## Diophantine Geometry, Fundamental Groups, and Non-Abelian Reciprocity

Minhyong Kim

Cambridge, March, 2015



Figure: John Coates at 700

## Diophantine Geometry: Abelian Case

The Hasse-Minkowski theorem says that

$$ax^2 + by^2 = c$$

has a solution in a number field F and only if it has a solution in  $F_v$  for all v.

There are straightforward algorithms for determining this. For example, we need only check for  $v = \infty$  and v|2abc, and there, a solution exists if and only if

$$(a,b)_v(b,c)_v(c,a)_v(c,-1)_v = 1.$$

Diophantine Geometry: Main Local-to-Global Problem

Locate

$$X(F) \subset X(\mathbb{A}_F) = \prod_{v}' X(F_v)$$

The question is

How do the global points sit inside the local points?

In fact, there is a classical answer of satisfactory sort for conic equations.

Diophantine Geometry: Main Local-to-Global Problem

In that case, assume for simplicity that there is a rational point (and that the points at infinity are rational), so that

$$X\simeq \mathbb{G}_m.$$

Then

$$X(F)=F^*,\quad X(F_v)=F_v^*.$$

Problem becomes that of locating

$$F^* \subset \mathbb{A}_F^{\times}$$
.

Diophantine Geometry: Abelian Class Field Theory

We have the Artin reciprocity map

$$\operatorname{Rec} = \prod_{v} \operatorname{Rec}_{v} : \mathbb{A}_{F}^{\times} \longrightarrow G_{F}^{ab}.$$

Here,

$$G_F^{ab} = \operatorname{Gal}(F^{ab}/F),$$

and

F<sup>ab</sup>

is the maximal abelian algebraic extension of F.

Diophantine Geometry: Abelian Class Field Theory

Artin's reciprocity law:

The map

$$F^* \hookrightarrow \mathbb{A}_F^{\times} \xrightarrow{\mathsf{Rec}} G_F^{ab}$$

is zero.

That is, the reciprocity map gives a *defining equation for*  $\mathbb{G}_m(F)$ .

We would like to generalize this to other equations by way of a *non-abelian reciprocity law*.

Start with a rather general variety  $\boldsymbol{X}$  for which we would like to understand

X(F)

via

$$X(F) \hookrightarrow X(\mathbb{A}_F) \xrightarrow{\mathsf{Rec}^{NA}} \text{ some target with base-point 0}$$

in such way that

$$\operatorname{Rec}^{NA} = 0$$

becomes an equation for X(F).

To rephrase: we would like to construct *class field theory with coefficients in a general variety* X generalizing CFT with coefficients in  $\mathbb{G}_m$ 

Will describe a version that works for smooth hyperbolic curves.

(Joint with Jonathan Pridham)

Notation:

 $\begin{array}{l} F: \mbox{ number field.} \\ G_F = \mbox{Gal}(\bar{F}/F). \\ G_v = \mbox{Gal}(\bar{F}_v/F_v) \mbox{ for a place } v \mbox{ of } F. \\ S: \mbox{ finite set of places of } F. \\ \mathbb{A}_F: \mbox{ Adeles of } F \\ \mathbb{A}_F^S: \mbox{ S-integral adeles of } F. \\ G_F^S = \mbox{Gal}(F^S/F), \mbox{ where } F^S \mbox{ is the maximal extension of } F \\ \mbox{ unramified outside } S. \end{array}$ 

X: a smooth curve over F with genus at least two;  $b \in X(F)$  (sometimes tangential).

$$\Delta = \pi_1(\bar{X}, b)$$
 :

Pro-finite étale fundamental group of  $\bar{X} = X \times_{\text{Spec}(F)} \text{Spec}(\bar{F})$  with base-point *b*.

 $\Delta^{[n]}$ 

Lower central series with  $\Delta^{[1]} = \Delta$ .

$$\Delta_n = \Delta/\Delta^{[n+1]}.$$
  
 $T_n = \Delta^{[n]}/\Delta^{[n+1]}.$ 

We then have a *nilpotent class field theory with coefficients in* X made up of a filtration

$$X(\mathbb{A}_F) = X(\mathbb{A}_F)_1 \supset X(\mathbb{A}_F)_2 \supset X(\mathbb{A}_F)_3 \supset \cdots$$

and a sequence of maps

$$Rec_n: X(\mathbb{A}_F)_n \longrightarrow \mathfrak{G}_n(X)$$

to a sequence  $\mathfrak{G}_n(X)$  of profinite abelian groups in such a way that

$$X(\mathbb{A}_F)_{n+1} = \operatorname{Rec}_n^{-1}(0).$$

. . .

 $Rec_n$  is defined not on all of  $X(\mathbb{A}_F)$ , but only on the kernel (the inverse image of 0) of all the previous  $rec_i$ .

The  $\mathfrak{G}_n(X)$  are defined as

 $\mathfrak{G}_n(X) :=$ 

Hom[ $H^1(G_F, D(T_n)), \mathbb{Q}/\mathbb{Z}$ ]

where

$$D(T_n) = \varinjlim_m \operatorname{Hom}(T_n, \mu_m).$$

When  $X = \mathbb{G}_m$ , then  $\mathfrak{G}_n(X) = 0$  for  $n \ge 2$  and

$$\mathfrak{G}_1 = \operatorname{Hom}[H^1(G_F, D(\hat{\mathbb{Z}}(1))), \mathbb{Q}/\mathbb{Z}]$$
  
=  $\operatorname{Hom}[H^1(G_F, \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z}] = G_F^{ab}.$ 

The reciprocity maps are defined using the local period maps

$$j^{\nu}: X(F_{\nu}) \longrightarrow H^{1}(G_{\nu}, \Delta);$$
$$x \mapsto [\pi_{1}(\bar{X}; b, x)].$$

Because the homotopy classes of étale paths

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

form a torsor for  $\Delta$  with compatible action of  $G_{\nu}$ , we get a corresponding class in non-abelian cohomology of  $G_{\nu}$  with coefficients in  $\Delta$ .

These assemble to a map

$$j^{loc}: X(\mathbb{A}_F) \longrightarrow \prod H^1(G_v, \Delta),$$

which comes in levels

$$j_n^{loc}: X(\mathbb{A}_F) \longrightarrow \prod H^1(G_v, \Delta_n).$$

The first reciprocity map is just defined using

$$x \in X(\mathbb{A}_F) \mapsto d_1(j_1^{loc}(x)),$$

where

$$d_1:\prod^{S}H^1(G_v,\Delta_1^M)\longrightarrow \prod^{S}H^1(G_v,D(\Delta_1^M))^{\vee}\xrightarrow{\mathsf{loc}^*}H^1(G_F^S,D(\Delta_1^M))^{\vee},$$

is obtained from Tate duality and the dual of localization. One needs first to work with a pro-M quotient for a finite set of primes M and  $S \supset M$ . Then take a limit over S and then M.

To define the higher reciprocity maps, we use the exact sequences

$$0 \longrightarrow H^1_c(G^S_F, T^M_{n+1}) \longrightarrow H^1_z(G^S_F, \Delta^M_{n+1}) \longrightarrow H^1_z(G^S_F, \Delta_n)$$
$$\xrightarrow{\delta_{n+1}} H^2_c(G^S_F, T^M_{n+1})$$

for non-abelian cohomology with support and Poitou-Tate duality

$$d_{n+1}: H^2_c(G^S_F, T^M_{n+1}) \simeq H^1(G^S_F, D(T^M_{n+1}))^{\vee}.$$

Essentially,  

$$\begin{aligned} & \operatorname{Rec}_{n+1}^{M} = d_{n+1} \circ \delta_{n+1} \circ \operatorname{loc}^{-1} \circ j_{n}. \\ & x \in X(\mathbb{A}_{F})_{n+1} \xrightarrow{j_{n}^{loc}} \prod_{r=1}^{S} H^{1}(G_{v}, \Delta_{n}^{M}) \xrightarrow{\operatorname{loc}^{-1}} H^{1}_{j_{n}^{loc}(x)}(G_{F}^{S}, \Delta_{n}^{M}) \\ & \xrightarrow{\delta_{n+1}} H^{2}_{c}(G_{F}^{S}, T_{n+1}^{M}) \xrightarrow{d_{n+1}} H^{1}(G_{F}^{S}, D(T_{n+1}^{M}))^{\vee}. \end{aligned}$$

At each stage, take a limit over S and M to get the reciprocity maps.

Put

$$X(\mathbb{A}_F)_{\infty} = \cap_{n=1}^{\infty} X(\mathbb{A}_F)_n.$$

### Theorem (Non-abelian reciprocity)

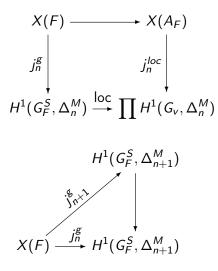
 $X(F) \subset X(\mathbb{A}_F)_{\infty}.$ 

Remark: When  $F = \mathbb{Q}$  and p is a prime of good reduction, suppose there is a finite set T of places such that

$$H^1(G_F^S, \Delta_n^p) \longrightarrow \prod_{v \in T} H^1(G_v, \Delta_n^p)$$

is injective. Then the reciprocity law implies finiteness of X(F).

Non-Abelian Reciprocity: idea of proof



## Non-Abelian Reciprocity: idea of proof

If  $x \in X(\mathbb{A}_F)$  comes from a global point  $x^g \in X(F)$ , then there will be a class

$$j_n^g(x^g) \in H^1_{j_n(x)}(G_F^S, \Delta_n^M)$$

for every n corresponding to the global torsor

$$\pi_1^{et,M}(\bar{X};b,x^g).$$

That is,  $j_n^g(x^g) = \log^{-1}(j_n^{loc}(x))$  and

 $\delta_{n+1}(j_n^g(x^g)) = 0$ 

for every n.

$$Pr_{v}: X(\mathbb{A}_{F}) \longrightarrow X(F_{v})$$

be the projection to the v-adic component of the adeles. Define

1

$$X(F_{\nu})_n := Pr_{\nu}(X(\mathbb{A}_F)_n).$$

#### Thus,

$$X(F_{\nu}) = X(F_{\nu})_1 \supset X(F_{\nu})_2 \supset X(F_{\nu})_3 \supset \cdots \supset X(F_{\nu})_{\infty} \supset X(F).$$

**Conjecture:** Let  $X/\mathbb{Q}$  be a projective smooth curve of genus at least 2. Then for any prime *p* of good reduction, we have

$$X(\mathbb{Q}_p)_{\infty} = X(\mathbb{Q}).$$

Can consider more generally integral points on affine hyperbolic X as well.

**Conjecture:** Let X be an affine smooth curve with non-abelian fundamental group and S a finite set of primes. Then for any prime  $p \notin S$  of good reduction, we have

 $X(\mathbb{Z}[1/S]) = X(\mathbb{Z}_p)_{\infty}.$ 

Should allow us to compute

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

or

$$X(\mathbb{Z}[1/S]) \subset X(\mathbb{Z}_p).$$

Whenever we have an element

$$k_n \in H^1(G_T, \operatorname{Hom}(T_n^M, \mathbb{Q}_p(1))),$$

we get a function

$$X(\mathbb{A}_{\mathbb{Q}})_n \xrightarrow{rec_n} H^1(G_T, D(T_n^M))^{\vee} \xrightarrow{k_n} \mathbb{Q}_p$$

that kills  $X(\mathbb{Q}) \subset X(\mathbb{A}_{\mathbb{Q}})_n$ .

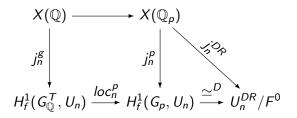
Need an explicit reciprocity law that describes the image

 $X(\mathbb{Q}_p)_n.$ 

Computational approaches all rely on the theory of

U(X, b),

the  $\mathbb{Q}_p$ -pro-unipotent fundamental group of  $\bar{X}$  with Galois action, and the diagram



The key point is that the map

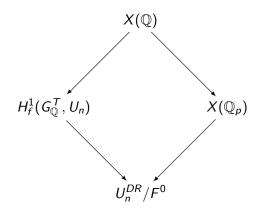
$$X(\mathbb{Q}_p) \xrightarrow{j^{DR}} U^{DR}/F^0$$

can be computed explicitly using iterated integrals, and

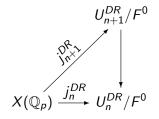
$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_n \subset [j_n^{DR}]^{-1}[\operatorname{Im}(D \circ \operatorname{loc}_n^p)].$$

Two more key facts:

1. As soon as  $D \circ \log_n^p$  has non-dense image,  $X(\mathbb{Q}_p)_n$  is finite. This follows from analytic properties of Coleman functions and the fact that  $j_n^{DR}$  has dense image. That is, in this case,  $Im(j_n^{DR}) \cap Im(D \circ \log_p)$  is finite.



2. If  $\mathcal{A}_n^{DR}$  denotes the coordinate ring of  $U_n^{DR}/F^0$ , then the functions  $[j_{n+1}^{DR}]^*(\mathcal{A}_{n+1}^{DR})$  contains many elements algebraically independent from  $[j_n^{DR}]^*(\mathcal{A}_n^{DR})$ .



Predicted phenomena: At some point  $X(\mathbb{Q}_p)_n$  should be finite, and then one should have a strongly increasing set of functions

 $[J_m^{DR}]^*(I_m^{DR})$ 

for  $m \ge n$  that vanish on  $X(\mathbb{Q})$ .

This is implied, for example, by the Fontaine-Mazur conjecture on geometric Galois representations, which implies

$$\dim[U_n^{DR}/F^0] - \dim[Im(D \circ \log_n^p)] \longrightarrow \infty$$

as *n* grows.

Can prove this for curves X that have CM Jacobians (joint with J. Coates).

A non-abelian conjecture of Birch and Swinnerton-Dyer type: Examples [Joint with Jennifer Balakrishnan, Ishai Dan-Cohen, Stefan Wewers]

Let 
$$\mathcal{X} = \mathbb{P}^1 \setminus \{0, 1, \infty\}$$
. Then  $\mathcal{X}(\mathbb{Z}) = \phi$ .

$$\mathcal{X}(\mathbb{Z}_p)_2 = \{z \mid \log(z) = 0, \log(1-z) = 0\}.$$

Must have  $z = \zeta_n$  and  $1 - z = \zeta_m$ , and hence,  $z = \zeta_6$  or  $z = \zeta_6^{-1}$ .

Thus, if p = 3 or  $p \equiv 2 \mod 3$ , we have

$$\mathcal{X}(\mathbb{Z}_p)_2 = \phi = \mathcal{X}(\mathbb{Z}),$$

so the conjecture holds already at level 2.

When  $p \equiv 1 \mod 3$ 

$$\mathcal{X}(\mathbb{Z}) = \phi \subsetneq \{\zeta_6, \zeta_6^{-1}\} = \mathcal{X}(\mathbb{Z}_p)_2$$

and we must go to a higher level.

Let

$$Li_2(z) = \sum_n \frac{z^n}{n^2}$$

be the *dilogarithm*. Then

$$\mathcal{X}(\mathbb{Z}_p)_3 = \{z \mid \log(z) = 0, \log(1-z) = 0, Li_2(z) = 0\}.$$

and the conjecture is true for  $\mathcal{X}(\mathbb{Z})$  if

 $Li_2(\zeta_6) \neq 0.$ 

Can check this numerically for all 2 .

Let  $\mathcal{X} = \mathcal{E} \setminus O$  where  $\mathcal{E}$  is a semi-stable elliptic curve of rank 0 and  $|\mathrm{III}(\mathcal{E})(p)| < \infty$ .

$$\log(z) = \int_b^z (dx/y).$$

(b is a tangential base-point.)

Then

$$\mathcal{X}(\mathbb{Z}_p)_2 = \{z \in X(\mathbb{Z}_p) \mid \log(z) = 0\} = \mathcal{E}(\mathbb{Z}_p)[tor] \setminus O.$$

For small p, it happens frequently that

$$\mathcal{E}(\mathbb{Z})[tor] = \mathcal{E}(\mathbb{Z}_p)[tor]$$

and hence that

$$\mathcal{X}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}_p)_2.$$

But of course, this fails as p grows.

Must then examine the inclusion

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)_3.$$

Let

$$D_2(z) = \int_b^z (dx/y)(xdx/y).$$

Let S be the set of primes of bad reduction. For each  $I \in S$ , let

$$N_I = \operatorname{ord}_I(\Delta_{\mathcal{E}}),$$

where  $\Delta_{\mathcal{E}}$  is the minimal discriminant. Define a set

$$W_{l} := \{ (n(N_{l} - n)/2N_{l}) \log l \mid 0 \le n < N_{l} \},\$$

and for each  $w = (w_l)_{l \in S} \in W := \prod_{l \in S} W_l$ , define

$$\|w\|=\sum_{I\in S}w_I.$$

## Theorem

Suppose  $\mathcal{E}$  has rank zero and that  $\amalg_E[p^{\infty}] < \infty$ . With assumptions as above

$$\mathcal{X}(\mathbb{Z}_p)_3 = \cup_{w \in W} \Psi(w),$$

where

$$\Psi(w) := \{ z \in \mathcal{X}(\mathbb{Z}_p) \mid \log(z) = 0, \ D_2(z) = \|w\| \}.$$

Of course,

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)_3,$$

but depending on the reduction of  $\mathcal{E}$ , the latter could be made up of a large number of  $\Psi(w)$ , creating potential for some discrepancy.

The curve

$$y^2 + xy = x^3 - x^2 - 1062x + 13590$$

has integral points

$$(19, -9), (19, -10).$$

We find

$$\mathcal{X}(\mathbb{Z}) = \{z \mid \log(z) = 0, D_2(z) = 0\} = \mathcal{X}(\mathbb{Z}_p)_3$$

for all p such that  $5 \le p \le 97$ .

Note that

$$D_2(19,-9) = D_2(19,-10) = 0$$

is already non-obvious. (A non-abelian reciprocity law.)

In fact, so far, we have checked

$$\mathcal{X}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}_p)_3$$

for the prime p = 5 and 256 semi-stable elliptic curves of rank zero.

Cremona label	number of   w  -values
1122m1	128
1122m2	384
1122m4	84
1254a2	140
1302d2	96
1506a2	112
1806h1	120
2442h1	78
2442h2	84
2706d2	120
2982j1	160
2982j2	140
3054b1	108

Cremona label	number of   w  -values
3774f1	120
4026g1	90
4134b1	90
4182h1	300
4218b1	96
4278j1	90
4278j2	100
4434c1	210
4774e1	224
4774e2	192
4774e3	264
4774e4	308
4862d1	216

Hence, for example, for the curve 1122m2,

$$y^2 + xy = x^3 - 41608x - 90515392$$

there are potentially 384 of the  $\Psi(w)$ 's that make up  $\mathcal{X}(\mathbb{Z}_p)_3$ .

Of these, all but 4 end up being empty, while the points in those  $\Psi(w)$  consist exactly of the integral points

(752, -17800), (752, 17048), (2864, -154024), (2864, 151160).

$$X : y^{2} = x^{6} - 4x^{4} + 3x^{2} + 1;$$
  

$$E_{1} : y^{2} = x^{3} - 4x^{2} + 3x + 1;$$
  

$$E_{2} : y^{2} = x^{3} + 3x^{2} - 4x + 1;$$
  

$$f_{1} : X \longrightarrow E_{1};$$
  

$$(x, y) \mapsto (x^{2}, y);$$
  

$$f_{2} : X \longrightarrow E_{2};$$
  

$$(x, y) \mapsto (1/x^{2}, y/x^{3});$$

 $z_1 \in E_1(\mathbb{Q}), z_2 \in E_2(\mathbb{Q}),$  generators for Mordell-Weil group.

 $h_i$ , *p*-adic height on  $E_i(\mathbb{Q})$ .

 $\log_i$ , *p*-adic log on  $E_i(\mathbb{Q}_p)$  with respect to suitable choice of invariant differential form.

 $\lambda_i$ , local *p*-adic height on  $E_i(\mathbb{Q}_p)$ . Hence, given by log of *p*-adic sigma function.

Define  $\rho: X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$  by

 $\rho(z)$ 

$$= 2\lambda_1(f_1(z)) - 2\frac{\log_1^2(f_1(z))}{\log_1^2(z_1)}h_1(z_1) - \lambda_2(f_2(z) - (0, 1)) - \lambda_2(f_2(z) + (0, 1)) + \frac{\log_2^2(f_2(z) - (0, 1)) + \log_2^2(f_2(z) + (0, 1)))}{\log_1^2(z_2)}h_2(z_2).$$

Then

$$X(\mathbb{Q}_{\rho})_{3} \subset \{\rho(z) = \log 2\} \cup \{\rho(z) = 2 \log 2\} \cup \{\rho(z) = (-1/3) \log 2\}$$

Get some nice explicit reciprocity laws like

 $ho(0,\pm 1) = \log 2;$   $ho(5/2,\pm 83/8) = 2\log 2;$  $ho(1,\pm 1) = (-1/3)\log 2.$  Non-abelian reciprocity: a brief comparison

Usual (Langlands) reciprocity:

$$L(M)=L(\pi)$$

where M is a motive and  $\pi$  is an algebraic automorphic representation on  $GL_n(\mathbb{A}_F)$ .

The relevance to arithemic comes from conjectures that say  $L(N^* \otimes M)$  encodes

RHom(N, M).

So in some sense, L functions classify motives.

However, in classical (non-linear) Diophantine geometry, we are interested in schemes, not motives, in particular, actual maps between schemes. Hence, a need for a nonlinear reciprocity of some sort.

Non-abelian reciprocity: a brief comparison

$$X/F$$
 as above,  $\Delta_n$ ,  $T_n = \Delta^n / \Delta^{n+1}$ , etc.

Langlands reciprocity

 $\rho \in H^1(G_F, GL(T_1)) \mapsto \text{functions on } GL(H_1^{DR}(F)) \setminus GL(H_1^{DR}(X)(\mathbb{A}_F)).$ 

 $\pi_1$  reciprocity

$$k \in H^1(G_F, T_n) \mapsto$$
functions on  $X(\mathbb{A}_F)$ 

via functions on

$$H^1(G_F, U_n) \setminus \prod' H^1(G_v, U_n).$$