Counting Points on Shimura Varieties
Lecture 4

Yihang Zhu, Aug 16

Some corrections

(1) Dieudonné mod M: finite free $\mathbb{Z}_q$-mod
with σ-linear F & σ^{-1}-linear V.

$FV = VF = p$ on M

existence of $V \Leftrightarrow pM \subset FM \subset M$.

When $\mathrm{rk}_{\mathbb{Z}_q} M = 2$, we also impose the following condition:

$\dim_{\mathbb{F}_q}(FM/pM) = 1$

0 or 1 or 2

We say M is "height 2 & dim 1".

Take a basis of M, $F \longleftrightarrow \delta\sigma$, $\delta \in GL_2(\mathbb{Q}_q)$

$pM \subset FM \subset M \Longleftrightarrow \delta \in GL_2(\mathbb{Z}_q)\begin{pmatrix} p^a & \\ & p^b \end{pmatrix} GL_2(\mathbb{Z}_q)$ for some $1 \geq a \geq b \geq 0$.

additional condition $\dim_{\mathbb{F}_q}(FM/pM) \Leftrightarrow (a,b) = (1,0)$.

In the def'n of Y_p: associated to some fixed $E_0/\mathbb{F}_q$,

$M_0 = M_0(E_0) \circlearrowleft F$

$Y_p := \{\mathbb{Z}_q\text{-lattices } \Lambda \subset M_0[\tfrac{1}{p}] \mid p\Lambda \subset \boxed{F\Lambda} \subset \Lambda \text{ \& } \dim_{\mathbb{F}_q}(F\Lambda/p\Lambda) = 1\}$

i.e. (Λ, F) is a D-mod of ht 2 & dim 1 itself.

$= \{\mathbb{Z}_q\text{-lattices } \Lambda \subset \mathbb{Q}_q^{\oplus 2} \mid p\Lambda \subset \boxed{\delta\cdot\sigma(\Lambda)} \subset \Lambda \text{ \& } \dim_{\mathbb{F}_q}(\delta\cdot\sigma(\Lambda)/p\Lambda) = 1\}$

choose basis of M_0

$\Lambda = g\cdot\mathbb{Z}_q^{\oplus 2}$, $g \in GL_2(\mathbb{Q}_q)/GL_2(\mathbb{Z}_q)$

$= \{g \in GL_2(\mathbb{Q}_q)/GL_2(\mathbb{Z}_q) \mid g^{-1}\cdot\delta\cdot\sigma(g) \in GL_2(\mathbb{Z}_q)\boxed{\begin{pmatrix} p & \\ & 1 \end{pmatrix}}GL_2(\mathbb{Z}_q)\}$

(2) $TO_\delta(f) = \sum_{x \in J_{n,\delta}(\mathbb{Q}_p)\backslash G(\mathbb{Q}_{p^n})/K} f(x^{-1}\delta\cdot\sigma(x)) \cdot \frac{\mathrm{vol}(\cdots)}{\mathrm{vol}(\cdots)}$

$J_{n,\delta}(\mathbb{Q}_p)\backslash G(\mathbb{Q}_{p^n})/K$ need NOT be finite.

But only finitely many x in this set satisfy

$f(x^{-1}\delta\sigma(x)) = 0$. K is sufficiently small σ-invariant cpt open subgp. of $G(\mathbb{Q}_{p^n})$ s.t. f is bi-invariant under K.

Point $\big(\underbrace{(\sigma\text{-conj. class of } x)}_{\text{an'n closed in } G(\mathbb{Q}_{p^n})} \cap \underbrace{\operatorname{supp} f}_{\text{cpt.}}\big)/\underbrace{K}_{\text{open}}$ is finite.

Last time $\#\mathcal{S}_K(\mathbb{F}_q) = \sum_{(\gamma_0,\delta)} c(\gamma_0,\delta)\cdot O_{\gamma_0}(1_{K^p})\cdot TO_\delta(f_n)$

If γ_0 comes from $E_0/\mathbb{F}_q$, then

$\#\{(E,\eta)\in \mathcal{S}_K(\mathbb{F}_q) \mid E \rightsquigarrow \gamma_0\} = c(\gamma_0,\delta)\cdot O_{\gamma_0}(1_{K^p})\cdot TO_\delta(f_n)$

Today If a pair (γ_0,δ) is s.t.

$O_{\gamma_0}(1_{K^p})\, TO_\delta(f_n) \neq 0$,

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

pf. ① We show: π is an eigenvalue of γ_0,

then π is a Weil q-number

i.e. an alg. integer π s.t. $\forall$ cplx embedding $\mathbb{Q}(\pi)\hookrightarrow\mathbb{C}$, the abs. val of π is $q^{1/2}$.

Recall $\det\gamma_0 = q$ (if $O_{\gamma_0}(1_{K^p})TO_\delta(f_n)\neq 0$)

$\Rightarrow \pi\cdot\bar{\pi} = q$.

Only need: π is an alg. integer.

Over $\mathbb{Q}_p$: $\gamma_0 \overset{\text{conj}}{\sim} \delta\cdot\sigma(\delta)\cdots\sigma^{n-1}(\delta)$

δ is σ-conj. to sth. in $GL_2(\mathbb{Z}_q)\begin{pmatrix} p & \\ & 1\end{pmatrix}GL_2(\mathbb{Z}_q)$

We may assume $\delta\in GL_2(\mathbb{Z}_q)\begin{pmatrix} p & \\ & 1\end{pmatrix}GL_2(\mathbb{Z}_q)$

i.e. $\delta\cdot\sigma(\delta)\cdots\sigma^{m-1}(\delta)\in M_2(\mathbb{Z}_q)$

$\Rightarrow \operatorname{tr}\gamma_0\in\mathbb{Z}_q\cap\mathbb{Q}$ i.e. p-adic val of $\operatorname{tr}\gamma_0\geq 0$.

<u>Similarly</u>: $\gamma_0 \overset{\text{conj.}}{\sim}$ sth. in K^p $(O_{\gamma_0}(1_{K^p})\neq 0)$

$\operatorname{tr}\gamma_0$ = trace of sth. in $K^p\subset GL_2(\hat{\mathbb{Z}}^{(p)})$

i.e. l-adic val of $\operatorname{tr}\gamma_0\geq 0$, $\forall l\neq p$.

$\Rightarrow \operatorname{tr}\gamma_0\in\mathbb{Z}$ $(\det\gamma_0=q)$

$\Rightarrow \pi$ is an alg. integer. $\square$

② <u>Hodge-Tate theory</u> If π is a Weil q-number,

then π comes from some <u>simple</u> abelian variety $A/\mathbb{F}_q$.

Need: $\dim A=1$. Moreover, A is uniquely determined by π

up to isogeny $/\mathbb{F}_q$.

In general, $\dim A$ can be computed from properties of π

(more precisely: if $\mathbb{Q}(\pi)=\mathbb{Q}$, then $\dim A=1$).

moreover, A is s.s. elliptic curve.

if not, $\dim A$ is def'd by val'n of π

at the place of $\mathbb{Q}(\pi)$ above p.

After some book keeping, we just need:

Suppose $\mathbb{Q}(\pi)\neq\mathbb{Q}$ i.e. $\mathbb{Q}(\pi)$ is an imag. quad. field

(b/c γ_0 is $\mathbb{R}$-elliptic).

We need: if p splits in $\mathbb{Q}(\pi)$,

then the two val'n v_1, v_2 of $\mathbb{Q}(\pi)$ above p

satisfy $v_1(\pi)=n$ & $v_2(\pi)=0$.

if p is inert or ramified in $\mathbb{Q}(\pi)$

then A is an elliptic curve (s.s.).

We ass. $\mathbb{Q}(\pi) \neq \mathbb{Q}$ & ass. p splits in $\mathbb{Q}(\pi)$.

<u>Def'n</u> F complete discrete valued field, γ s.s. $\in GL_n(F)$.

We say γ has a polar decomposition if $\gamma = \nu(p) \cdot k$

- ν cocharacter of GL_n/F, commuting with γ

  $\nu(p) \in GL_n(\overline{F})$

- $k \in GL_n(\overline{F})$ s.t. all eigenvalues of k have valuation 0.

<u>Fact</u> (Exercise)

If γ has a polar decomposition then it must be unique!

($\Rightarrow$ in this case, both $\nu(p)$ & $k \in GL_n(F)$).

<u>Fact</u> (non-trivial)

Suppose $\gamma \in GL_N(\mathbb{Q}_p)$ semi-simple s.t.

$\exists\, \delta \in GL_N(\mathbb{Q}_{p^n})$ s.t. $\gamma \sim \delta \cdot \sigma(\delta) \cdots \sigma^{n-1}(\delta)$.

<u>Then</u> $\exists\, t \geq 1$ s.t. over $F = \widehat{\mathbb{Q}_p^{ur}}$, γ^t has a polar decomposition

& the radical part is $\nu_\delta^{nt}(p)$.

Here ν_δ is the Newton cocharacter of δ.

<u>In our case</u> $TO_\delta(f_n) \neq 0 \Rightarrow \delta$ is σ-conj. to sth. in $GL_2(\mathbb{Z}_q)\begin{pmatrix} p & \\ & 1 \end{pmatrix} GL_2(\mathbb{Z}_q)$.

<u>Fact</u> In this case, ν_δ has only two choices up to conjugacy.

either $\nu_\delta : z \longmapsto \begin{pmatrix} z & \\ & 1 \end{pmatrix}$

or $z \longmapsto \begin{pmatrix} z^{1/2} & \\ & z^{1/2} \end{pmatrix}$

(In the second case, really just ν_δ^2 is well-def'd).

$\Rightarrow \exists t$, the radical part of γ_0^t is conjugate to

either $\begin{pmatrix} p^{nt} & \\ & 1 \end{pmatrix}$ or $\begin{pmatrix} p^{nt/2} & \\ & p^{nt/2} \end{pmatrix}$.

<u>Recall</u> We assume $\mathbb{Q}(\pi)$ splits $/p$

$\Rightarrow$ over $\mathbb{Q}_p$, γ_0 has two distinct eigenvalues λ_1, λ_2

So $\gamma_0 \underset{/\mathbb{Q}_p}{\sim} \begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix} \overset{\uparrow}{=} \underbrace{\begin{pmatrix} p^{v_p(\lambda_1)} & \\ & p^{v_p(\lambda_2)} \end{pmatrix}}_{=\nu(p)} \cdot \begin{pmatrix} k_1 & \\ & k_2 \end{pmatrix}$

polar decomp $\qquad$ $=\nu(p)$, $\nu: z \longmapsto \begin{pmatrix} z^{v_p(\lambda_1)} & \\ & z^{v_p(\lambda_2)} \end{pmatrix}$

is conjugate to $\begin{pmatrix} p^{v_p(\lambda_1)t} & \\ & p^{v_p(\lambda_2)t} \end{pmatrix}$

but is also conj. to $\begin{pmatrix} p^{nt} & \\ & 1 \end{pmatrix}$ or $\begin{pmatrix} p^{\frac{nt}{2}} & \\ & p^{\frac{nt}{2}} \end{pmatrix}$

<u>Case 1</u> $\begin{pmatrix} p^{v_p(\lambda_1)t} & \\ & p^{v_p(\lambda_2)t} \end{pmatrix} \sim \begin{pmatrix} p^{nt} & \\ & 1 \end{pmatrix}$

$\Rightarrow v_p(\lambda_1) = n, \; v_p(\lambda_2) = 0$

<u>Case 2</u> $\begin{pmatrix} p^{v_p(\lambda_1)t} & \\ & p^{v_p(\lambda_2)t} \end{pmatrix} \sim \begin{pmatrix} p^{\frac{nt}{2}} & \\ & p^{\frac{nt}{2}} \end{pmatrix}$

$\Rightarrow v_p(\lambda_1) = v_p(\lambda_2) = \frac{n}{2}$

$\Rightarrow$ n must be even (o/w p is ramified in $\mathbb{Q}(\pi)$)

<u>Moreover</u> $\frac{\lambda_1}{\lambda_2} \in \mathbb{Q}(\pi)$ has all val'ns 0

at v of $\mathbb{Q}(\pi)$ coprime to p, $N|\ell$,

$\gamma_0 \overset{\mathbb{Q}_\ell}{\sim}$ sth. $GL_2(\mathbb{Z}_q) \Rightarrow v(\lambda_1) = v(\lambda_2) = 0$

at $v|p$, $v(\lambda_1) = v(\lambda_2)$.

$\Rightarrow \lambda_1/\lambda_2 \in \mathcal{O}^\times_{\mathbb{Q}(\pi)} \Rightarrow$ $\boxed{\lambda_1/\lambda_2 \text{ is a root of unity.}}$

imag. quad.

Now we deduce a contradiction

$\Rightarrow \gamma_0^k$ is central (k even) since $\det \gamma_0 = q$.

$\Rightarrow \gamma_0^k = \begin{pmatrix} q^{k/2} & \\ & q^{k/2} \end{pmatrix} \Rightarrow \gamma_0 = \begin{pmatrix} \zeta\sqrt{q} & \\ & \zeta^{-1}\sqrt{q} \end{pmatrix}$, $\zeta = k$th root of unity.

If $k=1$, contradiction!

γ_0 is central $\Rightarrow \pi = q^{1/2} \in \mathbb{Q} \Rightarrow \mathbb{Q}(\pi)$ is not imag. quad.

So $k>1$.

$$\gamma_0 \sim \text{sth.} \in K^p \subset \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\hat{\mathbb{Z}}^{(p)}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv 1 \bmod N \right\}$$

for $\boxed{N \geq 3}$ & $p \nmid N$.

So we can take some prime power $\ell^i | N$, $\ell \neq p$

$\Rightarrow \gamma_0 \in G(\mathbb{Q}_p)$ is conj. to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_\ell) \;\&\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv 1 \bmod \ell^i.$$

$\Rightarrow \zeta\sqrt{q} \equiv \zeta^{-1}\sqrt{q} \bmod \ell^2$ (inside $\bar{\mathbb{Z}}_\ell$)

$\Rightarrow \zeta^2 \equiv 1 \bmod \ell^i$ i.e. $v_\ell(\zeta^2 - 1) \geq i$ ($\zeta^2 \in \bar{\mathbb{Q}}_\ell$)

Exercise Using $\ell^i \geq 3$ & $v_\ell(\zeta^2-1) \geq i \Rightarrow \zeta^2 = 1$

arbitrary root of unity.

$\Rightarrow \gamma_0$ is central, so $\mathbb{Q}(\pi) = \mathbb{Q}$, contradiction! $\square$

Rmk Abstractly, we used the following property called "neat".

K^p is "neat" $\Rightarrow \forall \gamma_0 \in G(\mathbb{Q}) \cap K^p$

then the equivalences of γ_0 cannot differ from each other by roots of unity.

i.e. the subgp they generate in $\bar{\mathbb{Q}}^\times$ is torsion free

Rmk From the pf: if some power of γ_0 is central, then γ_0 is central.

Actually: $\begin{cases} \text{non-central case} \\ \text{central case} \end{cases} \Leftrightarrow \begin{cases} \text{ordinary case} & \gamma_0 \leftrightsquigarrow \text{ordinary } E \\ \text{s.s. case} & \gamma_0 \leftrightsquigarrow \text{s.s. } E. \end{cases}$

Next time (1) Discuss some new features in the general formula that don't show up in GL_2.

(2) Informal introduction to the idea of TF, stabilization & how point counting formula is related to TF (after stabilization)

(3) The proof of point counting formula in the abelian-type case (rough).