Kolyvagin's theorem

The conjecture of Birch and Swinnerton-Dyer

David Kurniadi Angdinata

University College London

Wednesday, 13 March 2024

Some recapitulation

Let E be a rational elliptic curve of conductor N, and let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field satisfying the **Heegner hypothesis**

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

For any n coprime to N, define a **Heegner point of conductor** n

$$P_n := \Phi_N(\mathbb{C}/\mathcal{O}_n, \mathbb{C}/\mathcal{N}_n) \in E(H_n).$$

For any ℓ coprime to nN that is inert in K, there are norm compatibilities

$$\mathrm{tr}_{H_n}^{H_{n\ell}} P_{n\ell} = a_\ell P_n.$$

These form a **Heegner system for** (E, K).

Furthermore, define the **basic Heegner point**

$$P_K := \mathrm{tr}_K^{H_1}(P_1) \in E(K).$$

Application to BSD

We will do the following next week:

Theorem (Gross–Zagier '86)

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

We will do the following this week:

Theorem (Kolyvagin '90)

If $\widehat{h}(P_K) \neq 0$, *then* $\mathrm{rk}_{\mathbb{Z}} E(K) = 1$ *and* $\#\text{Ш}(E/K) < \infty$.

In particular, $E(K)_{/\,\mathrm{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K$.

This almost proves the following:

Corollary (of Gross–Zagier '86, Kolyvagin '90, etc)

If $\mathrm{ord}_{s=1} L(E, s) \leq 1$, *then* $\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E, s)$ *and* $\#\text{Ш}(E) < \infty$.

The missing ingredient is the existence of K.

Existence of Heegner fields

Let $-\epsilon$ be the sign in the functional equation

$$\Lambda(E, s) = -\epsilon \cdot \Lambda(E, 2 - s).$$

Theorem (Waldspurger '85, Murty–Murty '97)

If $\epsilon = +$, there are many imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$ satisfying the Heegner hypothesis such that $\operatorname{ord}_{s=1} L(E_D, s) = 0$.

In particular,

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{ord}_{s=1} L(E/K, s).$$

Theorem (Bump–Friedberg–Hoffstein '90, Murty–Murty '91)

If $\epsilon = -$, there are many imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$ satisfying the Heegner hypothesis such that $\operatorname{ord}_{s=1} L(E_D, s) = 1$.

In particular,

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{ord}_{s=1} L(E/K, s) - 1.$$

Complex conjugation on Heegner points

Lemma (τ)

Complex conjugation τ maps $P_n \in E(H_n)_{/\,\mathrm{tor}}$ to

$$\tau(P_n) = \epsilon \cdot \sigma(P_n),$$

for some $\sigma \in \mathrm{Gal}(H_n/K)$.

Proof.

Note that ϵ is precisely the eigenvalue of the Fricke involution w_N on the eigenform f_E associated to E. On the other hand,

$$w_N(\mathbb{C}/\mathcal{O}_n, \mathbb{C}/\mathcal{N}_n) = (\mathbb{C}/\mathcal{N}_n^{-1}, \mathbb{C}/\overline{\mathcal{N}_n}),$$

which differs from $\tau(\mathbb{C}/\mathcal{O}_n, \mathbb{C}/\mathcal{N}_n)$ by some $\sigma \in \mathrm{Gal}(H_n/K) \cong \mathrm{Cl}(\mathcal{O}_n)$. Now apply Φ_N and the Manin–Drinfeld theorem. □

In particular, $P_K \in E(\mathbb{Q})_{/\,\mathrm{tor}}$ precisely if $\epsilon = +$.

Proof of Gross–Zagier–Kolyvagin

Proof of BSD for $\mathrm{ord}_{s=1} L(E,s) \leq 1$.

The functional equation says that $L(E,1) = -\epsilon \cdot L(E,1)$ and $L'(E,1) = \epsilon \cdot L'(E,1)$. Since $\mathrm{ord}_{s=1} L(E,s) \leq 1$,

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

Choose any imaginary quadratic field K satisfying the Heegner hypothesis such that $\mathrm{ord}_{s=1} L(E/K,s) = 1$, which exists by W/MM and BFH/MM. By Gross–Zagier and Kolyvagin, $E(K)_{/\,\mathrm{tor}} = \mathbb{Z} \cdot \frac{1}{n} P_K$. By Lemma (τ),

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}) = \begin{cases} 1 & \text{if } \epsilon = +, \\ 0 & \text{if } \epsilon = -. \end{cases}$$

Finally, $\#\text{Ш}(E) < \infty$ follows from $\#\text{Ш}(E/K) < \infty$ by Kolyvagin. □

A weaker version of Kolyvagin

Theorem (Kolyvagin '90)

If $\widehat{h}(P_K) \neq 0$*, then* $\operatorname{rk}_{\mathbb{Z}} E(K) = 1$ *and* $\#Ш(E/K) < \infty$*.*

For any prime ℓ,

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

Choose any prime $\ell \nmid 6ND$ such that $\overline{\rho_{E,\ell}}$ is surjective and $P_K \notin \ell E(K)$.
Then $E(K)[\ell] = 0$, so $\operatorname{rk}_{\mathbb{Z}} E(K) = \dim_{\mathbb{F}_\ell} E(K)/\ell E(K)$.

Theorem (weak Kolyvagin '90)

$\mathrm{Sel}_\ell(E/K) = \mathbb{F}_\ell \cdot \delta(P_K)$*, so* $\operatorname{rk}_{\mathbb{Z}} E(K) \leq 1$ *and* $\#Ш(E/K)[\ell] < \infty$*.*

When E has no complex multiplication, this excludes finitely many primes by Serre's theorem, so this proves that $\widehat{h}(P_K) \neq 0$ implies $\operatorname{rk}_{\mathbb{Z}} E(K) = 1$.
Kolyvagin proves $\#Ш(E/K) < \infty$ by refining the argument for these primes and bounding the ℓ-primary components using Iwasawa theory.

Selmer structures

Let M be a discrete finite irreducible self-dual $\mathbb{F}_\ell[G_K]$-module.

The inflation-restriction exact sequence says

$$0 \to H^1(G_p^{\mathrm{nr}}, M^{I_p}) \to H^1(K_p, M) \to H^1(I_p, M)^{G_p^{\mathrm{nr}}} \to 0.$$

For $M = E[\ell]$ and good $p \nmid \ell$, this can be identified with

$$0 \to E(K_p)/\ell E(K_p) \to H^1(K_p, E[\ell]) \to H^1(K_p, E)[\ell] \to 0.$$

More generally, a **Selmer structure** for (K, M) is an assignment

$$p \longmapsto H^1_f(K_p, M) \subseteq H^1(K_p, M),$$

such that $H^1_f(K_p, M) = H^1(G_p^{\mathrm{nr}}, M^{I_p})$ for all but finitely many places p of K. Its associated **singular quotient** $H^1_s(K_p, M)$ sits in

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

Selmer groups

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

$$0 \to \mathrm{Sel}(K, M) \to H^1(K, M) \xrightarrow{\prod_p (\cdot)_p^s} \prod_p H^1_s(K_p, M).$$

For $M = E[\ell]$ and $H^1_f(K_p, M) = E(K_p)/\ell E(K_p)$, this is just $\mathrm{Sel}_\ell(E/K)$.

Let S be a finite set of places of K.

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

$$0 \to \mathrm{Sel}(K, M) \to \mathrm{Sel}^S(K, M) \xrightarrow{\bigoplus_{p \in S} (\cdot)_p^s} \bigoplus_{p \in S} H^1_s(K_p, M).$$

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

$$0 \to \mathrm{Sel}_S(K, M) \to \mathrm{Sel}(K, M) \xrightarrow{\bigoplus_{p \in S} (\cdot)_p} \bigoplus_{p \in S} H^1_f(K_p, M).$$

Duality of Selmer groups

Corollary (of Tate duality)

$$0 \longrightarrow \mathrm{Sel} \longrightarrow \mathrm{Sel}^S \longrightarrow \bigoplus_{p \in S} H^1_s(K_p, M)$$

$$||$$

$$\bigoplus_{p \in S} H^1_f(K_p, M)^\vee \longrightarrow \mathrm{Sel}^\vee \longrightarrow \mathrm{Sel}_S^\vee \longrightarrow 0.$$

Proof.

Local Tate duality gives a perfect pairing $H^1_s(K_p, M) \times H^1_f(K_p, M) \to \mathbb{F}_\ell$. The Poitou–Tate exact sequence gives exactness at

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

Now apply the snake lemma and diagram chase. □

Complex conjugation on Selmer groups

To compute Sel, it suffices to consider the last three terms

$$0 \to \mathrm{coker}\left(\mathrm{Sel}^S \to \bigoplus_{p \in S} H^1_s(K_p, M)\right) \to \mathrm{Sel}^\vee \to \mathrm{Sel}_S^\vee \to 0,$$

for some appropriate finite set of places S of K.

If $\tau \in G_{\mathbb{Q}}$ is an involution with non-zero eigenspaces M^+ and M^-, then

$$0 \to \mathrm{coker}\left(\mathrm{Sel}^{S_1+} \to \bigoplus_{p \in S_1} H^1_s(K_p, M)^+\right) \to \mathrm{Sel}^{+\vee} \to \mathrm{Sel}_{S_1}^{+\vee} \to 0,$$

$$0 \to \mathrm{coker}\left(\mathrm{Sel}^{S_2-} \to \bigoplus_{p \in S_2} H^1_s(K_p, M)^-\right) \to \mathrm{Sel}^{-\vee} \to \mathrm{Sel}_{S_2}^{-\vee} \to 0,$$

for some appropriate finite sets of places S_1 and S_2 of K.

Computing Selmer groups

Now consider $M = E[\ell]$.

Corollary (of Chebotarev density)

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

$$\operatorname{coker}\left(\underbrace{\mathrm{Sel}^{S-\epsilon}}_{\bigoplus_{p\in S}\mathbb{F}_\ell\cdot c(p)_p^s} \to \bigoplus_{p\in S}\underbrace{H^1(K_p,E)[\ell]^{-\epsilon}}_{\mathbb{F}_\ell\cdot c(p)_p^s}\right) \to \mathrm{Sel}^{-\epsilon\vee} \to \underbrace{\mathrm{Sel}_S^{-\epsilon\vee}}_{0}.$$

For any $p \in S$, there is a finite set S_p of primes of $\mathbb{Q}$ inert in K such that

$$\operatorname{coker}\left(\underbrace{\mathrm{Sel}^{S_p\epsilon}}_{\bigoplus_{q\in S_p}\mathbb{F}_\ell\cdot c(pq)_q^s} \to \bigoplus_{q\in S_p}\underbrace{H^1(K_p,E)[\ell]^{\epsilon}}_{\mathbb{F}_\ell\cdot c(pq)_q^s}\right) \to \mathrm{Sel}^{\epsilon\vee} \to \underbrace{\mathrm{Sel}_{S_p}^{\epsilon\vee}}_{\mathbb{F}_\ell\cdot\delta(P_K)} \to 0.$$

Proof.

Chebotarev density and a lot of Galois cohomology. □

Derivative operators

The classes $c(n) \in H^1(K, E[\ell])$ are derived from $P_n \in E(H_n)$.

It suffices to let n be a product of primes $p \nmid ND\ell$ inert in K, so

$$\mathrm{Gal}(H_n/H_1) \cong \prod_{p|n} \mathrm{Gal}(H_p/H_1) \cong \prod_{p|n} \mathbb{Z}/(p+1)\mathbb{Z} \cdot \sigma_p.$$

Define the **derivative operator** $D_n \in \mathbb{Z}[\mathrm{Gal}(H_n/H_1)]$ by

$$D_n := \prod_{p|n} D_p,$$

where D_p is any solution to $(\sigma_p - 1)D_p = p + 1 - \mathrm{tr}_{H_1}^{H_p}$, and define

$$\mathcal{P}_n := \sum_{\tau \in T_n} \tau(D_n P_n),$$

where T_n is a set of coset representatives for $\mathrm{Gal}(H_n/H_1)$ in $\mathrm{Gal}(H_n/K)$.

Derived classes

Lemma

The class of $\mathcal{P}_n$ in $E(H_n)/\ell E(H_n)$ is invariant under the action of $G_n := \mathrm{Gal}(H_n/K)$ and lies in the $\epsilon_n := \epsilon \cdot (-1)^{\sigma_0(n)}$ eigenspace.

Proof.

Norm compatibilities and Lemma (τ). □

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

$$
\begin{array}{ccccc}
 & & H^1(G_n, E(H_n)[\ell])^{\epsilon_n} = 0 & & \\
 & & \downarrow \mathrm{inf}_n & & \\
H^1_f(K, E[\ell])^{\epsilon_n} & \xrightarrow{\delta} & H^1(K, E[\ell])^{\epsilon_n} & \longrightarrow & H^1_s(K, E[\ell])^{\epsilon_n} \\
\downarrow & & \downarrow \mathrm{res}_n & & \downarrow \\
H^1_f(H_n, E[\ell])^{G_n \epsilon_n} & \xrightarrow[\delta_n]{} & H^1(H_n, E[\ell])^{G_n \epsilon_n} & \longrightarrow & H^1_s(H_n, E[\ell])^{G_n \epsilon_n} \\
 & & \downarrow \mathrm{tra}_n & & \\
 & & H^2(G_n, E(H_n)[\ell])^{\epsilon_n} = 0. & &
\end{array}
$$

Ramification of derived classes

Lemma

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

Proof of 1 for good $p \nmid \ell$.

Note that $H^1_s(I_p, E[\ell]) = \mathrm{Hom}(I_p, E[\ell])^{G_p^{\mathrm{nr}}}$. Since $(H_n)_p/K$ is unramified at p, the inertia subgroups of K_p and $(H_n)_p$ are both I_p, so

$$\begin{array}{ccccc} H^1_f(K_p, E[\ell]) & \longrightarrow & H^1(K_p, E[\ell]) & \xrightarrow{(\cdot)^s} & \mathrm{Hom}(I_p, E[\ell]) \\ \downarrow & & \downarrow \mathrm{res}_n & & || \\ H^1_f((H_n)_p, E[\ell]) & \xrightarrow[\delta_n]{} & H^1((H_n)_p, E[\ell]) & \xrightarrow[(\cdot)^s]{} & \mathrm{Hom}(I_p, E[\ell]). \end{array}$$

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

Note that 2 is precisely the reason for the assumption $P_K \notin \ell E(K)$.

References

Different accounts of Kolyvagin's paper on Euler systems:

- K Rubin (1989) The work of Kolyvagin on the arithmetic of elliptic curves
- B Gross (1991) Kolyvagin's work on modular elliptic curves
- T Weston (2001) The Euler system of Heegner points
- H Darmon (2004) Rational points on modular elliptic curves

Relevant papers on non-vanishing of L-functions:

- J-L Waldspurger (1985) Sur les valeurs de certaines fonctions L automorphes en leur centre de symetrie
- D Bump, S Friedberg, and J Hoffstein (1990) Nonvanishing theorems for L-functions of modular forms and their derivatives
- M R Murty and V K Murty (1991) Mean values of derivatives of modular L-series
- M R Murty and V K Murty (1997) Non-vanishing of L-functions and applications