Introduction to Euler systems

김찬호

JBNU

SNU Algebra Camp 2025

Why (not) Euler systems?

Most lectures would begin with

Why (blah)? (e.g. Why Euler systems?)

Let me go with the opposite direction.

Why (not) Euler systems?

Most lectures would begin with

Why (blah)? (e.g. Why Euler systems?)

Let me go with the opposite direction.

Why you did not have to know Euler systems (still yet)?

Probably, some of you might hear the notion of Euler systems many times in various lectures, but did it work? Maybe not (e.g. me until 2013). Let me tell you why.

Why (not) Euler systems?

Most lectures would begin with

Why (blah)? (e.g. Why Euler systems?)

Let me go with the opposite direction.

Why you did not have to know Euler systems (still yet)?

Probably, some of you might hear the notion of Euler systems many times in various lectures, but did it work? Maybe not (e.g. me until 2013). Let me tell you why.
Although Euler systems are regarded as an important tool "in number theory", the method of Euler systems itself is a very specific and single-minded technique

Why (not) Euler systems?

Most lectures would begin with

Why (blah)? (e.g. Why Euler systems?)

Let me go with the opposite direction.

Why you did not have to know Euler systems (still yet)?

Probably, some of you might hear the notion of Euler systems many times in various lectures, but did it work? Maybe not (e.g. me until 2013). Let me tell you why.
Although Euler systems are regarded as an important tool “in number theory”, the method of Euler systems itself is a very specific and single-minded technique (to bound certain “arithmetically interesting” modules) in the framework of special values of L-functions.

The simplest application of Kato's Euler systems 0

We first illustrate a simple application of (the bottom of) Beilinson–Kato elements to the arithmetic of elliptic curves. Let's fix the convention:

- p, a prime.
- E, an elliptic curve over $\mathbb{Q}$ (without complex multiplication).
- $T = \mathrm{Ta}_p E = \varprojlim_n E(\overline{\mathbb{Q}})[p^k]$, the p-adic Tate module of E.
- $V = V_p E = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, the 2-dimensional $\mathbb{Q}_p$-vector space endowed with the continuous action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_p}(V) \simeq \mathrm{GL}_2(\mathbb{Q}_p)$, the corresponding Galois representation.

Let Σ be a finite set of places of $\mathbb{Q}$ containing p, ∞, and bad reduction primes for E, and denote by $\mathbb{Q}_\Sigma$ the maximal extension of $\mathbb{Q}$ unramified outside Σ. Then the information of $E(\mathbb{Q})$ can be detected in Galois cohomology group $\mathrm{H}^1(\mathbb{Q}, V) = \mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, V)$ via Kummer map

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p \to \mathrm{H}^1(\mathbb{Q}, V)$$

which makes the connection between geometry and cohomology.

The simplest application of Kato's Euler systems 1

Exercise

- Why $\mathrm{H}^1(\mathbb{Q}, V) = \mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, V)$? In other words, why does the action of $G_{\mathbb{Q}}$ on V factor through $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$?
- Can you write down the Kummer map explicitly?

The simplest application of Kato's Euler systems 2

The same rule applies to the local case. We first investigate the local nature of Galois cohomology at p. The local Kummer map $E(\mathbb{Q}_p) \otimes \mathbb{Q}_p \hookrightarrow \mathrm{H}^1(\mathbb{Q}_p, V)$ embeds a 1-dimensional geometric object into a 2-dimensional cohomological one (why?). The Weil pairing

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

induces a non-degenerate cup product pairing (the local Tate pairing)

$$\langle -, - \rangle_p : \mathrm{H}^1(\mathbb{Q}_p, V) \times \mathrm{H}^1(\mathbb{Q}_p, V) \xrightarrow{\cup} \mathrm{H}^2(\mathbb{Q}_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p.$$

Under this pairing, we have the following orthogonality

$$E(\mathbb{Q}_p) \otimes \mathbb{Q}_p \perp E(\mathbb{Q}_p) \otimes \mathbb{Q}_p$$

due to local Tate duality.
The base field $\mathbb{Q}_p$ can be replaced by other local fields $\mathbb{Q}_\ell$ (with $\ell \neq p$) and $\mathbb{R}$. The formalism applies in the same way, but the actual computation will be different.

The simplest application of Kato's Euler systems 3

Exercise

- Check the statement of the local Tate duality.
- Compute the $\mathbb{F}_p$-dimension of $\mathrm{H}^1(\mathbb{Q}_p, E[p])$ (Hint: Use the local Euler characteristic formula.) Can you do the same thing for $\mathrm{H}^1(\mathbb{Q}_p, V)$?
- Compute the $\mathbb{Q}_p$-dimension of $\mathrm{H}^1(\mathbb{Q}_\ell, V)$ (Hint: Use the local Euler characteristic formula again.)
- Did you recognize that V is self-dual, i.e. $V \simeq \mathrm{Hom}(V, \mathbb{Q}_p(1))$, thanks to the Weil pairing?

The simplest application of Kato's Euler systems 4

We expand the picture of the cup product pairing:

$$
\begin{tikzcd}
\mathrm{H}^1(\mathbb{Q}_p, V) & \times & \mathrm{H}^1(\mathbb{Q}_p, V) \arrow[r] \arrow[dd, "\exp^*_{\omega_E}"] & \mathbb{Q}_p \arrow[dd, equal] \\
E(\mathbb{Q}_p) \otimes \mathbb{Q}_p \arrow[u, hook] & & & \\
\mathbb{Q}_p \arrow[u, "\exp_{\widehat{E}}", "\simeq"'] & \times & \mathbb{Q}_p \arrow[r] & \mathbb{Q}_p \\
& & \mathrm{H}^0(E/\mathbb{Q}_p, \Omega^1). \arrow[u, "\simeq"'] &
\end{tikzcd}
$$

and explain the precise meaning of each term:

- The map $\exp_{\widehat{E}} : \mathbb{Q}_p \to E(\mathbb{Q}_p) \otimes \mathbb{Q}_p$ extends the formal exponential map $\exp_{\widehat{E}} : p\mathbb{Z}_p \to \widehat{E}(p\mathbb{Z}_p)$. Denote by ω^*_E the basis of the tangent space $\mathbb{Q}_p\omega^*_E$ of $E/\mathbb{Q}_p$ at the identity characterized by the natural pairing $\langle \omega_E, \omega^*_E \rangle = 1$. If we identify the source $\mathbb{Q}_p$ with $\mathbb{Q}_p\omega^*_E$ by sending 1 to ω^*_E, then the exponential map coincides with the Lie group exponential map.
- The latter $\mathbb{Q}_p$ in the diagram is isomorphic to the space of global 1-forms $\mathrm{H}^0(E/\mathbb{Q}_p, \Omega^1) = \mathbb{Q}_p\omega_E$, i.e. the cotangent space and of $E/\mathbb{Q}_p$ at the identity, by sending 1 to ω_E.
- The above dual exponential map $\exp^*_{\omega_E} : \mathrm{H}^1(\mathbb{Q}_p, V) \to \mathbb{Q}_p$ is the composition of Bloch–Kato's dual exponential map $\exp^* : \mathrm{H}^1(\mathbb{Q}_p, V) \to \mathrm{H}^0(E/\mathbb{Q}_p, \Omega^1)$ and the above isomorphism $\mathrm{H}^0(E/\mathbb{Q}_p, \Omega^1) \simeq \mathbb{Q}_p$.
- The bottom pairing of the diagram is given by multiplication: $(a, b) \mapsto a \cdot b$.

The simplest application of Kato's Euler systems 5

The characterization of the kernel of the dual exponential map is important.

$$\ker(\exp^*_{\omega_E}) = E(\mathbb{Q}_p) \otimes \mathbb{Q}_p \subseteq \mathrm{H}^1(\mathbb{Q}_p, V). \tag{1}$$

We now see the simplest form of Kato's work and feel its power for the first time.

Theorem (Kato)

There exists a global Galois cohomology class $z_{\mathbb{Q}} \in \mathrm{H}^1(\mathbb{Q}, V)$ *such that*

$$\begin{array}{ccccc} \mathrm{H}^1(\mathbb{Q}, V) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1(\mathbb{Q}_p, V) & \xrightarrow{\exp^*} & \mathbb{Q}_p\omega_E \\ z_{\mathbb{Q}} & \longmapsto & & & \exp^*(\mathrm{loc}_p(z_{\mathbb{Q}})) \end{array}$$

and

$$\exp^*(\mathrm{loc}_p(z_{\mathbb{Q}})) = \frac{L^{(p)}(E,1)}{\Omega^+_E} \cdot \omega_E$$

where $L^{(p)}(E,1)$ *is the* L*-value of* E *at* $s=1$ *removing the Euler factor at* p*.*

The simplest application of Kato's Euler systems 6

Corollary (Kato)

If $\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) > 0$, *then* $L(E,1) = 0$.

Proof.

Let $P \in E(\mathbb{Q})$ be a point of infinite order. Under the natural map

$$E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p) \to E(\mathbb{Q}_p)\widehat{\otimes}_{\mathbb{Z}}\mathbb{Z}_p \to E(\mathbb{Q}_p) \otimes \mathbb{Q}_p,$$

the image of P generates $E(\mathbb{Q}_p) \otimes \mathbb{Q}_p$. Since both $z_{\mathbb{Q}} \in \mathrm{H}^1(\mathbb{Q}, V)$ and P are global, the global reciprocity law implies that

$$\sum_{\ell \leq \infty} \langle \mathrm{loc}_\ell(z_{\mathbb{Q}}), P \rangle_\ell = 0.$$

Since $\mathrm{H}^1(\mathbb{Q}_\ell, V) = 0$ for every place $\ell \neq p$ (including the infinite place), we have $\langle \mathrm{loc}_\ell(z_{\mathbb{Q}}), P \rangle_p = 0$. By the self-orthogonality of $E(\mathbb{Q}_p) \otimes \mathbb{Q}_p$, we have $\mathrm{loc}_p(z_{\mathbb{Q}}) \in E(\mathbb{Q}_p) \otimes \mathbb{Q}_p$. By (1), $\exp^* \circ \mathrm{loc}_p(z_{\mathbb{Q}}) = 0$. Thus, $L(E,1) = 0$ by Kato's theorem. $\square$

This is the very starting point of Kato's Euler systems, and the cohomology class $z_{\mathbb{Q}}$ is just a part of a much deeper object.

The simplest application of Kato's Euler systems 7

Exercise

Check the statement of this form of the global reciprocity law (in class field theory).

L-functions and Galois cohomology: the set up

Recall the convention (with slight generalizations)

- $p > 2$, a prime
- $F/\mathbb{Q}_p$, finite extension (the coefficient field)
- $\mathcal{O} = \mathcal{O}_F$ with uniformizer ϖ
- T, a free $\mathcal{O}$-module of finite rank n with the continuous action of $G_{\mathbb{Q}}$
- $V = T \otimes_{\mathcal{O}} F$
- $W = V/T$, the discrete Galois module, which is co-free over $\mathcal{O}$.
- For $m \geq 1$, write $W_m = W[\varpi^m]$, $T_m = T/\varpi^m T$.
- $V^*(1) = \mathrm{Hom}(V, F(1))$, $W^*(1) = \mathrm{Hom}(T, F/\mathcal{O}(1))$.

Assume V is geometric (in the sense of Fontaine–Mazur), i.e.

- V is unramified outside a finite set of primes Σ.
- V is de Rham at p in the sense of Fontaine's theory of p-adic periods.

Exercise (a big one)

Study p-adic Hodge theory (for future).

L-functions and Galois cohomology: L-functions

For $\ell \notin \Sigma$, let

$$P_\ell(V,x) = \det(I_n - x \cdot \rho(\mathrm{Frob}_\ell)|_V)$$

where Frob_ℓ is the arithmetic Frobenius at ℓ. Set

$$L^\Sigma(V,s) = \prod_{\ell \notin \Sigma} P(V, \ell^{-s})^{-1}$$

which converges for $\mathrm{Re}(s) \gg 0$ (depending on the behavior of Frobenius eigenvalues).
For elliptic curves, we have $P(V, \ell^{-s}) = 1 - a_\ell \ell^{-s} + \ell^{1-2s}$ where $a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell)$. It is known that the Hasse bound $|a_\ell| \leq 2\sqrt{\ell}$ gives the convergence abscissa $\mathrm{Re}(s) > \dfrac{3}{2}$.

L-functions and Galois cohomology: Selmer structures

We recall the notion of Selmer structures/local conditions.

- For every prime ℓ except p and ∞, define

$$\mathrm{H}^1_f(\mathbb{Q}_\ell, V) = \ker\left(\mathrm{H}^1(\mathbb{Q}_\ell, V) \to \mathrm{H}^1(I_\ell, V)\right)$$

  where $I_\ell \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ is the inertia subgroup at ℓ.
- For $\ell = \infty$, we have $\mathrm{H}^1_f(\mathbb{R}, V) = 0$ since $p > 2$.
- For $\ell = p$, we consider two different structures:
  - $\mathrm{H}^1_f(\mathbb{Q}_p, V) = 0$ for the p-strict Selmer groups.
  - $\mathrm{H}^1_f(\mathbb{Q}_p, V) = \ker\left(\mathrm{H}^1(\mathbb{Q}_p, V) \to \mathrm{H}^1(\mathbb{Q}_p, V \otimes \mathbf{B}_{\mathrm{cris}})\right)$ for the Bloch–Kato Selmer groups.

In any case, $\mathrm{H}^1_f(\mathbb{Q}_\ell, T)$ and $\mathrm{H}^1_f(\mathbb{Q}_\ell, W)$ are defined as the preimage and the image of $\mathrm{H}^1_f(\mathbb{Q}_\ell, V)$ with respect to $T \to V \to W$, respectively. Write $\mathrm{H}^1_{/f} = \dfrac{\mathrm{H}^1}{\mathrm{H}^1_f}$.

Exercise

Check $\mathrm{H}^1_f(\mathbb{Q}_\ell, V) = \mathrm{H}^1(\mathbb{F}_\ell, V^{I_\ell})$, i.e. be comfortable with the inflation-restriction sequence argument. (a part of "Hochschild–Serre spectral sequence" in group cohomology)

L-functions and Galois cohomology: Selmer groups

Let Σ' be a finite set of primes and M be a Galois module. Then the Σ'-relaxed Selmer group of M is defined by

$$\begin{aligned}\mathrm{Sel}^{\Sigma'}(\mathbb{Q}, M) &= \ker\left(\mathrm{H}^1(\mathbb{Q}, M) \to \prod_{\ell \notin \Sigma'} \mathrm{H}^1_{/f}(\mathbb{Q}_\ell, M)\right) \\ &= \ker\left(\mathrm{H}^1(\mathbb{Q}_{\Sigma\cup\Sigma'}/\mathbb{Q}, M) \to \prod_{\ell \notin (\Sigma\cup\Sigma')\setminus\Sigma} \mathrm{H}^1_{/f}(\mathbb{Q}_\ell, M)\right)\end{aligned}$$

and the Σ'-strict Selmer group of M is defined by

$$\mathrm{Sel}_{\Sigma'}(\mathbb{Q}, M) = \ker\left(\mathrm{Sel}^{\Sigma'}(\mathbb{Q}, M) \to \prod_{\ell \in \Sigma'} \mathrm{H}^1(\mathbb{Q}_\ell, M)\right).$$

Exercise

See Milne's Arithmetic duality theorems for checking the notion of Selmer groups is independent of Σ (not Σ' above!).

L-functions and Galois cohomology

The weak form of the Bloch–Kato conjecture can be stated as follows:

Conjecture (Bloch–Kato)

$$\mathrm{ord}_{s=0} L(V,s) = \dim_F \mathrm{Sel}(\mathbb{Q}, V^*(1)) - \dim_F \mathrm{H}^0(\mathbb{Q}, V^*(1)).$$

In fact, Kato proved the following stronger theorem.

Theorem (Kato)

Let E be an elliptic curve without complex multiplication. Let $p > 2$ be a prime such that T has large image. If $L(E,1) \neq 0$, then $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$ is finite, so $\mathrm{Sel}(\mathbb{Q}, V) = 0$.

We need more than $z_{\mathbb{Q}}$ for this statement.

Definition of Euler systems

Let $\mathbb{Q}^{\mathrm{ab}}$ be the maximal abelian extension of $\mathbb{Q}$.

Definition

An **Euler system for** T is a collection of cohomology classes

$$\mathbf{z} = \left\{ z_K \in \mathrm{H}^1(K, T) : \mathbb{Q} \subseteq K \subseteq \mathbb{Q}^{\mathrm{ab}} \right\}$$

where K runs over *finite* extensions of $\mathbb{Q}$ in $\mathbb{Q}^{\mathrm{ab}}$ such that

$$\mathrm{cores}_{\mathbb{Q}(\zeta_{n\ell})/\mathbb{Q}(\zeta_n)}(z_{\mathbb{Q}(\zeta_{n\ell})}) = \begin{cases} z_{\mathbb{Q}(\zeta_n)} & \text{if } \ell | n \text{ or } \ell \in \Sigma \\ P_\ell(V^*(1), \mathrm{Frob}_\ell^{-1}) \cdot z_{\mathbb{Q}(\zeta_n)} & \text{otherwise.} \end{cases}$$

This system remembers most Euler factors of the L-function (of the dual side). This is why we call it an Euler system.

As a rough picture, $z_{\mathbb{Q}(\zeta_n)}$ is related to $L(V \otimes \mathbb{Q}(\zeta_n), 0)$ and $\mathrm{cores}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(z_{\mathbb{Q}(\zeta_n)}\right)$ is related to $L^{\Sigma_n}(V, 0)$ where $\Sigma_n = \Sigma \cup \{\ell | n\}$.

The "main theorem" of Euler systems

Theorem (Rubin)

Let $\mathbf{z}$ *be an Euler system for* T*. Suppose that* T *has large image:*

- $T/\varpi T$ *is irreducible, and*
- *there exists* $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_{p^\infty}))$ *such that* $T/(\tau - 1)T$ *is free of rank one over* $\mathcal{O}$*.*

If $z_{\mathbb{Q}}$ *is not a torsion in* $\mathrm{H}^1(\mathbb{Q}, T)$*, then* $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1))$ *is finite.*

We try to explain how the Euler system works intuitively. We actually bound $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*_m(1))$ independently of m. The main tools are (of course) local and global dualities in Galois cohomology.

Local and global dualities

Let

$$\langle -, - \rangle_\ell : \mathrm{H}^1(\mathbb{Q}_\ell, W_m) \times \mathrm{H}^1(\mathbb{Q}_\ell, W_m^*(1)) \to \mathcal{O}/\varpi^m\mathcal{O}$$

be the local Tate pairing. Then the local duality says $\mathrm{H}^1_f(\mathbb{Q}_\ell, W_m)^\perp = \mathrm{H}^1_f(\mathbb{Q}_\ell, W_m^*(1))$. Fix a finite set of primes Σ' not including p. Consider the diagram

$$\begin{tikzcd}
\mathrm{Sel}^{\{p\}}(\mathbb{Q}, W_m) \arrow[r, hook] & \mathrm{Sel}^{\Sigma' \cup \{p\}}(\mathbb{Q}, W_m) \arrow[r, "\mathrm{loc}^s_{\Sigma'}"] & \bigoplus_{\ell \in \Sigma'} \mathrm{H}^1_{/f}(\mathbb{Q}_\ell, W_m) \\
 & & \times \\
\mathrm{Sel}_{\Sigma' \cup \{p\}}(\mathbb{Q}, W_m^*(1)) \arrow[r, hook] & \mathrm{Sel}_{\{p\}}(\mathbb{Q}, W_m^*(1)) \arrow[r, "\mathrm{loc}^f_{\Sigma'}"] & \bigoplus_{\ell \in \Sigma'} \mathrm{H}^1_f(\mathbb{Q}_\ell, W_m^*(1)) \arrow[d, "\sum_{\ell \in \Sigma'} \langle -, - \rangle_\ell"'] \\
 & & \mathcal{O}/\varpi^m\mathcal{O}
\end{tikzcd} \tag{2}$$

where

$$\mathrm{loc}^s_{\Sigma'} = \bigoplus_{\ell \in \Sigma'} \mathrm{loc}^s_\ell : \mathrm{Sel}^{\Sigma' \cup \{p\}}(\mathbb{Q}, W_m) \to \bigoplus_{\ell \in \Sigma'} \mathrm{H}^1(\mathbb{Q}_\ell, W_m) \to \bigoplus_{\ell \in \Sigma'} \mathrm{H}^1_{/f}(\mathbb{Q}_\ell, W_m),$$

$$\mathrm{loc}^f_{\Sigma'} = \bigoplus_{\ell \in \Sigma'} \mathrm{loc}^f_\ell : \mathrm{Sel}_{\{p\}}(\mathbb{Q}, W_m^*(1)) \to \bigoplus_{\ell \in \Sigma'} \mathrm{H}^1_f(\mathbb{Q}_\ell, W_m^*(1)).$$

The global duality implies

$$\mathrm{im}(\mathrm{loc}^s_{\Sigma'})^\perp = \mathrm{im}(\mathrm{loc}^f_{\Sigma'}).$$

The key intuition of the Euler system argument

One of the key intuitions of the Euler system argument is the following behavior:

If $\mathrm{im}(\mathrm{loc}^s_{\Sigma'})$ *gets larger, then* $\mathrm{im}(\mathrm{loc}^f_{\Sigma'})$ *gets smaller.*

Therefore, it suffices to construct "relevant" Σ' and elements $\kappa_{\Sigma'} \in \mathrm{Sel}^{\Sigma' \cup \{p\}}(\mathbb{Q}, W_m)$ from $\mathbf{z}$ such that

- $\kappa_{\Sigma'}$ is ramified at primes in Σ', so its image under $\mathrm{loc}^s_{\Sigma'}$ is non-trivial, and
- $\mathrm{length}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma'}))$ and $\mathrm{length}(\mathrm{Sel}_{\Sigma' \cup \{p\}}(\mathbb{Q}, W^*_m(1)))$ are bounded independently of m.

Here, $\kappa_{\Sigma'}$'s are called **Kolyvagin derivative classes**.

Remark

Also, "relevant" Σ' means that the image of the arithmetic Frobenius Frob_ℓ at $\ell \in \Sigma'$ is equivalent to the image of $\tau \in \mathrm{Gal}(\mathbb{Q}(W_m)(\zeta_{p^m})/\mathbb{Q})$. Chebotarev density theorem plays the key role to construct such a Σ'.

The finiteness of the p-strict Selmer group $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1))$ can be proved in this way.

Application of the explicit reciprocity law

From now on, we consider the case of elliptic curves only.
How to obtain the finiteness of $\mathrm{Sel}(\mathbb{Q}, W^*(1))$ from the finiteness of $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1))$? We now compare the difference between $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1))$ and $\mathrm{Sel}(\mathbb{Q}, W^*(1))$. We consider the following variant of (2) with the Bloch–Kato local condition at p. In other words, we have

$$\begin{tikzcd}
\mathrm{Sel}(\mathbb{Q}, T) \arrow[r, hook] & \mathrm{Sel}^{\{p\}}(\mathbb{Q}, T) \arrow[r, "\mathrm{loc}^s_p"] & \mathrm{H}^1_{/f}(\mathbb{Q}_p, T) \\
 & & \times \\
\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1)) \arrow[r, hook] & \mathrm{Sel}(\mathbb{Q}, W^*(1)) \arrow[r, "\mathrm{loc}^f_p"] & \mathrm{H}^1_f(\mathbb{Q}_p, W^*(1)) \arrow[d, "\langle -,- \rangle_p"'] \\
 & & F/\mathcal{O}
\end{tikzcd}$$

with $\mathrm{im}(\mathrm{loc}^s_p)^\perp = \mathrm{im}(\mathrm{loc}^f_p)$. Note that $\mathrm{H}^1_f(\mathbb{Q}_p, T)^\perp = \mathrm{H}^1_f(\mathbb{Q}_p, W^*(1))$.

The finiteness of Selmer groups

Therefore, the proof of the finiteness of $\mathrm{Sel}(\mathbb{Q}, W^*(1))$ reduces to showing that the rational restriction map

$$\mathrm{loc}^s_p : \mathrm{Sel}^{\{p\}}(\mathbb{Q}, V) \to \mathrm{H}^1_{/f}(\mathbb{Q}_p, V)$$

is surjective. Since we have

$$\begin{array}{ccccc} \mathrm{Sel}^{\{p\}}(\mathbb{Q}, V) & \xrightarrow{\mathrm{loc}^s_p} & \mathrm{H}^1_{/f}(\mathbb{Q}_p, V) & \xrightarrow[\simeq]{\exp^*} & \mathrm{Fil}^0(\mathbf{D}_{\mathrm{cris}}(V)) \\ z_{\mathbb{Q}} & \longmapsto & & & \exp^* \circ \mathrm{loc}^s_p(z_{\mathbb{Q}}) = \dfrac{L^{(p)}(E,1)}{\Omega^+_E} \cdot \omega_E \neq 0, \end{array}$$

loc^s_p is surjective. The finiteness of Selmer groups follows.

From Euler systems to Kolyvagin systems

We move to *Kolyvagin systems*.
First, why Kolyvagin systems? There are at least two advantages.

1. The sharp bound via the primitivity, which gives a mod p criterion for verifying the exact Bloch–Kato type formula and the Iwasawa main conjecture.
2. The structure theorem, not only the size.

We focus on the second advantage. By utilizing the Kolyvagin system argument, the following statement

> *If* $\mathbf{z} = \{z_K\}_K$ *is an Euler system and* $z_{\mathbb{Q}}$ *is not a torsion, then* $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1))$ *is finite.*

can be refined as follows:

> *Let* $\boldsymbol{\kappa} = \{\kappa_n\}_n$ *be the Kolyvagin system attached to the above Euler system* $\mathbf{z}$*. If* $\boldsymbol{\kappa}$ *is non-trivial, then the structure of* $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, W^*(1))$ *is described in terms of all* κ_n*'s.*

Kolyvagin derivatives

We restrict ourselves to the case of elliptic curves again. Let $\mathbf{z} = \{z_K\}_K$ be Kato's Euler system. Then $z_K \in \mathrm{H}^1(K, T)$ is characterized by

$$\sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} (\exp^* \circ \mathrm{loc}_p^s z_K^\sigma) \cdot \chi(\sigma) = \frac{L^{(Sp)}(E, \chi, 1)}{\Omega_E^{\chi(-1)}} \cdot \omega_E$$

where χ is an even character of $\mathrm{Gal}(K/\mathbb{Q})$, and S is the product of the ramified primes of $K/\mathbb{Q}$.

For an integer $m \geq 1$, denote by $\mathcal{P}_m$ the set of primes ℓ such that $(\ell, Np) = 1$, $a_\ell \equiv \ell + 1 \pmod{p^m}$ and $\ell \equiv 1 \pmod{p^m}$. For each $\ell \in \mathcal{P}_m$, fix a primitive root η_ℓ mod ℓ and write

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) & \xleftarrow{\simeq} & (\mathbb{Z}/\ell\mathbb{Z})^\times \\ \sigma_{\eta_\ell} & \longleftarrow\!\!\shortmid & \eta_\ell \end{array}$$

the Kolyvagin derivative operator D_ℓ at $\ell \in \mathcal{P}_m$ is defined by

$$D_\ell = \sum i \cdot \sigma_{\eta_\ell}^i$$

Let $\mathcal{N}_m$ be the set of square-free products of primes in $\mathcal{P}_m$ and $n \in \mathcal{N}_m$. Then we define $D_n = \prod_{\ell | n} D_\ell$.

Exercise

$$(\sigma_{\eta_\ell} - 1) \cdot D_\ell = (\ell - 1) - \mathrm{Nm}_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}$$

in $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})]$.

Refining Selmer structures

What should we do for the refinement? We need to be more careful about the Selmer structure. We need slightly more than ramified classes.
Let $z_{\mathbb{Q}(\zeta_n)}$ be an Euler system class. Applying the Kolyvagin derivative $D_n \in \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})]$ to $z_{\mathbb{Q}(\zeta_n)}$, we have *a priori*

$$\kappa'_n := D_{\mathbb{Q}(\zeta_n)} z_K \mathbb{Q}(\zeta_n) \pmod{\varpi^m} \in \mathrm{Sel}^{\{p,\ell:\ell|n\}}(\mathbb{Q}, W_m).$$

Indeed, we can organize $\kappa'_{\mathbb{Q}(\zeta_n)}$ with more controlled local conditions at primes dividing n.
Let ℓ be a prime with $\ell \equiv 1 \pmod{\varpi^m}$. Then the transverse local condition at ℓ is defined by

$$\mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, W_m) = \ker\left(\mathrm{H}^1(\mathbb{Q}_\ell, W_m) \to \mathrm{H}^1(\mathbb{Q}_\ell(\zeta_\ell), W_m)\right),$$

and it can be viewed as the complement of H^1_f at ℓ. There exists the finite-singular comparison isomorphism

$$\varphi^{\mathrm{fs}}_\ell : \mathrm{H}^1_f(\mathbb{Q}_\ell, W_m) \to \mathrm{H}^1_{/f}(\mathbb{Q}_\ell, W_m) = \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, W_m)$$

obtained from the Euler factor at ℓ. We would like to construct

$$\kappa_n \in \mathrm{Sel}^{\{p\}}_{n\text{-tr}}(\mathbb{Q}, W_m),$$

i.e. $\mathrm{loc}_\ell(\kappa_n) \in \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, W_m)$ for every ℓ dividing n. In Kato's case, $\kappa_n = \kappa'_n$.

Why the transverse local condition?

The axiom for Kolyvagin systems is the following local relation

$$\mathrm{loc}_\ell(\kappa_{n\ell}) = \varphi_\ell^{\mathrm{fs}}(\mathrm{loc}_\ell(\kappa_n)).$$

Proposition

1. $\mathrm{H}^1_f(\mathbb{Q}_\ell, W_m)$ *and* $\mathrm{H}^1_f(\mathbb{Q}_\ell, W_m^*(1))$ *are orthogonal to each other with respect to* $\langle -, - \rangle_\ell$.
2. $\mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, W_m)$ *and* $\mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, W_m^*(1))$ *are orthogonal to each other with respect to* $\langle -, - \rangle_\ell$.

The Euler-to-Kolyvagin map

Write $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ for convenience. Let $\mathrm{ES}(\mathbb{Q}(\zeta_n), T) \subseteq \mathrm{H}^1(\mathbb{Q}(\zeta_n), T)$ be the $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})]$-submodule generated by cohomology classes in $\mathrm{H}^1(\mathbb{Q}(\zeta_n), T)$ which are parts of Euler systems for T. Then we have the commutative diagram

$$\begin{tikzcd}
\mathrm{ES}(\mathbb{Q}(\zeta_n), T) \arrow[r, "D_n"] \arrow[rrdd] & D_n\left(\mathrm{ES}(\mathbb{Q}(\zeta_n), T)\right) \arrow[r, "\mathrm{mod}\ p^m"] & \left(\mathrm{H}^1(\mathbb{Q}(\zeta_n), T)/p^m\right)^{G_n} \arrow[d, hook] \\
& & \mathrm{H}^1(\mathbb{Q}(\zeta_n), T/p^mT)^{G_n} \arrow[d, "\mathrm{res}^{-1}", "\simeq"'] \\
& & \mathrm{H}^1(\mathbb{Q}, T/p^mT)
\end{tikzcd}$$

and the Euler system class $z_{\mathbb{Q}(\zeta_n)}$ maps to the Kolyvagin system class κ_n following the above diagram

$$z_{\mathbb{Q}(\zeta_n)} \mapsto D_n z_{\mathbb{Q}(\zeta_n)} \mapsto D_n z_{\mathbb{Q}(\zeta_n)} \pmod{p^m} \mapsto \kappa_n.$$

Here, the restriction map is an isomorphism since we assume the large Galois image assumption. (Why is $D_n z_{\mathbb{Q}(\zeta_n)} \pmod{p^m}$ Galois invariant?)

Kolyvagin system argument

We now explain how the Kolyvagin system argument works. We now fix *one* integer $m \geq 1$ while every positive integer m was considered together before. Let $\boldsymbol{\kappa}^{(m)} = (\kappa_n^{(m)})_{n \in \mathcal{N}_m}$ be the mod p^m reduction of Kato's Kolyvagin system $\boldsymbol{\kappa}$, and

$$\lambda(n, E[p^m]) = \mathrm{length}_{\mathbb{Z}_p}\left(\mathrm{Sel}_{\{p\},n\text{-}\mathrm{tr}}(\mathbb{Q}, E[p^m])\right),$$

$$\partial^{(r)}(\boldsymbol{\kappa}^{(m)}) = \min\left\{m - \mathrm{length}_{\mathbb{Z}_p}\left(\mathbb{Z}/p^m\mathbb{Z} \cdot \kappa_n^{(m)}\right) : n \in \mathcal{N}_m, \nu(n) = r\right\}.$$

Theorem (Mazur–Rubin)

Suppose that $\boldsymbol{\kappa}^{(m)}$ is non-trivial. Then there exists an integer $j \geq 0$ such that

$$\mathbb{Z}/p^m\mathbb{Z} \cdot \kappa_n^{(m)} = p^{j+\lambda(n,E[p^m])} \cdot \mathrm{Sel}^{\{p\}}_{n\text{-}\mathrm{tr}}(\mathbb{Q}, E[p^m])$$

for every $n \in \mathcal{N}_m$.

It is also known that there is a non-canonical isomorphism

$$\mathrm{Sel}^{\{p\}}_{n\text{-}\mathrm{tr}}(\mathbb{Q}, E[p^m]) \simeq \mathbb{Z}/p^m\mathbb{Z} \oplus \mathrm{Sel}_{\{p\},n\text{-}\mathrm{tr}}(\mathbb{Q}, E[p^m])$$

for every $n \in \mathcal{N}_m$.

The structure theorem

Theorem (Mazur–Rubin)

Suppose that $\boldsymbol{\kappa}^{(m)}$ is non-trivial. Write

$$\mathrm{Sel}_{\{p\}}(\mathbb{Q}, E[p^m]) \simeq \bigoplus_{i \geq 1} \mathbb{Z}/p^{d_i}\mathbb{Z}$$

with $d_1 \geq d_2 \geq \cdots$. Then for every $r \geq 0$, we have

$$\partial^{(r)}(\boldsymbol{\kappa}^{(m)}) = \min \left\{ m, j + \sum_{i > r} d_i \right\}.$$

The proof 1

What we know is:

$$\partial^{(r)}(\boldsymbol{\kappa}^{(m)}) = \min\{m, j + \lambda(n, E[p^m]) : \nu(n) = r\}.$$

Therefore, the $r = 0$ case follows from

$$\lambda(1, E[p^m]) = \sum_{i>0} d_i.$$

Suppose $n \in \mathcal{N}_m$ and $\nu(n) = r > 0$. Consider the map

$$\bigoplus_{\ell | n} \mathrm{loc}_\ell : \mathrm{Sel}_{\{p\}}(\mathbb{Q}, E[p^m]) \to \bigoplus_{\ell | n} E(\mathbb{Q}_\ell) \otimes \mathbb{Z}/p^m\mathbb{Z} \simeq (\mathbb{Z}/p^m\mathbb{Z})^{\oplus \nu(n)}.$$

The RHS is free of rank r over $\mathbb{Z}/p^m\mathbb{Z}$. Thus, the image is a quotient of $\mathrm{Sel}_{\{p\}}(\mathbb{Q}, E[p^m])$ generated by at most r elements. Thus, the length of the image is at most $\sum_{i \leq r} d_i$, and the length of the kernel is at least $\sum_{i>r} d_i$. Also, the kernel of this map is contained in

$$\mathrm{Sel}_{\{p\}, n\text{-tr}}(\mathbb{Q}, E[p^m]).$$

Therefore, $\lambda(n, E[p^m]) \geq \sum_{i>r} d_i$, so

$$\partial^{(r)}(\boldsymbol{\kappa}^{(m)}) \geq \min\left\{m, j + \sum_{i>r} d_i\right\}.$$

The proof 2

It suffices to prove the opposite inequality. We use induction on r. The $r = 0$ case is already done. Using Chebotarev density theorem, we can (carefully) choose a prime $\ell \in \mathcal{P}_m$ such that

- $\mathrm{Sel}_{\{p,\ell\},n\text{-tr}}(\mathbb{Q}, E[p^m]) \simeq \bigoplus_{i>r+1} \mathbb{Z}/p^{d_i}\mathbb{Z}$, and
- $\mathrm{Sel}_{\{p,\ell\},n\text{-tr}}(\mathbb{Q}, E[p^m]) = \mathrm{Sel}_{\{p\},n\ell\text{-tr}}(\mathbb{Q}, E[p^m])$.

We are done. It is remarkable that each choice of ℓ kills one generator of the p-strict Selmer group.

Exercise

Exercise

Fix a positive integer m and Let S be the set of square-free products of primes ℓ such that $\ell \equiv \pm 1 \pmod{m}$, i.e. the Frobenius at ℓ is trivial in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})$. For $r \in S$, let

$$\xi_r = \left(\zeta_m \cdot \prod_{\ell | r} \zeta_\ell - 1 \right) \cdot \left(\zeta_m^{-1} \cdot \prod_{\ell | r} \zeta_\ell - 1 \right)$$

where $\zeta_\square$ is a $\square$-th primitive root of unity. For ℓ dividing r, we have

$$\mathrm{Nm}_{\mathbb{Q}(\zeta_{mr})/\mathbb{Q}(\zeta_{mr/\ell})} (\xi_r) = \left(\xi_{r/\ell}\right)^{\mathrm{Frob}_\ell - 1}.$$

Exercise

Exercise

Fix a positive integer m and Let S be the set of square-free products of primes ℓ such that $\ell \equiv \pm 1 \pmod{m}$, i.e. the Frobenius at ℓ is trivial in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})$. For $r \in S$, let

$$\xi_r = \left(\zeta_m \cdot \prod_{\ell \mid r} \zeta_\ell - 1\right) \cdot \left(\zeta_m^{-1} \cdot \prod_{\ell \mid r} \zeta_\ell - 1\right)$$

where $\zeta_\square$ is a $\square$-th primitive root of unity. For ℓ dividing r, we have

$$\mathrm{Nm}_{\mathbb{Q}(\zeta_{mr})/\mathbb{Q}(\zeta_{mr/\ell})}(\xi_r) = \left(\xi_{r/\ell}\right)^{\mathrm{Frob}_\ell - 1}.$$

This is the Euler system relation of cyclotomic units.