Lecture # 1

- General intro / motivation

Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, $4A^3 + 27B^2 \neq 0$ (!! Δ)

an elliptic curve over $\mathbb{Q}$.

The L-function of E:

$$L(E,s) = \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \times \prod_{p \mid \Delta} \left(1 - \alpha_p p^{-s}\right)^{-1}$$

convergent for ($\mathrm{Re}(s) > \frac{3}{2}$ by Hasse's bound)

where

$$a_p = p + 1 - \#E(\mathbb{F}_p)$$

$$\alpha_p \in \{0, 1, -1\}.$$

By modularity (Wiles et al.) $\exists\, f_E \in S_2(\Gamma_0(N))$ (↑ cond E)

s.t. $L(E,s) = L(f_E, s)$.

In particular, $L(E,s)$ has an analytic continuation to all $s \in \mathbb{C}$ with a function equation

$$L(E,s) = -\varepsilon\, L(E, 2-s) \quad \text{for some } \varepsilon \in \{\pm 1\}$$

By Mordell-Weil theorem,

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \oplus E(\mathbb{Q})_{\text{tors}}$$

for some $r_E \geq 0$.
$\because \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$

Conjecture (BSD)

(1) $r_E = \operatorname{ord}_{s=1} L(E,s)$. (BSD conjecture)

(2) $$\frac{L^{(r_E)}(E,1)}{r_E!\, \Omega_E \cdot R_E} = \frac{\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tors}})^2} \prod_{p \mid \Delta} c_p.$$

(BSD formula)

A major result towards BSD from the 1980s:

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\operatorname{ord}_{s=1} L(E,s) = r$, with $r \in \{0, 1\}$.

Then

(1) $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$, so BSD holds.

(2) $\#Ш(E/\mathbb{Q}) < \infty$

with an upper bound on its size consistent with the BSD formula.

Remarks (a) For CM elliptic curves and $r=0$ earlier major by Coates-Wiles & Rubin.

(b) More recently (2010s, pioneered by Skinner & W. Zhang)

Suppose $\operatorname{corank}_{\mathbb{Z}_p} Sel_{p^\infty}(E/\mathbb{Q}) = r$,

with $r \in \{0, 1\}$.

Then (under some assumptions on p)

(1)' $\operatorname{ord}_{s=1} L(E, s) = r$, so BSD holds.

(p-converse)

(2)' $$\operatorname{ord}_p\left(\frac{L^{(r)}(E,1)}{\Omega_E \cdot R_E}\right) = \operatorname{ord}_p\left(\frac{\#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{tors}\right)^2} \cdot \prod_{\ell \mid \Delta} c_\ell\right)$$

so the "p-part" of BSD formula holds.

- Overview of the theorem of Gross-Zagier & Kolyvagin

Let $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}_{<0}$ squarefree

Write $E : y^2 = x^3 + Ax + B$.

and consider

$$E^K : Dy^2 = x^3 + Ax + B.$$

$$L(E/K, s) = L(E, s) L(E^K, s).$$

- Step 1. Gross-Zagier formula.

Suppose $\operatorname{ord}_{s=1} L(E, s) =: r \leq 1$.

Then can choose K so that:

- $\operatorname{ord}_{s=1} L(E/K, s) = 1$.
- $L'(E/K, 1) = \begin{pmatrix} \text{nonzero} \\ \text{const.} \end{pmatrix} \times \langle y_K, y_K \rangle_{NT}$

where $y_K \in E(K)$ is a Heegner point.

Since $\langle y_K, y_K \rangle_{NT} \neq 0 \iff y_K \notin E(K)_{tors}$

get

$$\text{ord}_{s=1} L(E,s) \leq 1 \implies y_K \notin E(K)_{tors}.$$

- Step 2. Kolyvagin's theorem.

  Suppose $y_K \notin E(K)_{tors}$.

  Then:

  (1) $\text{rank}_{\mathbb{Z}} E(K) = 1$.

  (2) $\#Ш(E/K) < \infty$

  with $\#Ш(E/K) \mid [E(K) : \mathbb{Z} y_K]^2 \cdot t_{E/K}$

  for certain $t_{E/K} \in \mathbb{Z}_{\geq 1}$

  divisible only by primes

  in an "explicit" finite set $\mathcal{S}_E$.

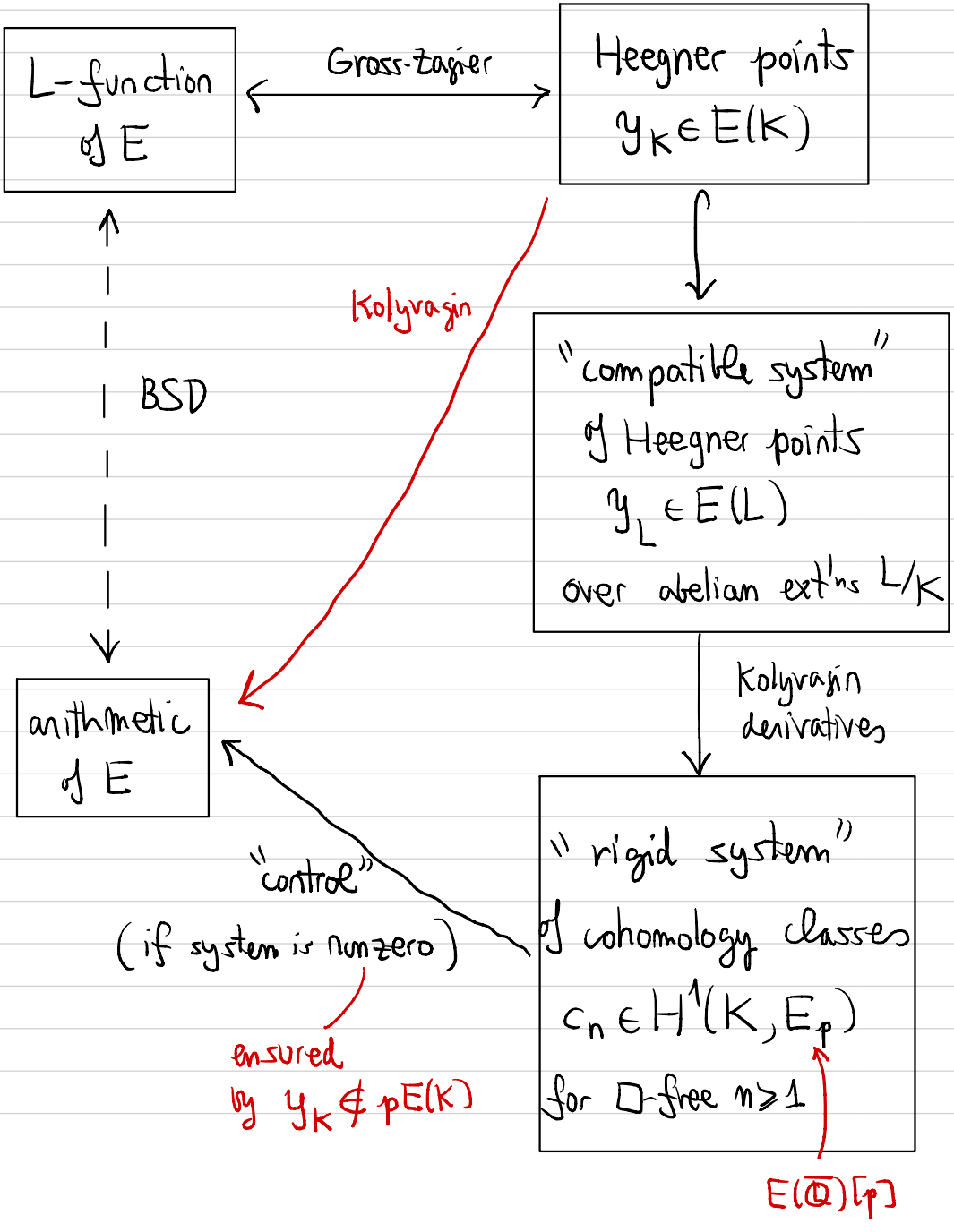
$\therefore \quad \#Ш(E/\mathbb{Q}) < \infty$

& (since $\gamma_K^{\sigma} = \varepsilon \gamma_K + \text{tors}$) $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$.

σ: complex conjugation

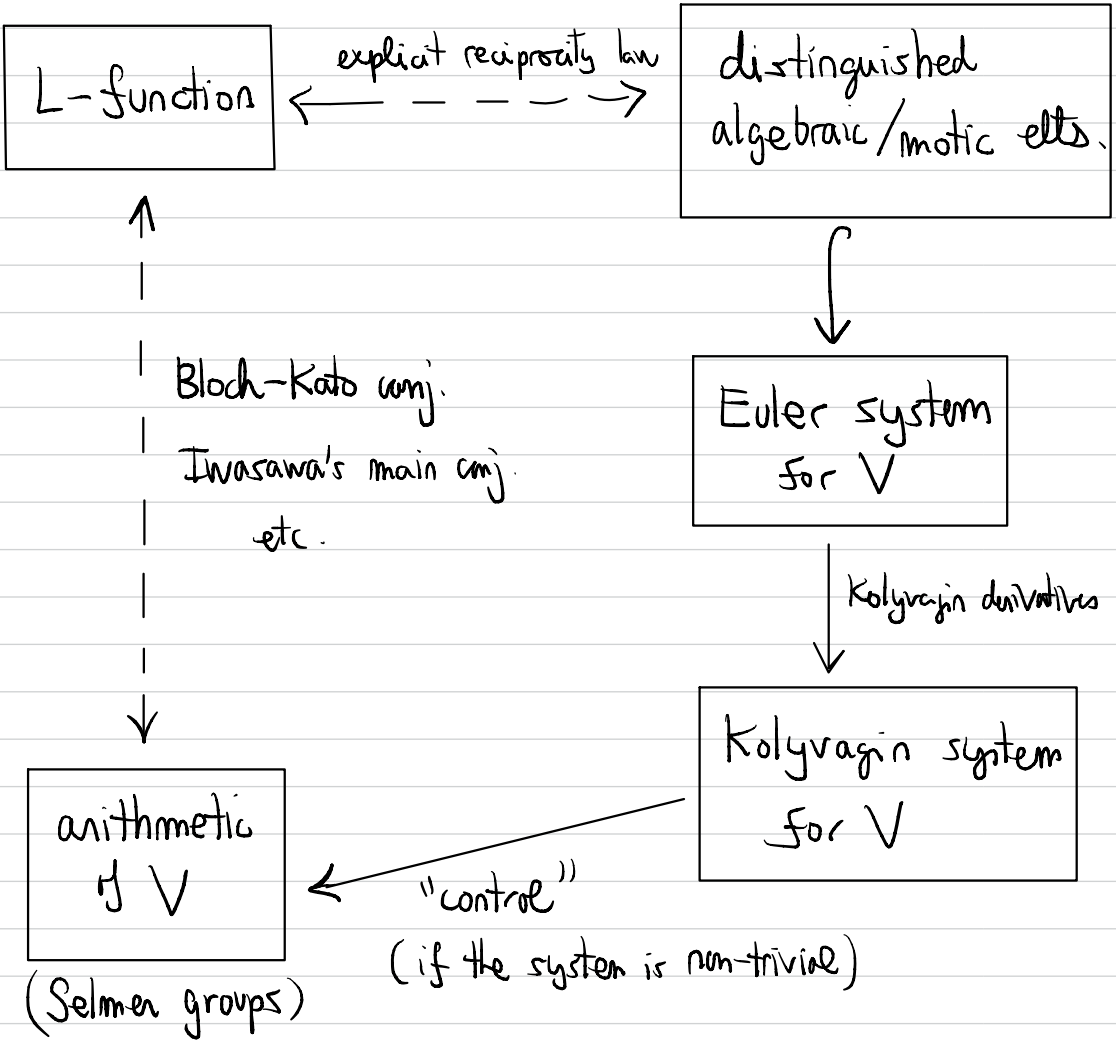
This mini-course: A proof of Kolyvagin's theorem.

Picture to be explained



This picture generalizes as follows:

V = finite dim'l $\mathbb{Q}_p$-vector space
w/ continuous linear $G_{\mathbb{Q}}$-action



- Heegner points

Recall from the theory of CM.

$K =$ imaginary quadratic field.

$\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ order of K of conductor $n \geq 1$.

$A = \mathbb{C}/\Lambda$ elliptic curve with CM by $\mathcal{O}_n$:

$$\mathrm{End}(A) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} \cong \mathcal{O}_n.$$

Then $\underset{\underset{j(\Lambda)}{\shortparallel}}{j(A)} \in \overline{\mathbb{Q}}$

and $K(j(A)) = H_n$, the ring class field of K of conductor n.

Picard group of $\mathcal{O}_n$

$$\mathrm{Gal}(H_n/K) \cong \mathrm{Cl}(\mathcal{O}_n)$$

$$\sigma_{\mathfrak{p}} = \left(\frac{H_n/K}{\mathfrak{p}}\right) \longleftrightarrow [\mathfrak{p}]$$

$\mathfrak{p}$: proper $\mathcal{O}_n$-ideal

$\sigma_{\mathfrak{p}}$: Frobenius elt.

Moreover, $j(A)^{\sigma_{\mathfrak{p}}} = j(\mathfrak{p}^{-1}\Lambda)$.

Now let $E/\mathbb{Q}$ be an elliptic curve of conductor N

By Wiles et. al., $\exists$ modular parametrization

$$\Phi : X_0(N) \longrightarrow E \quad \text{over } \mathbb{Q}$$

with $X_0(N)$ is the modular curve satisfying

$$\underbrace{X_0(N)(\mathbb{C}) \setminus \{\text{cusps}\}}_{\| \; Y_0(N)(\mathbb{C})} = \Gamma_0(N) \backslash \mathcal{H}$$

$$\updownarrow \; 1:1$$

$$\left\{ \begin{array}{c} \text{isogenies} \\ \mathbb{C}/\Lambda \xrightarrow{\varphi} \mathbb{C}/\Lambda' \\ \text{w/ } \ker\varphi \cong \mathbb{Z}/N\mathbb{Z} \end{array} \right\}_{/\cong}$$

Let $K = \mathbb{Q}(\sqrt{D})$ imaginary quadratic field ($\neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{3})$ for simplicity)

satisfying

every prime $\ell \mid N$ splits in K

"Heegner hypothesis"

$$\Rightarrow \exists \, \mathcal{N} \subset \mathcal{O}_K \text{ s.t. } \mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

Definition. Let $n \geq 1$ coprime to N.

The **Heegner point of conductor n** is

$$y_n = \Phi(z_n) \in E(H_n).$$

where

$$z_n = \left[\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/(\mathcal{N}_n \mathcal{O}_n)^{-1} \right] \in X_0(N)(H_n)$$

Note. The Heegner point $y_K \in E(K)$ in the statement of GZ & Kolyvagin's thm. is

$$y_K := \mathrm{Norm}_{H_1/K}(y_1)$$

where

$$\mathrm{Norm}_{H_1/K} : E(H_1) \to E(K)$$
$$x \mapsto \sum_{\sigma \in \mathrm{Gal}(H_1/K)} \sigma x.$$

Proposition 1 (Norm relations).

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ inert in K.

Then

$$\boxed{\mathrm{Norm}_{H_n/H_m}(y_n) = a_\ell \cdot y_m}$$

where $a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell)$.

Proof. Just the case $m = 1$ for simplicity.

We have $T_\ell \cdot f_E = a_\ell \cdot f_E$

$$\Rightarrow \Phi(\ell\tau) + \sum_{k=0}^{\ell-1} \Phi\left(\frac{\tau + k}{\ell}\right) = a_\ell \cdot \Phi(\tau)$$

$$\forall \tau \in \mathcal{H}.$$

Writing $\mathcal{O}_K = \underbrace{\mathbb{Z}\theta + \mathbb{Z}}_{\| \; [\theta, 1]}$

the lattices $\underbrace{[\ell\theta, 1]}_{\| \; \mathcal{O}_\ell}$, $[\theta + k, \ell]$ $(0 \le k \le \ell - 1)$

define $\ell + 1$ different classes

in $\ker\left(Cl(\mathcal{O}_\ell) \longrightarrow Cl(\mathcal{O}_K)\right)$

$\| ?$ $\qquad a \longmapsto a\mathcal{O}_K$

$Gal(H_\ell / H_1)$

$\uparrow$ cyclic of order $\ell + 1$.

and $Gal(H_\ell / H_1)$ acts simply transitively on them (by CM theory)

$$\Rightarrow \quad a_\ell \, y_1 = a_\ell \, \Phi(\theta)$$

$$= \underbrace{\Phi(\ell\theta)}_{\| \; y_\ell} + \sum_{k=0}^{\ell-1} \Phi\left(\frac{\theta+k}{\ell}\right)$$

$$= \sum_{\sigma \in Gal(He/H_1)} \sigma y_\ell$$

$$= \text{Norm}_{He/H_1}(y_\ell). \qquad \blacksquare$$