COMPOSITIO MATHEMATICA

P. BAYER
J. C. LARIO

On Galois representations defined by torsion points of modular elliptic curves

Compositio Mathematica, tome 84, n° 1 (1992), p. 71-84
<http://www.numdam.org/item?id=CM_1992__84_1_71_0>

Compositio Mathematica **84**: 71–84, 1992.

On Galois representations defined by torsion points of modular elliptic curves

P. BAYER[1] and J. C. LARIO[2]

[1]*Universitat de Barcelona, Dept. d'Àlgebra i Geometria, Gran Via de les Corts Catalanes, 585, 08007 Barcelona;* [2]*Universitat Politècnica de Catalunya, Dept. de Matemàtica Aplicada II, Pau Gargallo, 5, 08025 Barcelona*

Received 7 May 1991; accepted 17 July 1991

Abstract. We verify Serre's conjecture (3.2.4$_?$), stated in [Se4], for the special case of irreducible Galois representations defined by the p-torsion points of modular elliptic curves with potentially good, ordinary reduction at p. Also we treat the semi-stable case when the representation is not finite at p.

Introduction

For a prime integer p, fix $\bar{\mathbb{F}}_p$ a closure of $\mathbb{F}_p$. Fix $\bar{\mathbb{Q}}$ a closure of $\mathbb{Q}$ and put $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For every continuous Galois representation $\rho: G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$, Serre defines two integers: the conductor N_ρ and the weight k_ρ, as well as a Dirichlet character $\varepsilon_\rho: (\mathbb{Z}/N_\rho\mathbb{Z})^* \to \bar{\mathbb{F}}_p^*$ by means of a recipe. When ρ is odd and irreducible, he conjectures that ρ arises from a cusp form of type $(N_\rho, k_\rho, \varepsilon_\rho)$ with coefficients in $\bar{\mathbb{F}}_p$ which is an eigenfunction of all the Hecke operators (cf. [Se4], (3.2.4$_?$)).

Suppose that E is an elliptic curve over $\mathbb{Q}$. For each prime p, the action of the absolute Galois group $G_{\mathbb{Q}}$ on the p-torsion points E_p of $E(\bar{\mathbb{Q}})$ defines a continuous representation

$$\rho: G_{\mathbb{Q}} \to \mathrm{Aut}(E_p) \simeq \mathrm{GL}_2(\mathbb{F}_p), \tag{1}$$

which is always odd and absolutely irreducible if $p > 163$ (cf. [Ma], [Se4]).

In this case, the character ε_ρ is trivial. Depending on the arithmetic of E, we compute the conductor and the weight of ρ in Section 1. If the representation ρ is finite at p, $p \geqslant 5$, and the elliptic curve is modular and has semi-stable reduction at p, we know that ρ verifies (3.2.4$_?$) (cf. [Ri], [Ca]). In Sections 2 and 3 we show that ρ verifies (3.2.4$_?$) when E is modular and has potentially good ordinary or semi-stable (non-finite) reduction at p. In these cases the weight k_ρ is greater than 2 and the cusp form f predicted by Serre's conjecture can be obtained by a manipulation of the weight-2 newform F attached to E by Eichler–Shimura theory.

Partially supported by DGICYT, PB89-0215-C02-01 and UPC, PRE89.

Section 1 reproduces the text of a talk given by the second author in the Frey–Lamprecht–Zimmer Seminar of the Universität des Saarlandes, in September '89. The results in this section are in accordance with the ones given in [Kr].

1. Conductor and weight formulae

The action of $G_{\mathbb{Q}}$ on the Tate module $T_p(E)$ of E gives rise to a p-adic representation $\rho_0: G_{\mathbb{Q}} \to \mathrm{Aut}(T_p(E) \otimes \mathbb{Q}_p) \simeq \mathrm{GL}_2(\mathbb{Q}_p)$ which is a lifting of the representation ρ. Let N be the conductor of ρ_0; i.e., N is the product of the local Artin conductors of ρ_0 at the primes $l \neq p$ (cf. [Se1]). We know that the conductor N_ρ of ρ must be a divisor of N. Since the wild ramification groups at l are pro-l-groups and $l \neq p$, the wild exponents of N and N_ρ coincide. We have

$$v_l(N/N_\rho) = \mathrm{codim}_{\mathbb{Q}_p}(T_p(E) \otimes \mathbb{Q}_p)^{I_l} - \mathrm{codim}_{\mathbb{F}_p} E_p^{I_l},$$

for every prime $l \neq p$. Here, I_l denotes some inertia group of $G_{\mathbb{Q}}$ for l.

Let now $\mathscr{E}_{\mathbb{F}_l}$ denote the special fibre of the Néron model of E at l and consider the exact sequence

$$0 \to \mathscr{E}^0_{\mathbb{F}_l} \to \mathscr{E}_{\mathbb{F}_l} \to \Phi_l \to 0,$$

where $\mathscr{E}^0_{\mathbb{F}_l}$, Φ_l are the identity component and the group of components of $\mathscr{E}_{\mathbb{F}_l}$, respectively. We recall that

$$\mathscr{E}^0_{\mathbb{F}_l} \simeq \begin{cases} \mathscr{E}_{\mathbb{F}_l} & \text{if } E \text{ has good reduction at } l, \\ \mathbb{G}_{m,\bar{\mathbb{F}}_l} \text{ (over } \bar{\mathbb{F}}_l) & \text{if } E \text{ has multiplicative reduction at } l, \\ \mathbb{G}_{a,\mathbb{F}_l} & \text{if } E \text{ has additive reduction at } l. \end{cases}$$

To compute $\mathrm{codim}_{\mathbb{F}_p} E_p^{I_l}$, we use the isomorphism $E(\bar{\mathbb{Q}}_l)[p]^{I_l} \simeq \mathscr{E}_{\mathbb{F}_l}(\bar{\mathbb{F}}_l)[p]$ obtained by reduction (cf. [Se-Ta]); one easily checks that

$$\dim \mathscr{E}_{\mathbb{F}_l}(\bar{\mathbb{F}}_l)[p] = \begin{cases} 2 & \text{if } E \text{ has good reduction at } l, \\ 1 + \dim \Phi_l(\bar{\mathbb{F}}_l)[p] & \text{if } E \text{ has multiplicative reduction at } l, \\ \dim \Phi_l(\bar{\mathbb{F}}_l)[p] & \text{if } E \text{ has additive reduction at } l. \end{cases}$$

On the other hand,

$$\dim(T_p(E) \otimes \mathbb{Q}_p)^{I_l} = \begin{cases} 2 & \text{if } E \text{ has good reduction at } l, \\ 1 & \text{if } E \text{ has multiplicative reduction at } l, \\ 0 & \text{if } E \text{ has additive reduction at } l. \end{cases}$$

From what precedes it is clear that

$$v_l(N) - v_l(N_\rho) = p\text{-rank } \Phi_l,$$

for every prime $l \neq p$.

The following tables yield the exact value of the 'abaissement' $v_l(N/N_\rho)$ in terms of the reduction type of the Néron model at l.

For $p=2$,

$v_l(N/N_\rho)$	Kodaira symbol of $\mathscr{E}_{\bar{\mathbb{F}}_l}$
2	I_{2v}^*
1	I_{2v}, I_{2v+1}^*, *III*, *III**
0	I_0, I_{2v+1}, *II*, *II**, *IV*, *IV**

For $p = 3$,

$v_l(N/N_\rho)$	Kodaira symbol of $\mathscr{E}_{\bar{\mathbb{F}}_l}$
1	I_v if $3 \mid v$, *IV*, *IV**
0	otherwise

For $p \geqslant 5$,

$v_l(N/N_\rho)$	Kodaira symbol of $\mathscr{E}_{\bar{\mathbb{F}}_l}$
1	I_v if $p \mid v$
0	otherwise

The recipe to compute the weight k_ρ is more subtle; it only involves the local representation at p. Let $\rho_p: G_p \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ be the representation obtained from ρ by restriction to some decomposition group $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ of $G_{\mathbb{Q}}$ for p. Let ρ_p^{ss} denote its semisimplification. The action under ρ_p^{ss} of the tame inertia group I_t of G_p is given by two characters ϕ, ϕ' of level 1 or 2; by writing them in a suitable way as powers of the fundamental characters one gets the value of k_ρ (cf. [Se4]). Recall that each character of I_t is determined by its invariant α mod $\mathbb{Z}[1/p]$, where α is a rational number (cf. [Se2]).

Assume for simplicity that $p > 7$ (cf. [Kr] for the cases $p \leqslant 7$). Let c_4, c_6 be the usual invariants of the elliptic curve E, determined up to p-units from a p-minimal Weierstrass equation for E.

PROPOSITION. *The weight* $k_\rho = 2 + \lambda(p-1)$ *and the invariants* $\alpha(\phi)$, $\alpha(\phi') = p/(p-1) - \alpha(\phi)$ *of the characters attached to the representation*

$$\rho: G_{\mathbb{Q}} \to \mathrm{Aut}(E_p)$$

can be read from the following table:

$\mathscr{E}_{\bar{\mathbb{F}}_p}$	Further conditions	$\alpha(\phi)$	λ
I_v	if $p \mid v$	$1/(p-1)$	0
	if $p \nmid v$	$1/(p-1)$	1
II	$p \equiv 1(3)$	$(5p+1)/6(p-1)$	$(p+5)/6$
	$p \equiv 2(3)$, $v_p(c_4) = 1$	$(5p-1)/6(p-1)$	$(p+7)/6$
	$p \equiv 2(3)$, $v_p(c_4) > 1$	$(5p^2+1)/6(p^2-1)$	$(p+7)/6$
III	$p \equiv 1(4)$	$(3p+1)/4(p-1)$	$(p+3)/4$
	$p \equiv 3(4)$, $v_p(c_6) = 2$	$(3p-1)/4(p-1)$	$(p+5)/4$
	$p \equiv 3(4)$, $v_p(c_6) > 2$	$(3p^2+1)/4(p^2-1)$	$(p+5)/4$
IV	$p \equiv 1(3)$	$(2p+1)/3(p-1)$	$(p+2)/3$
	$p \equiv 2(3)$, $v_p(c_4) = 2$	$(2p-1)/3(p-1)$	$(p+4)/3$
	$p \equiv 2(3)$, $v_p(c_4) > 2$	$(2p^2+1)/3(p^2-1)$	$(p+4)/3$
I_v^*	if $p \mid v$	$(p+1)/2(p-1)$	$(p+1)/2$
	if $p \nmid v$	$(p+1)/2(p-1)$	$(p+3)/2$
*II**	$p \equiv 1(3)$	$(p+5)/6(p-1)$	$(p+11)/6$
	$p \equiv 2(3)$, $v_p(c_4) = 4$	$(p+1)/6(p-1)$	$(p+7)/6$
	$p \equiv 2(3)$, $v_p(c_4) > 4$	$(p^2+5)/6(p^2-1)$	$(p+1)/6$
*III**	$p \equiv 1(4)$	$(p+3)/4(p-1)$	$(p+7)/4$
	$p \equiv 3(4)$, $v_p(c_6) = 5$	$(p+1)/4(p-1)$	$(p+5)/4$
	$p \equiv 3(4)$, $v_p(c_6) > 5$	$(p^2+3)/4(p^2-1)$	$(p+1)/4$
*IV**	$p \equiv 1(3)$	$(p+2)/3(p-1)$	$(p+5)/3$
	$p \equiv 2(3)$, $v_p(c_4) = 3$	$(p+1)/3(p-1)$	$(p+4)/3$
	$p \equiv 2(3)$, $v_p(c_4) > 3$	$(p^2+2)/3(p^2-1)$	$(p+1)/3$

Proof. The results in the second table can be obtained from the results in the first table by twisting with the quadratic character ramified only at p. If E has semi-stable reduction at p, the values of $\alpha(\phi)$ and λ are already given in [Se4]. Therefore, we only need to consider the cases when E has reduction type *II*, *III*, or *IV* at p.

Let

$$e = \begin{cases} 6 & \text{if } E \text{ is of type } II \text{ at } p, \\ 4 & \text{if } E \text{ is of type } III \text{ at } p, \\ 3 & \text{if } E \text{ is of type } IV \text{ at } p. \end{cases}$$

The elliptic curve E acquires good reduction over the field $L = \mathbb{Q}_p^{\mathrm{nr}}(\pi)$, where $\pi^e = p$. Let $E_L = E \otimes_{\mathbb{Q}_p^{\mathrm{nr}}} L$ and let $m: E_L(\bar{\mathbb{Q}}_p) \to E(\bar{\mathbb{Q}}_p)$ be the $\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$-

isomorphism obtained by base change. We search for some 1-dimensional subspace V of the $\bar{\mathbb{F}}_p[I_t]$-module $(\bar{\mathbb{F}}_p \otimes_{\mathbb{F}_p} E_p)^{ss}$.

We first recall the basic setup of [Se2]. Let $\hat{E}$ be the formal group of E_L and let h be its height. The kernel $\hat{E}_p$ of the multiplication by $[p]$ contains always a non-zero $\mathbb{F}_p$-vector space V_L on which the tame inertia group $I_{t,L}$ of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$ acts. The $\dim_{\mathbb{F}_p} V_L$ and the action of $I_{t,L}$ on $\mathbb{F}_{p^h} \otimes V_L$ can both be read from the Newton polygon of the formal series of the multiplication by $[p]$ on $\hat{E}$. A case-by-case verification shows:

h	Further conditions	$\dim_{\mathbb{F}_p} V_L$	$I_{t,L}$ on $\bar{\mathbb{F}}_p \otimes V_L$
1	*II*, $p \equiv 1(3)$	1	θ_{p-1}^e
	III, $p \equiv 1(4)$		
	IV, $p \equiv 1(3)$		
2	*II*, $p \equiv 2(3)$, $v_p(c_4)=1$	1	θ_{p-1}^4
	III, $p \equiv 3(4)$, $v_p(c_6)=2$		θ_{p-1}^2
	IV, $p \equiv 2(3)$, $v_p(c_4)=2$		θ_{p-1}
2	*II*, $p \equiv 2(3)$, $v_p(c_4) > 1$	2	$\theta_{p^2-1}^e$, $\theta_{p^2-1}^{pe}$
	III, $p \equiv 3(4)$, $v_p(c_6) > 2$		
	IV, $p \equiv 2(3)$, $v_p(c_4) > 2$		

where $\theta_{p-1}, \theta_{p^2-1}: I_{t,L} \to \bar{\mathbb{F}}_p^*$ are fundamental characters on $I_{t,L}$ of level one and two, respectively.

Let us take $V := \mathbb{F}_{p^h} \otimes m(V_{E_L})$, where V_{E_L} is the image of V_L under the embedding of $\hat{E}_p$ into the group $E_{L,p}$ of p-torsion points of $E_L(\bar{\mathbb{Q}}_p)$. Now I_t acts on V and its action can be computed by means of m. For that, we look at the action of $s_m := m^{-1} \circ s \circ m$ on $\mathbb{F}_{p^h} \otimes V_L$, for $s \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})$. We carry out the whole computations only when E has reduction type *IV* at p, $p \equiv 2 \pmod 3$, and $v_p(c_4) > 2$:

$$E: Y^2 = X^3 - p^2AX + p^2B \quad \text{with } A, B \in \mathbb{Z}, \quad (p, B) = 1,$$

$$E_L: Y^2 = X^3 - \pi^2 AX + B, \quad \text{height}(\hat{E}) = 2, \quad \dim_{\mathbb{F}_p} V_L = 2,$$

$$m^{-1}: E(\bar{\mathbb{Q}}_p) \to E_L(\bar{\mathbb{Q}}_p), \quad m^{-1}(x, y) = \left(\frac{x}{\pi^2}, \frac{y}{\pi^3}\right),$$

and

$$V_L = \left\{ z = -\pi x/y \,\middle|\, \left(\frac{x}{\pi^2}, \frac{y}{\pi^3}\right) \in E_{L,p},\ v_\pi(-\pi x/y) = \frac{3}{p^2-1} \right\}$$

$$= \left\{ z = -\pi x/y \,\middle|\, \left(\frac{x}{\pi^2}, \frac{y}{\pi^3}\right) \in E_{L,p},\ v_p(-x/y) = \frac{-p^2+4}{3(p^2-1)} \right\},$$

$$V = \mathbb{F}_{p^2} \otimes \left\{ (x, y) \in E_p \,\middle|\, \frac{-\pi x}{y} \in V_L \right\}.$$

If $s \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}})$ and $z = -\pi x/y \in V_L$, then

$$s\left(\frac{x}{y}\right) = \theta_{p^2-1}^{(-p^2+4)/3}(s)\frac{x}{y} = \theta_{p^2-1}^{(2p^2+1)/3}(s)\frac{x}{y}.$$

Finally, for $1 \otimes (x, y) \in V$ we get

$$\begin{aligned} s(1 \otimes (x, y)) &= 1 \otimes (m \circ s_m \circ m^{-1})(x, y) \\ &= 1 \otimes (m \circ s_m)(x/\pi^2, y/\pi^3) \\ &= 1 \otimes m(sx/\pi^2, sy/\pi^3) \\ &= \theta_{p^2-1}^{(2p^2+1)/3}(s) \otimes m(x/\pi^2, y/\pi^3) \\ &= \theta_{p^2-1}^{(2p^2+1)/3}(s)(1 \otimes m(x/\pi^2, y/\pi^3)) \\ &= \theta_{p^2-1}^{(2p^2+1)/3}(s)(1 \otimes (x, y)). \end{aligned}$$

Now, case-by-case, we fill up the table by taking into account the recipe for the weight.

2. Serre's conjecture in the ordinary case

Our goal is to prove the following

THEOREM. *Serre's conjecture* (3.2.4$_?$) *is true for an irreducible representation*

$$\rho: G_{\mathbb{Q}} \to \mathrm{Aut}(E_p)$$

provided that E over $\mathbb{Q}$ *is a modular elliptic curve with potentially good, ordinary reduction at* $p > 7$.

We look for a modular form $f = \Sigma a_n q^n$ of type (N_ρ, k_ρ) with coefficients in $\bar{\mathbb{F}}_p$, eigenfunction of all the Hecke operators, and satisfying

$$\mathrm{trace}(\rho(\mathrm{Frob}_l)) = a_l \quad \text{and} \quad \det(\rho(\mathrm{Frob}_l)) = l^{k_\rho - 1},$$

for all $l \nmid pN_\rho$. We should like to remark that numerical evidence, collected by computer calculations, led us to guess how the normalized newform F attached to our elliptic curve E should be handled to produce f. First of all we fix some terminology:

Set C_n for a cyclic group of order n. Fix a primitive root mod p or, equivalently, fix an isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \simeq C_{p-1}$. Let ζ_p in $\bar{\mathbb{Q}}$ be a primitive pth root of unity. Realize the group C_{p-1} as Galois group as follows:

$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$, by sending a conjugation class Frob_l to l mod p for all $l \neq p$.

Fix embeddings

$$\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_l$$

for each prime l and define a Dirichlet character

$$\psi: (\mathbb{Z}/p\mathbb{Z})^* \to \mu_{p-1}$$

so that under the mapping $\mu_{p-1} \to \mathbb{Q}_p^*$ we have

$$\psi(n)n \equiv 1 \pmod{p}, \quad \text{for all } n \in \mathbb{Z}, \quad (n, p) = 1.$$

We denote by

$$\psi_l: G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mu_{p-1} \to \bar{\mathbb{Q}}_l^*,$$

the Galois l-adic character deduced from ψ. Note that by reduction mod p, ψ_p yields the inverse of the cyclotomic character mod p

$$\chi: G_{\mathbb{Q}} \to \mathbb{F}_p^*,$$

which is given by the action of $G_{\mathbb{Q}}$ on the pth roots of unity.

Finally, for future use we state the following notations:

Type	I_0^*	*II*	*III*	*IV*	*II**	*III**	*IV**
e	2	6	4	3	6	4	3
a	0	1	1	1	1	1	1

From now on we put $m = \dfrac{p-1}{e}$.

LEMMA 1. *Let F be the normalized newform associated to an elliptic curve E satisfying the same hypothesis as in the theorem and let N be as in Section* 1. *Then the level of F is p^2N and there exists a newform*

$$g = \sum b_n q^n \in S_2(p^a N, \psi^{2m}), \qquad q = e^{2\pi i z},$$

having the same eigenvalues system as the twisted form $F \otimes \psi^m$.

Proof. The first claim follows from the assumptions and [Ca]. Observe that $F \otimes \psi^m$ is an eigenfunction for the Hecke operators with eigenvalues system $\{a_l\psi^m(l),\ \psi^{2m}\}_{l\nmid pN}$. Therefore there exists a divisor M of p^2N and a newform $g \in S_2(M, \psi^{2m})$ having the same eigenvalues system as $F \otimes \psi^m$. In fact,

$$F \otimes \psi^m = g - g|U_p|B_p$$

being U_p, resp. B_p, the Atkin, resp. the degeneracy, operators as in [At-Li].

We must prove that $M = N$ if E is of type I_0^* at p, and $M = pN$ otherwise.

Let l be a prime such that $(l, pN) = 1$. Using Eichler–Shimura, if

$$\rho_l\colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_l(E) \otimes \bar{\mathbb{Q}}_l) \simeq \mathrm{GL}_2(\bar{\mathbb{Q}}_l)$$

denotes the l-adic representation attached to E then

$$\rho_l \otimes \psi_l^m\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_l)$$

is the l-adic representation arising from $F \otimes \psi^m$. Notice that $\rho_l \otimes \psi_l^m$ is also the l-adic representation for the newform g.

Since after Carayol's work it is known that the level of a newform agrees (outside l) with the Artin conductor of its l-adic representation, we have reduced the problem to compute the conductor of $\rho_l \otimes \psi_l^m$ attached to g. Moreover, since ψ_l is unramified outside p we only need to compute the action of I_p, the inertia subgroup of Gal $(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Since E has potentially good ordinary reduction at p, E acquires good reduction over the ring of integers of $\mathbb{Q}_p(\pi)$, with $\pi^e = p$ and $p \equiv 1 \pmod{e}$; therefore ρ_l restricted at I_p factorizes through a cyclic group C_e of order e. In particular, this forces the restriction ρ_{l/I_p} to be diagonalizable. Moreover $\det \rho_l(I_p) = 1$ and hence

$$\rho_{l/I_p} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

with a character $\varepsilon\colon C_{p-1} \to \mu_e(\bar{\mathbb{Q}}_l)$. We may view ε as a Galois character unramified outside p, still denoted by ε,

$$\varepsilon\colon G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq C_{p-1} \to C_e \to \mu_e(\bar{\mathbb{Q}}_l).$$

But, ε should be $\psi_l^{\pm m}$. Since, being $\bar{\mathbb{Q}}_l$ fixed, only two characters of $C_{p-1} \to \mu_{p-1}(\bar{\mathbb{Q}}_l)$ of order e exist if $e = 3, 4$ or 6, and only one if $e = 2$. So, now it is

clear that $\rho_l \otimes \psi_l^m$ has Artin conductor with exponent 1 at p if $e=3$, 4, 6 or 0 if $e=2$.

We also need some knowledge on the behavior of the 'hidden' coefficient b_p of the newform g attached to the modular form F. In the next lemma, we reject the easy case when E is of type I_0^* at p.

LEMMA 2. *Let $g=\Sigma b_n q^n$ be the normalized newform of Lemma* 1 *and assume $a=1$. Let K be the number field generated by the Fourier coefficients b_n for all $n \geqslant 1$. Then we have*:

(i) *The field K is equal to*

$$\mathbb{Q}(\psi^m) = \begin{cases} \mathbb{Q}(\sqrt{-3} & \text{if } e = 3, 6, \\ \mathbb{Q}(\mathrm{i}) & \text{if } e=4. \end{cases}$$

(ii) $|b_p| = \sqrt{p}$.

(iii) *If v_p denotes the normalized p-adic valuation of $\bar{\mathbb{Q}}$ fixed by $\bar{\mathbb{Q}}_p$, then*

$$v_p(b_p) \in \{0, 1\}.$$

Proof. It is clear that the coefficients b_l with $l \nmid pN$ belong to the field $\mathbb{Q}(\psi^m)$. Since g is a newform, it then follows from a theorem of Miyake (cf. Theorem B in [Mi]), that all the coefficients of g lie in $\mathbb{Q}(\psi^m)$.

Since g is a normalized newform and it has primitive p-Nebentypus (in the sense that its level and the conductor of its character have the same valuation at p), a result of Ogg–Li–Asai (cf. [Og], [Li], [As]) yields $|b_p| = \sqrt{p}$, and therefore $v_p(b_p) + v_p(\overline{b_p}) = 1$, where the bar denotes complex conjugation. Since b_p is an integer of K and p splits completely in K, we have $v_p(b_p) \in \{0, 1\}$.

The next lemma makes use of the theory of deforming residual Galois representations. Recent work of Mazur and Tilouine suggest how to make explicit links between ordinary deformations and ordinary (potentially) elliptic curves (cf. [Ma-Ti], [Hi]).

We let $\bar{g} = \Sigma \overline{b_n} q^n$ denote the 'complex conjugate' form of g.

LEMMA 3. *Either g or $\bar{g}$ is ordinary at p, depending on the p-Kodaira symbol of E: II, III, IV or II*, III*, IV*.*

Proof. Since E has potentially good ordinary reduction at p, the restriction of ρ to I_p is reducible. It is given by

$$\begin{pmatrix} \chi^{p-m} & * \\ 0 & \chi^m \end{pmatrix} \quad \text{when } E \text{ is of type } II, III \text{ or } IV \text{ at } p,$$

and

$$\begin{pmatrix} \chi^{m+1} & * \\ 0 & \chi^{m(e-1)} \end{pmatrix} \quad \text{when } E \text{ is of type } II^*, III^*, IV^* \text{ at } p.$$

We obtain

Form	Representation	p-type$(E) = II, III, IV$	p-type$(E) = II^*, III^*, IV^*$
g	$\rho \otimes \chi_{\|I_p}^{-m}$	$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} * & * \\ 0 & \chi^{(e-2)m} \end{pmatrix}$
$\bar{g}$	$\rho \otimes \chi_{\|I_p}^{m}$	$\begin{pmatrix} * & * \\ 0 & \chi^{2m} \end{pmatrix}$	$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$

Therefore, by a theorem of Wiles (cf. [Wi]), g cannot be ordinary in the cases when E is of type II^*, III^* or IV^* at p, resp. $\bar{g}$ cannot be ordinary in the cases when E is of type II, III or IV at p. Since we know a priori that one of the two forms is p-ordinary, the claim follows.

REMARK. From now on let $\mathfrak{P}$ be the place of $\bar{\mathbb{Q}}$ fixed by our choice of $\bar{\mathbb{Q}}_p$. Let $\tilde{g}$ denote the p-ordinary cusp form in Lemma 3. In the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\psi^m)$ we write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$. Denote by $A/_{\mathbb{Q}}$ the abelian subvariety of $J_1(pN)$ attached to $\tilde{g}$ by Shimura's theory and consider the $\mathbb{Q}$-rational multiplication

$$\iota\colon \mathcal{O} \to \mathrm{End}(A/_{\mathbb{Q}})$$

under which the action of $\iota(\tilde{b}_n)$ is given by the Hecke operator $T_{n,\mathrm{Alb}}$ acting on A.

By using a theorem of Langlands [La], A acquires good reduction over $\mathbb{Q}_p(\zeta_p)$ (or even more precisely, over the splitting field of the character ψ^{2m}). Denote by B the Néron model of A over $\mathrm{Spec}\,\mathbb{Z}_p[\zeta_p]$. Lemma 3 simply tells us that the p-divisible group $B[\mathfrak{p}^\infty]$ is ordinary at $\mathfrak{p}$; i.e. in the exact sequence of p-divisible groups

$$0 \to B[\mathfrak{p}^\infty]^0 \to B[\mathfrak{p}^\infty] \to B[\mathfrak{p}^\infty]^{\mathrm{et}} \to 0$$

all the terms are non-zero.

The last lemma we need makes use of the Eisenstein series $E_{1,\psi}$. Briefly, we summarize its definition and properties:

$$E_{1,\psi} = 1 + c_\psi \sum_{m,m_1>0} \psi(m) e^{2\pi i m m_1 z},$$

where

$$c_\psi = -\frac{2\pi i C(\bar{\psi})}{pL(1,\bar{\psi})}.$$

Here, $L(s,\psi)$ is the Dirichlet's L-function for the character ψ, and

$$C(\psi) = \sum_{1 \leqslant n \leqslant p-1} \psi(n) e^{2\pi i n/p}$$

is the Gauss sum. The Eisenstein series $E_{1,\psi}$ is a modular form of weight 1 and character ψ on $\Gamma_0(p)$ which satisfies

$$E_{1,\psi} \equiv 1 \pmod{\mathfrak{P}}$$

and

$$E_{1,\psi}\left|\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}_1 = \frac{\sqrt{p}}{C(\bar{\psi})}\frac{C_\psi}{c_{\bar{\psi}}} E_{1,\bar{\psi}} \quad \text{(cf. [Ko])}. \right. \tag{2}$$

Also we are going to recall the trace operator between modular forms. For sake of simplicity we only take care of the case

$$\mathrm{Tr}\colon S_\kappa(pN, \phi) \to S_\kappa(N, \phi), \qquad \mathrm{Tr}(g) = \sum_{j=1}^{p+1} g\,|\,[\sigma_j]_\kappa,$$

where ϕ is a Dirichlet character mod N, and σ_j denotes a set of representatives of the right cosets $\Gamma_0(pN)\backslash\Gamma_0(N)$.

Let $W_p = \begin{pmatrix} px & 1 \\ pNy & p \end{pmatrix}$, with some integers x, y satisfying $\det W_p = p$. It is the well-known Fricke involution. Let U_p be the pth Hecke operator acting on $S_\kappa(pN, \phi)$. In our case, the trace operator has the simple expression

$$\mathrm{Tr}(g) = g + \phi(p)^{-1} p^{1-\kappa/2} g\,|\,[W_p]_\kappa\,|\,U_p.$$

LEMMA 4. *Let $h = \Sigma c_n q^n \in S_\kappa(pN, \psi^{-t})$ be a newform with $1 \leqslant t < p-1$. Let d be a positive integer with $d \equiv t \pmod{p-1}$. Then*

$$\mathrm{Tr}(hE_{1,\psi}^d) \equiv h \pmod{\mathfrak{P}} \Leftrightarrow 2 - \kappa + \frac{d-t}{p-1} + v_p(\bar{c}_p) > 0.$$

Proof. For the proof we borrow some ideas of Koike and Shimura (cf. [Ko]).

We write for a moment

$$\mathrm{Tr}(hE^d_{1,\psi}) = hE^d_{1,\psi} + p^{1-(\kappa+d)/2}(hE^d_{1,\psi})\,|\,[W_p]_{k+d}\,|\,U_p.$$

Since $E_{1,\psi} \equiv 1 \pmod{\mathfrak{P}}$, we look for an integer d such that

$$p^{1-(\kappa+d)/2}(hE^d_{1,\psi})\,|\,[W_p]_{\kappa+d}\,|\,U_p \equiv 0 \pmod{\mathfrak{P}}.$$

Following Asai [As], let us define $c_n^{(p)}$ by

$$\begin{cases} c_n^{(p)} = \bar{\psi}^{-t}(n)c_n & \text{if } (n, p) = 1, \\ c_n^{(p)} = \bar{c}_n & \text{if } (n, N) = 1, \\ c_{nm}^{(p)} = c_n^{(p)}c_m^{(p)} & \text{if } (n, m) = 1, \end{cases}$$

and put

$$h^{(p)} = \sum c_n^{(p)} q^n.$$

Then $h\,|\,[W_p]_\kappa = \delta_p h^{(p)}$ being $\delta_p = C(\psi^{-t})p^{-\kappa/2}\bar{c}_p$ the pseudo-eigenvalue of W_p at h.

By using (2) we rewrite

$$(hE^d_{1,\psi})\,|\,[W_p]_{\kappa+d} = h\,|\,[W_p]_\kappa \cdot (E_{1,\psi}\,|\,[W_p]_1)^d = \delta_p h^{(p)} \cdot \left(\frac{\sqrt{p}}{C(\bar{\psi})}\frac{c_\psi}{c_{\bar{\psi}}}\right)^d E^d_{1,\bar{\psi}}.$$

Finally, by taking into account Stickelberger's theorem we get

$$v_p\left(p^{1-(\kappa+d)/2}\cdot\delta_p\cdot\left(\frac{\sqrt{p}}{C(\bar{\psi})}\frac{c_\psi}{c_{\bar{\psi}}}\right)^d\right) = 2-\kappa+\frac{d-t}{p-1}+v_p(\bar{c}_p),$$

and this proves the lemma.

Proof of the theorem. We give the proof when E is of type *II*, *III*, or *IV* at p. For the other cases, except when E is of type I_0^* which is even easier, we proceed in the same way, and therefore the proof is left to the reader.

By Lemma 1 we take $g = \Sigma b_n q^n \in$ in $S_2(pN, \psi^{2m})$. From Lemmas 2 and 3 we know that in this case g is a p-ordinary newform satisfying $v_p(\overline{b_p}) = 1$. By normalizing the exponent in the character of g, we can take $d = m(e-2)$ in accordance with Lemma 4.

Let λ be as in Section 1. If θ denotes the Ramanujan operator (cf. [Se3]) it is immediate that

$$\theta^m \operatorname{Tr}(gE_{1,\psi}^{m(e-2)}) \in S_{2+\lambda(p-1)}(N)_{/\bar{\mathbb{F}}_p},$$

and its coefficients are congruent to the traces of $\rho(\mathrm{Frob}_l)$ for all $l \nmid pN$. The weight of this form is now the right one and its level is prime to p.

If N is the conductor predicted by (3.2.4?) (cf. table of conductors in Section 1), we can take the form f predicted by Serre's conjecture as $\theta^m \operatorname{Tr}(gE_{1,\psi}^d)$. Otherwise, since N is prime to p, Theorem 1 in [Jo-Li] allows to change the form $\operatorname{Tr}(gE_{1,\psi}^d)$ by a form g' such that $f = \theta^m g'$.

REMARK. Notice that the newform $\bar{g}$ can be used to produce the modular form predicted by the conjecture of Serre for the representation arising from the p-torsion points of E^*, the twisted elliptic curve of E by the quadratic character ramified only at p.

3. Serre's conjecture in the semi-stable non-finite case

Using the same techniques as in the preceeding section we also give the following

THEOREM. *Serre's conjecture* (3.2.4?) *is true for an irreducible representation*

$$\rho: G_{\mathbb{Q}} \to \mathrm{Aut}(E_p)$$

provided that E over $\mathbb{Q}$ is a modular elliptic curve with semi-stable reduction at a prime $p \geqslant 5$.

Proof. When the representation ρ is finite, which is equivalent to say that the weight predicted by Serre's conjecture equals 2, it is a consequence of results given in [Ri] and [Ca].

Thus, we suppose ρ is non-finite; then the weight attached to ρ is $k_\rho = p+1$. Applying the same kind of arguments as in the previous section, now we have that $FE_{1,\psi}^{p-1}$ belongs to $S_{p+1}(pN)$, being $F = \Sigma a_n q^n$ the newform attached to the elliptic curve E. It is easy to check that $g = \operatorname{Tr}(FE_{1,\psi}^{p-1})$ will produce the cusp form predicted by (3.2.4?) because it has the correct weight, p does not divide its level and since $a_p = \pm 1$ it satisfies

$$\operatorname{Tr}(FE_{1,\psi}^{p-1}) \equiv F \pmod{\mathfrak{P}}.$$

Acknowledgement

We would like to express our thanks to J. Quer for many key discussions and, especially, for his valuable help to perform the algorithm quoted in [Se4], 2.9. *Remarque* 2.

References

[As] Asai, T.: On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution, *J. Math. Soc. Japan* 28 (1976), 48–61.

[At-Le] Atkin, A.O.L. and Lehner, J.: Hecke operators on $\Gamma_0(N)$, *Math. Ann.* 185 (1970), 134–160.

[At-Li] Atkin, A.O.L. and Li, W.-C.: Twists of newforms and pseudo-eigenvalues of W-operators, *Invent. Math.* 48 (1978), 221–243.

[Ca] Carayol, H.: Sur les représentations l-adiques attachées aux formes modulaires de Hilbert, *Ann. scient. E.N.S.* 19 (1986), 409–468.

[Hi] Hida, H.: Galois representations into $GL_2[[X]]$ attached to ordinary cusp forms, *Inv. Math.* 85 (1986), 545–577.

[Jo-Li] Jordan, B.W. and Livné, R.: Conjecture 'epsilon' for weight $k > 2$, *Bull. Amer. Math. Soc.* 21 (1989), 51–69.

[Ko] Koike, M.: Congruences between cusp forms and linear representations of the Galois group, *Nagoya Math. J.* 64 (1976), 63–85.

[Kr] Kraus, A.: 'Thèse: Sur l'arithmétique des courbes elliptiques', 1990.

[La] Langlands, R.P.: Automorphic forms and l-adic representations, *Modular Forms of One Variable II*, 361–500; *Springer Lect. Notes* 349, 1973.

[Ma] Mazur, B.: Rational isogenies of prime degree, *Invent. Math.* 44 (1978), 129–162.

[Ma-Ti] Mazur, B. and Tilouine, J.: Représentations galoisiennes, différentielles de Kähler, et 'conjectures principales',*Publ. Math. IHES* 71 (1990), 65–103.

[Mi] Miyake, T.: On automorphic forms on GL_2 and Hecke operators, *Ann. of Math.* 94 (1971), 174–189.

[Og] Ogg, A.: On the eigenvalues of the Hecke operators, *Math. Ann.* 79 (1969), 101–108.

[Ri] Ribet, K.: On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* 100 (1990), 431–476.

[Se1] Serre, J.-P.: Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures); Séminaire Delange–Pisot–Poitou 19 (1969/70); Œ 87. Springer, 1986.

[Se2] Serre, J.P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331; Œ 94, 1986.

[Se3] Serre, J.-P.: Valeurs propres des opérateurs de Hecke modulo l, *Astérisque* 24–25 (1975), 109–117; Œ 104, Springer, 1986.

[Se4] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54 (1987), 179–230.

[Se-Ta] Serre, J.-P. and Tate, J.: Good reduction of abelian varieties, *Ann. of Math.* 88 (1968), 492–517; Œ 79, Springer, 1986.

[Sh] Shimura, G.: On the factors of the Jacobian variety of a modular function field, *J. Math. Soc. Japan* 25 (1976), 523–544.

[Wi] Wiles, A.: On p-adic representations for totally real fields, *Ann. of Math.* 123 (1986), 407–456.