Modular forms and ℓ-adic representations

Contents

Chapter 1

Introduction

Let

$$D(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \quad (|q| < 1)$$

and

$$\Delta(z) = D(e^{2\pi i z}) \quad (\mathrm{Im}(z) > 0),$$

It is known that, up to a constant factor, the function Δ is the unique parabolic modular form of weight 12 for the group $SL_2(\mathbb{Z})$.

For a prime p, define

$$H_p(X) = 1 - \tau(p) X + p^{11} X^2.$$

According to Hecke's theory, the Dirichlet series

$$L_\tau(s) = \sum_{n=1}^{\infty} \tau(n) n^{-s} = \prod_{p \in P} \frac{1}{H_p(p^{-s})}$$

extends to an entire function of s, and the function

$$(2\pi)^{-s} \Gamma(s) L_\tau(s)$$

is invariant under $s \leftrightarrow 12 - s$.

Ramanujan's conjecture asserts that the roots of the polynomial H_p have absolute value $p^{-11/2}$ (i.e., $|\tau(p)| < 2p^{11/2}$).

These proven or conjectural properties are analogous to the conjectural properties of zeta functions of algebraic varieties over $\mathbb{Q}$. This suggests, as a first approximation, trying to interpret L_τ as the zeta function of such a variety.

For each prime ℓ, let K_ℓ be the largest extension of $\mathbb{Q}$ unramified outside ℓ, and for $p \neq \ell$, let F_p be the inverse of the Frobenius element φ_p in the Galois group $\mathrm{Gal}(K_\ell/\mathbb{Q})$. The latter is well-defined up to conjugation.

Translating this into terms of ℓ-adic cohomology, Serre conjectured the existence, for each ℓ, of a representation of $\mathrm{Gal}(K_\ell/\mathbb{Q})$ into a $\mathbb{Q}_\ell$-vector space V_ℓ of rank 2 such that for each $p \neq \ell$,

$$H_p(X) = \det(1 - F_p X; V_\ell).$$

Moreover, the representation V_ℓ should fall within the scope of the Weil conjectures, making Ramanujan's conjecture a special case of the latter.

This program was successfully carried out by Kuga-Shimura [4] in the analogous case of modular forms related to certain compact quotient subgroups of $SL_2(\mathbb{R})$. Reduced to the present case, the fundamental idea of Sato-Kuga-Shimura is as follows: if E is the universal elliptic curve over the moduli scheme S of elliptic curves (ignoring for now that it does not exist) and if E^k is the k-fold fiber product of E with itself over S, then $L_\tau(s)$ is essentially the zeta function of E^k for $k = 10 = 12 - 2$.

What follows explains how to resolve the difficulties created by the cusps and how to construct the representations V_ℓ with the properties indicated above. For more historical details and applications, we refer to Serre [6].

Notations

- Let $\mathbb{A}$ denote the ring of adeles of $\mathbb{Q}$, $\mathbb{A}^f$ the ring of "finite" adeles, the restricted product over all primes of the fields $\mathbb{Q}_p$, and for S a set of primes, define

$$\mathbb{A}^f_S = \prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p \subset \mathbb{A}^f.$$

For $S = \emptyset$, write $\hat{\mathbb{Z}} = \mathbb{A}^f_\emptyset$.

- If X is a topological space (or the étale site of a scheme) and G a set, denote by $\underline{G}$ the constant sheaf on X defined by G.

- Let $\mathbb{G}_a$ and $\mathbb{G}_m$ denote the additive and multiplicative groups, respectively.

- An elliptic curve is a one-dimensional abelian variety, in particular equipped with an origin.

- If $\mathcal{L}$ is an invertible sheaf and $n \in \mathbb{Z}$, denote by $\mathcal{L}^n$ its n-th tensor power.

- Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

- The symbol $\square$ marks the end of a proof or its absence.

Chapter 2

The Shimura Isomorphism

No. 2 - The Shimura Isomorphism

(2.1) An elliptic curve over a complex analytic space S is a proper and flat morphism of analytic spaces $f : E \to S$, equipped with a section e, whose fibers are elliptic curves. An elliptic curve over S admits a unique S-group law $\mu : E \times_S E \to E$ with identity section e. To an elliptic curve are associated:

(a) The invertible sheaf $\omega_E = e^*\Omega^1_{E/S}$. The relative Lie algebra $\underline{\mathrm{Lie}}_S(E)$ is the invertible sheaf ω^{-1}, dual to ω. We have $f_*\Omega^1_{E/S} \cong \omega$.

(b) The local system of free $\mathbb{Z}$-modules of rank 2 $R^1f_*\mathbb{Z}$. Set $T_{\mathbb{Z}}(E) = R^1f_*\mathbb{Z}^\vee$ and $T_{\mathbb{Q}}(E) = T_{\mathbb{Z}}(E) \otimes \mathbb{Q}$ (local system of the homology of E over S).

The exponential map defines an exact sequence of sheaves of sections:

$$0 \to T_{\mathbb{Z}}(E) \xrightarrow{\alpha} \omega^{-1} \to E \to 0,$$

so that the elliptic curve E is reconstructed from the map α.

The local system $\Lambda^2 R^1 f_*\underline{\mathbb{Z}} \cong R^2 f_*\underline{\mathbb{Z}}$ is canonically isomorphic to $\underline{\mathbb{Z}}$. An isomorphism between $\underline{\mathbb{Z}}^2$ and $R^1f_*\underline{\mathbb{Z}}$ is called *permitted* if it induces -1 on the second exterior powers.

Let $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$ denote the set of isomorphisms (of $\mathbb{R}$-vector spaces) between $\mathbb{R}^2$ and $\mathbb{C}$ that do *not* preserve the natural orientations of $\mathbb{R}^2$ and $\mathbb{C}$ (defined by $e_1 \wedge e_2 > 0$ and $1 \wedge i > 0$). Such a homomorphism is determined by its restriction to $\mathbb{Z}^2$, and we set

$$\mathrm{Hom}^+(\mathbb{Z}^2, \mathbb{C}) = \mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C}).$$

This space is endowed with the complex structure induced by its inclusion into the complex vector space $\mathrm{Hom}(\mathbb{Z}^2, \mathbb{C})$. Over this space, there exists a universal exact sequence:

$$0 \to \underline{\mathbb{Z}}^2 \xrightarrow{\alpha} \mathbb{G}_a \to E_0 \to 0.$$

PROPOSITION 2.2. (i) The functor associating to each analytic space S the set of isomorphism classes of elliptic curves E over S, equipped with isomorphisms $\omega_E \cong \mathbb{G}_a$ and $R^1f_*\mathbb{Z} \cong \mathbb{Z}^2$ (the latter being permitted), is represented by the analytic space $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$, endowed with the universal elliptic curve E_0.

(ii) The functor associating to each analytic space S the set of isomorphism classes of elliptic curves over S, equipped with a permitted isomorphism $R^1 f_* \underline{\mathbb{Z}} \cong \underline{\mathbb{Z}}^2$, is represented by the analytic space $X = \mathbb{C}^\times \backslash \mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$ (Poincaré upper half-plane).

(iii) The space $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$ is a principal homogeneous space with group $\mathbb{G}_m$ over X. □

We may also view X as the set of complex structures on $\mathbb{R}^2$. By (ii), it is equipped with a universal elliptic curve E_X, whose real cohomology local system is canonically isomorphic to $\underline{\mathbb{R}}^2$. Let ω be the invertible sheaf associated to E_X.

The coherent analytic sheaf $R^1 f_* \underline{\mathbb{R}} \otimes_{\mathbb{R}} \mathcal{O}_X$ is the sheaf of relative de Rham cohomology of E_X over X, fitting into an exact sequence (Hodge filtration):

$$0 \to \omega \to R^1 f_* \underline{\mathbb{R}} \otimes_{\mathbb{R}} \mathcal{O}_X \xrightarrow{q} \omega^{-1} \to 0$$

(since by Serre duality, $\omega^{-1} \cong R^1 f_* \mathcal{O}$).

The functorial description 2.2(ii) makes evident a right action of the group $SL_2(\mathbb{Z})$ on (X, E_X): for $\gamma \in SL_2(\mathbb{Z})$, to the elliptic curve E with $\alpha : \underline{\mathbb{Z}}^2 \to R^1 f_* \underline{\mathbb{Z}}$, associate $(E, \alpha \circ \gamma)$. Similarly, viewing X with $q : \underline{\mathbb{R}}^2 \otimes \mathcal{O}_X \cong R^1 f_* \underline{\mathbb{R}} \otimes_{\underline{\mathbb{R}}} \mathcal{O}_X \to \omega^{-1}$ as classifying complex structures on $\mathbb{R}^2$, we see a right action of $GL_2^+(\mathbb{R})$ on $(X, \underline{\mathbb{R}}^2, \omega, q)$.

(2.3) Choose a basis (x_1, x_2) of $\mathbb{R}^2$ such that $x_1 \wedge x_2 > 0$. A point $f : \mathbb{R}^2 \to \mathbb{C}$, modulo $\mathbb{C}^\times$, of X is parameterized by $z = f(x_1)/f(x_2)$ ($\mathrm{Im}(z) > 0$), and the map q identifies with:

$$q : \mathbb{R}^2 \to \mathbb{G}_a : a x_1 + b x_2 \mapsto a z + b.$$

This reveals a non-equivariant trivialization of ω^{-1} over X. Relative to this trivialization, a section $f(z)$ of ω^k on X is transformed by an element $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$ of $GL_2^+(\mathbb{R}^2)$ (matrix in the basis (x_1, x_2)) into:

$$f \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} (z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

From the identity:

$$dz = (cz + d)^2 d\left(\frac{az + b}{cz + d}\right) \cdot \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{-1},$$

we deduce that dz is a section of $\omega^{-2} \otimes \Omega^1_X$ invariant under $SL_2(\mathbb{R})$. This section is nowhere vanishing and defines an isomorphism of $SL_2(\mathbb{R})$-equivariant sheaves between ω^2 and Ω^1_X.

(2.4) Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$ with no elements of finite order and with finite volume quotient. It is known that the quotient space X/Γ identifies with a smooth projective curve $\overline{X/\Gamma}$ minus finitely many points. The group Γ acts without fixed points on X. The equivariant local system $\mathbb{R}^2$ on X, along with the equivariant exact sequence:

$$0 \to \omega \to \underline{\mathbb{R}}^2 \otimes_{\mathbb{R}} \mathcal{O}_X \xrightarrow{q} \omega^{-1} \to 0,$$

thus defines on X/Γ a local system U and an exact sequence:

(2.5)

$$0 \to \omega \to U \otimes_{\mathbb{R}} \mathcal{O}_{X/\Gamma} \to \omega^{-1} \to 0.$$

In the special case where $\Gamma \subset SL_2(\mathbb{Z})$, these structures are derived from the elliptic curve

E on X/Γ whose pullback is the equivariant elliptic curve E_X on X.

(2.6) The cusps of $\overline{X/\Gamma}$ are described as follows (see [9]):

(a) They correspond to conjugacy classes in Γ of non-trivial subgroups of Γ, maximal among subgroups consisting of unipotent elements.

(b) Let $\Gamma_0 \subset \Gamma$ be such a subgroup, and choose a basis (x_1, x_2) of $\mathbb{R}^2$ such that, in this basis, Γ_0 is represented by matrices:

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \qquad (n \in \mathbb{Z}).$$

Let z be the coordinate (2.3) on X defined by (x_1, x_2). There exists N such that the region $X_N = \{z | \operatorname{Im}(z) > N\}$ of X is disjoint from its conjugates under $\gamma \notin \Gamma_0$, so that $X_N/\Gamma_0 \hookrightarrow X/\Gamma$. The function $q = e^{2\pi i z}$ establishes an isomorphism between X_N/Γ_0 and the punctured disk $0 < |q| < e^{-2\pi N}$. If P_{Γ_0} is the cusp of $\overline{X/\Gamma} - X/\Gamma$ associated to Γ_0, this isomorphism extends to an isomorphism of a neighborhood of P_{Γ_0} with the disk $0 \le |q| < e^{-2\pi N}$.

By (2.3), sections of ω over X_N which are invariant under Γ_0 are identified with holomorphic periodic functions of period 1 on X_N. We still denote by ω the invertible sheaf on $\overline{X/\Gamma}$ extending ω such that near a cusp P_{Γ_0}, the section of ω over X_N/Γ_0 defined by the constant function 1 extends to an invertible section over $\overline{X_N/\Gamma_0}$.

(2.7) On $\overline{X/\Gamma}$, we have two invertible sheaves Ω^1 and ω, and an isomorphism φ (2.3) between their restrictions to X/Γ. From the formula:

$$dq = de^{2\pi i z} = 2\pi i e^{2\pi i z} dz = 2\pi i q \, dz,$$

it follows that the map:

$$\varphi : \Omega^1 \to \omega^2$$

extends to $\overline{X/\Gamma}$ and has a simple zero at each cusp.

DEFINITION 2.8. The space of parabolic automorphic forms of weight $k+2$, relative to Γ, is the space of global sections:

$$H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k).$$

By (2.7), this space also identifies with the space of global sections of ω^{k+2} that vanish at the cusps.

(2.9) Let U^k denote the k-th symmetric power of the local system U on $\overline{X/\Gamma}$. The map (2.5) induces a map:

$$\iota^k : \omega^k \to U^k \otimes_{\mathbb{R}} \mathbb{C},$$

and hence a map, still denoted by ι^k:

$$\iota^k : \Omega^1 \otimes \omega^k \to \Omega^1(U^k),$$

where $\Omega^1(U^k)$ is the sheaf of holomorphic differential forms on $\overline{X/\Gamma}$ with coefficients in U^k.

The de Rham resolution of $U^k \otimes_{\mathbb{R}} \mathbb{C}$:

$$0 \to U^k \otimes_{\mathbb{R}} \mathbb{C} \to U^k \otimes_{\mathbb{R}} \mathcal{O}_{X/\Gamma} \xrightarrow{d} U^k \otimes_{\mathbb{R}} \Omega^1 \to 0$$

induces a map:

$$\delta : H^0(X/\Gamma, \Omega^1(U^k)) \to H^1(X/\Gamma, U^k \otimes \mathbb{C}).$$

Furthermore, the cohomology space $H^1(X/\Gamma, U^k \otimes \mathbb{C})$ has a natural complex conjugation, so δ defines a conjugate-linear map $\overline{\delta}$ from the complex conjugate space of $H^0(X/\Gamma, \Omega^1(U^k))$ to $H^1(X/\Gamma, U^k \otimes \mathbb{C})$. This gives a map $sh_0 = \delta \cdot H^0(\iota^k) \oplus \overline{\delta} \cdot H^0(\iota^k)$:

$$sh_0 : H^0(X/\Gamma, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(X/\Gamma, \Omega^1 \otimes \omega^k)} \to H^1(X/\Gamma, U^k \otimes \mathbb{C}).$$

For any sheaf F on a space Y, denote by $\tilde{H}^i(Y, F)$ the image of the compactly supported cohomology $H^i_c(Y, F)$ in the ordinary cohomology $H^i(Y, F)$.

Theorem 4.2.6 of [9] is essentially equivalent to the following theorem (in loc. cit., k is assumed even, but the same proof works in general):

THEOREM 2.10 (Shimura [7]). There exists an isomorphism sh making the following diagram commute:

$$\begin{tikzcd}
H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \arrow[r, "sh"] \arrow[d, hook] & \tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \arrow[d, hook] \\
H^0(X/\Gamma, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(X/\Gamma, \Omega^1 \otimes \omega^k)} \arrow[r, "sh_0"] & H^1(X/\Gamma, U^k \otimes \mathbb{C})
\end{tikzcd}$$

We call sh the *Shimura isomorphism.*

(2.11) In the special case where Γ is a finite-index subgroup of $SL_2(\mathbb{Z})$, the elliptic curve E on X/Γ comes from a scheme of elliptic curves over the algebraic curve X/Γ (i.e., its modular invariant is meromorphic at infinity); it thus admits a Néron model $\overline{E}$ over $\overline{X/\Gamma}$. One can show that the fibers of $\overline{E}$ at the cusps are of multiplicative type, and that over the entire $\overline{X/\Gamma}$, we have $\omega = e^*\Omega^1_{\overline{E}/(\overline{X/\Gamma})}$.

In this case, $U = R^1 f_* \mathbb{Z} \otimes \mathbb{R}$, so the target of the Shimura isomorphism rewrites:

$$\tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \cong \tilde{H}^1(X/\Gamma, \mathrm{Sym}^k(R^1 f_* \underline{\mathbb{Z}})) \otimes_{\mathbb{Z}} \mathbb{C}.$$

Chapter 3

Hecke operators and fundamental ℓ-adic representations

No. 3 – Hecke Operators and the Fundamental Adjoint Representation.

(3.1) Recall (cf. [3]) that the category of ”locally constant” constructible $\mathbb{Z}_\ell$-sheaves (abbreviated as l.c.c.) on a scheme S consists of projective systems of sheaves $\{F_n\}$ on the étale site $S_{\text{ét}}$ satisfying:

(i) $\underline{F}_n$ is a locally constant sheaf of $\mathbb{Z}/(\ell^n)$-modules of finite type;

(ii) If $n \leq m$, then $\underline{F}_m \otimes \mathbb{Z}/(\ell^n) \simeq \underline{F}_n$.

The l.c.c. $\mathbb{Z}_\ell$-sheaves form a stack in abelian categories over S; the stack of l.c.c. $\mathbb{Q}_\ell$-sheaves is the quotient of this stack by the thick sub-stack of l.c.c. $\mathbb{Z}_\ell$-sheaves annihilated by a power of ℓ. We denote by $\otimes\mathbb{Q}_\ell$ the canonical functor from the category of l.c.c. $\mathbb{Z}_\ell$-sheaves to that of l.c.c. $\mathbb{Q}_\ell$-sheaves.

If S is connected with a geometric point s, the category of l.c.c. $\mathbb{Z}_\ell$-sheaves (resp. $\mathbb{Q}_\ell$-sheaves) on S is equivalent, via the ”Fiber at s” functor, to the category of continuous representations of the fundamental group $\pi_1(S, s)$ on a finite-type $\mathbb{Z}_\ell$-module (resp. a finite-rank $\mathbb{Q}_\ell$-vector space).

For a finite set T of primes, an l.c.c. A^T-sheaf consists of data: for each prime ℓ, a l.c.c. $\mathbb{Z}_\ell$-sheaf if $\ell \notin T$, and a l.c.c. $\mathbb{Q}_\ell$-sheaf if $\ell \in T$. For $T = \emptyset$, we speak of l.c.c. $\mathbb{Z}_\ell$-sheaves rather than l.c.c. A^T-sheaves.

For arbitrary T, the category of l.c.c. A^T-sheaves is the inductive limit of categories of l.c.c. $A^{T'}$-sheaves for finite $T' \subset T$. We set:

$$\underline{\mathbb{Z}}_\ell = \varprojlim \underline{\mathbb{Z}/(\ell^n)}, \quad \underline{\mathbb{Q}}_\ell = \underline{\mathbb{Z}}_\ell \otimes \mathbb{Q},$$
$$\underline{\widehat{\mathbb{Z}}} = \prod_\ell \underline{\mathbb{Z}}_\ell \quad \text{and} \quad \underline{\mathbb{A}}^f_T = \underline{\widehat{\mathbb{Z}}} \otimes \mathbb{A}^f_T.$$

The stack of elliptic curves up to isogeny over S is obtained by formally inverting isogenies in the stack of elliptic curves over S. Denote by $\otimes\mathbb{Q}$ the functor associating to an elliptic curve its underlying isogeny class. For S quasi-compact, we have

$$\mathrm{Hom}(E, F) \otimes \mathbb{Q} \simeq \mathrm{Hom}(E \otimes \mathbb{Q}, F \otimes \mathbb{Q}),$$

and for S normal, every elliptic curve up to isogeny over S underlies an elliptic curve over S.

(3.2) Let $f : E \to S$ be an elliptic curve over a scheme S. Define $T_\ell(E)$ as the projective system of kernels $E[\ell^n]$ of multiplication by ℓ^n in E, with transition maps $E[\ell^n] \to E[\ell^m]$ ($n \geq m$) given by multiplication by ℓ^{n-m}. Similarly for $\mathbb{G}_m$, set $T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(1)$. If ℓ is invertible on S, $T_\ell(E)$ and $\mathbb{Z}_\ell(1)$ are $\mathbb{Z}_\ell$-sheaves on S. Define $T_\infty(E)$ as the relative Lie algebra of E over S (the invertible sheaf dual to ω in (2.1(a))).

Assume S has characteristic 0. Define the $\widehat{\mathbb{Z}}$-sheaf $T_f(E)$ on S as the system of $T_\ell(E)$, and set $V_f(E) = T_f(E) \otimes \mathbb{A}^f$. For an isogeny $u : E \to F$, u induces isomorphisms $V_f(E) \to V_f(F)$ and $T_\infty(E) \to T_\infty(F)$; thus the functors V_f and T_∞ factor through the category of elliptic curves up to isogeny over S.

PROPOSITION 3.3. Let S be a scheme of characteristic 0, $\underline{E}_1(S)$ the category of elliptic curves over S, and $\underline{E}_2(S)$ the category of triples: an elliptic curve up to isogeny E over S, a $\widehat{\mathbb{Z}}$-sheaf T isomorphic to $\widehat{\underline{\mathbb{Z}}}^2$, and an isomorphism $\beta : V_f(E) \simeq T \otimes \mathbb{A}$. The functor $I : E \mapsto (E \otimes \mathbb{Q}, T_f(E), V_f(E) \sim T_f(E) \otimes \mathbb{A})$ from $\underline{E}_1(S)$ to $\underline{E}_2(S)$ is an equivalence of categories.

The question is local on S, which we may assume to be quasi-compact. If $f : E \to F$ is a morphism of elliptic curves over S, and if f is an isogeny, we have an exact sequence (3.4):

$$0 \to T_f(E) \to T_f(F) \to \mathrm{Ker}(f) \to 0.$$

A morphism f is divisible by n iff it annihilates the kernel $E[n]$, since multiplication by n on $E/E[n]$ is an isomorphism. By (3.4), this occurs iff $T_f(f)$ is divisible by n, showing that $\mathrm{Hom}_S(E, F)$ is the subgroup of $\mathrm{Hom}_S(E \otimes \mathbb{Q}, F \otimes \mathbb{Q})$ consisting of morphisms f where $V_f(f)$ maps $T_f(E)$ into $T_f(F)$. Thus I is fully faithful.

Let $X \in \mathrm{Ob}(E_2(S))$. Locally on S, X is defined by an elliptic curve up to isogeny $E \otimes \mathbb{Q}$ and a "lattice" T in $V_f(E)$ coinciding with $T_\ell(E)$ for almost all ℓ. For $q \in \mathbb{Q}$, $(E \otimes \mathbb{Q}, T)$ is isomorphic to $(E \otimes \mathbb{Q}, qT)$, allowing us to assume $T_f(E) \subset T$.

The quotient $K = T/T_f(E)$ is canonically isomorphic to a finite subgroup of E, and X is the image under I of E/K (cf. 3.4). □

COROLLARY 3.5. The functor F_1 (resp. F_1') associating to each scheme S of characteristic 0 the set of isomorphism classes of elliptic curves E over S equipped with an isomorphism $\alpha : T_f(E) \xrightarrow{\sim} \widehat{\underline{\mathbb{Z}}}^2$ (resp. and an isomorphism $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathbb{G}_a$) is isomorphic to the functor F_2 (resp. F_2') associating to S the set of isomorphism classes of elliptic curves up to isogeny F over S equipped with an isomorphism $\beta : V_f(F) \xrightarrow{\sim} (\mathbb{A}^f)^2$ (resp. and an isomorphism $\beta_\infty : T_\infty(F) \xrightarrow{\sim} \mathbb{G}_a$).

PROPOSITION 3.6. The functor F_1 (resp. F_1') is represented by a scheme $\mathcal{M}_\infty$ (resp. $\mathcal{M}'_\infty$) over $\mathbb{Q}$.

Let $n \geq 3$. The functor associating to each scheme S the set of isomorphism classes of elliptic curves equipped with an isomorphism $\alpha_n : E[n] \xrightarrow{\sim} (\mathbb{Z}/n)^2$ (resp. and $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$) is represented by an affine curve $\mathcal{M}_n$ (resp. an affine surface $\mathcal{M}'_n$) over $\mathrm{Spec}(\mathbb{Z}[1/n])$. For $n|m$, the morphism $\mathcal{M}_m \to \mathcal{M}_n$ defined by

$$(E, \alpha_m : E[m] \xrightarrow{\sim} (\mathbb{Z}/m)^2) \mapsto (E, \tfrac{n}{m}\alpha_m : E[n] \xrightarrow{\sim} (\mathbb{Z}/n)^2)$$

is finite étale over $\operatorname{Spec}(\mathbb{Z}[1/m])$, and we have

$$\mathcal{M}_\infty = \varprojlim_n \mathcal{M}_n.$$

The same procedure applies to represent F_1'.

(3.7) The scheme $\mathcal{M}_\infty$ (resp. $\mathcal{M}'_\infty$) carries a universal elliptic curve $f_\infty : \mathcal{E} \to \mathcal{M}_\infty$ (resp. $f'_\infty : \mathcal{E}_\infty \to \mathcal{M}'_\infty$) and an isomorphism $\alpha : T_f(\mathcal{E}) \xrightarrow{\sim} \hat{\mathbb{Z}}^2$ (resp. and $\alpha_\infty : T_\infty(\mathcal{E}_\infty) \xrightarrow{\sim} \mathbb{G}_a$).

By (3.5), $\mathcal{M}_\infty$ represents F_2 (resp. F_2'), which highlights a left action of the adelic group $\mathrm{GL}_2(\mathbb{A}^f)$ on $(\mathcal{M}_\infty, \mathcal{E}_\infty \otimes \mathbb{Q}, \alpha \otimes (\mathbb{A}^f)^2)$ (resp. $(\mathcal{M}_\infty, \mathcal{E}_\infty \otimes \mathbb{Q}, \alpha \otimes (\mathbb{A}^f)^2, \alpha_\infty)$), given on the functor, for $g \in \mathrm{GL}_2(\mathbb{A}^f)$ by:

$$g : (F, \beta : V_f(E) \xrightarrow{\sim} (\mathbb{A}^f)^2, \beta_\infty) \mapsto (F, g \circ \beta : V_f(E) \xrightarrow{\sim} (\mathbb{A}^f)^2, \beta_\infty).$$

Šafarevič first noted this fact.

Let Y be a scheme over $\mathbb{C}$, which is a projective limit of finite-type schemes Y_i over $\mathbb{C}$ with finite transition maps. The locally ringed space Y^{an}, as the projective limit of Y_i^{an}, depends only on Y and not on its representation as a projective limit. If Y is a scheme over $\mathbb{Q}$, which is a projective limit of finite-type schemes Y_i over $\mathbb{Q}$ with finite transition maps, set $Y^{\mathrm{an}} = (Y \otimes \mathbb{C})^{\mathrm{an}}$. This applies to $\mathcal{M}_\infty$ and $\mathcal{M}'_\infty$.

PROPOSITION 3.8. We have canonical isomorphisms:

$$\mathcal{M}'^{\mathrm{an}}_\infty \simeq \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times (\mathbb{A}^f)^2)/\mathrm{GL}_2(\mathbb{Q})$$

$$\mathcal{M}^{\mathrm{an}}_\infty \simeq \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times (\mathbb{A}^f)^2)/\mathrm{GL}_2(\mathbb{Q}),$$

or less canonically:

$$\mathcal{M}'^{\mathrm{an}}_\infty \simeq \mathrm{GL}_2(\mathbb{A})/\mathrm{GL}_2(\mathbb{Q}),$$

$$\mathcal{M}^{\mathrm{an}}_\infty \simeq K_\infty \backslash \mathrm{GL}_2(\mathbb{A})/\mathrm{GL}_2(\mathbb{Q}),$$

where K_∞ is the maximal compact subgroup at infinity plus real homotheties. These isomorphisms respect the $\mathrm{GL}_2(\mathbb{A}^f)$-action.

The notion of elliptic curves up to isogeny extends to complex analytic geometry. An isogeny $\varphi : E \to F$ induces an isomorphism φ^* between rational cohomology local systems, which allows to define the latter for a curve up to isogeny. For a complex analytic space S, using (2.1), giving an elliptic curve up to isogeny over S is equivalent to giving: an invertible sheaf T_∞, a local system $T_\mathbb{Q}$ of $\mathbb{Q}$-vector spaces, and a morphism $u : T_\mathbb{Q} \to T_\infty$ inducing pointwise isomorphisms between $T_\mathbb{Q} \otimes \mathbb{R}$ and T_∞.

Let n be an integer and K_n the kernel of the natural map $\prod \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/n)$.

Let G_1 be the functor associating to S the set of isomorphism classes of elliptic curves $f : E \to S$ over S equipped with isomorphisms $\varphi : \underline{\mathbb{Q}}^2 \xrightarrow{\sim} T_\mathbb{Q}(E)$, $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, and $\alpha_n : E[n] \xrightarrow{\sim} (\mathbb{Z}/n)^2$. As in (3.3), G_1 is isomorphic to the functor G_2 associating to S isogeny classes of elliptic curves E over S with $\varphi : \mathbb{Q}^2 \xrightarrow{\sim} T_\mathbb{Q}(E)$, $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, and an isomorphism $V_f(E) \xrightarrow{\sim} (\mathbb{A}^f)^2$ given locally over S up to the composition by an element of K_n. Such objects are determined by a composite map φ' (defined locally modulo K_n):

$$\varphi' : \mathbb{Q}^2 \xrightarrow{\varphi} T_{\mathbb{Q}}(E) \to T_\infty(E) \times V_f(E) \xrightarrow{\sim} \mathcal{O}_S \times (\mathbb{A}^f)^2,$$

we have

$$E = \mathcal{O}_S/\varphi'(\mathbb{Q}^2 \cap \varphi'^{-1}(T_\infty(E) \times T_f(E))) = \widehat{\mathbb{Z}}^2 \backslash \mathcal{O}_S \times (\mathbb{A}^f)^2/\varphi'(\mathbb{Q}^2),$$

so that (cf. 2.2) G_1 and G_2 are represented by

$$K_n \backslash \operatorname{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times (\mathbb{A}^f)^2).$$

Assuming now $n \geq 3$, so that $\mathrm{GL}_2(\mathbb{Q})$ acts freely on the previous space. The analytic space $\mathcal{M}_n^{\mathrm{an}}$ (resp. $\mathcal{M}_n'^{\mathrm{an}}$) represents the analogous functor ,in analytical geometry, of the functor that is represented by $\mathcal{M}_n$ (resp. $\mathcal{M}_n'$) because this functor X, is representable and the map $X \to \mathcal{M}_n^{\mathrm{an}}$ (resp. $X \to \mathcal{M}_n^{'\mathrm{an}}$) induces a bijection on the set of points with values in any finite rank $\mathbb{C}$-algebra.

Thus we get:

$$\mathcal{M}_n^{'\mathrm{an}} \simeq K_n \backslash \operatorname{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times (\mathbb{A}^f)^2)/\operatorname{GL}_2(\mathbb{Q}).$$

Similarly for $\mathcal{M}_n$, we obtain the first claim in (3.8) via passing to the projective limit of n.

A point x in $\operatorname{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times (\mathbb{A}^f)^2)/\operatorname{GL}_2(\mathbb{Q})$ corresponds to a "lattice" $L_x \subset \mathbb{C} \times (\mathbb{A}^f)^2$, and the curve corresponding to x is:

$$E_x \sim \widehat{\mathbb{Z}}^2 \backslash \mathbb{C} \times (\mathbb{A}^f)^2/L_x,$$

equipped with $V_f(E_x) \simeq L_x \otimes \mathbb{A}^f \simeq (\mathbb{A}^f)^2$. This easily yields the last claim in (3.8). □

Let $f_n : \mathcal{E} \to \mathcal{M}_n$ be the universal elliptic curve over $\mathcal{M}_n$. Fixing an integer k, we define:

DEFINITION 3.9. Let W (or ${}^kW$ if there is risk of ambiguity) be the $\mathbb{Q}$-vector space:

$$W = \varinjlim_n \tilde{H}^1(\mathcal{M}_n^{\mathrm{an}}, \operatorname{Sym}^k(R^1 f_{n*}\mathbb{Q})) = \varinjlim {}_nW.$$

This vector space does not depend on the universal elliptic curve (up to isogeny) $f_\infty : \mathcal{E} \to M_\infty$ so that, by transport of structure, it is endowed with a left action of $\mathrm{GL}_2(\mathbb{A}^f)$.

For a prime ℓ, the $\mathbb{Q}_\ell$-vector space $W_\ell = W \otimes \mathbb{Q}_\ell$ admits an algebraic definition via ℓ-adic cohomology over $\overline{\mathbb{Q}}$ deduced from extension of scalar of $\mathcal{M}_n$:

$$(3.10) \quad W_\ell = \varinjlim_n \tilde{H}^1(\mathcal{M}_n \otimes \overline{\mathbb{Q}}, \operatorname{Sym}^k(R^1 f_{n*}\mathbb{Q}_\ell)) = \varinjlim {}_nW_\ell,$$

endowed with a Galois action on W_ℓ and ${}_nW_\ell$.

Finally, the space $\mathcal{M}_n^{\mathrm{an}}$ is a disjoint union of quotients of the Poincaré upper half-plane by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Let ω be the invertible sheaf on $\mathcal{M}_n$ defined by $\mathcal{E}$. Shimura's theory (2.10) gives:

$$(3.11) \quad W_\infty = W \otimes \mathbb{C} = \varinjlim_n \left(H^0(\overline{\mathcal{M}}_n^{\mathrm{an}}, \Omega^1 \otimes \omega^k) \oplus H^0(\overline{\mathcal{M}}_n^{\mathrm{an}}, \overline{\Omega}^1 \otimes \omega^k) \right).$$

This decomposition of $W \otimes \mathbb{C}$ into two complex conjugate subspaces- one being the space of holomorphic parabolic modular forms of weight $k+2$–resembles a Hodge decomposition of type $(0, k+1) + (k+1, 0)$.

The adelic action commutes with the Galois action and preserves this decomposition.

Though the ℓ-adic local system $R^1 f_{n*}\underline{\mathbb{Q}_\ell}$ is trivial on $\mathcal{M}_\infty$, I do not know if W_ℓ relates to $\varinjlim_n \left(\tilde{H}^1(\mathcal{M}_n \otimes \overline{\mathbb{Q}}, \underline{\mathbb{Q}_\ell}) \otimes \mathrm{Sym}^k(\mathbb{Q}_\ell^2)\right)$.

(3.12) For $n \geq 3$ and K_n as in (3.8), we have $W^{K_n} = {}_nW$. This is verified by passing to the limit, and results from the fact that in rational cohomology, the cohomology of a quotient of a space by a finite group is obtained by taking the invariants of this group in the cohomology.

Let, for p prime, $W^{(p)} = W^{\mathrm{GL}_2(\mathbb{Z}_p)}$. By passing to the limit,we get

$$W^{(p)} = \varinjlim_{(n,p)=1} {}_nW.$$

This cohomology space carries actions by:

(i) The subgroup $\prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{Q}_\ell) \subset \mathrm{GL}_2(\mathbb{A}^f)$, centralizing $\mathrm{GL}_2(\mathbb{Z}_p)$;

(ii) The Hecke algebra $\underline{H}(\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p))$, algebra of integer measures on the discrete space $\mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p)$ left-invariant under action by $\mathrm{GL}_2(\mathbb{Z}_p)$: This sub-algebra of the group algebra $\mathrm{GL}_2(\mathbb{Q}_p)$ acts on W in accordance with $W^{(p)}$. This algebra already acts on each ${}_nW$ for every n prime to p.

The Hecke algebra has a basis of (measures associated to characteristic functions) double cosets of $\mathrm{GL}(\mathbb{Z}_p)$ in $\mathrm{GL}(\mathbb{Q}_p)$, and we know that

$$\underline{H}(\mathrm{GL}(\mathbb{Q}_p), \mathrm{GL}(\mathbb{Z}_p)) = \mathbb{Z}[T_p, R_p, R_p^{-1}],$$

where T_p and R_p correspond to the double cosets of $\begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix}$ and $\begin{pmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{pmatrix}$.

(3.13) For a prime p, integer $n \geq 3$ coprime to p, define $F_{n,p}$ as the functor that associates to a scheme S the set of isomorphism classes of commutative diagrams of S-schemes:

$$\begin{tikzcd} & (\underline{\mathbb{Z}}/n)^2 & \\ E[n] \arrow[ur, "\alpha"] \arrow[rr] \arrow[d, hook] & & F[n] \arrow[ul, "\alpha'"'] \arrow[d, hook] \\ E \arrow[rr, "\varphi"] & & F \end{tikzcd} \tag{3.14}$$

where φ is a p-isogeny between elliptic curves and α is an isomorphisms. Let $q_1, q_2 : F_{n,p} \to \mathcal{M}_n$ be the morphism of functors that associates to a diagram (3.14) the subdiagram (E, E_n, α), or (F, F_n, α').

PROPOSITION 3.15. The functor $F_{n,p}$ is represented by a scheme $\mathcal{M}_{n,p}$, with $q_1, q_2 : \mathcal{M}_{n,p} \to \mathcal{M}_n$ finite.

The automorphism σ of $F_{n,p}$ swapping $\varphi : E \to F$ and ${}^t\varphi : F \to E$ exchanges q_1 and q_2. It suffices then to consider q_1. This morphism identifies $F_{n,p}$ with the functor of subgroups of order p of the universal elliptic curve $\mathcal{E}$ over $\mathcal{M}_n$, such that, by the theory of Hilbert schemes, $F_{n,p}$ is representable and $\mathcal{M}_{n,p}$ is proper over $\mathcal{M}_n$. If s is a geometric point of $\mathcal{M}_n$, $q_1^{-1}(s)$ is the set of subgroups of order p of E_s, and has $p+1$ elements if $\operatorname{char}(k(s)) \neq p$, has one element (the kernel of Frobenius) if $\operatorname{char}(k(s)) = p$. □

One can show that $M_{n,p}$ is regular, and that q_1 and q_2 are finite and flat; We do not use this delicate result,contenting ourselves here to note that over $\operatorname{Spec}(\mathbb{Z}[1/p])$, each q_i becomes étale of degree $p+1$ on $\mathcal{M}_n$.

These morphisms $q_i(i = 1, 2)$ fit into a commutative diagram:

$$\begin{tikzcd}
 & q_1^*\mathcal{E} \arrow[rr, "\varphi"] \arrow[dl] \arrow[dr, "u"'] & & q_2^*\mathcal{E} \arrow[dl, "v"] \arrow[dr] & \\
\mathcal{E} \arrow[dr, "f_n"'] & & \mathcal{M}_{n,p} \arrow[dl, "q_1"'] \arrow[dr, "q_2"] & & \mathcal{E} \arrow[dl, "f_n"'] \\
 & \mathcal{M}_n & & \mathcal{M}_n &
\end{tikzcd} \tag{3.16}$$

where (φ, u, v) is a part of universal diagram (3.14).

Let I_p denote the endomorphism of $\mathcal{M}_n$ induced by $(E, \alpha) \mapsto (E, \alpha/p)$:

$$I_p^*(E, \alpha) = (E, \alpha/p),$$

$$\begin{tikzcd}
\mathcal{E} \arrow[r] \arrow[d] & \mathcal{E} \arrow[d] \\
\mathcal{M}_n \arrow[r, "I_p"] & \mathcal{M}_n
\end{tikzcd} \tag{3.17}$$

I_p^* is an automorphism of $\tilde{H}^i(\mathcal{M}_n^{\mathrm{an}}, \operatorname{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}))$.

It is tedious but routine to show that

PROPOSITION 3.18.

(i) The Hecke operator T_p on W_n is expressed, with the help of (3.16), as the composite map

$$\tilde{H}^1(\mathcal{M}_n^{\mathrm{an}}, \operatorname{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}})) \xrightarrow{q_2^*} \tilde{H}^1(\mathcal{M}_{n,p}^{\mathrm{an}}, \operatorname{Sym}^k(R^1 v_*\underline{\mathbb{Q}}))$$

$$\xrightarrow{\qquad\qquad\varphi^*\qquad\qquad} \tilde{H}^1(\mathcal{M}_n^{\mathrm{an}}, \operatorname{Sym}^k(R^1 u_*\underline{\mathbb{Q}})) \xrightarrow{q_{1*}} \tilde{H}^1(\mathcal{M}_n^{\mathrm{an}}, \operatorname{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}}))$$

where q_{1*} is the ”trace map” for the covering q_1.

(ii) Similarly, $R_p = p^k I_p^*$. □

The suspicious reader might forget about the adelic preliminaries and define T_p by (i).

For $n = 1$ or 2, set ${}_nW = W^{K_n}$, so that

$${}_1W = {}_nW^{\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})}.$$

Let S_{k+2} denote the space of parabolic modular forms of weight $k+2$ for $\mathrm{SL}_2(\mathbb{Z})$. Shimura's isomorphism (3.11) gives:

$${}_1^kW_\infty = {}_1^kW \otimes \mathbb{C} = S_{k+2} \oplus \overline{S_{k+2}}.$$

It is tedious but routine to show that

PROPOSITION 3.19.- The Hecke operator T_p on ${}^k_1W_\infty$ corresponds under Shimura's isomorphism to the direct sum of T_p on S_{k+2} (including p^{k-1} factor) and its conjugate. □

(3.20) We have canonically:

$$\Lambda^2 R^1 f_{n*}\underline{\mathbb{Z}}_\ell \simeq R^2 f_{n*}\underline{\mathbb{Z}}_\ell \simeq \underline{\mathbb{Z}}_\ell(-1),$$

endowing $\mathrm{Sym}^k(R^1 f_{n*}\mathbb{Z}_\ell)$ with a bilinear form (symmetric/alternating for k even/odd) valued in $\underline{\mathbb{Z}}_\ell(-k)$. The form that is induced by tensoring with $\mathbb{Q}_\ell$ is nondegenerate.

If $\underline{F}$ is a l.c.c $\mathbb{Q}_\ell$ sheaf on a scheme X smooth purely of dimension n on an algebraically closed field k, then the Poincaré duality gives

$$\begin{aligned} H^i(X,\underline{F})^\vee &\simeq H_c^{2n-i}(X,\underline{\mathrm{Hom}}(\underline{F},\underline{\mathbb{Q}}_\ell(n))) \\ H_c^i(X,\underline{F})^\vee &\simeq H^{2n-i}(X,\underline{\mathrm{Hom}}(\underline{F},\underline{\mathbb{Q}}_\ell(n))) \\ \text{from which}\quad \tilde{H}^i(X,\underline{F})^\vee &\simeq \tilde{H}^{2n-i}(X,\underline{\mathrm{Hom}}(\underline{F},\underline{\mathbb{Q}}_\ell(n))). \end{aligned}$$

Take $X = \overline{\mathcal{M}}_n$ and $\underline{F} = \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}}_\ell)$ into consideration, we define a nondegenerate bilinear form ${}_n(\ ,\ )$ on ${}^k_nW_\ell$ with value in $\mathbb{Q}_\ell(-k-1)$. This form is symmetric for odd k, alternative for even k. This is the ℓ-adic analogue of Petersson scalar product. For $n|m$ with covering $\psi : \mathcal{M}_m \to \mathcal{M}_n$ of degree d, we have:

$${}_m(\psi^* x, \psi^* y) = d \cdot {}_n(x, y).$$

Chapter 4

The congruence formula

No. 4 – The Congruence Formula.

We fix in this section integers $k \geq 0$ and $n \geq 3$, and prime numbers p and ℓ. We assume that p is prime to n and to ℓ. Let $f : \mathcal{E} \to \mathcal{M}_n$ be the universal elliptic curve on $\mathcal{M}_n$, equipped with $\alpha : \mathcal{E}[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

For any scheme Y, we denote by a the unique morphism from Y to $\mathrm{Spec}(\mathbb{Z})$, or, if appropriate, to a subscheme of $\mathrm{Spec}(\mathbb{Z})$. If Y is separated and of finite type over $\mathrm{Spec}(\mathbb{Z})$ and if $\underline{F}$ is a $\mathbb{Z}_\ell$- or $\mathbb{Q}_\ell$-sheaf on Y, we denote by $R^i a_*(Y, \underline{F})$ (resp. $R^i a_!(Y, \underline{F})$) the ith direct image (resp. the ith direct image with proper support, resp. $\mathrm{Im}(R^i a_!(Y, \underline{F}) \to R^i a_*(Y, \underline{F}))$) of $\underline{F}$ by a.

We set, for an integer m, $Y[m] = Y \times \mathrm{Spec}(\mathbb{Z}[1/m])$.

THEOREM 4.1 (Igusa [1]). - The scheme $\mathcal{M}_n$ can be compactified into a curve scheme $\mathcal{M}_n^*$, projective and smooth over $\mathrm{Spec}(\mathbb{Z}[1/n])$, such that $\mathcal{M}_n^* \backslash \mathcal{M}_n$ is an étale cover of $\mathrm{Spec}(\mathbb{Z}[1/n])$.

The scheme $\mathcal{M}_n$ is formally smooth, thus smooth over $\mathrm{Spec}(\mathbb{Z})$.

The modular invariant j of the universal curve on $\mathcal{M}_n$ defines a morphism

$$j : \mathcal{M}_n \longrightarrow \mathbb{A}^1_{\mathrm{Spec}(\mathbb{Z}[1/n])}.$$

over $\mathrm{Spec}(\mathbb{Z}[1/n])$.

This morphism j is finite and is an étale covering outside the sections 0 and 1728 of $\mathbb{A}^1$; indeed:

(a) Two elliptic curves over an algebraically closed field with the same j-invariant are isomorphic (e.g., [8] 6.3), so that the geometric fibers of j are finite. Since the schemes $\mathcal{M}_n$ and $\mathbb{A}^1$ are smooth of the same relative dimension over $\mathrm{Spec}(\mathbb{Z})$, j is quasi-finite and flat.

(b) If E is an elliptic curve over the field of fractions K of a discrete valuation ring R, with $j \in R$ and whose n-torsion points are rational over K, then E has good reduction. The valuative criterion of properness then shows that j is proper.

(c) If E and F are two elliptic curves over a scheme S with the same j-invariant, and if j and $j - 1728$ are invertible, then the scheme $\mathrm{Isom}(S; E, F)$ of isomorphisms between E

and F is étale over S (see [8] 6.3). In the diagram

$$\begin{tikzcd}
\underline{\mathrm{Isom}}(\mathcal{M}_n \times_{\mathbb{A}^1} \mathcal{M}_n; \mathrm{pr}_1^*\mathcal{E},\ \mathrm{pr}_2^*\mathcal{E}) \arrow[r, "\simeq"] \arrow[d] & \mathcal{M}_n \times \mathrm{GL}_2(\mathbb{Z}/n) \arrow[d] \\
\mathcal{M}_n \times_{\mathbb{A}^1} \mathcal{M}_n \arrow[r, "\mathrm{pr}_1"] & \mathcal{M}_n
\end{tikzcd}$$

where $j \neq 1, 1728$ and where u and v are surjective étale, the projection pr_1 is étale and, by faithfully flat descent, j is étale.

The section at infinity of the projective line $\mathbb{P}^1_{\mathrm{Spec}(\mathbb{Z}[1/n])} \supset \mathbb{A}^1_{\mathrm{Spec}(\mathbb{Z}[1/n])}$ over $\mathrm{Spec}(\mathbb{Z}[1/n])$ is a regular divisor, with generic point of characteristic 0, in a regular scheme. It then follows from a theorem of Abyankhar (see [5]) that, along this divisor $j = \infty$, the scheme $\mathcal{M}_n$ is tamely ramified over $\mathbb{P}^1$, and that the normalization $\mathcal{M}_n^*$ of $\mathbb{P}^1$ in $\mathcal{M}_n$ satisfies (4.1).□

From the same theorem, it follows that the $\mathbb{Z}_\ell$-sheaves l.c.c. on $\mathcal{M}_n[1/\ell]$ are tamely ramified at infinity. Hence, from (4.1) and from the specialization theorems in ℓ-adic cohomology (see [5]), it follows that $R^i a_*(\mathcal{M}_n, \mathrm{Sym}^k(R^1 f_* \mathbb{Z}_\ell))$, $R^i a_!(\mathcal{M}_n, \mathrm{Sym}^k(R^1 f_* \mathbb{Z}_\ell))$ and thus $R^i \tilde{a}(\mathcal{M}_n, \mathrm{Sym}^k(R^1 f_* \mathbb{Z}_\ell))$ are $\mathbb{Z}_\ell$-adic sheaves l.c.c. on $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$, whose formation is compatible with any base change.

COROLLARY 4.2. - The Galois module ${}_nW_\ell$ is isomorphic to the fiber at the geometric point $\overline{\mathbb{Q}}$ of $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$ of the l.c.c $\mathbb{Q}_\ell$-sheaf $R^i \tilde{a}(\mathcal{M}_n, \mathrm{Sym}^k(R^1 f_* \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell)$. It is unramified outside of n and ℓ.

Consider, over $\mathcal{M}_n \otimes \mathbb{F}_p$, the two commutative diagrams

$$\begin{tikzcd}
 & (\mathbb{Z}/n)^2 & \\
E_n \arrow[ur, "\alpha"] \arrow[rr] \arrow[d] & & E_n^{(p)} \arrow[ul, "\alpha^{(p)}"'] \arrow[d] \\
E \arrow[rr, "F"] & & E^{(p)}
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
 & (\mathbb{Z}/n)^2 & \\
E_n^{(p)} \arrow[ur, "p\cdot\alpha^{(p)}"] \arrow[rr] \arrow[d] & & E_n \arrow[ul, "\alpha"'] \arrow[d] \\
E^{(p)} \arrow[rr, "V"] & & E
\end{tikzcd}$$

abbreviated as:

$$F : (E, \alpha) \longrightarrow (E^{(p)}, \alpha^{(p)}) \qquad \text{and} \qquad V : (E^{(p)}, p\alpha^{(p)}) \longrightarrow (E, \alpha) \qquad ,$$

where F is the Frobenius morphism and V, its transpose, is the "Verschiebung". These diagrams define morphisms Φ_1 and Φ_2 from $\mathcal{M}_n \otimes \mathbb{F}_p$ to $\mathcal{M}_{n,p} \otimes \mathbb{F}_p$. These morphisms are finite (as sections of q_1 or q_2) and define a morphism

$$\Phi = \Phi_1 \coprod \Phi_2 : \mathcal{M}_n \otimes \mathbb{F}_p \coprod \mathcal{M}_n \otimes \mathbb{F}_p \to \mathcal{M}_{n,p} \otimes \mathbb{F}_p.$$

Let Φ^h be the restriction of Φ to the open sets $\mathcal{M}_n^h$ and $\mathcal{M}_{n,p}^h$ of $\mathcal{M}_n \otimes \mathbb{F}_p$ and $\mathcal{M}_{n,p} \otimes \mathbb{F}_p$ which correspond to curves of nonzero Hasse invariant h.

PROPOSITION 4.3. — The morphism Φ^h is an isomorphism.

Let $\varphi : E_1 \to E_2$ be a p-isogeny between elliptic curves with invertible Hasse invariant on a scheme S of characteristic p. At each geometric point of S, either the kernel $\mathrm{Ker}(\varphi)$ of φ is étale over S, or its Cartier dual, isomorphic to $\mathrm{Ker}({}^t\varphi)$, is étale over S. The property "$\ker(\varphi)$ is étale" is an open property, so that locally on S either $\mathrm{Ker}(\varphi)$ is purely infinitesimal or $\mathrm{Ker}({}^t\varphi)$ is infinitesimal. The only infinitesimal subgroup of order p of E_1 or E_2 being the kernel of Frobenius, in the first case, φ is isomorphic to $F : E_1 \to E_1^{(p)}$ and in the second case, ${}^t\varphi$ is isomorphic to $F : E_2 \to E_2^{(p)}$ thus φ to $V : E_2^{(p)} \to E_2$. □

PROPOSITION 4.4.

(i) The scheme $\mathcal{M}_{n,p}$ is smooth over $\mathrm{Spec}(\mathbb{Z})$ outside the points of characteristic p where $h = 0$.

(ii) The morphisms q_1 and q_2 induce finite and flat morphisms q_1' and q_2' from the normalization $\mathcal{M}'_{n,p}$ of $\mathcal{M}_{n,p}$ to $\mathcal{M}_n$.

(iii) The morphism Φ factors through a surjective morphism

$$\Phi' : \mathcal{M}_n \otimes \mathbb{F}_p \coprod \mathcal{M}_n \otimes \mathbb{F}_p \to \mathcal{M}'_{n,p} \otimes \mathbb{F}_p.$$

The automorphism σ of (3.15) exchanges φ and ${}^t\varphi$, so that it suffices to prove (i) at the points of characteristic p of $\mathcal{M}_{n,p}$ where the kernel of φ is infinitesimal: there is no obstruction to lifting an elliptic curve infinitesimally and to lifting the infinitesimal part of the kernel of multiplication by p.

Where $p = h = 0$, the fiber of the finite morphism (3.15)$q_i : \mathcal{M}_{n,p} \to \mathcal{M}_n$ is reduced to a point, so that the smooth locus of $\mathcal{M}_{n,p}$ is dense in $\mathcal{M}_{n,p}$ and $\mathcal{M}'_{n,p}$ is everywhere of dimension 2. The scheme $\mathcal{M}_n$ being regular, by EGA 0_{IV} 16.5.1 and 17.3.5 (ii), the morphism $q_i : \mathcal{M}'_{n,p} \to \mathcal{M}_n$ is flat. Finally, (iii) results from the fact that Φ is finite and $\mathcal{M}_n \otimes \mathbb{F}_p$ is a normal curve. □

The Hecke endomorphism T_p of ${}_nW_\ell$, as is explained in (3.18), is the $\mathbb{Q}_\ell$-tensor of the fiber at the geometric point $\overline{\mathbb{Q}}$ of $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$ of the endomorphism(again denoted T_p) of

$$R^1\tilde{a}\Big(\mathcal{M}_n, \mathrm{Sym}^k\big(R^1 f_{n*}(\mathbb{Z}_\ell)\big)\Big)$$

defined by the "correspondence".

$$\begin{tikzcd}
 & q_1'^*\mathcal{E} \arrow[rr, "\varphi"] \arrow[dl] \arrow[dr, "u"] & & q_2'^*\mathcal{E} \arrow[dl, "v"'] \arrow[dr] & \\
\mathcal{E} \arrow[dr, "f_n"] & & \mathcal{M}'_{n,p} \arrow[dl, "q_1'"] \arrow[dr, "q_2'"'] & & \mathcal{E} \arrow[dl, "f_n"] \\
 & \mathcal{M}_n & & \mathcal{M}_n &
\end{tikzcd} \tag{4.5}$$

$$T_p = q'_{1*}\varphi^* q_2'^* \qquad \text{(cf. 3.18).}$$

The endomorphisms R_p and I_p are interpreted in a similar way.

LEMMA 4.6. - Let S be a noetherian scheme and let X, Y, Z_1, Z_2 be four S-schemes, separated and of finite type; let F be a $\mathbb{Z}_\ell$-sheaf on X, and $\underline{G}$ a $\mathbb{Z}_\ell$-sheaf on Y; and denote by a each of the structural maps of X, Y, Z_1 or Z_2 into S.

Suppose given a commutative diagram of S-schemes, and morphisms of sheaves:

$$y_1^*\underline{G} \xrightarrow{z_1} x_1^*\underline{F} \qquad\qquad y_2^*\underline{G} \xrightarrow{z_2} x_2^*\underline{F}$$

$$\begin{tikzcd}
 & Z_1 \arrow[r, "f"] \arrow[dl, "x_1"'] \arrow[drr, "y_1"', pos=0.7] & Z_2 \arrow[dr, "y_2"] \arrow[dll, "x_2", pos=0.7] & \\
X & & & Y
\end{tikzcd}$$

Assume that $f^*z_2 = z_1$, that y_1 and y_2 are proper, that x_1 and x_2 are finite and flat, and that for every geometric point s of Z_2 the multiplicity of s in its fiber $x_2^{-1}(x_2(s))$ is equal to the sum of the multiplicities in the fiber (for x_1) of the geometric points of Z_1 lying over s via f.

Then the diagram

$$\begin{tikzcd}
R^i\tilde{a}(Y,\underline{G}) \arrow[r, "y_1^*"] \arrow[d, equal] & R^i\tilde{a}(Z_1,\underline{G}) \arrow[r, "z_1"] & R^i\tilde{a}(Z_1,\underline{F}) \arrow[r, "x_{1*}"] & R^i\tilde{a}(X,\underline{F}) \arrow[d, equal] \\
R^i\tilde{a}(Y,\underline{G}) \arrow[r, "y_2^*"] & R^i\tilde{a}(Z_2,\underline{G}) \arrow[r, "z_2"] \arrow[u] & R^i\tilde{a}(Z_2,\underline{F}) \arrow[r, "x_{2*}"] \arrow[u] & R^i\tilde{a}(X,\underline{F})
\end{tikzcd}$$

is commutative.

This lemma results from analogous lemmas for $R^1a_!$ and R^1a_*. The commutativity of the first squares is trivial. The last square rewrites as

$$\begin{tikzcd}
R^i\tilde{a}(Z_1,\underline{F}) & R^i\tilde{a}(X,x_{1*}x_1^*\underline{F}) \arrow[l, "\sim"'] \arrow[r, "\mathrm{Tr}"] & R^i\tilde{a}(X,\underline{F}) \arrow[d, equal] \\
R^i\tilde{a}(Z_2,\underline{F}) \arrow[u] & R^i\tilde{a}(X,x_{2*}x_2^*\underline{F}) \arrow[l, "\sim"'] \arrow[r, "\mathrm{Tr}"] \arrow[u] & R^i\tilde{a}(X,\underline{F})
\end{tikzcd}$$

and one returns to the definition of the trace to verify that the square

$$\begin{tikzcd}
x_{1*}x_1^*\underline{F} \arrow[r, "\mathrm{Tr}"] & \underline{F} \arrow[d, equal] \\
x_{2*}x_2^*\underline{F} \arrow[r, "\mathrm{Tr}"] \arrow[u] & \underline{F}
\end{tikzcd}$$

commutes.

(4.7) We denote by $T_p/\mathbb{F}_p$ the endomorphism induced by T_p on the restriction to $\mathrm{Spec}(\mathbb{F}_p)$ of the l.c.c. $\mathbb{Z}_\ell$-sheaf $R^1\tilde{a}\Big(\mathcal{M}_n,\ \mathrm{Sym}^k\big(R^1f_{n*}\underline{\mathbb{Z}_\ell}\big)\Big)$ We have

$$R^1\tilde{a}\Big(\mathcal{M}_n, \mathrm{Sym}^k\big(R^1f_{n*}\underline{\mathbb{Z}_\ell}\big)\Big)\big|\mathrm{Spec}(\mathbb{F}_p) \simeq R^1\tilde{a}\Big(\mathcal{M}_n\otimes\mathbb{F}_p, \mathrm{Sym}^k\big(R^1f_{n*}\underline{\mathbb{Z}_\ell}\big)\Big);$$

The formation of the trace morphism for a finite and flat morphism is compatible with base change, so that one may construct, on the model (3.18), from the fiber over $\mathbb{F}_p$ of the "correspondence" (4.5). Lemma (4.6), applied to the commutative diagram

$$\begin{tikzcd}
 & \mathcal{M}_n \otimes \mathbb{F}_p \coprod \mathcal{M}_n \otimes \mathbb{F}_p \arrow[rr, "\Phi'"] \arrow[dl] \arrow[drrr] & & \mathcal{M}'_{n,p} \otimes \mathbb{F}_p \arrow[dlll, "q'_1"] \arrow[dr, "q'_2"] & \\
\mathcal{M}_n \otimes \mathbb{F}_p & & & & \mathcal{M}_n \otimes \mathbb{F}_p
\end{tikzcd}$$

then provides a decomposition of $T_p/\mathbb{F}_p$ as the sum of the endomorphisms defined by the following two correspondences:

(a)
$$\begin{tikzcd}
 & (\mathcal{E}, \alpha) \arrow[rr] \arrow[dl, equal] \arrow[dr] & & (\mathcal{E}^{(p)}, \alpha^{(p)}) = F^*(\mathcal{E}, \alpha) \arrow[dl] \arrow[dr] & \\
(\mathcal{E}, \alpha) \arrow[dr] & & \mathcal{M}_n \otimes \mathbb{F}_p \arrow[dl, equal] \arrow[dr, "F"] & & (\mathcal{E}, \alpha) \arrow[dl] \\
 & \mathcal{M}_n \otimes \mathbb{F}_p & & \mathcal{M}_n \otimes \mathbb{F}_p &
\end{tikzcd}$$

where F is the absolute Frobenius. One recognizes in this correspondence the geometric Frobenius.

(b)
$$\begin{tikzcd}
 & x^*(\mathcal{E}, \alpha) = (\mathcal{E}^{(p)}, p\alpha^{(p)}) \arrow[rr, "V"] \arrow[dl] \arrow[dr, "f_n^{(p)}"] & & (\mathcal{E}, \alpha) \arrow[dl, "f_n"] \arrow[dr, equal] & \\
(\mathcal{E}, \alpha) \arrow[dr] & & \mathcal{M}_n \otimes \mathbb{F}_p \arrow[dl, "x"] \arrow[dr, equal] & & (\mathcal{E}, \alpha) \arrow[dl] \\
 & \mathcal{M}_n \otimes \mathbb{F}_p & & \mathcal{M}_n \otimes \mathbb{F}_p &
\end{tikzcd}$$

The map x is the composite map $I_p^{-1} \circ F$:

$$\begin{tikzcd}
(\mathcal{E}, \alpha) \arrow[d] & (\mathcal{E}, p\alpha) \arrow[l] \arrow[d] & (\mathcal{E}^{(p)}, p\alpha^{(p)}) \arrow[l] \arrow[d] \\
\mathcal{M}_n \otimes \mathbb{F}_p & \mathcal{M}_n \otimes \mathbb{F}_p \arrow[l, "I_p^{-1}"'] & \mathcal{M}_n \otimes \mathbb{F}_p \arrow[l, "F"']
\end{tikzcd}$$

The corresponding endomorphism is then the composition of

$$V : R^1\tilde{a}\Big(\mathcal{M}_n \otimes \mathbb{F}_p, \mathrm{Sym}^k\big(R^1 f_{n*}\underline{\mathbb{Z}}_\ell\big)\Big) \xrightarrow{V^*} R^1\tilde{a}\Big(\mathcal{M}_n \otimes \mathbb{F}_p, \mathrm{Sym}^k\big(R^1 f_{n*}^{(p)}\underline{\mathbb{Z}}_\ell\big)\Big)$$

$$\xrightarrow{\qquad\qquad \mathrm{Tr}_F \qquad\qquad} R^1\tilde{a}\Big(\mathcal{M}_n \otimes \mathbb{F}_p, \mathrm{Sym}^k\big(R^1 f_{n*}\underline{\mathbb{Z}}_\ell\big)\Big)$$

and of

$$I_P^* = \mathrm{Tr}_{I_p^{-1}} : \text{endomorphism of } R^1\tilde{a}\Big(\mathcal{M}_n \otimes \mathbb{F}_p, \mathrm{Sym}^k\big(R^1 f_{n*}\underline{\mathbb{Z}}_\ell\big)\Big).$$

PROPOSITION 4.8. — We have $T_p/\mathbb{F}_p = F + I_p^* V$, and

(i) F is identified with the inverse of the Frobenius element ("arithmetic") φ_p of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acting on $\tilde{H}^1\big(\mathcal{M}_n \otimes \mathbb{F}_p, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}_\ell})\big)$;

(ii) F and V are transpose with respect to the scalar product (3.20);

(iii) $FV = VF = p^{k+1}$.

For the relation (i) between the geometric and arithmetic Frobenius, see the exposition of C. Houzel (SGA 5, XV). The composite VF is the composite of the homomorphisms deduced from the following morphisms:

$$\begin{tikzcd}
\mathcal{E} \arrow[d] & \mathcal{E}^{(p)} \arrow[l] \arrow[r, "F_{\mathcal{E}}"] \arrow[dr] & \mathcal{E} \arrow[r, "V_{\mathcal{E}}"] \arrow[d] & \mathcal{E}^{(p)} \arrow[r] \arrow[dl] & \mathcal{E} \arrow[d] \\
\mathcal{M}_n & & \mathcal{M}_n \arrow[ll, "F"'] \arrow[rr, "F"] & & \mathcal{M}_n
\end{tikzcd}$$

$$VF = \mathrm{Tr}_F \circ F_{\mathcal{E}}^* \circ V_{\mathcal{E}}^* \circ F^*.$$

The morphism $F_{\mathcal{E}}^* V_{\mathcal{E}}^* = (F_{\mathcal{E}} V_{\mathcal{E}})^* = (p \cdot 1_E)^*$ acts by multiplication by p^k on $\mathrm{Sym}^k\big(R^1 f_* \underline{\mathbb{Z}_\ell}\big)$, so that $VF = p^k \cdot \mathrm{Tr}_F \circ F^* = p^k \cdot p = p^{k+1}$, since $F : \mathcal{M}_n \to \mathcal{M}_n$ is of degree p.

By transport of structure, φ_p respects the scalar product (3.20) taking values in $\mathbb{Q}_\ell(-k-1)$, a group on which φ_p acts by multiplication by p^{-k-1}. Hence one has

$$(Fx, y) = p^{k+1}(\varphi_p F x, \varphi_p y) = (x, p^{k+1} F^{-1} y) = (x, Vy). \quad \square$$

The following theorem, synonymous with (4.8), goes back to Eichler.

THEOREM 4.9 (Congruence Formula). — Let $K_{n,\ell}$ be the largest subextension of $\mathbb{Q}$ unramified outside n and ℓ, and let φ_p be a Frobenius element relative to p in $\mathrm{Gal}(K_{n,\ell}/\mathbb{Q})$. Let F be the endomorphism φ_p^{-1} of W_ℓ and V its transpose with respect to the scalar product (3.20). Then,

$$T_p = F + I_p^* V, \; FV = p^{k+1}$$

and

$$1 - T_p X + p R_p X^2 = (1 - FX)(1 - I_p^* V X). \; \square$$

Chapter 5

Weil implies Ramanujan

No. 5 – Weil implies Ramanujan.

If p is a prime number and X is a scheme over $\mathbb{F}_p$, we denote by $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$, by $F : X \longrightarrow X$ the (geometric) Frobenius endomorphism, and we set $\overline{X} = X \otimes \overline{\mathbb{F}}_p$. Throughout, ℓ will always denote a prime number distinct from p.

By "Weil conjectures" we mean the following statement:

> Let X be a projective and smooth scheme over $\mathbb{F}_p$ and let ℓ be a prime different from p. Then the eigenvalues of the endomorphism F^* on $H^i(X, \mathbb{Q}_\ell)$ are algebraic integers, all of whose complex conjugates have absolute value $p^{i/2}$.

With the hypotheses and notations of (4.9) (recall that $(p, n) = 1$), we have:

THEOREM 5.1. - If the Weil conjectures are true, then the eigenvalues of the endomorphism F of W_ℓ are algebraic integers (all of whose complex conjugates have absolute value $p^{(k+1)/2}$).

Admit the Weil conjectures.

LEMMA 5.2. (modulo Weil).- Let X be a smooth scheme over $\mathbb{F}_p$ which can be represented as an open subset of a projective smooth scheme X^*. Then the eigenvalues of the endomorphism F^* on $\tilde{H}^i(X, \mathbb{Q}_\ell)$ are algebraic integers of absolute value $p^{i/2}$.

The natural map from $H^i_c(\overline{X}, \mathbb{Q}_\ell)$ to $H^i(\overline{X}, \mathbb{Q}_\ell)$ factors through $H^i(\overline{X^*}, \mathbb{Q}_\ell)$:

$$H^i_c(\overline{X}, \mathbb{Q}_\ell) \to H^i(\overline{X^*}, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$$

so that as a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-module, $\tilde{H}^i(\overline{X}, \mathbb{Q}_\ell)$ is a subquotient of $H^i(\overline{X^*}, \mathbb{Q}_\ell)$. □

LEMMA 5.3 (modulo Weil).- Let S be a smooth scheme over $\mathbb{F}_p$ and let $f : A \longrightarrow S$ be an abelian scheme over S. Suppose that A can be represented as an open subset of a projective smooth scheme A' over $\mathbb{F}_p$. Then the geometric Frobenius endomorphism F^* of $\tilde{H}^i(\overline{S}, R^j f_* \mathbb{Q}_\ell)$ has eigenvalues which are algebraic integers of absolute value $p^{(i+j)/2}$.

Let $m > 1$ be an integer, and consider the Leray spectral sequence

$$E : E_2^{ij} = H^i(\overline{S}, R^jf_*\mathbb{Q}_\ell) \Rightarrow H^{i+j}(\overline{A}, \mathbb{Q}_\ell)$$
$${}_cE : {}_cE_2^{ij} = H_c^i(\overline{S}, R^jf_*\mathbb{Q}_\ell) \Rightarrow H^{i+j}(\overline{A}, \mathbb{Q}_\ell).$$

The endomorphism of multiplication by $m : \psi_m = m1_A$, defines endomorphisms of E and ${}_cE$ which are inserted into a commutative diagram:

$$\begin{tikzcd}
{}_cE \arrow[r] \arrow[d, "\psi_m^*"] & E \arrow[d, "\psi_m^*"] \\
{}_cE \arrow[r] & E
\end{tikzcd}$$

On $R^jf_*\mathbb{Q}_\ell$, ψ_m^* acts by multiplication by m^j, such that on the terms ${}_cE_r^{ij}$ and E_r^{ij} of ${}_cE$ and E, ψ_m^* is the multiplication by m^j. The maps d_r $(r \geq 2)$ commutes with ψ_m^*, and send E_r^{ij}(resp. ${}_cE_r^{ij}$) into $E_r^{i'j'}$ (resp. ${}_cE_r^{i'j'}$) with $j \neq j'$. They are therefore 0, and E_2^{ij} (resp. ${}_cE_2^{ij}$) is identified with the subspace of $H^{i+j}(\overline{A}, \mathbb{Q}_\ell)$ (resp. of $H_c^{i+j}(\overline{A}, \mathbb{Q}_\ell)$) where $\psi_m^* = m^j$. Therefore, $\tilde{H}^i(\overline{S}, R^jf_*\mathbb{Q}_\ell)$ is identified with the galois submodule of $\tilde{H}^{i+j}(\mathbb{A}, \mathbb{Q}_\ell)$ where $\psi_m^* = m^j$ and we apply (5.2). The trick used here is due to Lieberman. □

Let $f_n : \mathcal{E} \to \mathcal{M}_n \otimes \mathbb{F}_p$ be the universal elliptic curve on $\mathcal{M}_n \otimes \mathbb{F}_p$ and let $f_{n,k} : \mathcal{E}_k \to \mathcal{M}_n \otimes \mathbb{F}_p$ be its iterated k-fold fiber product with itself. The Kunneth's formula shows that the $\mathbb{Q}_\ell$-sheaf $R^kf_{n,k*}\mathbb{Q}_\ell$ admits as direct factor the k-th tensor power of $R^1f_{n*}\mathbb{Q}_\ell$; this in turn contains as direct factor the $\mathbb{Q}_\ell$-sheaf $\mathrm{Sym}^k(R^1f_{n*}\mathbb{Q}_\ell)$. Theorem 5.1 is thus a result of (5.3) and of

LEMMA 5.4. - The scheme $\mathcal{E}^{(k)}$ is an open subset of a scheme $\mathcal{E}^*$ which is projective and smooth over $\mathbb{F}_p$.

Let $\mathcal{E}^*$ be the minimal Néron model of $\mathcal{E}$ over $\mathcal{M}_n^* \otimes \mathbb{F}_p$ (4.1). The scheme $\mathcal{E}^*$ is projective and smooth over $\mathbb{F}_p$. Since $n \geq 3$ and since the n-torsion points of $\mathcal{E}$ form a trivial covering of $\mathcal{M}_n \otimes \mathbb{F}_p$, this Néron model is "semi-stable" (case a or b_m in Néron's classification). In particular, the projection $f : \mathcal{E}^* \longrightarrow \mathcal{M}_n^*$ has only finitely many non-smooth points, and at these points f_n is non-degenerate (exhibiting an ordinary quadratic singularity).

Let $\mathcal{E}_k^{**}$ be the k-th iterated fiber product of $\mathcal{E}^*$ over $\mathcal{M}_n^*$. To prove (5.4), it suffices to resolve the singularity of $\mathcal{E}_k^{**}$ without touching the open subset $\mathcal{E}_k$. Let's prove first:

LEMMA 5.5. - Let V be the subvariety of the affine space over a field k (with coordinates $X_0, Y_0, \ldots, X_r, Y_r, T_1 \ldots T_s$) defined by the equations

$$X_0Y_0 = X_1Y_1 = \cdots = X_rY_r.$$

Let m be the ideal of $\mathcal{O}_V$ generated by the monomials obtained from the monomials deduced from $\prod_{i=0}^r X_i^i$ by any permutation of the coordinates that respects the set of pairs $\{X_i, Y_i\}$ (for $0 \leq i \leq r$). Then, $m = \mathcal{O}_V$ outside the singular locus of V, and the variety $\tilde{V}$ obtained from V by blowing up the ideal m is smooth over k.

The singular locus is the locus where, for some $i \neq j$, the four coordinates X_i, Y_i, X_j, Y_j vanish simultaneously. The affine open subset of $\tilde{V}$ defined by the element $\prod_1^r X_i^i$ of the ideal m is the spectrum of the regular ring

$$k\Big[Y_0/X_1,\, X_0/X_1,\, X_1/X_2,\, \ldots,\, X_{r-1}/X_r, X_r, T_1, \ldots T_s\Big].$$

(To verify, note that $X_i/X_{i+1} = Y_{i+1}/Y_i$), and Lemma 5.5 follows. □

One now shows that, locally for the étale topology, the singularities of $\mathcal{E}_k^{**}$ are isomorphic to those of V (with $r = k-1$), and that this permits one to define on $\mathcal{E}_k^{**}$ an ideal m analogous to the ideal m in Lemma 5.5. Blowing up this ideal yields $\mathcal{E}_k^{*}$. □

An approximation of the following theorem has been proved by Ihara [2]:

THEOREM 5.6. - (Weil Implies Ramanujan.) The Weil conjectures imply the Ramanujan conjecture.

Note first that (5.1) remains true for $n = 1$, because ${}_1^kW_\ell$ is the galois submodule of ${}_mW_\ell^k$ that is invariant under $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. On ${}_1W_\ell^k$, I_p^* induces the identity, and (4.8) reduces to

$$1 - T_pX + p^{k+1}X^2 = (1 - FX)(1 - VX).$$

The endomorphisms F and V are transposed with respect to one another, so that

$$\det(1 - FX; {}_1^kW_\ell) = \det(1 - VX; {}_1^kW_\ell).$$

The action of T_p on ${}_1^kW_\ell$ is induced by its action on ${}_1^kW$ and is compatible with the decomposition of ${}_1^kW \otimes \mathbb{C}$ into the direct sum of the space S_{k+2} of parabolic modular forms of weight $k+2$ for $SL_2(\mathbb{Z})$ and its complex conjugate. Since T_p is a hermitian operator(for the Petersson scalar product) and (3.19), one then deduces that

$$\det(1 - T_pX + p^{k+1}X^2; {}_1^kW_\ell) = \det(1 - T_pX + p^{k+1}X^2; S_{k+2})^2,$$

and

$$\det(1 - T_pX + p^{k+1}X^2; S_{k+2})^2 = \det(1 - FX; {}_1^kW_\ell)^2$$

i.e.

$$\det(1 - T_pX + p^{k+1}X^2; S_{k+2}) = \det(1 - FX; {}_1^kW_\ell). \tag{5.7}$$

Returning to the notations of chapter 1 and taking $k = 10$, by Hecke's theory and (3.19), (5.7) is rewritten as

$$H_p(X) = \det(1 - FX; {}_1^{10}W_\ell)$$

and one applies (5.1). □

One similarly verifies that the Weil conjectures imply the generalization by Petersson of the Ramanujan conjecture.

Bibliography

[1] J. Igusa, *Kroneckerian Model of Fields of Elliptic Modular Functions*, Am. J. Math. 81 (1959), 561–577.

[2] Y. Ihara, *Hecke Polynomials as Congruence Zeta Functions in the Elliptic Modular Case*, Ann. of Math. S.2, 85 (1967), 267–295.

[3] J.-P. Jouanolou, *Exposés V et VI de SGA 5.*

[4] M. Kuga and G. Shimura, *On the zeta functions of a fibre variety whose fibres are abelian varieties*, Ann. of Math., S.2, 82 1965, 478-539.

[5] M. Raynaud *Exposé XIII de SGA 1 and appendix.*

[6] J.-P. Serre, *Une interprétation des congruences relative à la fonction τ de Ramanujan* , Séminaire Delange-Pisot-Poitou, 1967/68, No. 14.

[7] G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. of Japan, 11 1959, 291-211.

[8] J. Tate, *Courbes elliptiques: formulaire* - updated by P.Deligne, Notes mimeographed by the IHES.

[9] J.-L. Verdier *Sur les intégrales attachées aux formes automorphes* (after G. Shimura), Bourbaki seminar, Feburary 1961, exp. 216.