In this talk, we will state Gross-Zagier and Kolyvagin's results on the Birch and Swinnerton–Dyer conjecture in analytic rank <=1. We will also introduce the Heegner points and explain their basic properties.
Reference: Lectures 1 and 2 of [Cas21] and the article [Gro91].

§ Outline of the talk:

1. Motivation (already discussed a bit in Lec. 1)
2. Heegner points
3. Norm relations → Euler system.

§1 Motivation

Let

$$E: y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}, \quad \Delta := 4A^3 + 27B^2 \neq 0$$

be an ell. curve $/\mathbb{Q}$.

$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ (convergent, by Hasse's bound)

Lec. 6 ⇝ assign an L-func. to E: for $\mathrm{Re}(s) > \frac{3}{2}$

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

w/ $a_p = p + 1 - \#E(\mathbb{F}_p)$, $\alpha_p \in \{0, 1, -1\}$

Lec. 6

$$L(E/F, s) \overset{!}{:=} \prod_p \underbrace{L_p(E/F, N_p^{-s})^{-1}}$$

$$= \begin{cases} 1 - a_p s + N_p s^2 & \text{good red'n} \\ 1 - s & \text{split mult.} \\ 1 + s & \\ 1 & \vdots \end{cases}$$

* in part., $L(E,s)$ has an analytic cont. to all $s \in \mathbb{C}$ w/ a functional eqn.:

$$L(E, s) = -\varepsilon L(E, 2-s)$$

(Modularity, Wiles et al.) $\Rightarrow \exists f_E \in S_2(\Gamma_0(N))$ s.t.

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

Thm. (Mordell-Weil) $\exists r_E \geq 0$ s.t. ($r_E = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$)

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

Conjecture (BSD)

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

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

- Ω_E: real period of E multiplied by the # of connected components of E
- R_E: regulator of E
- $Ш(E/\mathbb{Q})$: Tate-Shafarevich gp.
- Δ: conductor of E
- c_p: Tamagawa # at a prime p

major result towards BSD

MAIN THEOREM

Thm. (Gross-Zagier, Kolyvagin, 1980's) Suppose $\operatorname{ord}_{s=1} L(E,s) = r$, w/ $r \in \{0,1\}$. Then

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

(ii) $\#Ш(E/\mathbb{Q}) < \infty$, w/ an upper bd. on its size consistent w/ the BSD formula

* Remarks:

(a) For CM ell. curves & $r=0$ this was done previously by Coates-Wiles & Rubin

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

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

w/ $r \in \{0,1\}$.

$\Rightarrow$ (under some assumpt. on p)

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

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

so the "p-part" of BSD formula holds

* Goal for the remaining lectures: a proof of Kolyvagin's thm.

⇝ overview of the thm. of Gross-Zagier & Kolyvagin:

Step 0: setup

Let $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}_{<0}$ squarefree, write $E: y^2 = x^3 + Ax + B$ & consider

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

$$L(E/K, s) = \underbrace{L(E, s)}_{\prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}} \underbrace{L(E^K, s)}_{\text{twisted } L\text{-func., w/ a twist on } E: \; y \mapsto y\sqrt{D}}$$

Step 1: Gross-Zagier formula

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

(G.-Z.) $\Rightarrow$ we can choose K s.t. (ell. curve E over K)

1. $\operatorname{ord} L(E/K, s) = 1$,
2. $L'(E/K, 1) = \#C_{E,K} \cdot \langle y_K, y_K \rangle_{NT}$, ($\#C_{E,K}$: $\circ$ const.; $\langle \cdot, \cdot \rangle_{NT}$: Neron-Tate height pairing)

where $y_K \in E(K)$ is a **Heegner point** (↑ so y_K satisfies the Heegner hypothesis!)

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

⇝ $$r = \operatorname{ord}_{s=1} L(E, s) = 1 \Rightarrow L'(E/K, 1) \neq 0 \overset{\text{G.-Z.}}{\Rightarrow} \langle y_K, y_K \rangle_{NT} \neq 0 \Rightarrow y_K \notin E(K)_{tors}$$

$$\Rightarrow r_E \geq 1 \quad \text{(Mordell-Weil)}$$

Step 2: Kolyvagin's thm.

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

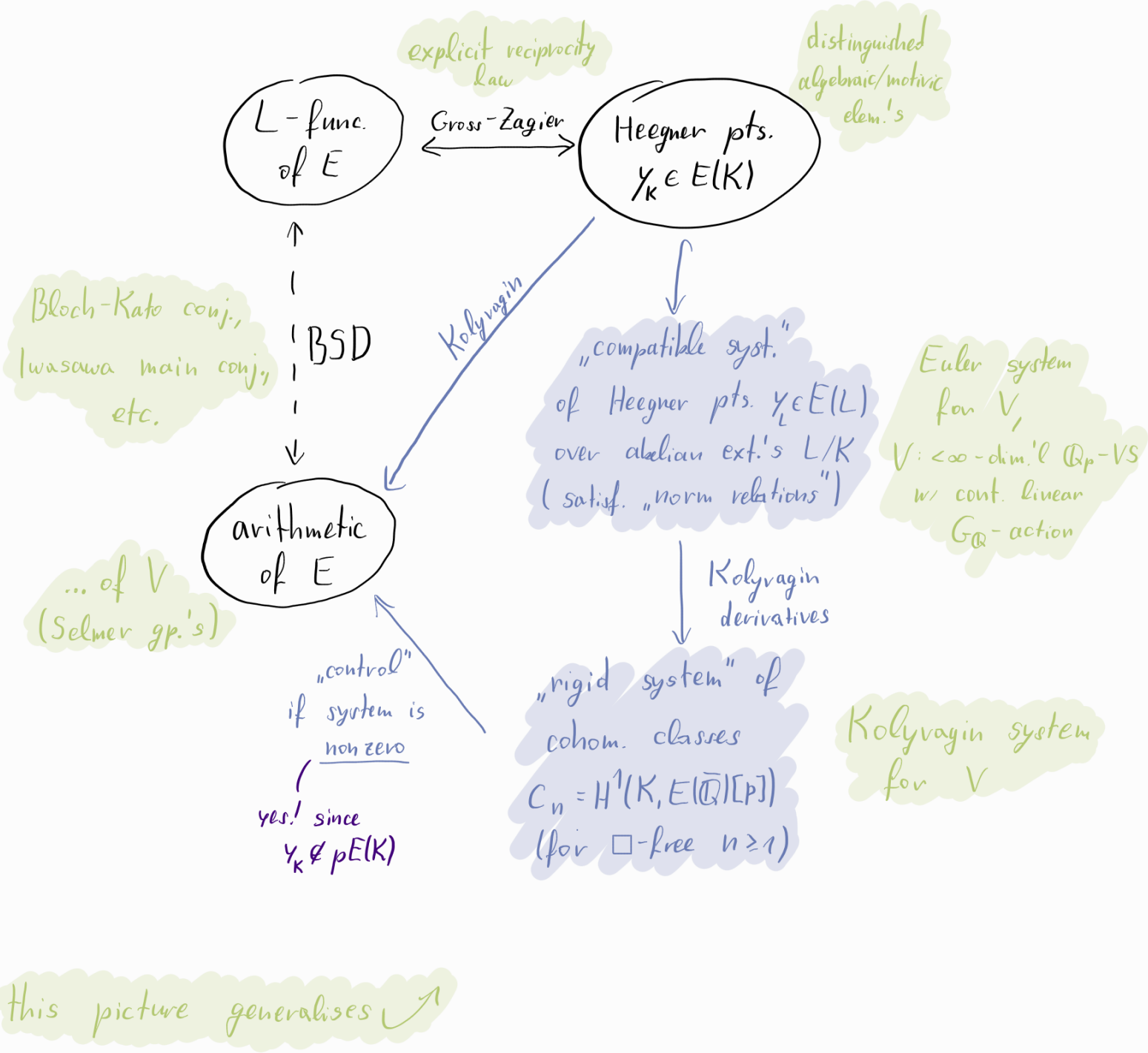
1. $\operatorname{rank}_{\mathbb{Z}} E(K) = 1$
2. $\#Ш(E/K) < \infty$ w/ $\#Ш(E/K) \mid [E(K) : \mathbb{Z} y_K]^2 \cdot t_{E/K}$, $t \in \mathbb{Z}_{\geq 1}$, divisible only by primes in an "explicit" $< \infty$ set

Assuming $\#Ш(E/\mathbb{Q}) < \infty$ (& since $y_K^{\tau} = \varepsilon y_K + \text{tors}$, (complex conjug.; $L(E,s) = \varepsilon L(E,2-s)$, $\varepsilon \in \{\pm 1\}$)

(Gross-Zagier & Kolyvagin) $\Rightarrow$

$\underbrace{\text{rank}_{\mathbb{Z}} E(\mathbb{Q})}_{= r_E} = 1 = r$

Summa summarum:



this picture generalises ↗

§2 Heegner points

* order $\mathcal{O}$ in quadratic field K: $\mathcal{O} \subset K$ s.t.
(i) $1 \in \mathcal{O} \subset K$ (subring) & $\mathcal{O} \supset \mathbb{Q}$-basis of K
(ii) $\mathcal{O}$: f.g. $\mathbb{Z}$-module

SETUP

Let $K :=$ imaginary quadratic field
$\mathcal{O}_n := \mathbb{Z} + n\mathcal{O}_K$ ($\mathcal{O}_K$: max.'l order; $\mathcal{O}_K = [1, \frac{d_K + \sqrt{d_K}}{2}]$, $d_K = -4D$) order of K of conductor $n \geq 1$
(bc. of $\wp$ func.: (complex torus) $\to$ (ell. curve))
$A := \underbrace{\mathbb{C}/\Lambda}_{\{z+\Lambda\}}$ ell. curve w/ CM by $\mathcal{O}_n$:

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

(theory of CM) $\Rightarrow$

$$j(A) = j(\Lambda) \in \overline{\mathbb{Q}} \quad \& \quad \underbrace{K(j(A))}_{\text{this is algebraic / } K} \overset{\text{see [Cox] Thm. 11.1}}{=} H_n =: \text{the ring class field of } K \text{ of conductor } n$$

(Abelian extension)

$Pic(\mathcal{O}_n) := H^1(\mathcal{O}_n, \mathcal{O}_n^*)$ (112) — how does the Galois gp. look like?

moreover:

$$\begin{cases} Cl(\mathcal{O}_n) \xrightarrow{\sim} Gal(H_n/K) \\ [\mathfrak{P}] \longmapsto \sigma_{\mathfrak{P}} = \left[\frac{H_n/K}{\mathfrak{P}}\right] \end{cases}$$

($\mathfrak{P}$: proper $\mathcal{O}_n$-ideal; $\sigma_{\mathfrak{P}}$: Frobenius elem.: unique $\sigma \in Gal(H_n/K)$ s.t. $\forall \alpha \in \mathcal{O}_K$: $\sigma(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{P}|} \pmod{\mathfrak{P}}$)

Let $E/\mathbb{Q}$ be an ell. curve of conductor N. ($End(E) = \mathbb{Z} + N\mathcal{O}_K$)

Thm. (Modularity) $\Rightarrow \exists$ modular parametrization

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

w/ $X_0(N)$: modular curve satisfying

$$\underbrace{X_0(N)(\mathbb{C}) \setminus \{\text{cusps}\}}_{= Y_0(N)(\mathbb{C})} = \Gamma_0(N)\backslash\mathcal{H} \quad \overset{1:1}{\longleftrightarrow} \quad \left\{ \begin{array}{c} \text{isogenies} \\ \mathbb{C}/\Lambda \xrightarrow{\varphi} \mathbb{C}/\Lambda' \\ \text{w/ } \ker\varphi \cong \mathbb{Z}/N\mathbb{Z} \end{array} \right\} / \cong$$

("enhanced ell. curves for $\Gamma_0(N)$")

$(\mathbb{C}/\Lambda, \langle \frac{1}{N} + \Lambda \rangle)$, $(\mathbb{C}/\Lambda', \langle \frac{1}{N} + \Lambda' \rangle)$ equal iff $\Gamma_0(N)T = \Gamma_0(N)T'$, i.e. if $\exists$ isom. taking $\mathbb{C}/\Lambda \mapsto \mathbb{C}/\Lambda'$ & $\langle \frac{1}{N} + \Lambda \rangle \mapsto \langle \frac{1}{N} + \Lambda' \rangle$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \ (N) \right\}$$

* $j(T)$ & $j(NT)$ are modular func.'s for $\Gamma_0(N)$ & modular func.'s for $\Gamma_0(N)$ are rational func.'s in $j(T)$ & $j(NT)$ $\Rightarrow$ field of merom. func.'s on $X_0(N)$ is $\mathbb{C}(j(T), j(NT))$

$\star$ $K := \mathbb{Q}(\sqrt{D})$ imaginary quad. field ($D \neq -1, -3$ for simplicity) satisfying

every prime $\ell \mid N$ splits in K (Heegner hypothesis)

$\Rightarrow \exists \mathcal{N} \subset \mathcal{O}_K : \mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$

Def. $n \geq 1$, $(n, N) = 1$. The **Heegner point of conductor n** is

$$Y_n := \Phi(z_n) \in E(H_n),$$

where $z_n = [\mathbb{C}/\mathcal{O}_n \longrightarrow \mathbb{C}/(\mathcal{N} \cap \mathcal{O}_n)^{-1}] \in X_0(N)(H_n)$

Heegner pts. are pairs (E, E') of N-isogenous curves w/ the same ring $\mathcal{O}_n$ of CM

also define

$$Y_K := \mathrm{Norm}_{H_1/K}(Y_1) \in E(K),$$

where

$$\mathrm{Norm}_{H_1/K} : \begin{cases} E(H_1) \longrightarrow E(K) \\ x \longmapsto \sum_{\sigma \in \mathrm{Gal}(H_1/K)} \sigma x \end{cases}$$

§3 Norm relations → Euler system

Prop. 1 (Norm relations) Suppose $n = \ell m$, w/ $\ell \nmid m$ inert in K. Then

$$\mathrm{Norm}_{H_n/H_m}(Y_n) = a_\ell \cdot Y_m,$$

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

pf. For the Hecke operator T_ℓ we have:

$$T_\ell \cdot f_E = a_\ell \cdot f_E,$$

(on modular forms)

so

$$\Phi(\ell z) + \sum_{k=0}^{\ell-1} \Phi\left(\frac{z+k}{\ell}\right) = a_\ell \cdot \Phi(z), \quad \forall z \in \mathcal{H}.$$

And for $[E,C] = [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau \rangle]$ (cyclic subgp.; lattice $[\tau, 1]$) in a modular space, we have

$$T_\ell[E,C] = [\mathbb{C}/\Lambda_{\ell\tau}, \langle 1/N + \Lambda_{\ell\tau}\rangle] + \sum_{k=0}^{\ell-1} [\mathbb{C}/\Lambda_{(\tau+k)/\ell}, \langle 1/N + \Lambda_{(\tau+k)/\ell}\rangle].$$

Write $\mathcal{O}_K = [\theta, 1]$. $\rightsquigarrow$ the lattices $[\ell\theta, 1] = \mathcal{O}_\ell, ([\theta+k, \ell])_{0\le k\le \ell-1}$ define $\ell+1$ different classes in

$$\ker\left(\begin{array}{c} Cl(\mathcal{O}_\ell) \longrightarrow Cl(\mathcal{O}_K) \\ a \longmapsto a\mathcal{O}_K \end{array}\right) \overset{\sim}{=} Gal(H_\ell/H_1) \cong (\mathcal{O}_K/\ell\mathcal{O}_K)^\times/(\mathbb{Z}/\ell\mathbb{Z})^\times$$

(why?) — cyclic of order $\ell+1$ — $\cong \mathbb{F}_\ell^\times$ — order $\ell-1$

$\{$ell. curves w/ CM$\}$ $\longleftrightarrow$ $Pic(\mathcal{O}) \cong Gal(K(j(\mathcal{O}))/K)$, $\mathbb{C}/a \longmapsto a$

ℓ inert

* if ℓ split $\Rightarrow$ $\mathcal{O}_K/\ell\mathcal{O}_K \cong \mathbb{F}_\ell[x]^2$ $\rightsquigarrow$ different Norm relations! & Gal. gp. has order $\ell-1$

& $Gal(H_\ell/H_1) \curvearrowright \mathcal{O}_\ell/[\theta+k, \ell]$ simply transitively (by CM Theory)

i.e.
$$\sum_{\sigma\in G_\ell} \sigma(\mathbb{C}/\mathcal{O}_n \longrightarrow \mathbb{C}/W_n^{-1}) = \sum_{\sigma\in G_\ell} \sigma((\mathbb{C}/\mathcal{O}_m)/C \longrightarrow (\mathbb{C}/W_m^{-1})/C), \quad C := (\mathbb{C}/\mathcal{O}_n)$$
$$= \sum ((\mathbb{C}/\mathcal{O}_m)/(Ca^{-1}) \longrightarrow (\mathbb{C}/W_m^{-1})/(Ca^{-1}))$$

$\Rightarrow$

$$a_\ell Y_1 = a_\ell \Phi(\theta)$$
$$= \underbrace{\Phi(\ell\theta|}_{Y_\ell} + \sum_{k=0}^{\ell-1} \Phi\left(\frac{\theta+k}{\ell}\right)$$
$$= \sum_{\sigma\in Gal(H_\ell/H_1)} \sigma Y_\ell = Norm_{H_\ell/H_1}(Y_\ell)$$

□

Prop. 2 (Congruence relations) Suppose $n = \ell m$, w $\ell \nmid m$ inert in K & write $\ell\mathcal{O}_K = \lambda$. ($n$ □-free $\Rightarrow \ell \nmid m$, prime satisf. Heegner cond.) $\Rightarrow$

(i) λ splits completely in H_m

(ii) $\forall$ prime $\lambda_m \mid \lambda$ in H_m is totally ramified in H_n ($\lambda_m \mathcal{O}_{H_m} = (\lambda_n)^{\ell+1}$)

(iii)
$$Y_n \equiv \left[\frac{H_n/\mathbb{Q}}{\lambda_m}\right] Y_m \pmod{\lambda_n},$$

where λ_n is the unique prime of H_n above λ_m

* equivalently,

$$\mathrm{red}_{\lambda_n}(Y_n) = \mathrm{Frob}_\ell \, \mathrm{red}_{\lambda_m}(Y_m) \quad \in \tilde{E}(\mathbb{F}_{\ell^2}),$$

where

$$\mathrm{red}_{\lambda_n} : E(H_n) \longrightarrow \tilde{E}(\mathcal{O}_{H_n}/\lambda_n)$$
$$\| $$
$$\mathrm{red}_{\lambda_m} : E(H_m) \longrightarrow \tilde{E}(\mathcal{O}_{H_m}/\lambda_m) = \tilde{E}(\mathbb{F}_{\ell^2})$$

are the reduction maps.

the prime λ is principal, & generated by an integer ℓ w/ $(\ell, m) = 1$

pf. (i) & (ii) Follows from class field theory.

(iii) (Prop. 1) $\Rightarrow$

$$a_\ell Y_m = \sum_{\sigma \in \mathrm{Gal}(H_n/H_m)} \sigma Y_n$$

$$\Rightarrow \quad a_\ell \cdot \mathrm{red}_{\lambda_m}(Y_m) = \sum_{\sigma \in \mathrm{Gal}(H_n/H_m)} \underbrace{\mathrm{red}_{\lambda_n}(\sigma Y_n)}_{= \sigma \, \mathrm{red}_{\lambda_n}(Y_n) = \mathrm{red}_{\lambda_n}(Y_n)}$$

$$= (\ell + 1) \, \mathrm{red}_{\lambda_n}(Y_n)$$

on the other hand:

(Eichler-Shimura congruence relation) $\ell \nmid N$ (prime), we have

$$T_\ell = \mathrm{Frob}_\ell + \mathrm{Frob}_\ell^{tr}$$

as correspondences on $X_0(N)/\mathbb{F}_\ell$. Here $\mathrm{Frob}_\ell^{tr} : Y \longmapsto \sum_{x \in \mathrm{Frob}_\ell^{-1}(Y)} x$.

this is the correspondence w.r.t. the transpose of the graph of Frob_ℓ

$\Rightarrow$

$$T_\ell z_m = \mathrm{Frob}_\ell z_m + \mathrm{Frob}_\ell^{tr} z_m \qquad \text{(as divisors on } X_0(N)(\mathbb{F}_{\ell^2})\text{)}$$

$\Rightarrow$ (apply $\Phi(\cdot)$)

$$\underbrace{a_\ell \cdot \mathrm{red}_{\lambda_m}(Y_m)}_{(\ell+1)\,\mathrm{red}_{\lambda_n}(Y_n)} = \mathrm{Frob}_\ell \, \mathrm{red}_{\lambda_m}(Y_m) + \mathrm{Frob}_\ell^{tr} \, \mathrm{red}_{\lambda_m}(Y_m)$$

(as divisors on $\tilde{E}(\mathbb{F}_{\ell^2})$ $\mod \ell$)

since $\forall \alpha \in \mathbb{F}_{\ell^2}$ ($\mathbb{F}_{\ell^2}$ has ℓ^2 elem.'s): $\alpha^{\ell} = \alpha^{\frac{1}{\ell}} \Rightarrow$ all pts. in the divisor $\tilde{E}(\mathbb{F}_{\ell^2})$ are congruent to $\mathrm{Frob}_\ell \, \mathrm{red}_{\lambda_m}(Y_m)$

$\Rightarrow$

$$\mathrm{red}_{\lambda_n}(Y_n) \equiv \mathrm{Frob}_\ell \, \mathrm{red}_{\lambda_m}(Y_m) \pmod{\lambda_n}$$

□

* Remark: (Prop 1 & 2) $\Rightarrow \forall$ prime p,

$$\left\{ \delta(Y_n) \in H^1(H_n, \overbrace{T_p E}^{E[p]}) \right\}_{(m,N)=1}$$

Kummer map: $(E(K_n)/pE(K_n))^{G_n} \xrightarrow{\delta_n} H^1(K_n, E[p])^{G_n}$

$\square$ - free product of primes inert in K

form an (anti-cyclotomic) Euler system for $T_p E$.

* next time: Kolyvagin's thm. „mod p"