The Euler system of Heegner points [1]

London Junior Number Theory Seminar

David Kurniadi Angdinata

London School of Geometry and Number Theory

Tuesday, 10 May 2022

[1] Victor Kolyvagin, 1989. **Euler Systems**, in *Grothendieck Festschrift*

Overview

- Introduction
  - From Gross–Zagier to Kolyvagin
  - Application to BSD
  - The main result
- Generalised Selmer groups
  - Selmer structures
  - Application of Tate duality
  - Application of Chebotarev density
- The Euler system of Heegner points
  - Heegner points of higher conductors
  - Derived Kolyvagin classes
  - Computing the Selmer group

From Gross–Zagier to Kolyvagin

Assumptions

- *Elliptic curve $E/\mathbb{Q}$ with modular parameterisation $\phi : X_0(N) \twoheadrightarrow E$.*
- *Imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ with* **Heegner condition***:* [2]

$$p \mid N \qquad \Longrightarrow \qquad p \text{ is split in } K.$$

Consequences

- *An ideal $\mathcal{N}_K \trianglelefteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}_K \cong \mathbb{Z}/N$.*
- *A cyclic N-isogeny $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$.*
- *A point $x_1 \in X_0(N)(K^1)$ by CM theory.*
- *A* **Heegner point** *$P_1 := \phi(x_1) \in E(K^1)$.*
- *A* **basic Heegner point**

$$P_K := \sum_{\sigma \in \mathrm{Gal}(K^1/K)} \sigma(P_1) \in E(K).$$

[2] assume $\mathrm{End}(E) \cong \mathbb{Z}$ and $D \neq 1, 3$

From Gross–Zagier to Kolyvagin

Recall the Gross–Zagier formula.

Theorem (Gross–Zagier, 1986)

There is some $c \neq 0$ *such that* $L'(E/K, 1) = c \cdot \widehat{h}(P_K)$.

Corollary

If $L'(E/K, 1) \neq 0$*, then* $\mathrm{rk}_{\mathbb{Z}}\, E(K) \geq 1$.

Theorem (Kolyvagin, 1989)

If $\widehat{h}(P_K) \neq 0$*, then* $E(K)_{/\,\mathrm{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K$.

Corollary

If $L'(E/K, 1) \neq 0$*, then* $\mathrm{rk}_{\mathbb{Z}}\, E(K) = 1$.

This *almost* proves weak BSD for analytic rank ≤ 1!

Application to BSD

Theorem (Weak BSD for analytic rank ≤ 1)

Assume $\operatorname{ord}_{s=1} \; L(E/\mathbb{Q}, s) \leq 1$. *Then* $\operatorname{ord}_{s=1} \; L(E/\mathbb{Q}, s) = \operatorname{rk}_{\mathbb{Z}} E(\mathbb{Q})$.

Proof.

Consider the functional equation

$$\Lambda(E/\mathbb{Q}, s) = \epsilon \cdot \Lambda(E/\mathbb{Q}, 2 - s).$$

Differentiating k times and evaluating at $s = 1$ gives

$$L^{(k)}(E/\mathbb{Q}, 1) = \epsilon \cdot (-1)^k \cdot L^{(k)}(E/\mathbb{Q}, 1).$$

Then

$$\operatorname{ord}_{s=1} \; L(E/\mathbb{Q}, s) = \begin{cases} 0 & \text{if } \epsilon = +, \\ 1 & \text{if } \epsilon = -. \end{cases}$$

Consider cases for ϵ.

Application to BSD

Theorem (Weak BSD for analytic rank ≤ 1)

Assume $\operatorname{ord}_{s=1} \; L(E/\mathbb{Q}, s) \leq 1$. *Then* $\operatorname{ord}_{s=1} \; L(E/\mathbb{Q}, s) = \operatorname{rk}_{\mathbb{Z}} E(\mathbb{Q})$.

Proof (for $\epsilon = -$).

Fact: There is Heegner $K = \mathbb{Q}(\sqrt{-D})$ such that $L(E_D/\mathbb{Q}, 1) \neq 0$. Then

$$\operatorname{ord}_{s=1} \; L(E/K, s) = \underbrace{\operatorname{ord}_{s=1} \; L(E/\mathbb{Q}, s)}_{1} + \underbrace{\operatorname{ord}_{s=1} \; L(E_D/\mathbb{Q}, s)}_{0}.$$

In particular

$$L'(E/K, 1) \neq 0 \quad \overset{\text{G–Z}}{\Longrightarrow} \quad \widehat{h}(P_K) \neq 0 \quad \overset{\text{K}}{\Longrightarrow} \quad E(K)_{/\,\text{tor}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

Fact: complex conjugation of K acts like $-\epsilon$ on $E(K)_{/\,\text{tor}}$.

Thus $E(\mathbb{Q})_{/\,\text{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K$, so $\operatorname{rk}_{\mathbb{Z}} E(\mathbb{Q}) = 1$. □

The main result

Theorem (Kolyvagin, 1989)

If $\widehat{h}(P_K) \neq 0$, *then* $E(K)_{/\,\mathrm{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K$.

Theorem (main result [3])

Let $\ell \in \mathbb{N}$ *be an odd prime of good reduction such that*

$$\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_\ell), \qquad P_K \notin \ell E(K).$$

Then $\mathrm{Sel}(K, E[\ell]) = \mathbb{F}_\ell \cdot \delta(P_K)$.

Proof (of Kolyvagin).

For any $\ell \in \mathbb{N}$, there is a short exact sequence

$$0 \to E(K)/\ell E(K) \xrightarrow{\delta} \mathrm{Sel}(K, E[\ell]) \to Ш(K, E)[\ell] \to 0.$$

Choose any $\ell \in \mathbb{N}$ such that K and $\mathbb{Q}(E[\ell])$ are linearly disjoint over $\mathbb{Q}$. Then $E(K)[\ell] = 0$, so that $\dim_{\mathbb{F}_\ell} E(K)/\ell E(K) = \mathrm{rk}_{\mathbb{Z}} E(K)$. □

[3] Benedict Gross, 1991. **Kolyvagin's work on modular elliptic curves**

Selmer structures

Selmer groups can be defined in general.

Let M be a (non-scalar, simple) self-dual $\mathbb{F}_\ell[\mathrm{Gal}(L/K)]$-module.

Example

Let $M = E[\ell]$.

- Fact: Galois equivariance of ℓ-Weil pairing implies M is non-scalar.
- Fact: surjective ℓ-adic representation implies M is simple.

By inflation-restriction, there is a short exact sequence

$$0 \to H^1(G_v^{\mathrm{nr}}, M^{I_v}) \to H^1(K_v, M) \to H^1(I_v, M)^{G_v^{\mathrm{nr}}} \to 0.$$

Example

Let $v \nmid \ell$ have good reduction. Then there is a short exact sequence

$$0 \to E(K_v)/\ell E(K_v) \xrightarrow{\delta} H^1(K_v, M) \to H^1(K_v, E)[\ell] \to 0.$$

Selmer structures

A **Selmer structure** on M is an assignment

$$v \longmapsto H^1_f(K_v, M) \subseteq H^1(K_v, M),$$

such that $H^1_f(K_v, M) = H^1(G_v^{\mathrm{nr}}, M^{I_v})$ for almost all places v of K.
Its **singular quotient** $H^1_s(K_v, M)$ sits in

$$0 \to H^1_f(K_v, M) \to H^1(K_v, M) \xrightarrow{(\cdot)^s} H^1_s(K_v, M) \to 0.$$

Example

- The **unramified** Selmer structure has

$$H^1_f(K_v, M) := H^1(G_v^{\mathrm{nr}}, M^{I_v}), \qquad H^1_s(K_v, M) := H^1(I_v, M)^{G_v^{\mathrm{nr}}}.$$

- The **geometric** Selmer structure has

$$H^1_f(K_v, M) := E(K_v)/\ell E(K_v), \qquad H^1_s(K_v, M) := H^1(K_v, E)[\ell].$$

Selmer structures

There is a localisation map

$$(\cdot)_v : H^1(K, M) \to H^1(K_v, M).$$

- The **classical** Selmer group $\mathrm{Sel}(K, M)$ sits in

$$0 \to \mathrm{Sel}(K, M) \to H^1(K, M) \xrightarrow{\prod_v (\cdot)_v^s} \prod_v H_s^1(K_v, M).$$

- The **relaxed** Selmer group $\mathrm{Sel}^S(K, M)$ sits in

$$0 \to \mathrm{Sel}(K, M) \to \mathrm{Sel}^S(K, M) \xrightarrow{\prod_{v \in S} (\cdot)_v^s} \bigoplus_{v \in S} H_s^1(K_v, M).$$

- The **restricted** Selmer group $\mathrm{Sel}_S(K, M)$ sits in

$$0 \to \mathrm{Sel}_S(K, M) \to \mathrm{Sel}(K, M) \xrightarrow{\prod_{v \in S} (\cdot)_v} \bigoplus_{v \in S} H_f^1(K_v, M).$$

Application of Tate duality

Proposition

Let $S' \subseteq S$ be finite sets of places of K. There is an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{S'} \longrightarrow \mathrm{Sel}^{S} \longrightarrow \bigoplus_{v \in S \setminus S'} H^1_s(K_v, M) \longrightarrow \mathrm{Sel}^{\vee}_{S'} \longrightarrow \mathrm{Sel}^{\vee}_{S} \longrightarrow 0.$$

Proof.

Local Tate duality gives a perfect pairing

$$H^1_s(K_v, M) \times H^1_f(K_v, M) \to \mathbb{F}_\ell.$$

By the snake lemma, may assume that S and S' contain all bad places. The Poitou–Tate exact sequence gives exactness at

$$\mathrm{Sel}^{S} \to \bigoplus_{v \in S} H^1(K_v, M) \to \mathrm{Sel}^{S\vee}.$$

Diagram chase. □

Application of Tate duality

Proposition

Let $S' \subseteq S$ be finite sets of places of K. There is an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{S'} \longrightarrow \mathrm{Sel}^{S} \longrightarrow \bigoplus_{v \in S \setminus S'} H^1_s(K_v, M) \longrightarrow \mathrm{Sel}^{\vee}_{S'} \longrightarrow \mathrm{Sel}^{\vee}_{S} \longrightarrow 0.$$

<u>Fact</u>: complex conjugation of K respects the exact sequence. Thus

$$0 \to \mathrm{Sel}^{S'\pm} \to \mathrm{Sel}^{S\pm} \to \bigoplus_{v \in S \setminus S'} H^1_s(K_v, M)^{\pm} \to \mathrm{Sel}^{\vee\pm}_{S'} \to \mathrm{Sel}^{\vee\pm}_{S} \to 0.$$

Specialising to $S' = \emptyset$ and $M = E[\ell]$,

$$0 \to \mathrm{coker}\left(\mathrm{Sel}^{S\pm} \to \bigoplus_{v \in S} H^1_s(K_v, E[\ell])^{\pm}\right) \to \mathrm{Sel}^{\vee\pm} \to \mathrm{Sel}^{\vee\pm}_{S} \to 0.$$

<u>Idea</u>: choose appropriate S.

Application of Chebotarev density

Assume M is non-scalar and simple.

Let $K(E[\ell]) \subseteq L \subseteq L'$ be finite extensions, and fix $\sigma \in \mathrm{Gal}(L'/L)^{-}$.
Choose a lift of complex conjugation $\tau \in \mathrm{Gal}(L'/\mathbb{Q})$.

Lemma

There is a finite set S of inert primes of $K/\mathbb{Q}$ such that

1. $\left(\frac{p}{L'/\mathbb{Q}}\right) \sim \sigma\tau$ *for all* $p \in S$, *and*
2. $\mathrm{Sel}_S^{\pm} \subseteq H^1(L'/K, E[\ell])^{\pm}$.

Proof.

- Chebotarev density gives S satisfying 1.
- Fact: non-scalar and simple imply 2.

□

Idea: choose appropriate L'/L to bound $\mathrm{Sel}_S^{\pm}$.

Heegner points of higher conductors

Both $\mathrm{Sel}^{S\pm}$ and $H^1_s(K_v, E[\ell])^\pm$ in

$$0 \to \mathrm{coker}\left(\mathrm{Sel}^{S\pm} \to \bigoplus_{v\in S} H^1_s(K_v, E[\ell])^\pm\right) \to \mathrm{Sel}^{\vee\pm} \to \mathrm{Sel}_S^{\vee\pm} \to 0$$

are generated by some $c(n) \in H^1(K, E[\ell])^\pm$ indexed by $n \in \mathbb{N}$.

Each $c(n)$ is generated by a **Heegner point of conductor** n.

conductor 1	conductor n
ring of integers $\mathcal{O}_K$	order $\mathcal{O}_{K,n}$
Hilbert class field K^1	ring class field K^n
Heegner point $P_1 \in E(K^1)$	Heegner point $P_n \in E(K^n)$

Heegner points of higher conductors

The Heegner points $P_n \in E(K^n)$ satisfy "Euler system" relations.

Consider only the square-free $n \in \mathbb{N}$ (coprime to $ND\ell$) such that:

$$p \mid n \qquad \Longrightarrow \qquad p \text{ is inert in } K.$$

By class field theory,

$$\mathrm{Gal}(K^n/K^1) \cong \mathrm{Cl}(\mathcal{O}_{K,n})/\,\mathrm{Cl}(\mathcal{O}_K) \cong (\mathcal{O}_K/n)^\times/(\mathbb{Z}/n)^\times.$$

Since n is square-free,

$$\mathrm{Gal}(K^n/K^1) \cong \prod_{p \mid n} \mathrm{Gal}(K^p/K^1).$$

Since $p \mid n$ is inert in K,

$$\mathrm{Gal}(K^p/K^1) = \mathbb{Z}/(p+1) \cdot \sigma_p.$$

Heegner points of higher conductors

Proposition (AX3)

Let $n = pq$. Then

1. $\sum_{i=0}^{p} \sigma_p^i P_{pq} = a_p P_q$ *in* $E(K^q)$, *and*
2. $\overline{P_{pq}} = \overline{\left(\frac{\mathfrak{p}_\mathfrak{q}}{K^q/K}\right) P_q}$ *in* $\overline{E}(\mathbb{F}_{\mathfrak{p}_\mathfrak{q}})$.

Proof (sketch of 1).

If $H_p : \mathrm{Div}(X_0(N)) \to \mathrm{Div}(X_0(N))$ is the Hecke correspondence, then

$$\sum_{i=0}^{p} \sigma_p^i x_{pq} = H_p x_q.$$

By Eichler–Shimura theory, for any $D \in \mathrm{Div}(X_0(N))$,

$$\phi(H_p D) = a_p \phi(D).$$

□

Derived Kolyvagin classes

Given $P_n \in E(K^n)$, how to derive $c(n) \in H^1(K, E[\ell])$?

Define a "trace"

$$T_n := \sum_{\tau \in T} \tau \in \mathbb{Z}[\mathrm{Gal}(K^n/K)],$$

where T is a set of coset representatives for $\mathrm{Gal}(K^n/K^1) \leq \mathrm{Gal}(K^n/K)$.

Define the **Kolyvagin derivative**

$$D_n := \prod_{p|n} D_p \in \mathbb{Z}[\mathrm{Gal}(K^n/K^1)],$$

where D_p is any solution in $\mathbb{Z}[\mathrm{Gal}(K^n/K)]$ to

$$(\sigma_p - 1)D_p = p + 1 - T_p.$$

Define $\mathcal{P}_n := [T_n D_n P_n] \in E(K^n)/\ell E(K^n)$.

Derived Kolyvagin classes

Fact: By AX3,

- $\mathcal{P}_n$ is fixed by $G_n := \mathrm{Gal}(K^n/K)$, and
- $\mathcal{P}_n$ lies in the $\epsilon_n := -\epsilon \cdot (-1)^{\#\{p|n\}}$ eigenspace.

There is an exact diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow \scriptstyle{\mathrm{inf}_n} & & & & \\
0 & \longrightarrow & H^1_f(K, E[\ell])^{\epsilon_n} & \xrightarrow{\delta} & H^1(K, E[\ell])^{\epsilon_n} & \longrightarrow & H^1_s(K, E[\ell])^{\epsilon_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \scriptstyle{\mathrm{res}_n} & & \downarrow & & \\
0 & \to & H^1_f(K^n, E[\ell])^{G_n \epsilon_n} & \underset{\delta_n}{\to} & H^1(K^n, E[\ell])^{G_n \epsilon_n} & \to & H^1_s(K^n, E[\ell])^{G_n \epsilon_n} & & \\
 & & & & \downarrow \scriptstyle{\mathrm{tra}_n} & & & & \\
 & & & & 0. & & & &
\end{array}$$

Define $c(n) \in H^1(K, E[\ell])^{\epsilon_n}$ by $\mathrm{res}_n(c(n)) = \delta_n(\mathcal{P}_n)$.

Derived Kolyvagin classes

Lemma

1. *If $v \nmid n$, then $c(n)_v^s = 0$ (i.e. $c(n) \in \mathrm{Sel}^{\{p|n\}\epsilon_n}$).*
2. *If $v \mid n$, then $c(n)_v^s = 0$ if and only if $\mathcal{P}_{n/v} \in \ell E(K_v)$.*

Proof (sketch of 1).

Assume $v \nmid \ell$ has good reduction. Then K_v^n/K_v is unramified, so

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1_f(K_v, E[\ell]) & \longrightarrow & H^1(K_v, E[\ell]) & \xrightarrow{(\cdot)^s} & \mathrm{Hom}(I_v, E[\ell]) \\
 & & \downarrow & & \downarrow \mathrm{res}_n & & \downarrow \wr \\
0 & \longrightarrow & H^1_f(K_v^n, E[\ell]) & \xrightarrow[\delta_n]{} & H^1(K_v^n, E[\ell]) & \xrightarrow[(\cdot)^s]{} & \mathrm{Hom}(I_v, E[\ell]).
\end{array}$$

Thus $(\mathrm{res}_n(c(n)_v))^s = 0$ by exactness. □

Computing the Selmer group

Compute Sel^{ϵ} and $\mathrm{Sel}^{-\epsilon}$ separately.

Use the short exact sequence

$$0 \to \mathrm{coker}\left(\mathrm{Sel}^{S\pm} \to \bigoplus_{p \in S} H^1_s(K_p, E[\ell])^{\pm}\right) \to \mathrm{Sel}^{\pm} \to \mathrm{Sel}^{\pm}_S \to 0.$$

Restricted:

- Choose L'/L to get S such that $\mathrm{Sel}^{\pm}_S \subseteq H^1(L'/K, E[\ell])^{\pm}$.
- Compute $H^1(L'/K, E[\ell])^{\pm}$.

Relaxed:

- Fact: each $H^1_s(K_p, E[\ell])^{\pm}$ is one-dimensional.
- Show $c(n) \in \mathrm{Sel}^{S\epsilon_n}$ is non-zero in $H^1_s(K_p, E[\ell])$ for some n.

Computing the Selmer group

Compute Sel^{ϵ}.

Let $L := K(E[\ell])$ and $L' := K(E[\ell], \frac{1}{\ell}P_K)$. Get S such that

$$\mathrm{Sel}_S^{\epsilon} \subseteq H^1(L'/K, E[\ell])^{\epsilon} \cong \underbrace{\mathbb{F}_\ell \cdot \delta(P_K)}_{-\epsilon}.$$

By Frobenius computations,

$$\forall p \in S, \qquad c(p) \in \mathrm{Sel}^{S\epsilon}, \qquad c(p)_p^s \neq 0.$$

Thus

$$0 \to \underbrace{\mathrm{coker}\left(\mathrm{Sel}^{S\epsilon} \to \bigoplus_{p \in S} H^1_s(K_p, E[\ell])^{\epsilon}\right)}_{0} \to \mathrm{Sel}^{\epsilon} \to \underbrace{\mathrm{Sel}_S^{\epsilon}}_{0} \to 0.$$

Computing the Selmer group

Compute $\mathrm{Sel}^{-\epsilon}$. Fix $p \in S$.

Let $L := K(E[\ell], \frac{1}{\ell}P_K)$ and $L' := \ker(G_L \xrightarrow{c(p)} E[\ell])$. Get S' such that

$$\mathrm{Sel}_{S'}^{-\epsilon} \subseteq H^1(L'/K, E[\ell])^{-\epsilon} \cong \underbrace{\mathbb{F}_\ell \cdot \delta(P_K)}_{-\epsilon} \oplus \underbrace{\mathbb{F}_\ell \cdot c(p)}_{\epsilon}.$$

By Frobenius computations,

$$\forall q \in S', \qquad c(pq) \in \mathrm{Sel}^{S'-\epsilon}, \qquad c(pq)_q^s \neq 0.$$

Thus

$$0 \to \underbrace{\mathrm{coker}\left(\mathrm{Sel}^{S'-\epsilon} \to \bigoplus_{q \in S'} H_s^1(K_q, E[\ell])^{-\epsilon}\right)}_{0} \to \mathrm{Sel}^{-\epsilon} \to \underbrace{\mathrm{Sel}_{S'}^{-\epsilon}}_{\subseteq \mathbb{F}_\ell \cdot \delta(P_K)} \to 0.$$