 ICTS Sept 11 – 15, 2023

Introduction to Mod. Forms, Ell. Curves & Mod. Curves

Lec 1: Mod. theorem for Ell. curves (Ch 1 of [DS])

§ Modular forms

$\mathcal{H}$ = upper half plane

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{array}{c} a, b, c, d \in \mathbb{Z} \\ ad - bc = 1 \end{array} \right\}$$

via: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \dfrac{az+b}{cz+d}$ $\quad z \in \mathcal{H}$.

$$\left(\text{NB: } \operatorname{Im}\left(\frac{az+b}{cz+d}\right) = \frac{\operatorname{Im}(z)}{|cz+d|^2} > 0 \right).$$

Def A mod. form of wt $k \geq 1$ is a holo. fn $f : \mathcal{H} \longrightarrow \mathbb{C}$

s.t. $f\left(\dfrac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ $\quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. $\forall z \in \mathcal{H}$

and s.t. f is holo. at ∞, i.e.

$z \longmapsto q = e^{2\pi i z}$

extends to a holo fn at $q = 0$ (or $z = \infty$).

Thus $f = \sum_{n=0}^{\infty} a_n q^n$ $\quad a_n \in \mathbb{C}$ called the Fourier coefficients.

Let $M_k(SL_2(\mathbb{Z})) = \{$mod. forms of wt k for $SL_2(\mathbb{Z})\}$.

E.g.: Eisenstein series.

Def A mod. form f of wt k is a <u>cusp form</u> if $a_0 = 0$ (i.e., f vanishes at ∞)

<u>E.g. Δ fn.</u>

Let $S_k(SL_2(\mathbb{Z})) = \{$ cusp forms of wt k for $SL_2(\mathbb{Z})\}$

<u>Higher levels:</u> Let $N \geq 1$

Set

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (N) \right\}$$

$$\cap$$

$$\Gamma_1(N) = \left\{ \qquad \cap \qquad \middle| \; \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (N) \right\}$$

$$\cap$$

$$\Gamma_0(N) = \left\{ \qquad \cap \qquad \middle| \; \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (N) \right\}$$

Def A holo fn $f : H \to \mathbb{C}$ is a <u>mod form</u> of wt $k \geq 1$ and level $N \geq 1$ if

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \text{ (or } \Gamma_0(N))$$

and f is holo at the cusps, i.e.

$$\forall\, s \in \Gamma_1(N) \backslash \mathbb{P}^1(\mathbb{Q}) \quad \text{w/} \quad s = \alpha(\infty)$$

$$s = \tfrac{a}{c}, \quad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \infty = [1:0]$$

$$f\Big|_{[\alpha]}(z) = f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-k} \text{ is holo at } \infty$$

(||ly for cusp forms require vanishes at ∞)

Let $M_k(\Gamma_1(N)) \supset M_k(\Gamma_0(N))$ $\quad S_k(\Gamma_1(N)) \supset S_k(\Gamma_0(N))$

§ <u>Elliptic Curves</u>

Def. A <u>lattice in $\mathbb{C}$</u> is $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ w/ ω_1, ω_2 a basis of $\mathbb{C}$ over $\mathbb{R}$ (normalized so that $\frac{\omega_1}{\omega_2} \in H$)

$\longrightarrow$ <u>Lemma:</u> $(\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = (\Lambda' = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2') \Leftrightarrow \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

. A <u>complex torus</u> is $\mathbb{C}/\Lambda$: . ab. gp.

cp. Riemann Surf. of genus 1!

<u>Fact:</u> Every non-zero holo gp homo $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is of the form $[z] \stackrel{\alpha}{\longmapsto} [\alpha z]$ for some $\alpha \neq 0$ w/ $\alpha \cdot \Lambda \subset \Lambda'$.

Now $\mathbb{C}/_{\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2} \xrightarrow[\sim]{\cdot \omega_2^{-1}} \mathbb{C}/\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$

w/ $\tau = \frac{\omega_1}{\omega_2} \in H.$

τ is not unique since clearly $\tau' = \dfrac{a\tau + b}{c\tau + d}$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

also possible.

Get a bijection:

$$\{\text{cx. tori}\}/_{\text{iso}} \longleftrightarrow SL_2(\mathbb{Z}) \backslash H$$

Let $\wp(z) = \dfrac{1}{z^2} + \sum'_{\omega \in \Lambda} \dfrac{1}{(z-\omega)^2} - \dfrac{1}{\omega^2}$ $\quad z \in \mathbb{C}$, $z \notin \Lambda$

Turns out $\mathbb{C}\left(\mathbb{C}/\Lambda\right) = \begin{matrix}\text{field of mero.} \\ \text{fn's on } \mathbb{C}/\Lambda\end{matrix} = \mathbb{C}(\wp, \wp')$

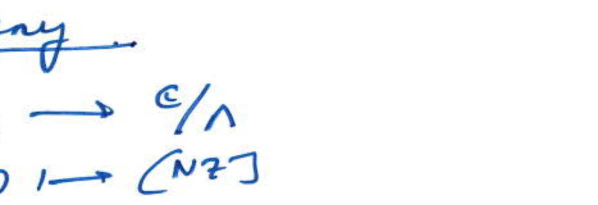
<u>Moreover:</u> $(\wp(z), \wp'(z))$ satisfy $E: y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$

w/ $g_2(\Lambda) = 60 \sum' \frac{1}{\omega^4}$ $\quad (g_2^3 - 27g_3^2 \neq 0)$, $\quad j_E = \dfrac{g_2^3}{\Delta}$

$g_3(\Lambda) = 140 \sum' \frac{1}{\omega^6}$

$\therefore \{\text{cx. tori}\}/_{\text{iso}} \longleftrightarrow \{\text{elliptic curves}/\mathbb{C}\}/_{\text{iso.}}$

<u>gp law:</u> $\mathbb{C}/\Lambda \longleftrightarrow$



Later:

<u>Def</u>. A non-zero holo. map (gp homo) between cx. tori is called an <u>isogeny</u>.

<u>E.g.</u> i) $[N]: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$

$[z] \longmapsto [Nz]$

ii) $[i]: \mathbb{C}/_{\mathbb{Z}[i]} \longrightarrow \mathbb{C}/\mathbb{Z}[i]$

$[z] \longmapsto [iz]$.

<u>Def</u> Let $E = \mathbb{C}/\Lambda$. <u>Weil Pairing</u> $E[N] \times E[N] \longrightarrow \mu_N$

w/ $\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \cdot \begin{pmatrix} \frac{\omega_1}{N} + \Lambda \\ \omega_2/N + \Lambda \end{pmatrix}$ $(\gamma \in M_2(\mathbb{Z}/N))$ $\langle P, Q \rangle \mapsto e^{2\pi i (\det \gamma)/N}$

Modularity Thm of Wiles

Every ell. curve over $\mathbb{Q}$ is modular, i.e.

$$f_{/\mathbb{Q}} \longleftrightarrow E_{/\mathbb{Q}}$$

$\in S_2(\Gamma_0(N))$ normalized newform (eigenform) of level N and wt 2 w/ $a_n \in \mathbb{Z}$.

$y^2 = x^3 + Ax + B$, cond $= N$, up to isogeny.

Get $b_n \in \mathbb{Z}$, $b_p = p+1 - |\tilde{E}(\mathbb{F}_p)|$, $p \nmid N$.

Thm $\boxed{a_n = b_n}$ $\forall n = 1, 2, \ldots$

Rmk: $L(s, E) = L(s, f)$.

(insert isog.)

§ Modular Curves as moduli spaces.

For $\Gamma = \Gamma_0(N) \supset \Gamma_1(N) \supset \Gamma(N)$, set $Y(\Gamma) = \Gamma \backslash \mathbb{H}$
= mod. curve.
= Riem. surface

Have: $Y_0(N) \leftarrow Y_1(N) \leftarrow Y(N)$

Def i) Let $N \geq 1$. An enhanced elliptic curve for $\Gamma_0(N)$ is a pair (E, C)

E: cx. ell. curve; C: cyclic subgp of order N

Write $(E, C) \sim (E', C')$ if $\exists$ iso $\varphi: E \xrightarrow{\sim} E'$, $C \longmapsto C'$

Set $S_0(N) = \{[E, C]\}$

ii) Similarly an enhanced ell. curve for $\Gamma_1(N)$ is a pair (E, Q)

E: cx. ell. curve; Q: pt. of exact order N

Again $(E, Q) \sim (E', Q')$ if $\exists$ iso $E \xrightarrow{\varphi} E'$, $Q \mapsto Q'$

Set $S_1(N) = \{[E, Q]\}$

- Finally an <u>enhanced ell. curve for $\Gamma(N)$</u> is a pair $(E, (P, Q))$ s.to P, Q generate $E[N]$ w/ $\langle P, Q\rangle = e^{\frac{2\pi i}{N}}$

E ← ex. ell curve; P, Q ← pts on E of order N; $\langle P, Q\rangle$ ← Weil pairing; $e^{\frac{2\pi i}{N}}$ ← fixed prim. rt.

Again $(E, (P, Q)) \sim (E', (P', Q'))$ if $\exists$ iso $\varphi : E \to E'$, $P \mapsto P'$, $Q \mapsto Q'$

Write $S(N) = \{[E, (P, Q)]\}$

<u>Thm</u>: <u>We have</u>

i) $S_0(N) = \{[E_z, \langle \frac{1}{N} + \Lambda_z\rangle]\}$, $E_z = \mathbb{C}/\Lambda_z$

ii) $S_1(N) = \{[E_z, \frac{1}{N} + \Lambda_z]\}$

iii) $S(N) = \{[E_z, (\frac{z}{N} + \Lambda_z, \frac{1}{N} + \Lambda_z)]\}$

<u>Moreover</u>: i) $(E_z, \langle \frac{1}{N} + \Lambda_z\rangle) \sim (E_{z'}, \langle \frac{1}{N} + \Lambda_{z'}\rangle)$
$\iff \Gamma_0(N) z = \Gamma_0(N) z'$

ii) $(E_z, \frac{1}{N} + \Lambda_z) \sim (E_{z'}, \frac{1}{N} + \Lambda_{z'})$
$\iff \Gamma_1(N) z = \Gamma_1(N) z'$

iii) $(E_z, (\frac{z}{N} + \Lambda_z, \frac{1}{N} + \Lambda_z)) \sim (E_{z'}, (\frac{z'}{N} + \Lambda_{z'}, \frac{1}{N} + \Lambda_{z'}))$
$\iff \Gamma(N) z = \Gamma(N) z'$

So $\exists$ <u>bijections</u> i) $S_0(N) \longleftrightarrow Y_0(N)$
ii) $S_1(N) \longleftrightarrow Y_1(N)$
iii) $S(N) \longleftrightarrow Y(N)$

<u>Pf</u>: <u>Prove ii)</u> (i), iii) similar):

$\xrightarrow{\text{surj?}}$ Say $[E, Q] \in S_1(N)$. Then $E \simeq \mathbb{C}/\Lambda_{z'}$, some z'

Write $Q = \frac{cz' + d}{N} + \Lambda_{z'}$ w/ $(c, d, N) = 1$ $\because$ exact order of $Q = N$.

⑥

$\therefore \quad \exists\ a, b, k \in \mathbb{Z}$ s.t. $\quad ad - bc - kN = 1$

$\therefore$ Under $\quad M_2(\mathbb{Z}) \longrightarrow M_2(\mathbb{Z}/N)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \quad \underset{\cup}{} SL_2(\mathbb{Z}/N)$$

WMA $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ ($\because SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/N)$ and changing c, d mod N doesn't change φ).

Let $\quad z := \dfrac{az'+b}{cz'+d}, \quad \alpha := cz'+d$

So $\alpha z = az'+b$

Then • $\alpha \Lambda_z = \mathbb{Z}\alpha z \oplus \mathbb{Z}\alpha = \mathbb{Z}(az'+b) \oplus \mathbb{Z}(cz'+d)$

$= \Lambda_{z'}$ (by Lemma!)

• $\alpha\left(\frac{1}{N} + \Lambda_z\right) = \dfrac{cz'+d}{N} + \Lambda_{z'} = \varphi$

$\therefore \quad (E, \varphi) = \left(E_{z'}, \dfrac{cz'+d}{N} + \Lambda_{z'}\right) \xleftarrow[\sim]{\cdot\alpha} \left(E_z, \frac{1}{N} + \Lambda_z\right)$

and so $\quad [E, \varphi] = \left[E_z, \frac{1}{N} + \Lambda_z\right]. \quad \therefore \exists$ map $\mathcal{H} \to S_1(N)$

→ Now say $\quad \Gamma_1(N) z = \Gamma_1(N) z', \quad$ so $\quad z = \gamma z'$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$

well defined? $\quad$ Again let $\quad \alpha = cz'+d. \quad \quad c \equiv 0\ (N),\ d \equiv 1\ (N)$

As above: $\quad$ • $\alpha \Lambda_z = \Lambda_{z'}$

• $\alpha\left(\frac{1}{N} + \Lambda_z\right) = \dfrac{cz'+d}{N} + \Lambda_{z'} = \frac{1}{N} + \Lambda_{z'}$

$\therefore \quad \left(\mathbb{C}/\Lambda_z, \frac{1}{N} + \Lambda_z\right) \xrightarrow[\sim]{\cdot\alpha} \left(\mathbb{C}/\Lambda_{z'}, \frac{1}{N} + \Lambda_{z'}\right)$

and $\quad \left[E_z, \frac{1}{N} + \Lambda_z\right] = \left[E_{z'}, \frac{1}{N} + \Lambda_{z'}\right]$

$\therefore \quad \exists$ map $\Gamma_1(N)\backslash\mathcal{H} \twoheadrightarrow S_1(N)$

→ Finally if $\left[\mathbb{C}/\Lambda_z, \frac{1}{N} + \Lambda_z\right] = \left[\mathbb{C}/\Lambda_{z'}, \frac{1}{N} + \Lambda_{z'}\right]$

inj? then $\exists\ \alpha$ s.t. $\left|\begin{array}{l} \alpha \Lambda_z = \Lambda_{z'} \\ \alpha\left(\frac{1}{N} + \Lambda_z\right) = \frac{1}{N} + \Lambda_{z'} \end{array}\right. \begin{array}{l} \Rightarrow \left|\begin{array}{l} \alpha z = az'+b \\ \alpha \cdot 1 = cz'+d \end{array}\right. \text{ w/ } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \\ \Rightarrow \frac{1}{N} + \Lambda_{z'} = \frac{cz'+d}{N} + \Lambda_{z'} \end{array}$

$\Rightarrow c \equiv 0\ (N),\ d \equiv 1\ (N)$

$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N). \quad \therefore \Gamma_1(N)\backslash\mathcal{H} \leftrightarrow S_1(N) \quad \blacksquare$