

Kolyvagin's work on the BSD conjecture ¹

Mini project presentation

David Kurniadi Angdinata

London School of Geometry and Number Theory

Thursday, 5 May 2022

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

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**:

$$p \mid N \quad \implies \quad p \text{ is split in } K.$$

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 $\mathbb{C}/\mathcal{O}_K \rightarrow \mathbb{C}/\mathcal{N}_K^{-1}$.
- ▶ 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**

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

From Gross–Zagier to Kolyvagin

Recall the Gross–Zagier formula.

Theorem (Gross–Zagier, 1986)

$$L'(E/K, 1) = c \cdot \widehat{h}(P_K).$$

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

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \quad \implies \quad E(K)_{\mathrm{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K.$$

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

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

From Gross–Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \quad \implies \quad E(K)_{/\text{tor}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

Idea: bound $\text{rk}_{\mathbb{Z}} E(K)$ with

$$\delta : E(K)/\ell E(K) \hookrightarrow \text{Sel}(K, E[\ell]),$$

for some prime $\ell \in \mathbb{N}$.

- Want $\dim_{\mathbb{F}_{\ell}} E(K)/\ell E(K) = \text{rk}_{\mathbb{Z}} E(K)$. Suffices to assume

$$\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_{\ell}).$$

Fact: this implies $E(K)[\ell] = 0$.

- Need

$$P_K \notin \ell E(K).$$

From Gross–Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \quad \implies \quad E(K)_{\text{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K.$$

Theorem (main result ²)

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

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

Then

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

Remark

There are infinitely many such $\ell \in \mathbb{N}$.

²Benedict Gross, 1991. **Kolyvagin's work on modular elliptic curves** 

Generalised Selmer groups

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

$$0 \rightarrow E[\ell] \rightarrow E \xrightarrow{\cdot \ell} E \rightarrow 0.$$

Applying $\text{Gal}(\overline{K}/K)$ cohomology,

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[\ell] & \longrightarrow & E(K) & \xrightarrow{\cdot \ell} & E(K) \\ & & & & \delta & & \\ & \searrow & & & & & \nearrow \\ & & H^1(K, E[\ell]) & \longrightarrow & H^1(K, E) & \xrightarrow{\cdot \ell} & H^1(K, E) \longrightarrow \dots \end{array}$$

Truncating at $H^1(K, E[\ell])$, and for each place v of K ,

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/\ell E(K) & \xrightarrow{\delta} & H^1(K, E[\ell]) & \longrightarrow & H^1(K, E)[\ell] \longrightarrow 0 \\ & & \downarrow & & (\cdot)_v \downarrow & \searrow (\cdot)_v & \downarrow \\ 0 & \longrightarrow & E(K_v)/\ell E(K_v) & \longrightarrow & H^1(K_v, E[\ell]) & \longrightarrow & H^1(K_v, E)[\ell] \longrightarrow 0. \end{array}$$

Generalised Selmer groups

There is an exact diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/\ell E(K) & \xrightarrow{\delta} & H^1(K, E[\ell]) & \longrightarrow & H^1(K, E)[\ell] \longrightarrow 0 \\ & & \downarrow & & (\cdot)_v \downarrow & \nearrow (\cdot)_v^* & \downarrow \\ 0 & \longrightarrow & E(K_v)/\ell E(K_v) & \longrightarrow & H^1(K_v, E[\ell]) & \longrightarrow & H^1(K_v, E)[\ell] \longrightarrow 0. \end{array}$$

- ▶ The **classical** Selmer group is

$$\mathrm{Sel}(K, E[\ell]) := \{c \in H^1(K, E[\ell]) : \forall v, c_v = 0\}.$$

- ▶ The **relaxed** Selmer group is

$$\mathrm{Sel}^S(K, E[\ell]) := \{c \in H^1(K, E[\ell]) : \forall v \notin S, c_v = 0\}.$$

- ▶ The **restricted** Selmer group is

$$\mathrm{Sel}_S(K, E[\ell]) := \{c \in \mathrm{Sel}^S(K, E[\ell]) : \forall v \in S, c_v = 0\}.$$

Generalised Selmer groups

Proposition

There is an exact sequence of \mathbb{F}_ℓ -vector spaces

$$0 \rightarrow \text{Sel} \rightarrow \text{Sel}^S \xrightarrow{\sigma_S} \prod_{v \in S} H^1(K_v, E)[\ell] \rightarrow \text{Sel}^\vee \rightarrow \text{Sel}_S^\vee \rightarrow 0.$$

Proof.

Local Tate duality and the Poitou–Tate exact sequence. □

Proposition (sort of)

There is a “magical” set S of primes, inert in K/\mathbb{Q} , such that

- ▶ $H^1(K_p, E)[\ell] = \mathbb{F}_\ell \cdot c(p)^p$ for all $p \in S$,
- ▶ $\text{im}(\sigma_S) = \prod_{p \in S} \mathbb{F}_\ell \cdot c(p)^p$, and
- ▶ $\text{Sel}_S = \mathbb{F}_\ell \cdot \delta(P_K)$.

Proof.

Chebotarev density and a lot of Galois cohomology. □

Derived Heegner points

For any $n \in \mathbb{N}$, there is a cohomology class $c(n) \in H^1(K, E[\ell])$ derived from a **Heegner point of conductor n** .

conductor 1	conductor n
ring of integers \mathcal{O}_K	order $\mathcal{O}_{K,n} := \mathbb{Z} + n\mathcal{O}_K$
ideal $\mathcal{N}_K \trianglelefteq \mathcal{O}_K$	ideal $\mathcal{N}_{K,n} := \mathcal{N}_K \cap \mathcal{O}_{K,n} \trianglelefteq \mathcal{O}_{K,n}$
N -isogeny $\mathbb{C}/\mathcal{O}_K \rightarrow \mathbb{C}/\mathcal{N}_K^{-1}$	N -isogeny $\mathbb{C}/\mathcal{O}_{K,n} \rightarrow \mathbb{C}/\mathcal{N}_{K,n}^{-1}$
Hilbert class field K^1	ring class field K^n
point $x_1 \in X_0(N)(K^1)$	point $x_n \in X_0(N)(K^n)$
Heegner point $P_1 \in E(K^1)$	Heegner point $P_n \in E(K^n)$

Derived Heegner points

The Heegner points $P_n \in E(K^n)$ satisfy “nice” relations over all $n \in \mathbb{N}$.

Fact: If p is inert in K/\mathbb{Q} , then

$$\mathrm{Gal}(K^p/K^1) = \{1, \sigma_p, \sigma_p^2, \dots, \sigma_p^p\}.$$

Proposition (don't worry about this)

Let $p \in S$. Then

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

Proof.

Consequence of the Eichler–Shimura congruence relation. □

These are the axioms of an **AX3 Euler system**.

Derived Heegner points

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

Define the **Kolyvagin derivative** operator by

$$D_p := \sigma_p + 2\sigma_p^2 + \cdots + p\sigma_p^p \in \mathbb{Z}[\mathrm{Gal}(K^p/K^1)].$$

Also define a “trace” operator by

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

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

Define the **Kolyvagin class** $c(p) \in H^1(K, E[\ell])$ by

$$c(p)(\sigma) := \sigma \left(\frac{1}{\ell} T_p D_p P_p \right) - \frac{1}{\ell} T_p D_p P_p - \frac{1}{\ell} (\sigma - 1)(T_p D_p P_p).$$

The Tate–Shafarevich group

Kolyvagin proved something more.

There is an exact diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/\ell E(K) & \xrightarrow{\delta} & H^1(K, E[\ell]) & \longrightarrow & H^1(K, E)[\ell] \longrightarrow 0 \\ & & \downarrow & & \downarrow & \searrow \sigma & \downarrow \tau[\ell] \\ 0 & \rightarrow & \prod_v E(K_v)/\ell E(K_v) & \rightarrow & \prod_v H^1(K_v, E[\ell]) & \rightarrow & \prod_v H^1(K_v, E)[\ell] \rightarrow 0. \end{array}$$

The classical Selmer group is

$$\mathrm{Sel}(K, E[\ell]) := \ker \sigma.$$

The **Tate–Shafarevich group** is

$$\mathrm{III}(K, E) := \ker \tau.$$

The Tate–Shafarevich group

Kolyvagin proved something more.

There is an exact sequence

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

Corollary

Let $\hat{h}(P_K) \neq 0$ and $\ell \in \mathbb{N}$ be an odd prime of good reduction such that

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

Then $\mathrm{rk}_{\mathbb{Z}} E(K) = 1$ and $\mathrm{III}(K, E)[\ell] = 0$.

Kolyvagin also proved $\mathrm{III}(K, E)$ is finite.

Thank you!

For more details:

The Euler system of Heegner points

London Junior Number Theory Seminar

Tuesday, 10 May 2022, 17:15 – 18:15

Room K6.63, King's Building, Strand Campus, King's College London

Please come!