The Galois Representation Associated to Modular Forms (Part I)

Modular Curves, Modular Forms and Hecke Operators

Chloe Martindale

May 20, 2015

Contents

This talk was presented at the Local Langlands Seminar at Leiden University in May 2015, organised by Santosh Nadimpalli and Carlo Pagano. It is largely based on the lecture notes of Bas Edixhoven from a course taught at the Summer School and Conference on Automorphic Forms and Shimura Varieties in Trieste in 2007, see [Edi07]. The author would like to thank Bas Edixhoven for helping me with some of the material. The author welcomes any corrections.

1 Motivation and Background

Constructing the Galois representation associated to modular forms will lead us to local Langlands correspondances, both ℓ-adic and conjecturally p-adic. We will vaguely state two theorems which show this correspondence, before giving the background knowledge of modular forms necessary to construct this Galois representation.

For any prime ℓ, denote by $\rho_{f,\ell}$ the Galois representation associated to a modular form f. This will turn out to be a representation of the form

$$\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(V),$$

where V is a prescribed $\mathbb{Q}_\ell$-vector space depending on f. Then, as we saw in an earlier lecture of Santosh Nadimpalli, for any prime p, we can restrict this representation to $G_{\mathbb{Q}_p}$, and we define

$$(\rho_{f,\ell})_p := \rho_{f,\ell}|_{G_{\mathbb{Q}_p}}.$$

We have the following result for $p \neq \ell$.

Theorem 1.1 (Langlands, Deligne, Carayol)**.** *For any prime ℓ, any prime $p \neq \ell$, and f a modular form, there is a prescribed representation $\pi_{f,p}$ of* $\mathrm{GL}_2(\mathbb{Q}_p)$ *such that $(\rho_{f,\ell})_p^{(\mathrm{F.s.s.})}$ corresponds under a suitably normalized Langlands correspondence to $\pi_{f,p}$, where* F.s.s. *denotes Frobenius semi-simplification.*

Remark 1.2 (Frobenius semi-simplification)**.** If there is a representation $\alpha : G_{\mathbb{Q}_p} \to \bar{\mathbb{Q}}_\ell^*$ such that $(\rho_{f,\ell})_p \otimes \alpha$ is unramified, then $\big((\rho_{f,\ell})_p \otimes \alpha\big)(\mathrm{Frob}_p)$ is semi-simple. Conjecturally the Frobenius semi-simplification in the above theorem is not necessary.

Furthermore, we have the following theorem for $p = \ell$:

Theorem 1.3 (Saito)**.** *For any prime p, let Weil-Deligne representation associated to $(\rho_{f,p})_p$, be denoted by* $\mathrm{WD}(\rho_{f,p})_p$. *Then we have a correspondence*

$$(\mathrm{WD}(\rho_{f,p})_p)^{(\mathrm{F.s.s.})} \leftrightarrow \pi_{f,p},$$

where F.s.s. *denotes Frobenius semi-simplification and $\pi_{f,p}$ is as in Theorem* 1.1.

Remark 1.4. If we could find the right hand side of the above correspondence for $(\rho_{f,p})_p$, this would be a p-adic Langlands correspondence.

For the remainder of this talk, we will recall the background knowledge required to construct $\rho_{f,\ell}$.

2 Modular Curves

Throughout this talk, $\mathbb{H}$ will denote the complex upper half plane and $\mathrm{GL}_2^+(\mathbb{R})$ will denote the general linear group of dimension two with real coefficients whose elements have positive determinant.

Definition 2.1. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. Then Γ is a *congruence subgroup* if there exists $N \in \mathbb{Z}_{>0}$ such that $\Gamma(N) \subset \Gamma$, where

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

Examples 2.2. Two key examples of congruence subgroups are the following:

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

and

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

Given a congruence subgroup Γ, one can check that it acts on $\mathbb{H}$ via Mobius transformations, which allows us to define the modular curve

$$Y_\Gamma(\mathbb{C}) := \Gamma\backslash\mathbb{H}.$$

It is a non-trivial fact that for any congruence subgroup Γ we have a correspondence

$$Y_\Gamma(\mathbb{C}) \leftrightarrow \left\{(E/\mathbb{C}, \phi \in \Gamma\backslash\mathrm{Isom}^+(\mathbb{Z}^2, \mathrm{H}_1(E,\mathbb{Z})))\right\}_{/\cong},$$

where E denotes an elliptic curve. For our two examples of congruence subgroups above this becomes

$$Y_1(N) := Y_{\Gamma_1(N)}(\mathbb{C}) = \{(E,P) : P \in E \text{ has order } N\}_{/\cong}$$

and

$$Y_0(N) := Y_{\Gamma_0(N)}(\mathbb{C}) = \{(E,G) : G \subset E \text{ a cyclic subgroup of order } N\}_{/\cong}.$$

Further, we can add a finite number of points, called cusps, to 'compactify' $Y_\Gamma(\mathbb{C})$. This gives compact projective algebraic curve denoted by $X_\Gamma(\mathbb{C})$, i.e.

$$X_\Gamma(\mathbb{C}) = Y_\Gamma(\mathbb{C}) \cup \Gamma\backslash\mathbb{P}^1(\mathbb{Q}).$$

3 Modular Forms

We will briefly recall the standard definition of modular forms and cusp forms, and then give an alternative way of defining cusp forms (for the case in which Γ acts freely on $\mathbb{H}$ and acts regularly at the cusps) as global sections of modular curves.

Definition 3.1. Let $k \in \mathbb{Z}$, $f : \mathbb{H} \to \mathbb{C}$ be a function and $\alpha = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$. Then for all $z \in \mathbb{H}$,

$$(f|_{[\alpha]_k})(z) := \det(\alpha)^{k-1}(cz+d)^{-k} f(\alpha \cdot z).$$

Definition 3.2. Let $k \in \mathbb{Z}_{\geq 0}$, Γ a congruence subgroup. A *modular form of weight k with respect to* Γ is a function $f : \mathbb{H} \to \mathbb{C}$ satisfying
(i) f holomorphic on $\mathbb{H}$
(ii) For all $\gamma \in \Gamma$, $f|_{[\gamma]_k} = f$
(iii) f is holomorphic at all the cusps.

Remark 3.3. We define f being holomorphic at the cusps in the following way. We know that there is an $h \in \mathbb{Z}_{>0}$ such that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$, and hence for any $z \in \mathbb{H}$, $f(z+h) = f(z)$. Therefore f has a Fourier expansion at infinity,

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q_h^n,$$

where $q_h := e^{2\pi iz/h}$. Then f is defined to be holomorphic at infinity if for every $n < 0$, $a_n = 0$, and f is defined to be holomorphic at all the cusps if for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $f|_{[\alpha]_k}$ is holomorphic at infinity.

We denote by $\mathcal{M}_k(\Gamma)$ the space of all modular forms of weight k with respect to Γ, and by $\mathcal{S}_k(\Gamma)$ the space of all cusp forms of weight k with respect to Γ, where a cusp form is a modular form that vanishes at all the cusps.

Examples 3.4. Examples of modular forms are
• Eisenstein series. In fact the Eisenstein of weight 4 and 6, E_4 and E_6, generate all of $\mathcal{M}_k(\Gamma)$, telling us the dimension of this space for any k.
• 'The Ramanujan τ-function', which is

$$\Delta(z) = q \prod_{n=1}^{\infty}(1-q^n)^{24} = 1/1728(E_4^3 - E_6^2) \in S_{12}(\Gamma_1(1)),$$

where $q = e^{2\pi iz}$.
• Cusp forms can be obtained via Hecke characters.. see next weeks lecture!

We now turn to the alternative (equivalent) definition of the space of cusp forms of weight k with respect to Γ, where Γ is a congruence subgroup which acts freely on $\mathbb{H}$ and acts regularly at the cusps. This holds for $\Gamma_1(N)$ when $N \geq 5$ but never for $\Gamma_0(N)$. That the two definitions are equivalent is left as an exercise...
Let $\mathbb{E}$ be defined as follows;

$$\mathbb{E} = \{(P,\tau) : \tau \in \mathbb{H},\, P \in \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}\}.$$

Then consider the following:

$$\begin{tikzcd} \mathbb{Z}^2 \times \mathbb{H} \arrow[r, hook] \arrow[dr] & \mathbb{C} \times \mathbb{H} \arrow[r, two heads] \arrow[d] & \mathbb{E} \arrow[dl] \\ & \mathbb{H} & \end{tikzcd} \tag{1}$$

where

$$\begin{array}{ccc} \mathbb{Z}^2 \times \mathbb{H} & \hookrightarrow & \mathbb{C} \times \mathbb{H} \\ ((n,m),\tau) & \mapsto & (n\tau + m, \tau), \end{array}$$

and the map $\mathbb{C} \times \mathbb{H} \to \mathbb{E}$ is just the quotient map. Then if Γ acts freely on $\mathbb{H}$ we get an elliptic curve $\mathbb{E} \to Y_\Gamma(\mathbb{C})$ by taking the quotient. Define the Γ action on $\mathbb{Z}^2 \times \mathbb{H}$ by

$$((n,m),\tau) \mapsto ((n,m)\gamma^{-1}, \gamma \cdot \tau)$$

and on $\mathbb{C} \times \mathbb{H}$ by

$$(z,\tau) \mapsto (z/c\tau + d, \tau),$$

where $\gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma$. Let

$$\mathbb{H} \overset{0}{\dashrightarrow} \mathbb{E}$$

be the zero section of the projection $\mathbb{E} \to \mathbb{H}$, and define $\underline{\omega} = 0^*\Omega^1_{\mathbb{E}/\mathbb{H}}$.

Lemma 3.5. We have

$$\underline{\omega} = \mathcal{O}_{\mathbb{H}}\mathrm{dz}.$$

Proof. To consider an open neighbourhood of 0 on $\mathbb{E}$, we can take the (open) fundamental domain of its defining lattice, and translate it by $-(1+\tau)/2$, so that 0 lies at the centre. This set is also a open neighbourhood of 0 in $\mathbb{C}$, and so locally at 0, the map $\mathbb{C}\times\mathbb{H}\to\mathbb{E}$ from Diagram 1 is an isomorphism. Therefore

$$0^*\Omega^1_{\mathbb{E}/\mathbb{H}} = 0^*\Omega^1_{\mathbb{C}\times\mathbb{H}/\mathbb{H}}.$$

Now the diagram

$$\begin{tikzcd} \mathbb{C}\times\mathbb{H} \arrow[r, "h"] \arrow[d] & \mathbb{C}\times\{\cdot\} \arrow[d] \\ \mathbb{H} \arrow[r] & \cdot \end{tikzcd}$$

gives us that

$$0^*\Omega^1_{\mathbb{C}\times\mathbb{H}/\mathbb{H}} = 0^*h^*\Omega^1_{\mathbb{C}} = 0^*\mathcal{O}_{\mathbb{C}\times\mathbb{H}}\mathrm{dz} = \mathcal{O}_{\mathbb{H}}\mathrm{dz}.$$

□

To understand to Γ-action on $\underline{\omega}$ we first look at the Γ-action on dz. Let $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma$. Then we have

$$\begin{array}{rccc} \gamma: & \mathbb{C}\otimes\mathbb{H} & \to & \mathbb{C}\otimes\mathbb{H} \\ & (z,\tau) & \mapsto & (z/c\tau+d, \gamma\tau), \end{array}$$

and so

$$(\gamma\cdot)^*\mathrm{dz} = \mathrm{d}(\gamma \mathrm{z}) = \mathrm{dz}/cz+d.$$

Now let $f\in\mathcal{O}_{\mathbb{H}}$. Then $f(\mathrm{dz})^{\otimes k}\in\underline{\omega}^{\otimes k}$ and

$$(\gamma\cdot)^*(f(\mathrm{dz})^{\otimes k}) = (f\circ\gamma)(c\tau+d)^{-k}(\mathrm{dz})^{\otimes k},$$

so in particular $f(\mathrm{dz})^{\otimes k}$ is Γ-invariant if and only if for all γ in Γ, $(f\circ\gamma)(\tau) = (c\tau+d)^k f(\tau)$. Then if Γ acts freely on $\mathbb{H}$, $\underline{\omega}$ is defined on $Y_\Gamma(\mathbb{C})$, and if Γ acts regularly at the cusps, then $\underline{\omega}$ is defined on $X_\Gamma(\mathbb{C})$.

Remark 3.6 (Acts regularly at the cusps)**.** Here, 'acts regularly at the cusps' means

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{\pm\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}.$$

Finally, we get

Definition 3.7. For an integer $k\geq 2$, and Γ a congruence subgroup which acts freely on $\mathbb{H}$ and acts regularly at the cusps, define the space of cusp forms of weight k with respect to Γ by

$$S_k(\Gamma) = \mathrm{H}^0(X_\Gamma(\mathbb{C}), \underline{\omega}^{\otimes k}(-\mathrm{cusps})).$$

Lemma 3.8 (Kodaira-Spencer)**.** We have an isomorphism of $\mathcal{O}_{\mathbb{H}}$-modules

$$\underline{\omega}^{\otimes k}(-\text{cusps}) \cong \Omega^1_{X_\Gamma(\mathbb{C})} \otimes \underline{\omega}^{\otimes(k-2)}.$$

Sketch. By Lemma 3.5 we have that $\underline{\omega}^{\otimes 2} = \mathcal{O}_{\mathbb{H}}\mathrm{dz}^{\otimes 2}$, hence as $\Omega^1_{\mathbb{H}} \cong \mathcal{O}_{\mathbb{H}}\mathrm{d}\tau$, we have an $\mathcal{O}_{\mathbb{H}}$-module isomorphism

$$\underline{\omega}^{\otimes 2} \cong \Omega^1_{\mathbb{H}}.$$

Now let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Then

$$(\gamma\cdot)^*(\mathrm{dz})^{\otimes 2} = \mathrm{d}(\gamma z)^{\otimes 2} = (\mathrm{d}z/(cz+d))^{\otimes 2} = (\mathrm{dz})^{\otimes 2}/(c\tau+d)^2,$$

and

$$(\gamma\cdot)^*\mathrm{d}\tau = \mathrm{d}(\gamma\tau) = \mathrm{d}\tau/(cz+d)^2,$$

hence they are also equivalent up to Γ-action. A further calculation to determine what happens at the cusps (omitted) then gives

$$\underline{\omega}^{\otimes 2}(-\text{cusps}) \cong \Omega^1_{X_\Gamma(\mathbb{C})}.$$

As $(-\text{cusps})$ commutes with tensor products, the result now follows. □

Corollary 3.9. *For an integer $k \geq 2$, and Γ a congruence subgroup which acts freely on $\mathbb{H}$ and acts regularly at the cusps, we have*

$$S_k(\Gamma) = \mathrm{H}^0(X_\Gamma(\mathbb{C}), \Omega^1_{X_\Gamma(\mathbb{C})} \otimes \underline{\omega}^{\otimes(k-2)}).$$

4 Hecke Operators

A crucial tool in the construction of the Galois representation of a modular form will be Hecke operators. They give rise to modular correspondences and they act on modular forms and the integral homology of modular curves. They can be realised in many different ways, and the consistency with which this is done makes them very interesting! To define Hecke operators on modular forms, we first show how to decompose $\mathcal{M}_k(\Gamma_1(N)$ and $\mathcal{S}_k(\Gamma_1(N)$ into a direct sum of eigenspaces.

Definition 4.1. Let χ be a Dirichlet character mod N, that is, a group homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$. Then a *modular form of type* (k, N, χ) is $f \in \mathcal{M}_k(\Gamma_1(N))$ such that for all $\gamma = \begin{pmatrix} * & * \\ * & d \end{pmatrix} \in \Gamma^0(N)$,

$$(f|_{[\gamma]_k})(z) = \chi(d)f(z).$$

The space of all such modular forms is denoted by $\mathcal{M}_k(N,\chi)$. Let $d \in (\mathbb{Z}/N\mathbb{Z})^*$, and define $\underline{d} = \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \bmod N$. Then d acts on $\mathcal{M}_k(\Gamma_1(N))$ by $[d]_k : f \mapsto f|_{[\underline{d}]_k}$, and $\mathcal{M}_k(N,\chi)$ is the χ-eigenspace with respect to the action. Further, we get the direct sum decomposition

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi(-1)=(-1)^k} \mathcal{M}_k(N,\chi).$$

Following exactly the same procedure for cusp forms, we get

$$\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi(-1)=(-1)^k} \mathcal{S}_k(N,\chi).$$

Definition 4.2. Let

$$\Delta_1(N) = \left\{ \gamma \in M_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod N,\ \det(\gamma) > 0 \right\},$$

and set $\Gamma = \Gamma_1(N)$. Let $f \in \mathcal{M}_k(\Gamma_1(N))$ and $\alpha \in \Delta_1(N)$. Define the *Hecke operator* by

$$T : f \mapsto f|_{[\Gamma\alpha\Gamma]_k} = \sum_i f|_{[\alpha_i]_k},$$

where $\{\alpha_i\}$ is a set of coset representatives for $\Gamma\backslash\Gamma\alpha\Gamma$. Then one can show that $[\Gamma\alpha\Gamma]_k$ acts on $\mathcal{M}_k(\Gamma)$ and preserves $\mathcal{S}_k(\Gamma)$.

Definition 4.3. The *Jacobian variety* of $X_\Gamma(\mathbb{C})$ is given by

$$J_\Gamma(\mathbb{C}) = \mathrm{H}^0(X_\Gamma(\mathbb{C}), \Omega^1_{X_\Gamma(\mathbb{C})})^\vee / \mathrm{H}_1(X_\Gamma(\mathbb{C},\mathbb{Z}),$$

so by the Kodaira-Spencer isomorphism, if Γ acts freely on $\mathbb{H}$ and regularly at the cusps,

$$J_\Gamma(\mathbb{C}) = S_2(\Gamma)^\vee / \mathrm{H}_1(X_\Gamma(\mathbb{C}), \mathbb{Z}).$$

So now we look at Hecke operators as endomorphisms of $J_\Gamma(\mathbb{C})$. We use without proof that

$$J_\Gamma(\mathbb{C}) = \mathrm{Pic}^0(X_\Gamma(\mathbb{C})) = \mathrm{Div}^0(X_\Gamma(\mathbb{C}))/\text{principal divisors},$$

so in particular we can write an element of $J_\Gamma(\mathbb{C})$ as $\overline{P_1 + \cdots + P_d - d\cdot\infty}$, where the P_i are in $X_1(N)$.

Definition 4.4. We define the Hecke operator on modular curves in a corresponding way to how we defined it for modular forms, that is,

$$\begin{array}{cccc} T_n & X_1(N) & \to & X_0(n) \\ & (\overline{E,P}) & \mapsto & \sum_{\substack{G\subset E \text{ order } n \\ \text{s.t.} <P>\cap G=0}} (\overline{E/G,\overline{P}}). \end{array}$$

This induces a map $T_n \in \mathrm{End}(J_{\Gamma^1(N)}(\mathbb{C}))$ via

$$T_n : \overline{P_1 + \cdots P_d - d\cdot\infty} \mapsto \overline{T_nP_1 \cdots T_nP_d - dT_n\infty}.$$

References

[CE11] Jean-Marc Couveignes and Bas Edixhoven, *Computational Aspects of Modular Forms and Galois Representations*, Ann. Math. 176, (2011).

[DI95] Fred Diamond and John Im, *Modular Forms and Modular Curves*, Can. Math. Soc. Conference Precedings, Vol. 17, (1995).

[Edi07] Bas Edixhoven, *Modular Curves*, Lecture Notes from the Summer School and Conference on Automorphic Forms and Shimura Varieties in Trieste, `http://pub.math.leidenuniv.nl/~edixhovensj/talks/2007/ICTP-Trieste.pdf` (2007).