Non-abelian Cohomology and Diophantine Geometry

Minhyong Kim

Bures-sur-Yvette, April, 2018

Some Coleman functions

In $\mathbb{Q}_2$,

$$\sum_{n=1}^{\infty} \frac{2^n}{n^2} = ?$$

Some Coleman functions

$$\sum_{n=1}^{\infty} \frac{2^n}{n^2} = 0$$

in the 2-adics.

Actually, also true in $\mathbb{Q}_p$ for all p.

$$\sum_{n=1}^{\infty} \frac{z^n}{n^2} = \int_0^z \frac{dt}{t} \frac{dt}{1-t} =: \ell_2(z)$$

Some Coleman functions

Right hand side can be defined via

$$M_b^z = \begin{bmatrix} 1 & \int_b^z dt/t & \int_0^z (dt/t)(dt/(1-t)) \\ 0 & 1 & \int_b^z dt/(1-t) \\ 0 & 0 & 1 \end{bmatrix}$$

where M_b^z is the holonomy of the rank 3 unipotent connection on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ given by the connection form

$$-\begin{bmatrix} 0 & dt/t & 0 \\ 0 & 0 & dt/(1-t) \\ 0 & 0 & 0 \end{bmatrix}$$

Some Coleman functions

Locally, we are solving the equations

$$d\ell_1 = dt/(1-t);\ d\ell_2 = \ell_1 dt/t.$$

Given a unipotent connection (V, ∇) and two points

$$x, y \in \mathbb{P}^1 \setminus \{0, 1, \infty\}(\mathbb{Q}_p)$$

(possibly tangental), there is a canonical isomorphism

$$M_x^y(V, \nabla) : V(]\bar{x}[)^{\nabla=0} \xrightarrow{\simeq} V(]\bar{y}[)^{\nabla=0}$$

determined by the property that it's compatible with Frobenius pull-backs. This is the holonomy matrix above.

Some Coleman functions

More generally, the k-logarithm

$$\ell_k(z) := \int_0^z (dt/t)(dt/t)\cdots(dt/t)(dt/(1-t))$$

is defined as the upper right hand corner of the holonomy matrix arising from the $(k+1)\times(k+1)$ connection form

$$-\begin{bmatrix} 0 & dt/t & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & dt/t & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & dt/t & \dots & 0 & 0 \\ & & \vdots & & \dots & dt/t & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & dt/(1-t) \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

Some Coleman functions

Coleman derived the following functional equations:

$$\ell_k(z) + (-1)^k \ell_k(z^{-1}) = \frac{-1}{k!} \log^k(z);$$

$$D_2(z) = -D_2(z^{-1});$$

$$D_2(z) = -D_2(1 - z);$$

where

$$D_2(z) = \ell_2(z) + (1/2) \log(z) \log(1 - z).$$

(The upper right hand corner of the log of the holonomy matrix.)

Some Coleman functions

From this, we get

$$D_2(-1) = -D_2(1/(-1)) = 0,$$

and

$$D_2(2) = -D_2(1-2) = 0.$$

But

$$D_2(2) = \ell_2(2) + (1/2)\log(2)\log(-1) = \ell_2(2).$$

Also,

$$D_2(1/2) = -D_2(2) = 0.$$

Some Coleman functions

Note:

$$\{-1, 2, 1/2\}$$

are exactly the 2-integral points of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, and one can give a *global* proof of the vanishing.

Use, in some sense, the arithmetic geometry of

$$\overline{\mathrm{Spec}(\mathbb{Z})} \setminus \{2, p, \infty\}.$$

Some Coleman functions

[Ishai Dan-Cohen and Stefan Wewers]

Let

$$D_4(z) = \zeta(3)\ell_4(z) + (8/7)[\log^3 2/24 + \ell_4(1/2)/\log 2]\log(z)\ell_3(z)$$

$$+[(4/21)(\log^3 2/24 + \ell_4(1/2)/\log 2) + \zeta(3)/24]\log^3(z)\log(1-z).$$

$$= \zeta(3)\ell_4(z) + A\log(z)\ell_3(z) + B\log^3(z)\log(1-z).$$

Some Coleman functions

Then

$$[\mathbb{P}^1 \setminus \{0, 1, \infty\}](\mathbb{Z}[1/2]) \subset \{D_2(z) = 0, D_4(z) = 0\}$$

and numerical computations for $p \leq 29$ indicate equality.

The inclusions above are examples of *non-abelian explicit reciprocity laws*.

Remark: The extra equation is definitely necessary in general, since, for example, $\sqrt{5} \in \mathbb{Z}_{11}$, and

$$D_2\left(\frac{-1 \pm \sqrt{5}}{2}\right) = D_2\left(\frac{3 \pm \sqrt{5}}{2}\right) = D_2\left(\frac{1 \pm \sqrt{5}}{2}\right) = 0.$$

Diophantine Geometry: Main Local-to-Global Problem

Given number field F and X/F smooth variety (with an integral model), 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 for $X = \mathbb{G}_m$, in which case

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

Problem becomes that of locating

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

Diophantine Geometry: Abelian Class Field Theory

We have the Artin reciprocity map

$$rec = \prod_v rec_v : \mathbb{A}_F^\times \longrightarrow G_F^{ab},$$

and the *reciprocity law*, which says that the composed map

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

is zero.

That is, the reciprocity map gives a *defining equation* for

$$\mathbb{G}_m(F) \subset \mathbb{G}_m(\mathbb{A}_F).$$

Diophantine Geometry: Non-Abelian Reciprocity?

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

Start with a rather general variety X for which we would like to understand

$$X(F)$$

via

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

in such way that

$$rec^{NA} = 0.$$

becomes an equation for $X(F)$.

Diophantine Geometry: Non-Abelian Reciprocity

Notation:

F: number field.
$G_F = \mathrm{Gal}(\bar{F}/F)$.
$G_v = \mathrm{Gal}(\bar{F}_v/F_v)$ for a place v of F.
S: finite set of places of F.
$\mathbb{A}_F$: finite Adeles of F

$\mathbb{A}_F^S$: finite S-integral adeles of F.
$G_S = \mathrm{Gal}(F^S/F)$, where F^S is the maximal extension of F unramified outside S.
$\prod_S$: product over non-Archimedean places in S.
$\prod^S H^1(G_v, A)$: product over non-Archimedean places in S and 'unramified cohomology' outside of S.

Diophantine Geometry: Non-Abelian Reciprocity

X: a smooth variety over F.
Fix base-point $b \in X(F)$ (sometimes tangential).

$$\Delta = \pi_1(\bar{X}, b)^{(2)},$$

pro-finite prime-to-2, étale fundamental group of

$$\bar{X} = X \times_{\mathrm{Spec}(F)} \mathrm{Spec}(\bar{F})$$

with base-point b.

$$\Delta^{[n]},$$

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

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

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

Denote by $\Delta^M, (\Delta_n)^M, T_n^M$ pro-M quotients for various finite sets of prime M.

Diophantine Geometry: Non-Abelian Reciprocity

[Coh]
For each n and M sufficiently large, T_n^M is torsion-free.

This implies

$$H^1(G_F^S, T_n^M) \xrightarrow{\text{loc}} {\prod}' H^1(G_v, T_n^M)$$

is injective.

Assuming [Coh], we get a non-abelian class field theory with coefficients in the nilpotent completion of X.

Diophantine Geometry: Non-Abelian Reciprocity

This consists of a filtration

$$X(\mathbb{A}_F) = X(\mathbb{A}_F)_1 \supset X(\mathbb{A}_F)_1^2 \supset X(\mathbb{A}_F)_2 \supset X(\mathbb{A}_F)_2^3$$

$$\supset X(\mathbb{A}_F)_3 \supset X(\mathbb{A}_F)_3^4 \supset \cdots$$

and a sequence of maps

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

$$rec_n^{n+1} : X(\mathbb{A}_F)_n^{n+1} \longrightarrow \mathfrak{G}_n^{n+1}(X)$$

to a sequence $\mathfrak{G}_n(X), \mathfrak{G}_n^{n+1}(X)$ of profinite abelian groups in such a way that

$$X(\mathbb{A}_F)_n^{n+1} = rec_n^{-1}(0)$$

and

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

Diophantine Geometry: Non-Abelian Reciprocity

$$\begin{tikzcd}
\cdots & rec_2^{-1}(0) \arrow[r, phantom, "\subset"] \arrow[d, equal] & (rec_1^2)^{-1}(0) \arrow[r, phantom, "\subset"] \arrow[d, equal] & rec_1^{-1}(0) \arrow[r, phantom, "\subset"] \arrow[d, equal] & X(\mathbb{A}_F) \arrow[d, equal] \\
\cdots & X(\mathbb{A}_F)_2^3 \arrow[r, phantom, "\subset"] \arrow[d, "rec_2^3"'] & X(\mathbb{A}_F)_2 \arrow[r, phantom, "\subset"] \arrow[d, "rec_2"'] & X(\mathbb{A}_F)_1^2 \arrow[r, phantom, "\subset"] \arrow[d, "rec_1^2"'] & X(\mathbb{A}_F)_1 \arrow[d, "rec_1"'] \\
\cdots & \mathfrak{G}_2^3(X) & \mathfrak{G}_2(X) & \mathfrak{G}_1^2(X) & \mathfrak{G}_1(X)
\end{tikzcd}$$

Diophantine Geometry: Non-Abelian Reciprocity

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

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

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

where

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

$$\mathfrak{G}_n^{n+1}(X) := \varprojlim_M [\varinjlim_S s\text{Ш}_S^2(T_{n+1}^M)]$$

where

$$s\text{Ш}_S^2(T_{n+1}^M) = \mathrm{Ker}[H^2(G_F^S, T_{n+1}^M) \longrightarrow {\prod}' H^2(G_v, T_{n+1}^M)].$$

Diophantine Geometry: Non-Abelian Reciprocity

When $X = \mathbb{G}_m$, then

$$\mathfrak{G}_n(X) = 0$$

for $n \geq 2$,

$$\mathfrak{G}_n^{n+1}(X) = 0$$

for all n, and

$$\mathfrak{G}_1 = \mathrm{Hom}[H^1(G_F, D(\hat{\mathbb{Z}}(1)^{(2)})), \mathbb{Q}/\mathbb{Z}]$$

$$= \mathrm{Hom}[H^1(G_F, [\mathbb{Q}/\mathbb{Z}]^{(2)}), \mathbb{Q}/\mathbb{Z}] = [G^{(2)}]_F^{ab}.$$

In this case, rec_1 reduces to the prime-to-2 part of the usual reciprocity map.

Diophantine Geometry: Non-Abelian Reciprocity

The reciprocity maps are defined using the local period maps

$$j^v : X(F_v) \longrightarrow H^1(G_v, \Delta);$$

$$x \mapsto [\pi_1^{(2)}(\bar{X}; b, x)].$$

Because the homotopy classes of étale paths

$$\pi_1^{(2)}(\bar{X}; b, x)$$

form a torsor for Δ with compatible action of G_v, we get a corresponding class in non-abelian cohomology of G_v with coefficients in Δ.

Diophantine Geometry: Non-Abelian Reciprocity

These assemble to a map

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

which comes in levels

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

Also have pro-M versions

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

and integral versions

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

Diophantine Geometry: Non-Abelian Reciprocity

To indicate the definition of the reciprocity maps, will just define pro-M versions on $X(\mathbb{A}_F^S)$ and assume that

$$H^1(G_F^S, T_n^M) \xrightarrow{\mathrm{loc}_S} \prod_S H^1(G_v, T_n^M)$$

are injective.

In general, 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 M.

Diophantine Geometry: Non-Abelian Reciprocity

The first reciprocity map is just defined using

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

where

$$D_1 : \prod_S H^1(G_v, \Delta_1^M) \longrightarrow \prod_S H^1(G_v, D(\Delta_1^M))^\vee \xrightarrow{\text{loc}^*} H^1(G_F^S, D(\Delta_1^M))^\vee,$$

is obtained from Tate duality and the dual of localization.

Diophantine Geometry: Non-Abelian Reciprocity

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

$$0 \longrightarrow H^1(G_F^S, T_{n+1}^M) \longrightarrow H^1(G_F^S, \Delta_{n+1}^M) \xrightarrow{p_n^{n+1}} H^1(G_F^S, \Delta_n)$$

$$\xrightarrow{\delta_{n+1}} H^2(G_F^S, T_{n+1}^M)$$

for non-abelian cohomology and Poitou-Tate duality stating that

$$H^1(G_F^S, T_{n+1}^M) \longrightarrow \prod_S H^1(G_v, T_n^M) \xrightarrow{D_{n+1}} H^1(G_S, D(T_{n+1}^M))^\vee$$

is exact.

Diophantine Geometry: Non-Abelian Reciprocity

We proceed as follows:

$$rec_1^2(x) = \delta_2 \circ \mathrm{loc}^{-1}(j_1(x)) \in Ш_S^2(T_2^M)$$

and

$$rec_2(x) = D_2(\mathrm{loc}((p_1^2)^{-1}(\mathrm{loc}^{-1}(j_1(x)))) - j_2(x)) \in H^1(G_S, D(T_2^M))^\vee.$$

Diophantine Geometry: Non-Abelian Reciprocity

$$\begin{tikzcd}
 & H^1(G_F^S, T_2^M) \arrow[r, hook] \arrow[d] & \prod_S H^1(G_v, T_2^M) \ni k_2 \arrow[d] \\
{[p_1^2]^{-1}(\mathrm{loc}^{-1}(j_1)) \in} & H^1(G_F^S, \Delta_2^M) \arrow[r, hook] \arrow[d] & \prod_S H^1(G_v, \Delta_2^M) \ni j_2 \arrow[d] \\
\mathrm{loc}^{-1}(j_1) \in & H^1(G_F^S, T_1^M) \arrow[r, hook] & \prod_S H^1(G_v, T_1^M) \ni j_1
\end{tikzcd}$$

$$k_2(x) := \mathrm{loc}[[p_1^2]^{-1}(\mathrm{loc}^{-1}(j_1(x)))] - j_2(x)$$
$$\mapsto D_2(k_2(x)) \in H^1(G_F^S, D(T_2^M))^\vee$$

In general,

$$rec_n^{n+1}(x) = \delta_{n+1} \circ \mathrm{loc}^{-1}(j_n(x)) \in \text{Ш}^2_S(T^M_{n+1})$$

and

$$\begin{aligned} &rec_{n+1}(x) \\ = D((&\mathrm{loc}(p_n^{n+1})^{-1}(j_n(x))) - j_{n+1}(x)) \in H^1(G_S, D(T_2^M))^\vee. \end{aligned}$$

Diophantine Geometry: Non-Abelian Reciprocity

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

$$\begin{tikzcd}
X(F) \arrow[r] \arrow[d, "j_n^g"'] & X(\mathbb{A}_F) \arrow[d, "j_n^{loc}"'] \\
H^1(G_F^S, \Delta_n^M) \arrow[r, "\mathrm{loc}"] & \prod H^1(G_v, \Delta_n^M)
\end{tikzcd}$$

$$\begin{tikzcd}
 & H^1(G_F^S, \Delta_{n+1}^M) \arrow[d] \\
X(F) \arrow[ur, "j_{n+1}^g"] \arrow[r, "j_n^g"] & H^1(G_F^S, \Delta_n^M)
\end{tikzcd}$$

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

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

for every n corresponding to the global torsor

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

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

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

and

$$\mathrm{loc}[(p_n^{n+1})^{-1}(\mathrm{loc}^{-1}(j_n(x)))] - j_{n+1}(x) = \mathrm{loc}(j_{n+1}^g) - j_{n+1}(x) = 0$$

for every n.

A non-abelian conjecture of Birch and Swinnerton-Dyer type

Let

$$Pr_v : X(\mathbb{A}_F) \longrightarrow X(F_v)$$

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

Define

$$X(F_v)_n := Pr_v(X(\mathbb{A}_F)_n)$$

and

$$X(F_v)_n^{n+1} := Pr_v(X(\mathbb{A}_F)_n^{n+1}).$$

Thus,

$$X(F_v) = X(F_v)_1 \supset X(F_v)_1^2 \supset X(F_v)_2 \supset \cdots \supset X(F_v)_\infty \supset X(F).$$

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

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

A non-abelian conjecture of Birch and Swinnerton-Dyer type

Can consider more generally S-integral points on affine hyperbolic X as well where we get an induced filtration

$$X(\mathbb{A}_F^S) \supset X(\mathbb{A}_F^S)_1^2 \supset X(\mathbb{A}_F^S)_2 \supset X(\mathbb{A}_F^S)_2^3 \supset \cdots .$$

By projecting to $X(O_{F_v})$ for $v \notin S$, get a flitration

$$X(O_{F_v}) \supset X(O_{F_v})_{S,1}^2 \supset X(O_{F_v})_{S,2} \supset X(O_{F_v})_{S,2}^3 \supset \cdots .$$

and

$$X(O_{F_v})_{S,\infty} = \cap_n X(O_{F_v})_{S,n}.$$

A non-abelian conjecture of Birch and Swinnerton-Dyer type

Conjecture: Let $X/\mathbb{Q}$ 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

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

These give us conjectural methods to 'compute'

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

or

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

A non-abelian conjecture of Birch and Swinnerton-Dyer type

Whenever we have an element

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

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

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

A non-abelian conjecture of Birch and Swinnerton-Dyer type

Computations 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

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j_n^g"'] & X(\mathbb{Q}_p) \arrow[d, "j_n^p"'] \arrow[dr, "j_n^{DR}"] & \\
H_f^1(G_T, U_n) \arrow[r, "loc_n^p"] & H_f^1(G_p, U_n) \arrow[r, "\simeq^D"] & U_n^{DR}/F^0
\end{tikzcd}$$

A non-abelian conjecture of Birch and Swinnerton-Dyer type

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

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

Explicit reciprocity laws: Examples

[Jennifer Balakrishnan, Ishai Dan-Cohen, Stefan Wewers, M.K.] and [Dan-Cohen, Wewers]

Let $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$. Then $X(\mathbb{Z}[1/2]) = \{2, -1, 1/2\}$.

$$X(\mathbb{Z}_p)_{\{2\},2} \subset \cup_{n,m}\{z \mid \log(z) = n\log(2), \log(1-z) = m\log(2)\}.$$

$$X(\mathbb{Z}_p)_{\{2\},3}$$

$$\subset [\cup_{m,n}\{z \mid \log(z) = n\log(2), \log(1-z) = m\log(2)\}] \cap \{D_2(z) = 0\}.$$

Explicit reciprocity laws: Examples

Probably,

$$X(\mathbb{Z}_p)_{\{2\},4} = X(\mathbb{Z}_p)_{\{2\},3}.$$

Also,

$$\begin{gathered} X(\mathbb{Z}_p)_{\{2\},5} \\ \subset [\cup_{m,n}\{z \mid \log(z) = n\log(2), \log(1-z) = m\log(2)\}] \\ \cap\{D_2(z) = 0\} \cap \{D_4(z) = 0\}. \end{gathered}$$

Numerically, this appears to be equal to $\{2, -1, 1/2\}$.

Explicit reciprocity laws: Examples

[Balakrishnan, Dan-Cohen, Wewers, K.]

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

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

(b is a tangential base-point.)

Then

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

Explicit reciprocity laws: Examples

Now examine the inclusion

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

Let

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

Explicit reciprocity laws: Examples

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

$$N_l = \mathrm{ord}_l(\Delta_{\mathcal{E}}),$$

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

$$W_l := \{(n(N_l - n)/2N_l) \log l \mid 0 \leq n < N_l\},$$

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

$$\|w\| = \sum_{l \in S} w_l.$$

Explicit reciprocity laws: Examples

Theorem

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

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

where

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

Of course,

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

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

Explicit reciprocity laws: Examples

In fact, so far, we have checked

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

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

Explicit reciprocity laws: Examples

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

Explicit reciprocity laws: Examples

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

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

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

Explicit reciprocity laws: Examples

[Jennifer Balakrishnan, Netan Dogra, Stefan Mueller-Stach, Jan Tuitman, Jan Vonk]

$$X_s^+(N) = X(N)/C_s^+(N),$$

where $X(N)$ is the compactification of the moduli space of pairs

$$(E, \phi : E[N] \simeq (\mathbb{Z}/N)^2),$$

and $C_s^+(N) \subset GL_2(\mathbb{Z}/N)$ is the normaliser of a split Cartan subgroup.

Bilu-Parent-Rebolledo had shown that $X_s^+(p)(\mathbb{Q})$ consists entirely of cusps and CM points for all primes $p > 7$, $p \neq 13$. They called $p = 13$ the 'cursed level'.

Explicit reciprocity laws: Examples

Theorem (BDMTV)

$$X_s^+(13)(\mathbb{Q}) = X_s^+(13)(\mathbb{Q}_{17})_3.$$

This set consists of 7 rational points, which are the cusp and 6 CM points.

This concludes an important chapter of a question of Serre:

Find an absolute constant A such that

$$G \longrightarrow \mathrm{Aut}(E[p])$$

is surjective for all non-CM elliptic curves $E/\mathbb{Q}$ and primes $p > A$.

Explicit reciprocity laws: Examples

Careful computation of the lower horizontal map, which is algebraic:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j_n^g"'] & X(\mathbb{Q}_p) \arrow[d, "j_n^p"'] \arrow[dr, "j_n^{DR}"] & \\
H_f^1(G_T, U_n) \arrow[r, "loc_n^p"] & H_f^1(G_p, U_n) \arrow[r, "\simeq^D"] & U_n^{DR}/F^0
\end{tikzcd}$$

The right vertical map is analytic and expressed in terms of iterated integrals.

Defining equation for $Im(loc_n^p)$ pulls back to analytic defining equation for rational points.

Explicit reciprocity laws: Examples

In fact, in this case, there is a pushout:

$$\begin{tikzcd}
0 \arrow[r] & U^2/U^3 \arrow[r] \arrow[d] & U_2 \arrow[r] \arrow[d] & U_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] & W_2 \arrow[r] & U_1 \arrow[r] & 0
\end{tikzcd}$$

induced by a polarisation

$$U^2/U^3 \simeq \wedge^2 U_1/\mathbb{Q}_p(1) \longrightarrow \mathbb{Q}_p(1)$$

orthogonal to the Weil pairing. Recall that $U_1 \simeq V_p = T_p J_X \otimes \mathbb{Q}_p$.

Explicit reciprocity laws: Examples

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d] & X(\mathbb{Q}_p) \arrow[d] \arrow[dr] & \\
H^1_f(G_T, W_2) \arrow[r] & H^1_f(G_p, W_2) \arrow[r] & W_2^{DR}/F^0
\end{tikzcd}$$

Explicit reciprocity laws: Examples

In fact, the target can be identified with a space of *mixed extensions*:

$$E \supset E^1 \supset E^2,$$

such that

$$E_2 \simeq \mathbb{Q}_p(1),\ E^1/E^2 \simeq V_p,\ E/E^1 \simeq \mathbb{Q}_p.$$

Thus, they are mixtures of

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow E^1 \longrightarrow V_p \longrightarrow 0$$

and

$$0 \longrightarrow V_p \longrightarrow E/E^2 \longrightarrow \mathbb{Q}_p \longrightarrow 0,$$

coming up in Nekovar's theory of height pairings

$$H^1_f(V) \times H^1_f(V) \longrightarrow \mathbb{Q}_p.$$

Explicit reciprocity laws: Examples

We give a general idea of how this works with a simpler example:

$$X = E \setminus 0$$

where $E/\mathbb{Q}$ is an elliptic curve of rank 1 with square-free minimal discriminant.

We have

$$h : E(\mathbb{Q}) \longrightarrow \mathbb{Q}_p,$$

the p-adic quadratic height.

Thus, if $y \in E(\mathbb{Q})$ is non-torsion, then

$$c_E := h(y)/\log^2(y)$$

is independent of y.

Explicit reciprocity laws: Examples

But log is an analytic function on $E(\mathbb{Q}_p)$, while h has a decomposition

$$h = h_p + \sum_{v \neq p} h_v,$$

with

$$h_p(z) = \int_b^z \alpha\beta + C_E,$$

where

$$C_E = (a_1^2 + 4a_2)/12 - Eis_2(E, \alpha)/12,$$

α is an integral invariant differential, and $\beta = x\alpha$.

But if z is integral, then

$$h(z) = h_p(z).$$

Explicit reciprocity laws: Examples

Thus, the equation

$$h(z)/\log^2(z) = c_E = h(y)/\log^2(y)$$

becomes

$$\int_b^z \alpha\beta + (C_E - c_E)\log^2(z) = 0,$$

a defining equation for integral points.

The case of $X_s^+(13)$ is a substantially more complicated version of this argument using relation between the functions

$$h(z), \quad \log_i(z)\log_j(z)$$

for $1 \leq i \leq j \leq 3$.

Some speculations on rational points and critical points

Actually, interested in

$$Im(H^1(G_T, U)) \cap \prod_{v \in T} H^1_f(G_v, U) \subset \prod_{v \in T} H^1(G_v, U),$$

where

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

is a subvariety defined by some integral or Hodge-theoretic conditions.

In order to apply symplectic techniques, replace U by

$$T^*(1)U := (LieU)^*(1) \rtimes U.$$

Rational points and critical points

Then

$$\prod_{v \in T} H^1(G_v, T^*(1)U)$$

is a symplectic variety and

$$Im(H^1(G_T, T^*(1)U)), \quad \prod_{v \in T} H^1_f(G_v, T^*(1)U)$$

are Lagrangian subvarieties.

Thus, the derived intersection

$$Im(H^1(G_T, T^*(1)U)) \cap \prod_{v \in T} H^1_f(G_v, T^*(1)U)$$

has a $[-1]$-shifted symplectic structure.

Should be the critical set of a function.