Galois representations and Modular forms

Bas Edixhoven

July 8, 2018

Abstract

These are notes for 3 lectures of 1.5 hours each at the Summer School "Explicit and computational approaches to Galois representations" held at the university of Luxemburg, 3-7 July 2018.

The notes are based on hand written notes for a series of 4 lectures of 1 hour each at the Summer School and Conference on Automorphic Forms and Shimura Varieties in Trieste, 9–27 July 2007, to be found at `http://pub.math.leidenuniv.nl/~edixhovensj/talks/2007/ICTP-Trieste.pdf`.

I thank the organisers of the Luxemburg Summer School for getting a first version of the hand written notes typed in latex.

Contents

1 The Galois representations associated to modular forms: main results.

We begin with the main results, to get motivated for the work that follows. The following theorem was proved by Eichler and Shimura for $k = 2$ in the 1950's (but formulated in terms of zeta-functions), and by Deligne for $k \geq 2$ in 1969.

Theorem 1. *Let N and k be positive integers such that $k \geq 2$, $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character, and $f = \sum_{n\geq 1} a_n(f)q^n$ a normalized ($a_1(f) = 1$) newform of type (N, k, ε). Then $K_f := \mathbb{Q}(a_1(f), a_2(f), \dots)$ is finite over $\mathbb{Q}$, and for every prime l there exists a unique continuous representation*

$$\rho_{f,l}\colon G_{\mathbb{Q}} \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_l \otimes K_f)$$

that is unramified at all primes $p \nmid lN$ and such that for every such p:

$$\det(\rho_{f,l}(\mathrm{Frob}_p)) = \varepsilon(p)p^{k-1}, \quad \textit{and} \quad \mathrm{tr}(\rho_{f,l}(\mathrm{Frob}_p)) = a_p(f).$$

Remark 2. *We note the following.*

1. *These $\rho_{f,l}$ are not smooth, i.e., not continuous for the discrete topology on $\mathrm{GL}_2(\mathbb{Q}_l \otimes K_f)$.*
2. *$\mathbb{Q}_l \otimes K_f = \prod_{\lambda|l} K_{f,\lambda}$.*
3. *Kuga, Sato and Shimura had already treated some higher weight cases for certain Shimura curves (no cusps) in terms of zeta functions.*
4. *For the uniqueness in the theorem: the $\rho_{f,l}$ are irreducible (Ribet, Deligne?)*
5. *Deligne-Serre proved the theorem for $k = 1$. Then the representations $\rho_{f,l}$ have finite image, independent of l. These cannot be constructed in the same way as the others.*

The theorem above gives us information on $(\rho_{f,l})_p := \rho_{f,l}|_{G_{\mathbb{Q}_p}}$ for primes p not dividing lN:

$$(i)\ \ (\rho_{f,l})_p \text{ is unramified and,}$$
$$(ii)\ \ \det(1 - T \cdot \rho_{f,l}(\mathrm{Frob}_p)) = 1 - a_p(f)T + \epsilon(p)p^{k-1}T^2.$$

To describe $(\rho_{f,l})_p$ for $p|N$ $(p \neq l)$ one needs representation theory. We will see (hopefully) that f induces an automorphic form φ on $\mathrm{GL}_2(\mathbb{A})$, which induces a cuspidal, irreducible automorphic representation $\pi_f = \otimes'_v \pi_{f,v}$ (restricted tensor product) in $\mathcal{A}_0(\mathrm{GL}_{2,\mathbb{Q}}, \epsilon)$.

Theorem 3 (Langlands, Deligne, Carayol, Nyssen)**.** *(vaguely formulated here) For all primes l and for all primes p which are different from l, the representations $(\rho_{f,l})_p^{F-s.s.}$ and $\pi_{f,p}$ correspond to each other via a suitably normalized local Langlands correspondence.*

Remark 4.

1. *The normalisation of the local Langlands correspondance is up to $V \mapsto V^\vee$ and $\rho \mapsto \rho \otimes \chi_l^m$ where $\chi_l : G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_l^\times = Aut(\bar{\mathbb{Q}}^\times[l^\infty])$ and $m \in \mathbb{Z}$ on the Galois side, and up to $\pi \mapsto \pi^\vee$ and $\pi \mapsto \pi \otimes (|\cdot| \circ \det)^{n/2}$ ($n \in \mathbb{Z}$).*

2. *π_f is complex, but can naturally be defined over K_f, hence also $\pi_{f,p}$.*

3. *F-s.s.= Frob. semi-semisimplification. This is a functor. If there exists an $\alpha : G_{\mathbb{Q}_p} \to \bar{\mathbb{Q}}_l^\times$ such that $(\rho_{f,l})_p \otimes \alpha$ is unramified, then it makes $((\rho_{f,l})_p \otimes \alpha)(Frob_p)$ semi-simple. Conjecturally, this is never necessary. Details: Tate's 'Number theoretic background,' in Corvallis, 1979.*

4. *For $p = l$: $(WD(\rho_{f,l})_p)^{F-s.s.}$ corresponds with $\pi_{f,p}$ (Saito, 1997); WD stands for Weil-Deligne representation, its definition involves functors of Fontaine. In p-adic LL: $(\rho_{f,l})_p$ itself should correspond to what? A representation of $\mathrm{GL}_2(\mathbb{Q}_p)$ on some infinite dimensional Banach space. See the work of Breuil, Colmez, etc.*

5. *All this is crucial for the recent work of Wiles, Taylor, Khare, Kisin...*

Goal of my series of 3 lectures: sketch a proof of Theorem 1, sketch Deligne's proof that $(\rho_{f,l})_p^{\text{F-s.s.}}$ is determined by $\pi_{f,p}$ if $\pi_{f,p}$ is cuspidal if there is time, and say something about computational aspects of Galois representations to GL_2 of finite fields.

The $\rho_{f,l}$ are constructed in the cohomology of certain sheaves on modular curves (and in the torsion of the Jacobian if $k = 2$). So now we will turn to modular curves.

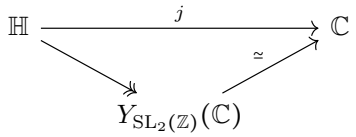
2 Modular curves over $\mathbb{C}$

As usual, $\mathbb{H}$ denotes the complex upper half plane, and we view it as half of $\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$. The group $\mathrm{GL}_2(\mathbb{R})^+$ of 2 by 2 real matrices with positive determinant acts on it, and therefore $\mathrm{SL}_2(\mathbb{R})$ as well. The subset

$$\{\tau \in \mathbb{H} : |\tau| \geq 1 \wedge |\Re(\tau)| \leq 1/2\}$$

is the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$. For $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ any subgroup, the quotient $Y_\Gamma(\mathbb{C}) := \Gamma\backslash\mathbb{H}$ is a 1-dimensional complex analytic manifold.

Example 5. *The function $j\colon \mathbb{H} \to \mathbb{C}$ sending τ to the j-invariant of the complex elliptic curve $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ factors via the quotient $Y_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$, and induces an isomorphism from $Y_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$ to $\mathbb{C}$. In a diagram:*



For $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ a subgroup of of finite index, $Y_\Gamma(\mathbb{C}) \to Y_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C}) = \mathbb{C}$ is a finite, possibly ramified, cover. The ramification occurs at points τ of $\mathbb{H}$ whose stabiliser in $\mathrm{SL}_2(\mathbb{Z})$ is bigger than $\{1, -1\}$, that is, at the points in the orbits of i and $e^{2\pi i/3}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Compactification

For $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ of finite index, we compactify $Y_\Gamma(\mathbb{C})$ by "normalization." That means that we first compactify $Y_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$. The following identity and inequality, for $\tau \in \mathbb{H}$ and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{R})$ with $c \neq 0$:

$$\Im\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\Im(\tau)}{|c\tau + d|^2} \quad \text{and} \quad \frac{\Im(\tau)}{|c\tau + d|^2} \leq \frac{\Im(\tau)}{\Im(c\tau)^2} = \frac{1}{c^2 \Im(\tau)}$$

show that on the part "$\Im(\tau) > 1$" of $\mathbb{H}$ the equivalence relation given by the $\mathrm{SL}_2(\mathbb{Z}$-action is given by the action of $\mathbb{Z}$ by translation. A quotient for that action is the map $\tau \mapsto \exp(2\pi i \tau)$, onto D^*, the punctured open disk of radius $e^{-2\pi}$. This gives us an open immersion of D^* into $Y_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$. The compactification $X_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$ is then obtained by replacing D^* with the non-punctured disk D, that is, by adding the center back into into the punctured disk; this extra point is called the cusp ∞. One can see that the function j on $Y_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$ has a pole of order 1 at ∞, giving an isomorphism from $X_{\mathrm{SL}_2(\mathbb{Z})}(\mathbb{C})$ to $\mathbb{P}^1(\mathbb{C})$.

Now let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be of finite index, and let $f\colon Y_\Gamma(\mathbb{C}) \to Y_{\mathrm{SL}_2(\mathbb{Z}}(\mathbb{C}$ be the natural map. Then the restriction of f to $f^{-1}D^*$ is a covering map, and hence a disjoint union of connected coverings of D^*. Now the fundamental group of D^* is $\mathbb{Z}$, hence the connected covers are of the form $D_n^* \to D^*$, $z \mapsto z^n$, with $n \in \mathbb{Z}_{>0}$, and D_n the disk of the appropriate radius. We compactify each D_n^* by $D *_n \subset D_n$, that is, by adding one cusp. In a diagram:

$$\begin{array}{ccccc} X_\Gamma(\mathbb{C}) & \xrightarrow{f} & X_{\mathrm{SL}_2(\mathbb{Z}}(\mathbb{C}) & = & \mathbb{P}^1(\mathbb{C}) \\ \uparrow & & \uparrow & & \uparrow \\ Y_\Gamma(\mathbb{C}) & \xrightarrow{f} & Y_{\mathrm{SL}_2(\mathbb{Z}}(\mathbb{C}) & = & \mathbb{C} \end{array}$$

Serre's GAGA theorem tells us that $X_\Gamma(\mathbb{C})$ is a projective complex algebraic curve and $Y_\Gamma(\mathbb{C})$ is an affine complex algebraic curve.

For administrative use, we note that, as sets, $X_\Gamma(\mathbb{C})$ is the quotient of $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by the action of Γ.

3 Modular curves over $\mathbb{C}$ as moduli spaces

Let us first look at them as complex analytic spaces. For V be a complex vector space of dimension 1 and $\Lambda \subset V$ a lattice, V/Λ is a complex elliptic curve. The theory of Weierstrass-functions gives an embedding in $\mathbb{P}^2(\mathbb{C})$, showing that they are algebraic curves. In the other direction, the exponential map of a complex elliptic curve E, $\exp_E : \mathrm{T}_E(0) \to E$, gives a natural isomorphism from $\mathrm{T}_E(0)/\ker(\exp_E)$ to E. Another way to get Λ and V from V/Λ is: $\Lambda = \mathrm{H}_1(V/\Lambda, \mathbb{Z})$, $V = \mathbb{R} \otimes \Lambda$ with the $\mathbb{C}$-vector space structure given as tangent space $\mathrm{T}_{V/\Lambda}(0)$.

Morphisms. For V and Λ and V' and Λ':

$$\mathrm{Hom}(V/\Lambda, V'/\Lambda') = \{f : V \to V' \ \mathbb{C}\text{-linear} \ : f(\Lambda) \subseteq \Lambda'\}.$$

Now we interpret the upper half plane $\mathbb{H}$ as a moduli space for all complex elliptic curves together with a basis of their lattice. That is, we look at triples (V, Λ, φ) with $\varphi : \mathbb{Z}^2 \to \Lambda$ an isomorphism of $\mathbb{Z}$-modules, such that $\varphi((1,0))/\varphi((0,1))$ (yes, we can divide in a 1-dimensional vector space) has positive imaginary part. And we look at pairs (E, φ) with E a complex elliptic curve and $\varphi : \mathbb{Z}^2 \to \mathrm{H}_1(E, \mathbb{Z})$ an isomorphism such that $\Im(\varphi((1,0))/\varphi((0,1))) > 0$. Then we have bijections:

$$\mathbb{H} \xrightarrow{\ \simeq\ } \{(V, \Lambda, \varphi)\}/\cong \ = = = = = = = = \ \{(E, \varphi\}/\cong$$

$$\tau \longmapsto (\mathbb{C}, \mathbb{Z}\tau + \mathbb{Z}, (n,m) \mapsto n\tau + m) \longmapsto (\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \varphi)$$

$$\varphi((1,0))/\varphi((0,1)) \longmapsto (V, \Lambda, \varphi)$$

We can interpret the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathbb{H}$ as an action on the set of (E, φ). For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ one has:

$$\mathbb{H} \xrightarrow{\ \simeq\ } \{(E, \varphi)\}/\cong$$

$$\tau \mapsto \gamma\tau \longleftrightarrow (E, \varphi) \mapsto (E, \varphi \circ \gamma^t)$$

In this way, we get, for Γ a subgroup of $\mathrm{SL}_2(Z)$, a bijection

$$Y_\Gamma(\mathbb{C}) \xrightarrow{\ \simeq\ } \{(E, \overline{\varphi})\}/\cong \qquad \overline{\varphi} \in \Gamma\backslash\mathrm{Isom}^+(\mathbb{Z}^2, \mathrm{H}_1(E, \mathbb{Z}))$$

Examples of some congruence subgroups

Let $N \geq 1$, $f : \mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be the group morphism induced by the ring morphism $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$. The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $(Z/N\mathbb{Z})^2$.

1. $\Gamma(N) \coloneqq \ker(f)$, called the principal congruence subgroup of level N. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if it contains some $\Gamma(N)$; this implies that it is of finite index, but there are subgroups of finite index that are not congruence subgroups.
2. $\Gamma_1(N) \coloneqq f^{-1}\mathrm{Stab}(\binom{1}{0})$.
3. $\Gamma_0(N) = f^{-1}\mathrm{Stab}(\binom{\bar{1}}{0})$ where $\binom{\bar{1}}{0}$ is the class of $\binom{1}{0}$ in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

This gives the following interpretations of the various $Y_\Gamma(\mathbb{C})$'s:

$$Y_{\Gamma(N)}(\mathbb{C}) = \{(E, \varphi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N] \text{ symplectic isomorphism})\}/\cong$$
$$Y_{\Gamma_1(N)}(\mathbb{C}) = \{(E, P) : P \in E \text{ has order } N\}/\cong$$
$$Y_{\Gamma_0(N)}(\mathbb{C}) = \{(E, G) : G \subset E \text{ cyclic subgroup of order } N\}/\cong$$

Actually, over $\mathbb{H}$ we have an $\mathrm{SL}_2(\mathbb{Z})$-equivariant family of elliptic curves:

$$(\binom{n}{m}, \tau) \longmapsto (n\tau + m, \tau)$$

$$\begin{array}{ccccc} \mathbb{Z}^2 \times \mathbb{H} & \hookrightarrow & \mathbb{C} \times \mathbb{H} & \twoheadrightarrow & \mathbb{E} \\ & \searrow & \downarrow & \swarrow & \\ & & \mathbb{H} & & \end{array}$$

On this diagram we have an action of the semi-direct product $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$, described as follows. The normal subgroup $\mathbb{Z}^2$ acts trivially on $\mathbb{H}$ and on $\mathbb{E}$, and acts by translations on $\mathbb{Z}^2 \times \mathbb{H}$ and $\mathbb{C} \times \mathbb{H}$: $\binom{n}{m}$ sends $(\binom{a}{b}, \tau)$ to $(\binom{a+n}{b+m}, \tau)$, and sends (z, τ) to $(z + n\tau + m, \tau)$. An element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ sends (z, τ) to $(\frac{z}{c\tau+d}, \gamma\tau)$, and sends $(\binom{n}{m}, \tau)$ to $(\gamma^{-1,t}\binom{n}{m}, \gamma\tau)$.

If $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ acts freely on $\mathbb{H}$, then we get an elliptic curve $\mathbb{E} \to Y_\Gamma(\mathbb{C})$, by taking the quotient by the action of Γ on $\mathbb{E}$ above.

This freeness condition is true for $\Gamma_1(N)$ for $N \geq 4$, $\Gamma(N)$ for $N \geq 3$ and never for $\Gamma_0(N)$.

4 Modular forms

The family of elliptic curves $\mathbb{E} \to \mathbb{H}$ with its section $0\colon \mathbb{H} \to \mathbb{E}$ gives us the invertible sheaf of $\mathcal{O}_\mathbb{H}$-modules $\underline{\omega} \coloneqq 0^*\Omega^1_{\mathbb{E}/\mathbb{H}}$. We have $\underline{\omega} = \mathcal{O}_\mathbb{H} dz$ (where z is our coordinate on $\mathbb{C}$, and τ will be our coordinate on $\mathbb{H}$, that is, z is the identity function on $\mathbb{C}$, and τ is the incusion of $\mathbb{H}$ in $\mathbb{C}$). For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ we have

$$(\gamma\cdot)^* dz = \frac{1}{c\tau + d} dz\,,$$

so

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

We see that the following conditions, for Γ a subgroup of $\mathrm{SL}_2(\mathbb{R})$, and $f\colon \mathbb{H} \to \mathbb{C}$ any function, are equivalent:

1. $f \cdot (dz)^{\otimes k}$ is Γ-invariant,

2. for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, for all $\tau \in \mathbb{H}$, $f((a\tau + b)/(c\tau + d)) = (c\tau + d)^k \cdot f(\tau)$.

If Γ acts freely on $\mathbb{H}$ then we get $\underline{\omega}$ on $Y_\Gamma(\mathbb{C})$, by dividing out the action of Γ.

From now on we assume that Γ is of finite index in $\mathrm{SL}_2(\mathbb{Z})$. We want to extend $\underline{\omega}$ to $X_\Gamma(\mathbb{C})$, and for that we need the notion that Γ acts regularly at the cusps. At the cusp $\infty \in \mathbb{P}^1(\mathbb{Q})$ this means that the stabiliser Γ_∞ of $\infty \in \mathbb{P}^1(\mathbb{Q})$ under the action of Γ is contained in $\{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\} \subset \mathrm{SL}_2(\mathbb{Z})$. At the other cusps c: for each element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma \cdot c = \infty$, $\gamma \Gamma_c \gamma^{-1}$ (which is $(\gamma \Gamma \gamma^{-1})_\infty$) must be contained in $\{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\} \subset \mathrm{SL}_2(\mathbb{Z})$. In more technical terms: all stabilisers of cusps in Γ must consist of unipotent elements. Note that the stabiliser of ∞ in $\mathrm{SL}_2(\mathbb{Z})$ is $\{\pm\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\} \subset \mathrm{SL}_2(\mathbb{Z})$, and consists of quasi-unipotent elements.

For $N \geq 1$, $\Gamma(N)$ acts regularly at the cusps precisely when $N \geq 3$, $\Gamma_1(N)$ does so precisely when $N \geq 5$, and $\Gamma_0(N)$ never does.

Let us now assume that Γ acts freely on $\mathbb{H}$, and regularly at the cusps. Then we already have $\underline{\omega}$ on $Y_\Gamma(\mathbb{C})$. We extend it to the neighborhood D of ∞ as follows. Note that dz on $\mathbb{H}$ is invariant under all $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$: $(\gamma \cdot)^* dz = dz$. This gives that $\underline{\omega}|_{D^*} = \mathcal{O}_{D^*} dz$. We extend $\underline{\omega}$ to D by deciding that our generating section dz on D^* has order 0 at ∞:

$$\underline{\omega}|_D = \mathcal{O}_D dz\,.$$

At the other cusps: use that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$.

Why did we do all this work? Well, to get that (still assuming Γ acts freely on $\mathbb{H}$ and regularly at the cusps):

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

that is, we can interpret these spaces of modular forms as spaces of global sections of holomorphic line bundles on compact Riemann surfaces.

Kodaira-spencer isomorphism

On $\mathbb{H}$, we have bases dz and $d\tau$ for the locally free $\mathcal{O}_\mathbb{H}$-modules $\underline{\omega}$ and $\Omega^1_\mathbb{H}$: $\underline{\omega} = \mathcal{O}_\mathbb{H}(dz)$ and and $\Omega^1_\mathbb{H} = \mathcal{O}_\mathbb{H} d\tau$. Now one may note that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ we have

$$(\gamma \cdot)^* d\tau = (c\tau + d)^{-2} d\tau, \quad \text{and} \quad (\gamma \cdot)^* (dz)^{\otimes 2} = (c\tau + d)^{-2} (dz)^{\otimes 2}\,.$$

Hence there is a $\mathrm{SL}_2(\mathbb{Z})$-equivariant isomorphism, called the Kodaira-Spencer isomorphism,

$$\underline{\omega}^{\otimes 2} \xrightarrow{\simeq} \Omega^1_\mathbb{H}\,, \qquad \left(\tfrac{dt}{t}\right)^{\otimes 2} \longmapsto \tfrac{dq}{q} = 2\pi i d\tau\,,$$

where $q = e^{2\pi i \tau}$ and $t = e^{2\pi i z}$. Note that $(\frac{dt}{t})^{\otimes 2} = (2\pi i)^2 (dz)^2$.

We have, for Γ acting freely on $\mathbb{H}$ and regularly at the cusps, the Kodaira-Spencer isomorphism between invertible $\mathcal{O}$-modules on $X_\Gamma(\mathbb{C})$:

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

For any $k \in \mathbb{Z}$ this gives us:

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

We deduce that $\deg(\underline{\omega}) > \deg(\Omega^1_{X_\Gamma}(\mathbb{C}))/2$, hence Riemann-Roch gives the dimension of $S_k(\Gamma)$ for $k \geq 2$, because the corresponding H^1 is zero by Serre duality and negative degree.

For Γ an arbitrary subgroup of finite index of $\mathrm{SL}_2(\mathbb{Z})$, and $N \geq 3$, let $\Gamma_N := \Gamma \cap \Gamma(N)$. Then Γ_N acts freely on $\mathbb{H}$, regularly at the cusps, is normal in Γ, and Γ/Γ_N is the image of Γ in $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Then we have, for every $k \in \mathbb{Z}$:

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

Eichler-Shimura isomorphism for $k = 2$

This isomorphism links spaces of modular forms to singular cohomology and hence also to cohomology of constant sheaves. It is given by the Hodge decomposition.

Assume that Γ acts freely on $\mathbb{H}$ and regularly at the cusps. We have seen that $S_2(\Gamma) = \mathrm{H}^0(X_\Gamma(\mathbb{C}), \Omega^1)$. We consider the de Rham resolution

$$\mathbb{C} \otimes \mathrm{H}^1(X_\Gamma(\mathbb{C}), \mathbb{Z}) = \mathbb{C} \otimes_{\mathbb{R}} \mathrm{H}^1\big(C^\infty_{\mathbb{R}}(X_\Gamma(\mathbb{C})) \to \text{real 1-forms} \to \text{real 2-forms}\big)\,.$$

Now $S_2(\Gamma)$ is the space of holomorphic 1-forms, hence closed 1-forms, so it maps to $\mathbb{C} \otimes \mathrm{H}^1(X_\Gamma(\mathbb{C}), \mathbb{Z})$. This map is injective because if $\omega = df$, then f is holomorphic, hence constant because $X_\Gamma(\mathbb{C})$ is compact and connected, and $\omega = 0$.

On $\mathbb{C} \otimes \mathrm{H}^1(X_\Gamma(\mathbb{C}), \mathbb{Z})$ we have $\iota \otimes \mathrm{id}$, with ι the complex conjugation. We denote the image of $S_2(\Gamma)$ under this by $\overline{S_2(\Gamma)}$. It consists of anti-holomorphic 1-forms. As $S_2(\Gamma) \cap \overline{S_2(\Gamma)} = \{0\}$, and both have $\mathbb{C}$-dimension g (the genus of $X_\Gamma(\mathbb{C})$) and $\mathrm{H}^1(X_\Gamma(\mathbb{C}), \mathbb{Z})$ is free as $\mathbb{Z}$-module of rank $2g$, we conclude that we have an isomorphism, called the Eichler-Shimura isomorphism:

$$\mathbb{C} \otimes \mathrm{H}^1(X_\Gamma(\mathbb{C}), \mathbb{Z}) = S_2(\Gamma) \oplus \overline{S_2(\Gamma)}\,.$$

The Jacobian of $X_\Gamma(\mathbb{C})$

For γ in $\mathrm{H}_1(X_\Gamma(\mathbb{C}), \mathbb{Z})$ (a 1-cycle, modulo boundaries of 2-cycles), and for ω in $S_2(\Gamma) = \Omega^1(X_\Gamma(\mathbb{C}))$, we have a well-defined integral $\int_\gamma \omega$. This gives an embedding

$$\mathrm{H}_1(X_\Gamma(\mathbb{C}), \mathbb{Z}) \hookrightarrow S_2(\Gamma)^\vee\,, \qquad \gamma \longmapsto \Big(\omega \mapsto \textstyle\int_\gamma \omega\Big)\,.$$

The the Jacobian of $X_\Gamma(\mathbb{C})$ is defined as

$$J_\Gamma(\mathbb{C}) := \Omega^1(X_\Gamma(\mathbb{C}))^\vee / \mathrm{H}_1(X_\Gamma(\mathbb{C}), \mathbb{Z}) = S_2(\Gamma)^\vee / \mathrm{H}_1(X_\Gamma(\mathbb{C}), \mathbb{Z})\,.$$

So, $S_2(\Gamma)$ is the tangent space at 0 of $J_\Gamma(\mathbb{C})$.

We also have the following description of $J_\Gamma(\mathbb{C})$:

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

$$\left(\omega \mapsto \textstyle\sum_i \int_\infty^{P_i} \omega\right) \longleftarrow P_1 + \cdots + P_d - d\infty$$

Hecke operators as endomorphisms of $J_\Gamma(\mathbb{C})$

Here it matters what kind of Γ we consider. For example, for $\Gamma(N)$ we would not get a commutative algebra of Hecke operators, as the group ring $\mathbb{Z}[\mathrm{SL}_2(\mathbb{F}_p)]$ would be part of it. So, we specialise to the congruence subgroups $\Gamma_1(N)$.

For $N \geq 1$, we define $X_1(N) := X_{\Gamma_1(N)}(\mathbb{C})$ as algebraic curve over $\mathbb{C}$ (just $\mathbb{C}$-points, Zariski topology, sheaf of regular functions $\mathcal{O}$; not (yet) as scheme). We recall that

$$Y_1(N) = \{(E,P) : E \text{ ell. curve } /\mathbb{C} \text{ and } P \text{ in } E \text{ of order } N\}/\cong\,.$$

We have an action of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ on $X_1(N)$ given explicitly by

$$\langle a \rangle (E,P) = a \cdot (E,P) = (E, aP)$$

for any $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. These automorphisms (and whatever they induce by functoriality) are called "diamond" operators (for the spape of the symbol). For example, the $\mathbb{C}$-vector space $S_2(\Gamma_1(N)) = \Omega^1(X_1(N))$ splits under the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ into a direct sum of eigenspaces

$$S_2(\Gamma_1(N)) = \bigoplus_\varepsilon S_2(\Gamma_1(N), \varepsilon)\,,$$

where the sum is over the characters $\varepsilon \colon (\mathbb{Z}/N\mathbb{Z})^\times) \to \mathbb{C}^\times$.

For any $n \geq 1$ we have a correspondence

$$T_n \colon (E,P) \longmapsto \textstyle\sum_{\substack{G \subset E \text{ of order } n \\ \text{and } \langle P \rangle \cap G = \{0\}}} (E/G, \bar{P})\,.$$

Note that for p prime, T_p has degree $p+1$ if $p \nmid N$ (it sends a divisor of degree d to a divisor of degree $(p+1)d$), and degree p otherwise.

Let $Y_1(N;n)$ be the modular curve whose points are isomorphism classes of (E,P,G) with E a complex elliptic curve, P in E of order N, and $G \subset E$ a subgroup of order n such that $\langle P \rangle \cap G = \{0\}$, and let $X_1(N;n)$ be its compactification. Then T_n is given by two morphisms s (source) and t (target):

$$X_1(N) \xleftarrow{\;s\;} X_1(N;n) \xrightarrow{\;t\;} X_1(N)$$

Then T_n sends a divisor D to $t_* s^* D$. It sends a divisor of degree 0 to a divisor of degree 0, and sends principal divisors to principal divisors. Therefore T_n induces

$$J_1(N) \xrightarrow{s^*} J_1(N;n) \xrightarrow{t_*} J_1(N), \qquad T_n = t_* s^*$$

Let $\mathbb{T}_N \subset \mathrm{End}(J_1(N))$ be the subring generated by all T_n and diamond operators. Note: $\mathrm{End}(J_1(N))$ is a finitely generated free $\mathbb{Z}$-module since it is contained in $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(X_1(N)), \mathbb{Z}))$.

Formulas on q-expansions show:

1. The pairing $(\mathbb{T}_N)_{\mathbb{C}} \times S_2(N) \to \mathbb{C}$ sending $(t, \omega) \mapsto a_1(t^*\omega)$ is perfect.
2. $S_2(N)^\vee$ is a free $(\mathbb{T}_N)_{\mathbb{C}}$-module of rank 1.
3. $S_2(N)$ is a free $(\mathbb{T}_N)_{\mathbb{C}}$-module of rank 1, use $(\omega, \eta) \mapsto \frac{i}{2} \int_{X_1(N)} \omega \cdot \bar{\eta}$.
4. $\mathrm{H}_1(X_1(N), \mathbb{Q})$ is a free $(\mathbb{T}_N)_{\mathbb{Q}}$-module of rank 2.

For l prime, $N \geq 1$, define $W_{N,l} := \mathbb{Q} \otimes (\varprojlim J_1(N)[l^n]) = \mathrm{H}_1(X_1(N), \mathbb{Q}_l)$. This is a free $(\mathbb{T}_N)_{\mathbb{Q}_l}$-module of rank 2.

Hecke operators, more conceptually

The above section on Hecke operators is not so inspiring: why precisely these correspondences, and why only for the $\Gamma_1(N)$'s? So here we explain in a few lines what is behind it.

On $\mathbb{H}$ we have the action of $\mathrm{GL}_2(\mathbb{Q})^+$. Even better, on $\mathbb{H}^\pm = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$ we have the action of $\mathrm{GL}_2(\mathbb{Q})$. For $k \geq 0$, $\mathrm{GL}_2(\mathbb{Q})$ acts on the union S_k of all $S_k(\Gamma)$, where Γ ranges over all congruence subgroups of $\mathrm{GL}_2(\mathbb{Z})$. For Γ a congruence subgroup, we have $S_k(\Gamma) = S_k^\Gamma$. So it makes sense to ask: for Γ a congruence subgroup of $\mathrm{GL}_2(\mathbb{Z})$, and for M a $\mathbb{Z}$-module with an action of $\mathrm{GL}_2(\mathbb{Q})$, what are the natural endomorphisms of M^Γ. In other words: what are the endomorphisms of the functor from $\mathbb{Z}[\mathrm{GL}_2(\mathbb{Q})]$-Mod to $\mathbb{Z}$-Mod, $M \mapsto M^\Gamma$? The answer is: the Hecke algebra $\mathbb{T}_\Gamma$. And what is this algebra? Well, the functor in question is representable:

$$M^\Gamma = \mathrm{Hom}_\Gamma(\mathbb{Z}, \mathrm{Res}_\Gamma^{\mathrm{GL}_2(\mathbb{Q})} M) = \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{Q})}(\mathrm{Ind}_\Gamma^{\mathrm{GL}_2(\mathbb{Q})} \mathbb{Z}, M)\,.$$

Hence, by Yoneda,

$$\mathbb{T}_\Gamma = \mathrm{End}_{\mathrm{GL}_2(\mathbb{Q})}(\mathrm{Ind}_\Gamma^{\mathrm{GL}_2(\mathbb{Q})} \mathbb{Z})\,.$$

With this knowledge, one can see that the choice of the $\Gamma_1(N)$ is motivated by the facts that they are sufficiently small to capture all congruence subgroups in the sense

$$\begin{pmatrix} n^{-1} & 0 \\ 0 & 1 \end{pmatrix} \Gamma(n) \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \supset \Gamma_1(n^2)\,,$$

and that their Hecke algebras are commutative. More precisely, there is the theory of newforms (Atkin, Lehner, Li).

5 Arithmetic moduli of elliptic curves

Definition 6. *Let S be a scheme. An elliptic curve over S is a proper smooth morphism $f: E \to S$ of relative dimension 1 with section $0: S \to E$ such that the geometric fibers are connected and of genus 1. Equivalently, locally on S, E/S is given by a Weierstrass equation in $\mathbb{P}^2_S$:*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

whose discriminant is a unit, and $0 = (0:1:0)$.

Let now S be any scheme, and $(f: E \to S, 0)$ be an elliptic curve. For every S-scheme $T \to S$ we have the base changed curve:

$$\begin{array}{ccc} E_T & \longrightarrow & E \\ {\scriptstyle 0_T}\uparrow\downarrow{\scriptstyle f_T} & & {\scriptstyle f}\downarrow\uparrow{\scriptstyle 0} \\ T & \longrightarrow & S \end{array}.$$

We consider the following functor, from Sch/S to Set, contravariant:

$$\mathrm{Pic}_{E/S}: \quad \mathrm{Sch}/S \to \mathrm{Set}, \quad T \mapsto \mathrm{Pic}(E_T)/f_T^*\mathrm{Pic}(T).$$

We remark that the section 0_T gives a decomposition $\mathrm{Pic}(E_T) = \ker(0_T^*) \oplus \mathrm{Pic}(T)$, so we could also have defined $\mathrm{Pic}_{E/S}(T)$ as $\ker 0_T^*: \mathrm{Pic}(E_T) \to \mathrm{Pic}(T)$.

For every $d \in \mathbb{Z}$ we have the subfunctor $\mathrm{Pic}^d_{E/S}$ of $\mathrm{Pic}_{E/S}$ such that $\mathrm{Pic}^d_{E/S}(T)$ is given by invertible $\mathcal{O}$-modules on E_T that are fibrewise of degree d. Then $\mathrm{Pic}_{E/S}$ is the coproduct of all $\mathrm{Pic}^d_{E/S}$.

Theorem 7. *The morphism (of functors) $E \to \mathrm{Pic}^1_{E/S}$ that sends, for T an S-scheme, P in $E(T)$ to the $[\mathcal{O}_{E_T}(P)]$, is an isomorphism.*

Here $\mathcal{O}_{E_T}(P)$ is the invertible $\mathcal{O}_{E_T}$-module of rational functions on E_T that may have a pole of order at most one at P (technically speaking, the image of P is a relative Cartier divisor, effective, of degree 1). It is the dual of the ideal sheaf of P defined by the short exact sequence

$$I_P \hookrightarrow \mathcal{O}_{E_T} \twoheadrightarrow P_*\mathcal{O}_T$$

This theorem is useful in 2 ways: first of all it tells us that $\mathrm{Pic}^1_{E/S}$ is represented by E itself. and secondly it gives us an S-groupscheme structure on E/S:

$$E \xrightarrow{\simeq} \mathrm{Pic}^1_{E/S} \xrightarrow{\simeq} \mathrm{Pic}^0_{E/S}$$

$$\mathcal{L} \longmapsto \mathcal{L} \otimes_{\mathcal{O}_{E_T}} I_{0_T}$$

It is not hard to deduce that any morphism $f: E_1 \to E_2$ between elliptic curves over a scheme S with $f(0_1) = 0_2$ is automatically a morphism of S-groupschemes.

Now do not panic because of the next definition: you do not need to know what a stack is, you will actually learn a lot about through this example.

Definition 8. *The stack* [Ell] *is the category with objects elliptic curves* $(f: E \to S, 0)$ *and with morphisms cartesian diagrams*

$$\begin{array}{ccc} E_1 & \longrightarrow & E_2 \\ {\scriptstyle 0_1}\uparrow\downarrow & \square & \downarrow\uparrow{\scriptstyle 0_2} \\ S_1 & \longrightarrow & S_2 \end{array}$$

We have the functor $[\mathrm{Ell}] \to (\mathrm{Sch})$ that sends $(E \to S)$ to S. This makes it into a kind of "sheaf of categories" on the category Sch with a suitable topology (Zariski, etale).

Fact: [Ell] has no final object (since, for example, $\pm 1 \in \mathrm{Aut}_S(E)$ for all E/S).

Let $N \geq 1$, then for any elliptic curve over S E/S, we have a "multiplication by N" map $N\cdot: E \to E$ which is finite locally free of rank N^2 and etale precisely when N is invertible on S.

For $N \geq 1$ we define the stack $[\Gamma_1(N)]_{\mathbb{Z}[1/N]}$ to be the category with objects elliptic curves $(f: E \to S, 0, P)$ with S a scheme over $\mathbb{Z}[1/N]$ and where $P \in E(S)$ is of order N in all fibers. The morphisms in $[\Gamma_1(N)]_{\mathbb{Z}[1/N]}$ are the cartesian diagrams

$$\begin{array}{ccc} E_1 & \longrightarrow & E_2 \\ {\scriptstyle P_1}\,{\scriptstyle 0_1}\uparrow\downarrow & \square & \downarrow\uparrow{\scriptstyle 0_2}\,{\scriptstyle P_2} \\ S_1 & \longrightarrow & S_2 \end{array}$$

Theorem 9 (Igusa)**.** *For* $N \geq 4, [\Gamma_1(N)]_{\mathbb{Z}[1/N]}$ *has a final object:*

$$\begin{array}{c} \mathbb{E} \\ \downarrow\uparrow{\scriptstyle 0}\ \mathbb{P} \\ Y_1(N)_{\mathbb{Z}[1/N]} \end{array}$$

where $Y_1(N)_{\mathbb{Z}[1/N]}$ *is a smooth affine curve over* $\mathbb{Z}[1/N]$ *with geometrically irreducible fibers, which can uniquely be compactified into a smooth proper curve:*

$$\begin{array}{ccccc} Y_1(N)_{\mathbb{Z}[1/N]} & \hookrightarrow & X_1(N)_{\mathbb{Z}[1/N]} & \hookleftarrow & \mathrm{cusps} \\ & \searrow & \downarrow & \swarrow_{\textit{finite etale}} & \\ & & \mathrm{Spec}(\mathbb{Z}[1/N]) & & \end{array}$$

Let $J_1(N)_{\mathbb{Z}[1/N]} := \mathrm{Pic}^0_{X_1(N)_{\mathbb{Z}[1/N]}}$. It is an abelian scheme over $\mathbb{Z}[1/N]$. The Hecke algebra $\mathbb{T}_N$ acts on it.

Then for all primes l, we have

$$W_{N,l} = \mathbb{Q} \otimes \left(\varprojlim J_1(N)(\overline{\mathbb{Q}})[l^n] \right),$$

which is a free $(\mathbb{T}_N)_{\mathbb{Q}_l}$-module of rank 2 with a natural action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Any choice of basis gives a Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_l} \mathrm{GL}_2((\mathbb{T}_N)_{\mathbb{Q}_l}).$$

The eigenform f gives us a ring morphism $\mathbb{T}_N \to K_f$, $T_n \mapsto a_n(f)$. Composition gives us the representation $\rho_{f,l}$ whose existence was promised:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_l} \mathrm{GL}_2((\mathbb{T}_N)_{\mathbb{Q}_l}) \xrightarrow{f} \mathrm{GL}_2(K_{f,l}).$$
$$\rho_{f,l}$$

We remark that $\rho_{f,l}$ is unramified at $p \nmid Nl$ because $p \neq l$ and $J_1(N)_{\mathbb{F}_p}$ is an abelian variety (more correctly: $J_1(N)_{\mathbb{Z}_p}$ is an abelian scheme over $\mathbb{Z}_p$). Now we want to prove that $\mathrm{tr}(\rho_{f,l}\mathrm{Frob}_p) = a_p(f)$ for $p \nmid Nl$. This result follows from the Eichler-Shimura relation

$$T_p = \mathrm{Frob} + \langle p \rangle \cdot V \quad \text{in} \quad \mathrm{End}_{\mathbb{F}_p}(J_1(N)_{\mathbb{F}_p}),$$

of which we will explain the meaning, and the proof of wich we take some time to sketch.

The fact that $J_1(N)_{\mathbb{Z}[1/N]}$ is an abelian scheme over $\mathbb{Z}[1/N]$ implies that every endomorphism of $J_1(N)_{\mathbb{Q}}$ extends over $\mathbb{Z}[1/N]$, uniquely, and that the reduction map from $\mathrm{End}_{\mathbb{Z}[1/N]}(J_1(N)_{\mathbb{Z}[1/N]})$ to $\mathrm{End}_{\mathbb{F}_p}(J_1(N)_{\mathbb{F}_p})$ is injective. In a diagram:

$$\mathrm{End}_{\mathbb{Q}}(J_1(N)_{\mathbb{Q}}) \xrightarrow{\simeq} \mathrm{End}_{\mathbb{Z}[1/N]}(J_1(N)_{\mathbb{Z}[1/N]}) \hookrightarrow \mathrm{End}_{\mathbb{F}_p}(J_1(N)_{\mathbb{F}_p}).$$

We want to understand the element T_p of $\mathrm{End}_{\mathbb{F}_p}(J_1(N)_{\mathbb{F}_p})$. We use that $J_1(N)_{\mathbb{F}_p} = \mathrm{Pic}^0(X_1(N)_{\mathbb{F}_p})$, and that T_p is given by the correspondence of p-isogenies:

$$\begin{array}{ccc} & X_1(N;p)_{\mathbb{F}_p} & \\ {\scriptstyle s}\swarrow & & \searrow{\scriptstyle t} \\ X_1(N)_{\mathbb{F}_p} & & X_1(N)_{\mathbb{F}_p}, \end{array}$$

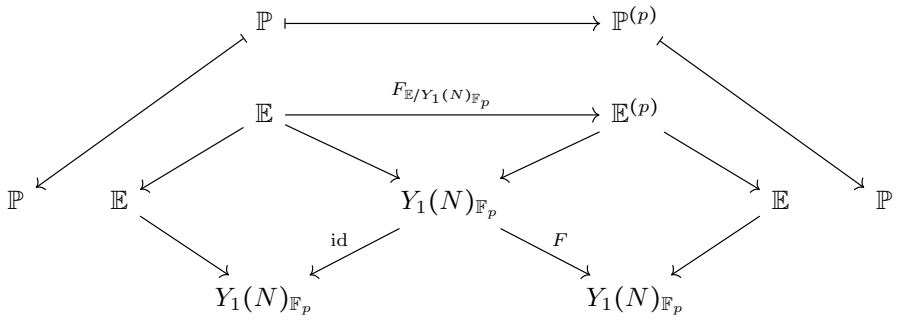
with s and t both finite locally free of rank p+1. Over an algebraically closed field k of characteristic p an ordinary elliptic curve E has $E[p] \cong \mu_{p,k} \times (\mathbb{Z}/p\mathbb{Z})_k$. This group scheme has precisely 2 subgroupschemes of rank p: the 2 factors. The quotient by $\mu_{p,k}$ is the relative Frobenius isogeny $F\colon E \to E^{(p)}$, given on coordinates as the p-power map, and where $E^{(p)}$ is given by the Weierstrass equation

with coefficients a_i^p, with a_i the coefficients of the equation for E. The quotient by $(\mathbb{Z}/p\mathbb{Z})_k$ is the isogeny $V\colon E \to E^{(1/p)}$ (equation with coefficients $a_i^{1/p}$). It is unique for the property that $FV = p\cdot$:

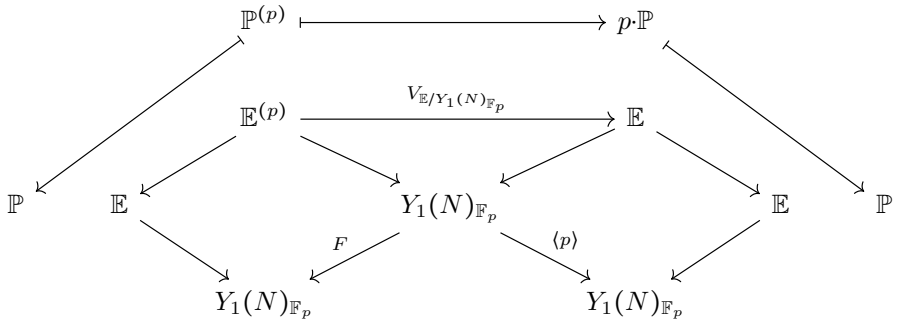
$$E \xrightarrow{V} E^{(1/p)} \xrightarrow{F} E\,, \qquad E \xrightarrow{p\cdot} E\,.$$

Apart from ordinary elliptic curves, there are only finitely many supersingular ones (about $p/12$). This explains that the curve $X_1(N;p)_{\mathbb{F}_p}$ has two irreducible components, meeting at the supersingular points. For the most basic case, that of $N = 1$, Kronecker already observed that the reduction over $\mathbb{F}_p$ of the polynomial $\Phi_p \in \mathbb{Z}[x,y]$ whose zero set is the image of $Y_0(p)$ in the product of the j-line with itself is $(x^p - y)(x - y^p)$.

Replacing $X_1(N;p)_{\mathbb{F}_p}$ by its normalisation $\widetilde{X_1(N;p)}_{\mathbb{F}_p}$ does not change the endomorphism T_p of $J_1(N)_{\mathbb{F}_p}$. The two irreducible components of $\widetilde{X_1(N;p)}_{\mathbb{F}_p}$ induce the following correspondences:



and



The first of these induces the endomorphism F of $J_1(N)_{\mathbb{F}_p}$, and the second induces $\langle p\rangle V$.

6 Construction of $\rho_{f,l}$ for $k \geq 2$

One can use congruences modulo powers of l with weight 2 forms of varying level $l^n N$ to construct $\rho_{f,l}$, but that does not, for example, give the Ramanujan conjecture. Thus, we want the construction in the cohomology.

Assume $N \geq 5$, then $\Gamma_1(N)$ acts freely on $\mathbb{H}$, regularly at the cusps. The universal elliptic curve (as complex manifold)

$$\begin{array}{ccc} \mathbb{E} & & \\ \downarrow{\scriptstyle p} & & \\ Y_1(N)(\mathbb{C}) & \overset{j}{\hookrightarrow} & X_1(N)(\mathbb{C}) \end{array}$$

gives the sheaf $(\mathrm{R}^1 p_*)\mathbb{Z}_{\mathbb{E}}$ on $Y_1(N)(\mathbb{C})$; it is a locally constant sheaf of free $\mathbb{Z}$-modules of rank 2. The $k-2$th symmetric power, and pushforward to $X_1(N)(\mathbb{C})$ give us

$$\mathcal{F}_k \coloneqq j_* \mathrm{Sym}^{k-2}((\mathrm{R}^1 p_*)\mathbb{Z}_{\mathbb{E}}) \quad \text{on } X_1(N)(\mathbb{C}).$$

As in the case of weight 2, there is an Eichler-Shimura isomorphism:

$$\mathbb{C} \otimes \mathrm{H}^1(X_1(N)(\mathbb{C}), \mathcal{F}_k) \xrightarrow{\simeq} S_k(N) \oplus \overline{S_k(N)}$$

This is a Hodge decomposition: $S_k(N)$ is of type $(k-1,0)$ and $\overline{S_k(N)}$ of type $(0,k-1)$ (see [BN81] for a nice exposition).

One can also embed $S_k(N)$ in $\mathrm{H}^{k-1}(\mathbb{E}^{k-2,*}, \mathbb{C})$ where $\mathbb{E}^{k-2}$ is the $k-2$ fold fiber product of $\mathbb{E} \to Y_1(N)(\mathbb{C})$, and $\mathbb{E}^{k-2,*}$ is a suitable non singular compactification of it over $X_1(N)(\mathbb{C})$. Then $f \in S_k(N)$ gives $f \cdot d\tau \cdot dz_1 \cdots dz_{k-2}$ on $\mathbb{H} \times \mathbb{C}^{k-2}$, then on $\mathbb{E}^{k-2}$ and then on $\mathbb{E}^{k-2,*}$.

As before, we have Hecke operators T_n and diamond operators $\langle a \rangle$ on the cohomology group $\mathrm{H}^1(X_1(N)(\mathbb{C}), \mathcal{F}_k)$, which is a finitely generated $\mathbb{Z}$-module. We let $\mathbb{T}_{N,k}$ be the subring of endomorphisms of $\mathbb{Q} \otimes \mathrm{H}^1(X_1(N)(\mathbb{C}), \mathcal{F}_k)$ generated by the T_n and $\langle a \rangle$; it is a free finitely generated $\mathbb{Z}$-module. Arguments similar to the weight 2 case show that $\mathbb{Q} \otimes \mathrm{H}^1(X_1(N)(\mathbb{C}), \mathcal{F}_k)$ is free of rank 2 over $\mathbb{T}_{N,k,\mathbb{Q}}$.

Let l be a prime. We define $\mathcal{F}_{k,l} \coloneqq j_* \mathrm{Sym}^{k-2}((\mathrm{R}^1 p_*)\mathbb{Q}_{l,\mathbb{E},et}$ where now $p : \mathbb{E}_{\mathbb{Q}} \to Y_1(N)_{\mathbb{Q}}$. Then $\mathcal{F}_{k,l}$ is an l-adic sheaf on $X_1(N)_{\mathbb{Q},et}$ and it extends well over $X_1(N)_{\mathbb{Z}[1/N]}$: "lisse" away from the cusps, and tamely ramified along the cusps.

We put $W_{N,k,l} \coloneqq \mathrm{H}^1(X_1(N)_{\overline{\mathbb{Q}},et}, \mathcal{F}_{k,l})^\vee$; this is free of rank 2 over $(\mathbb{T}_{N,k})_{\mathbb{Q}_l}$. By construction, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $W_{N,k,l}$: σ acts as $(\mathrm{id} \times \mathrm{Spec}(\sigma^{-1})^{*,\vee})$.

As in the weight 2 case, a basis of $W_{N,k,l}$ as $(\mathbb{T}_{N,k})_{\mathbb{Q}_l}$-module gives us the desired $\rho_{f,l}$:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_l} \mathrm{GL}_2((\mathbb{T}_{N,k})_{\mathbb{Q}_l}) \xrightarrow{f} \mathrm{GL}_2(K_{f,l})\,.$$

$$\rho_{f,l}$$

Unramifiedness and $\mathrm{tr}(\rho_{f,l}(\mathrm{Frob}_p)) = a_p(f)$ and $\det(\rho_{f,l}(\mathrm{Frob}_p)) = \varepsilon(p)p^{k-1}$ are proved, modulo technicalities, as before.

7 What about $\rho_{f,l,p}$ for $p|N$, $p \neq l$?

We want to understand the local Galois representations $\rho_{f,l,p} := \rho_{f,l}|_{G_{Q_p}}$ for $p|N$, $p \neq l$. The good question to ask is: in terms of what do we want to describe these local Galois representations? And the answer to that question is: in terms of the representation theory of $\mathrm{GL}_2(\mathbb{A}^\infty)$ (where $\mathbb{A}^\infty = \mathbb{Q} \otimes \hat{\mathbb{Z}} = \cup_{n\geq 1} n^{-1}\hat{\mathbb{Z}}$ is the $\mathbb{Q}$-algebra of finite adèles of $\mathbb{Q}$), using the formalism of Shimura varieties (don't panic, you do not need to know what a Shimura variety is, you just get a nice example in your hands, here).

The case $k \geq 2$ is not really harder than the case $k = 2$. So we only discuss $k = 2$.

We start with the Shimura datum $(\mathrm{GL}_{2,\mathbb{Q}}, \mathbb{H}^\pm)$, where $\mathbb{H}^\pm = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$, acted upon, transitively, by $\mathrm{GL}_2(\mathbb{R})$. Actually, we consider the $\mathrm{GL}_2(\mathbb{R})$-orbit in $\mathrm{Hom}(\mathbb{C}^\times, \mathrm{GL}_2(\mathbb{R}))$, on which $\mathrm{GL}_2(\mathbb{R})$ acts by post-composition with inner automorphisms, of

$$h_0 : a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

One easily checks that the stabiliser in $\mathrm{GL}_2(\mathbb{R})$ of h_0 is the same as the stabiliser of $i \in \mathbb{H}^\pm$, and that gives an isomorphism from the orbit of h_0 to that of i. In fact, we are now viewing $\mathbb{H}^\pm$ as the set of $\mathbb{R}$-Hodge structures on $\mathbb{R}^2$ of type $\{(-1,0),(0,-1)\}$.

For $K \subset \mathrm{GL}_2(\mathbb{A}^\infty)$ a open compact subgroup, we define

$$Y_K(\mathbb{C}) := \mathrm{GL}_2(\mathbb{Q}) \backslash \Big(\mathbb{H}^\pm \times \mathrm{GL}_2(\mathbb{A}^\infty)/K \Big).$$

As $\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}^\infty)/K$ is finite, $Y_K(\mathbb{C})$ is a finite disjoint union of quotients $\Gamma_i \backslash \mathbb{H}$. One compactifies by adding cusps, $X_K(\mathbb{C}) := Y_K(\mathbb{C}) \cup \text{cusps}$, a compact Riemann surface (not necessarily connected). We let $X_{K,\mathbb{C}}$ be the algebraic curve over $\mathbb{C}$ attached to $X_K(\mathbb{C})$. The interpretation as moduli space of elliptic curves gives a canonical model $X_{K,\mathbb{Q}}$ over $\mathbb{Q}$.

Example 10. *For $N \geq 1$ we define $K_N := \ker(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}))$. Then, for any $\mathbb{Q}$-scheme S, the set of S-points of $Y_{K_N,\mathbb{Q}}$ is the set of isomorphism classes of pairs $(E/S, \varphi)$, where E/S is an elliptic curve, and φ is an isomorphism from the constant group scheme $(\mathbb{Z}/N\mathbb{Z})^2_S$ to $E[N]$:*

$$Y_{K_N,\mathbb{Q}}(S) = \{(E/S,\varphi) : \varphi : (\mathbb{Z}/N\mathbb{Z})^2_S \xrightarrow{\sim} E[N]\}/\cong .$$

The $X_{K,\mathbb{Q}}$ form a filtered system: $K' \subset K$ gives a morphism $X_{K',\mathbb{Q}} \to X_{K,\mathbb{Q}}$. As these transition morphisms are finite, the limit exists as a scheme (colimit

of structure sheaves) profinite over the j-line:

$$X_{\mathbb{Q}} := \lim_K X_{K,\mathbb{Q}} \quad \circlearrowleft \quad \mathrm{GL}_2(\mathbb{A}^\infty)$$

The group $\mathrm{GL}_2(\mathbb{A}^\infty)$ acts on this limit because it acts on the system (that is precisely the reason why we do not only consider K that are contained in $\mathrm{GL}_2(\hat{\mathbb{Z}})$). This action is smooth in the sense that the stabiliser of every $\varphi \in \mathcal{O}_{X_{\mathbb{Q}}}(U)$ is open. From the limit we can recover the $X_{K,\mathbb{Q}}$: for each $K \subset \mathrm{GL}_2(\mathbb{A}^\infty)$ open compact, $X_{K,\mathbb{Q}} = X_{\mathbb{Q}}/K$. All Hecke correspondences can be described in terms of $X_{\mathbb{Q}}$ with its $\mathrm{GL}_2(\mathbb{A}^\infty)$-action.

For l prime we define

$$\mathrm{H}_l := \mathrm{colim}_K \, \mathrm{H}^1(X_{K,\overline{\mathbb{Q}},et}, \overline{\mathbb{Q}}_l) = \mathrm{colim}_K \left(\overline{\mathbb{Q}}_l \otimes_{\mathbb{Z}_l} \lim_n J_K(\overline{\mathbb{Q}})[l^n] \right)^\vee .$$

By construction, the $\overline{\mathbb{Q}}_l$-vector space has an action by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \times \mathrm{GL}_2(\mathbb{A}^\infty)$. We choose en embedding of $\overline{\mathbb{Q}}$ (defined as a subset of $\mathbb{C}$) into $\overline{\mathbb{Q}}_l$. From q-expansion formulas we get a decomposition:

$$\Omega^1(X_{\mathbb{Q}})(\mathbb{C}) \;\overset{=}{=}\; \mathrm{colim}_K \, \Omega^1(X_{K,\mathbb{Q}}(\mathbb{C})) \;\overset{=}{=}\; \oplus_f \pi_f \,,$$

where the direct sum is over the newforms of weight 2 of all levels, and where π_f is defined as follows. Let f be a newform on some $\Gamma_1(N)$, and let $p\colon X_{\mathbb{C}} \to X_1(N)_{\mathbb{C}}$ be the quotient morphism. Then we have p^*f in $\Omega^1(X_{\mathbb{Q}}(\mathbb{C}))$ and then V_f is the sub-$\mathbb{C}$-vector space of $\Omega^1(X_{\mathbb{Q}}(\mathbb{C}))$ generated by the $g{\cdot}p^*f$, $g \in \mathrm{GL}_2(\mathbb{A}^\infty)$, and π_f denotes the representation of $\mathrm{GL}_2(\mathbb{A}^\infty)$ on V_f.

Hodge decomposition at level K gives us:

$$\mathrm{H}^1(X_{K,\mathbb{Q}}(\mathbb{C}), \mathbb{C}) \;\overset{=}{=}\; \Omega^1(X_{K,\mathbb{Q}}(\mathbb{C})) \oplus \overline{\Omega^1(X_{K,\mathbb{Q}}(\mathbb{C}))} \,.$$

This implies that all π_f have multiplicity 2 in the colimit of all $\mathrm{H}^1(X_{K,\mathbb{Q}}(\mathbb{C}), \mathbb{C})$. We conclude that H_l decomposes as

$$\mathrm{H}_l = \bigoplus_f \rho_f^\vee \otimes \pi_f \,,$$

where f ranges over the newforms of weight 2 in $\Omega^1(X_{\overline{\mathbb{Q}}_l})$, and where ρ_f is as characterised by Theorem 1.

In a letter to Piatetski-Shapiro from 1973, [Del73], the following was proved.

Theorem 11 (Deligne)**.** *For all $p \neq l$, $\pi_{f,p}$ determines $\rho_{f,p}$.*

The ingredients of the proof are:

1. a good model over $\mathbb{Z}$ of $X_{\mathbb{Q}}$ (Drinfeld level structures),

2. vanishing cycle theory,

3. Serre-Tate theory at the supersingular points,

4. Jacquet-Langlands correspondence.

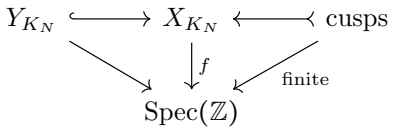
We will now briefly mention all of these things.

Models over $\mathbb{Z}$ (Katz-Mazur)

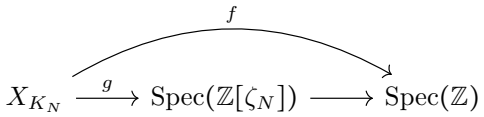
For $N \geq 1$ and E/S an elliptic curve over any base scheme, a Drinfeld level N structure on E/S is a $\varphi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E(S)$ such that

$$E[N] = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^2} \varphi(x)$$

as relative effective Cartier divisors on $E \to S$. A basic result that one can find in [KM85] is the following. For N divisible by at least 2 distinct prime powers both ≥ 3, the stack $[\Gamma(N)]$ has a final object $(\mathbb{E} \to Y_{K_N}, \varphi)$, with Y_{K_N} an affine curve over $\mathbb{Z}$, with a compactification



with Y_{K_N} affine, and f projective and X_{K_N} regular. The morphism f factors naturally (by the Weil pairing) as



The geometric fibers of g are connected. For p prime, writing $N = p^n N'$ with $p \nmid N'$, and $X_{K_N, \overline{\mathbb{F}}_p}$ obtained by a base change $\mathbb{Z}[\zeta_{N'}] \to \overline{\mathbb{F}}_p$, the irreducible components of $X_{K_N, \overline{\mathbb{F}}_p}$ are smooth, meeting all at all supersingular points, and the set of these irreducible components is in bijection with $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. So, if $n > 0$, this curve X_{K_N} over Spec($\mathbb{Z}[\zeta_N]$) is not stable at p. However, the fibres at p are reduced, and their singular points are precisely the supersingular points. The closed subscheme of X_{K_N} where the morphism g is not smooth consists of precisely the supersingular points over the primes dividing N.

Vanishing cycle theory

Here, for the details, see [Del73] or [Car86], or the more recent work of Scholze and Weinstein, or [EN01].

Let p be a prime, and let $N \geq 5$ be prime to p. Let K_N^1 be the inverse image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of the stabiliser of $\binom{1}{0}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let

$$X_N \coloneqq \lim_n X_{K_{p^n} \cap K_N}.$$

This X_N, where the level at p has gone to infinity and the level outside p is fixed, has an action by $\mathrm{GL}_2(\mathbb{Q}_p)$. We let

$$\mathrm{H}_{l,p} \coloneqq \mathrm{H}^1(X_{N,\overline{\mathbb{Q}}_p,et}, \overline{\mathbb{Q}}_l), \quad \text{it has an action by } \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \times \mathrm{GL}_2(\mathbb{Q}_p) \times \mathbb{T}'_N.$$

where $\mathbb{T}'_N$ is generated by T_n for $p \nmid n$ and the $\langle a \rangle$ for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. We consider the cohomology of the fiber at p:

$$\mathrm{H}^s_{l,p} \coloneqq \mathrm{H}^1(X_{N,\overline{\mathbb{F}}_p,et}, \overline{\mathbb{Q}}_l) \quad \text{action by same, } \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \text{ factors through } \mathbb{Z}_p^\times.$$

Then the vanishing cycle sequence is

$$\begin{array}{ccccccc} H^s_{l,p} & \hookrightarrow & H_{l,p} & \longrightarrow & \oplus_x \Psi_x & \twoheadrightarrow & \text{small cokernel from } \mathrm{H}^2, \\ & & & & \| & & \\ & & & & \Psi & & \end{array}$$

where the sum is over the singular points in $X_{N,\overline{\mathbb{F}}_p}$. Langlands determined $H^s_{l,p}$ in [Lan73]; the action of $\mathrm{GL}_2(\mathbb{Q}_p)$ is through non-cuspidal (induced from Borel) representations. For Ψ, wait and see.

Serre-Tate theory

The vanishing cycle space Ψ_x depends only on the $\mathcal{O}^\wedge_{X_{K_{n,N},x}}$, that is, on the deformation theory of $\mathbb{E}_x$, hence, only on the deformation theory of the p-divisible group $\mathbb{E}_x[p^\infty]$. Hence the automorphism group $\mathrm{Aut}(\mathbb{E}_x[p^\infty])$ acts on $\mathcal{O}^\wedge_{X_{K_{n,N},x}}$. This automorphism group is the unit group of the endomorphism ring, and so it is equal to $(\mathbb{Z}_p \otimes B)^\times$, where $B \coloneqq \mathrm{End}(\mathbb{E}_x)$ is a maximal order in $B_\mathbb{Q}$, the quaternion algebra "ramified" at p and ∞.

$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \times \mathrm{GL}_2(\mathbb{Q}_p) \times \mathbb{T}'_N$ and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \times \mathrm{GL}_2(\mathbb{Q}_p) \times B^\times_{\mathbb{Q}_p}$ act on Ψ. Now note that $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \times \mathrm{GL}_2(\mathbb{Q}_p) \times B^\times_{\mathbb{Q}_p}$ is the product of 3 local groups. As a representation of this, Ψ is a direct sum of finitely many copies of Deligne's "fundamental local representation," which decomposes as $\bigoplus_i \rho_i \otimes \pi_i \otimes \pi'_i$, with ρ_i, π_i and π'_i irreducible representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, $\mathrm{GL}_2(\mathbb{Q}_p)$, and $B^\times_{\mathbb{Q}_p}$, respectively.

Now isogenies of degree prime to p between the $\mathbb{E}_x$ induce isomorphisms between the completed local rings of $X_{K_{n,N}}$. This implies that $\mathbb{T}'_N$ act on Ψ as matrices with coefficients in $\overline{\mathbb{Q}_l}[B^\times_{\mathbb{Q}_p}]$, via $B^\times_\mathbb{Q} \subset B^\times_{\mathbb{Q}_p}$. A consequence: in each triple $\rho_i \otimes \pi_i \otimes \pi'_i$, π'_i determines π_i and ρ_i.

Jacquet-Langlands correspondence

Relates automorphic representations of the algebraic group $\underline{B}^\times$ to those of $\mathrm{GL}_{2,\mathbb{Q}}$). This is not so surprising (if one is sufficiently optimistic), as for all $l \neq p$, $\underline{B}^\times(\mathbb{Q}_l) = B^\times_{\mathbb{Q}_l}$ and $\mathrm{GL}_2(\mathbb{Q}_l)$ are isomorphic. In [JL70] Jacquet and Langlands pioneered this approach to modular forms. One of the consequences is that newforms for $\underline{B}^\times$ correspond to newforms on $\mathrm{GL}_{2,\mathbb{Q}}$), and that the image of this consists of the newforms on $\mathrm{GL}_{2,\mathbb{Q}}$) with a special behaviour at the places where B is ramified.

What has in fact happened in *this* story is that the geometry of the $X_{K_{n,N}}$ has provided an inverse of the Jacquet-Langlands correspondence: a newform f that contributes to Ψ gives a newform f' on $\underline{B}^\times$. One can express this in terms of automorphic representations (each $\pi_{f'}$ gives a π_f, this satisfies local rules, and the local map is injective), but the more classical Brandt matrices do the same (but give less information).

Anyway: the results of [JL70] give that in each triple $\rho_i \otimes \pi_i \otimes \pi_i'$, π_i determines π_i' and hence also ρ_i.

To conclude: $\pi_{f,p}$ determines $\rho_{f,p}$. At the unramified places this rule is what we saw (Eichler-Shimura congruence relation). At the ramified places this is more complicated, but for $p > 2$ wild intertia at p cannot act irreducibly and CM-forms plus class field theory tell us the rule. For $p = 2$ wild inertia at 2 can act irreducibly, the corresponding forms are called extraordinary, and base change was used by Carayol in [Car86] for deal with this. Later, Nyssen obtained a much simpler proof in [Nys99] via congruences with forms of weight 1.

Let us finish by mentioning that the local Langlands correspondence is characterised conceptually in terms of L-factors and (more importantly at the ramified places) ε-factors (constants in the functional equations). If I'm not mistaken, the only direct proof that the global correspondence in the cohomology of modular curves respects local L and ε-factors is by Colmez, using p-adic coefficients $p = l$, and indeed, in this situation one can sufficiently deform the action of wild inertia and get the required identities by "analytic continuation."

8 Computational aspects

Let us start with the good news: although this section comes after the very difficult Section 7, that section is not needed for what we want to do here.

What does it mean to compute a Galois representation? We tend to write such a representation as $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$, where V is finite dimensional vector space over some field. But the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \mathrm{Aut}(\overline{\mathbb{Q}})$ is too big, and so is $\overline{\mathbb{Q}}$. So, we only want to compute such representations that factor as

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \xhookrightarrow{\rho} \mathrm{GL}(V)\,,$$

with K a finite Galois extension of $\mathbb{Q}$, contained in $\overline{\mathbb{Q}}$, and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ is the map that restricts an automorphism to K. Then we can describe K as

$\mathbb{Q}[x]/(f)$, with f the minimal polynomial of a generator α of K. And each σ in $\mathrm{Gal}(K/\mathbb{Q})$ can be described as a matrix with coefficients in $\mathbb{Q}$, and $\rho(\sigma)$ can be described as a matrix with coefficients in k.

So we will not compute the l-adic Galois representations attached to eigenforms, because those do not have a finite image (well, unless the weight is 1). But we will compute the *residual* reprepsentations. So let f be an eigenform on some $\Gamma_1(N)$ and of some weight k, and with character ε, and let $\rho_{f,\lambda}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(E)$, with E a finite extension of $\mathbb{Q}_l$ be a Galois representation attached to it. The compactness of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ implies that after a suitable change of basis of E^2, $\rho_{f,\lambda}$ has values in $\mathrm{GL}_2(O_E)$, where O_E is the ring of integers of E. But then we can reduce ρ modulo the maximal ideal of O_E, which means that we consider the composition

$$\begin{array}{ccccc} & & \overset{\overline{\rho}_{f,\lambda}}{\frown} & & \\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_{f,\lambda}} & \mathrm{GL}_2(O_E) & \longrightarrow & \mathrm{GL}_2(\mathbb{F})\,, \end{array}$$

where $O_E \to \mathbb{F}$ is the map to the residue field. This $\overline{\rho}_{f,\lambda}$ factors through a finite Galois group:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\overline{\rho}_{f,\lambda}} \mathrm{GL}_2(\mathbb{F})\,,$$

and we ask ourselves how we can compute it.

Of course, the construction in Section 6 tells us how to do this: the representation $\rho_{f,\lambda}$ is realised by $J_1(N)(\overline{\mathbb{Q}})[l^\infty]$ (or its Tate-module) if $k = 2$, or in the dual of the l-adic etale cohomology group $\mathrm{H}^1(X_1(N)_{\overline{\mathbb{Q}},et}, \mathcal{F}_{k,l})$ if $k > 2$. Then we use the principle that algebraic geometry is so nice that almost everything in it that admits a finite description can be made explicit and even be computed. And indeed, there are results by Mumford that make abelian varieties explicit via theta functions, and results by Madore-Orgogozo and Jin that etale cohomology of constructible sheaves can be computed. But it is far from easy or even feasible to actually do such computations. A basic tool in computer algebra, Groebner basis computations, takes a lot of time (at least exponential in the number of variables).

Anyway, especially the appearance of etale cohomology seems to make it difficult. Fortunately, this is easily solved by congruences between modular forms: at the cost of replacing $\Gamma_1(N)$ by $\Gamma_1(Nl)$ (assuming $l \nmid N$, we get a modular form g on $\Gamma_1(Nl)$ of weight 2 such that g gives the same representation as $\overline{\rho}_{f,\lambda}$.

Let $\mathbb{T}_{Nl}$ be the weight 2 Hecke algebra, it is the subring of $\mathrm{End}(J_1(Nl)$ generated by the T_n and $\langle a\rangle$. Then g can be seen as a morphism of rings $\varphi_g\colon \mathbb{T}_{Nl} \to \mathbb{F}$ such that for all t in $\mathbb{T}_{Nl}$: $t^*g = \varphi_g(t)\cdot g$, it sends each Hecke operator to its eigenvalue on g. Let $m \coloneqq \ker(\varphi_g)$. Note that $l \in m$.

Under a mild multiplicity one assumption, our representation is realised by

$$V \coloneqq J_1(Nl)(\overline{\mathbb{Q}})[m] = \{x \in J_1(Nl)(\overline{\mathbb{Q}})[l] : \text{for all } t \in m,\ t(x) = 0.\}$$

In principle, everything here is explicit. One can describe the curve $X_1(Nl)$ as a cover of the j-line by computing the minimal polynomial over $\mathbb{Q}(j)$ of a generator of the function field. Then one can (theoretically) compute $J_1(Nl)$ as an abelian variety over $\mathbb{Q}$, or one can choose to work with the complex uniformisation of $J_1(Nl)(\mathbb{C})$. One can locate the points in V, and the field extension of $\mathbb{Q}$ generated by their coordinates. That's all.

Now to actually do this, one should see the work of Johan Bosman: [Bos11b], [Bos11a], [Bos07]. And that of Nicolas Mascot: [Mas18], [Mas13] (note that all this can be found on arxiv). And by Jinxiang Zhen and Linsheng Yin: [ZY15] and [Yi], and by Peng Tian: [Tia14].

And for the theoretical framework, even including a theorem that says that such computations can be done in polynomial time, and an application to the computation of coefficients of modular forms, see [EC11], and of course the work of Peter Bruin (where complex computations are replaced with computations over finite fields): [Bru11] and [Bru13]. For an introduction to this that gives ideas of how to do the computations, see [CE12].

9 Guide to the literature

I'm sorry for the horrible haste with which I finish this section. Hopefully I will get an opportunity to improve it, but the lectures almost start, and the organisers are at my heels.

A nice introduction is in [DS05], and at a slightly higher level, without proofs but with complete references in [DI95]. The book [EC11] gives a brief description, with references (often to [DI95]).

For modular curves, at a high technical level: [KM85], and [DR75].

For Weil-Deligne representations, how they are related to Local Langlands, and how one computes with this (even implemented in Magma and Sage): [LW12]. But see also [EN01], and appendix A in [Edi02].

For p-adic local Langlands, see [Col13], and the recent work of Scholze (and Weinstein), hopefully mentioned in Scholze's ICM lecture of this Summer [Sch17] (otherwise: use MathSciNet).

References

[BN81] Pilar Báyer and Jürgen Neukirch. "On automorphic forms and Hodge theory". In: *Math. Ann.* 257.2 (1981), pp. 137–155. ISSN: 0025-5831. DOI: 10.1007/BF01458280. URL: https://doi.org/10.1007/BF01458280.

[Bos07] Johan Bosman. "A polynomial with Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$". In: *LMS J. Comput. Math.* 10 (2007), pp. 1461–1570. ISSN: 1461-1570. DOI: 10.1112/S1461157000001467. URL: https://doi.org/10.1112/S1461157000001467.

[Bos11a] Johan Bosman. "Computations with modular forms and Galois representations". In: *Computational aspects of modular forms and Galois representations*. Vol. 176. Ann. of Math. Stud. Princeton Univ. Press, Princeton, NJ, 2011, pp. 129–157.

[Bos11b] Johan Bosman. "Polynomials for projective representations of level one forms". In: *Computational aspects of modular forms and Galois representations*. Vol. 176. Ann. of Math. Stud. Princeton Univ. Press, Princeton, NJ, 2011, pp. 159–172.

[Bru11] Peter Bruin. "Computing coefficients of modular forms". In: *Actes de la Conférence "Théorie des Nombres et Applications"*. Vol. 2011. Publ. Math. Besançon Algèbre Théorie Nr. Presses Univ. Franche-Comté, Besançon, 2011, pp. 19–36.

[Bru13] Peter Bruin. "Computing in Picard groups of projective curves over finite fields". In: *Math. Comp.* 82.283 (2013), pp. 1711–1756. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2012-02650-0. URL: https://doi.org/10.1090/S0025-5718-2012-02650-0.

[Car86] Henri Carayol. "Sur les représentations l-adiques associées aux formes modulaires de Hilbert". In: *Ann. Sci. École Norm. Sup. (4)* 19.3 (1986), pp. 409–468. ISSN: 0012-9593. URL: http://www.numdam.org/item?id=ASENS_1986_4_19_3_409_0.

[CE12] Jean-Marc Couveignes and Bas Edixhoven. "Approximate computations with modular curves". In: *Geometry and arithmetic*. EMS Ser. Congr. Rep. Eur. Math. Soc., Zürich, 2012, pp. 91–112. DOI: 10.4171/119-1/6. URL: https://arxiv.org/pdf/1205.5896.pdf.

[Col13] Pierre Colmez. "Le programme de Langlands p-adique". In: *European Congress of Mathematics*. Eur. Math. Soc., Zürich, 2013, pp. 259–284.

[Del73] P. Deligne. *Dear Piatetski-Shapiro*. 1973. URL: http://math.bu.edu/people/jsweinst/DeligneLetterToPiatetskiShapiro.pdf.

[DI95] Fred Diamond and John Im. "Modular forms and modular curves". In: *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*. Vol. 17. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[DR75] P. Deligne and M. Rapoport. "Les schémas de modules de courbes elliptiques (*Modular functions of one variable, II* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316, Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973)". In: (1975), p. 149. Lecture Notes in Math., Vol. 476.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pp. xvi+436. ISBN: 0-387-23229-X.

[EC11] Bas Edixhoven and Jean-Marc Couveignes, eds. *Computational aspects of modular forms and Galois representations*. Vol. 176. Annals of Mathematics Studies. How one can compute in polynomial time the value of Ramanujan's tau at a prime. Princeton University Press, Princeton, NJ, 2011, pp. xii+425. ISBN: 978-0-691-14202-9. DOI: 10.1515/9781400839001. URL: http://www.math.u-bordeaux1.fr/~couveign/publi/book.pdf.

[Edi02] Bas Edixhoven. "Rational elliptic curves are modular (after Breuil, Conrad, Diamond and Taylor)". In: *Astérisque* 276 (2002). Séminaire Bourbaki, Vol. 1999/2000, pp. 161–188. ISSN: 0303-1179.

[EN01] Bas Edixhoven and Jean-Baptiste Nortier. "lectures at the CRM, Bellaterra". In: (2001). URL: http://pub.math.leidenuniv.nl/~edixhovensj/talks/2001/crmedix.pdf.

[JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970, pp. vii+548.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*. Vol. 108. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 1985, pp. xiv+514. ISBN: 0-691-08349-5; 0-691-08352-5.

[Lan73] R. P. Langlands. "Modular forms and ℓ-adic representations". In: (1973), 361–500. Lecture Notes in Math., Vol. 349.

[LW12] David Loeffler and Jared Weinstein. "On the computation of local components of a newform". In: *Math. Comp.* 81.278 (2012), pp. 1179–1200. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2011-02530-5. URL: https://doi.org/10.1090/S0025-5718-2011-02530-5.

[Mas13] Nicolas Mascot. "Computing modular Galois representations". In: *Rend. Circ. Mat. Palermo (2)* 62.3 (2013), pp. 451–476. ISSN: 0009-725X. DOI: 10.1007/s12215-013-0136-4. URL: https://doi.org/10.1007/s12215-013-0136-4.

[Mas18] Nicolas Mascot. "Certification of modular Galois representations". In: *Math. Comp.* 87.309 (2018), pp. 381–423. ISSN: 0025-5718. DOI: 10.1090/mcom/3215. URL: https://doi.org/10.1090/mcom/3215.

[Nys99] Louise Nyssen. "Représentations extraordinaires". In: *Compositio Math.* 115.3 (1999), pp. 329–357. ISSN: 0010-437X. DOI: 10.1023/A:1000602707982. URL: https://doi.org/10.1023/A:1000602707982.

[Tia14] Peng Tian. "Computations of Galois representations associated to modular forms of level one". In: *Acta Arith.* 164.4 (2014), pp. 399–412. ISSN: 0065-1036. DOI: 10.4064/aa164-4-5. URL: https://doi.org/10.4064/aa164-4-5.

[Yi] In: ().

[ZY15] Jinxiang Zeng and Linsheng Yin. "On the computation of coefficients of modular forms: the reduction modulo p approach". In: *Math. Comp.* 84.293 (2015), pp. 1469–1488. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2014-02892-5. URL: https://doi.org/10.1090/S0025-5718-2014-02892-5.

[Sch17] P. Scholze. "p-adic geometry". In: *ArXiv e-prints* (Dec. 2017). arXiv: 1712.03708 [math.AG].