Counting Points on Shimura Varieties
Lecture 3

Yihang Zhu, Aug 13

<u>Last time</u> $(G,X) = (GL_2, \mathcal{H}^{\pm})$. $K = K^p K_p$, $K_p = GL_2(\mathbb{Z}_p)$,

K^p is "small enough" (neat).

For us, require $\exists N \geq 3$, s.t. $p \nmid N$,

$$K^p \subset \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\hat{\mathbb{Z}}^p) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv 1 \bmod N \right\}.$$

<u>Formula</u> $$\# S_K(\mathbb{F}_{p^n}) = \sum_{(\gamma_0, \delta)} c_1(\gamma_0, \delta) \cdot O_\gamma(1_{K^p}) \cdot TO_\delta(f_n).$$

where · γ_0 : <u>$\mathbb{R}$-elliptic</u> elt of $G(\mathbb{Q})$ up to conj.

$\Leftrightarrow$ either central, or char poly is irred. $/\mathbb{R}$.

· $\delta \in G(\mathbb{Q}_{p^n})$ up to σ-conjugacy s.t.

$$\delta \cdot \sigma(\delta) \cdots \sigma^{n-1}(\delta) \underset{\text{conj.}}{\sim} \gamma_0$$

· $$O_\gamma(1_{K^p}) = \int_{G_{\gamma_0}(\mathbb{A}_f^p) \backslash G(\mathbb{A}_f^p)} 1_{K^p}(x^{-1}\gamma_0 x)\, dx$$

· $$TO_\delta(f_n) = \int_{G(\mathbb{Q}_{p^n})_{\delta\sigma} \backslash G(\mathbb{Q}_{p^n})} f_n(x^{-1}\delta\sigma(x))\, dx$$

with f_n = char func'n of $G(\mathbb{Z}_{p^n}) \begin{pmatrix} p & \\ & 1 \end{pmatrix} G(\mathbb{Z}_{p^n})$

· $G(\mathbb{Q}_{p^n})_{\delta\sigma}$ = $\mathbb{Q}_p$-points of the reductive gp $J_{n,\delta}/\mathbb{Q}_p$

$\forall \mathbb{Q}_p$-alg. R, $J_{n,\delta}(R) = \{ g \in G(\mathbb{Q}_{p^n} \otimes_{\mathbb{Q}_p} R) \mid g^{-1}\delta\sigma(g) = \delta \}$

$J_{n,\delta}$ is an inner form of G_{γ_0}.

· $c_1(\gamma_0, \delta) = \mathrm{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f))$

with I = the inner form of G_{γ_0} $/\mathbb{Q}$.

s.t. $I_{\mathbb{R}}$ is cpt mod Z_G;

$I_{\mathbb{Q}_\ell} \cong G_{\gamma_0}$, $\forall \ell \neq p$; $I_{\mathbb{Q}_p} \cong J_{n,\delta}$.

§1 Key lemma

Lemma $\gamma_0 \in GL_2(\mathbb{Q}_p)$ semi-simple. $\delta \in GL_2(\mathbb{Q}_{p^n})$

s.t. $\delta \cdot \sigma(\delta) \cdots \sigma^{n-1}(\delta) \sim \gamma_0$.

Then the σ-conj. class of δ is uniquely det'd by γ_0.

pf. Fact 1 G red. $/\mathbb{Q}_p$ s.t. G_{der} is simply conn.

Suppose $\delta \cdot \sigma(\delta) \cdots \sigma^{n-1}(\delta) \overset{\overline{\mathbb{Q}_p}}{\sim} \gamma_0 \in G(\mathbb{Q}_p)$ conj. $/\overline{\mathbb{Q}_p}$.

In this case, $J_{n,\delta}$ is an inner form of G_{γ_0}.

Fact 2 $\{\delta' \in G(\mathbb{Q}_{p^n}) \mid \delta' \cdot \sigma(\delta) \cdots \sigma^{n-1}(\delta) \sim \gamma_0\} / \sigma$-conj.

basically $J_{n,\delta} \subset \mathrm{Res}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p} G$.

$\longleftrightarrow \ker(H^1(\mathbb{Q}_p, J_{n,\delta}) \longrightarrow H^1(\mathbb{Q}_p, \mathrm{Res}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p} G))$

For $G = GL_2$, we show: $H^1(\mathbb{Q}_p, J_{n,\delta}) = \{0\}$.

δ, δ' both satisfy ...

$\Rightarrow \exists g \in \mathrm{Res}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p} G(\overline{\mathbb{Q}_p})$ s.t. $g \delta \theta(g)^{-1} = \delta'$,

$\theta \in \mathrm{Aut}(\mathrm{Res}\, G)$

Fact 3 F: non-archimedean field (char 0).

J: red gp$/F$. J': red gp$/F$, inner form of J.

then $\boxed{H^1(F, J) \cong H^1(F, J')}$ a deep theorem!

Back to $G = GL_2$. $H^1(\mathbb{Q}_p, J_{n,\delta}) = H^1(\mathbb{Q}_p, G_{\gamma_0})$, $\gamma_0 \in G(\mathbb{Q}_p)$ ss.

$$G_{\gamma_0} = \begin{cases} G, & \text{if } \gamma_0 \text{ is central} \\ \mathrm{Res}_{F/\mathbb{Q}_p} \mathbb{G}_m, & \text{where } F \text{ is the quad ext'n of } \mathbb{Q}_p \text{ generated by the eigenvalues of } \gamma_0. \\ & \text{if } \gamma_0 \text{ is non-central \& char poly is irred } /\mathbb{Q}_p. \\ \mathbb{G}_m \times \mathbb{G}_m, & \text{if char poly of } \gamma_0 \text{ has two distict roots } /\mathbb{Q}_p. \end{cases}$$

$*$ $H^1(\mathbb{Q}_p, J_{n,\delta}) = H^1(\mathbb{Q}_p, G_{\gamma_0}) = \{0\}$

by Hilbert 90 + Shapiro's Lemma.

Last time, we did a rough classification of γ_0 : $\boxed{\det \gamma_0 = p^n}$.

Correction 1) central case: γ_0 is central

$\Rightarrow$ n must be even,

$$\gamma_0 = \begin{pmatrix} p^{\frac{n}{2}} & \\ & p^{\frac{n}{2}} \end{pmatrix} \text{ or } \begin{pmatrix} -p^{\frac{n}{2}} & \\ & -p^{\frac{n}{2}} \end{pmatrix}.$$

$I = D^\times$, D = quaternion alg. ram'd at p & ∞.

2) non-central case: γ_0 is non-central

$\Rightarrow$ $F = \mathbb{Q}(\text{eigenvalues of } \gamma_0)$ = imag. quad. / $\mathbb{Q}$.

$G_{\gamma_0} \cong \mathrm{Res}_{F/\mathbb{Q}} \mathbb{G}_m \longrightarrow GL_2$. $I \cong G_{\gamma_0}$.

Rmk * supersingular $\Leftrightarrow$ some power of γ_0 is central

* ordinary $\Leftrightarrow$ none of the powers of γ_0 is central.

E.g. $p=3$, $n=1$. $\gamma_0 = \begin{pmatrix} \sqrt{-3} & \\ & -\sqrt{-3} \end{pmatrix}$ non-central

$\gamma_0^2 = \begin{pmatrix} -3 & \\ & -3 \end{pmatrix}$ central

§2 General way of computing (twisted) orbital integrals

Twisted case G red gp/$\mathbb{Q}_p$, $n \geq 1$, $\delta \in G(\mathbb{Q}_{p^n})$

Assumptions (i) $J_{n,\delta}$ is red.

(ii) the G-conj. class of δ in $G(\mathbb{Q}_{p^n})$ is a closed subset.

(iii) Fix Haar measures on $G(\mathbb{Q}_{p^n})$ & $J_{n,\delta}(\mathbb{Q}_p)$

(iv) $f \in \mathcal{C}_c^\infty(G(\mathbb{Q}_{p^n}))$

$$\rightsquigarrow TO_\delta(f) = \int_{J_{n,\delta}(\mathbb{Q}_p)\backslash G(\mathbb{Q}_{p^n})} f(x^{-1}\delta\sigma(x))\,dx$$

Fix a sufficiently small cpt open subgp $K \subset G(\mathbb{Q}_{p^n})$ s.t.

f is K-bi-invariant & K is σ-invariant.

$$\Rightarrow \boxed{TO_\delta(f) = \sum_{\underbrace{x \in J_{n,\delta}(\mathbb{Q}_p)\backslash G(\mathbb{Q}_{p^n})/K}_{\text{finite}}} f(x^{-1}\delta\sigma(x)) \cdot \frac{\mathrm{vol}_G(K)}{\mathrm{vol}_{J_{n,\delta}}(xKx^{-1} \cap J_{n,\delta}(\mathbb{Q}_p))}}$$

Pf. of $\#\mathcal{S}_K(\mathbb{F}_{p^n}) = \sum_{(\gamma_0,\delta)} c(\gamma_0,\delta)\, O_{\gamma_0}(1_{K^p})\, TO_\delta(f_n)$.

<u>Recall</u> $q=p^n$, $\mathcal{S}_K(\mathbb{F}_{p^n}) = \left\{ (E,\eta) \;\middle|\; \begin{array}{l} E \text{ ell curve}/\mathbb{F}_q, \\ \eta \text{ a } \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\text{-stable} \\ K^p\text{-orbit of isoms} \\ \hat{\mathbb{Z}}^p \oplus \hat{\mathbb{Z}}^p \xrightarrow{\sim} T^p(E_{\overline{\mathbb{F}}_q}) \end{array} \right\}$

$K^p \circlearrowright \hat{\mathbb{Z}}^p \oplus \hat{\mathbb{Z}}^p$, $\quad T^p(E_{\overline{\mathbb{F}}_q}) \circlearrowleft \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

<u>Idea</u> $E/\mathbb{F}_q \rightsquigarrow (\gamma_0,\delta)$

Given E, for any $\ell\neq p$, $T_\ell(E) \circlearrowleft \pi\in \mathrm{End}(E)$ q-Frobenius endo.

If we choose a $\boxed{\text{basis}}$

$$\pi \longleftrightarrow \gamma_\ell \in GL_2(\mathbb{Q}_\ell)$$

$\rightsquigarrow$ <u>Fact</u> char poly of γ_ℓ is def'd $/\mathbb{Z}$, and indep. of ℓ.

i.e. $\mathbb{Q}(\pi) \subset \mathrm{End}(E)\otimes_{\mathbb{Z}}\mathbb{Q}$

field $\qquad$ $\min(\pi:\mathbb{Q}) = $ char poly of γ_ℓ, $\forall \ell$

Define $\gamma_0\in G(\mathbb{Q})$ whose min poly is $\min(\pi:\mathbb{Q})$ (up to conj.)

$\Rightarrow \gamma_0\sim\gamma_\ell$, $\forall\ell$.

<u>Observation</u> γ_0 is $\mathbb{R}$-elliptic i.e. either central or char poly is irred. $/\mathbb{R}$.

b/c char poly $= T^2 - \mathrm{Tr}(\gamma_0)\cdot T + \det(\gamma_0)$

From general facts : $\mathrm{Tr}(\gamma_0) = q+1-\#E(\mathbb{F}_q)$.

$\det(\gamma_0) = q$.

either Irred. $/\mathbb{R}$ $\qquad$ $\boxed{\mathrm{Tr}(\gamma_0)^2 \le 4\cdot\det(\gamma_0)}$

or $(T\pm\sqrt{q})^2$, $\sqrt{q}\in\mathbb{Q}$ $\quad\Leftrightarrow\quad$ Hasse's bound.

$|q+1-\#E(\mathbb{F}_q)| \le 2\sqrt{q}$. okay!

Construct δ: $M_0 = M_0(E) = $ Dieudonné module of $E[p^\infty]$.

Recall this is a free $\mathbb{Z}_q$-module of rk 2

together with σ-lin. $F: M_0 \longrightarrow M_0$

i.e. $F(a \cdot x) = \sigma(a) \cdot F(x)$, $\forall a \in \mathbb{Z}_q$, $x \in M_0$.

& σ^{-1}-linear $V: M_0 \longrightarrow M_0$

s.t. $FV = VF = p$.

Choose a basis of M_0. F becomes $\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \sigma(x) \\ \sigma(y) \end{pmatrix}$

for some fixed $\delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_q)$

Note: V can be reconstructed from F

& the condition that $M_0 \supset F(M_0) \supset p \cdot M_0$

$\rightsquigarrow$ δ is well-def'd up to σ-conjugacy.

Moreover, $\delta \cdot \sigma(\delta) \cdots \sigma^{n-1}(\delta) \sim \gamma_0$ holds!

Rmk $\delta \notin GL_2(\mathbb{Z}_q)$ but $\delta \in GL_2(\mathbb{Z}_q) \begin{pmatrix} p & \\ & 1 \end{pmatrix} GL_2(\mathbb{Z}_q)$!

(This corresponds to $F(M_0)/p \cdot M_0$ is an $\mathbb{F}_q$-vector space of dim 1).

* We say that M_0 is a Diendonné module of height 2, dim 1.

Summary $E/\mathbb{F}_q \rightsquigarrow (\gamma_0, \delta)$ up to conj. & σ-conj.

$$\# S_K(\mathbb{F}_q) = \sum_{(\gamma_0, \delta)} N(\gamma_0, \delta)$$

$$N(\gamma_0, \delta) = \# \{ (E, \eta) \mid E \longmapsto (\gamma_0, \delta) \}.$$

Step 1 Suppose $N(\gamma_0, \delta) \neq 0$. To prove

$$N(\gamma_0, \delta) = C_1(\gamma_0, \delta) \cdot O_{\gamma_0}(1_{K^p}) \, TO_\delta(f_n).$$

Step 2 If (γ_0, δ) is s.t. $O_{\gamma_0}(1_{K^p}) \, TO_\delta(f_n) \neq 0$,

then γ_0 comes from some $E/\mathbb{F}_q$.

§3 Proof of Step 1

Step 1 Take $E_0/\mathbb{F}_q \rightsquigarrow (\gamma_0, \delta)$.

Thm (Honda–Tate)

If $E/\mathbb{F}_q \longmapsto (\gamma_0, \delta)$, then $E \sim E_0$. quasi-isog.

The converse is also true.

$N(\gamma_0,\delta) = \{(E,\eta) \mid E \sim E_0 \text{ quasi-isog.}\}$

$Y := \{(E,\eta,\iota) \mid \iota \text{ is a quasi-isog.}$

Define algebraic subgp I_{E_0} $/\mathbb{Q}$:

$\forall\, \mathbb{Q}\text{-alg. } R,\ I_{E_0}(R) = (\mathrm{End}_{\mathbb{F}_q}(E_0) \otimes_{\mathbb{Z}} R)^\times$ (red. $/\mathbb{Q}$).

E.g. $I_{E_0}(\mathbb{Q}) = \{\text{self-quasi-isog. of } E_0\}$

$|N(\gamma_0,\delta)| = |I_{E_0}(\mathbb{Q}) \backslash Y|$

$$Y^p = \left\{ \begin{array}{c} \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\text{-stable } K^p\text{-orbits of embeddings} \\ (\hat{\mathbb{Z}}^p)^{\oplus 2} \hookrightarrow \underbrace{T^p(E_0)\otimes_{\mathbb{Z}}\mathbb{Q}}_{\text{non-canonically } (\mathbb{A}_f^p)^{\oplus 2}} \end{array} \right\}$$

K^p

image $\neq T^p(E_0)$.

Frob. endo

$$= \left\{ \begin{array}{c} \pi\text{-stable } K^p\text{-orbits of embeddings} \\ (\hat{\mathbb{Z}}^p)^{\oplus 2} \hookrightarrow T^p(E_0)\otimes_{\mathbb{Z}}\mathbb{Q} \end{array} \right\}$$

after choosing a basis on $T^p(E_0)$

$$= \left\{ \begin{array}{c} \gamma_\ell\text{-stable } K^p\text{-orbits of embeddings} \\ (\hat{\mathbb{Z}}^p)^{\oplus 2} \hookrightarrow (\mathbb{A}_f^p)^{\oplus 2} \end{array} \right\}$$

given by some $g \in GL_2(\mathbb{A}_f^p)$ up to right mult'n by K^p.

$= \{ g \in GL_2(\mathbb{A}_f^p)/K^p \mid g^{-1}\gamma_\ell g \in K^p \}$

$\mathbb{Q}_q$-v.s.

(Λ, F) is a Dieudonné mod of ht 2 & dim 1.

$$Y_p = \left\{ \begin{array}{l} \mathbb{Z}_q\text{-lattices } \Lambda \subset M_0(E_0)[\tfrac{1}{p}] \text{ s.t. } \boxed{p\Lambda \subset F\Lambda \subset \Lambda} \\ \quad \& \ F : M_0(E_0)[\tfrac{1}{p}] \longrightarrow M_0(E_0)[\tfrac{1}{p}] \text{ induced by } F \text{ on } M_0(E_0) \end{array} \right\}$$

choose basis

$$\begin{aligned}
&\quad g\cdot \mathbb{Z}_q^{\oplus 2}\\
&\quad\;\, \|\\
&= \{ \mathbb{Z}_q\text{-lattices } \Lambda \subset \mathbb{Q}_q^{\oplus 2} \mid p\Lambda \subset \delta\cdot\Lambda \subset \Lambda \}\\
&= \{ g \in GL_2(\mathbb{Q}_q)/GL_2(\mathbb{Z}_q) \mid g^{-1}\delta\,\sigma(g) \in G(\mathbb{Z}_q)\begin{pmatrix} p & \\ & 1\end{pmatrix} G(\mathbb{Z}_q) \}
\end{aligned}$$

$$\begin{array}{ccc}
Y & \longrightarrow & Y^p \times Y_p \\
\| & & \\
\{(E,\eta,\iota)\} & & (E,\eta,\iota)
\end{array}$$

looking at $\iota : E \longrightarrow E_0$ quasi-isog.

$\rightsquigarrow$

$$\begin{tikzcd}
 & T^p(E)_{\mathbb{Q}} \arrow[r, "\iota"] & T^p(E_0)_{\mathbb{Q}} \\
(\hat{\mathbb{Z}}^p)^{\oplus 2} \arrow[ur, "\eta"] \arrow[urr] & &
\end{tikzcd}$$

an elt of Y^p.

Also looking at

$$\begin{array}{ccc}
M_0(E)[\tfrac{1}{p}] & \xrightarrow{\ \iota\ } & M_0(E_0)[\tfrac{1}{p}] \\
\circlearrowleft & & \circlearrowleft \\
F & & F
\end{array}$$

$\iota(M_0(E)) \subset M_0(E_0)[\frac{1}{p}]$ is a lattice Λ s.t. $p\Lambda \subset F\Lambda \subset \Lambda$.

$\rightsquigarrow$ an elt. of Y_p.

Big Theorem (Tate's isogeny theorem).

$$Y \ (= \{(E,\eta,\iota)\}) \xrightarrow{\ \sim\ } Y^p \times Y_p.$$

Moreover, $I_{E_0}(\mathbb{Q}) \circlearrowright Y$ will correspond to an autom of $I_{E_0}(\mathbb{Q})$ on $Y^p \times Y_p$, given as follows:

$$I_{E_0}(\mathbb{Q}) \hookrightarrow I(\mathbb{A}_f) = G_{\gamma_0}(\mathbb{A}_f^p) \times J_{\eta,\delta}(\mathbb{Q}_p) \circlearrowright Y^p \times Y_p.$$

built from γ_0 & δ.

(Actually $I_{\mathbb{A}_f} \cong (I_{E_0})_{\mathbb{A}_f}$).

$$N(\gamma_0, S) = \# I_{E_0}(\mathbb{Q}) \backslash Y^p \times Y_p$$

$$\overset{\boxed{\text{Exc}}}{=} \boxed{\mathrm{vol}(I_{E_0}(\mathbb{Q}) \backslash I(\mathbb{A}_f))} \cdot O_{\gamma_0}(1_{K^p}) \cdot TO_S(f_n).$$

$$\| \quad \mathrm{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f))$$

<u>Subtlety</u> $I(\mathbb{Q}) \hookrightarrow I(\mathbb{A}_f)$

$I_{E_0}(\mathbb{Q}) \hookrightarrow I(\mathbb{A}_f)$ only agree up $I(\mathbb{A}_f)$-conj.

But that doesn't matter for computing vol!