

# COMPOSITIO MATHEMATICA

ENRIC NART

**Formal group laws for certain formal groups  
arising from modular curves**

*Compositio Mathematica*, tome 85, n° 1 (1993), p. 109-119

[http://www.numdam.org/item?id=CM\\_1993\\_\\_85\\_1\\_109\\_0](http://www.numdam.org/item?id=CM_1993__85_1_109_0)

© Foundation Compositio Mathematica, 1993, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

## Formal group laws for certain formal groups arising from modular curves

ENRIC NART

*Dept. de Matemàtiques, Univ. Autònoma Barcelona, Edifici C, 08193 Bellaterra, Barcelona, Spain*

Received 10 July 1991; accepted 11 November 1991

Let  $N \geq 5$  be an odd square-free natural number. Let  $\mathcal{J}_{\mathbb{Z}}^{\text{new}}$  be the Néron model of  $J_0(N)^{\text{new}}$ , the new part of the jacobian of the modular curve  $X_0(N)_{\mathbb{Q}}$ . In [De-Na] we proved that the formal completion of  $\mathcal{J}^{\text{new}}$  along the zero section is determined by the relative L-series of  $J_0(N)^{\text{new}}$  with respect to  $\mathbb{T} \otimes \mathbb{Q}$ , where  $\mathbb{T}$  is the Hecke algebra. In fact, we explained how to construct a formal group law for  $(\mathcal{J}^{\text{new}})^{\wedge}$  from a formal Dirichlet series made with the integral matrices reflecting the action of the Hecke operators on the Lie algebra of  $\mathcal{J}^{\text{new}}$ .

In this note we apply this result to show that a formal version of the Shimura–Taniyama–Weil conjecture implies the conjecture itself. In Section 2 we give first an effective version of the mentioned theorem of [De-Na]. We show that a formal group law for  $(\mathcal{J}^{\text{new}})^{\wedge}$  can also be constructed with the integral matrices deduced from the action of the Hecke operators on the  $\mathbb{Z}$ -module  $S^{\text{new}}$  of all cusp forms (of weight two, with respect to  $\Gamma_0(N)$ ) with integral Fourier development at infinity and belonging to the new part. In Section 3, as an application of this computation of  $(\mathcal{J}^{\text{new}})^{\wedge}$  we prove the following: if  $\mathcal{E}_{\mathbb{Z}}$  is the Néron model of an elliptic curve  $E_{\mathbb{Q}}$  with conductor  $N$ , then, the existence of a non-trivial homomorphism of formal groups over  $\mathbb{Z}$ :  $(\mathcal{J}^{\text{new}})^{\wedge} \rightarrow \mathcal{E}^{\wedge}$  is sufficient to imply the existence of a non-trivial homomorphism:  $J_0(N)^{\text{new}} \rightarrow E$ .

### 1. The action of Hecke

Let  $N \geq 5$  be an odd square-free integer. Let  $M_0(N)$  be the curve over  $\text{Spec}(\mathbb{Z})$  representing the moduli stack classifying generalized elliptic curves with a cyclic subgroup of order  $N$  [Ka-Ma]. If  $d, D$  are positive integers such that  $dD \mid N$ , one has a finite morphism:

$$B_d: M_0(N) \rightarrow M_0(D),$$

defined by the rule [Ma2, §2]:

$$(E, (H_d, H_D, H_{N/dD})) \rightarrow (E/H_d, H_D).$$

Let  $X_0(N) \xrightarrow{i} M_0(N)$  be the minimal regular resolution of  $M_0(N)$  over  $\text{Spec}(\mathbb{Z})$ . Let us denote  $X = X_0(N)$ ,  $X' = X_0(D)$ . The morphisms  $B_d$  extend to finite morphisms between the minimal regular resolutions, hence, they induce homomorphisms:

$$\text{Pic}_{X/\mathbb{Z}}^0 \xrightleftharpoons[(B_d)^*]{(B_d)_*} \text{Pic}_{X'/\mathbb{Z}}^0.$$

$(B_d)^*$  is the usual operator on invertible sheaves, whereas  $(B_d)_*$  is the norm-homomorphism [Gr, 6.5]. One gets homomorphisms:

$$\begin{aligned} H^1(X, \mathcal{O}) &\xrightleftharpoons[(B_d)^*]{(B_d)_*} H^1(X', \mathcal{O}) \\ H^0(X, \Omega) &\xrightleftharpoons[(B_d)^*]{(B_d)_*} H^0(X', \Omega), \end{aligned} \tag{1.1}$$

the former by the identification of  $H^1(X, \mathcal{O})$  with the tangent space of  $\text{Pic}^0$  at zero; the latter by Grothendieck's duality.  $\Omega_X$  is the dualizing sheaf, that is, the sheaf of regular differentials, which is defined as the only non-vanishing homology group (in degree  $-1$ ) of the complex  $R\pi^! \mathcal{O}_{\text{Spec}(\mathbb{Z})}$ , where  $\pi$  is the structural morphism of  $X$ .

(1.2) PROPOSITION. *After tensoring with  $\mathbb{Q}$ , both homomorphisms  $(B_d)^*$  in (1.1) are the natural ones induced by  $B_d: X_{\mathbb{Q}} \rightarrow X'_{\mathbb{Q}}$ .*

*Proof.* This is a well-known general fact. The identification of  $H^1(X_{\mathbb{Q}}, \mathcal{O})$  with the tangent space of  $\text{Pic}^0$  is realized through the exact sequence:

$$0 \longrightarrow H^1(X_{\mathbb{Q}}, \mathcal{O}) \xrightarrow{\text{exp}} H^1(X_{\mathbb{Q}} \otimes \mathbb{Q}[\varepsilon], \mathcal{O}^*) \longrightarrow H^1(X_{\mathbb{Q}}, \mathcal{O}^*),$$

where  $\mathbb{Q}[\varepsilon]$  is the ring of dual numbers and  $\text{exp}(s) = 1 + s\varepsilon$ . Easy computation with Čech cocycles shows that, at the level of  $H^1(X_{\mathbb{Q}}, \mathcal{O})$ ,  $(B_d)^*$  induces the natural homomorphism and  $(B_d)_*$  induces the trace-homomorphism. Now the classical trace formula [Se, p. 32] shows that the Serre-dual homomorphism of  $(B_d)_*$  is the natural operation on differentials.  $\square$

For any prime  $p$  dividing  $N$ , the Atkin involution  $w_p$  extends to an involution of  $M_0(N)$  [Ka-Ma] and by minimality to an involution of  $X_0(N)$  commuting with  $i$ .

For any prime  $l$  not dividing  $N$ , the Hecke operator  $T_l$  is, by definition, the endomorphism of  $J_0(N)$  induced by the correspondence on  $X_0(N)_{\mathbb{Q}}$  determined by the morphisms:

$$\begin{array}{c}
 X_0(N)_{\mathbb{Q}} \\
 \uparrow \\
 B \\
 X_0(Nl)_{\mathbb{Q}} \\
 B_l \\
 \downarrow \\
 X_0(N)_{\mathbb{Q}},
 \end{array}$$

where we denote  $B=B_l$ . That is,  $T_l$  is the composition of the two homomorphisms:

$$T_l: J_0(N) \xrightarrow{(B_l)^*} J_0(Nl) \xrightarrow{B_*} J_0(N).$$

The Hecke algebra is by definition the subalgebra  $\mathbb{T}$  of  $\text{End}_{\mathbb{Q}}(J_0(N))$  generated by all  $T_l$  and  $w_p$ .

By the universal property,  $T_l$  operates on the Néron model  $\mathcal{J}$  of  $J_0(N)$  and on its connected component as:

$$T_l: \mathcal{J}^0 \xrightarrow{(B_l)^*_{\mathbb{Z}}} (\mathcal{J}')^0 \xrightarrow{(B_*)_{\mathbb{Z}}} \mathcal{J}^0,$$

where  $\mathcal{J}'$  is the Néron model of  $J_0(Nl)$ . By a theorem of Raynaud [Ra, 8.1.4],  $\mathcal{J}^0$  represents the functor  $\text{Pic}^0_{X_0(N)/\mathbb{Z}}$ . Hence, at the level of  $\text{Pic}^0$ , the homomorphisms  $(B_l)^*$ ,  $B_*$  coincide with  $(B_l)^*_{\mathbb{Z}}$ ,  $(B_*)_{\mathbb{Z}}$ , since they induce the same homomorphism on the generic fiber. Hence,  $T_l$  operates on  $H^1(X, \mathcal{O})$  and on  $H^0(X, \Omega)$ , always by the same rule:  $T_l = B_* (B_l)^*$ , with the homomorphisms  $B_*$ ,  $(B_l)^*$  considered in (1.1).

Let  $S_2(\Gamma_0(N), \mathbb{Z})$  be the lattice of cusp forms of weight 2, with respect to  $\Gamma_0(N)$ , with integral Fourier coefficients. The following theorem is essentially due to Mazur:

(1.3) THEOREM. *Lie*  $(\mathcal{J})$  and  $S_2(\Gamma_0(N), \mathbb{Z})$  are isomorphic as  $\mathbb{T}$ -modules.

*Proof.* Let us denote  $X=X_0(N)$ ,  $X'=X_0(Nl)$ ,  $M=M_0(N)$ ,  $M'=M_0(Nl)$ . Consider the canonical isomorphisms:

$$\text{Lie}(\mathcal{J}) \simeq T_0(\mathcal{J})^\vee \simeq H^1(X, \mathcal{O})^\vee \simeq H^0(X, \Omega),$$

with compatible (by definition) action of  $\mathbb{T}$  everywhere. We need to check the compatibility of the action of  $\mathbb{T}$  on  $H^0(X, \Omega)$  with the action on  $H^0(M, \Omega)$  as defined by Mazur in [Ma1]. More precisely, we need the following diagrams to commute:

$$\begin{array}{ccc}
 H^1(X', \mathcal{O}) & \xleftarrow{B^*} & H^1(X, \mathcal{O}) \\
 \uparrow i^* & & \uparrow i^* \\
 H^1(M', \mathcal{O}) & \xleftarrow{c^*} & H^1(M, \mathcal{O}) \\
 H^0(X', \Omega) & \xleftarrow{(B)_*} & H^0(X, \Omega) \\
 \downarrow i_* & & \downarrow i_* \\
 H^0(M', \Omega) & \xleftarrow{(c_w)_*} & H^0(M, \Omega),
 \end{array} \tag{1.4}$$

where  $i_*$  is defined from  $i^*$  by duality and  $c^*, c_*$  are as in [Ma1, p. 88]. The same argument as in [Ma1, II, Lemma 3.3] shows that all the  $\mathbb{Z}$ -modules involved are free; hence, the commutativity of the diagrams can be checked after tensoring with  $\mathbb{Q}$ . Then, it is a consequence of (1.2). Taking the dual diagram of (1.4) we have a commutative diagram:

$$\begin{array}{ccccc}
 H^0(X, \Omega) & \xrightarrow{(B)_*} & H^0(X', \Omega) & \xrightarrow{B_*} & H^0(X, \Omega) \\
 \downarrow i_* & & \downarrow i_* & & \downarrow i_* \\
 H^0(M, \Omega) & \xrightarrow{(c_w)_*} & H^0(M', \Omega) & \xrightarrow{c_*} & H^0(M, \Omega),
 \end{array}$$

showing that the isomorphism  $i_*$  (same proof as [Ma1, II, Prop. 3.4]) is a  $\mathbb{T}$ -isomorphism. Finally,  $H^0(M, \Omega)$  is  $\mathbb{T}$ -isomorphic to  $S_2(\Gamma_0(N), \mathbb{Z})$  as shown by Mazur [Ma1, II, (4.6) and (6.2)].  $\square$

## 2. A formal group law for $(\mathcal{G}^{\text{new}})^\wedge$

Under the canonical identification:

$$S_2(\Gamma_0(N)) \simeq H^0(X_0(N)_\mathbb{C}, \Omega^1),$$

given by  $f(z) \rightarrow f(z)dz$ , the homomorphisms (1.1) can be interpreted by means of

the action of certain double classes. Following the terminology of [Sh] we have:

(2.1) PROPOSITION. Let  $A_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$  and  $A'_d = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ . The homomorphisms  $(B_d)^*$ ,  $(B_d)_*$  act on modular forms as:

$$(B_d)^* = [\Gamma_0(D)A_d\Gamma_0(N)]_2, \quad (B_d)_* = [\Gamma_0(N)A'_d\Gamma_0(D)]_2.$$

In particular, they are adjoint with respect to Petersson scalar product.

*Proof.*  $B_d$  induces the morphism:

$$\mathbb{H}^*/\Gamma_0(N) \simeq X_0(N)(\mathbb{C}) \rightarrow \mathbb{H}^*/\Gamma_0(D) \simeq X_0(D)(\mathbb{C}),$$

given by,  $[z] \rightarrow [dz]$ . Hence,  $(B_d)^*(f(z)) = df(dz)$ . On the other hand,  $\Gamma_0(D)A_d\Gamma_0(N) = \Gamma_0(D)A_d$ , since  $\Gamma_0(N) \subseteq A_d^{-1}\Gamma_0(D)A_d$ ; hence:

$$f|_2[\Gamma_0(D)A_d\Gamma_0(N)]_2 = f|_2A_d = df(dz).$$

The double class  $\Gamma_0(N)A'_d\Gamma_0(D)$  determines the transpose correspondence of that determined by  $\Gamma_0(D)A_d\Gamma_0(N)$  [Sh, 7.2]. Hence, it determines the homomorphism  $(B_d)_*: J_0(N)_{\mathbb{C}} \rightarrow J_0(D)_{\mathbb{C}}$ . The last assertion is consequence of [Sh, 3.4.5].  $\square$

(2.2) REMARK. The operator  $B_d$  introduced by Atkin–Lehner [At-Le] corresponds in our notation to  $\frac{1}{d}(B_d)^*$ .

The old part  $S_2(\Gamma_0(N))^{\text{old}}$  of  $S_2(\Gamma_0(N))$  is, by definition, the subspace generated by all images of  $(B_d)^*$  for all possible choices of  $d, D$  satisfying  $dD \mid N, D < N$ . The new part  $S_2(\Gamma_0(N))^{\text{new}}$  is defined to be the orthogonal complement of  $S_2(\Gamma_0(N))^{\text{old}}$  with respect to the Petersson scalar product. By (2.1) we have also:

$$S_2(\Gamma_0(N))^{\text{new}} = \bigcap_{dD \mid N, D < N} \text{Ker}(B_d)_*.$$

Since  $(B_d)_*$  and  $(B_d)^*$  leave  $S_2(\Gamma_0(N), \mathbb{Z})$  invariant, we may define:

$$S^{\text{new}} := S_2(\Gamma_0(N))^{\text{new}} \cap S_2(\Gamma_0(N), \mathbb{Z}) = \bigcap_{dD \mid N, D < N} \text{Ker}((B_d)_*|_{S_2(\Gamma_0(N), \mathbb{Z})}).$$

We do not know a priori that  $S^{\text{new}}$  is a lattice in  $S_2(\Gamma_0(N))^{\text{new}}$ . Nevertheless, this will be clear from the proof of Theorem (2.3) below.

Finally, we define  $J_0(N)^{\text{new}}$  as the quotient of  $J_0(N)$  by the abelian subvariety generated by the images of all  $(B_d)^*$  for all possible choices of  $d, D$  satisfying  $dD \mid N$  and  $D < N$ . Let  $g$  be the dimension of  $J_0(N)^{\text{new}}$  and let  $\mathcal{J}^{\text{new}}$  be its Néron model.

(2.3) THEOREM. For the primes  $p$  dividing  $N$  and the primes  $l$  not dividing  $N$ , let  $U_p, T_l \in M_g(\mathbb{Z})$  be the matrices of the Atkin–Lehner operators and the Hecke operators, with respect to any basis of  $S^{\text{new}}$ . Since these matrices commute, the formal Dirichlet series:

$$\sum_{n=1}^{\infty} A_n \cdot n^{-s} = \prod_p (I_g - U_p \cdot p^{-s})^{-1} \cdot \prod_l (I_g - T_l \cdot p^{-s} + I_g \cdot p^{1-2s})^{-1},$$

is well-defined and  $A_n \in M_g(\mathbb{Z})$  for all  $n$ . Let  $L(X, Y)$  be the  $g$ -dimensional formal group law with logarithm:

$$F(X) = \sum_{n=1}^{\infty} \frac{1}{n} A_n X^n \in \mathbb{Q}[[X_1, \dots, X_g]]^g,$$

where  $X^n$  is the notation for  $(X_1^n, \dots, X_g^n)^t$ . Then,  $L(X, Y)$  is defined over  $\mathbb{Z}$  and it is isomorphic to the formal completion of  $\mathcal{J}^{\text{new}}$  along the zero section.

*Proof.* After [De-Na] it is sufficient to show that  $\text{Lie}(\mathcal{J}^{\text{new}})$  and  $S^{\text{new}}$  are isomorphic as  $\mathbb{T}$ -modules. If  $N$  is a prime,  $S^{\text{new}} = S_2(\Gamma_0(N), \mathbb{Z})$ ,  $\mathcal{J}^{\text{new}} = \mathcal{J}$  and this is given by (1.3) (cf. [Na]). In general, under the  $\mathbb{T}$ -isomorphisms of (1.3),  $S^{\text{new}}$  corresponds to the sub- $\mathbb{T}$ -module:

$$S^{\text{new}} \simeq \bigcap_{d|N, d < N} \text{Ker}(B_d)_*$$

of  $\text{Lie}(\mathcal{J})$ . To check that  $\text{Lie}(\mathcal{J}^{\text{new}})$  is isomorphic to this submodule is equivalent to check the dual assertion:

$$T_0(\mathcal{J}^{\text{new}}) \simeq T_0(\mathcal{J}) / \langle \text{Im}(B_d)_* \rangle.$$

Now, the epimorphism  $J_0(N) \rightarrow J_0(N)^{\text{new}}$  induces an homomorphism  $T_0(\mathcal{J}) \rightarrow T_0(\mathcal{J}^{\text{new}})$ , obviously compatible with  $\mathbb{T}$  and which clearly factorizes through:

$$T_0(\mathcal{J}) / \langle \text{Im}(B_d)_* \rangle \rightarrow T_0(\mathcal{J}^{\text{new}}).$$

Since  $\mathcal{J}$  has semistable reduction and  $N$  is odd, we can apply a result of Mazur [Ma2, Corollary 1.1] to deduce that this is an isomorphism.  $\square$

(2.4) REMARKS. This is an effective computation of  $(\mathcal{J}^{\text{new}})^\wedge$  since, with the aid of a computer, it is always possible to find an explicit  $\mathbb{Z}$ -basis of  $S^{\text{new}}$  and to compute the action of the Hecke algebra.

If one defines  $J_0(N)^{\text{new}}$  to be the abelian subvariety of  $J_0(N)$  generated by all

$\text{Im}(B_d)^*$ , then one obtains an analogous result substituting  $S^{\text{new}}$  by  $S_2(\Gamma_0(N), \mathbb{Z})/\langle \text{Im}((B_d)^*_{S_2(\Gamma_0(D), \mathbb{Z})}) \rangle$ .

### 3. A formal version of the Shimura–Taniyama–Weil conjecture

The work of Cartier [Ca] and Honda [Ho] was motivated by congruence properties of modular forms and by the Shimura–Taniyama–Weil conjecture. If the coefficients of the L-series of an elliptic curve have to be the Fourier coefficients of a cusp form of weight two, they should satisfy the same type of congruences; and in fact they do: the Atkin–Swinnerton–Dyer congruences [Ha, §33].

As an application of (2.3) and the theorem of Cartier–Honda we prove now that the existence of a relation, at a formal level, between  $J_0(N)$  and an elliptic curve over  $\mathbb{Q}$  with conductor  $N$ , is already sufficient to imply the existence of a morphism between the varieties.

(3.1) THEOREM. *Let  $E_{|\mathbb{Q}}$  be an elliptic curve with odd, square-free conductor  $N$ . Let  $\mathcal{E}_{|\mathbb{Z}}$  be the Néron model of  $E$ . The following conditions are equivalent:*

- (1) *There exists a non-zero homomorphism,  $(\mathcal{J}^{\text{new}})^\wedge \rightarrow \mathcal{E}^\wedge$ , of formal groups over  $\mathbb{Z}$ .*
- (2) *There exists a normalized new form,  $f \in S_2(\Gamma_0(N))$ , such that  $L(f, s) = L(E, s)$ .*
- (3) *There exists a non-zero homomorphism,  $J_0(N)^{\text{new}} \rightarrow E$ , defined over  $\mathbb{Q}$ .*

*Proof.* It is well-known that (2) and (3) are equivalent, and (3)  $\Rightarrow$  (1) is clear. Let us see that (1)  $\Rightarrow$  (2).

The theorem of Cartier–Honda asserts that if  $a_n, n \geq 1$ , are the coefficients of the Dirichlet series  $L(E, s)$ , then, the formal series:

$$G(X) = \sum_{n=1}^{\infty} \frac{1}{n} a_n X^n \in \mathbb{Q}[[X]],$$

is the logarithm of a formal group law for  $\mathcal{E}^\wedge$ . Let:

$$F(X) = \sum_{n=1}^{\infty} \frac{1}{n} A_n X^n \in \mathbb{Q}[[X_1, \dots, X_g]]^g,$$

be the logarithm, defined in (2.3), of the formal group law isomorphic to  $(\mathcal{J}^{\text{new}})^\wedge$ .

For the standard facts on formal groups which follow we refer to [Ha]. (1) is equivalent to the existence of a matrix  $M \in M_{1 \times g}(\mathbb{Z})$  such that  $G^{-1}(MF(X))$  has integral coefficients. Or, equivalently to:

- (1')  $G^{-1}(MF(X))$  has coefficients in  $\mathbb{Z}_q$  for all primes  $q$ .

Our formal groups satisfy what Hazewinkel calls “functional equations” over  $\mathbb{Z}_q$  for all  $q$ . In our case, these functional equations are of the following type: for each prime  $q$  there exists:

$$R_q = 1 + b_1 t + \cdots \in M_g(\mathbb{Q}_q)[[t]],$$

$$S_q = 1 + c_1 t + \cdots \in \mathbb{Q}_q[[t]],$$

with  $qb_i, qc_i$  integral for all  $i$ , such that (if  $b_0 = I_g, c_0 = 1$ ):

$$R_q * F(X) := \sum_{i=0}^{\infty} b_i F(X^{q^i}), \quad S_q * G(X) := \sum_{i=0}^{\infty} c_i G(X^{q^i}),$$

have integral coefficients. By the respective Euler-product expansion of  $\Sigma A_n n^{-s}$  and  $\Sigma a_n n^{-s}$ , we know more precisely that possible choices for  $R_q, S_q$  are:

$$R_q = \begin{cases} I_g - \frac{1}{p} U_p t, & \text{if } q=p \text{ divides } N, \\ I_g - \frac{1}{l} T_l t + \frac{1}{l} I_g t^2, & \text{if } q=l \text{ does not divide } N, \end{cases}$$

$$S_q = \begin{cases} 1 - \frac{1}{p} \varepsilon_p t, & \text{if } q=p \text{ divides } N, \\ 1 - \frac{1}{l} a_l t + \frac{1}{l} t^2, & \text{if } q=l \text{ does not divide } N, \end{cases}$$

where  $\varepsilon_p = \pm 1$ . By the functional equation lemma of Honda–Hazewinkel we have that (1') is equivalent to:

$$(1'') \quad S_q M R_q^{-1} \in M_{1 \times g}(\mathbb{Z}_q)[[t]], \quad \text{for all } q.$$

(In fact, let  $i(X) = X, F_R(X) = R_q^{-1} * i(X), G_S(X) = S_q^{-1} * i(X)$ . By the functional equation lemma,  $F$  and  $F_R$  (resp.  $G$  and  $G_S$ ) are the logarithms of strongly isomorphic formal groups. Now,  $G_S^{-1}(M F_R(X))$  has integral coefficients iff  $M F_R(X)$  satisfies the functional equation  $S_q$  iff  $S_q * M F_R(X) = S_q M R_q^{-1} * i(X)$  has integral coefficients.)

For the primes  $p$  dividing  $N$ , (1'') asserts the existence of matrices  $N_i \in M_{1 \times g}(\mathbb{Z}_p)$  such that:

$$(p - \varepsilon_p t) M = \left( \sum_{i=0}^{\infty} N_i t^i \right) (p I_g - U_p t).$$

It is easily checked that this is equivalent to:

$$N_0 = M, \quad N_1 = \frac{1}{p}(MU_p - \varepsilon_p M), \quad N_i = \frac{1}{p}N_{i-1}U_p, \quad i \geq 2.$$

Thus, the existence of the matrices  $N_i$  amounts to:

$$MU_p^i \equiv \varepsilon_p MU_p^{i-1} \pmod{p^i}, \quad \forall i \geq 1.$$

Since  $U_p$  is invertible (by the work of Atkin–Lehner,  $U_p$  is diagonalizable with eigenvalues all equal to  $\pm 1$ ), this implies:

$$MU_p = \varepsilon_p M. \tag{3.2}$$

For the primes  $l$  not dividing  $N$  ( $l''$ ) is equivalent to the existence of matrices  $N_i \in M_{1 \times g}(\mathbb{Z}_l)$  such that:

$$(l - a_l t + t^2)M = \left( \sum_{i=0}^{\infty} N_i t^i \right) (II_g - T_l t + I_g t^2),$$

which, denoting  $T = T_l$ ,  $a = a_l$ , is equivalent to:

$$\begin{cases} N_0 = M \\ N_1 = \frac{1}{l}(MT - aM) \\ N_2 = \frac{1}{l^2}(MT - aM)T \\ N_i - N_{i+1}T + lN_{i+2} = 0, \quad i \geq 1 \end{cases} \tag{3.3}$$

Let  $\mathcal{O}$  be the ring of integers of a finite extension of  $\mathbb{Q}_l$ , containing an eigenvalue  $\alpha$  of  $T$ , and let  $V \in M_{g \times 1}(\mathcal{O})$  be a column vector such that  $TV = \alpha V$ . Denote  $P = MT - aM$  and multiply (3.3) to the right by  $V$ :

$$\begin{cases} N_1 V = \frac{1}{l} P V \\ N_2 V = \frac{1}{l^2} \alpha P V \\ N_i V - \alpha N_{i+1} V + l N_{i+2} V = 0, \quad i \geq 1. \end{cases} \tag{3.4}$$

Let  $l$  be the prime of  $\mathcal{O}$  dividing  $l$ . From (3.4) we deduce:

$$l \mid \alpha \Rightarrow l \mid N_i V \ \forall i \geq 1 \Rightarrow l^r \mid N_i V \ \forall i \geq 1, \ \forall r \geq 1 \Rightarrow N_i V = 0 \ \forall i \geq 1$$

$$l \nmid \alpha, \ l^r \mid N_i V \ \forall i \geq 1 \Rightarrow l^{r+1} \mid N_i V \ \forall i \geq 1.$$

By recurrence (starting with  $r = 0$ ), we see that  $N_i V = 0$  for all  $i \geq 1$ , as in the former case. Since  $T$  is diagonalizable, we may vary  $V$  among a system of independent columns. We get  $N_i = 0$  for all  $i \geq 1$ . In particular we have proved:

$$MT_l = a_l M. \tag{3.5}$$

Thus, by transposing the matrices in (3.2) and (3.5) we have seen that condition (1) of the theorem is equivalent to the existence of a matrix  $L = M^t \in M_{g \times 1}(\mathbb{Z})$  such that:

$$T_l^t L = a_l L, \quad U_p^t L = \varepsilon_p L,$$

simultaneously for all primes  $p, l$ . Let  $f_1, \dots, f_g$  be the previously chosen basis of  $S^{\text{new}}$  and let  $B \in M_g(\mathbb{C})$  be the matrix of the Petersson scalar product with respect to this basis. Since  $T_l$  and  $U_p$  are hermitian and have integral coefficients, they satisfy:  $T_l = B^{-1} T_l^t B$ ,  $U_p = B^{-1} U_p^t B$ . Thus,

$$f := (f_1 \cdots f_g) B^{-1} L \in S_2(\Gamma_0(N))^{\text{new}},$$

is an eigenvector of the Hecke algebra with eigenvalues  $a_l$  and  $\varepsilon_p$  respectively. If  $f$  is assumed to be normalized, this is equivalent to [Sh, 3.43]:

$$L(f, s) = \prod_p (1 - \varepsilon_p p^{-s})^{-1} \prod_l (1 - a_l p^{-s} + p^{1-2s})^{-1},$$

which is equal to  $L(E, s)$ . □

**References**

[At-Le] A. O. L. Atkin-J. Lehner: Hecke operators on  $\Gamma_0(m)$ , *Math. Ann.* 185 (1970), 134–160.  
 [Ca] P. Cartier: *Groupes formels, fonctions automorphes et fonctions zêta des courbes elliptiques*, Actes du Congrès Int. Math. Nice 1970, Tome 2:290-299, Paris, Gauthiers-Villars, 1971.  
 [De-Na] C. Deninger-E. Nart: Formal groups and L-series, *Comment. Math. Helv.* 65 (1990), 318–333.  
 [Gr] A. Grothendieck: Étude globale élémentaire de quelques classes de morphismes (EGA II), *Publ. Math. IHES* 8 (1961).  
 [Ha] M. Hazewinkel: *Formal groups and applications*, New York, Academic Press, 1978.  
 [Ho] T. Honda: Formal groups and zeta functions, *Osaka J. Math.* 5 (1968), 199–213.

- [Ka-Ma] N. M. Katz-B. Mazur: *Arithmetic moduli of elliptic curves*, Annals of Math. Studies n. 108, Princeton Univ. Press, Princeton, New Jersey, 1985.
- [Ma1] B. Mazur: Modular curves and the Eisenstein ideal, *Publ. Math. IHES* 47 (1977), 33–186.
- [Ma2] B. Mazur: Rational isogenies of prime degree, *Inv. Math.* 44 (1978), 129–162.
- [Na] E. Nart: The formal completion of the Néron model of  $J_0(p)$ , *Publ. Mat.* 35 (1991), 537–542.
- [Ra] M. Raynaud: Spécialisation du foncteur de Picard, *Publ. Math. IHES* 38 (1970), 27–76.
- [Se] J. P. Serre: *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.
- [Sh] G. Shimura: *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, New Jersey, 1971.