v, U).$$

Non-abelian duality: difficulties

1. We would like a function on

$$H^1_f(G_v, U),$$

depending on a class in $H^1(G_v, L^*(1))$. Hence, need some splitting of

$$H^1(G_{\nu}, L^*(1) \rtimes U) \longrightarrow H^1(G_{\nu}, U).$$

2. When U is a unipotent fundamental group, L is not graded in way that's compatible with the Galois action.

This second difficulty is resolved by Hain's theory of weighted completions.

This second difficulty is resolved by Hain's theory of weighted completions.

For the subsequent discussion, v is any prime in S. Let R_v be the Zariski closure of the image of

 $G_{v} \rightarrow \operatorname{Aut}(H_{1}(\bar{X}, \mathbb{Q}_{p})).$

This second difficulty is resolved by Hain's theory of weighted completions.

For the subsequent discussion, v is any prime in S. Let R_v be the Zariski closure of the image of

 $G_{v} \rightarrow \operatorname{Aut}(H_{1}(\bar{X}, \mathbb{Q}_{p})).$

Assume $\mathbb{G}_m \subset R_v$.

This second difficulty is resolved by Hain's theory of weighted completions.

For the subsequent discussion, v is any prime in S. Let R_v be the Zariski closure of the image of

 $G_{v} \rightarrow \operatorname{Aut}(H_{1}(\bar{X}, \mathbb{Q}_{p})).$

Assume $\mathbb{G}_m \subset R_v$.

Key statement:

 $H^1(G_v, U) \simeq H^1(\mathcal{G}_v, U)) \simeq H^1(Gr_W(\mathcal{G}_v), Gr_W(U))$

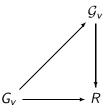
where \mathcal{G}_{v} is the weighted completion of \mathcal{G}_{v} .

Basic idea:

Consider the universal pro-algebraic extension

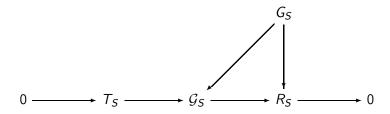
$$0 \rightarrow T_v \rightarrow G_v \rightarrow R_v \rightarrow 0$$

equipped with a lift



such that T_v is pro-unipotent and the action of \mathbb{G}_m on $H_1(T_v)$ has negative weights.

Note: Similar compatible construction G_S for G_S :



Then

$$\begin{array}{rcl} H^{1}(G_{S},U) &\simeq & H^{1}(\mathcal{G}_{S},U) \\ \downarrow & & \downarrow \\ H^{1}(G_{v},Gr^{W}(U)) &\simeq & H^{1}(\mathcal{G}_{v},Gr^{W}(U)). \\ H^{1}(G_{S},L^{*}(1)\rtimes U) &\simeq & H^{1}(\mathcal{G}_{S},Gr^{W}(L^{*}(1))\rtimes Gr^{W}(U)) \\ \downarrow & & \downarrow \\ H^{1}(G_{v},L^{*}(1)\rtimes U) &\simeq & H^{1}(\mathcal{G}_{v},Gr^{W}(L^{*}(1))\rtimes Gr^{W}(U)). \end{array}$$
and

 $H^{1}(\mathcal{G}_{S}, Gr^{W}(L^{*}(1)) \rtimes Gr^{W}(U)) \simeq H^{1}(Gr_{W}(\mathcal{G}_{S}), Gr^{W}(L^{*}(1)) \rtimes Gr^{W}(U));$ $H^{1}(\mathcal{G}_{v}, Gr^{W}(L^{*}(1)) \rtimes Gr^{W}(U)) \simeq H^{1}(Gr_{W}(\mathcal{G}_{v}), Gr^{W}(L^{*}(1)) \rtimes Gr^{W}(U))$

Recalling the interpretation of $H^1(\mathcal{G}_v, U)$ as the splittings of

$$0 \rightarrow U \rightarrow U \rtimes \mathcal{G}_{v} \rightarrow \mathcal{G}_{v} \rightarrow 0,$$

we find there are isomorphisms

 $\begin{aligned} H^{1}(\mathcal{G}_{v},U) &\simeq Split_{W}(Gr_{W}(Lie\mathcal{G}_{v}),Gr_{W}(L)\rtimes Gr_{W}(Lie\mathcal{G}_{v})). \\ H^{1}(\mathcal{G}_{v},L^{*}(1)\rtimes U) &\simeq \\ Split_{W}(Gr_{W}(Lie\mathcal{G}_{v}),Gr_{W}(L^{*}(1))\rtimes Gr_{W}(L)\rtimes Gr_{W}(Lie\mathcal{G}_{v})). \end{aligned}$

Theorem There is a canonical central extension

 $0 \rightarrow \mathbb{Q}_{p}(1) \rightarrow \mathcal{E} \rightarrow Gr_{W}(L^{*}(1)) \rtimes Gr_{W}(L) \rtimes Gr_{W}(Lie\mathcal{G}_{v}) \rightarrow 0$

giving rise to a boundary map

 $H^1(G_v, L^*(1) \rtimes U)$

 $\simeq Split_{W}(Gr_{W}(Lie\mathcal{G}_{v}), Gr_{W}(L^{*}(1)) \rtimes Gr_{W}(L) \rtimes Gr_{W}(Lie\mathcal{G}_{v}))$ $\rightarrow H^{2}(G_{v}, \mathbb{Q}_{p}(1)).$

Managed to construct the diagram

$$H^{1}(G_{\nu}, L^{*}(1)) \longrightarrow H^{1}(G_{\nu}, L^{*}(1) \rtimes U) \xrightarrow{\delta_{\nu}} \mathbb{Q}_{p}$$

$$\downarrow$$

$$H^{1}(G_{\nu}, U)$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

in general.

Theorem The image of $H^1(G_S, L^*(1) \rtimes U)$ in $\prod_{v \in S} H^1(G_v, L^*(1) \rtimes U)$ is annihilated by

 $\sum \delta_{\mathbf{v}}.$

◆□▶ ◆□▶ ★□▶ ★□▶ □ のQ@