Talk 4. Modular Curves & Thm A

Yiannis Fam

Functor $F_{\Gamma_?(N)} : \mathrm{Sch}/\mathbb{Z}[1/N] \to \mathrm{Set}$

$S \mapsto \{\text{EC } E/S \text{ w/ level } \Gamma_?(N)\}$

- $\Gamma(N) : (\mathbb{Z}/N\mathbb{Z})^2_S \xrightarrow{\sim} E[N]$
- $\Gamma_1(N) :$ $P \in E(S)[N]$ order N
- $\Gamma_0(N) : (\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow E[N]$

To be representable means $\exists\ Y_?(N) \to \operatorname{Spec}\mathbb{Z}[1/N]$ w/

$Y_?(N)(S) = \{\text{EC w/ level } \Gamma_?(N)\}$.

Taking $S = Y_?(N) \rightsquigarrow \mathcal{E} \to Y_?(N)$ (univ.) w/ univ. level str. e.g. $Y(N)$ (w.r.t. $\Gamma(N)$)

$$\begin{tikzcd} E \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathcal{E}(N) \arrow[d] \\ S \arrow[r] & Y(N) \end{tikzcd}$$

Facts: 1) For $N \geq 3$, $F_{\Gamma(N)}$ & $F_{\Gamma_1(N)}$ are rep. by a sm. aff. sch. $/\mathbb{Z}[1/N]$ called $Y(N)$, $Y_1(N)$, resp.

2) $F_{\Gamma_0(N)}$ rep. by a sm. DM stack $Y_0(N)/\mathbb{Z}[1/N]$, but <u>NOT</u> by a sch. bc. e.g. $[-1]$ is an automorphism. of order N

3) Can def. $Y_0(N)$ over $\mathbb{Z}$ (by replacing $\mathbb{Z}/N\mathbb{Z}$ w/ a $\underbrace{\text{fin. flat gp sch.}}_{\text{"FFGS"}}$)

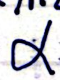
Compactify $Y_0(N) \rightsquigarrow X_0(N)$ since $Y_0(N)$ is not proper.

Def: A <u>gen. ell. curve</u> E/S is a proper flat sch. s.t.

1) E^{sm} has a gp sch str.

2) Fibres are ell. curves are <u>n-gons</u> 

Def: An n-gon is $C_n := \mathbb{P}^1_k \times \mathbb{Z}/n\mathbb{Z} / \sim$ where $(\infty, i) \sim (0, i+1)$

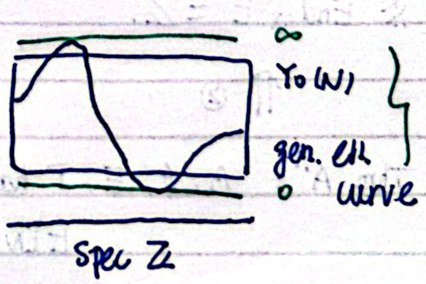
e.g. a 1-gon is a nodal curve  ; in gen. $C_n^{sm} = \mathbb{G}_m \times \mathbb{Z}/n\mathbb{Z}$

e.g. C_N has 2 level N-strs $\mu_N \leq \mathbb{G}_m$, $\mathbb{Z}/N\mathbb{Z}$

Add 2 pts (N prime):

- $\infty := (C_1, \mu_N)$
- $0 := (C_N, \mathbb{Z}/N\mathbb{Z})$

In every fiber $/\mathbb{Z}$



e.g. $E/\mathbb{Q}$ everywhere semi-stab. redn. ; $\mathcal{E}_{reg}/\mathbb{Z}$ min. reg. model is a GEC because

- $\mathcal{E}_{reg}^{sm} = \mathcal{E}_{Nér}$ is a gp. sch.
- fibers are EC at good redn (or generic fiber.)
  are n-gon at multn. redn.

Thm A: $N > 7$ prime. Suppose $\exists$ ab var $A/\mathbb{Q}$ & $f: X_0(N) \to A$ s.t.

1) A has good redn away from N
2) $A(\mathbb{Q})$ rk 0
3) $f(0) \neq f(\infty)$

Then $\nexists$ EC$/\mathbb{Q}$ w/ $\mathbb{Q}$-pt of order N.

$\Uparrow$ ①

Thm A' A, f as above. Suppose $E/\mathbb{Q}$ w/ rat'l pt P of order N. Then

$$E[N] \simeq \underset{\langle P \rangle}{\mathbb{Z}/N\mathbb{Z}} \oplus \mu_N$$

① Weil pairing $\langle\, ,\, \rangle : E[N] \times E[N] \to \mu_N \rightsquigarrow \langle P, - \rangle : E[N] \to \mu_N$
$\Rightarrow \exists$ SES

has fin. fibers
$$0 \to \mathbb{Z}/N\mathbb{Z} \to E[N] \to \mu_N \to 0.$$

2) f is non-const. $X_0(N) \to A$ + $A(\mathbb{Q})$ fin. $\Rightarrow X_0(N)(\mathbb{Q})$ fin.

3) $\forall E/\mathbb{Q}$, $\mathrm{End}_{\mathbb{Q}} E = \mathbb{Z}$ (for CM ell. curves, their extra end. not def. over $\mathbb{Q}$)
  ($\mathrm{End}_{\mathbb{Q}} E \to \mathrm{End}_{\mathbb{Q}}(T_0 E) = \mathbb{Q}$)

Proof of ①: Suppose $P_1 \in E_1[N](\mathbb{Q})$. by A' $\Rightarrow E_1[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$
$\Rightarrow$ set $E_2 = E_1/\mu_N$, $P_2 = P_1$ mod μ_N $\Rightarrow \exists$ inf. chain

$$\begin{array}{ccccccc} E_1 & \to & E_2 & \to & E_3 & \to & \cdots \\ \Downarrow & & \Downarrow & & \Downarrow & & \\ P_1 & \mapsto & P_2 & \mapsto & P_3 & & \end{array}$$

$X_0(N)(\mathbb{Q})$ fin. $\Rightarrow \exists\, i < j$ s.t. $(E_i, P_i) \simeq (E_j, P_j) \simeq (E, P)$. Now, $E_i \to E_j$ is an endomorphism of E of deg N^{j-i} not killing P but $\divideontimes$ $\mathrm{End}_{\mathbb{Q}} E = \mathbb{Z}$. $\square$

$\Uparrow$ ②

Thm A'': A, f, E, P has above. p prime of bad redn for E. Then

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N / \mathbb{Q}_p.$$

②

② : $\rho: G_{\mathbb{Q}} \to GL_2(\mathbb{F}_N)$ action on $E[N]$. From the SES,

$$\rho = \begin{pmatrix} 1 & f_0 \\ & \chi_N \end{pmatrix}$$

where f_0 is a 1-cocycle $G_{\mathbb{Q}} \to \mathbb{F}_N$.

Let $K = \mathbb{Q}(\mu_N)$, then $\rho|_K = \begin{pmatrix} 1 & f \\ & 1 \end{pmatrix}$ w/ $f \in \mathrm{Hom}(G_K, \mathbb{F}_N)$. WTS: $f = 0$.

PNP: Given Thm A'', $\rho|_K$ is everywhere unr.

Pf: i) $p \neq N$ of good redn ✓ by NOS

ii) p bad redn. by A'' ✓

iii) $p = N$ good redn. $\mathcal{E}$ = Néron model $/ \mathbb{Z}_p$ $E[N] = \mathcal{E}[N] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$

$$0 \to \mathbb{Z}/N\mathbb{Z} \to \mathcal{E}[N] \to \mu_N \to 0$$

FFGS

(which goes the opposite direction)

conn-ét seq. $\Rightarrow \mathcal{E}[N] = \mu_N \oplus \mathbb{Z}/N\mathbb{Z} \Rightarrow$ so is $E[N]$ □.

$\Rightarrow f$ factors through the Hilbert cls field of K.

$\Rightarrow f \in \mathrm{Hom}(Cl(K), \mathbb{F}_N)$

Under $Gal(K/\mathbb{Q}) \curvearrowright Cl(K)$, $f^\sigma = \chi(\sigma) f$

Herbrand's thm. $\Rightarrow f = 0$. $\Rightarrow f$ factors through the fin gp $Gal(K/\mathbb{Q})$.

Now, since $[K:\mathbb{Q}] = N-1$ coprime to N. ρ is semisimple. $\Rightarrow$ ✓

Recall:

- R a DVR. A ab var. $/ Frac(R)$, then $\exists$ Néron model $\mathcal{A}/R$ sm gp sch. NMP $\Rightarrow \mathcal{A}(R) \leftrightarrow A(Frac(R))$
- Do the same w/ Dedekind domains
- $E/\mathbb{Q}$ $P \in E(\mathbb{Q})[N]$. $\mathcal{E}/\mathbb{Z}$ Néron model

NOTN P exists ~~iff~~ & $P \in \mathcal{E}(\mathbb{Z})$

E has add redn if $\mathcal{E}^0_{\mathbb{F}_p} = G_{a,\mathbb{F}_p}$

multi. $G_{m,\mathbb{F}_p}$

- Consequence of ~~the~~ Raynaud's thm: $K/\mathbb{Q}_p$ $e < p-1$. G FFGS $/\mathcal{O}_K$.

$$G(\mathcal{O}_K) \hookrightarrow G(K)$$

Cor: A/K ab var. w/ good redn (w/ $(N,p)=1$)

$$A[N](\mathcal{O}_K) \hookrightarrow A[N](K).$$

Proof of Thm A''

- Step 1. Show E has everywhere semi-stab redn.

Néron models)

• $p \neq N$. Suppose $\mathcal{E}^\circ_{\mathbb{F}_p} = \mathbb{G}_a$ $\quad \# \, \mathcal{E}/\mathcal{E}^\circ \leq 4$ (clsn for special fibers of

Fact: $\mathcal{E}_{\mathbb{F}_p}$ has ≤ 4 components $\Rightarrow P_{\mathbb{F}_p} \in \mathcal{E}^\circ_{\mathbb{F}_p}(\mathbb{F}_p) = \mathbb{F}_p \Rightarrow P_{\mathbb{F}_p} = 0$

$(N, p) = 1 \Rightarrow \mathcal{E}[N](\mathbb{Z}) \hookrightarrow \mathcal{E}[N](\mathbb{F}_p)$ ※

• $p = N$. Suppose $\mathcal{E}^\circ_{\mathbb{F}_p} = \mathbb{G}_a$

Fact: $\exists \, K / \mathbb{Q}_p$ deg ≤ 6 s.t. E/K has semi-stab redn. at p. $\mathcal{E}' / \mathcal{O}_K$ Néron

$\mathcal{E}^\circ_k = \mathbb{G}_{a,k}$; $\mathcal{E}'^\circ_k$ = ell. curve / torus

NMP: $f: \mathcal{E}_{\mathcal{O}_K} \to \mathcal{E}' \rightsquigarrow \bar{f}: \mathcal{E}_k \to \mathcal{E}'_k$ $\bar{f}$ is triv. on $\mathcal{E}^\circ_k$. Now

the arguement that $P_{\mathbb{F}_p} \in \mathcal{E}^\circ_{\mathbb{F}_p}$ works when $p = N$ as well

$f(P)$ is the pt. extending $f(P)$)

$$\begin{array}{ccccc} P & \mathcal{E}_{\mathcal{O}_K} & \to & \mathcal{E}' & f(P) \\ \updownarrow & \downarrow & & \downarrow & \updownarrow \\ P_k \in & \mathcal{E}^\circ_k & \to & \mathcal{E}'^\circ_k & 0 \end{array}$$

since $\nexists$ non-const maps from $\mathbb{G}_a$ to ell. cur. or torus

$\Rightarrow \mathcal{E}'[N](\mathcal{O}_K) \to \mathcal{E}'[N](k)$, not $\hookrightarrow$ inj. ※. □

Lem: E has bad (mult.) redn at $p = 2, 3$.

Pf: If not, Hasse bd. $\# \mathcal{E}(\mathbb{F}_p) \leq 7.5$ but $N > 7$. □

(hence mult.)

Step 2. p prime bad redn. $P_{\mathbb{F}_p} \notin \mathcal{E}^\circ_{\mathbb{F}_p}(\mathbb{F}_p)$

Pf: $\# \mathcal{E}^\circ_{\mathbb{F}_p}(\mathbb{F}_p) = p-1$ or $p+1$ (split or non-split torus)

• $p = 2, 3$ $\quad p+1 < N$ ✓

• $p = N$ $\quad (p, p-1) = 1$, $(p, p+1) = 1$ ✓

By Step 1, $x = (\exists \, \mathcal{E}, \mathbb{Z}/N\mathbb{Z} = \langle P \rangle) \in X_0(N)(\mathbb{Z})$:

$0 = (C_N, \mathbb{Z}/N\mathbb{Z})$

$\infty = (C_1, \mu_N)$

Else, $p \neq 2, 3, N$. Néron model $A / \mathbb{Z}$

$$\begin{array}{ccc} A(\mathbb{Z})_{tors} & \hookrightarrow & A(\mathbb{Z}_p)_{tors} \\ \| & & \wr\!\| \\ A(\mathbb{Z}) & \hookrightarrow & A(\mathbb{F}_p) \end{array}$$

FFGS / $\mathbb{Z}_p$ becase A has good redn. away from N

E has mult red at 3. $P_{\mathbb{F}_3} \notin \mathcal{E}^\circ_{\mathbb{F}_3} \Rightarrow$ x & 0 red to the same pt in $X_0(N)(\mathbb{F}_3) \Rightarrow f(x), f(0) \in A(\mathbb{Z})$ red to the same pt of $A(\mathbb{F}_3) \overset{\text{Inj}}{\Rightarrow}$ $f(x) = f(0)$.

because they have the same moduli interpretation.

If $P_{\mathbb{F}_p} \in \mathcal{E}^\circ_{\mathbb{F}_p}$, then x & ∞ red to the same pt. of $X_0(N)(\mathbb{F}_p)$. $\Rightarrow$ $f(x) = f(\infty)$ ※ $f(0) \neq f(\infty)$. □

Cor: p bad redn. $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N / \mathbb{Q}_p$.

Pf: $\mathcal{E}^\circ_{\mathbb{F}_p} = \mathbb{G}_m$ has N-torsion $\mu_N \Rightarrow \mathcal{E}^\circ_{\mathbb{Z}_p}[N] \neq 0$ (order $\geq N$) but this doesn't intersect $\langle P \rangle = \mathbb{Z}/N\mathbb{Z} \Rightarrow E_{\mathbb{Q}_p}[N] = \mathcal{E}^\circ_{\mathbb{Z}_p}[N] \oplus \mathbb{Z}/N\mathbb{Z}$
$\Rightarrow E_{\mathbb{Q}_p}[N] = \mu_N \oplus \mathbb{Z}/N\mathbb{Z}$. $\square$