Formes modulaires et représentations ℓ-adiques
Séminaire Bourbaki, 21e année, 1968/69, n° 355

by Pierre Deligne

June 28, 2004

1 Introduction.

Let

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

and

$$\Delta(z) = D(e^{2\pi iz}) \qquad (\mathrm{Im}(z)>0).$$

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

Put, for p prime,

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

Following Hecke's theory, the Dirichlet series

$$L_\tau(s) = \sum\tau(n)n^{-s} = \prod_p\frac{1}{H_p(p^{-s})}$$

extends to an entire function of s and the function

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

is invariant under $s\mapsto 12-s$. The Ramanujan conjecture affirms that the roots of the polynomial H_p are of absolute value $p^{-11/2}$ (i.e. that $|\tau(p)|<2p^{11/2}$).

These properties, proven or conjectural, are similar to conjectural properties of zeta functions of algebraic varieties over Q. Suggested by this, in a first approximation, it is tempting to interpret the function L_τ as the zeta function of one such variety.

For each prime number ℓ, let K_ℓ be the maximal extension of $\mathbb{Q}$ unramified away from ℓ and, for $p\neq\ell$, let F_p the inverse in the Galois group $\mathrm{Gal}(K_\ell/Q)$, of the Frobenius element φ_p relative to p. This last object is well defined up to conjugation.

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

$$H_p(X) = \det\left(1-F_pX;W_\ell\right).$$

Moreover, the representation W_ℓ ought to lie in the range of application of the Weil conjectures, and the Ramanujan conjecture ought to be a particular case of these.

This program has been carried out, by Kuga–Shimura [4], in the analogous case of modular forms relative to certain subgroups of $SL_2(\mathbb{R})$ with *compact quotient*. Reduced to the present case, the fundamental idea of Sato–Kuga–Shimura is the following: if E is the universal elliptic curve over the moduli scheme S of elliptic curves (we forget that it does not exist) and if E^k is the fibered product of E with itself over S repeated k times, then $L_\tau(s)$ is essentially the zeta function of E^k for $k = 10 = 12 - 2$.

We show in that which follows how to resolve the difficulties creeted by the points, and how to construct the representations W_ℓ having the above indicated properties. For more historical details and for applications, refer to Serre [6].

Notations.

— One denotes by $\mathbb{A}$ the ring of adeles of $\mathbb{Q}$; by $\mathbb{A}^f$ the ring of "finite" adeles, the restricted product, extended over all prime numbers, of the fields $\mathbb{Q}_p$; and, for S a finite set of prime numbers, one puts

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

For $S = \emptyset$, one write $\widehat{Z} = \mathbb{A}_\emptyset^f$.

— If S is a topological space (or the étale site of a scheme) and G a set, one denotes by $\underline{G}$ the constant sheaf over X defined by G.

— One denotes by $\mathbb{G}_a$ and $\mathbb{G}_m$ the additive and multiplicative groups.

— An elliptic curve is an abelian variety of dimension one, and in particular is equipped with an origin.

— If $\mathcal{L}$ is an invertible sheaf and if $n \in \mathbb{Z}$, one denotes by $\mathcal{L}^n$ the nth tensor power $\mathcal{L}^{\otimes n}$.

— One denotes by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

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

2 The Shimura Isomorphism.

(2.1) An *elliptic curve* over a complex analytic space S is a proper and flat morphism of analytic spaces $f\colon E \to S$, equipped with a section e, whose fibers are elliptic curves. An elliptic curve over S admits one and only one S-group law $\mu\colon E \times_S E \to E$, whose unit section is e. Associated to an elliptic curve are the following:

(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. One has $f_*\Omega^1_{E/S} \xrightarrow{\sim} \omega$.

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

The exponential mapping 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 canb e reconstructed starting from the map α.

The local system $\bigwedge^2 R^1 f_* \underline{\mathbb{Z}} \sim R^2 f_* \underline{\mathbb{Z}}$ is canonically isomorphic to $\underline{\mathbb{Z}}$. An isomorphism between $\underline{\mathbb{Z}}^2$ and $R^1 f_* \underline{\mathbb{Z}}$ is said to be *admissible* if it induces 1 on the second exterior powers.

Denote by $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$ the set of ($\mathbb{R}$-vector space) isomorphism between $\mathbb{R}^2$ and $\mathbb{C}$ which do respect the natural orientations of $\mathbb{R}^2$ and $\mathbb{C}$ (defiend by $e_1 \wedge e_2 > 0$ and $1 \wedge i > 0$). One such homomorphism is determined by its restriction to $\mathbb{Z}^2$, and one puts

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

This space is equipped with the complex structure obtained from its inclusion in the complex vector space $\mathrm{Hom}(\mathbb{Z}^2, \mathbb{C})$. One arranges a "universal" exact sequence over this space,

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

Proposition 2.2 *(i) The fuctor which associates to each analytic space S the set of isomorphism classes of elliptic curves E over S, equipped with isomorphisms $\omega_E \sim \mathbb{G}_a$ and $R^1 f_* \underline{\mathbb{Z}} \sim \mathbb{Z}^2$ (the last being admissible), is representable by the analytic space* $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$*, equipped with a universal ellptic curve E_0.*

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

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

One can again regard X as the set of complex structures over $\mathbb{R}^2$. This space is, by (ii), equipped with a universal elliptic curve E_X, whose local system of real cohomology 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 relative De Rham cohomology sheaf of E_X over X, and as such it is inserted into an exact sequence (the 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, $\omega^{-1} \sim R^1 f_* \mathcal{O}_{E_X}$).

The functorial description 2.2(ii) evidently yields a right action of the group $SL_2(\mathbb{Z})$ on (X, E_X): to $\gamma \in SL_2(\mathbb{Z})$ and to the elliptic curve E, eqiupped with $\alpha \colon \underline{\mathbb{Z}}^2 \xrightarrow{\sim} R^1 f_* \underline{\mathbb{Z}}$, one associates $(E, \alpha \circ \gamma)$. If one regards X, equipped with

$$q \colon \underline{\mathbb{R}}^2 \otimes_{\mathbb{R}} \mathcal{O}_X \sim R^1 f_* \underline{\mathbb{R}} \otimes_{\mathbb{R}} \mathcal{O}_X \to \omega^{-1},$$

as classifying the complex structures on $\mathbb{R}^2$, one puts the same evident action of the group $GL_2^+(\mathbb{R})$ on $(X, \underline{\mathbb{R}}^2, \omega, q)$.

(2.3) We choose a basis (x_1, x_2) of $\mathbb{R}^2$ such that $x_1 \wedge x_2 > 0$. A point ($f \colon \mathbb{R}^2 \to \mathbb{C}$, (mod $\mathbb{C}^\times$)) of X is located by $z = f(x_1)/f(x_2)$ ($\mathrm{Im}(z) > 0$) and the map q is identified with

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

This gives an evident trivialization of ω^{-1} over X, which is not equivariant. Relative to this trivialization, a section $f(z)$ of ω^k over X is transformed by an element $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)^{-1}$ of $GL^+(\mathbb{R}^2)$ (with respect to the basis (x_1, x_2)) via

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

From the identity

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

once deduces that dz is a section of $\omega^{-2}\Omega^1_X$ that is invariant under the group $SL_2(\mathbb{R})$. This section is everywhere nonzero and defines an equivariant isomorphism of $SL_2(\mathbb{R})$-sheaves between ω^2 and Ω^1_X.

(2.4) Let Γ be a discrete subgroup of the group $SL_2(\mathbb{R})$ that has no elements of finite order and has quotient of finite volume. One knows then that the quotient space X/Γ is identified with a smooth projective curve $\overline{X/\Gamma}$ minus a finite number of points. The group Γ acts on X without fixed points. The equivariant local system $\underline{\mathbb{R}}^2$ on X, as well as the exact sequence

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

define thus a local system U over X/Γ and an exact sequence

$$0 \to \omega \to U \otimes_{\mathbb{R}} \mathcal{O} \to \omega^{-1} \to 0. \tag{2.5}$$

In the particular case where $\Gamma \subset SL_2(\mathbb{Z})$, these structures are obtained from an elliptic curve E over X/Γ with inverse image the equivariant elliptic curve E_X over X.

(2.6) The points at infinity of X/Γ are described as follows (see [9]):

(a) They correspond to conjugacy classes in Γ of nontrivial subgroups of Γ that are maximal among the subgroups of Γ consisting of unipotent elements.

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

$$\left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}.$$

Let z be the coordinate (2.3) on X defined by (x_1, x_2). There exists N such that the subset $X_N = \{z \mid \mathrm{Im}(z) > N\}$ of X is disjoint from its conjugates for all $\gamma \in \Gamma/\Gamma_0$, 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 point of $\overline{X/\Gamma} - X/\Gamma$ associated to Γ_0, this isomorphism is extended to an isomorphism of a neighborhood of P_{Γ_0} with the disk $0 \leq q < e^{-2\pi N}$.

By virtue of (2.3), the sections of ω over X_N that are invariant under Γ_0 are identified with periodic holomorphic functions of period one on X_N. One denotes again by ω the invertible sheaf over $\overline{X/\Gamma}$ that extends ω and such that in a neighborhood of a point P_{Γ_0}, the section of ω over X_N/Γ_0 defined by the function 1 is extended to an invertible section on $\overline{X_N/\Gamma_0}$.

(2.7) Over $\overline{X/\Gamma}$, one has the twho invertible sheaves Ω^1 and ω^2, and an isomorphism φ (2.3) between the restrictions of these sheaves to X/Γ. From the formula

$$dq = de^{2\pi iz} = 2\pi i e^{2\pi iz}\,dz = 2\pi iq\,dz$$

results that the map

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

extends to $\overline{X/\Gamma}$, and shows a simple zero at each of the points at infinity.

Definition 2.8 *The space of cusp forms of weight $k+2$, relative to the group Γ, is the space of global sections*

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

By vertue of (2.7), this space is again identified to the space of global sections of ω^{k+2} that vanish at infinity (i.e. at each “point”).

(2.9) Denote by U^k the kth symetric power of the local system over X/Γ. The map (2.5) induces an map

$$\iota^k\colon \omega^k \to U^k \otimes_{\mathbb{R}} \mathcal{O},$$

whence an map, again denoted by ι^k:

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

the target being the sheaf of holomorphic differential forms over X/Γ, with coefficients in the local system U^k.

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

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

induces an map

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

Moreover, the cohomology space $H^1(X/\Gamma, U^k \otimes \mathbb{C})$ is equipped with a natural complex conjugation, such that δ defines a conjugate-linear mapping $\overline{\delta}$ from the space complex conjugate to $H^0(X/\Gamma, \Omega^1(U^k))$ into $H^1(X/\Gamma, U^k \otimes \mathbb{C})$. One obtains thus an map $sh_0 = \delta \circ H^0(\iota^k) \oplus \overline{\delta} \circ H^0(\iota^k)$:

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

For an arbitrary sheaf $\underline{F}$ on a space Y, one denotes by $\widetilde{H}^i(Y, \underline{F})$ the image of the cohomology with compact supports $H^i_c(Y, \underline{F})$ in the cohomology without supports $H^i(Y, \underline{F})$.

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

Theorem 2.10 (Shimura [7]) *There exists an isomorphism sh making the following diagram commutative:*

$$\begin{array}{ccc} H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} & \xrightarrow{sh} & \widetilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \\ \bigcap & & \bigcap \\ H^0(X/\Gamma, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(X/\Gamma, \Omega^1 \otimes \omega^k)} & \xrightarrow{sh_0} & H^1(X/\Gamma, U^k \otimes \mathbb{C}). \end{array}$$

One calls *sh* the *Shiumra isomorphism.*

(2.11) In the particluar case where Γ is a subgroup of finite index of $SL_2(\mathbb{Z})$, the elliptic curve E over X/Γ fournishes a elliptic curve schme over the algebraic curve X/Γ (i.e., its modular invariant is meromorphic at infinity); this admits thus a Néron model $\overline{E}$ over $\overline{X/\Gamma}$. One can show that the fibers of $\overline{E}$ at the points at infinity are of multiplicative type, and that over all of $\overline{X/\Gamma}$ one has $\omega = e^*\Omega^1_{\overline{E}/\overline{X/\Gamma}}$.

In this particular case, one has $U = R^1 f_* \underline{\mathbb{Z}} \otimes \mathbb{R}$, so that the target of the Shimura isomorphism can be rewritten:

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

3 Hecke Operators and the Fundamental ℓ-adic Representation.

(3.1) Recall (cf. [3]) that the category of "locally constant" constructible $\mathbb{Z}_\ell$-sheaves (abbreviated lcc) over a scheme S is the category of projective systems $(\underline{F}_n)_{n \in \mathbb{N}}$ over the étale site S_{et} of S that satisfy:

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

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

The lcc $\mathbb{Z}_\ell$-sheaves form a stack of abelian categories over S; the stack of lcc $\mathbb{Q}_\ell$-sheaves is the quotient of this stack by the thick substack of lcc $\mathbb{Z}_\ell$-sheaves killed by a power of ℓ. One denotes by $\otimes\mathbb{Q}_\ell$ the canonical functor from the category of lcc $\mathbb{Z}_\ell$-sheaves into that of lcc $\mathbb{Q}_\ell$-sheaves.

If S is connected and equipped with a geometric point s, the category of lcc $\mathbb{Z}_\ell$-sheaves (resp. $\mathbb{Q}_\ell$-sheaves) over S is equivalent by the functor "fiber over s", to the category of continuous representations of the fundamental group $\pi_1(S, s)$ on $\mathbb{Z}_\ell$-modules of finite type (resp. on $\mathbb{Q}_\ell$-vector spaces of finite rank).

If T is a finite set of prime numbesr, an lcc $\mathbb{A}^f_T$-sheaf consists in the giving of, for each prime number ℓ, an lcc $\mathbb{Z}_\ell$-sheaf if $l \notin T$ and an lcc $\mathbb{Q}_\ell$-sheaf if $\ell \in T$. For $T = \emptyset$, one speaks of lcc $\widehat{\mathbb{Z}}$-sheaves rather than of lcc $\mathbb{A}^f_\emptyset$-sheaves.

For general T, the category of lcc $\mathbb{A}^f_T$-sheaves is the inductive limit of the categories of lcc $\mathbb{A}^f_{T'}$-sheaves for $T' \subseteq T$ finite. One puts:

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

The stack of *elliptic curves up to isogeny* over S is the stack obtained from the stack of eliptic curves over S by "formally inverting isogenies". One denotes by $\otimes\mathbb{Q}$ the functor associating to an elliptic curve its underlying elliptic curve up to isogeny. For S quasi-compact, one has

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

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

(3.2) Let $f\colon E\to S$ be an elliptic curve over a scheme S. One denotes by $T_\ell(E)$ the projective system of kernels E_{ℓ^n} of multiplication by ℓ^n on E, the transition maps from E_{ℓ^n} to E_{ℓ^m} $(n\geq m)$ being multiplication by ℓ^{n-m}. Proceeding the same for $\mathbb{G}_m$, one puts $T_\ell(\mathbb{G}_m)=\mathbb{Z}_\ell(1)$. If ℓ is invertible over S, then $T_\ell(E)$ and $\mathbb{Z}_\ell(1)$ are $\mathbb{Z}_\ell$-sheaves on S. One defines $T_\infty(E)$ to be the relative Lie algebra of E over S (the invertible dual sheaf to the invertible sheaf ω of (2.1(a))).

Suppose S is of characteristic 0. One defines then the $\widehat{Z}$-sheaf $T_f(E)$ over S to be the system of $T_\ell(E)$ and one puts $V_f(E)=T_f(E)\otimes\mathbb{A}^f$. If $u\colon e\to F$ is an isogeny, then u induces an isomorphism of $V_f(E)$ onto $V_f(F)$ and of $T_\infty(E)$ onto $T_\infty(F)$; the functors V_f and T_∞ factor thus through the category of elliptic curves up to isogeny over S.

Proposition 3.3 *Let S be a scheme of characteristic 0; $E_1(S)$ the category of elliptic curves over S; and $E_2(S)$ the category of triples composed of an elliptic curve up to isogeny E over S, a $\widehat{\mathbb{Z}}$-sheaf T that is a twisted form of $\underline{\widehat{\mathbb{Z}}}^2$, and an isomorphism $\beta\colon V_f(E)\xrightarrow{\sim} T\otimes\mathbb{A}^f$. Then the functor $I\colon E\mapsto(E\otimes\mathbb{Q},T_f(E),V_f(E)\sim T_f(E)\otimes\mathbb{A}^f)$ from $E_1(s)$ to $E_2(s)$ is an equivalence of categories.*

The question is local on S, which one can suppose to be quasi-compact. If $f\colon E\to F$ is a morphism of S-elliptic curves, and if f is an isogeny, then one has an exact sequence

$$0\to T_f(E)\to T_f(F)\to\ker(f)\to 0. \tag{3.4}$$

The morphism f is divisible by n if and only if it kills the kernel E_n of multiplication by n, because the map "multiplication by n" of E/E_n to E is an isomorphism. By (3.4), this takes place if and only if $T_f(f)$ is divisible by n, and one deduces from this that $\mathrm{Hom}_s(E,F)$ is the subgroup of $\mathrm{Hom}_S(E\otimes\mathbb{Q},F\otimes\mathbb{Q})$ consising of morphisms f such that $V_f(f)$ sends $T_f(E)$ into $T_f(F)$. The functor I is thus faithfully flat.

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 by a "lattice" T in $V_f(E)$ which, for almost all ℓ, coincides with $T_\ell(E)$. For $q\in\mathbb{Q}$, $(E\otimes\mathbb{Q},T)$ is isomorphic to $(E\otimes\mathbb{Q},qT)$, which allows us to suppose that $T_f(E)\subseteq T$.

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

Corollary 3.5 *The functor $F_1(S)$ (resp. $F_1'(S)$) which associates to each scheme S of characteristic 0 the set of isomorphism classes of elliptic curves over S, equipped with an isomorphism $\alpha\colon T_f(E)\xrightarrow{\sim}\underline{\widehat{\mathbb{Z}}}^2$ (resp. and an isormorphism $\alpha_\infty\colon T_\infty(E)\xrightarrow{\sim}\mathbb{G}_a$) is isomorphic to the functor $F_2(S)$ (resp. $F_2'(S)$) which associates to S the set of isomorphism classes of elliptic curves up to isogeny over S, equipped with an isomorphism $\beta\colon V_f(F)\xrightarrow{\sim}\underline{\mathbb{A}}^{f2}$ (resp. and an isomorphism $\beta_\infty\colon T_\infty(F)\xrightarrow{\sim}\mathbb{G}_a$).*

Proposition 3.6 *The functor F_1 (resp. F_1') is representable by a schem M_∞ (resp. M'_∞) over $\mathbb{Q}$.*

Let n be an integer ≥ 3. The functor which associates to each scheme S the set of isomorphism classes of elliptic curves, equipped with an isomorphism $\alpha_n\colon E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ (resp. and $\alpha_\infty\colon T_\infty(E) \xrightarrow{\sim} \mathcal{O}_X$), is represented by an affine curve M_n (resp. by an affine surface M'_n) over $\mathrm{Spec}(\mathbb{Z}[1/n])$. For $n \mid m$, the morphism of M_m to M_n defined by

$$(E, \alpha_m\colon E_m \xrightarrow{\sim} (\mathbb{Z}/m)^2) \mapsto (E, \tfrac{n}{m}\alpha_m\colon E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2)$$

is finite and étale over $\mathrm{Spec}(\mathbb{Z}[1/m])$, and one has

$$M_\infty = \varprojlim M_n.$$

One goes one proceeds in the same way to represent F_1'. $\square$

(3.7) The scheme M_∞ (resp. M'_∞) is equipped with a universal elliptic curve $f_\infty\colon E_\infty \to M_\infty$ and an isomorphism $\alpha\colon T_f(E_\infty) \xrightarrow{\sim} \widehat{\mathbb{Z}}^2$ (resp. also with an isomorphism $\alpha_\infty\colon T_\infty(E'_\infty) \xrightarrow{\sim} \mathbb{G}_a$).

Following (3.5), the scheme M_∞ (resp. M'_∞) represents the functor F_2 (resp. F_2'), which makes for an evident left action of the adelic group $GL_2(\mathbb{A}^f)$ on $(M_\infty, E_\infty \otimes \mathbb{Q}, \alpha \otimes \mathbb{A}^{f2})$ (resp. on $(M'_\infty, E'_\infty, \alpha \otimes \mathbb{A}^{f2}, \alpha_\infty))$ given on the functor, for $g \in GL_2(\mathbb{A}^f)$, by

$$g\colon (F, \beta\colon V_f(E) \xrightarrow{\sim} \mathbb{A}^{f2}, \beta_\infty) \longmapsto (F, g \circ \beta\colon V_f(E) \xrightarrow{\sim} \mathbb{A}^{f2}, \beta_\infty).$$

Shafarevich first noted this fact.

Let Y be a scheme over $\mathbb{C}$, equal to the projective limit of schemes Y_i of finite type over $\mathbb{C}$, the transition maps being finite. The locally compact [annelé] space Y^{an}, equal to the projective limit of the Y_i^{an}, depends only on Y and not on its representation as a projective limit. If Y is a scheme over $\mathbb{Q}$, equal to the projective limit of schemes Y_i of finite type over $\mathbb{Q}$, the transition maps being finite, one puts $Y^{\mathrm{an}} = (Y \otimes \mathbb{C})^{\mathrm{an}}$. This applies to M_∞ and M'_∞.

Proposition 3.8 *One has canonically*

$$\begin{aligned} {M'_\infty}^{\mathrm{an}} &\sim \mathrm{Hom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f2})/GL_2(\mathbb{Q}) \qquad \textit{and} \\ M_\infty &\sim \mathbb{C}^\times \backslash \mathrm{Hom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f2})/GL_2(\mathbb{Q}), \end{aligned}$$

and, less canonically,

$$\begin{aligned} {M'_\infty}^{\mathrm{an}} &\sim GL_2(\mathbb{A})/GL_2(\mathbb{Q}) \qquad \textit{and} \\ M_\infty^{\mathrm{an}} &\sim K_\infty \backslash GL_2(\mathbb{A})/GL_2(\mathbb{Q}), \end{aligned}$$

where K_∞ is [a/the, bad copy] maximal compact subgroup with [bad copy] real. These isomorphisms are compatible with the action of $GL_2(\mathbb{A}^f)$.

The notion of elliptic curve up to isogeny, and its variants, extends to the complex analytic case. On the other hand, an isogeny $\varphi\colon E \to F$ induces an isomorphism φ^* between the local systems of rational cohomology of E and F, which allows us to define this last object for an elliptic curve up to isogeny. Let S be a complex analytic space. One sees with the aid of (2.1) that it amounts to the same to give an elliptic curve up to isogeny over S, or to give an invertible sheaf T_∞, a local system $T_\mathbb{Q}$ of $\mathbb{Q}$-vector spaces, and a morphism $\alpha\colon T_\mathbb{Q} \to T_\infty$ inducing an isomorphism between $T_\mathbb{Q} \otimes \mathbb{R}$ and T_∞ point-by-point.

Let n be an integer and let K_n be the kernel of the natural mapping of $\prod GL_2(\mathbb{Z}_\ell)$ onto $GL_2(\mathbb{Z}/(n))$.

Let G_1 be the functor which associates to S the set of isomorphism classes of elliptic curves $f\colon E \to S$ over S, equipped with an isomorphism $\varphi\colon \underline{\mathbb{Q}}^2 \xrightarrow{\sim} T_\mathbb{Q}(E)$, an isomorphism $\alpha_\infty\colon T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, and an isomorphism $\alpha_n\colon E_n \xrightarrow{\sim} (\mathbb{Z}/(n))^2$. One sees as in (3.3) that G_1 is isomorphic to the functor G_2 which associates to S the set of isomorphism classes of elliptic curves up to isogeny E over S, equipped with $\varphi\colon \mathbb{Q}^2 \xrightarrow{\sim} T_\mathbb{Q}(E)$, $\alpha_\infty\colon T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, and an isomorphism $V_f(E) \xrightarrow{\sim} \underline{\mathbb{A}}^{f2}$, given locally over S up to composition with an element of K_n. One such object is determined by the composite map φ' (given, locally, mod K_n) which is obtained from:

$$\varphi'\colon \mathbb{Q}^2 \xrightarrow{\varphi} T_\mathbb{Q}(E) \to T_\infty(E) \times V_f(E) \xrightarrow{\sim} \mathcal{O}_S \times \mathbb{A}^{f2}.$$

One has

$$E = \mathcal{O}_S/\varphi'(\mathbb{Q}^2 \cap \varphi'^{-1}(T_\infty(E) \times T_f(E))) = \widehat{\mathbb{Z}}^2 \backslash \mathcal{O}_S \times \mathbb{A}^{f2}/\varphi'(\mathbb{Q}^2),$$

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

$$K_n \backslash \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f2}).$$

Suppose still that $n \geq 3$, sot hat $GL_2(\mathbb{Q})$ acts freely on the preceding space. The analytic space M_n^{an} (resp. $M_n'^{a}n$) represents the analogous functor, in analytic geometry, to the functor that represents M_n (resp. M_n') beause this functor, call it X, is representable and the arros $X \to M_n^{\mathrm{an}}$ (resp. $X \to M_n'^{\mathrm{an}}$) induces a bijection on the sets of points with values in a general algebra of finite rank over $\mathbb{C}$.

Once deduces consequently from the preceeding that

$$M_n'^{\mathrm{an}} \sim K_n \backslash \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f2})/GL_2(\mathbb{Q}).$$

Proceeding the same for M_n, one obtains the first assertion of (3.8) by passage to the limit on n.

A point x of $\mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f^2})/GL_2(\mathbb{Q})$ is identified with a "lattice" L_x of $\mathbb{C} \times \mathbb{A}^{f2}$, and the curve corresponding to x is

$$E_x \sim \widehat{\mathbb{Z}}^2 \backslash \mathbb{C} \times \mathbb{A}^{f2}/L_x,$$

equipped with $V_f(E) \sim L_x \otimes \mathbb{A}^f \xrightarrow{\sim} \mathbb{A}^{f2}$. The last assertion of (3.8) follows easily from this. □

Denote by $f_n\colon E \to M_n$ the universal elliptic curve over M_n. The integer k being fixed, one makes the

Definition 3.9 *One denotes by W (or by ${}^kW$ if any confusion arises) the $\mathbb{Q}$-vector space*

$$W = \varinjlim_n \widetilde{H}^1(M_n^{\mathrm{an}}, \mathrm{Sym}^k(R^1 f_*(\underline{\mathbb{Q}}))) = \varinjlim {}_nW.$$

This vector space doesn't depend on the universal elliptic curve (up to isogeny) $f_\infty\colon E \to M_\infty$ so that, by transport of structure, if is equipped with a left action of the adelic group $GL_2(\mathbb{A}^f)$.

If ℓ is a prime number, the vector space $W_\ell = W \otimes \mathbb{Q}_\ell$ admits a purely algebraic definition, in terms of the ℓ-adic cohomology of the scheme over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ obtained by extension of scalars from M_n:

$$W_\ell = \varinjlim_n \widetilde{H}^1(M_n \otimes \overline{\mathbb{Q}}, \mathrm{Sym}^k(R^1 f_{n*}(\underline{\mathbb{Q}}_\ell))) = \varinjlim \ {}_nW_\ell \tag{3.10}$$

so that the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ acts, by transport of structure, on W_ℓ and the ${}_nW_\ell$.

Finally, the space M_n^{an} is the disjoint union of quotients of the Poincaré half-plane by congruence subgroups of $SL_2(\mathbb{Z})$, so that, denoting by ω the invertible sheaf on M_n defined by E, Shimura's theory (2.10) gives

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

This decomposition of $W \otimes \mathbb{C}$ into two complex conjugate subspace, one of which is the space of all cusp forms of weight $k+2$, relative to a general congruence subgroup of $SL_2(\mathbb{Z})$, is analogous to a Hodge decomposition ("of type $(0, k+1) + (k+1, 0)$").

The action of the adelic group commutes with the action of the Galois group and respects the preceding decomposition.

While the ℓ-adic local system $R^1 f_* \underline{\mathbb{Q}}_\ell$ is trivial on M_∞, I am unaware of whether there is a relation between W_ℓ and $\varinjlim(\widetilde{H}^1(M_n \otimes \overline{\mathbb{Q}}, \underline{\mathbb{Q}}_\ell)) \otimes \mathrm{Sym}^k(\mathbb{Q}_\ell^2)$.

(3.12) Let $n \geq 3$ be an integer and K_n as in (3.8). One has then $W^{K_n} = {}_nW$. This is verified by passage to the limit, and results from that in *rational cohomology*, the cohomology of the quotient of a space by a finite group is obtained by taking the invariants of this group in the cohomology.

Put, for p prime, $W^{(p)} = W^{GL_2(\mathbb{Z}_p)}$. By passage to the limit, one obtains

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

On this cohomology space acts again:

(i) the subgroup $\prod_{\ell \neq p} GL_2(\mathbb{Q}_\ell)$ of $GL_2(\mathbb{A}^f)$, because this subgroup centralizes $GL_2(\mathbb{Z}_p)$;

(ii) the Hecke algebra $\underline{H}(GL_2(\mathbb{Q}_p), GL_2(\mathbb{Z}_p))$, which is the algebra of integral mesasures on the discrete space $GL_2(\mathbb{Q}_p)/GL_2(\mathbb{Z}_p)$ invariant on the left by $GL_2(\mathbb{Z}_p)$: this subalgebra of the group algebra of $GL_2(\mathbb{Q}_p)$ acts on W and respects $W^{(p)}$. This algebra acts already on each of the ${}_nW$ for n prime to p.

The Hecke algebra admits as a basis the (measures associated to characteristic functions of) double cosets of $GL_2(\mathbb{Z}_p)$ in $GL_2(\mathbb{Q}_p)$, and one knows that

$$\underline{H}(GL_2(\mathbb{Q}_p), GL_2(\mathbb{Z}_p)) = \mathbb{Z}[T_p, R_p, R_p^{-1}],$$

where T_p and R_p are the double cosets of

$$\begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{pmatrix}.$$

(3.13) Let p be a prime number, $n \geq 3$ an integer prime to p, and $F_{n,p}$ the functor which associates to each scheme S the set of isomorphism classes of commutative diagrams of S-schemes

$$\begin{array}{ccc} & \underline{\mathbb{Z}}/(n)^2 & \\ \alpha \nearrow & & \nwarrow \alpha' \\ E_n & \longrightarrow & F_n \\ \cap & & \cap \\ E & \xrightarrow{\varphi} & F \end{array} \tag{3.14}$$

where ϕ is a p-isogeny between elliptic curves and α an isomorphism. One denotes by q_1 and $q_2 \colon F_{n,p} \to M_n$ the morphisms of functors associating to a diagram (3.14) the subdiagrams (E, E_n, α) and (F, F_n, α').

Proposition 3.15 *The functor $F_{n,p}$ is represented by a scheme $M_{n,p}$, and the morphisms $q_1, q_2 \colon M_{n,p} \to M_n$ are finite.*

The automorphism σ of $F_{n,p}$ sending $\varphi \colon E \to F$ to ${}^t\varphi \colon F \to E$ exchanges q_1 and q_2; it suffices thus to consider q_1. This morphism identifies $F_{n,p}$ with the functor of subgroups of order p of the universal elliptic curve E over M_n, so that, by the theory of Hilbert schemes, $F_{n,p}$ is representable and $M_{n,p}$ is proper over M_n. If s is a geometric point of M_n, $q_1^{-1}(s)$ is the set of subgroups of order p of E_s, and has $p+1$ elements if $char(k(s)) \neq p$, and only one (the kernel of Frobenius) if $char(k(s)) = p$. $\square$

One can show that $M_{n,p}$ is regular, and that q_1 and q_2 are finite flat; we don't use this delicate result, but we content ourselves here to note that over $\mathrm{Spec}(\mathbb{Z}[1/p])$, each q_i makes $M_{n,p}$ an étale covering of degree $p+1$ of M_n.

The morphisms q_i can be inserted into a commutative diagram

$$\begin{array}{ccccccccc} & & q_1^*E & & \xrightarrow{\varphi} & & q_2^*E & & \\ & \swarrow & & u \searrow & & \swarrow v & & \searrow & \\ E & & & & M_{n,p} & & & & E \\ & f_n \searrow & & \swarrow q_1 & & q_2 \searrow & & \swarrow f_n & \\ & & M_n & & & & M_n & & \end{array} \tag{3.16}$$

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

One denotes by I_p the morphism from M_n to M_n corresponding to the morphism of functors $(E, \alpha) \mapsto (E, \alpha/p)$:

$$\begin{array}{ccc} E & \longrightarrow & E \\ \downarrow & & \downarrow \\ M_n & \xrightarrow{I_p} & M_n \end{array} \qquad I_p^*(E, \alpha) = (E, \alpha/p). \tag{3.17}$$

I_p^* is an *automorphism* of $\widetilde{H}^i(M_n^{\mathrm{an}}, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}))$.

It is tiresome, but routine, to prove

Proposition 3.18 *(i) The endomorphism T_p of ${}_nW$ is expressed, with the aid of (3.16), as the composite map*

$$\begin{aligned}\widetilde{H}^1(M_n^{\mathrm{an}}, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}})) &\xrightarrow{q_2^*} \widetilde{H}^1(M_{n,p}^{\mathrm{an}}, \mathrm{Sym}^k(R^1 v_*\underline{\mathbb{Q}})) \\ &\xrightarrow{\varphi^*} \widetilde{H}^1(M_{n,p}^{\mathrm{an}}, \mathrm{Sym}^k(R^1 u_*\underline{\mathbb{Q}})) \xrightarrow{q_{1*}} \widetilde{H}^1(M_n^{\mathrm{an}}, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}})),\end{aligned}$$

where q_{1*} is the "trace morphism" for the covering q_1.

(ii) Similarly, $R_p = p^k I_p^*$. □

The distrustful reader could forget the adelic preliminaries and define T_p by (i).

When $n = 1$ or 2, one puts ${}_nW = W^{K_n}$, so that

$${}_1W = {}_nW^{GL_2(\mathbb{Z}/(n))}.$$

If S_{k+2} denotes the space of cusp forms, for the group $SL_2(\mathbb{Z})$, of weight $k+2$, the Shimura isomprhism (3.11) induces an isomorphism

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

It is tiresome, but routine, to prove

Proposition 3.19 *The endomorphism T_p of ${}_1^kW_\infty$ is identified, via the Shimura isomorphism, with the direct sum of the Hecke operator on S_{k+2} (including the factor p^{k-1}), and its conjugate.* □

(3.20) One has canonically

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

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

If $\underline{F}$ is a lcc $\mathbb{Q}_\ell$-sheaf over a smooth scheme X of pure dimension n over an algebraically closed field k, then Poincaré duality gives

$$\begin{aligned}H^i(X, \underline{F})^\vee &\sim H_c^{2n-i}(X, \underline{\mathrm{Hom}}(\underline{F}, \underline{\mathbb{Q}_\ell}(n))) \\ H_c^i(X, \underline{F})^\vee &\sim H^{2n-i}(X, \underline{\mathrm{Hom}}(\underline{F}, \underline{\mathbb{Q}_\ell}(n))) \\ \widetilde{H}^i(X, \underline{F})^\vee &\sim \widetilde{H}^{2n-i}(X, \underline{\mathrm{Hom}}(\underline{F}, \underline{\mathbb{Q}_\ell}(n))).\end{aligned}$$

Taking $X = \overline{M}_n$ and $\underline{F} = \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}_\ell})$ in these considerations, one defines a nondegenerate bilinear form ${}_n(\ ,\ )$ on ${}_n^kW_\ell$ with values in $\mathbb{Q}_\ell(-k-1)$. This form is symmetric for k odd, and alternating for k even. This is the ℓ-adic analogue of the Peterson inner product. If $n \mid m$, and if the covering $\psi\colon M_m \to M_n$ is of degree d, then one has

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

4 The Congruence Formula.

One fixes in this n° integers $k \geq 0$ and $n \geq 3$, and prime numbers p and ℓ. One supposes that p is prime to ℓ and n. One denotes by $f_n\colon E \to M_n$ the universal elliptic curve over M_n, equipped with $\alpha\colon E_n \xrightarrow{\sim} \mathbb{Z}/(n)^2$.

Whatever the scheme Y, one denotes by a the unique morphism of Y to $\mathrm{Spec}(\mathbb{Z})$, or, if necessary, 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, one denotes by $R^i a_*(Y, \underline{F})$ (resp. $R^i a_!(Y, \underline{F})$, resp. $R^i \widetilde{a}(Y, \underline{F})$) the $\mathbb{Z}_\ell$- or $\mathbb{Q}_\ell$-sheaf over $\mathrm{Spec}(\mathbb{Z})$ that is the ith higher direct image of $\underline{F}$ under a (resp. ith direct image with proper supports, resp. $\mathrm{Im}(R^i a_!(Y, \underline{F}) \to R^i a_*(Y, \underline{F}))$). One puts, for $m \in \mathbb{N}$, $Y[1/m] = Y \times \mathrm{Spec}(\mathbb{Z}[1/m])$.

Theorem 4.1 (Igusa [1]) *The scheme M_n can be compactified to a scheme of curves M_n^* that is projective and smooth over* $\mathrm{Spec}(\mathbb{Z}[1/n])$*, such that $M_n^* \backslash M_n$ is an étale covering of* $\mathrm{Spec}(\mathbb{Z}[1/n])$.

The schemes M_n is formally smooth, thus smooth over $\mathrm{Spec}(\mathbb{Z})$.

The modular invariant j of the universal curve over M_n is a morphism of M_n to the affine line A^1 over $\mathrm{Spec}(\mathbb{Z}[1/n])$. The morphism j is finite, and is an étale covering away from the sections 0 and 1728 of A^1; in fact:

(a) Two elliptic curves over an algebraically closed field with the same j-invariant are isomorphic (e.g., [8] 6.3), thus the geometric fibers of j are finite. The schemes M_n and A^1 being smooth of the same 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, of j-invariant in R, and whose points of order n are rational over K, then E has a good reduction. The valuative criterion for properness shows thus that j is proper.

(c) If E and F are two elliptic curves over a scheme S, of the same j-invariant, and if j and $j - 1728$ are invertible, then the scheme $\underline{\mathrm{Isom}}(S; E, F)$ of isomorphisms between E and F is étale over S ([8] 6.3). In the diagram

$$\begin{array}{ccc} \underline{\mathrm{Isom}}(M_n \times_{A^1} M_n; \mathrm{pr}_1^* E, \mathrm{pr}_2^* E) & \sim & M_n \times GL_2(\mathbb{Z}/(n)) \\ \downarrow u & & \downarrow v \\ M_n \times_{A^1} M_n & \xrightarrow{\mathrm{pr}_1} & M_n \end{array},$$

where $j \neq 0,\ 1728$, u and v are étale surjective, thus pr_1 is étale and, by flat descent, j is étale.

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

It results from the same theorem that the lcc $\mathbb{Z}_\ell$-sheaves $R^i f_{n*} \underline{\mathbb{Z}_\ell}$ on $M_n[1/\ell]$ are moderately ramified at infinity. Hence, from (4.1) and the specialization theorems for ℓ-adic cohomology (see [5]), it results that $R^i a_*(M_n, \mathrm{Sym}^k(R^1 f_{n*} \underline{\mathbb{Z}_\ell}))$, $R^i a_!(M_n, \mathrm{Sym}^k(R^1 f_{n*} \underline{\mathbb{Z}_\ell}))$, and thus $R^i \widehat{a}(M_n, \mathrm{Sym}^k(R^1 f_{n*} \underline{\mathbb{Z}_\ell}))$ are lcc $\mathbb{Z}_\ell$-sheaves over $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$, whose formation is compatible with all base changes.

Corollary 4.2 *The Galois module ${}_nW_\ell$ is the fiber of the lcc $\mathbb{Q}_\ell$-sheaf*

$$R^i\widetilde{a}(M_n, \mathrm{Sym}^k(R^1f_{n*}\underline{\mathbb{Z}_\ell})) \otimes \mathbb{Q}_\ell$$

over $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$ *at the geometric point $\overline{\mathbb{Q}}$. It is unramified away from n and ℓ.* □

Let the two commutative diagrams over $M_n \otimes \mathbb{F}_p$

$$\begin{array}{ccc} & \underline{\mathbb{Z}}/(n)^2 & \\ \alpha \nearrow & & \nwarrow \alpha^{(p)} \\ E_n & \longrightarrow & E_n^{(p)} \\ \cap & & \cap \\ E & \xrightarrow{F} & E^{(p)} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} & \underline{\mathbb{Z}}/(n)^2 & \\ p\alpha^{(p)} \nearrow & & \nwarrow \alpha \\ E_n^{(p)} & \longrightarrow & E_n \\ \cap & & \cap \\ E^{(p)} & \xrightarrow{V} & E \end{array},$$

be written more briefly

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

where F is the Frobenius morphism and V, its transpose, is the "Verschiebung." These diagrams define morphism Φ_1 and Φ_2 of $M_n \otimes \mathbb{F}_p$ to $M_{n,p}$. These morphisms are finite, considered as sections of q_1 and q_2, and define a morphism

$$\Phi = \Phi_1 \amalg \Phi_2 \colon M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p \to M_{n,p} \otimes \mathbb{F}_p.$$

Let Φ^h be the restriction of Φ to the opens M_n^h and $M_{n,p}^h$ of $M_n \otimes \mathbb{F}_p$ and $M_{n,p} \otimes \mathbb{F}_p$ corresponding to curves of nonzero Hasse invariant h.

Proposition 4.3 *Φ^h is an isomorphism.*

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

Proposition 4.4 *(i) The scheme $M_{n,p}$ is smooth over* $\mathrm{Spec}(\mathbb{Z})$ *away from points of characteristic p where $h = 0$.*

(ii) The morphisms q_1 and q_2 induce finite flat morphisms q_1' and q_2' from the normalization $M_{n,p}'$ of $M_{n,p}$ to M_n.

(iii) The morphism Φ can be factored through a surjective morphism

$$\Phi'\colon M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p \to M_{n,p}' \otimes \mathbb{F}_p.$$

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 $M_{n,p}$ where the kernel of φ is infinitesimal: there is no obstruction to infinitesimally lifting an elliptic curve and the infinitesimal part of the kernel of multiplication by p.

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

The Hecke endomorphism T_p of ${}_nW_\ell$, such as is made explicit in (3.18), is the tensorization with $\mathbb{Q}_\ell$ of the fiber at the geometric point $\overline{\mathbb{Q}}$ of $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$ of the endomorphism (again denoted by T_p) of $R^1\widetilde{a}(M_n, \mathrm{Sym}^k(R^1 f_{n*}(\underline{\mathbb{Z}_\ell})))$ defined by the "correspondence"

$$\begin{array}{ccccccccc} & & {q'_1}^*E & & \xrightarrow{\varphi} & & {q'_2}^*E & & \\ & \swarrow & & \searrow u & & v \swarrow & & \searrow & \\ E & & & & M'_{n,p} & & & & E \ , \\ & f_n \searrow & & \swarrow q'_1 & & q'_2 \searrow & & \swarrow f_n & \\ & & M_n & & & & M_n & & \end{array} \tag{4.5}$$

$$T_p = q'_{1*}\varphi^* {q'_2}^* \quad \text{(cf. 3.18)}.$$

The endomorphisms R_p and I_p can be interpreted in the same way.

Lemma 4.6 *Let X, Y, Z_1, and Z_2 be four schemes that are separated and of finite type over a noetherian scheme S, let $\underline{F}$ be a $\mathbb{Z}_\ell$-sheaf on X, $\underline{G}$ a $\mathbb{Z}_\ell$-sheaf on Y, and denote by a each of the structural maps from X, Y, Z_1 or Z_2 to S. Suppose we have the following commutative diagram of S-schemes and morphisms of sheaves:*

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

$$\begin{array}{ccc} Z_1 & \xrightarrow{f} & Z_2 \\ x_1 \downarrow & \swarrow x_2 & \\ X & & \end{array} \qquad\qquad \begin{array}{ccc} Z_1 & \xrightarrow{f} & Z_2 \\ & y_1 \searrow & \downarrow y_2 \\ & & Y \end{array}$$

Suppose 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 their fibers (for x_1) of the geometric points of Z_1 in the inverse image of s under f. Then, the diagram

$$\begin{array}{ccccccc} R^i\widetilde{a}(Y,\underline{G}) & \xrightarrow{y_1^*} & R^i\widetilde{a}(Z_1,\underline{G}) & \xrightarrow{z_1} & R^i\widetilde{a}(Z_1,\underline{F}) & \xrightarrow{x_{1*}} & R^i\widetilde{a}(X,\underline{F}) \\ \| & & f^*\uparrow & & f^*\uparrow & & \| \\ R^i\widetilde{a}(Y,\underline{G}) & \xrightarrow{y_2^*} & R^i\widetilde{a}(Z_2,\underline{G}) & \xrightarrow{z_2} & R^i\widetilde{a}(Z_2,\underline{F}) & \xrightarrow{x_{2*}} & R^i\widetilde{a}(X,\underline{F}) \end{array}$$

commutes.

This lemma results from the analogous lemmas for $R^ia_!$ and R^ia_*. The commutativity of the first squares is trivial. The last is rewritten

$$\begin{array}{ccccc} R^i\widetilde{a}(Z_1, x_1^*\underline{F}) & \xleftarrow{\sim} & R^i\widetilde{a}(X, x_{1*}x_1^*\underline{F}) & \xrightarrow{\mathrm{Tr}} & R^i\widetilde{a}(X,\underline{F}) \\ \uparrow & & \uparrow & & \| \\ R^i\widetilde{a}(Z_2, x_2^*\underline{F}) & \xleftarrow{\sim} & R^i\widetilde{a}(X, x_{2*}x_2^*\underline{F}) & \xrightarrow{\mathrm{Tr}} & R^i\widetilde{a}(X,\underline{F}) \end{array}$$

and one recalls the definition of the trace in verifying that the square

$$\begin{array}{ccc} x_{1*}x_1^*\underline{F} & \xrightarrow{\mathrm{Tr}} & \underline{F} \\ \uparrow & & \| \\ x_{2*}x_2^*\underline{F} & \xrightarrow{\mathrm{Tr}} & \underline{F} \end{array}$$

is commutative. $\square$

(4.7) One denotes by $T_p/\mathbb{F}_p$ the endomorphism induced by T_p on the restriction to $\mathrm{Spec}(\mathbb{F}_p)$ of the lcc $\mathbb{Z}_\ell$-sheaf $R^1\widetilde{a}(M_n, \mathrm{Sym}^k R^1 f_{n*}\underline{\mathbb{Z}_\ell})$. One has

$$R^1\widetilde{a}(M_n, \mathrm{Sym}^k R^1 f_{n*}\underline{\mathbb{Z}_\ell}) \mid \mathrm{Spec}(\mathbb{F}_p) \xrightarrow{\sim} R^1\widetilde{a}(M_n \otimes \mathbb{F}_p, \mathrm{Sym}^k R^1 f_{n*}\underline{\mathbb{Z}_\ell});$$

the formation of the trace morphism for a finite flat morphism is compatible with change of base, so that $T_p/\mathbb{F}_p$ can be constructed, over the model (3.18), starting from the *fiber* over $\mathbb{F}_p$ of the "correspondence" (4.5). Lemma (4.6), applied to the commutative diagrams

$$\begin{array}{ccc} M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p & \xrightarrow{\Phi'} & M'_{n,p} \otimes \mathbb{F}_p \\ \downarrow & \swarrow q'_1 & \\ M_n \otimes \mathbb{F}_p & & \end{array} \qquad \begin{array}{ccc} M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p & \xrightarrow{\Phi'} & M'_{n,p} \otimes \mathbb{F}_p \\ & q'_2 \searrow & \downarrow \\ & & M_n \otimes \mathbb{F}_p, \end{array}$$

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

$$\text{(a)} \qquad \begin{array}{ccccccccc} & & (E,\alpha) & & \xrightarrow{F} & & (E^{(p)},\alpha^{(p)}) = F^*(E,\alpha) & & \\ & // & & \searrow & & \swarrow & & \searrow & \\ (E,\alpha) & & & & M_n \otimes \mathbb{F}_p & & & & (E,\alpha) \\ & \searrow & & // & & \searrow F & & \swarrow & \\ & & M_n \otimes \mathbb{F}_p & & & & M_n \otimes \mathbb{F}_p & & \end{array}$$

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

$$\text{(b)} \qquad \begin{array}{ccccccccc} & & x^*(E,\alpha) = (E^{(p)}, p\alpha^{(p)}) & & \xrightarrow{V} & & (E,\alpha) & & \\ & \swarrow & & f_n^{(p)} \searrow & & \swarrow f_n & & \backslash\backslash & \\ (E,\alpha) & & & & M_n \otimes \mathbb{F}_p & & & & (E,\alpha) \cdot \\ & \searrow & & \swarrow x & & \backslash\backslash & & \swarrow & \\ & & M_n \otimes \mathbb{F}_p & & & & M_n \otimes \mathbb{F}_p & & \end{array}$$

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

$$\begin{array}{ccccc} (E,\alpha) & \longleftarrow & (E, p\alpha) & \longleftarrow & (E^{(p)}, p\alpha^{(p)}) \\ \downarrow & & \downarrow & & \downarrow \\ M_n \otimes \mathbb{F}_p & \xleftarrow{I_p^{-1}} & M_n \otimes \mathbb{F}_p & \xleftarrow{F} & M_n \otimes \mathbb{F}_p \end{array} .$$

The corresponding endomorphism is thus the composite of

$$\begin{aligned} V \quad : \quad & R^1\widetilde{a}(M_n \otimes \mathbb{F}_p, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}_\ell})) \xrightarrow{V^*} R^1\widetilde{a}(M_n \otimes \mathbb{F}_p, \mathrm{Sym}^k(R^1 f_{n*}^{(p)}\underline{\mathbb{Z}_\ell})) \\ & \xrightarrow{\mathrm{Tr}_F} R^1\widetilde{a}(M_n \otimes \mathbb{F}_p, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}_\ell})) \end{aligned}$$

and of

$$I_p^* = \mathrm{Tr}_{I_p^{-1}} \colon \text{endomorphism of } R^1\widetilde{a}(M_n \otimes \mathbb{F}_p, \mathrm{Sym}^k R^1 f_{n*}\underline{\mathbb{Z}}_\ell).$$

Proposition 4.8 *One has* $T_p/\mathbb{F}_p = F + I_p^* V$, *and*

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

(ii) F *and* V *are transposes of one another, relative to the scalar product (3.20).*

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

For the relation (i) between the geometric and arithmetic Frobenius, one is referred to the exposé of C. Houzel (SGA 5.XV). The composite VF is the composite of the homomorphisms obtained from the following maps:

$$\begin{array}{ccccccccc} E & \leftarrow & E^{(p)} & \xrightarrow{F_E} & E & \xrightarrow{V_E} & E^{(p)} & \rightarrow & E \\ \downarrow & & & \searrow & \downarrow & \swarrow & & & \downarrow \\ M_n & & & \xrightarrow{F} & M_n & & \xrightarrow{F} & & M_n \end{array}$$

$$VF = \mathrm{Tr}_F \circ F_E^* \circ V_E^* \circ F^*.$$

The map $F_E^* V_E^* = (F_E V_E)^* = (p \cdot 1_E)^*$ acts by multiplication by p^k on $\mathrm{Sym}^k R^1 f_{n*}\underline{\mathbb{Z}}_\ell$, so that $VF = p^k \cdot \mathrm{Tr}_F \circ F^* = p^k \cdot p = p^{k+1}$ because $F \colon M_n \to M_n$ is of degree p.

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

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

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

Theorem 4.9 (The Congruence Formula) *Let* $K_{n,\ell}$ *be the largest subextension of* $\overline{\mathbb{Q}}$ *that is unramified away from* n *and* ℓ*, 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* ${}_nW_\ell$*, and let* V *be the transpose of* F *relative to the scalar product (3.20). Then,*

$$T_p = F + I_p^* V, \qquad FV = p^{k+1}, \qquad \textit{and} \qquad 1 - T_p X + pR_p X^2 = (1 - FX)(1 - I_p^* V X). \quad \square$$

5 Weil implies Ramanujan

If p is a prime number and X a scheme over $\mathbb{F}_p$, then one denotes by $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$, by $F \colon X \to X$ the ("geometric") Frobenius endomorphism, and one puts $\overline{X} = X \otimes \overline{\mathbb{F}}_p$; ℓ always denotes a prime number different from p.

By the "Weil conjectures," one means to claim the following:

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

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

Theorem 5.1 *If the Weil conjectures are true, then the absolute values of the endomorphism F of ${}^k_nW_\ell$ are algebraic integers (all of whose complex conjugates are) of absolute value $p^{k+1/2}$.*

Assume 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 in a smooth projective scheme X^*. Then, the absolute values of endomorphism F^* of $\widetilde{H}^i(\overline{X}, \mathbb{Q}_\ell)$ are algebraic integers of absolute value $p^{i/2}$.*

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

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

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

Lemma 5.3 (modulo Weil) *Let S be a smooth scheme over $\mathbb{F}_p$ and $f\colon A \to S$ an abelian scheme over S. Suppose that A can be represented as an open in a projective smooth scheme A^* over $\mathbb{F}_p$. Then, the geometric Frobenius F^* of $\widetilde{H}^i(\overline{S}, R^jf_*\underline{\mathbb{Q}_\ell})$ a eigenvalues that are algebraic integers of absolute value $p^{i+j/2}$.*

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

$$\begin{aligned} E &: \quad E_2^{ij} = H^i(\overline{S}, R^jf_*\underline{\mathbb{Q}_\ell}) \implies H^{i+j}(\overline{A}, \mathbb{Q}_\ell), \\ {}_cE &: \quad {}_cE_2^{ij} = H^i_c(\overline{S}, R^jf_*\underline{\mathbb{Q}_\ell}) \implies H^{i+j}_c(\overline{A}, \mathbb{Q}_\ell). \end{aligned}$$

The endomorphism of multiplication by m: $\psi_m = m \cdot 1_A$, defines endomorphisms of E and ${}_cE$ that fit into a commutative diagram:

$$\begin{array}{ccc} {}_cE & \to & E \\ \psi_m^* \downarrow & & \psi_m^* \downarrow \\ {}_cE & \to & E \end{array} .$$

ψ_m^* acts on $R^jf_*\underline{\mathbb{Q}_\ell}$ by multiplication by m^j, so that ψ_m^* acts is multiplication by m^j on the terms ${}_cE_r^{ij}$ and E_r^{ij} of ${}_cE$ and E. The maps d_r ($r \geq 2$) commute with ψ_m^*, and send E_r^{ij} (resp. ${}_cE_r^{ij}$) to $E_r^{i'j'}$ (resp. ${}_cE_r^{i'j'}$) with $j \neq j'$. These are nonzero, and E_2^{ij} (resp. ${}_cE_2^{ij}$) can be identified with a subspace of $H^{i+j}(\overline{A}, \mathbb{Q}_\ell)$ (resp. of $H^{i+j}_c(\overline{A}, \mathbb{Q}_\ell)$) where $\psi_m^* = m^j$. Consequently, $\widetilde{H}^i(\overline{S}, R^jf_*\mathbb{Q}_\ell)$ is identified, as a Galois module, with a subspace of $\widetilde{H}^{i+j}(\overline{A}, \mathbb{Q}_\ell)$ where $\psi_m^* = m^j$ and one applies (5.2). The trick used here is due to Lieberman. □

Let $f_n\colon E \to M_n \otimes \mathbb{F}_p$ be the universal elliptic curve over $M_n \otimes \mathbb{F}_p$, let $f_{n,k}\colon E_k \to M_n \otimes \mathbb{F}_p$ be its k-fold fiber product with itself. The Kunneth formula shows that the $\mathbb{Q}_\ell$-sheaf $R^kf_{n,k*}\underline{\mathbb{Q}_\ell}$ admits as a direct factor the k-fold tensor power of $R^1f_{n*}\underline{\mathbb{Q}_\ell}$; the latter in turn contains as a direct factor the $\mathbb{Q}_\ell$-sheaf $\mathrm{Sym}^k(R^1f_{n*}\mathbb{Q}_\ell)$. Theorem 5.1 results thus from (5.3) and

Lemma 5.4 *The scheme E_k is an open in a smooth projective scheme E_k^* over $\mathbb{F}_p$.*

Let E^* be the Néron minimal model of E over $M_n^* \otimes \mathbb{F}_p$ (4.1). The scheme E^* is smooth and projective over $\mathbb{F}_p$. Since $n \geq 3$ and the points of order n of E form a trivial covering of $M_n \otimes \mathbb{F}_p$, the Néron model is "semistable" (case a or $\mathrm{b}_{\mathfrak{m}}$ in Néron's classification). In particular, the projection $f_n \colon E^* \to M_n^*$ has only a finite number of nonsmooth points, and at these points, f_n is nondegenerate (presents an ordinary quardratic singularity).

Let E_k^{**} be the k-fold fiber product of E^* over M_n^*. To prove (5.4), it suffices to resolve the singularities of E_k^{**} without touching the open E_k. We prove first:

Lemma 5.5 *Let V be the subvariety of affine space over a field k (coordinates $(X_i)_{0 \leq i \leq r}$, $(Y_i)_{0 \leq i \leq r}$, $(T_i)_{1 \leq i \leq s}$) with equation*

$$X_0 Y_0 = X_1 Y_1 = \cdots = X_r Y_r.$$

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

The singular locus is the place where the four coordinates X_i, Y_i, X_j, Y_j $(i \neq j)$ vanish. The open affine of $\widetilde{V}$ defined by the element $\prod_{i=0}^r X_i^i$ of the ideal $\mathfrak{m}$ of blowing up is the spectrum of the regular ring

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

(for the proof, note that $X_i/X_{i+1} = Y_{i+1}/Y_i$), and 5.5 results. □

One shows still that, locally for the étale topology, the singularities of E_k^{**} are isomorphic to those of V (for $r = k-1$), and that this aloows the definition on E_k^{**} of an ideal $\mathfrak{m}$ analogous to the ideal $\mathfrak{m}$ of (5.5). Blowing up this ideal, one obtains E_k^*. □

An approximation to the following theorem has been proven by Ihara [2]:

Theorem 5.6 *The Weil conjectures imply the Ramanujan conjecture.*

We note first that (5.1) is true for $n = 1$, because ${}_1^k W_\ell$ is the Galois submodule of ${}_m^k W_\ell$ invariant under $GL_2(\mathbb{Z}/(m))$. On ${}_1^k W_\ell$, I_p^* induces the identity, and (4.8) reduces to

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

The endomorphisms F and V are transposes of each other, so that

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

The action of T_p on ${}_1^k W_\ell$ is induced by its action on ${}_1^k W$, and is compatible with the decomposition of ${}_1^k W \otimes \mathbb{C}$ into the sum of the space S_{k+2} of cusp forms relative to $SL_2(\mathbb{Z})$ of weight $k+2$, and of the complex conjugate space. From the Hermitian property for T_p (for the Peterson inner product), and from (3.19), one deduces then that

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

and

$$\det(1 - T_pX + p^{k+1}X^2; S_{k+2})^2 = \det(1 - FX; {}^k_1W_\ell)^2,$$

so that

$$\det(1 - T_pX + p^{k+1}X^2; S_{k+2}) = \det(1 - FX; {}^k_1W_\ell). \tag{5.7}$$

Resume the notations of n° 1 and make $k = 10$. By vurtue of Hecke's theory and of (3.19), (5.7) can be rewritten

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

and one applies (5.1). □

One verifies in the same way that the Weil conjectures imply Pertersson's generalization of the Ramanujan conjecture.

References

[1] J. Igusa — *Kroneckerian model of fields of elliptic modular functions*, Am. J. of Math., **81** 1959, p. 561–577.

[2] Y. Ihara — *Hecke polynomials as congruence zeta functions in elliptic modular case*, Ann. of Math., S.2 **85** 1967, p. 267–295.

[3] J.-P. Jouanolou — Exposés V and VI of SGA 5.

[4] M. Kuga and G. Shimura — *On the zeta function of a fibre variety whose fibers are abelian varieties*, Ann. of Math., S.2 **82** 1965, p. 478–539.

[5] M. Raynaud — Exposé XIII of SGA 1 and appendix (in preparation).

[6] J.-P. Serre — *Une interpreétation des congruences relatives á la fonction τ de Ramanujan*, Sém. Delange–Pistot–Poitou, 1967/68, n° 14.

[7] G. Shimura — *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. of Japan, **11** 1959, p. 291–311.

[8] J. Tate — *Courbes elliptiques: formulaire — mis au gout du jour par P. Deligne*, Mimeographed notes by I.H.E.S.

[9] J.-L. Verdier — *Sur les intégrales attachées aux formes automorphes* (d'apres G. Shimura). Sém. Bourbaki, Févier 1961, exp. 216.

Initials:

EGA: *Eléments de géométrie algébrique*, by A. Grothendieck and J. Dieudonné, Publ. Math. I.H.E.S.

SGA: *Séminaire de géométrie algébrique du Bois-Marie*, Mimeographed notes by I.H.E.S., in preparation by North-Holland.