London School of Geometry and Number Theory

Mini Project

Kolyvagin's work on the BSD conjecture [1]

David Ang

Thursday, 5 May 2022

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

From Gross-Zagier to Kolyvagin

Assumptions

- Elliptic curve $E/\mathbb{Q}$ with modular parameterisation $\phi : X_0(N) \twoheadrightarrow E$.

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**:

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

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**:

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

Consequences

- An ideal $\mathcal{N}_K \trianglelefteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}_K \cong \mathbb{Z}/N$.

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**:

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

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 $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$.

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**:

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

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 $x_1 \in X_0(N)$

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**:

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

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.

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**:

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

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** $P_1 := \phi(x_1) \in E(K^1)$.

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**:

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

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**

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

From Gross-Zagier to Kolyvagin

Recall the Gross-Zagier formula.

Theorem (Gross-Zagier, 1986)

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

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 $\mathrm{rk}_{\mathbb{Z}} E(K) \geq 1$.

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)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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

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)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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

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

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

From Gross-Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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

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

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

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

From Gross-Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

<u>Idea</u>: bound $\mathrm{rk}_{\mathbb{Z}} E(K)$ with

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

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

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

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

From Gross-Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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

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

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

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

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

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

From Gross-Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

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

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

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

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

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

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

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

From Gross-Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

Theorem (main result [2])

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

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

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

From Gross-Zagier to Kolyvagin

Theorem (Kolyvagin, 1989)

$$\widehat{h}(P_K) \neq 0 \qquad \Longrightarrow \qquad E(K)_{/\mathrm{tors}} = \mathbb{Z} \cdot \tfrac{1}{n} P_K.$$

Theorem (main result [2])

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

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

Remark

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

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

Generalised Selmer groups

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

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

Generalised Selmer groups

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

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

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

$$\begin{tikzcd}
0 \arrow[r] & E(K)[\ell] \arrow[r] & E(K) \arrow[r, "\cdot\ell"] & E(K) \arrow[dlll, "\delta"'] & \\
H^1(K, E[\ell]) \arrow[r] & H^1(K, E) \arrow[r, "\cdot\ell"'] & H^1(K, E) \arrow[r] & \ldots.
\end{tikzcd}$$

Generalised Selmer groups

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

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

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

$$\begin{tikzcd} 0 \arrow[r] & E(K)[\ell] \arrow[r] & E(K) \arrow[r, "\cdot \ell"] & E(K) \arrow[dll, "\delta"] & \\ & H^1(K, E[\ell]) \arrow[r] & H^1(K, E) \arrow[r, "\cdot \ell"'] & H^1(K, E) \arrow[r] & \cdots . \end{tikzcd}$$

Truncating at $H^1(K, E[\ell])$,

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

Generalised Selmer groups

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

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

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

$$\begin{tikzcd}
0 \arrow[r] & E(K)[\ell] \arrow[r] & E(K) \arrow[r, "\cdot \ell"] & E(K) \arrow[dll, rounded corners, "\delta"'] & \\
& H^1(K, E[\ell]) \arrow[r] & H^1(K, E) \arrow[r, "\cdot \ell"'] & H^1(K, E) \arrow[r] & \ldots.
\end{tikzcd}$$

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

$$\begin{array}{l}
0 \longrightarrow E(K)/\ell E(K) \xrightarrow{\delta} H^1(K, E[\ell]) \longrightarrow H^1(K, E)[\ell] \longrightarrow 0 \\
0 \longrightarrow E(K_v)/\ell E(K_v) \longrightarrow H^1(K_v, E[\ell]) \longrightarrow H^1(K_v, E)[\ell] \longrightarrow 0
\end{array}$$

Generalised Selmer groups

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

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

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

$$\begin{tikzcd}
0 \arrow[r] & E(K)[\ell] \arrow[r] & E(K) \arrow[r, "\cdot \ell"] & E(K) \arrow[dll, out=-10, in=170, "\delta"'] & \\
& H^1(K, E[\ell]) \arrow[r] & H^1(K, E) \arrow[r, "\cdot \ell"'] & H^1(K, E) \arrow[r] & \cdots .
\end{tikzcd}$$

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

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

Generalised Selmer groups

There is an exact diagram

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

Generalised Selmer groups

There is an exact diagram

$$\begin{tikzcd}
0 \arrow[r] & E(K)/\ell E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\ell]) \arrow[r] \arrow[d] \arrow[dr, dashed, "(\cdot)^v"] & H^1(K, E)[\ell] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K_v)/\ell E(K_v) \arrow[r] & H^1(K_v, E[\ell]) \arrow[r] & H^1(K_v, E)[\ell] \arrow[r] & 0
\end{tikzcd}.$$

- The **classical** Selmer group is

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

Generalised Selmer groups

There is an exact diagram

$$\begin{tikzcd}
0 \arrow[r] & E(K)/\ell E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\ell]) \arrow[r] \arrow[d] \arrow[dr, dashed, "(\cdot)^v"] & H^1(K, E)[\ell] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K_v)/\ell E(K_v) \arrow[r] & H^1(K_v, E[\ell]) \arrow[r] & H^1(K_v, E)[\ell] \arrow[r] & 0
\end{tikzcd}.$$

- The **classical** Selmer group is

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

- The **relaxed** Selmer group is

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

Generalised Selmer groups

There is an exact diagram

$$
\begin{tikzcd}
0 \arrow[r] & E(K)/\ell E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\ell]) \arrow[r] \arrow[d, "(\cdot)_v"'] \arrow[dr, dashed, "(\cdot)^v"] & H^1(K, E)[\ell] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K_v)/\ell E(K_v) \arrow[r] & H^1(K_v, E[\ell]) \arrow[r] & H^1(K_v, E)[\ell] \arrow[r] & 0
\end{tikzcd}
.
$$

- The **classical** Selmer group is

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

- The **relaxed** Selmer group is

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

- The **restricted** Selmer group is

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

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

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

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

Local Tate duality and the Poitou-Tate exact sequence. $\square$

Proposition

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

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

Local Tate duality and the Poitou-Tate exact sequence. $\square$

Proposition

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 $p \in S$,

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

Local Tate duality and the Poitou-Tate exact sequence. $\square$

Proposition

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 $p \in S$,
- $\mathrm{im}(\sigma_S) = \prod_{p \in S} \mathbb{F}_\ell \cdot c(p)^p$, and

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

Local Tate duality and the Poitou-Tate exact sequence. $\square$

Proposition

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 $p \in S$,
- $\mathrm{im}(\sigma_S) = \prod_{p \in S} \mathbb{F}_\ell \cdot c(p)^p$, and
- $\mathrm{Sel}_S = \mathbb{F}_\ell \cdot \delta(P_K)$.

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

Local Tate duality and the Poitou-Tate exact sequence. $\square$

Proposition

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 $p \in S$,
- $\mathrm{im}(\sigma_S) = \prod_{p \in S} \mathbb{F}_\ell \cdot c(p)^p$, and
- $\mathrm{Sel}_S = \mathbb{F}_\ell \cdot \delta(P_K)$.

Proof.

Chebotarev density and a lot of Galois cohomology. $\square$

Generalised Selmer groups

Proposition

There is an exact sequence of $\mathbb{F}_\ell$-vector spaces

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

Proof.

Local Tate duality and the Poitou-Tate exact sequence. $\square$

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 $p \in S$,
- $\mathrm{im}(\sigma_S) = \prod_{p \in S} \mathbb{F}_\ell \cdot c(p)^p$, and
- $\mathrm{Sel}_S = \mathbb{F}_\ell \cdot \delta(P_K)$.

Proof.

Chebotarev density and a lot of Galois cohomology. $\square$

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.

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 $\mathcal{O}_K$	
ideal $\mathcal{N}_K \trianglelefteq \mathcal{O}_K$	
N-isogeny $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	
Hilbert class field K^1	
point $x_1 \in X_0(N)(K^1)$	
Heegner point $P_1 \in E(K^1)$	

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 $\mathcal{N}_K \trianglelefteq \mathcal{O}_K$	
N-isogeny $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	
Hilbert class field K^1	
point $x_1 \in X_0(N)(K^1)$	
Heegner point $P_1 \in E(K^1)$	

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 $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	
Hilbert class field K^1	
point $x_1 \in X_0(N)(K^1)$	
Heegner point $P_1 \in E(K^1)$	

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 $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	N-isogeny $\mathbb{C}/\mathcal{O}_{K,n} \to \mathbb{C}/\mathcal{N}_{K,n}^{-1}$
Hilbert class field K^1	
point $x_1 \in X_0(N)(K^1)$	
Heegner point $P_1 \in E(K^1)$	

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 $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	N-isogeny $\mathbb{C}/\mathcal{O}_{K,n} \to \mathbb{C}/\mathcal{N}_{K,n}^{-1}$
Hilbert class field K^1	ring class field K^n
point $x_1 \in X_0(N)(K^1)$	
Heegner point $P_1 \in E(K^1)$	

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 $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	N-isogeny $\mathbb{C}/\mathcal{O}_{K,n} \to \mathbb{C}/\mathcal{N}_{K,n}^{-1}$
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 $P_1 \in E(K^1)$	

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 $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}_K^{-1}$	N-isogeny $\mathbb{C}/\mathcal{O}_{K,n} \to \mathbb{C}/\mathcal{N}_{K,n}^{-1}$
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 $n \in \mathbb{N}$.

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

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

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

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

Proposition

Let $p \in S$. Then

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

Derived Heegner points

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

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

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

Proposition (don't worry about this)

Let $p \in S$. Then

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

Proof.

Consequence of the Eichler-Shimura congruence relation. $\square$

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

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

Proposition (don't worry about this)

Let $p \in S$. Then

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

Proof.

Consequence of the Eichler-Shimura congruence relation. $\square$

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

Derived Heegner points

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

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

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

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 $\mathrm{Gal}(K^p/K^1) \leq \mathrm{Gal}(K^p/K)$.

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.

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact diagram

$$\begin{tikzcd} 0 \arrow[r] & E(K)/\ell E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\ell]) \arrow[r] \arrow[d] & H^1(K, E)[\ell] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \prod_v E(K_v)/\ell E(K_v) \arrow[r] & \prod_v H^1(K_v, E[\ell]) \arrow[r] & \prod_v H^1(K_v, E)[\ell] \arrow[r] & 0 \end{tikzcd}.$$

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact diagram

$$\begin{tikzcd} 0 \arrow[r] & E(K)/\ell E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\ell]) \arrow[r] \arrow[d] \arrow[dr, dashed, "\sigma"] & H^1(K, E)[\ell] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \prod_v E(K_v)/\ell E(K_v) \arrow[r] & \prod_v H^1(K_v, E[\ell]) \arrow[r] & \prod_v H^1(K_v, E)[\ell] \arrow[r] & 0 \end{tikzcd}.$$

The classical Selmer group is

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

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact diagram

$$\begin{tikzcd}
0 \arrow[r] & E(K)/\ell E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\ell]) \arrow[r] \arrow[d] \arrow[dr, dashed, "\sigma"'] & H^1(K, E)[\ell] \arrow[r] \arrow[d, "\tau[\ell]"] & 0 \\
0 \arrow[r] & \prod_v E(K_v)/\ell E(K_v) \arrow[r] & \prod_v H^1(K_v, E[\ell]) \arrow[r] & \prod_v H^1(K_v, E)[\ell] \arrow[r] & 0
\end{tikzcd}.$$

The classical Selmer group is

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

The **Tate-Shafarevich group** is

$$Ш(K, E) := \ker \tau.$$

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact sequence

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

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact sequence

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

Corollary

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

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

Then $\mathrm{rk}_{\mathbb{Z}} E(K) = 1$

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact sequence

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

Corollary

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

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

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

The Tate-Shafarevich group

Kolyvagin proved something more.

There is an exact sequence

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

Corollary

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

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

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

Kolyvagin also proved $\text{Ш}(K, E)$ 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! ☺