Modular Curves + Heegner Points Ricky

$\boxed{\S 1 \quad \text{CM Theory}}$

Let $E/\mathbb{C}$ be an elliptic curve, so $E(\mathbb{C}) = \mathbb{C}/\Lambda_\tau$ where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ writing $E = E_\tau$, $\tau \in \mathcal{H}$.

Recall that $\text{End}(E) = \begin{cases} \mathbb{Z} \\ \mathcal{O} \underset{\text{order}}{\subseteq} K, \ K/\mathbb{Q} \text{ im quadratic} \end{cases}$

Lemma $\text{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') = \{ \alpha \in \mathbb{C} \mid \alpha \Lambda \subseteq \Lambda' \}$.

Pf Lift $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ to $\varphi : \mathbb{C} \to \mathbb{C}$ to see $\varphi(z) = \alpha z$, $\exists \alpha \in \mathbb{C}^\times$. $\square$

So $\text{End}(E_\tau) = \{ \alpha \in \mathbb{C} \mid \alpha \Lambda_\tau \overset{?}{\subseteq} \Lambda_\tau \}$

If ~~$\alpha\alpha$~~ $\alpha \cdot 1 = m_1 + m_2 \tau$

$\alpha \cdot \tau = n_1 + n_2 \tau$ Then .. (by mult $\alpha \cdot 1 \cdot \tau - \alpha \cdot \tau$)

$$\underbrace{m_2}_{A} \tau^2 + \underbrace{(m_1 - n_1)}_{B} \tau \underbrace{- n_1}_{C} = 0 \qquad A, B, C \in \mathbb{Z}$$

$\boxed{\Delta := B^2 - 4AC}$, $\Delta = -f^2 d < 0$ call $\boxed{\begin{array}{l} f = \text{conductor of } \tau \\ d = \text{discriminant of } \tau \end{array}}$

Then if $\text{End}(E_\tau) \neq \mathbb{Z}$, $\text{End}(E_\tau) =$

$$\mathbb{Z} \oplus f\,\mathbb{Z}\left[\frac{-d + \sqrt{-d}}{2}\right] =: \mathcal{O}_\Delta \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$$

We say E has CM by $\mathcal{O}_\Delta$.

Rmk: We can create elliptic curves w/ CM by $\mathcal{O}$ by creating:

- $\mathbb{C}/\mathcal{O}$
- In fact, all elliptic curves w/ CM by $\mathcal{O}$ are iso to $\mathbb{C}/\mathfrak{a}$, $\mathfrak{a}$ fractional ideal of $\mathcal{O}$.

Thm: Let $E/\mathbb{C}$ be an elliptic curve w/ CM by $\mathcal{O}_K$, $K/\mathbb{Q}$ im quadratic. Then $j(E) \in \mathcal{O}_{H_K}$, where H_K = Hilbert class field of K.
(ie E admits a model over a # field.)

Thm: Let $G = \mathrm{Gal}(H_K/K)$ then we have an isomorphism

$$s: \mathrm{Pic}(\mathcal{O}_K) \longrightarrow G$$
$$\mathfrak{b} \longmapsto s(\mathfrak{b})$$
$$j(\mathfrak{a})^{s(\mathfrak{b})} = j(\mathfrak{b}^{-1}\mathfrak{a})$$

(The j-invariants generate $\mathcal{O}_H$ / this characterizes G as a Galois group)

(Jan Vonk notes)

§2 Modular Curves

Let $\Gamma_0(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid N \mid c \}$

Define $Y_0(N) := \Gamma_0(N) \backslash \mathcal{H}$, $X_0(N) = \Gamma_0(N) \backslash \overline{\mathcal{H}}$

Then $X_0(N)$ can be made into a projective algebraic variety$/\mathbb{Q}$.

Then for $L/\mathbb{Q}$ a field we have the modular interpretation

$Y_0(N)(L) = \{ (E, E', \phi) \mid E, E'/L$ ell curves, $\phi: E \to E'/L$ cyclic isog of deg $N \}$

(ϕ is cyclic of deg N $\Leftrightarrow$ $(\ker \phi)(\mathbb{C}) \simeq \mathbb{Z}/N\mathbb{Z}$)

Atkin-Lehner Involutions let $d \mid N$, $(d, N/d) = 1$. We get an involution $w_d : X_0(N) \to X_0(N)$ such that

$$w_N(\phi: E \to E') = (\hat{\phi} : E' \to E),$$ and it swaps the two cusps.

These generate a group $W \subseteq \mathrm{Aut}(X_0(N))$ w/ the reln

$$w_d w_{d'} = w_{dd'/(d,d')^2}$$

so $W \simeq (\mathbb{Z}/2\mathbb{Z})^s$ where s = # of primes dividing N.

Hecke Algebra: Let $J = \mathrm{Jac}(X_0(N))$. For $m \geq 1$, have Hecke morphisms $T_m : J \to J$ by

$$\sum (P_i - Q_i) \mapsto \sum T_m(P_i) - T_m(Q_i)$$

where $T_m(D) = \sum_C (x_C)$, C running over cyclic subgrps of order m in E s.t. $C \cap \ker\phi = 0$

$$x_C = (E/C \to E'/\phi(C))$$

$$(m, N) = 1.$$

Let $\mathbb{T}$ denote the algebra generated by all the T_m (including $(m,N) \neq 1$, even though we didn't define them) inside $\mathrm{End}_{\mathbb{Q}} J$.

Rmk Interpretation via correspondences, can show principal divisors go to principal divisors.

$\boxed{\text{§3 Heegner Points}}$

Let $E/\mathbb{Q}$ be an elliptic curve, how do we create points in $E(\mathbb{Q}) \setminus \{0\}$?

- $\mathbb{C}$-uniformization is not algebraic!

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$$

- Modularity: $\exists \varphi : X_0(N) \to E$ morphism of varieties$/\mathbb{Q}$!!

Hence, if $x \in X_0(N)(\overline{\mathbb{Q}})$ then $\varphi(x) \in E(\overline{\mathbb{Q}})$ and $\mathrm{tr}(\varphi(x)) \in E(\mathbb{Q})$.

Defn $x \in X_0(N)(\mathbb{C})$ is a $\boxed{\text{Heegner point}}$ if $x = E \to E'$ w/ $\mathrm{End}(E) \simeq E(E') \simeq \mathcal{O} \neq \mathbb{Z}$. CM theory tells us for x a
$\mathcal{O} \subseteq \mathcal{O}_K$
Heegner point, $x \in X_0(N)(H_K)$.

Today: Specialize to case $\mathcal{O} = \mathcal{O}_K$.

Lemma: $N \geq 1$, $\mathcal{O} = \mathcal{O}_K$ then the set of Heegner points in $X_0(N)(\mathbb{C})$ of disc D ($= \operatorname{disc}(\mathcal{O})$) is nonempty iff $\boxed{\exists\, \mathfrak{n} \underset{\text{ideal}}{\subset} \mathcal{O} \text{ s.t. } \mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}}$

Heegner hypothesis for $(N, \mathcal{O})$

~~Rmk HH ⇒ primes dividing N spli~~

Pf $(E \to E')$ Heegner pt on $X_0(N)(\mathbb{C})$.

$E = \mathbb{C}/\mathfrak{a}$, $E' = \mathbb{C}/\mathfrak{b}$ for $\mathfrak{a}, \mathfrak{b}$ fractional ideals of $\mathcal{O}$

WLOG can assume $\mathfrak{a} \subseteq \mathfrak{b}$ so our isogeny is given by

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}, \quad z + \mathfrak{a} \mapsto z + \mathfrak{b}$$

Set $\mathfrak{n} = \mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathcal{O}$.

Then $\mathcal{O}/\mathfrak{n} \simeq \mathfrak{b}\mathfrak{b}^{-1}/\mathfrak{a}\mathfrak{b}^{-1} \simeq \mathfrak{b}/\mathfrak{a} \simeq \mathbb{Z}/N\mathbb{Z}$.

Conversely, given $\mathfrak{n} \subseteq \mathcal{O}$ as above, then take $\mathfrak{a}$ fractional ideal of $\mathcal{O}$, and $x_{\mathfrak{a}} : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ is a cyclic isog of deg N, ie

$x_{\mathfrak{a}} \in X_0(N)$ is Heegner. $\left(\ker = \mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \simeq \mathfrak{n}^{-1}/\mathcal{O} \simeq \mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\right)$.

$\square$

Rmk The proof (no longer just $\mathcal{O}_K$, any order (? ..)) shows that if $(E \to E')$ is a Heegner pt for $(N, \mathcal{O})$ then it looks like

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$$

for $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$.

This gives us a bijection (for a fixed N)

$$\left\{ \begin{matrix} \text{Heegner pts} \\ \text{on } X_0(N)(\mathbb{C}) \end{matrix} \right\} \longleftrightarrow \left\{ (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) \;\middle|\; \begin{matrix} \mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N \\ [\mathfrak{a}] \in \operatorname{Pic}(\mathcal{O}) \end{matrix} \right\}.$$

We have 3 groups acting on the RHS:

- For fixed $\mathcal{O} = \mathcal{O}_K$ for simplicity, $\operatorname{Gal}(H_K/K)$ acts on Heegner points by $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^{s(\mathfrak{b})} = (\mathcal{O}, \mathfrak{n}, [\mathfrak{b}^{-1}\mathfrak{a}])$

switch to ring class field for other orders

• For fixed $\mathcal{O}$ = anything acts on Heegner' W (gp of Atkin-Lehner involutions) (gen'd by W_p for p prime)

$N = p^k m$, $p \nmid m$

$\mathfrak{n} = \mathfrak{p}^k \mathfrak{m}$ then $w_p(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \bar{\mathfrak{p}}^k \mathfrak{m}, [\mathfrak{a}\mathfrak{p}^{-k}])$

Rmk HH $\Rightarrow$ primes dividing N split in K so let $\mathfrak{p} \mapsto \bar{\mathfrak{p}}$ (conj)

Claim $G \times W$ acts simply transitively on the set of Heegner points of fixed disc, so there are $2^s \cdot h_K$ of them, $s = \# p \mid N$.
($\mathcal{O} = \mathcal{O}_K$ here)

Hecke action: $\ell \nmid N$, then $T_\ell(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = \sum_{\mathfrak{a}/\mathfrak{b} \cong \mathbb{Z}/\ell\mathbb{Z}} (\mathcal{O}_{\mathfrak{b}}, \mathfrak{n}_{\mathfrak{b}}, [\mathfrak{b}])$

fractional ideals of $\mathcal{O}$

where $\mathcal{O}_{\mathfrak{b}} = \mathrm{End}(E_{\mathfrak{b}})$, $\mathfrak{n}_{\mathfrak{b}} = \underbrace{\mathfrak{n}\mathcal{O}_{\mathfrak{a}} \cap \mathcal{O}_{\mathfrak{b}}}_{??}$.

If $x \in X_0(N)(\mathbb{C})$ Heegner, want to understand $M := \langle (x) - (\infty) \rangle \subseteq J(H)$ as a cyclic module over

$\mathbb{T}[G]$

Hecke algebra; Galois gp of H

Given χ char of G, f eigenform of wt 2, level N, want to understand / we'll see a reln ship between a "$c_{f,\chi}$ eigen component" of M and the vanishing of the first derivative of an L-fn associated to f, χ evaluated at 1