Lecture 1: Kottiwtz-Langlands-Rapoport Conjecture

Haitao Zou

Contents

1 Review of Modular Curves

Let's start with the moduli interpretation of the modular curves, which is the initial example for our major goal of this seminar. Let $N \geq 3$ be an integer. Let $\mathcal{M}_0(N)$ be the moduli functor defined as

$$\begin{aligned} \mathrm{Sch}\,/\mathbb{Z}[\frac{1}{N}] &\to \mathrm{Sets} \\ T &\mapsto \{ \text{ all elliptic curves on } T \text{ together with an isomorphism} \\ &\quad \text{of étale finite group scheme } \alpha\colon E[N] \cong \underline{\mathbb{Z}/N\mathbb{Z}}^2 \} \end{aligned}$$

Here the isomorphism α is called a N-level structure of E.

Theorem 1.1. Under our assumption, the $\mathcal{M}_0(N)$ is representable by a quasi-projective scheme.

Proof. Consider the forgetful functor from $\mathcal{M}_0(N)$ the moduli functor of 1-pointed elliptic curves $\mathcal{M}_{1,1}$. Viewed as a morphism between stacks, the forgetful functor is finite étale, see [1, Theorem 3.7.1]. It is well-known that $\mathcal{M}_{1,1}$ is a Deligne-Mumford stack, hence so is $\mathcal{M}_0(N)$. To show that $\mathcal{M}_0(N)$ is representable by an $\mathbb{Z}[\frac{1}{N}]$-scheme, it is sufficient to show that each object in the fiber category at some T has no non-trivial automorphism.

The requirement $N \geq 3$ is for the rigidity of N-level structures. That means when $N \geq 3$ the endmorphism groups of a pair (E, α) is trivial while when $N = 2$, it is isomorphic to $\{\pm 1\}$. $\square$

Moreover, the represent scheme of $\mathcal{M}_0(N), N \geq 3$ is a smooth affine curve over $\mathbb{Z}[\frac{1}{N}]$, which will be denoted by $Y(N)$. We can compatify $Y(N)$ to be a smooth proper curve over $\mathbb{Z}[\frac{1}{N}]$, which will be denoted by $X(N)$ called the modular curve of N-level. This compactification in the viewpoint of modular forms is given by adding the cusp forms.

Let $\Gamma(N)$ be the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e.

$$1 \to \Gamma(N) \to \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\text{mod } N} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to 1.$$

A congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is defined to be an subgroup Γ that contains $\Gamma(N)$ for some integer N. Another way is to identify the $\mathbb{C}$-points set $Y(N)(\mathbb{C})$ as the quotient of upper half-plane by the congruence subgroup $\Gamma(N) \subset \mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma(N)\backslash\mathfrak{H},$$

and then attach the quotient $\Gamma(N)\backslash\mathbb{P}^1(\mathbb{Q})$. Since the $\mathrm{SL}_2(\mathbb{Z})$-action on the upper half-plane $\mathfrak{H}$ is transitively and $\Gamma(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$, the attached piece is finite as a set. Let $\mathfrak{H}^*$ be the union

$$\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

In term of the Galois theory, we have the following well-known fact for the N-level structures of elliptic curves.

Proposition 1.2. Let $E/\mathbb{Q}(t)$ be an elliptic curve over the complex j-line such that $j(E) = t$. Then the Galois representation of its N-torsion points

$$\rho\colon\ \mathrm{Gal}\left((\mathbb{Q}(t, E[N])/\mathbb{Q}(t)\right) \hookrightarrow{}^{1}\, \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

is an isomorphism.

Proof. Consider the base-change of E to $\mathbb{C}(t)$. There is an isomorphism

$$\mathrm{Gal}(\mathbb{C}(t, E[N])/\mathbb{C}(t)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}); \tag{1}$$

see [2, Theorem 1]. We have the following field extensions:

$$\begin{tikzcd}[arrows=dash]
\mathbb{C}(t, E[N]) \arrow[d] \arrow[dr] & \\
\mathbb{C}(t) \arrow[d] & \mathbb{Q}(t, E[N]) \arrow[dl] \\
\mathbb{Q}(t, \mu_N) \arrow[d] & \\
\mathbb{Q}(t) &
\end{tikzcd}$$

Hence $[\mathbb{Q}(t, E[N])\colon \mathbb{Q}(t, \mu_N)] \leq [\mathbb{C}(t, E[N])\colon \mathbb{C}(t)]$. However, since the Galois action on $E[N]$ is compatible with the Weil pairing

$$e_N\colon E[N] \times E[N] \to \mu_N,$$

the image of $\mathrm{Gal}(\mathbb{Q}(t, E[N])/\mathbb{Q}(t, \mu_N)) \subset \mathrm{Gal}\left((\mathbb{Q}(t, E[N])/\mathbb{Q}(t)\right)$ is contained in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Thus its image is $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Moreover, we know that the determinant $\det(\rho)$ is the character

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(t, \mu_N)/\mathbb{Q}(t)) &\to (\mathbb{Z}/N\mathbb{Z})^\times \\ \xi^k &\mapsto k \pmod{N}.\end{aligned}$$

Hence ρ is surjective. □

From the Proposition 1.2, we can see the N-level structure of an elliptic curve $E_0/\mathbb{Q}$ with good reduction at $[N]$ can be viewed as the conjugacy classes of some $\gamma_0 \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

2 Mod p points of Modular Curves

From the moduli interpretation of modular curves, we can see

$$\begin{aligned}Y(N)(\mathbb{F}_q) \cong &\mathcal{M}_0(N)(\mathbb{F}_q) \\ &= \{\text{ the isomorphism classes of elliptic curves over } \mathbb{F}_q \text{ with } N\text{-level structures }\}\end{aligned}$$

for any $p \nmid N$. In this part, we will discuss the group-theoretic description for the set of $\mathbb{F}_q$-points of modular curves.

Recall that we have the following isogeny theorem for abelian varieties

Theorem 2.1. Let k be a field finitely generated over $\mathbb{F}_p$. Let A_1 and A_2 be two abelian varieties over k. Then there is a canonical (e.g. functorial at both A_1 and A_2) isomorphism

$$\mathrm{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{G_k}(T_\ell(A_1), T_\ell(A_2)).$$

Here ℓ is allowed to be p, in which case $T_\ell(-)$ is the p-divisible group of the abelian variety (also called Barsotti-Tate group in Grothendieck's terminology).

Proof. We deal with the simplest case: elliptic curves over a finite field. The case for general abelian varieties over finite field owes to J. Tate.

For any $\varphi \otimes t \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$, the $\eta(\varphi \otimes t) \coloneqq T_\ell(\varphi) \otimes t$ since the set of morphisms bewteen ℓ-typical Tate modules forms a free $\mathbb{Z}_\ell$-module and the formation is canonical. □

[1] The ρ is induced by taking the automorphism of $E[N]$ after fixing a $\underline{\mathbb{Z}/N\mathbb{Z}}$-basis. It is injective since $E[N]$ is free $\mathcal{O}_E$-module.

Remark 2.2. We can discuss the details of the proof in the future lecture about "p-divisible group".

There are only two kinds of p-divisible groups $T_pE := E[p^\infty]$ among the elliptic curves over an algebraically closed field k such that $\mathrm{char}(k) = p > 0$:

- $\mu_p \times \mathbb{Q}_p/\mathbb{Z}_p$;
- the formal group of height 2.

The first case is called ordinary and the second case is called supersingular. In term of the Dieudonné theory, the ordinart corresponds to the F-isocrystal whose Newton polygon is coincide with Hodge polygon and the supersingular case corresponds to the F-isocrystal whose Newton polygon is a straight line.

Let $x_0 = (E_0, \alpha_0) \in \mathcal{M}_0(N)(\mathbb{F}_q)$ and X the set

$$\{(E, \alpha) \in \mathcal{M}_0(N)(\mathbb{F}_q) | E \text{ is isogenous to } E_0 \ \}.$$

Let $I(\gamma_0) := (\mathrm{End}(E_0) \otimes \mathbb{Q})^\times$, which is the set of self-isogenies of E_0. Let

$$H^p := H^1(E_0, \mathbb{A}_f^p) \quad H_p := H^1_{\mathrm{crys}}(E_0/W(\mathbb{F}_q))[\frac{1}{p}].$$

The theory of étale cohomology and crystalline cohomology shows that any isogeny $g\colon E_0 \to E$ induces isomorphisms between rational cohomologies:

$$H^p(E) := H^1(E, \mathbb{A}_f^p) \xrightarrow[\sim]{g^*} H^p \quad H_p(E) := H^1_{\mathrm{crys}}(E/W(\mathbb{F}_q)[\frac{1}{p}] \xrightarrow[\sim]{g^*} H_p.$$

Moreover, the image of Tate module $\prod_{\ell \neq p} T_\ell(E)$ (resp. BT-group $T_p(E)$) of E in H^p (resp. H_p) can be viewed as $\hat{\mathbb{Z}}^p$-lattice (resp. $\mathbb{Z}_p$-lattice). Let

$$X_p := \{\Lambda_p \subset H_p \big| \Lambda_p \text{ is a } F\text{-crystal over } W(\mathbb{F}_q)\}$$
$$X^p := \{(\lambda^p, \alpha) \big| \Lambda^p \subset H^p \text{is } G_{\mathbb{F}_q}\text{-stable lattice and persevering the } N\text{-level structure.}\}$$

As a corollary of Tate's isogeny theorem, we have

Proposition 2.3. The map

$$X \to I \backslash X^p \times X_p$$
$$[(E, \alpha)] \mapsto [\{H^p(E), \widetilde{\alpha}), H_p(E)\}]$$

is a bijection.

Let Frob_q be the geometric Frobenius element of the Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Let γ be the induced $\mathbb{A}_f^p$-linear automorphism on H^p, as an element in $\mathrm{GL}_2(\mathbb{A}_f^p)$. As $\mathrm{GL}_2(\mathbb{A}_f^p)$ acts transitively on H^p, the automoprhism of H^p which fixes the N-level structure α one-to-one corresponding to

$$\mathrm{GL}_2(\mathbb{A}_f^p)/K^p(N),$$

where $K^p(N)$ is the subgroup

$$\left\{g \in \mathrm{GL}_2(\widehat{\mathbb{Z}}^p) \big| g \equiv \mathrm{id} \pmod N \right\}.$$

Thus those g which are compatible with the Galois action can be written as

$$I \backslash X^p \simeq \left\{[g] \in \mathrm{GL}_2(\mathbb{A}_f^p)/K^p(N) \big| g\gamma g^{-1} \in K^p(N) \right\}$$

The requirement for elements g in X_p is equivalent to

$$Fg\,\mathrm{GL}_2(\mathbb{Z}_p) = g\,\mathrm{GL}_2(\mathbb{Z}_p),$$

where F is the induced absolute Frobenius endmorphism on E_0, it is σ-linear. It is furthermore equivalent to

$$p \cdot g\,\mathrm{GL}_2(\mathbb{Z}_p) \subset Fg\,\mathrm{GL}_2(\mathbb{Z}_p) \subset g\,\mathrm{GL}_2(\mathbb{Z}_p).$$

Then choose the linearization δ of F, i.e. $F = \delta\sigma$, we can see $\delta \in \mathrm{GL}_2(\mathbb{Q}_q)$ and

$$p \cdot g \,\mathrm{GL}_2(\mathbb{Z}_p) \subset g^{-1}\delta\sigma(g)\,\mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Z}_p).$$

It is known that the Hodge slopes of F is $(0,1)$, thus we have

$$X_p \simeq \left\{ g \in \mathrm{GL}_2(\mathbb{Q}_{\shortparallel})/\,\mathrm{GL}_2(\mathbb{Z}_p) \middle| g^{-1}\delta\sigma(g) \in \mathrm{GL}_2(\mathbb{Z}_q) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_p) \right\}.$$

To summary, we can describe $Y(N)(\mathbb{F}_q)$ as an disjoint union

$$Y(N)(\mathbb{F}_q) \simeq \coprod_{(\gamma_0;\gamma,\delta)} I(\gamma_0)\backslash X^p(\gamma) \times X_p(\delta),$$

where

- γ is the q-Frobenius endmorphism in $H^1(E, \mathbb{A}_f^p)$ of the elliptic curve isogenous to E_0;
- δ is the induced absolute Frobenius on the crystalline cohomology. Denote $\delta\sigma(\delta)\cdots\sigma^{r-1}(\delta)$ by γ_p, where σ is the Frobenius of the unramified closure $\mathbb{Q}_p^{ur}$;
- $\gamma_0 \in \mathrm{End}(E) \otimes \mathbb{Q}$ the q-Frobenius and from Tate's isogeny theorem, it is conjugate to γ and γ_p stably.

The index $(\gamma_0;\gamma,\delta)$ is called a *Kottwitz triple*. For an elliptic curve $E/\mathbb{F}_q$, let π be the q-Frobenius endmorphism in $\mathrm{End}(E) \otimes Q$[2]. Let p_π be its characteristic polynomial. It can be written as

$$p_\pi = t^2 - \mathrm{tr}(\pi)t + q \quad \mathrm{tr}(\pi) \in \mathbb{Z}.$$

Its eigenvalues are Weil q-number which are Galois conjugate with each other, that is $|\mathrm{tr}\,\pi| < 2\sqrt{q}$. The index $(\gamma_0;\gamma,\delta)$ is effective if

- $\gamma_0 \in \mathrm{GL}_2(\mathbb{Q})$ such that $\mathrm{tr}(\gamma_0) \in \mathbb{Z}$ and $|\mathrm{tr}(\gamma_0)| < 2\sqrt{q}$, and γ_0 is *elliptic* in $\mathrm{GL}_2(\mathbb{R})$;
- γ and γ_0 are conjugate after base-change to $\bar{\mathbb{Q}}_\ell$;
- $N\delta := \delta\sigma(\delta)\cdots\sigma^{r-1}(\delta)$ is conjugate to γ_0 in $\mathrm{GL}_2(\bar{\mathbb{Q}}_p)$.

3 The Statement of Kottiwtz-Langlands-Rapoport Conjecture

Let (G, X) be a reductive Shimura datumn.

Definition 3.1. A connected Shimura datumn (G, X^+) is called of primitive abelian type if

- G is simple group;
- there is an injective homomorphism $G \hookrightarrow \mathrm{Sp}(V,\psi)$ for some symplectic space (V,ψ) such that the image of X^+ is contained in $X(V,\psi)$.

Definition 3.2. A connected Shimura datumn (G, X^+) is called of abelian type if (G, X^+) is isogenous to a product of Shimura datumn (G_i, X_i^+), i.e. there is an isogeny $\prod_i G_i \to G$ such that the image of $\prod_i X_i^+$ is contained into X^+.

In general, the Shimura datumn (G, X) is called of abelian type if (G^{der}, X^+) is of abelian type.

Fix an compact open subgroup of $G(\mathbb{Q}_p)$. Let $\mathrm{Sh}_p(G,X)/K_p$.

Definition 3.3 (Milne17)**.** A model of $\mathrm{Sh}_p(G,X)$ over $\mathcal{O}_L$ is a scheme S over $\mathcal{O}_L$ together with a continuous action of $G(\mathbb{A}_f^p)$ and a $G(\mathbb{A}_f^p)$-equivariant isomorphism

$$S \times_{\mathcal{O}_L} L \xrightarrow{\sim} \mathrm{Sh}_p(G,X)_L.$$

[2]Since $E^r \cong E$ as $q = p^r$.

Conjecture 3.1. Let $\mathrm{Sh}(X,G)$ be a Shimura variety of abelian type. Suppose that $\mathrm{Sh}(X,G)$ admits a canonical integral model $\mathscr{S}(X,G)$ defined over the ring of integers of the reflex field $E = E(G,X)$. For any prime $\lambda \mid p$ of E, there is a bijection

$$\mathscr{S}(X,G)_p(\overline{\mathbb{F}}_p) \cong \coprod_{\phi} S(\phi).$$

Here ϕ runs over the set of admissible morphisms. For finite field $\mathbb{F}_q$ such that $k(v) \subset \mathbb{F}_q$ the description is

$$\mathscr{S}(X,G)_p(\mathbb{F}_q) \cong \coprod_{\varphi,\delta} \varprojlim_{K^p} I_{\varphi,\delta}(\mathbb{Q})\backslash X^p(\varphi,\delta) \times X_p(\varphi,\delta)/K^p. \tag{2}$$

Theorem 3.4. The bijection (2) is true for Shimura variety of abelian type when

- $p > 2$;
- K_p is hyperspecial, i.e. G extends to a reductive group $G_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$ such that $K_p = G_{\mathbb{Z}_p}(\mathbb{Z}_p) = K^p$.

4 Canonical Integral Model of Siegel Modular Variety

Let (V,Φ) be a symplectic space and G the associated symplectic group.

5 Motivic Galois Gerbs

Let F be a field in characteristic zero and L/F a Galois extension. Let G be an algebraic group over F. The Galois group $\mathrm{Gal}(L/K)$ naturally acts on $G(L)$. Consider the following extension of $\mathrm{Gal}(L/K)$-modules:

$$1 \to G(L) \to E \to \mathrm{Gal}(L/F) \to 1.$$

Such extension will be called

- *split*, if it corresponds to the trivial element in

$$\mathrm{Ext}^1_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L/K), G(L)) = H^2(\mathrm{Gal}(L/K), G(L)).$$

- *affine* if there is an open-subgroup of $\mathrm{Gal}(L/F)$ such that E is split after pull-back.

References

[1] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569

[2] David E. Rohrlich, *Modular curves, Hecke correspondence, and L-functions*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 1997, pp. 41–100. MR1638476