

# Selmer varieties

Minhyong Kim

April, 2009

Heidelberg

I. Non-abelian descent

II. Diophantine finiteness

III. Preliminary remarks on non-abelian duality

IV. Explicit formulas.

General comment:

Usual approach to the Diophantine geometry of curves emphasizes the differences between three cases: genus zero, genus one, and genus  $\geq 2$ .

However, we wish to focus on the parallels, especially between

$$(E, e),$$

a compact curve of genus one equipped with an integral point, and

$$(X, b),$$

a hyperbolic curve<sup>a</sup> equipped with an integral point.

---

<sup>a</sup>That is,  $X(\mathbb{C})$  has a hyperbolic metric. Equivalently,  $X$  is genus zero minus at least three points, genus one minus at least one point, or genus  $\geq 2$ .

## I. Non-abelian descent

$(E, e)$  elliptic curve over  $\mathbb{Z}_S$ .  $p$  prime not in  $S$ .  $T = S \cup \{p\}$ .

$G := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ . Kummer theory provides an injection

$$E(\mathbb{Z}_S)/p^n E(\mathbb{Z}_S) \hookrightarrow H^1(G_T, E[P^n]).$$

BSD conjectured an isomorphism

$$E(\mathbb{Z}_S) \otimes \mathbb{Z}_p \simeq H_{f, \mathbb{Z}}^1(G, T_p(E))$$

where

$$T_p(E) := \varprojlim E[p^n]$$

is the  $p$ -adic Tate module of  $E$  and the subscript  $f, \mathbb{Z}$  refers to local ‘Selmer’ conditions.

When  $X/\mathbb{Z}_S$  is a smooth hyperbolic curve and  $b \in X(\mathbb{Z}_S)$ , analogue of above construction is

$$X(\mathbb{Z}_S) \xrightarrow{\kappa} H_f^1(G, H_1^{et}(\bar{X}, \mathbb{Z}_p))$$

using the  $p$ -adic étale homology

$$H_1^{et}(\bar{X}, \mathbb{Z}_p) := \pi_1^{et,p}(\bar{X}, b)^{ab}$$

of  $\bar{X} := X \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(\bar{\mathbb{Q}})$ .

Several different descriptions of this map.

But in any case, it factors through the Jacobian

$$X(\mathbb{Z}_S) \rightarrow J(\mathbb{Z}_S) \rightarrow H_f^1(G, T_p J)$$

using the isomorphism

$$H_1^{et}(\bar{X}, \mathbb{Z}_p) \simeq T_p J,$$

where the first map is the Albanese map

$$x \mapsto [x] - [b]$$

and the second is again provided Kummer theory on the abelian variety  $J$ .

Consequently, difficult to disentangle  $X(\mathbb{Z}_S)$  from  $J(\mathbb{Z}_S)$ .

Efforts of Weil, Mumford, Vojta.

The theory of *Selmer varieties* refines this to a tower:

$$\begin{array}{ccc}
 & \vdots & \\
 & \vdots & H_f^1(G, U_4) \\
 & \nearrow \kappa_4 & \downarrow \\
 & \nearrow \kappa_3 & H_f^1(G, U_3) \\
 & \nearrow \kappa_2 & \downarrow \\
 X(\mathbb{Z}_S) & \xrightarrow{\kappa_1} & H_f^1(G, U_2) \\
 & & \downarrow \\
 & & H_f^1(G, U_1) = H_f^1(G, T_p J \otimes \mathbb{Q}_p)
 \end{array}$$

where the system  $\{U_n\}$  is the  $\mathbb{Q}_p$ -unipotent étale fundamental group  $\pi_1^{u, \mathbb{Q}_p}(\bar{X}, b)$  of  $\bar{X}$ .

Brief remarks on the constructions.

1. The étale site of  $\bar{X}$  defines a category

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

of locally constant unipotent  $\mathbb{Q}_p$ -sheaves on  $\bar{X}$ . A sheaf  $\mathcal{V}$  is unipotent if it can be constructed using successive extensions by the constant sheaf  $[\mathbb{Q}_p]_{\bar{X}}$ .

2. We have a fiber functor

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

that associates to a sheaf  $\mathcal{V}$  its stalk  $\mathcal{V}_b$ . Then

$$U := \mathrm{Aut}^{\otimes}(F_b),$$

the tensor-compatible automorphisms of the functor.  $U$  is a pro-algebraic pro-unipotent group over  $\mathbb{Q}_p$ .

3.

$$U = U^1 \supset U^2 \supset U^3 \supset \dots$$

is the descending central series of  $U$ , and

$$U_n = U^{n+1} \setminus U$$

are the associated quotients. There is an identification

$$U_1 = H_1^{et}(\bar{X}, \mathbb{Q}_p) = V := T_p J \otimes \mathbb{Q}_p$$

at the bottom level and exact sequences

$$0 \rightarrow U^{n+1} \setminus U^n \rightarrow U_n \rightarrow U_{n-1} \rightarrow 0$$

for each  $n$ .

For example, for  $n = 2$ ,

$$0 \rightarrow \wedge^2 V \rightarrow U_2 \rightarrow V \rightarrow 0,$$

for affine  $X$ .

When  $X = E \setminus \{e\}$  for an elliptic curve  $E$ , this becomes

$$0 \rightarrow \mathbb{Q}_p(1) \rightarrow U_2 \rightarrow V \rightarrow 0.$$

When  $X$  is compact, we get

$$0 \rightarrow [\wedge^2 V / \mathbb{Q}_p(1)] \rightarrow U_2 \rightarrow V \rightarrow 0,$$

where

$$\mathbb{Q}_p(1) \hookrightarrow \wedge^2 V$$

comes from the Weil pairing.

4.  $U$  has a natural action of  $G$  lifting the action on  $V$ , and  $H^1(G, U_n)$  denotes continuous Galois cohomology with values in the points of  $U_n$ . For  $n \geq 2$ , this is *non-abelian cohomology*, and hence, does not have the structure of a group.

5.  $H_f^1(G, U_n) \subset H^1(G, U_n)$  denotes a subset defined by local ‘Selmer’ conditions that require the classes to be

(a) unramified outside a set  $T = S \cup \{p\}$ , where  $S$  is the set of primes of bad reduction;

(b) and *crystalline* at  $p$ , a condition coming from  $p$ -adic Hodge theory.

6. The system

$$\cdots \rightarrow H_f^1(G, U_{n+1}) \rightarrow H_f^1(G, U_n) \rightarrow H_f^1(G, U_{n-1}) \rightarrow \cdots$$

is a pro-algebraic variety, the *Selmer variety* of  $X$ . That is, each  $H_f^1(G, U_n)$  is an algebraic variety over  $\mathbb{Q}_p$  and the transition maps are algebraic.

$$H_f^1(G, U) = \{H_f^1(G, U_n)\}$$

is the moduli space of principal bundles for  $U$  in the étale topology of  $\text{Spec}(\mathbb{Z}[1/S])$  that are crystalline at  $p$ .

If  $\mathbb{Q}_T$  denotes the maximal extension of  $\mathbb{Q}$  unramified outside  $T$  and  $G_T := \text{Gal}(\mathbb{Q}_T/\mathbb{Q})$ , then  $H_f^1(G, U_n)$  is naturally realized as a closed subvariety of  $H^1(G_T, U_n)$ .

For the latter, there are exact sequences

$$0 \rightarrow H^1(G_T, U^{n+1} \setminus U^n) \rightarrow H^1(G_T, U_n) \rightarrow H^1(G_T, U_{n-1}) \xrightarrow{\delta} \\ H^2(G_T, U^{n+1} \setminus U^n)$$

in the sense of fiber bundles, and the algebraic structures are built up iteratively from the  $\mathbb{Q}_p$ -vector space structure on the

$$H^i(G_T, U^{n+1} \setminus U^n)$$

and the fact that the boundary maps  $\delta$  are algebraic. (It is non-linear in general.)

7. The map

$$\kappa^{na} = \{\kappa_n\} : X(\mathbb{Z}_S) \longrightarrow H_f^1(G, U)$$

is defined by associating to a point  $x$  the principal  $U$ -bundle

$$P(x) = \pi_1^{u, \mathbb{Q}_p}(\bar{X}; b, x) := \text{Isom}^{\otimes}(F_b, F_x)$$

of tensor-compatible isomorphisms from  $F_b$  to  $F_x$ , that is, *the  $\mathbb{Q}_p$ -pro-unipotent étale paths* from  $b$  to  $x$ .

For  $n = 1$ ,

$$\kappa_1 : X(\mathbb{Z}_S) \longrightarrow H_f^1(G, U_1) = H_f^1(G, T_p J \otimes \mathbb{Q}_p)$$

reduces to the map from Kummer theory. But the map  $\kappa_n$  for  $n \geq 2$  does not factor through the Jacobian. Hence, suggests the possibility of separating the structure of  $X(\mathbb{Z}_S)$  from that of  $J(\mathbb{Z}_S)$ .

8. If one restricts  $U$  to the étale site of  $\mathbb{Q}_p$ , there are local analogues

$$\kappa_p^{na} : X(\mathbb{Z}_p) \rightarrow H_f^1(G_p, U_n)$$

that can be explicitly described using non-abelian  $p$ -adic Hodge theory. More precisely, there is a compatible family of isomorphisms

$$D : H_f^1(G_p, U_n) \simeq U_n^{DR} / F^0$$

to homogeneous spaces for quotients of the *De Rham fundamental group*

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

of  $X \otimes \mathbb{Q}_p$ .

$U^{DR}$  classifies unipotent vector bundles with flat connections on  $X \otimes \mathbb{Q}_p$ , and  $U^{DR} / F^0$  classifies principal bundles for  $U^{DR}$  with compatible Hodge filtrations and crystalline structures.

Given a crystalline principal bundle  $P = \text{Spec}(\mathcal{P})$  for  $U$ ,

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

where  $B_{cr}$  is Fontaine's ring of  $p$ -adic periods. This is a principal  $U^{DR}$  bundle.

The two constructions fit into a diagram

$$\begin{array}{ccc} X(\mathbb{Z}_p) & \xrightarrow{\kappa_p^{na}} & H_f^1(G_p, U) \\ & \searrow \kappa_{dr/cr}^{na} & \downarrow D \\ & & U^{DR}/F^0 \end{array}$$

whose commutativity reduces to the assertion that

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

9. The map

$$\kappa_{dr/cr}^{na} : X(\mathbb{Z}_p) \rightarrow U^{DR}/F^0$$

is described using  $p$ -adic iterated integrals

$$\int \alpha_1 \alpha_2 \cdots \alpha_n$$

of differential forms on  $X$ , and has a highly transcendental natural:

For any residue disk  $]y[ \subset X(\mathbb{Z}_p)$ ,

$$\kappa_{dr/cr,n}^{na}(]y[) \subset U_n^{DR}/F^0$$

is Zariski dense for each  $n$  and its coordinates can be described as convergent power series on the disk.

10. The local and global constructions fit into a family of commutative diagrams

$$\begin{array}{ccccc}
 X(\mathbb{Z}_S) & \longrightarrow & X(\mathbb{Z}_p) & & \\
 \downarrow & & \downarrow & \searrow & \\
 H_f^1(G, U_n) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U_n) & \xrightarrow{D} & U_n^{DR}/F^0
 \end{array}$$

where the bottom horizontal maps are algebraic, while the vertical maps are transcendental. Thus, the difficult inclusion  $X(\mathbb{Z}_S) \subset X(\mathbb{Z}_p)$  has been replaced by the algebraic map  $\text{loc}_p$ .

## II. Diophantine Finiteness

**Theorem 1** *Suppose*

$$\text{loc}_p(H_f^1(G, U_n)) \subset H_f^1(G_p, U_n)$$

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

Theorem is a crude application of the methodology. Eventually would like refined descriptions of the image of the global Selmer variety, and hence, of  $X(\mathbb{Z}_S) \subset X(\mathbb{Z}_p)$  by extending the method of Chabauty and Coleman and the work of Coates-Wiles, Kolyvagin, Rubin, Kato on the conjecture of Birch and Swinnerton-Dyer.

Idea of proof: There is a non-zero algebraic function  $\alpha$

$$\begin{array}{ccc}
 X(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Z}_p) \\
 \downarrow \kappa_n^{na} & & \downarrow \kappa_{p,n}^{na} \\
 H_f^1(G, U_n) & \xrightarrow{D \circ \text{loc}_p} & H_f^1(G_p, U_n) \\
 & & \downarrow \exists \alpha \neq 0 \\
 & & \mathbb{Q}_p
 \end{array}$$

vanishing on  $\text{loc}_p[H_f^1(G, U_n)]$ . Hence,  $\alpha \circ \kappa_{p,n}^{na}$  vanishes on  $X(\mathbb{Z}_S)$ . But using the comparison with the De Rham realization, we see that this function is a non-vanishing convergent power series on each residue disk.  $\square$

-Hypothesis of the theorem expected to always hold for  $n$  sufficiently large, but difficult to prove. For example, Bloch-Kato conjecture on surjectivity of  $p$ -adic Chern class map, or Fontaine-Mazur conjecture on representations of geometric origin all imply the hypothesis for  $n \gg 0$ .

That is, Grothendieck expected

Non-abelian ‘finiteness of III’ (= *section conjecture*)  $\Rightarrow$  finiteness of  $X(\mathbb{Z}_S)$ .

Instead we have:

‘Higher abelian finiteness of III’  $\Rightarrow$  finiteness of  $X(\mathbb{Z}_S)$ .

Can prove the hypothesis in cases where the image of  $G$  inside  $\text{Aut}(H_1(\bar{X}, \mathbb{Z}_p))$  is essentially abelian. That is, when

- $X$  has genus zero;

- $X = E \setminus \{e\}$  where  $E$  is an elliptic curve with complex multiplication;

-(with John Coates)  $X$  compact of genus  $\geq 2$  and  $J_X$  factors into abelian varieties with complex multiplication. For example,  $X$  might be

$$ax^n + by^n = cz^n,$$

for  $n \geq 4$ .

In the CM cases, need to choose  $p$  to split inside the CM fields.

Idea: Construct a quotient

$$U \rightarrow W \rightarrow 0$$

and a diagram

$$\begin{array}{ccccc}
 X(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Z}_p) & & \\
 \downarrow \kappa_n^{na} & & \downarrow \kappa_{p,n}^{na} & & \\
 H_f^1(G, U_n) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U_n) & \xrightarrow{D} & U_n^{DR}/F^0 \\
 \downarrow & & \downarrow & & \downarrow \\
 H_f^1(G, W_n) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, W_n) & \xrightarrow{D} & W_n^{DR}/F^0
 \end{array}$$

such that

$$\dim H_f^1(G, W_n) < \dim W_n^{DR} / F^0$$

for  $n \gg 0$ .

When  $J_X$  has CM, can construct a ‘polylogarithmic quotient’<sup>a</sup>

$$W = U / [[U, U], [U, U]]$$

such that all CM characters

$$\chi_{i_1} \chi_{i_2} \cdots \chi_{i_n}$$

appearing in  $W^n / W^{n+1}$  have multiplicity one.

---

<sup>a</sup>The terminology is adopted by analogy with the quotient of the fundamental group of  $\mathbf{P}^1 \setminus \{0, 1, \infty\}$  that provides the natural setting for the theory of polylogarithms according to Beilinson and Deligne.

Elementary Iwasawa theory can be used to show that

$$H^2(G_T, \chi_{i_1} \chi_{i_2} \cdots \chi_{i_n}) = 0$$

rather generically, allowing us to control

$$\dim H_f^1(G, W_n) \leq \sum_{i=1}^n \dim H_f^1(G, W^i / W^{i+1}).$$

$$\leq \sum_{i=1}^n \dim H^1(G_T, W^i / W^{i+1})$$

and show that it grows more slowly than

$$\dim W_n^{DR} / F^0.$$

### III. Preliminary remarks on non-abelian duality

As far as the arithmetic of curves is concerned one major goal of the theory is to give an explicit description of

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

This should come from a non-abelian local-global duality together with a non-abelian explicit reciprocity law.<sup>a</sup> Wish to provide a hint of this idea using a very special situation:

$$X = E \setminus \{e\},$$

where  $E_{\mathbb{Q}}$  is an elliptic curve such that

$$L(E_{\mathbb{Q}}, 1) = 0, \quad L'(E_{\mathbb{Q}}, 1) \neq 0.$$

Here, we will assume that  $E$  is in fact a minimal  $\mathbb{Z}$ -model of  $E_{\mathbb{Q}}$  and  $X = E \setminus \{e\}$ .

---

<sup>a</sup>Of course both notions are highly speculative at present.

Choose  $S$  so that  $E_S := E \times_{\text{Spec}(\mathbb{Z})} \text{Spec}(\mathbb{Z}_S)$  is smooth. Our assumptions imply that

$$\text{III}(E)$$

is finite and

$$\text{rank}E(\mathbb{Z}) = \text{rank}E(\mathbb{Z}_S) = \text{rank}E(\mathbb{Q}) = 1,$$

but still difficult to analyze the inclusion

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

Some archimedean progress using Diophantine approximation supplemented by LLL-algorithm. Here, we focus on non-archimedean techniques and the inclusion

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

Pick a tangential base-point  $b \in T_e E$  and only use  $U_2$ , identified with its Lie algebra  $L_2$ .  $L_2$  has a natural graded structure

$$L_2 = L[1] \oplus L[2]$$

such that  $L[1] \simeq L_1 \simeq V(E)$  and  $L[2] \simeq \mathbb{Q}_p(1)$  is the one-dimensional center of  $L_2$ . The group law on  $U_2$  can be thought of as a twisted operation on  $L_2$  given by<sup>a</sup>

$$(l_1 + l_2) * (l'_1 + l'_2) = l_1 + l'_1 + l_2 + l'_2 + (1/2)[l_1, l'_1].$$

The grading is compatible with the Galois action (in fact, with the motivic structure):

$$g(l_1 + l_2) = g(l_1) + g(l_2).$$

---

<sup>a</sup>This kind of structure is often referred to as a *Heisenberg group*.

If  $a$  is a cochain on  $G_T$  or  $G_p$  with values in  $U_2$ , then we can write

$$a = a_1 + a_2$$

with  $a_1$  taking values in  $L[1]$  and  $a_2$  taking values in  $L[2]$ . The cocycle condition for the group law is written in terms of these components as

$$da_1 = 0$$

$$da_2 = -(1/2)a_1 \cup a_1,$$

where the cup product of two cochains  $\xi$  and  $\eta$  is defined by

$$\xi \cup \eta(g, h) = [\xi(g), g\eta(h)].$$

We will construct a function on  $H_f^1(G_p, U_2)$  using *secondary cohomological operations*.

Let  $c : G_T \rightarrow \mathbb{Q}_p$  be the log of the  $p$ -adic cyclotomic character and  $c^p = c|_{G_p}$ . Given a cocycle  $\xi = \xi_1 + \xi_2 : G_p \rightarrow U_2$ , the function is, in essence,

$$\xi \mapsto (c, \xi_1, \xi_1),$$

where the bracket refers to a *Massey triple product*, taking values in

$$H^2(G_p, L[2]) \simeq \mathbb{Q}_p.$$

This notion comes from rational homotopy theory, and is usually defined for cohomology classes of an associative differential graded algebra  $A$ .

If

$$[a] \in H^1(A), \quad [b] \in H^1(A), \quad [c] \in H^1(A)$$

are classes with the property that

$$[a][b] = 0, \quad [b][c] = 0,$$

then we can solve the equations

$$dx = ab, \quad dy = bc.$$

We see then that

$$xc + ay$$

is a cocycle, defining a class in  $H^2(A)$ . Note that the class depends on the choice of  $x$  and  $y$ , a *defining system*. Well-defined class lives only inside

$$H^2(A)/[aH^1(A) + H^1(A)c].$$

In our situation, the complex of cochains on  $G_p$  with values in

$$\mathbb{Q}_p \oplus L[1] \oplus L[2]$$

forms an associative differential graded algebra. Given a cocycle

$$\xi = \xi_1 + \xi_2 : G_p \rightarrow U_2,$$

we have

$$[c^p] \cup [\xi_1] = 0,$$

since  $H^2(G_p, L[1]) = 0$ . Also,

$$[\xi_1] \cup [\xi_1] = 0,$$

since  $d(-2\xi_2) = \xi_1 \cup \xi_1$ .

Therefore, we can form the Massey triple product

$$(c^p, \xi_1, \xi_1) \in H^2(G_p, L[2]) / [c^p \cup H^1(G_p, L[1])] + \xi_1 \cup H^1(G_p, L[1]).$$

Unfortunately, zero.

But note that this naive Massey product does not use the full data of  $\xi$  or the strength of our assumptions. Firstly, part of a defining system for the Massey product is encoded in  $\xi$ :

$$d(-2\xi_2) = \xi_1 \cup \xi_1.$$

Secondly, if  $[\xi] \in H_f^1(G_p, U_2)$ , then  $[\xi_1] \in H_f^1(G_p, L[1])$  is in the image of the localization map

$$H_{f,\mathbb{Z}}^1(G, L[1]) \simeq H_f^1(G_p, L[1]).$$

Hence, the equation

$$dx = c \cup \xi_1$$

makes sense globally.

Key point:

*Using Using our restrictive hypotheses, there is a global solution*

$$x^{glob} : G_T \rightarrow L[1]$$

*to the equation*

$$dx = c \cup \xi_1.$$

Uses the finiteness of III and a generator for  $E(\mathbb{Z})$ .

**Proposition 2** *The class*

$$\psi_p(\xi) := [\text{loc}_p(x^{\text{glob}}) \cup \xi_1 + c^p \cup (-2\xi_2)] \in H^2(G_p, L[2])$$

*is independent of all choices.*

Thus,

$$\psi_p : H_f^1(G_p, U_2) \rightarrow \mathbb{Q}_p$$

is a well-defined algebraic function on the local Selmer variety.

Remark: The map

$$\mathbb{Z}_p^* \otimes \mathbb{Q}_p \simeq H_f^1(G_p, L[2]) \hookrightarrow H_f^1(G_p, U_2) \xrightarrow{\psi_p} \mathbb{Q}_p$$

is the log map, and hence,  $\psi_p$  is non-zero.

Define ('refined Selmer variety')

$$H_{f,\mathbb{Z}}^1(G, U_2) \subset H_f^1(G, U_2)$$

to be the intersection of the kernels of

$$\text{loc}_l : H_f^1(G, U_2) \rightarrow H_f^1(G_l, U_2)$$

for all  $l \neq p$ .

In fact, we have a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Z}) & \hookrightarrow & X(\mathbb{Z}_S) \\ \downarrow & & \downarrow \\ H_{f,\mathbb{Z}}^1(G, U_2) & \hookrightarrow & H_f^1(G, U_2) \end{array}$$

Joint work with A. Tamagawa.

**Theorem 3 (local-global duality)** *The map*

$$H_{f,0}^1(G, U_2) \xrightarrow{\text{loc}_p} H_f^1(G_p, U_2) \xrightarrow{\psi_p} \mathbb{Q}_p$$

*is zero.*

Proof is straightforward using the standard the exact sequence

$$0 \rightarrow H^2(G_T, \mathbb{Q}_p(1)) \hookrightarrow \bigoplus_{v \in T} H^2(G_v, \mathbb{Q}_p(1)) \rightarrow \mathbb{Q}_p \rightarrow 0.$$

## IV. Explicit formulas

Choose a Weierstrass equation for  $E$  and let

$$\alpha = dx/y, \quad \beta = xdx/y.$$

Define

$$\log_{\alpha}(z) := \int_b^z \alpha, \quad \log_{\beta}(z) := \int_b^z \beta,$$

$$D_2(z) := \int_b^z \alpha\beta,$$

via (iterated) Coleman integration.

**Corollary 4** *Suppose we have a point  $y \in X(\mathbb{Z})$  of infinite order.*

*Then the set*

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

*lies inside the zero set of the analytic function*

$$\log_\alpha^2(y)(D_2(z) - \log_\alpha(z) \log_\beta(z)) - \log_\alpha^2(z)(D_2(y) - \log_\alpha(y) \log_\beta(y)).$$

Actually,

$$\psi_p \circ D^{-1} \circ \kappa_{DR/cr,2}^{na} = \text{Res}_e(vdx/y) \times$$

$$\left[ D_2(z) - \log_\alpha(z) \log_\beta(z) - \left( \frac{\log_\alpha(z)}{\log_\alpha(y)} \right)^2 (D_2(y) - \log_\alpha(y) \log_\beta(y)) \right],$$

where  $dv = xdx/y$ .

Remark:

-In particular, the function

$$(D_2(z) - \log_\alpha(z) \log_\beta(z)) / (\log_\alpha(z))^2$$

is constant on the integral points of infinite order.

-Parts of this construction generalize to affine curves  $X$  of genus  $g \geq 2$  whose Jacobians have Mordell-Weil rank  $g$ .

-Also to compact curves  $X$  provided

$$\text{rank} NS(J_X) \geq 2.$$

→ Possibility of computing points on curves of genus 2 with rank 2 Jacobians.