

# Selmer varieties

Minhyong Kim

20 October, 2008

Toronto

## I. General background

$(E, e)$  elliptic curve over  $\mathbb{Q}$ .

$G := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ .

The exact sequence

$$0 \rightarrow E[n] \rightarrow E(\bar{\mathbb{Q}}) \xrightarrow{n} E(\bar{\mathbb{Q}}) \rightarrow 0$$

of groups with  $G$ -action leads to the Kummer exact sequence:

$$0 \rightarrow E(\mathbb{Q})[n] \rightarrow E(\mathbb{Q}) \xrightarrow{n} E(\mathbb{Q}) \xrightarrow{\kappa} H^1(G, E[n])$$

In fact, the boundary map induces an injection

$$E(\mathbb{Q})/nE(\mathbb{Q}) \hookrightarrow H_f^1(G, E[n]),$$

where the subscript  $f$  refers to a subgroup of Galois cohomology satisfying a collection of local conditions: A *Selmer group*.

Because  $H_f^1(G, E[n])$  often admits an explicit description, this inclusion is applied to the problem of determining the group  $E(\mathbb{Q})$ . Usually, we fix a prime and run over its powers

$$E(\mathbb{Q})/p^n E(\mathbb{Q}) \hookrightarrow H_f^1(G, E[p^n])$$

leading to a conjectural isomorphism

$$E(\mathbb{Q}) \otimes \mathbb{Z}_p \simeq H_f^1(G, T_p(E))$$

where

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

is the  $p$ -adic Tate module of  $E$ .

When  $X/\mathbb{Q}$  is a curve of genus  $g \geq 2$  and  $b \in X(\mathbb{Q})$ , analogue of above construction

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

uses 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

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

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  $X(\mathbb{Q})$  from  $J(\mathbb{Q})$ .

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

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

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  $n = 2$ ,

$$0 \rightarrow \left[ \bigwedge^2 V / \mathbb{Q}_p(1) \right] \rightarrow U_2 \rightarrow V \rightarrow 0.$$

4.  $H^1(G, U_n)$  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.)

So the underlying input from Arakelov theory is the finiteness of the ideal class group, leading to finite-dimensionality of the  $H^i(G_T, U^{n+1} \setminus U^n)$ .

7. The map

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

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  $n = 1$ ,

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

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

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

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

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

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

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

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

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  $]y[ \subset X(\mathbb{Q}_p)$ ,

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

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

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

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

**Theorem 0.1** *Suppose*

$$\dim H_f^1(G, U_n) < \dim H_f^1(G_p, U_n)$$

*for some  $n$ . Then  $X(\mathbb{Q})$  is finite.*

Remarks:

-Theorem is a crude application of the methodology. Eventually would like refined descriptions of  $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$  as an amalgam of the method of Chabauty and Coleman and the work of Coates-Wiles, Kolyvagin, Rubin, Kato on the conjecture of Birch and Swinnerton-Dyer.

-Hypothesis of the theorem expected to always hold for  $n$  sufficiently large. But difficult to prove.

-Strategy is also inspired by an old conjecture of Lang.

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

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

vanishing on  $\text{Im}[H_f^1(G, U_n)]$ . Hence,  $\alpha \circ \kappa_{p,n}^{na}$  vanishes on  $X(\mathbb{Q})$ . But this function is a non-vanishing convergent power series on each residue disk.  $\square$

## II. Polylogarithmic quotients and CM Jacobians.

The complicated structure of  $U$  is an obstruction to direct usage. However, there are quotients of  $U$  with simpler structures. The *polylogarithm quotient* of  $U$  is defined by

$$W := U/[U^2, U^2].$$

Also comes with a De Rham realization

$$W^{DR} = U^{DR}/[(U^{DR})^2, (U^{DR})^2],$$

and the previous discussion carries over verbatim.

But now, we can control the dimension of Selmer varieties in a larger number of cases.

**Theorem 0.2 (with John Coates)** *Suppose  $J$  is isogenous to a product of abelian varieties having potential complex multiplication. Choose the prime  $p$  to split in all the CM fields that occur. Then*

$$\dim H_f^1(G, W_n) < \dim H_f^1(G_p, W_n)$$

*for  $n$  sufficiently large.*

**Corollary 0.3 (Faltings' theorem, special case)**  $X(\mathbb{Q})$  *is finite.*

Applies, for example, to the twisted Fermat curves

$$ax^m + by^m = cz^m$$

for  $a, b, c \in \mathbb{Q} \setminus \{0\}$  and  $m \geq 4$ .

Preliminaries:

Need to control

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

as  $n$  grows. This leads via the exact sequences

$$0 \rightarrow H^1(G_T, W^{n+1} \setminus W^n) \rightarrow H^1(G_T, W_n) \rightarrow H^1(G_T, W_{n-1})$$

to control of  $H_f^1(G, W_n) \subset H^1(G_T, W_n)$ . That is,

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

Since  $W^{n+1} \setminus W^n$  is a usual  $\mathbb{Q}_p$  representation, we have the Euler characteristic formula

$$\begin{aligned} & \dim H^0(G_T, W^{n+1} \setminus W^n) - \dim H^1(G_T, W^{n+1} \setminus W^n) \\ & + \dim H^2(G_T, W^{n+1} \setminus W^n) = -\dim[W^{n+1} \setminus W^n]^-. \end{aligned}$$

But the  $H^0$  term always, vanishes, so we get the formula

$$\begin{aligned} & \dim H^1(G_T, W^{n+1} \setminus W^n) = \\ & \dim[W^{n+1} \setminus W^n]^- + \dim H^2(G_T, W^{n+1} \setminus W^n). \end{aligned}$$

A fairly simple combinatorial analysis of the structure of  $W^{DR}$  shows that

$$\dim W_n^{DR}/F^0 \geq (2g - 2) \frac{n^{2g}}{(2g)!} + O(n^{2g-1}).$$

Meanwhile,

$$\sum_{i=1}^n \dim[W^{i+1} \setminus W^i]^- \leq [(2g - 1)/2] \frac{n^{2g}}{(2g)!} + O(n^{2g-1})$$

Since  $g \geq 2$ , we have

$$\sum_{i=1}^n \dim[W^{i+1} \setminus W^i]^- \ll \dim W_n^{DR}/F^0.$$

Therefore, it suffices to show that

$$\sum_{i=1}^n \dim H^2(G_T, W^{i+1} \setminus W^i) = O(n^{2g-1}).$$

Input from basic Iwasawa theory:

Let  $F/\mathbb{Q}$  be a finite extension such that all the CM is defined and such that  $F \supset \mathbb{Q}(J[p])$ . We can enlarge  $T$  to include all the primes that ramify in  $F$ . So we have

$$G_{F,T} := \text{Gal}(\mathbb{Q}_T/F) \subset G_T.$$

Because the corestriction map is surjective, it suffices to bound

$$\sum_{i=1}^n \dim H^2(G_{F,T}, W^{i+1} \setminus W^i).$$

If we examine the localization sequence

$$0 \rightarrow \mathbb{H}^2(W^{i+1} \setminus W^i) \rightarrow H^2(G_{F,T}, W^{i+1} \setminus W^i) \rightarrow \prod_{v|T} H^2(G_v, W^{i+1} \setminus W^i)$$

we see readily that

$$H^2(G_v, ) \simeq H^0(G_v, [W^{i+1} \setminus W^i]^*(1)) = 0$$

for  $i \neq 2$ . Thus, by Poitou-Tate duality, it suffices to bound

$$\mathbb{H}^2(W^{i+1} \setminus W^i) \simeq \mathbb{H}^1([W^{i+1} \setminus W^i]^*(1))^*.$$

The last group is defined by

$$\begin{aligned} 0 \rightarrow \mathbb{H}^1([W^{i+1} \setminus W^i]^*(1)) &\rightarrow H^1(G_{F,T}, [W^{i+1} \setminus W^i]^*(1)) \\ &\rightarrow \prod_{v|T} H^1(G_v, [W^{i+1} \setminus W^i]^*(1)). \end{aligned}$$

By the Hochschild-Serre sequence, the group

$$\mathbb{H}^1([W^{i+1} \setminus W^i]^*(1))$$

is included in

$$\mathrm{Hom}_\Gamma(M, [W^{i+1} \setminus W^i]^*(1)) = \mathrm{Hom}_\Gamma(M(-1), [W^{i+1} \setminus W^i]^*),$$

where  $\Gamma = \mathrm{Gal}(F_\infty/F)$  for the field

$$F_\infty = F(J[p^\infty])$$

generated by the  $p$ -power torsion of  $J$  and

$$M = \mathrm{Gal}(H/F_\infty)$$

is the Galois group of the  $p$ -Hilbert class field  $H$  of  $F_\infty$ .

Key fact (Greenberg following Iwasawa):

$M$  is a finitely generated torsion module over the Iwasawa algebra

$$\Lambda := \mathbb{Z}_p[[\Gamma]].$$

Let  $\mathcal{L} \in \Lambda$  be an annihilator for  $M(-1)/(\mathbb{Z}_p - \text{torsion})$ . Thus, if we knew an *Iwasawa main conjecture* for the  $\mathbb{Z}_p^r$ -extension  $F_\infty/F$ , we could take  $\mathcal{L}$  could to be a reduced multi-variable  $p$ -adic  $L$ -function.

For simplicity, we now assume that  $J$  itself has complex multiplication so that  $\Gamma \simeq \mathbb{Z}_p^{2g}$  and

$$\Lambda \simeq \mathbb{Z}_p[[T_1, \dots, T_{2g}]].$$

Let  $\{\chi_i\}_{i=1}^{2g}$  be the characters of  $G_{F,T}$  appearing in  $T_p J$  and  $\psi_i = \chi_i^*$ .

The characters that appear in  $[W^{i+1} \setminus W^i]^*$  are all of the form

$$\psi_{j_1} \psi_{j_2} \psi_{j_3} \cdots \psi_{j_i},$$

where  $j_1 < j_2 \geq j_3 \geq \cdots \geq j_i$ , each with multiplicity at most one.

For such a character to contribute to  $\text{Hom}_\Gamma(M(-1), [W^{i+1} \setminus W^i]^*)$ , we must have

$$\psi_{j_1} \psi_{j_2} \psi_{j_3} \cdots \psi_{j_i}(\mathcal{L}) = 0.$$

Furthermore, for each such character, we have a bound

$$\text{Hom}_\Gamma(M(-1), \psi_{j_1} \psi_{j_2} \psi_{j_3} \cdots \psi_{j_i}) < B,$$

where  $B$  is the number of  $\Lambda$  generators for  $M$ .

Thus the problem reduces to counting the number of zeros of  $\mathcal{L}$  among such characters.

The bulk of the contribution comes from indices of the form

$$k < 2g \geq j_3 \geq j_4 \geq \cdots j_i.$$

So we can count the zeros for the  $2g - 1$  twists

$$\mathcal{L}_k = \mathcal{L}(c_{k1}(T_1 + 1) - 1, c_{k2}(T_2 + 1) - 1, \dots, c_{k,2g}(T_{2g} + 1) - 1),$$

for  $c_{kj} = \psi_k(T_j + 1)\psi_{2g}(T_j + 1)$ , among

$$\psi_{j_3} \cdots \psi_{j_i}$$

for decreasing sequences  $(j_3, \dots, j_i)$  of numbers from  $\{1, 2, \dots, 2g\}$ .

When we try to bound

$$\sum_{i=2}^n \dim H^2(G_T, W^{i+1} \setminus W^i),$$

the possible multi-indices as  $i$  goes from 2 to  $n$  run over the lattice points inside a simplex of edge length  $n - 2$  inside a  $2g$ -dimensional space. Using a change of variable one can always reduce to  $\mathcal{L}$  of the form

$$\begin{aligned} \mathcal{L} = & a_0(T_1, \dots, T_{2g-1}) + a_1(T_1, \dots, T_{2g-1})T_{2g} + \dots \\ & + a_{l-1}(T_1, \dots, T_{2g-1})T_{2g}^{l-1} + T_{2g}^l. \end{aligned}$$

From this formula, one easily deduces a bound  $O(n^{2g-1})$  for the number of zeros.  $\square$

Remark:

Finiteness for elliptic curves follows the pattern

Non-vanishing of  $L$ -function  $\Rightarrow$  finiteness of Selmer group  
 $\Rightarrow$  finiteness of points.

For curves of higher genus with CM Jacobians, the implications are

Sparseness of  $L$ -zeros  $\Rightarrow$  bounds for Selmer varieties  $\Rightarrow$   
finiteness of points.