On the two-dimensional modular representations of[*][†] $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Jean-Pierre Serre

To Yuri Ivanovich Manin, for his 50-th birthday

This paper revisits and strengthens a *conjecture* stated in 1973, a particular case of which can be found in [42, Section 3].

It concerns "modular" representations (in the sense of Brauer) of dimension two of the Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

If $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is such a representation, which we assume to be irreducible and of odd determinant, the conjecture says that ρ really is "modular", in the sense that it arises from a cusp form mod p that is an eigenfunction for the Hecke operators.

In order for this statement to be both useful and computationally verifiable, it is necessary to pinpoint the type of the modular form corresponding to ρ: level N, weight k, character ε. As far as N is concerned, the known examples suggest a simple answer: N should be the *Artin conductor* of ρ (see Subsection 1.2); in particular, it would only depend on the ramification of ρ away from p. As soon as N is known, the congruence class of k mod $(p-1)$ and the character ε are easily obtained from the determinant of ρ (see Subsection 1.3). It remains to determine the exact value of the *weight* k (or rather its minimal value). This is a delicate question, which was not broached in [42]. It seems that k only depends on the ramification of ρ at p (exponents of the characters of the tame inertia, wild inertia, etc.); the precise recipe that I propose is described in Subsections 2.2, 2.3 and 2.4.

The definitions of N, k and ε sketched above can be found in Sections 1 and 2. Section 3 contains the main statement, with various complements. Section 4 explores the pleasant consequences that this statement would have, if true: Fermat's theorem, the Taniyama-Weil conjecture, etc. Finally, Section 5 gives a number of numerical examples, for $p = 2$, 3 and 7.

This text owes much to the following mathematicians, and it is my pleasure to thank them:

---

[*]This paper appeared in the *Duke Mathematical Journal, Vol. 54, No. 1, 1987*.
[†]Translated from the original French by Alexandru Ghitza <aghitza@alum.mit.edu>.

- John Tate, for his many letters (especially in 1973 and 1974) about the conjecture, as well as about the relations between the weight and the inertia at p;
- Jean-Marc Fontaine, whose results on the local representations attached to cohomology have confirmed Tate's ideas, and have allowed to pinpoint the value of the weight k attached to a representation;
- Gerhard Frey, who had the fundamental idea (see [17]) that the Taniyama-Weil conjecture, completed appropriately, implies Fermat's theorem; i.e. "Weil + epsilon[1] $\Rightarrow$ Fermat";

finally, and especially:

- Jean-François Mestre, who succeeded in programming and verifying sufficiently many examples to convince me that the conjecture was worth taking seriously.

Contents

1 Definition of N, ε, and k mod $(p-1)$

1.1 Notation

The letter p denotes a prime number. We write $\overline{\mathbb{F}}_p$ for an algebraic closure of the field $\mathbb{F}_p$, and $\overline{\mathbb{Q}}$ for an algebraic closure of the field $\mathbb{Q}$. We set $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We consider a continuous homomorphism

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V),$$

where V is a two-dimensional vector space over $\overline{\mathbb{F}}_p$. The image of ρ is a finite group, which we denote G; by definition, this group is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$, where q is an appropriate power of p. (If $p \neq 2$, or if ρ is irreducible, we can take $\mathbb{F}_q$ to be the field generated by the *traces* of the elements of G.)

We aim to attach to ρ positive integers N and k, as well as a Dirichlet character $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$.

[1] It appears that Ribet has recently succeeded in eliminating "epsilon", so that "Weil $\Rightarrow$ Fermat"

1.2 Definition of N

The integer N is simply the *Artin conductor* of ρ, defined as in characteristic zero (cf. [1], [45]), except that we restrict to places that are prime to p.

More precisely, let ℓ be a prime number $\neq p$. We choose an extension to $\overline{\mathbb{Q}}$ of the ℓ-adic valuation of $\mathbb{Q}$, and we let

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset \cdots$$

be the sequence of ramification groups of G corresponding to this valuation ([45, Chapter IV]). Let V_i be the subspace of V consisting of those elements fixed by G_i, and let

$$n(\ell, \rho) = \sum_{i=0}^{\infty} \frac{1}{[G_0 : G_i]} \dim V/V_i. \tag{1.2.1}$$

We can rewrite (1.2.1) as

$$n(\ell, \rho) = \dim V/V_0 + b(V), \tag{1.2.2}$$

where $b(V)$ is the "wild invariant" of the G_0-module V, cf. [44, Subsection 19.3].

These formulas imply that

1. $n(\ell, \rho)$ is an integer ≥ 0;
2. $n(\ell, \rho) = 0$ if and only if $G_0 = \{1\}$, i.e. if and only if ρ is unramified at ℓ;
3. $n(\ell, \rho) = \dim V/V_0$ if and only if $G_1 = \{1\}$, i.e. if and only if ρ is tamely ramified at ℓ.

It follows from (a) and (b) that we can define an integer N by the formula

$$N = \prod_{\ell \neq p} \ell^{n(\ell, \rho)}. \tag{1.2.3}$$

We will call N the *conductor* of ρ; by construction, N is coprime to p.

1.3 Definition of the character ε and the class of k mod $(p-1)$

The *determinant* of the representation ρ is a homomorphism

$$\det \rho \colon G_{\mathbb{Q}} \longrightarrow \overline{\mathbb{F}}_p^{\times}.$$

Its image is a finite cyclic subgroup of $\overline{\mathbb{F}}_p^{\times}$, of order coprime to p. We can therefore think of $\det \rho$ as a character of $G_{\mathbb{Q}}$. The conductor of this character divides pN: this can be seen, for instance, by comparing the formulas giving the conductors of ρ and of $\det \rho$. We can therefore identify $\det \rho$ with a homomorphism from $(\mathbb{Z}/pN\mathbb{Z})^\times$ to $\overline{\mathbb{F}}_p^\times$, or, equivalently, with a pair of homomorphisms

(1.3.1) $$\varphi\colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \overline{\mathbb{F}}_p^\times$$

and

(1.3.2) $$\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \overline{\mathbb{F}}_p^\times.$$

As $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, the homomorphism φ is of the form

(1.3.3) $$x \mapsto x^h, \text{ with } h \in \mathbb{Z}/(p-1)\mathbb{Z}.$$

This can be rewritten as

(1.3.4) $$\varphi = \chi^h,$$

where $\chi\colon G_\mathbb{Q} \to \overline{\mathbb{F}}_p^\times$ denotes the p-th *cyclotomic character* of $G_\mathbb{Q}$ (the character that gives the action of $G_\mathbb{Q}$ on the p-th roots of unity).

We can summarize these formulas by saying that, if ℓ is a prime number not dividing pN, and if $\mathrm{Frob}_{\ell,\rho}$ is corresponding Frobenius element of G (defined up to conjugation), we have

(1.3.5) $$\det(\mathrm{Frob}_{\ell,\rho}) = \ell^h \varepsilon(\ell) \quad \text{in } \overline{\mathbb{F}}_p^\times.$$

In §2, we will define a certain integer k attached to ρ and we will see (in 2.5) that h is simply the congruence class of $k-1$ mod $(p-1)$, so that (1.3.5) can be rewritten as:

(1.3.6) $$\det(\mathrm{Frob}_{\ell,\rho}) = \ell^{k-1} \varepsilon(\ell) \quad \text{in } \overline{\mathbb{F}}_p^\times.$$

Remark. Let c be the element of order 2 of $G_\mathbb{Q}$ given by complex conjugation (relative to an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$). The image of c in $(\mathbb{Z}/pN\mathbb{Z})^\times$ is -1. We conclude that

(1.3.7) $$\det \rho(c) = (-1)^{k-1} \varepsilon(-1).$$

In the rest of this paper, we will only consider the case where $\det \rho$ is *odd*, i.e.

(1.3.8) $$\det \rho(c) = -1,$$

in other words

(1.3.9) $$\varepsilon(-1) = (-1)^k \quad \text{in } \overline{\mathbb{F}}_p^\times.$$

If $p = 2$, this condition is automatically satisfied, since $-1 = 1$. If $p \neq 2$, the condition means that $\rho(c)$ is conjugate to the matrix $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$.

2 The integer k

The objective of this section is to define the integer k (the "weight") attached to a representation ρ. Subsections 2.1 to 2.4 contain the general definition; Subsections 2.5 to 2.9 give various examples.

2.1 Preliminaries

The integer k depends only on the restriction of the representation ρ to the decomposition group at p (in fact, only on the inertia group). Therefore, in order to define it, we will start with a representation "local at p":

$$\rho_p \colon G_p \longrightarrow \mathrm{GL}(V) \cong \mathrm{GL}_2(\overline{\mathbb{F}}_p),$$

where $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

We write I for the inertia group of G_p, and I_p for the largest pro-p-subgroup of I (the *wild* inertia group). The quotient $I_t = I/I_p$ is the *tame inertia group* of G_p; it is identified with $\varprojlim_n \mathbb{F}_{p^n}^\times$, cf. [39, Proposition 2]. A character of I_t is said to have *level* n if it factors through $\mathbb{F}_{p^n}^\times$, and it does not factor through $\mathbb{F}_{p^m}^\times$ for any strict divisor m of n.

If V^{ss} denotes the semisimplification of V with respect to the action of G_p, the group I_p acts trivially on V^{ss} ([39, Proposition 4]), so that I_t acts on V^{ss}. This action of I_t is diagonalizable; it is given by two characters

$$\varphi, \varphi' \colon I_t \longrightarrow \overline{\mathbb{F}}_p^\times.$$

Proposition 1. *The characters φ and φ' giving the action of I_t on V^{ss} have level 1 or 2. If they have level 2, then they are conjugate: we have $\varphi' = \varphi^p$ and $\varphi = \varphi'^p$.*

Proof. Let s be an element of G_p whose image in $G_p/I = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is the Frobenius automorphism $x \mapsto x^p$. We check easily that, if $u \in I$, we have $sus^{-1} \equiv u^p \pmod{I_p}$): conjugation by s acts on $I_t = I/I_p$ via $u \mapsto u^p$. It follows that the set $\{\varphi, \varphi'\}$ is stable under taking p-th power. There are then two cases:

1. we have $\varphi^p = \varphi$, $\varphi'^p = \varphi'$ and the two characters φ and φ' have level 1;
2. we have $\varphi^p = \varphi'$, $\varphi'^p = \varphi$, $\varphi \neq \varphi'$, and the two characters φ and φ' have level 2.

□

We now treat these two cases separately.

2.2 Definition of k when φ and φ' have level 2

Suppose that φ and φ' have level 2. The representation V is then *irreducible*: if it contains a stable one-dimensional subspace, then the action of I_t on this subspace would be via a character that can be extended to G_p, hence of level 1. Let ψ and $\psi' = \psi^p$ denote the two *fundamental characters of level* 2 of I_t ([39, Subsection 1.7]), in other words the two characters $I_t \to \mathbb{F}_{p^2}^\times \to \overline{\mathbb{F}}_p^\times$ corresponding to the two embeddings of $\mathbb{F}_{p^2}$ into the field $\overline{\mathbb{F}}_p$. We can write φ uniquely as

(2.2.1) $$\varphi = \psi^{a+pb} = \psi^a \psi'^b, \quad \text{with } 0 \leq a, b \leq p-1.$$

We have $b \neq a$, since otherwise φ would equal $(\psi\psi')^a = \chi^a$, where χ is the cyclotomic character (or rather its restriction to I), which would contradict the assumption that φ has level 2. Moreover, since φ' is conjugate to φ, we have

(2.2.2) $$\varphi' = \psi^b \psi'^a.$$

Interchanging φ and φ' if necessary, we can therefore assume that

(2.2.3) $$0 \leq a < b \leq p-1.$$

Then the integer k attached to ρ_p is defined by:

(2.2.4) $$k = 1 + pa + b.$$

Remarks

(1) The smallest possible value of k is $k = 2$, attained when $a = 0$, $b = 1$, that is when φ and φ' are equal to the *fundamental characters* ψ and ψ' of level 2.

(2) In the particular case $a = 0$, we have $(\varphi, \varphi') = (\psi^b, \psi'^b)$, with $1 \leq b \leq p-1$, and the definition of k simplifies to

$$k = 1 + b \quad (\text{hence } 2 \leq k \leq p).$$

The general case can be reduced to the case $a = 0$ by "twisting". Indeed, we can write ρ_p as

$$\rho_p = \chi^a \otimes \rho'_p,$$

where χ is the cyclotomic character (viewed as a character of G_p, and not just of I). The pair (a, b) attached to ρ'_p is then $(0, b-a)$, and the corresponding integer k is $k' = 1 + b - a$. We can therefore rewrite (2.2.4) as

(2.2.5) $$k = k' + a(p+1).$$

(Compare this to the formula giving the filtration of the "twist" of a given modular form, cf. [24], [40].)

2.3 Definition of k when φ and φ' have level 1, and I_p acts trivially

We suppose that the action of I on V is semisimple, and given by two characters (φ, φ') which are powers χ^a and χ^b of the cyclotomic character χ:

$$\rho_p|I = \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}$$

The integers a and b are determined mod $(p-1)$. We normalize them so that $0 \leq a, b \leq p-2$. Moreover, by interchanging φ and φ' if necessary, we may assume that $a \leq b$. We have then

(2.3.1) $$0 \leq a \leq b \leq p-2.$$

The integer k is then defined by

(2.3.2) $$k = \begin{cases} 1 + pa + b & \text{if } (a,b) \neq (0,0) \\ p & \text{if } (a,b) = (0,0). \end{cases}$$

Remarks

(1) Once again, the smallest possible value of k is $k = 2$, corresponding to $\varphi = 1$, $\varphi' = \chi$.

(2) The case $(a,b) = (0,0)$ corresponds to I acting trivially on V, in other words the representation ρ_p being *unramified*. The general formula $k = 1 + pa + b$ would give $k = 1$. Given that modular forms of weight 1 behave in an exceptional way, I prefer to avoid them, and to "translate" k by $p-1$; whence the value $k = p$ adopted here.

(3) When we twist ρ_p by the successive powers $\chi, \chi^2, \ldots$ of the character χ, the corresponding integers k form a *Tate cycle*, cf. [22], [21].

2.4 Definition of k when I_p does not act trivially

Suppose I_p does not act trivially, i.e. that the action of I is not tame. The elements of V fixed by I_p form a line D, stable under G_p. The action of G_p on V/D (respectively on D) is via a character θ_1 (respectively θ_2) of G_p:

(2.4.1) $$\rho_p = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}$$

We can write θ_1 and θ_2 uniquely as

(2.4.2) $$\theta_1 = \chi^\alpha \varepsilon_1, \quad \theta_2 = \chi^\beta \varepsilon_2, \qquad (\alpha, \beta \in \mathbb{Z}/(p-1)\mathbb{Z}),$$

where ε_1 and ε_2 are unramified characters of G_p with values in $\overline{\mathbb{F}}_p^\times$. The restriction of ρ_p to I is therefore

$$\rho_p|I = \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}.$$

We normalize the exponents α and β by

(2.4.3) $$0 \leq \alpha \leq p-2 \quad \text{and} \quad 1 \leq \beta \leq p-1.$$

(Note that χ^α and χ^β do not play symmetric roles here.) We set

(2.4.4) $$a = \min\{\alpha, \beta\} \quad \text{and} \quad b = \max\{\alpha, \beta\}.$$

In order to define k, we distinguish two cases:

(i) *The case $\beta \neq \alpha + 1$ (i.e. $\chi^\beta \neq \chi \cdot \chi^\alpha$).* We set then, as in Subsection 2.3:

(2.4.5) $$k = 1 + pa + b.$$

(Note the case $\chi^\alpha = \chi^\beta = 1$, $p \geq 3$, where (2.4.3) forces $\alpha = 0$, $\beta = p-1$, in such a way that (2.4.5) gives $k = p$, as in (2.3.2).)

(ii) *The case $\beta = \alpha + 1$ (i.e. $\chi^\beta = \chi \cdot \chi^\alpha$).*

The definition of k then depends on the type of wild ramification. There are two possible types, which I will call respectively *peu ramifié* and *très ramifié*. We define them as follows:

Let $K_0 = \mathbb{Q}_{p,\mathrm{nr}}$ be the maximal unramified extension of $\mathbb{Q}_p$; we have $I = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K_0)$. The group $\rho_p(I)$ is the Galois group of a certain totally ramified extension K of K_0, and the wild inertia group $\rho_p(I_p)$ is the Galois group of K/K_t, where K_t is the largest tamely ramified extension of K_0 contained in K.

$$\begin{array}{c} K \\ | \\ K_t \\ | \\ K_0 \end{array}$$

Since $\beta = \alpha + 1$, we deduce that $\mathrm{Gal}(K_t/K_0) = (\mathbb{Z}/p\mathbb{Z})^\times$, so $K_t = K_0(z)$, where z is a primitive p-th root of unity. On the other hand, the group $\mathrm{Gal}(K/K_t) = \rho_p(I_p)$ is an elementary abelian group of type $(p, \ldots, p)$, representable as matrices by $\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]$. Moreover, the hypothesis $\beta = \alpha + 1$ means that the conjugation action of $\mathrm{Gal}(K_t/K_0) = (\mathbb{Z}/p\mathbb{Z})^\times$ on $\mathrm{Gal}(K/K_t)$ is the obvious action. Using Kummer theory, we deduce that K can be written as

(2.4.6) $$K = K_t\left(x_1^{1/p}, \ldots, x_m^{1/p}\right), \quad \text{where } p^m = [K\colon K_t],$$

the x_i being elements of $K_0^\times/K_0^{\times p}$. If v_p denotes the valuation of K_0, normalized so that $v_p(p) = 1$, we will say that the extension K (or the representation ρ_p) is *peu ramifiée* if

$$v_p(x_i) \equiv 0 \pmod p \quad \text{for } i = 1, \dots, m, \tag{2.4.7}$$

i.e. if the x_i can be chosen among the *units* of K_0. Otherwise, we will say that K and ρ_p are *très ramifiées*.

Remarks

(1) The très ramifié case is only possible if the characters ε_1 and ε_2 defined by (2.4.2) are equal, in which case we have $m = 1$ or $m = 2$: this can be seen by using the conjugation action of G_p on $\rho_p(I_p)$.

(2) Let π be a uniformizer of K_t, for instance $\pi = 1 - z$ or $\pi = p^{1/(p-1)}$. If K/K_t is peu ramifiée, the $p^m - 1$ characters of order p attached to this extension all have conductor (π^2); in the très ramifié case, $p^m - p^{m-1}$ of these characters have conductor $(\pi^{p+1}) = (p\pi^2)$ and the other $p^{m-1} - 1$ have conductor (π^2).

We can now define the integer k:

(ii_1) *The case $\beta = \alpha + 1$, peu ramifié*

The formula is the same as in the case $\beta \neq \alpha + 1$:

$$k = 1 + pa + b = 2 + \alpha(p + 1). \tag{2.4.8}$$

(ii_2) *The case $\beta = \alpha + 1$, très ramifié*

We add $p - 1$ (respectively 2 if $p = 2$) to the result of (2.4.8):

$$k = \begin{cases} 1 + pa + b + p - 1 = (\alpha + 1)(p + 1) & \text{if } p \neq 2 \\ 4 & \text{if } p = 2. \end{cases} \tag{2.4.9}$$

The formulas (2.2.4), (2.3.2), (2.4.5), (2.4.8), (2.4.9) give the complete definition of the integer k attached to the given representation ρ_p. Here are some properties that follow from this definition.

2.5 Class of k mod $(p - 1)$

Proposition 2. *We have*

$$\det \rho_p | I = \chi^{k-1}. \tag{2.5.1}$$

(Since χ has order $p - 1$, this formula show that the class of k mod $(p - 1)$ is determined by $\det \rho_p$, more precisely by the restriction of $\det \rho_p$ to the inertia group I.)

Proof. We check (2.5.1) in the case of level 2 (cf. Subsection 2.2). We have then

$$\det \rho_p | I = \varphi \cdot \varphi' = (\psi^a \psi'^b)(\psi^b \psi'^a) = (\psi\psi')^{a+b} = \chi^{a+b} = \chi^{k-1},$$

as $k - 1 = pa + b \equiv a + b \bmod (p-1)$.

The other cases are analogous. □

We can rewrite (2.5.1) as

$$\det \rho_p = \varepsilon_p \cdot \chi^{k-1}, \tag{2.5.2}$$

where ε_p is an *unramified character* of G_p with values in $\overline{\mathbb{F}}_p^\times$. When ρ_p comes from a global representation ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the character ε_p is just the *p-component* of the character ε defined in Subsection 1.3; we have

$$\varepsilon_p(\mathrm{Frob}_p) = \epsilon(p), \tag{2.5.3}$$

where Frob_p is the Frobenius element of G_p.

2.6 Values of k

If $p \neq 2$, the possible values of k are the integers in the interval $[2, p^2 - 1]$ that can be written as

$$k = 1 + a_0 + pa_1, \quad 0 \leq a_0, a_1 \leq p - 1,$$

with $a_1 \leq a_0 + 1$. For instance, if $p = 3$, we have $k = 2, 3, 4, 5, 6$ or 8.

If $p = 2$, we have $k = 2$ if the action of I_p is trivial or peu ramifiée, and $k = 4$ if the action of I_p is très ramifiée.

Example. Let $p = 2$. Let $u\colon G_2 \to \mathbb{Z}/2\mathbb{Z}$ be a surjective homomorphism, and let $\rho_2\colon G_2 \to \mathrm{GL}_2(\mathbb{F}_2)$ be the representation given by

$$s \mapsto \begin{pmatrix} 1 & u(s) \\ 0 & 1 \end{pmatrix}.$$

Let $K/\mathbb{Q}_2$ be the quadratic extension corresponding to the kernel of u. We have then

- $k = 2$ if $K/\mathbb{Q}_2$ is unramified, i.e. $K = \mathbb{Q}_2(\sqrt{5})$;
- $k = 2$ if $\mathrm{disc}(K/\mathbb{Q}_2) = (4)$, i.e. $K = \mathbb{Q}_2(\sqrt{-1})$ or $\mathbb{Q}_2(\sqrt{-5})$;
- $k = 4$ if $\mathrm{disc}(K/\mathbb{Q}_2) = (8)$, i.e. $K = \mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{10})$ or $\mathbb{Q}_2(\sqrt{-10})$.

2.7 Conditions that imply $k \leq p + 1$, when $p \neq 2$

Suppose $p \neq 2$. We have $k \leq p + 1$ if and only if one of the following conditions is satisfied:

(2.7.1) There exists a quotient V/D of V, of dimension one, on which I acts trivially (i.e. *V has an étale quotient of dimension one*); it is the case $a = 0$ of Subsections 2.3 and 2.4.

(2.7.2) The action of I on V is given by two tame characters of the form (ψ^b, ψ'^b), with $1 \leq b \leq p-1$, where ψ and ψ' are the two fundamental characters of level 2 of I_t; it is the case $a = 0$ of Subsection 2.2.

Remarks

(1) We have $k = p+1$ if and only if the restriction of ρ_p to the inertia group I is of the form $\left[\begin{smallmatrix}\chi & * \\ 0 & 1\end{smallmatrix}\right]$ and is très ramifiée.

(2) Given any representation ρ_p, there exists a "twist" $\chi^m \otimes \rho_p$ of ρ_p whose invariant k is $\leq p+1$ (compare to [42, Theorem 3]).

2.8 Conditions that imply $k = 2$

The following statement follows immediately from the definitions:

Proposition 3. *The invariant k of ρ_p is equal to 2 if and only if $\rho_p|I$ is of one of the following types:*

(2.8.1) $$\rho_p|I \cong \begin{pmatrix}\psi' & 0 \\ 0 & \psi\end{pmatrix},$$

where $\psi, \psi' \colon I \to I_t \to \mathbb{F}_{p^2}^\times$ are the two fundamental characters of I of level 2; or

(2.8.2) $$\rho_p|I \cong \begin{pmatrix}\chi & 0 \\ 0 & 1\end{pmatrix} \quad \textit{or} \quad \begin{pmatrix}\chi & * \\ 0 & 1\end{pmatrix},$$

the action of the wild inertia group I_p being either trivial, or peu ramifiée.

We can given another characterization of this case, in terms of *group schemes of type* (p,p). To state this, I will restrict to the case where ρ_p takes values in $\mathrm{GL}_2(\mathbb{F}_p)$, therefore defines an (étale) group scheme of type (p,p) over the field $\mathbb{Q}_p$ (in the general case, we must talk about "$\mathbb{F}_q$-vector space schemes" as in Raynaud [35]). We can ask whether this group scheme extends to a finite flat group scheme over $\mathbb{Z}_p$, cf. [35]; if so, I will say (cf. [48]) that the representation ρ_p is *finite* at p.

Proposition 4. *We have $k = 2$ if and only if the following two conditions are satisfied:*

(2.8.3) $$\det \rho_p|I = \chi;$$

(2.8.4) $$\rho_p \textit{ is finite at } p.$$

Proof. According to Subsection 2.5, condition (2.8.3) is equivalent to:

(2.8.5) $$k \equiv 2 \bmod (p-1).$$

The condition is therefore necessary so that k be equal to 2. Let's show that it is also sufficient when ρ_p is finite at p. According to [35, Corollary 3.4.4], each of the characters φ and φ' of I_t associated to ρ_p can be written as

$$\psi^n \psi'^{n'}, \quad \text{with } 0 \leq n, n' \leq 1,$$

where ψ and ψ' are, as before, the two fundamental characters of level 2. This gives four possibilities

$$1, \psi, \psi' \text{ and } \psi\psi' = \chi$$

(which can be reduced to three when $p = 2$ as χ is then 1). As $\varphi\varphi' = \chi$ by (2.8.1), only two possibilities remain:

$$\text{(i)} \quad \{\varphi, \varphi'\} = \{\psi, \psi'\}$$

and

$$\text{(ii)} \quad \{\varphi, \varphi'\} = \{1, \chi\}.$$

The case (i) gives (2.8.1), whence $k = 2$, as stated. It remains to deal with the case (ii); for simplicity, we will restrict to the case $p \neq 2$ (the case $p = 2$ is somewhat different, but can be treated analogously). Let J be the finite flat group scheme over $\mathbb{Z}_p$ extending the scheme over $\mathbb{Q}_p$ defined by ρ_p (according to [35, Proposition 3.3.2], this scheme is unique). It follows from (ii) that ρ_p is reducible, and so is J. So we have an exact sequence of finite flat group schemes over $\mathbb{Z}_p$:

(2.8.6) $$0 \longrightarrow A \longrightarrow J \longrightarrow B \longrightarrow 0,$$

where A and B are finite flat group schemes of order p. Moreover, (ii) forces one of these schemes to be étale, and the other one multiplicative. Therefore it exists a finite étale extension R of $\mathbb{Z}_p$ over which A or B becomes isomorphic to the constant étale scheme $\mathbb{Z}/p\mathbb{Z}$, and B or A to the scheme μ_p of p-th roots of unity. Over R, the exact sequence (2.8.6) becomes

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow J \longrightarrow \mu_p \longrightarrow 0$$

or

$$0 \longrightarrow \mu_p \to J \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

In the first case, it is easy to see that the extension J is *split* (use the connected component of the identity), i.e. isomorphic over R to $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$; whence (2.8.2), with trivial action of I_p, which indeed implies that $k = 2$. In the second case, we note (by the Kummer exact sequence) that the class of the extension J is given by an element $u \in R^\times / R^{\times p}$, therefore

$$\rho_p | I \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix},$$

and the field K of Subsection 2.4 is equal to $K_t(u^{1/p})$; as u is a unit, the extension K/K_t is either unramified or peu ramifiée, whence again $k = 2$ by (2.8.2). (The fact that K/K_t is not très ramifiée can also be deduced from a general result of Fontaine, cf. [15, Theorem 1].)

It remains to prove that $k = 2$ implies that ρ_p is finite at p. According to Proposition 3, we have to consider two cases:

1. the case where $\rho_p | I$ is given by the two fundamental characters ψ and ψ'. This case is treated in Raynaud [35, Theorem 2.4.3].

2. the case where $\rho_p | I$ is of the form $\left[\begin{smallmatrix} \chi & * \\ 0 & 1 \end{smallmatrix}\right]$, with the action of I_p trivial or peu ramifiée. We then perform a direct construction, based on the classification of extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p, cf. above (a little more precisely, we start by replacing $\mathbb{Z}_p$ by a suitable finite étale extension R, we construct the extension in question over R, then we descend to $\mathbb{Z}_p$).

□

2.9 Example of calculation of k: p-torsion points on a semistable elliptic curve

Let E be an elliptic curve over $\mathbb{Q}_p$, with modular invariant j_E, and let E_p be the group of p-torsion points of E. The action of G_p on E_p defines a representation

$$\rho_p \colon G_p \longrightarrow \mathrm{Aut}(E_p) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

Since $\det \rho_p = \chi$, the invariant k attached to ρ_p satisfies

(2.9.1) $$k \equiv 2 \bmod (p-1).$$

We will determine the value of k in the case where E is *semistable*, i.e. either has good reduction, or has multiplicative reduction (cf. [39, Subsections 1.11 and 1.12]):

Proposition 5. *(i) If E has good reduction, then $k = 2$.*

(ii) If E has multiplicative reduction, then

$$k = \begin{cases} 2 & \text{if } v_p(j_E) \text{ is divisible by } p \\ p+1 & \text{otherwise.} \end{cases}$$

(Here, and in the following, we write v_p for the p-adic valuation, normalized so that $v_p(p) = 1$.)

Proof. If E has good reduction, ρ_p is clearly finite at p, and statement (i) follows from Proposition 4.

If E has multiplicative bad reduction, we use the Tate model ([39, Subsection 1.12]). This shows that, after an unramified quadratic extension of $\mathbb{Q}_p$, we have an exact sequence of Galois modules

$$0 \longrightarrow \mu_p \longrightarrow E[p] \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

hence

$$\rho_p|I \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}.$$

Let q_E be the element of $\mathbb{Q}_p^\times$ defined by the identity

$$j_E = q_E^{-1} + 744 + 196884 q_E + \dots$$

We note that the extension K/K_t from Subsection 2.4 is $K = K_t(q_E^{1/p})$. This extension is therefore très ramifiée if and only if $v_p(q_E)$ is not divisible by p; since $v_p(q_E) = -v_p(j_E)$, we deduce (ii). □

Remarks

(1) Suppose we are in case (ii) with $k = 2$, i.e. that E has multiplicative bad reduction and $v_p(j_E)$ is divisible by p. Let $m = -v_p(j_E)/p$ and $u = p^{pm} j_E$, so that u is a p-adic unit and q_E is equal to the product of u^{-1} and the p-th power of an element of K_t. We then have $K = K_t(u^{1/p})$ and we see that

  a) if $u^{p-1} \equiv 1 \pmod{p^2}$, we have $K = K_t$ and $\rho_p|I \cong \left[\begin{smallmatrix} \chi & 0 \\ 0 & 1 \end{smallmatrix}\right]$;

  b) if $u^{p-1} \not\equiv 1 \pmod{p^2}$, we have $[K\colon K_t] = p$ and $\rho_p|I \cong \left[\begin{smallmatrix} \chi & * \\ 0 & 1 \end{smallmatrix}\right]$.

Case (b) can indeed occur, contrary to what is stated in [6, Proposition 5.1.(3)(d)].

(2) Calculations analogous to those of Proposition 5 (but more complicated) are possible when E has additive bad reduction. I will simply give the result in a typical special case, that of $p \equiv 1 \pmod 3$, with the minimal equation of E of the form

$$y^2 = x^3 + Ax + B,$$

with $v_p(A) \geq 1$ and $v_p(B) = 1$ (Néron type c_1).

We then find

$$\rho_p|I \cong \begin{pmatrix} \chi^\beta & 0 \\ 0 & \chi^\alpha \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix},$$

with $\alpha = (p-1)/6$ and $\beta = (5p+1)/6$.

If $p > 7$, this implies that $k = 1 + p\alpha + \beta = 2 + (p-1)(p+5)/6$. However, for $p = 7$, we can have either $k = 2 + (p-1)(p+5)/6 = 14$, or $k = 2$, the latter occurring if $v_p(A) \geq 2$.

3 Statement of the conjecture

3.1 Review of cusp forms in characteristic p

Let

- N be an integer ≥ 1, coprime to p;
- k be an integer ≥ 2;
- ε be a character $(\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$.

Suppose that

$$\begin{cases} (-1)^k = \varepsilon(-1) & \text{if } p \neq 2 \\ k \text{ is even} & \text{if } p = 2. \end{cases} \tag{3.1.1}$$

We will use the notion of *cusp form of type* (N, k, ε) *with coefficients in* $\overline{\mathbb{F}}_p$. As several definitions are possible (cf. [23] and [24] for instance), we better explain what we mean:

Identify $\overline{\mathbb{Q}}$ with a subfield of $\mathbb{C}$, and choose a place of $\overline{\mathbb{Q}}$ over p. If $\overline{\mathbb{Z}}$ denotes the ring of integers of $\overline{\mathbb{Z}}$, this choice of place defines a homomorphism $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$ which we denote $z \mapsto \tilde{z}$. Finally denote

$$\varepsilon_0 \colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Z}}^\times$$

the multiplicative lift of ε, i.e. the unique character with values in the prime-to-p roots of unity such that

$$\widetilde{\varepsilon_0(x)} = \varepsilon(x) \quad \text{for all } x \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

According to (3.1.1), we have $\varepsilon_0(-1) = (-1)^k$. We can therefore talk about *cusp forms of type* (k, ε_0) *on* $\Gamma_0(N)$, in the usual sense. Recall (cf. for instance [11]) that such a form is a series

$$F = \sum_{n \geq 1} A_n q^n \quad (q = e^{2\pi i z}), \tag{3.1.2}$$

which converges in the half-plane $\mathrm{Im}(z) > 0$ and satisfies the two conditions:

1. $F((az+b)/(cz+d)) = \varepsilon_0(d)(cz+d)^k F(z)$ for all $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(N)$ and all $z \in \mathbb{C}$ such that $\mathrm{Im}(z) > 0$;
2. F vanishes at the cusps, i.e. for all $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, the function

   $$z \mapsto (cz+d)^{-k} F((az+b)/(cz+d))$$

   has a power series expansion of the type (3.1.2), with q replaced by $q^{1/N}$.

For short, we will say that such a form F is *of type* (N, k, ε_0).

We can now define the analogous notion in characteristic p:

Definition. A cusp form of type (N, k, ε) with coefficients in $\overline{\mathbb{F}}_p$ is a formal power series

$$f = \sum_{n \geq 1} a_n q^n, \quad a_n \in \overline{\mathbb{F}}_p,$$

such that there exists a cusp form

$$F = \sum_{n=1}^{\infty} A_n q^n, \quad A_n \in \overline{\mathbb{Z}},$$

of type (N, k, ε_0) in the sense discussed above, such that $\tilde{F} = f$, i.w. that $\tilde{A}_n = a_n$ for all n.

(Instead of assuming that the A_n belong to $\overline{\mathbb{Z}}$, we could just demand that they belong to the *local ring* of the place of $\overline{\mathbb{Q}}$ chosen at the start. This would not change anything.)

We wrte $S(N, k, \varepsilon)$ for the space of f of the type described above. This space has the following properties:

(3.1.3) $S(N, k, \varepsilon)$ does not depend on the choice of p-adic place of $\overline{\mathbb{Q}}$ used to define it. Moreover, its dimension over $\overline{\mathbb{F}}_p$ is equal to the dimension of the corresponding space $S(N, k, \varepsilon_0)$ over $\mathbb{C}$.

This follows from Shimura's result [52, Theorem 3.52] (see also [11, Proposition 2.7]).

(3.1.4) $S(N, k, \varepsilon)$ is stable under the action of the Hecke operators:

$$\begin{aligned} T_\ell\colon \sum a_n q^n &\mapsto \sum a_{\ell n} q^n + \varepsilon(\ell)\ell^{k-1} \sum a_n q^{\ell n} && (\ell \nmid pN), \\ U_\ell\colon \sum a_n q^n &\mapsto \sum a_{\ell n} q^n && (\ell \mid pN). \end{aligned}$$

For the T_ℓ and U_ℓ (ℓ prime not equal to p), this follows from the similar properties in characteristic zero. For U_p, one observes that it is the reduction (mod p) of the Hecke operator

$$T_p\colon \sum a_n q^n \mapsto \sum a_{pn} q^n + \varepsilon_0(p)p^{k-1} \sum a_n q^{pn},$$

thanks to the hypothesis $k \geq 2$.

(3.1.5) The Hecke operators commute. If

$$f = \sum a_n q^n, \quad f \neq 0,$$

if an eigenfunction for these operators, we can multiply f by a nonzero scalar so that $a_1 = 1$. Once f has been normalized in this way, we have $T_\ell(f) = a_\ell f$ for $\ell \nmid pN$ and $U_\ell(f) = a_\ell f$ for $\ell \mid pN$: the a_ℓ are the eigenvalues of T_ℓ and U_ℓ. Moreover, the formal Dirichlet series

$$L_f(s) = \sum a_n n^{-s} \quad \text{(with coefficients in } \overline{\mathbb{F}}_p\text{)}$$

is given by the usual Euler product:

$$L_f(s) = \prod_{\ell \mid pN} (1 - a_\ell \ell^{-s})^{-1} \prod_{\ell \nmid pN} (1 - a_\ell \ell^{-s} + \varepsilon(\ell)\ell^{k-1}\ell^{-2s})^{-1}.$$

In particular, f is determined by the a_ℓ.

(3.1.6) If $f = \sum a_n q^n$ is an eigenfunction of the Hecke operators normalized as above, there exists a cusp form $F = \sum A_n q^n$ of type (N, k, ε_0) with coefficients in $\overline{\mathbb{Z}}$, which is an eigenfunction for the T_ℓ ($\ell \nmid N$) and the U_ℓ ($\ell \mid N$) and satisfies:

$$A_1 = 1; \quad \tilde{F} = f.$$

Indeed, since the operators T_ℓ and U_ℓ commute, any system of eigenvalues for these operators over $\overline{\mathbb{F}}_p$ can be lifted to characteristic 0 (cf. for instance [11, Lemma 6.11]). We conclude that there exists a cusp form $F = \sum A_n q^n$, of type (N, k, ϵ_0), an eigenfunction for the T_ℓ and the U_ℓ, normalized, and such that $\tilde{A}_\ell = a_\ell$ for any prime number ℓ. It follows immediately that $\tilde{F} = f$.

(Of course, F is not unique: two distinct eigenfunctions in characteristic 0 can have the same reduction to characteristic p.)

(3.1.7) Let $f = \sum a_n q^n$ be as above. According to a theorem of Deligne ([11, Theorem 6.7]), there exists a continuous semisimple representation

$$\rho_f \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

characterized (up to conjugation) by the following property:

(D). For any prime number ℓ not dividing pN, the representation ρ_f is unramified at ℓ, and, if we write $\rho_f(\mathrm{Frob}_\ell)$ for the corresponding Frobenius element (defined up to conjugation), we have

(3.1.8) $$\mathrm{Tr}\rho_f(\mathrm{Frob}_\ell) = a_\ell$$

and

(3.1.9) $$\det \rho_f(\mathrm{Frob}_\ell) = \varepsilon(\ell)\ell^{k-1}.$$

Formula (3.1.9) can be rewritten with the notation of Subsection 1.3 as

(3.1.10) $$\det \rho_f = \varepsilon\chi^{k-1}.$$

Taking into account (3.1.1), this means that $\det\rho_f(c) = -1$, in other words thata $\det\rho_f$ is an *odd* character.

Remark. I assumed at the start that the level is coprime to p. In fact, this is not necessary: all the stated results remain true in the general case. However, the gained generality does not supply "mod p forms" that are genuinely new; indeed we know that any cusp form with coefficients in $\overline{\mathbb{F}}_p$ of level $p^m N$ is also of level N, at the expense of increasing the weight. A typical example is that of forms of weight 2 and level p, which are also of weight $p+1$ and level 1, cf. [41, Theorem 11].

3.2 The conjecture and some variants

Let us return to the notation of Section 1, and let

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V) \cong \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

be a continuous homomorphism, V being a two-dimensional vector space over $\overline{\mathbb{F}}_p$. We assume that

(3.2.1) ρ *is irreducible*,

and

(3.2.2) $\det\rho$ *is odd*, cf. (1.3.8).

The *conjecture* then states that ρ is of type ρ_f as in (3.1.7). In other words:

(3.2.3?) *There exists a cusp form f (of suitable type) with coefficients in $\overline{\mathbb{F}}_p$ which is an eigenform for the Hecke operators, and whose associated representation ρ_f is isomorphic to the given representation ρ.*

It is useful to make (3.2.3?) precise by giving the type (N, k, ε) of f:

(3.2.4?) *The cusp form f of (3.2.3?) can be chosen to be of type (N, k, ε), where N, k and ε are the invariants of ρ defined in Sections 1 and 2.*

If $f = \sum a_n q^n$ is normalized ($a_1 = 1$), the fact that ρ_f is isomorphic to ρ translates into the equalities

(3.2.5) $$\mathrm{Tr}(\mathrm{Frob}_{\ell,\rho}) = a_\ell \quad \text{and} \quad \det(\mathrm{Frob}_{\ell,\rho}) = \varepsilon(\ell)\ell^{k-1},$$

which should hold for any prime number ℓ not dividing pN. (It is enough to have the first equality of (3.2.5) hold for a set of ℓ of density 1.)

Insofar as the a_ℓ for ℓ dividing pN are concerned, we conjecture

(3.2.6$_?$) *Suppose $f = \sum a_n q^n$ satisfies (3.2.3$_?$) and (3.2.4$_?$) and is normalized. Let ℓ be a prime divisor of pN. Then:*

1. *If $a_\ell \neq 0$, there exists a line D in V stable under the decomposition group at ℓ (relative to a given ℓ-adic place of $\overline{\mathbb{Q}}$) and such that the inertia group at ℓ acts trivially on V/D. (In other words, the restriction of ρ to the decomposition group at ℓ has a one-dimensional étale quotient.)*

   Moreover, a_ℓ is equal to the eigenvalue of the Frobenius element at ℓ acting on V/D.

2. *If $a_\ell = 0$, there are no lines in V with the properties stated in* (a).

Remarks on (3.2.6$_?$)

(1) If ℓ divides N, there exists at most one line D in V satisfying (a). Indeed, if there are two such lines, ρ would be étale at ℓ, and ℓ would not divide the conductor N.

We see then that, in this case, a_ℓ is completely determined by ρ.

[It is not hard to prove that D exists if and only if:

- either $v_\ell(N) = 1$, v_ℓ being the ℓ-adic valuation;
- or $v_\ell(N) = v_\ell(\text{cond}(\varepsilon))$, where $\text{cond}(\varepsilon)$ denotes the conductor of the character ε.

Moreover, if $v_\ell(N) = 1$ and $v_\ell(\text{cond}(\varepsilon)) = 0$, we can show that the eigenvalue λ of the Frobenius element at ℓ acting on V/D is such that $\lambda^2 = \varepsilon_{\text{prim}}(\ell)\ell^{k-2}$, where $\varepsilon_{\text{prim}}$ is the primitive character defined by ε. According to (3.2.6$_?$), we would then have

$$a_\ell^2 = \varepsilon_{\text{prim}}(\ell)\ell^{k-2},$$

which agrees perfectly with [27, Theorem 3(iii)].]

(2) If $\ell = p$ and ρ is ramified at p, the situation is the same as if ℓ divides N: the line D is unique if it exists; the eigenvalue a_p is completely determined. Hence the *uniqueness* of the form f in this case; its coefficients belong to the field of rationality of ρ, and generate this field over $\mathbb{F}_p$.

(3) If $\ell = p$ and ρ is unramified at p (which means that $k = p$ according to our conventions, cf. Subsection 2.3), the situation is different. There are then two possible values for a_p, namely the two eigenvalues λ and μ of the Frobenius element at p; we have $\lambda\mu = \varepsilon(p)$. Of course, it is possible that $\lambda = \mu$, in which case a_p is completely determined. If $\lambda \neq \mu$, in all the cases I know, there are *two* distinct cusp forms f such that $\rho_f \cong \rho$, one with $a_p = \lambda$ and the other with $a_p = \mu$. Note that λ and μ do not necessarily lies in the field of definition of ρ (which is generated by the a_ℓ for $\ell \neq p$): they could be quadratic over this field; we will see such examples in Section 5.1.

(4) If should be possible to make (3.2.6$_?$) more precise by determining the action on f of the Atkin-Lehner-Li operators W_ℓ ($\ell \mid N$), [3]. The corresponding pseudo-eigenvalues (in the sense of [3]) can undoubtedly be written in terms of the *local constants* of ρ (Deligne [9, Section 6]).

Remarks on (3.2.4$_?$)

(5) It is likely that N and k are *minimal* for ρ, in other words that, if ρ is isomorphic to $\rho_{f'}$ with f' of type (N', k', ε'), N' coprime to p, $k' \geq 2$, then N' is a multiple of N and k' is $\geq k$. In particular, if we write f as $\tilde{F}$ as in (3.1.6), F must be a *newform* (cf. [11], [27]) of type (N, k, ε_0).

(6) Instead of defining cusp forms with coefficients in $\overline{\mathbb{F}}_p$ by reduction from characteristic 0, as we have done, we could have used Katz's definition [23], which leads to a space that is *a priori* larger[2], hence could give rise to more representations ρ_f. It would be interesting to see if the additional representations obtained in this way can be irreducible; I know no such example (for $k \geq 2$), but, if this were to happen, one should modify (3.2.4$_?$) and (3.2.6$_?$). It would also be interesting to study from this point of view the case $k = 1$, which we have so far excluded; maybe Katz's definition then gives rise to many more representations ρ_f?

3.3 Example $k = 2$

We apply the conjectures of the previous subsection to a representation

$$\rho \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

satisfying:

1. $\det \rho = \chi$;
2. ρ is absolutely irreducible (i.e. irreducible over $\overline{\mathbb{F}}_p$);
3. ρ is finite at p, in the sense of Subsection 2.8.

[When $p \neq 2$, we can replace (b) by the following condition, which seems a priori weaker:

(b′) ρ is irreducible (over $\mathbb{F}_p$).

Indeed, (a) implies that $\det \rho$ is odd, so that the eigenvalues of $\rho(c)$ are $+1$ and -1; since $p \neq 2$, these eigenvalues are distinct. Suppose that ρ decomposes over $\overline{\mathbb{F}}_p$ into a direct sum of two one-dimensional representations; this decomposition would then

[2] Katz's definition has the following pleasant property: any form of weight k is also of weight $k + p - 1$. With the definition we have adopted, this is true for $p \geq 5$, but false for $p = 2$ or 3.

have to be the one given by the eigenvalues of $\rho(c)$, and therefore rational over $\mathbb{F}_p$, contradicting (b′).]

Let N, k and ε be the invariants of ρ. According to Subsection 1.3, we have $\varepsilon = 1$, and then Proposition 4 of Subsection 2.8 tells us that $k = 2$. Conjecture (3.2.4$_?$) then gives:

(3.3.1$_?$) *There exists a cusp form of weight 2 and level N, with coefficients in $\overline{\mathbb{F}}_p$, which is an eigenfunction of the Hecke operators and whose associated representation ρ_f is isomorphic to ρ.*

According to (3.2.6$_?$), this cusp form has coefficients in $\mathbb{F}_p$, except maybe in the case when ρ is unramified at p (which can only occur if $p = 2$).

We can restate (3.3.1$_?$) in terms of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ associated with the group $\Gamma_0(N)$:

(3.3.2$_?$) *The representation ρ occurs as a Jordan-Hölder quotient of the representation of $G_{\mathbb{Q}}$ on the p-torsion points of $J_0(N)$.*

3.4 Questions

We give two questions, one for pessimists, the other for optimists:

(1) How could one construct counter-examples to the conjectures of Subsection 3.2? I have made many attempts in this direction. They have all failed, as we will see in Section 5.

(2) Can we reformulate these conjectures in the framework of a theory of representations (mod p) of adelic groups? In other words, is there a "Langlands philosophy modulo p", as Ash and Stevens ask in [2]? If so, this might allow us to:

- give a more natural definition of the weight k attached to ρ;
- replace GL_2 by GL_N, or even by a reductive group;
- replace $\mathbb{Q}$ by other global fields.

4 Applications

These applications include:

- Fermat's equation and its variants (Sections 4.1 to 4.3);
- the discriminants of semi-stable elliptic curves (Section 4.4);
- the structure of group schemes of type (p, p) over $\mathbb{Z}$ (Section 4.5);

- the Taniyama-Weil conjecture, and its extension to abelian varieties with real multiplication (Sections 4.6 and 4.7);
- the cohomology of smooth projective varieties over $\mathbb{Q}$ with Betti number 2 in odd dimension (Section 4.8).

Except for the latter, these applications only use the conjecture (3.2.4$_?$) in the case $\varepsilon = 1$, $k = 2$, cf. Section 3.3.

4.1 Review of certain elliptic curves over $\mathbb{Q}$

Let A, B, C be three non-zero integers, pairwise coprime, and such that

$$A + B + C = 0.$$

Let us choose integers x_1, x_2, x_3 such that

$$x_1 - x_2 = A,\ x_2 - x_3 = B,\ x_3 - x_1 = C.$$

The elliptic curve with equation

$$y^2 = (x - x_1)(x - x_2)(x - x_3)$$

is independent of the choice of x_i (up to isomorphism). To make things precise, we will take $x_1 = A,\ x_2 = 0,\ x_3 = -B$, so that the above equation can be written

(4.1.1) $$y^2 = x(x - A)(x + B).$$

We denote the curve thus defined by $E_{A,B,C}$, or simply E.

Remark. A permutation of A, B, C of signature 1 (resp. -1), does not change E (resp. replaces E by its “twist” by the quadratic extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$).

Let us now give some properties of *bad reduction* of E (cf. Frey [17]).

(4.1.2) *Bad reduction at* $\ell \neq 2$. Let ℓ be a prime number $\neq 2$. The curve E has bad reduction at ℓ if and only if ℓ divides ABC, and this bad reduction is then of *multiplicative type*.

This follows immediately from (4.1.1). We also note that this equation provides a *minimal model* of E at ℓ, cf. Tate [4, p. 47].

(4.1.3) *Bad reduction at* 2. We shall confine ourselves to the case:

(4.1.4) $$A \equiv -1 \pmod 4 \ \text{ and } \ B \equiv 0 \pmod{32}.$$

By the change of variables

$$x = 4X, \qquad y = 8Y + 4X,$$

we transform (4.1.1) into the equation

$$Y^2 + XY = X^3 + cX^2 + dX, \quad \text{with } c = (B - 1 - A)/4, d = -AB/16, \tag{4.1.5}$$

whose reduction (mod 2) is:

$$Y^2 + XY = \begin{cases} X^3 & \text{if } A \equiv 7 \pmod 8 \\ X^3 + X^2 & \text{if } A \equiv 3 \pmod 8. \end{cases}$$

We thus obtain a cubic on $\mathbb{F}_2$ with a double point at $(0, 0)$ having distinct tangents (these tangents being rational over $\mathbb{F}_2$ if and only if $A \equiv 7 \pmod 8$). It follows that E has *bad reduction of multiplicative type at* 2 (Tate, loc. cit.) and that (4.1.5) is a *minimal equation* at 2, hence also over $\mathrm{Spec}(\mathbb{Z})$ according to what we have just seen. The corresponding discriminant Δ is:

$$\Delta = 2^{-8} A^2 B^2 C^2. \tag{4.1.6}$$

Thus E has everywhere either good reduction or bad reduction of multiplicative type: it is a *semi-stable* curve. Its *conductor* is given by:

$$\mathrm{cond}(E) = \mathrm{rad}(ABC), \tag{4.1.7}$$

where $\mathrm{rad}(X)$ designates the product of the primes dividing X (i.e. the largest square-free divisor of X).

The modular invariant j_E of E is:

$$j_E = 2^8 (C^2 - AB)^3 / A^2 B^2 C^2. \tag{4.1.8}$$

If ℓ divides ABC, we have:

$$v_\ell(j_E) = -v_\ell(\Delta) = \begin{cases} -2v_\ell(ABC) & \text{if } \ell \neq 2 \\ 8 - 2v_\ell(ABC) & \text{if } \ell = 2. \end{cases} \tag{4.1.9}$$

p-torsion points of E. Let p be a prime number ≥ 5. We will focus on the representation

$$\rho_p^E : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(F_p)$$

given by the p-torsion points of E.

First we have:

Proposition 6. *The representation ρ_p^E is irreducible.*

(As its determinant is equal to the cyclotomic character χ, the representation is even *absolutely irreducible*, cf. Section 3.3.).

Proof. Suppose that ρ_p^E is reducible, i.e. that E contains a subgroup X of order p which is $\mathbb{Q}$-rational. Since E is semi-stable, the action of $G_{\mathbb{Q}}$ on X is either via the trivial character or via the character χ ([39, p. 307]). In the first case, E has a $\mathbb{Q}$-rational point of order p; as the points of order 2 of E are also $\mathbb{Q}$-rational, the order of the torsion group of $E(\mathbb{Q})$ is $\geq 4p \geq 20$, which contradicts a theorem of Mazur ([28, Theorem 8]). In the second case, the curve $E' = E/X$ has a $\mathbb{Q}$-rational point of order p, and one applies the same argument as above. □

Remark. Instead of using Theorem 8 of [28], we could have employed more general results of Mazur [29].

We will now determine the *invariants* (N, k, ε) attached to ρ_p^E:

(4.1.10) As $\det \rho_p^E = \chi$, we have $\varepsilon = 1$.

(4.1.11) *We have* $k = 2$ *if* $v_p(\Delta)$ *is divisible by* p (i.e. if $v_p(ABC)$ is divisible by p), *and* $k = p + 1$ *otherwise*. This follows from Proposition 5 of Section 2.9, using the fact that E is semi-stable.

(4.1.12) *The conductor* N *of* ρ_p^E *is equal to the product of the primes* $\ell \neq p$ *such that* $v_\ell(\Delta)$ *is not divisible by* p. This is a general property of semi-stable curves, which can be checked immediately on the Tate models "$\mathbf{G}_m/q^{\mathbb{Z}}$".

Remark. Given (4.1.6), the condition "$v_\ell(\Delta)$ is not divisible by p" is equivalent to:

(4.1.13)
$$v_\ell(ABC) \not\equiv \begin{cases} 0 \pmod{p} & \text{if } \ell \neq 2 \\ 4 \pmod{p} & \text{if } \ell = 2. \end{cases}$$

4.2 Fermat's theorem

Let p be a prime number ≥ 5.

Theorem 1. *Assume (3.3.1$_?$). Then the equation*

$$a^p + b^p + c^p = 0$$

has no solution with $a, b, c \in \mathbb{Z}$ *and* $abc \neq 0$.

Proof. Let (a, b, c) be such a solution. After homothety and permutation, we may assume that a, b and c are coprime, and $b \equiv 0 \pmod{2}$, $a \equiv -1 \pmod{4}$. If we set

$$A = a^p,\ B = b^p,\ C = c^p,$$

the conditions (4.1.2) of Section 4.1 are met. Let $E = E_{A,B,C}$ be the corresponding elliptic curve, and let ρ_p^E be the representation of $G_{\mathbb{Q}}$ given by its p-torsion points. By construction, we have

$$v_\ell(ABC) \equiv 0 \pmod{p} \text{ for all primes } \ell.$$

It follows, using (4.1.11) and (4.1.13), that the invariants k and N attached to ρ_p^E are equal to 2. Moreover ρ_p^E is irreducible (Proposition 6). Conjecture ($3.3.1_?$) then says that ρ_p^E is isomorphic to the representation ρ_f attached to a normalized cusp form f of weight 2 and level 2 with coefficients in $\overline{\mathbb{F}}_p$. But such a form does not exist: the modular curve $X_0(2)$ has genus 0. Hence the theorem. □

Remark. The relationship between "solutions of the Fermat equation" and "p-torsion points on certain elliptic curves" appears already in work of Hurwitz ([20]) from 1886.

Since then, it has been used by various authors, including Hellegouarch [19], Vélu [54] and Frey [16], [17]. The method followed here is taken from Frey [17].

4.3 Variants of Fermat's theorem

Let p be a prime number ≥ 11.

Theorem 2. *Assume ($3.3.1_?$). Let L be a prime number $\neq p$ belonging to the set*

$$S = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\},$$

and let α be an integer ≥ 0. Then the equation

$$a^p + b^p + L^\alpha c^p = 0 \tag{4.3.1}$$

has no solutions with $a, b, c \in \mathbb{Z}$ and $abc \neq 0$.

Proof. We proceed as in Theorem 1. First of all, we can obviously assume that $0 < \alpha < p$. Let (a, b, c) be a solution of the equation (4.3.1), with a, b, c pairwise coprime. Let A, B, C be the three integers $a^p, b^p, L^\alpha c^p$ (which are easily seen to be pairwise coprime), rearranged so that B is even (hence divisible by 2^p and *a fortiori* by 32) and $A \equiv -1 \pmod 4$. We consider the representation ρ_p^E attached to the elliptic curve $E = E_{A,B,C}$. By (4.1.11) and (4.1.13) the invariants k and N of this representation are $k = 2$ and $N = 2L$ (note that L was assumed to be distinct from p). By ($3.3.1_?$), there is a cusp form

$$f = q + a_2(f)q^2 + \cdots + a_n(f)q^n + \ldots$$

with coefficients in $\overline{\mathbb{F}}_p$, of weight 2 and level $2L$, which is an eigenfunction of the Hecke operators, and such that the associated representation ρ_f is isomorphic to ρ_p^E. We will show that this is impossible. This is clear for $L = 3, 5$ since no such f exist in this case: the modular curves $X_0(6)$ and $X_0(10)$ have genus 0. We assume therefore that $L \geq 7$.

Lemma 1. *(a) The form f is the reduction to characteristic p of a primitive form F of level $2L$ in characteristic 0.*

(b) We have $a_3(f) = 0$ *or* ± 4.

(c) We have $a_5(f) = \pm 2$ *or* ± 6.

Proof. By (3.1.6) we have $f = \tilde{F}$, where F is a cusp form of weight 2 and level $2L$, with coefficients in $\overline{\mathbb{Z}}$, and which is a normalized eigenfunction of the Hecke operators. If F were not primitive, it would arise in level L and the representation ρ_f would be unramified at 2. But ρ_p^E is ramified at 2, since its conductor is $2L$. Part (a) follows.

To prove (b) we distinguish two cases:

(1) *The curve E has good reduction at 3, i.e. $ABC \not\equiv 0 \pmod 3$.*

Let $\tilde{E}$ be the reduction of E at 3. It is an elliptic curve over $\mathbb{F}_3$ whose points of order 2 are rational. The number of rational points of $\tilde{E}$ is therefore a multiple of 4. As this number is between $1 + 3 - 2\sqrt{3}$ and $1 + 3 + 2\sqrt{3}$, it is equal to 4. This means that the trace of the Frobenius endomorphism of $\tilde{E}$ is 0. Hence $a_3(f) = 0$ (in $\mathbb{F}_3$) by (3.1.8).

(2) *The curve E has bad reduction at 3.*

We have seen that this bad reduction is multiplicative. If it is split (i.e. if over $\mathbb{Q}_3$, E is isomorphic to a Tate curve), the $G_{\mathbb{Q}_3}$-module E_p is an extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p; the eigenvalues of the Frobenius endomorphism at 3 are then 1 and 3; their sum is 4. Hence $a_3(f) = 4$ in this case. When the reduction is not split, there is a quadratic "twist", and we get $a_3(f) = -4$.

The proof of (c) is analogous to the one of (b): we find that $a_5(f) = \pm 2$ when E has good reduction at 5, and $a_5(f) = \pm 6$ otherwise. □

Lemma 2. *Let $L \in S$ with $L \geq 7$ and let*

$$F = q + A_2 q^2 + \cdots + A_n q^n + \ldots, \qquad A_n \in \overline{\mathbb{Z}},$$

a normalized primitive form of weight 2 and level $2L$. We then have

$$A_3 = \pm 1, \pm 2 \text{ or } \pm 3 \text{ if } L \neq 23$$

and

$$A_5 = 4 \text{ if } L = 23.$$

Proof. This can be verified case-by-case:

L	7	13	17	19	29	53	59
values of A_3	-2	$1, -3$	-2	$1, -1$	$-1, -3$	$1, -1, 2, -2$	$-1, -1, 2, 2$

($L = 11$ is missing from this table since there are no primitive forms of weight 2 for level 22.) □

We can now finish the proof of Theorem 2. For $L = 23$, comparing Lemmas 1 and 2 shows that we have

$$\pm 2 \text{ or } \pm 6 \equiv 4 \pmod{p},$$

which is impossible for $p \geq 7$. Similarly, if $L \neq 23$, $L \in S$ and $L \geq 7$, we have

$$0 \text{ or } \pm 4 \equiv \pm 1, \pm 2 \text{ or } \pm 3 \pmod{p},$$

which is impossible for $p \geq 11$. □

Remarks

(1) The hypothesis $p \neq L$ is not essential; it was only used to ensure that the weight k is 2, which allowed us to apply (3.3.1$_?$). If $p = L$, we have $k = p+1$, $N = 2$, and the arguments go through if we assume the validity of (3.2.4$_?$) for $k = p + 1$ as well as for $k = 2$.

(2) It is possible that Theorem 2 remains true for $p = 5$ and $p = 7$. The question could be treated, without using conjectures, by traditional methods of factorization and descent (cf. for example Dénes [12]).

(3) The smallest value of L that does not appear in the set S of Theorem 2 is $L = 31$ (which is a Mersenne number–cf. above). For this value, the described method leads to a representation ρ_p^E that could, for instance, be isomorphic to the one attached to the following primitive form F of level 62:

$$F = q + q^2 + q^4 - 2q^5 + q^8 + \ldots$$

I do not see how to get to a contradiction from here, especially since the equation $a^5 + b^5 + 31c^5 = 0$ has indeed the solution $(1, -2, 1)$; this solution leads to the curve E of equation $y^2 = x(x+1)(x-32)$, which is a Weil curve of level 62 corresponding to F.

I also do not see how to attack the equations

$$a^p + b^p + 15c^p = 0 \quad \text{and} \quad a^p + 3b^p + 5c^p = 0,$$

for which the conductor N is 30.

(4) If we fix L, we can ask what happens for p sufficiently large. In this direction, Mazur has pointed out the following result:

Assume (3.3.1$_?$). *Let L be a prime number $\neq 2$ that is neither a Fermat number nor a Mersenne number* (i.e. L cannot be written in the form $2^n \pm 1$). *There exists a constant C_L such that, if $p \geq C_L$ and $\alpha \geq 0$, the equation*

$$a^p + b^p + L^\alpha c^p = 0$$

has no solutions with $a, b, c \in \mathbb{Z}$ and $abc \neq 0$.

The demonstration is similar to that of Theorem 2; the hypothesis on L is used to show that there is no elliptic curve of conductor $2L$ whose three points of order 2 are rational over $\mathbb{Q}$.

4.4 Discriminants of semistable elliptic curves

Conjecture ($3.3.1_?$) would allow a positive answer to questions of Brumer-Kramer ([6, Section 9]):

Proposition 7. *Assume ($3.3.1_?$). Let E be a semi-stable elliptic curve over $\mathbb{Q}$, and let Δ be the discriminant of its minimal model. Suppose that $|\Delta|$ is a p-th power. Then E has a $\mathbb{Q}$-rational subgroup of order p, and $p \leq 7$.*

Proof. For $p = 2$, we note that the extension of $\mathbb{Q}$ generated by the points of order 2 of E is unramified outside of 2; its Galois group is then neither $\mathfrak{S}_3$ nor $\mathfrak{A}_3$, and this shows that one of these points is $\mathbb{Q}$-rational. For $p = 3, 5, 7$, we use an analogous argument (cf. [6, Proposition 9.2]). It remains to show that the case $p > 7$ is impossible. If $p > 7$, the representation ρ_p^E is irreducible (Mazur [29, Theorem 4]). On the other hand, the hypotheses on E imply that the invariants (N, k, ε) of ρ_p^E are equal to $(1, 2, 1)$. According to ($3.3.1_?$), ρ_p^E would come from a normalized cusp form of weight 2 and level 1. We get a contradiction: such a form does not exist. □

Proposition 8. *Assume ($3.3.1_?$). Let E be an elliptic curve over $\mathbb{Q}$ whose conductor is a prime number P. Let $\Delta = \pm P^m$ be the discriminant of the minimal model of E. We then have $m = 1$, except if E is a Setzer-Neumann curve, or if $P = 11, 17, 19$ or 37.*

Proof. Suppose $m > 1$. Then there exists a prime number p dividing m, and we can apply Proposition 7. We conclude therefore that $p \leq 7$. If $p = 2$, E has a rational point of order 2, and it is a Setzer-Neumann curve ([33], [50]) unless P is equal to 17. If $p = 3, 5$ or 7, there exists a curve that is $\mathbb{Q}$-isogenous to E and has a rational point of order p ([39, p. 307]); according to Miyawaki [32], this is impossible for $p = 7$ and this implies that $P = 11$ for $p = 5$, and $P = 19$ or 37 for $p = 3$. □

4.5 Group schemes of type (p, p) over $\mathbb{Z}$

Let p be a prime number ≥ 3.

Theorem 3. *Assume ($3.3.1_?$). Any finite flat group scheme of type (p, p) over $\mathbb{Z}$ is then isomorphic to one of the following three:*

$$\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}, \qquad \mathbb{Z}/p\mathbb{Z} \oplus \mu_p, \quad \mu_p \oplus \mu_p.$$

Let J be a finite flat group scheme of type (p, p) over $\mathbb{Z}$. We know that J is étale over $\mathrm{Spec}(\mathbb{Z}) - \{p\}$, hence defines a representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

which is unramified outside p. As $p \neq 2$, knowing ρ determines J (Raynaud [35, Proposition 3.3.2]).

Lemma 3. *If ρ is reducible, J is isomorphic to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$ or $\mu_p \oplus \mu_p$.*

Proof. The reducibility of ρ is equivalent to the existence of an exact sequence

$$0 \longrightarrow A \longrightarrow J \longrightarrow B \longrightarrow 0,$$

where A and B are finite flat group scheme of order p over $\mathbb{Z}$. According to Oort-Tate [34], A and B are isomorphic to either $\mathbb{Z}/p\mathbb{Z}$ or μ_p. The lemma then follows from the fact that any extension of B by A is split (Fontaine [15, Section 3.4.3]). □

Lemma 4. *If ρ is irreducible, we have $\det \rho = \chi$.*

Proof. The character $\det \rho\colon G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ is unramified outside p, hence of the form χ^i, with $0 \leq i \leq p-2$. Raynaud's local results [35] (cf. Section 2.8, proof of Proposition 4) show that the only possibilities for i are $i = 0, 1$ and 2. Moreover (loc. cit.) the case $i = 0$ is only possible if J is étale at p, in which case ρ is everywhere unramified, hence $\rho = 1$ by Minkowski, contradicting the hypothesis that ρ is irreducible. Similarly, $i = 2$ is only possible if the dual of J is étale at p, leading to a contradiction by the same argument. We are left with $i = 1$, hence the lemma. □

Proof of Theorem 3. Theorem 3 now follows immediately. Indeed, if ρ is reducible, we apply Lemma 3. If ρ is irreducible, Lemma 4 together with Proposition 4 of Section 2.8 show that the invariants (N, k, ε) attached to ρ are $(1, 2, 1)$; we get a contradiction with (3.3.1$_?$) by the argument employed in the proof of Proposition 7. □

Remarks

(1) For $p = 3, 5, 7, 11, 13$ or 17, Fontaine [15] proved (without using any conjecture) a result more general than Theorem 3: any finite flat group scheme of type $(p, \ldots, p)$ over $\mathbb{Z}$ is a direct sum of copies of $\mathbb{Z}/p\mathbb{Z}$ and μ_p.

(2) Theorem 3 does not extend to the case $p = 2$: apart from $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mu_2$ and $\mu_2 \oplus \mu_2$, there is a fourth possibility, namely a certain non-split extension of $\mathbb{Z}/2\mathbb{Z} \oplus \mu_2$. The corresponding representation ρ can be written as

$$\rho = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

where $u\colon G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ is the homomorphism with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$. This group scheme of type $(2,2)$ can be obtained as the 2-torsion group of the elliptic curve

$$y^2 + xy + y = x^3 - x^2 - x - 14,$$

of conductor 17 and discriminant -17^4.

4.6 The Taniyama-Weil conjecture

Let E be an elliptic curve over $\mathbb{Q}$, let j_E be its modular invariant, and let N be its conductor.

Theorem 4. *Assume (3.3.1$_?$). Then E is a Weil curve of level N.*

(In particular, E is isomorphic to a quotient of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$.)

Proof. For any prime number p, write $\rho_p^E\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ for the representation of $G_{\mathbb{Q}}$ given by the p-torsion points of E. We have

(4.6.1) $$\det \rho_p^E = \chi.$$

Moreover:

Lemma 5. *There exists a constant C_E such that, for all $p \geq C_E$, we have:*

(4.6.2) ρ_p^E is irreducible;

(4.6.3) the conductor of ρ_p^E is N.

Proof. This is a well-known result. Indeed, according to Mazur [29], (4.6.2) holds as soon as $p > 163$. On the other hand the definition of the conductor of E in terms of ℓ-adic representations (cf. [18], [38], [49]) shows that the conductor N_p of ρ_p^E *divides* N (which is in fact sufficient for our purposes). Moreover, if $p \geq 5$, we check that $N_p = N$ if and only if p satisfies the following two conditions:

1. p does not divide N;
2. for any ℓ such that $v_\ell(N) = 1$, p does not divide $v_\ell(j_E)$.

   (Note, regarding (b), that the hypothesis $v_\ell(N) = 1$ means that E has bad multiplicative reduction at ℓ, and hence we have $v_\ell(j_E) < 0$.)

□

Let's restrict to those prime numbers $p \geq C_E$. According to (3.3.1?), ρ_p^E is isomorphic to the representation ρ_{f_p} attached to a cusp form of weight 2 and level N

$$f_p = \sum a_{n,p} q^n,$$

with coefficients in $\overline{\mathbb{F}}_p$, which is a normalized eigenform for the Hecke operators.

According to (3.1.6), f_p lifts to characteristic 0: there exists a cusp form of weight 2 and level N

$$F = \sum A_n q^n,$$

with coefficients in $\overline{\mathbb{Z}}$, which is a normalized Hecke eigenform and such that $\tilde{F} = f_p$. *A priori*, F depends on p. But there are only finitely many possible such F, since the weight and the level are fixed. We conclude that there exists a choice of F such that

$$\tilde{F} = f_p$$

for all $p \in P$, where P is an infinite set of prime numbers. Let then ℓ be a prime not dividing N. The curve E has good reduction at ℓ. Let a_ℓ be the trace of the corresponding Frobenius endomorphism. We have

$$a_\ell \equiv a_{\ell,p} \pmod{p} \qquad \text{for all } p \neq \ell.$$

It follows that the image of the algebraic integer $A_\ell - a_\ell$ in $\overline{\mathbb{F}}_p$ *is equal to* 0 *for all* $p \in P$, $p \neq \ell$. As P is infinite, this implies that

(4.6.4) $$A_\ell = a_\ell \qquad \text{for all } \ell \nmid N.$$

In particular, the A_ℓ belong to $\mathbb{Z}$. They define a *Weil curve* E_F whose level divides N; according to (4.6.2), the ℓ-adic representation attached to E and E_F are isomorphic, and it is known (Faltings [13], [14]) that this forces E and E_F to be isogenous over $\mathbb{Q}$. This proves Theorem 4. □

Remarks

(1) Theorem 4 was suggested to me by P. Colmez at the Colloquium in Luminy, in June 1986. Until then, I had not realized the full extent (both interesting and worrisome) of the consequences of the conjectures from Section 3.

(2) The form F constructed in the above proof is a *newform*; this follows from a theorem of Carayol [8].

(3) The method described here applies to other questions of the same type. Here is one example, taken from [51]:

Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field; let σ denote the involution of K. Let E be an elliptic curve over K, let E^σ be its conjugate, and let $\lambda\colon E \to E^\sigma$ be an isogeny such that $\lambda^\sigma \circ \lambda = -c$, where c is an integer > 0. Shimura asks the following question ([51, p. 184]): is it true that E comes (via the construction given in [51]) from a newform of type $(N, 2, \varepsilon)$, where N is an appropriate integer, and ε is the quadratic character attached to K? We can show that the answer is "yes" if we assume Conjecture ($3.2.4_?$). The proof is analogous to that of Theorem 4 (we work with a system of ℓ-adic representations which is rational over $\mathbb{Q}(\sqrt{-c})$, and whose determinant is the product of ε and the cyclotomic character).

For other examples, see Sections 4.7 and 4.8.

4.7 Abelian varieties with real multiplication

Let X be an abelian variety over $\mathbb{Q}$ of dimension $n \geq 1$. We say that X has *real multiplication* (cf. Ribet [36]) if the $\mathbb{Q}$-algebra $K_X = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(X)$ is a totally real number field of degree n. It is known that such varieties appear when we decompose the Jacobians $J_0(N)$ under the action of the Hecke operators, cf. Shimura [52, Section 7.5]. te Conversely:

Theorem 5. *Assume ($3.3.1_?$). Then any n-dimensional abelian variety X over $\mathbb{Q}$ with real multiplication is isomorphic to a quotient of $J_0(N)$, where N is the n-th root of the conductor of X.*

The proof is analogous to that of Theorem 4 (which we recover when $n = 1$). I will simply give a sketch. First of all:

(4.7.1) *The abelian variety X defines a "system of λ-adic representations" of $G_{\mathbb{Q}}$ of degree 2 and rational over K_X; the determinant of this system is the cyclotomic character.*

This is explained in Ribet [36].

If X has good reduction at ℓ, we write a_ℓ for the trace of the corresponding endomorphism (in the above λ-adic system); it is an integer in the field K_X.

(4.7.2) *The conductor of X is of the form N^n, with N an integer ≥ 1.*

The definition of the conductor given in [18, Exposé IX, Section 4] (see also [38, nr. 2.1]) involves certain local characters of degree $2n$, with values in $\mathbb{Q}$. We observe (as for (4.7.1) above) that these characters can be written as sums of n conjugates of characters of degree 2 with values in K_X. The claim (4.7.2) follows easily from this.

We now fix an embedding of K_X into $\overline{\mathbb{Q}}$. For any prime number p, we chose in Section 3.1 a p-adic place of $\overline{\mathbb{Q}}$, hence we get a place λ_p of K_X. If we assume that p is *totally split* in K_X, the residue field of λ_p is $\mathbb{F}_p$; by reduction $\pmod{\lambda_p}$, the corresponding λ_p-adic representation defines a representation

$$\rho_p^X : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

The representations ρ_p^X satisfy the following properties:

$$\det \rho_p^X = \chi. \tag{4.7.1}$$

This follows from (4.7.1).

(4.7.4) *If p is sufficiently large, then ρ_p^X is irreducible.*

This follows from a theorem of Faltings [14, p. 204], and can also be seen by an elementary argument, analogous to the one we will use in the next section to prove Theorem 6.

(4.7.5) *If p is sufficiently large, then the conductor of ρ_p^X is N.*

This can be verified using the properties of Néron models described in [18, Exposé X, Section 4]. (The fact that the conductor of ρ_p^X *divides* N is much easier to prove, and will suffice us.)

(4.7.6) *If p is sufficiently large, then the invariant k of ρ_p^X is* 2.

This follows from Proposition 4 of Section 2.8.

Once (4.7.3),...,(4.7.6) are established, we can apply (3.3.1$_?$). Therefore, for any sufficiently large p that is totally split in K_X, there is a cusp form of weight 2 and level N:

$$f_p = \sum a_{n,p} q^n,$$

with coefficients in $\overline{\mathbb{F}}_p$, which is a normalized eigenfunction of the Hecke operators, and such that $\rho_p^X \cong \rho_{f_p}$; in particular

$$a_{\ell,p} = \tilde{a}_\ell \qquad \text{for all } \ell \nmid N, \ell \neq p.$$

By lifting f_p to characteristic zero via (3.1.6) we obtain a cusp form of weight 2 and level N:

$$F = \sum A_n q^n,$$

with coefficients in $\overline{\mathbb{Z}}$, which is a normalized eigenfunction of the Hecke operators, and such that $\tilde{F} = f_p$ for all $p \in P$, where P is an infinite set of prime numbers that are totally split in K_X. If $\ell \nmid N$, we have then

$$\tilde{A}_\ell = a_{\ell,p} = \tilde{a}_\ell \qquad \text{for all } p \in P, p \neq \ell,$$

hence $A_\ell = a_\ell$ since P is infinite. The systems of λ-adic representations defined by X and by F are therefore isomorphic. The theorem follows from Faltings [13].

Remark. Here also, F is *primitive*, cf. Carayol [8].

4.8 Projective varieties with Betti number 2 in odd dimension

Let:

X be a smooth projective variety over $\mathbb{Q}$;

$X_\mathbb{C} = X(\mathbb{C})$ the complex manifold defined by X;

m an odd integer ≥ 1;

$H^m(X_\mathbb{C}, \mathbb{C})$ the m-th cohomology group of $X_\mathbb{C}$ with complex coefficients.

We make the following two assumptions:

(4.8.1) $\dim H^m(X_\mathbb{C}, \mathbb{C}) = 2$ (i.e. the m-th Betti number of $X_\mathbb{C}$ is 2);

(4.8.2) The Hodge decomposition of $H^m(X_\mathbb{C}, \mathbb{C})$ is of type $(m, 0) + (0, m)$.

Let us choose a finite set S of primes that is sufficiently large so that X has good reduction outside S. If $\ell \notin S$, we can define a reduction modulo ℓ of X, which is a smooth variety $\tilde{X}_\ell$ over $\mathbb{F}_\ell$. Let π_ℓ and π'_ℓ the eigenvalues of the Frobenius endomorphism of $\tilde{X}_\ell$, acting on the cohomology in degree m. According to Deligne, π_ℓ and π'_ℓ are integers in a quadratic imaginary field, and we have

$$\pi'_\ell = \overline{\pi}_\ell \quad \text{and} \quad \pi_\ell \overline{\pi}_\ell = \ell^{\cdot} \tag{4.8.1}$$

We set

$$a_\ell(X) = \pi_\ell + \overline{\pi}_\ell. \tag{4.8.2}$$

We have $a_\ell(X) \in \mathbb{Z}$ and $|a_\ell(X)| \leq 2\ell^{m/2}$.

(Note that $\tilde{X}_\ell$ is not unique in general, as opposed to the case of abelian varieties. However, any two choices of $\tilde{X}_\ell$ give the same $a_\ell(X)$, cf. [38, Section 1.2].)

Theorem 6. *Assume (3.2.4$_?$). There are then:*

(a) an integer $N \geq 1$ all of whose prime divisors belong to S,

(b) and a cusp form of type $(N, m+1, 1)$:

$$F = q + \cdots + A_n q^n + \ldots,$$

which is a normalized eigenfunction of the Hecke operators,

such that

$$A_\ell = a_\ell(X) \qquad \textit{for all } \ell \notin S. \tag{4.8.3}$$

(In other words, the $a_\ell(X)$ are the eigenvalues attached to a form of weight $m+1$ whose level only involves prime numbers in S.)

It is useful to restate Theorem 6 in terms of Galois representations.

Let $\overline{X}$ be the $\overline{\mathbb{Q}}$-variety obtained from X by extension of scalars from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$, and let $H^m_{\text{et}}(\overline{X}, \mathbb{Q}_p)$ be the m-th étale cohomology group of $\overline{X}$ with coefficients in $\mathbb{Q}_p$. We write H_p for the $\mathbb{Q}_p$-*dual* of $H^m_{\text{et}}(\overline{X}, \mathbb{Q}_p)$. The group $G_\mathbb{Q}$ acts on H_p. We obtain a p-adic representation of $G_\mathbb{Q}$ of dimension 2; its determinant is the m-th power of the cyclotomic character $G_\mathbb{Q} \to \mathbb{Z}_p^\times$. As p varies, these representations form a compatible rational system of p-adic representations, where the traces of Frobenius elements are the a_ℓ. (Note that these are the "arithmetic" Frobenius elements, rather than the "geometric" ones, which explains why we work with the dual.) Theorem 6 is equivalent to saying that *this system of representations is isomorphic to the one given by a cusp form of weight $k = m+1$.*

Proof of Theorem 6. We reuse the method employed for Theorem 4. Write T for the set of p such that either $H^m_{\text{et}}(\overline{X}, \mathbb{Z}_p)$ or $H^{m+1}_{\text{et}}(\overline{X}, \mathbb{Z}_p)$ has nonzero torsion; this T is a finite set. If $p \notin T$, we have $\dim H^m_{\text{et}}(\overline{X}, \mathbb{F}_p) = 2$; so the action of $G_{\mathbb{Q}}$ on the dual of $H^m_{\text{et}}(\overline{X}, \mathbb{F}_p)$ defines a representation

$$\rho_p \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p),$$

which is unramified outside S and p (it is a reduction modulo p of the representation of $G_{\mathbb{Q}}$ on H_p considered above; in particular, we have $\det \rho_p = \chi^m$). It is essential for what follows to know the behavior of ρ_p at p, and more precisely, its invariant k in the sense of Section 2. According to a theorem of J-M. Fontaine (proved using some of his recent results obtained in collaboration with W. Messing), we have

(4.8.6) (Fontaine–unpublished). *If p is sufficiently large, the invariant k of the representation ρ_p is $m+1$.*

(Here is where we use the hypothesis on the Hodge decomposition of $H^m(X_{\mathbb{C}}, \mathbb{C})$.)

We now consider the conductor N_p of ρ_p. It is clear that N_p is of the form

$$N_p = \prod_{\ell \in S} \ell^{n(\ell,p)} \qquad \text{with } n(\ell,p) \geq 0.$$

We have to bound the exponents $n(\ell,p)$, for fixed ℓ and varying p. Conjecture C_3 of [38] implies that $n(\ell,p)$ is *bounded* when ℓ varies (in fact, it is likely that for p sufficiently large $n(\ell,p)$ is *equal* to the exponent of the conductor defined in [38, Formula (11)].) Since C_3 has not been proved, we restrict ourselves to primes p satisfying the following congruences:

(4.8.4)
$$\begin{cases} p \not\equiv \pm 1 \pmod{2^3} & \text{if } 2 \in S, \\ p \not\equiv \pm 1 \pmod{3^2} & \text{if } 3 \in S, \\ p \not\equiv \pm 1 \pmod{\ell} & \text{for all } \ell \in S, \ell \geq 5. \end{cases}$$

We can then bound $n(\ell,p)$:

(4.8.8) *If p satisfies* (4.8.4) *and $\ell \in S$, $\ell \neq p$, we have:*

$$\begin{aligned} n(\ell,p) &\leq 9 \quad \textit{for } \ell = 2, \\ n(\ell,p) &\leq 5 \quad \textit{for } \ell = 3, \\ n(\ell,p) &\leq 2 \quad \textit{for } \ell \geq 5. \end{aligned}$$

Indeed, let $I_{\ell,p}$ be the inertia subgroup at ℓ of $\rho_p(G_{\mathbb{Q}})$. As $\det \rho_p$ is not ramified at ℓ, $I_{\ell,p}$ is contained in $\mathrm{SL}_2(\mathbb{F}_p)$, and its cardinality divides $p(p^2-1)$. If $\ell \geq 5$, hypothesis (4.8.4) implies that $I_{\ell,p}$ has cardinality coprime to ℓ; the representation ρ_p is tame at ℓ, and from Section 1.2 we have $n(\ell,p) \leq 2$. When $\ell = 3$ (resp. $\ell = 2$), the Sylow ℓ-subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$ are cyclic of order 3 (resp. quaternionic of order 8);

applying the bound on conductors in the Section 4.9 that follows, we conclude that $n(3,p) \leq 5$ (resp. $n(2,p) \leq 9$).

We denote by P the set of primes p satisfying the conditions (4.8.6) and (4.8.7). It is a infinite set.

(4.8.9) *If $p \in P$ is sufficiently large, then the representation ρ_p is irreducible.*

Let P' be the set of $p \in P$ such that ρ_p is reducible. If $p \in P'$, the semisimplification of ρ_p is given by two characters

$$\alpha, \beta \colon G_{\mathbb{Q}} \longrightarrow \overline{\mathbb{F}}_p^{\times} \qquad \text{with } \alpha\beta = \chi^m.$$

It follows from (4.8.6) that one of these characters, say α, is unramified at p. The conductor of α divides N_p and we have

$$a_\ell(X) \equiv \alpha(\ell) + \alpha(\ell)^{-1}\ell^m \pmod{p} \tag{4.8.5}$$

for all $\ell \notin S$, $\ell \neq p$.

Let $\alpha_0 \colon (\mathbb{Z}/N_p\mathbb{Z})^{\times} \to \overline{\mathbb{Z}}^{\times}$ be the multiplicative lift of α, cf. Section 3.1. According to (4.8.8), N_p has only finitely many possible values. There are therefore only finitely many possibilities for α_0. If P' were infinite, there would be an α_0 that appears for an infinite subset P'' of P'. If $\ell \notin S$, set

$$b_\ell = \alpha_0(\ell) + \alpha_0(\ell)^{-1}\ell^m.$$

By (4.8.10), $a_\ell(X)$ and b_ℓ have the same image in $\overline{\mathbb{F}}_p$ for all $p \in P''$, $p \neq \ell$. As P'' is infinite, this implies

$$a_\ell(X) = b_\ell \qquad \text{for all } \ell \notin S,$$

hence

$$\{\pi_\ell, \pi'_\ell\} = \{\alpha_0(\ell), \alpha_0(\ell)^{-1}\ell^m\},$$

which is absurd. This gives us (4.8.9).

By combining (4.8.6), (4.8.8), and (4.8.9), we can find an infinite set P_1 or prime numbers, and an integer N of the form $\prod_{\ell \in S} \ell^{n_\ell}$, such that for all $p \in P_1$ the representation ρ_p has the following properties:

(a) ρ_p is irreducible with determinant χ^m;

(b) the conductor of ρ_p is N;

(c) the invariant k of ρ_p is $m+1$.

As m is odd, (a) implies that ρ_p is absolutely irreducible if $p \in P_1$, $p \neq 2$. We can then apply (3.2.4$_?$). Hence for all $p \in P_1$, $p \neq 2$, there exists a cusp form of weight $k = m+1$ and level N:

$$f_p = \sum a_{n,p} q^n,$$

with coefficients in $\overline{\mathbb{F}}_p$, which is a normalized eigenfunction of the Hecke operators, and such that $\rho_p \cong \rho_{f_p}$. We conclude as in the proof of Theorem 4, by lifting f_p to characteristic 0, and observing that there are only finitely many possibilities. □

Remarks

(1) We find in Schoen [37] an example where conditions (4.8.1) and (4.8.2) are satisfied, with $m = \dim X = 3$, $k = 4$, $S = \{5\}$, $N = 5^2$. It is a variety X that resolves the singularities of the hypersurface in $\mathbb{P}_4$ of equation

$$X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 - 5X_0X_1X_2X_3X_4 = 0.$$

We can then find the cusp form F and prove the relation (4.8.5) without using any conjectures: it is enough to apply Faltings's method ([13, p. 362–363], see also [47]) to the 2-adic representations defined by X and by F.

(2) As was noticed by S. Bloch [5], the conclusion of Theorem 6 can also be deduced from the "archimedean" (rather than modulo p) conjectures on the L-functions attached to motives (Deligne [10]), combined with Weil's [55] characterization of modular forms. From this point of view, hypothesis (4.8.2) insures that the factor at infinity of the L-function is indeed $(2\pi)^{-s}\Gamma(s)$.

(3) If we remove hypothesis (4.8.2), the Hodge decomposition of $H^m(X_{\mathbb{C}}, \mathbb{C})$ is of type $(m - r, r) + (r, m - r)$ with $0 \leq r < m/2$. Assuming (3.2.4$_?$), we can prove the existence of a normalized cusp form

$$F = \sum A_n q^n,$$

of weight $m - 2r$, such that $a_\ell(X) = \ell^r A_\ell$ for all $\ell \notin S$: the representation of $G_{\mathbb{Q}}$ on H_p is obtained from the one attached to F via an r-th "Tate twist". The proof is essentially the same.

4.9 An upper bound on conductors

Since the question is *local*, we use the following standard notations:

K is a field complete with respect to a discrete valuation;

$v_K \colon K^\times \to \mathbb{Z}$ is the normalized valuation of K;

$\overline{K}$ is the algebraic closure of K;

$G_K = \mathrm{Gal}(\overline{K}/K)$ is the Galois group of $\overline{K}$ over K.

We assume that K is of characteristic 0, and that its residue field is perfect of characteristic $p > 0$. We denote

$$e_K = v_K(p)$$

the absolute ramification index of K.

(Beware of the change of notation: in the previous section, the residue characteristic was denoted ℓ.)

Let V be a finite-dimensional vector space over a field Ω of characteristic $\neq p$, and let $\rho \colon G_K \to \mathrm{GL}(V)$ be a continuous homomorphism. The *exponent of the conductor of* ρ is an integer $n(\rho) \geq 0$, which we define as in Section 1.2:

if $(G_i)_{i\geq 0}$ is the sequence of ramification groups of the finite group $G = \rho(G_K)$, we have

$$n(\rho) = \sum_{i\geq 0} \frac{g_i}{g_0} \dim(V/V_i), \tag{4.9.1}$$

where g_i is the cardinality of G_i, and V_i is the subspace of V fixed by G_i.

It is useful to rewrite this definition as

$$n(\rho) = \dim(V/V_0) + b(\rho), \tag{4.9.2}$$

where

$$b(\rho) = \sum_{i\geq 1} \frac{g_i}{g_0} \dim(V/V_i)$$

is the *wild invariant* of ρ ([44, Section 19.3]).

The upper bound we are aiming for is the following:

Proposition 9. *Let p^c be the cardinality of the wild inertia group G_1, and let N be the dimension of V over Ω. We have*

$$b(\rho) \leq N e_K \left(c + \frac{1}{p-1}\right). \tag{4.9.3}$$

Moreover, if G_1 is not cyclic, this inequality is strict.

Given (4.9.2), this implies:

Corollary 1. *We have*

$$n(\rho) \leq N(1 + e_K c + e_K/(p-1)), \tag{4.9.4}$$

where the inequality is strict if G_1 is not cyclic.

Proof of Proposition 9. Let I be the largest index $i \geq 1$ such that $G_i \neq \{1\}$. We bound $\dim V/V_i$ above by N if $i \leq I$, and by 0 if $i > I$. Hence

$$b(\rho) \leq \frac{N}{g_0}(g_1 + \cdots + g_I) \leq \frac{N}{g_0}\left(I + \sum_{i\geq 1}(g_i - 1)\right). \tag{4.9.5}$$

By an elementary result on ramification groups ([45, p. 79, Exercise 3]), we have:

$$I \leq g_0 e_K/(p-1), \tag{4.9.6}$$

where the inequality is strict if G_1 is not cyclic.

On the other hand, the integer

$$d = \sum_{i\geq 0}(g_i - 1)$$

equals the valuation of the different of the extension L/K of Galois group G ([45, p. 72]). By a bound due to Hensel (reproduced in [45, p. 67]), we have

$$d \leq g_0 - 1 + g_0 e_K c,$$

hence

$$\sum_{i \geq 1} (g_i - 1) \leq g_0 e_K c. \tag{4.9.7}$$

By combining (4.9.5), (4.9.6), and (4.9.7), we obtain the desired inequality (4.9.3), and we see that this inequality is strict if G_1 is not cyclic. □

Remark. When G_1 is *abelian* of exponent p^h, we can prove that

$$b(\rho) \leq N e_K \left(h + \frac{1}{p-1} \right).$$

As $h \leq c$, this improves (4.9.3).

Application to (4.8.8). In the situation of (4.8.8), there are two cases to consider:

(a) *Residue characteristic* 3. With the notation in Proposition 9 (which differ from those in Section 4.8, as already mentioned), we have $p = 3$, $N = 2$, $e_K = 1$ and $c \leq 1$, hence $n(\rho) \leq 5$ by (4.9.4). This bound is optimal: there are elliptic curves of conductor 3^5.

(b) *Residue characteristic* 2. We have $p = 2$, $N = 2$, $e_K = 1$, and $c \leq 3$, with G_1 cyclic if $c = 3$; hence $n(\rho) \leq 9$ according to (4.9.4). In fact, a more detailed analysis shows that $n(\rho) \leq 8$, which is optimal: there are elliptic curves of conductor 2^8.

5 Examples

This section gathers a number of examples for which we can verify, at least partly, the conjectures of Section 3. Most of the verifications required the use of a computer; these were programmed and done by J-F. Mestre.

The considered values of p are:

- $p = 2$ (sections 5.1 and 5.2),
- $p = 3$ (sections 5.3 and 5.4),
- $p = 7$ (section 5.5).

5.1 Examples coming from $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$

Let K be a nonabelian cubic field and let K^{gal} be its Galois closure. The group $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$ is isomorphic to the symmetric group $\mathfrak{S}_3$, which is in turn isomorphic to $\mathrm{GL}_2(\mathbb{F}_2)$. We obtain a representation

$$\rho^K : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_2),$$

which is absolutely irreducible, and to which we can apply the conjectures of Section 3.

The invariants (N, k, ε) of ρ^K are easy to determine. If we write the discriminant D of the field K as

$$D = \pm 2^m N, \text{ with } N \text{ odd} > 0, \text{ and } m = 0, 2 \text{ or } 3,$$

we observe that

- the conductor of ρ^K is N;
- the character ε is 1;
- the weight k of ρ^K is 2 (respectively 4) if $m = 0, 2$ (respectively if $m = 3$).

Conjecture (3.2.4$_?$) predicts the existence of a cusp form f with coefficients in $\mathbb{F}_2$ (or in $\mathbb{F}_4$ if $m = 0$, i.e., if K is unramified at 2), of type $(N, k, 1)$, which is a normalized eigenvector for the Hecke operators, and such that ρ^K is isomorphic to ρ_f. The following table lists the cases where this was verified by computer:

$D < 0$	$k =$ weight	$N =$ level
-23	2	23
-31	2	31
-44	2	11
-59	2	59
-76	2	19
-104	4	13

$D > 0$	$k =$ weight	$N =$ level
148	2	37
229	2	229
257	2	257
316	2	79

(In the cases $D = -23$, $D = -31$ and $D = 257$, the ideal (2) is inert in K, and the eigenvalue of U_2 is a primitive root of 1, i.e., an element of $\mathbb{F}_4 - \mathbb{F}_2$, according to (3.2.6$_?$). For the other values of D, the eigenvalue of U_2 is 0 or 1, and all the coefficients of f are in $\mathbb{F}_2$.)

In the general case, I only know how to prove a result that is weaker than (3.2.4$_?$):

Proposition 10. *There exists a form f of type $(N, k', 1)$, for a suitable k', such that ρ^K is isomorphic to ρ_f.*

(In particular, ρ^K satisfies (3.2.3?).)

Proof. We use the obvious embedding $\mathfrak{S}_3 \to \mathrm{GL}_2(\mathbb{Z})$, which gives a representation

$$\rho_0^K : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C}),$$

which "lifts" ρ_K to characteristic 0. The determinant of ρ_0^K is the quadratic character

$$\varepsilon_D : G_{\mathbb{Q}} \longrightarrow \mathfrak{S}_3 \xrightarrow{\text{sgn}} \{\pm 1\}$$

which corresponds to the field $\mathbb{Q}(\sqrt{D})$. We then distinguish two cases:

(i) $D < 0$, *i.e.,* K *is a cubic imaginary field.*

The character $\varepsilon_D = \det \rho_0^K$ is then *odd.* As the image of ρ_0^K is $\mathfrak{S}_3$, which is a dihedral group, we conclude (cf. [11],]cite45) that ρ_0^K is the representation attached to a cusp form F_1 of weight 1, character ε_D and level $|D|$; we can even write F explicitly in terms of theta functions of binary quadratic forms of discriminant D. Let E_D be the Eisenstein series of weight 1 and character ε_D (which is also a theta function). The product $F = F_1 \cdot E_D$ is a cusp form of weight 2, character 1 and level $|D|$. If $f = \tilde{F}$ is the mod 2 reduction of F, we have $f = \tilde{F}_1$, since $\tilde{E}_D = 1$. The form f is then the desired form; indeed, by construction f is of type $(2^m N, 2, 1)$, hence also of type $(N, k', 1)$ for a suitable k'.

(It should be possible to make this proof more precise and obtain the exact value of k'. I have only done this for $m = 0$, i.e., $D = -N$, where one obtains $k' = 2$, as expected.)

(ii) $D > 0$, *i.e.,* K *is a totally real cubic field.*

The field $\mathbb{Q}(\sqrt{D})$ is then a real quadratic field, and the representation ρ_0^K is induced by a character ψ of order 3 of $\mathbb{Q}(\sqrt{D})$. Choose an auxiliary character α of $\mathbb{Q}(\sqrt{D})$ with the following properties:

(11_1) the order of α is a power of 2;

(22_2) α has signatures $+$ and $-$ at the two infinite places of $\mathbb{Q}(\sqrt{D})$;

(33_3) α is unramified at every finite place of $\mathbb{Q}(\sqrt{D})$ of residual characteristic $\neq 2$.'

(The existence of such a character is easy to prove.)

Let $\rho_0' = \mathrm{Ind}(\psi\alpha)$ be the representation of $G_{\mathbb{Q}}$ *induced* by the character $\psi\alpha$ of the field $\mathbb{Q}(\sqrt{D})$. According to (ii_1), its reduction in characteristic 2 is isomorphic to $\mathrm{Ind}(\psi) \cong \rho^K$. According to ($\mathrm{ii}_2$), its determinant is odd, and from (ii_3) we know that its conductor is of the form $2^M N$, with M an integer. We can then apply to ρ_0' the argument used in case (i) for ρ_0^K: this representation is associated with a cusp form F' of weight 1 and level $2^M N$; by reduction to characteristic 2, F' gives the desired form f. (Note that here F' is a linear combination of theta functions of indefinite binary forms.)

Remark. The same kind of argument applies to any representation

$$\rho_p\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p), \qquad p \neq 2,$$

of odd determinant, and such that the image of $\rho_p(G_{\mathbb{Q}})$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is a *dihedral* group; in particular,the weak conjecture (3.2.3$_?$) holds for such a representation.

□

5.2 Examples coming from $\mathrm{SL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$

Let K be a degree 5 field extension of $\mathbb{Q}$ whose Galois closure K^{gal} has Galois group the alternating group $\mathfrak{A}_5$. As $\mathfrak{A}_5$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_4)$, we get a surjective homomorphism $G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{F}_4)$, hence an absolutely irreducible representation

$$\rho^K\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_4)$$

with $\det \rho^K = 1$.

Once again, we wish to verify the conjectures of Section 3 for ρ^K. As the conductor N of ρ^K is often very large, the computations are only practical if N is a prime number, and if the weight k is 2, as this allows us to apply the "graph method" ([30], [31]). The following table indicates the different cases studied by Mestre; we wrote D for the square root of the discriminant of K, with sign $+$ if K is real and sign $-$ if K is imaginary.

$D < 0$	$N =$ level
-2083	2083
-2707	2707
-3203	3203
-3547	3547
-4027	4027

$D > 0$	$N =$ level
$2^3 887$	887
8311	8311
$2^2 8447$	8447
13613	13613
$2^2 24077$	24077

The examples with $D < 0$ are extracted from a table of J. Buhler [7, pp. 136–141]; those with $D > 0$ come from [31, Section 4.2].

Remarks

(1) In each of the cases considered, Mestre obtains a cusp form f with coefficients in $\mathbb{F}_4$ (or, sometimes, in $\mathbb{F}_{16}$), of the desired type $(N, 2, 1)$, which is an eigenform of the Hecke operators U_2, T_3, $T_5, \ldots$, whose eigenvalues for the first three operators are the correct ones. It is therefore likely that the representation ρ_f attached to f is isomorphic to ρ^K; however, a complete proof would require considerable work, which has not been done.

(2) The case $D < 0$ is not very surprising. Indeed, the representation ρ^K can be lifted to characteristic 0, its image then being a certain central extension of $\mathfrak{A}_5$ by a cyclic group of order a power of 2 (use an embedding of $\mathfrak{A}_5$ into $\mathrm{PGL}_2(\mathbb{C})$ and apply the results of Tate appearing in [43, Section 6]). If $D < 0$, this representation has odd determinant, and therefore comes from a cusp form F of weight 1 (if we assume the validity of Artin's conjecture for L-functions). By reducing F to characteristic 2, we obtain a form f such that $\rho_f \cong \rho^K$ (cf. the proof of Proposition 10), which shows that ρ^K satisfies the weak conjecture (3.2.3$_?$).

The case $D > 0$ is more surprising: we don't see *a priori* any way of attaching ρ^K to any modular form whatsoever.

5.3 Examples coming from $\mathrm{GL}_2(\mathbb{F}_3) \cong \tilde{\mathfrak{S}}_4$

The group $\mathrm{PGL}_2(\mathbb{F}_3)$ acts on the projective line $\mathbb{P}_1(\mathbb{F}_3)$, which has 4 points, and this defines an isomorphism $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$. As the kernel of $\mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{PGL}_2(\mathbb{F}_3)$ is $\{\pm 1\}$, we conclude that $\mathrm{GL}_2(\mathbb{F}_3)$ is a central extension of degree 2 of $\mathfrak{S}_4$; in fact, it is the extension denoted $\tilde{\mathfrak{S}}_4$ in [46, Section 1.5].

It is well-known that $\tilde{\mathfrak{S}}_4$ can be embedded into $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}])$, and this embedding gives, via reduction modulo 3, the above isomorphism $\tilde{\mathfrak{S}}_4 \cong \mathrm{GL}_2(\mathbb{F}_3)$. This allows us to associate to any representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$$

its *lift* to characteristic 0

$$\rho_0\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \subset \mathrm{GL}_2(\mathbb{C}).$$

Suppose that ρ satisfies the conditions of Section 3.2, i.e., that it is irreducible with odd determinant. Then so does ρ_0, and we can apply the results of Langlands [26] and Tunnell [53]. We conclude that ρ_0 comes from a cusp form of weight 1 and level equal to the conductor of ρ_0, which we can write as $3^m N_0$, where N_0 is coprime to 3. Therefore, as in Section 5.1, we obtain:

Proposition 11. *There exists a form f of type (N_0, k', ε), for a suitable k', such that ρ is isomorphic to ρ_f.*

(Here, ε is the character $G_{\mathbb{Q}} \to \{\pm 1\}$ constructed from $\det \rho$ as explained in Section 1.3.)

In particular ρ *satisfies the weak conjecture* (3.2.3$_?$).

Remark. The conductor $3^m N_0$ of ρ_0 is closely related to the conductor N of ρ defined in Section 1. If we put

$$N = \prod_{\ell \neq 3} \ell^{n(\ell)} \qquad \text{and} \qquad N_0 = \prod_{\ell \neq 3} \ell^{n_0(\ell)},$$

we observe indeed that:

(5.3.1) If the inertia group at ℓ of $\rho(G_{\mathbb{Q}}) \cong \rho_0(G_{\mathbb{Q}})$ is cyclic of order 3, we have $n(\ell) = 1$ and $n_0(\ell) = 2$.

(5.3.2) In all other cases, we have $n(\ell) = n_0(\ell)$.

In particular, N *divides* N_0, and the prime factors of N and N_0 are the same. The conjecture (3.2.4$_?$) then states (among other things) that the level N_0 from Proposition 11 can be lowered to N. Here are some examples where this level lowering does indeed occur:

Examples coming from elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$. Suppose there is a prime number $\ell > 3$ at which E has bad reduction of type c_3 or c_6 in the sense of Néron (types IV or IV* of Kodaira). With the notations of [39, Section 5.6], this is equivalent to saying that E has potentially good reduction at ℓ, and that the corresponding group Φ_ℓ is cyclic of order 3. Let ρ be the representation

$$\rho^E\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$$

defined by the 3-torsion points of E. According to (5.3.1), the exponent of ℓ in N (respectively N_0) is 1 (respectively 2). We should therefore witness a lowering. Indeed:

Example (Example (5.3.3)). *The curve* 121_F (cf. [4, p. 97]). The equation of E is

$$y^2 + xy = x^3 + x^2 - 2x - 7.$$

It has good reduction outside of $\ell = 11$, and bad reduction of type c_3 at 11, hence $N_0 = 11^2$ and $N = 11$. Moreover, the representation ρ^E is irreducible. Conjecture (3.2.4$_?$) predicts that ρ^E comes from a form of weight 2 and level 11. But there is only one such form (up to multiplication by a scalar): the one corresponding to the curve E' of conductor 11 and equation

$$y^2 + y = x^3 - x^2.$$

We conclude that the representations ρ^E and $\rho^{E'}$ must be isomorphic, so that the traces a_ℓ and a'_ℓ of their Frobenius endomorphisms must satisfy:

$$a_\ell \equiv a'_\ell \pmod 3 \qquad \text{for all } \ell \neq 3, 11.$$

The following table (taken from [4, pp. 117–119]) shows that this is indeed the case, at least for $\ell < 50$:

ℓ	2	5	7	13	17	19	23	29	31	37	41	43	47
a_ℓ	1	1	−2	1	−5	6	2	9	−2	−3	−5	0	2
a'_ℓ	−2	1	−2	4	−2	0	−1	0	7	3	−8	−6	8

Example (Example (5.3.4)). *The curve* 147_I (cf. [4, p. 103]). The equation of E is

$$y^2 + y = x^3 + x^2 - 114x + 473.$$

Its conductor is $147 = 3 \cdot 7^2$. It has multiplicative bad reduction at 3, and bad reduction of type c_6 at 7, hence $N_0 = 7^2$, $N = 7$. The representation ρ^E has conductor 7; as it is très ramifiée at 3, its weight k is 4. The conjecture ($3.2.4_?$) predicts that ρ^E comes from a cusp form of weight 4 and level 7. Once again, there is a unique such form (up to normalization):

$$\begin{aligned} F &= q + \sum_{n \geq 2} A_n q^n \\ &= q - q^2 - 2q^3 - 7q^4 + 16q^5 + 2q^6 - 7q^7 + 15q^8 + \dots. \end{aligned}$$

(See below for the computation of the coefficients of F.)

If a_ℓ denotes the trace of the Frobenius endomorphism of E at ℓ, we must then have

$$a_\ell \equiv A_\ell \pmod 3 \qquad \text{for all } \ell \neq 3, 7.$$

This is indeed the case, at least for $\ell < 50$:

ℓ	2	5	11	13	17	19	23	29	31	37	41	43	47
a_ℓ	2	−2	−2	1	0	1	0	4	9	3	−10	5	−6
A_ℓ	−1	16	−8	28	54	−110	48	−110	12	−246	182	128	324

Computation of F. Let L be the ring of integers of the field $\mathbb{Q}(\sqrt{-7})$. The series

$$f_1 = \sum_{z \in L} q^{z\bar{z}} = 1 + 2q + 4q^2 + 6q^4 + 2q^7 + \dots$$

$$f_2 = \frac{1}{2} \sum_{z \in L} z^2 q^{z\bar{z}} = q - 3q^2 + 5q^4 - 7q^7 - 3q^8 + \dots$$

are the modular forms of weights 1 and 3 respectively, of level 7 and character the Legendre character mod 7. Their product $f_1 \cdot f_2$ is the form F considered above; whence the computation of the coefficients of F.

5.4 Examples coming from $\mathrm{SL}_2(\mathbb{F}_9) \cong \tilde{\mathfrak{A}}_6$

Let G be the subgroup of $\mathrm{GL}_2(\mathbb{F}_9)$ formed by the elements of determinant ± 1. We have

$$G = \{\pm 1, \pm i\} \cdot \mathrm{SL}_2(\mathbb{F}_9) = \mathrm{SL}_2(\mathbb{F}_9) \cup i \cdot \mathrm{SL}_2(\mathbb{F}_9),$$

where i denotes an element of order 4 in $\mathbb{F}_9^\times$. The image of this group in $\mathrm{PGL}_2(\mathbb{F}_9)$ is $\mathrm{PSL}_2(\mathbb{F}_9)$, which is isomorphic to the alternating group $\mathfrak{A}_6$. We thus have a projection

$\varphi\colon G \to \mathfrak{A}_6$. The pair $(\varphi, \det)$ defines a surjective homomorphism $G \to \mathfrak{A}_6 \times \{\pm 1\}$, with kernel $\{\pm 1\}$. We thus have an exact sequence:

(5.4.1) $$\{1\} \longrightarrow \{\pm 1\} \longrightarrow G \longrightarrow \mathfrak{A}_6 \times \{\pm 1\} \longrightarrow \{1\}.$$

Let us know take a field K of degree 6 over $\mathbb{Q}$, with $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q}) \cong \mathfrak{A}_6$, as well as a quadratic field $\mathbb{Q}(\sqrt{D})$. We get homomorphisms

$$\alpha^K\colon G_{\mathbb{Q}} \longrightarrow \mathfrak{A}_6 \qquad \text{and} \qquad \epsilon_D\colon G_{\mathbb{Q}} \longrightarrow \{\pm 1\},$$

whence

$$\alpha\colon G_{\mathbb{Q}} \longrightarrow \mathfrak{A}_6 \times \{\pm 1\}.$$

Let us try to *lift* α to a homomorphism

$$\rho\colon G_{\mathbb{Q}} \longrightarrow G.$$

Given (5.4.1), there is an *obstruction* to this lifting, namely a cohomology class

$$\mathrm{obs}(\alpha) \in \mathrm{H}^2(G_{\mathbb{Q}}, \{\pm 1\}) \cong \mathrm{Br}_2(\mathbb{Q}),$$

cf. [46, Section 1.1]. The following lemma gives a way of computing this class:

Lemma 6. *Let $w \in \mathrm{Br}_2(\mathbb{Q})$ be the Witt invariant of the quadratic form $\mathrm{Tr}_{K/\mathbb{Q}}(x^2)$, cf. [46]. We have:*

(5.4.2) $$\mathrm{obs}(\alpha) = w + (-1)(D).$$

(Recall, *loc. cit.*, that $(-1)(D)$ is the element of $\mathrm{Br}_2(\mathbb{Q})$ that corresponds to the quaternion algebra $(-1, D)$.)

Proof. According to Theorem 1 of [46], w is the obstruction to lifting

$$\alpha^K\colon G_{\mathbb{Q}} \longrightarrow \mathfrak{A}_6 \cong \mathrm{PSL}_2(\mathbb{F}_9)$$

to a homomorphism

$$G_{\mathbb{Q}} \longrightarrow \tilde{\mathfrak{A}}_6 \cong \mathrm{SL}_2(\mathbb{F}_9).$$

On the other hand, $(-1)(D)$ is the obstruction to lifting

$$\varepsilon_D\colon G_{\mathbb{Q}} \longrightarrow \{\pm 1\}$$

to a homomorphism

$$G_{\mathbb{Q}} \longrightarrow \{\pm 1, \pm i\}.$$

The lemma follows from these two facts, via an easy argument. □

Let us now make particular choices for K and D. We will take:

- $D = -3$;
- K = the sextic field defined by an equation

$$X^6 + aX + b = 0, \qquad a, b \in \mathbb{Z},$$

  the pair (a, b) being chosen such that the equation is irreducible with Galois group $\mathfrak{A}_6$.

[Here are some possible choices of a and b, obtained by Mestre: $(a, b) = (24, -20)$; $(30, 25)$; $(240, 400)$; $(240, -400)$; $(48, -80)$; $(432, 720)$; $(480, -400)$.]

According to [46, Section 3.3], the fact that K is defined by such an equation implies that

$$w = (3)(-1) + (-1)(-1) = (-1)(-3),$$

whence

$$\mathrm{obs}(\alpha) = 0$$

by Lemma 6. We can therefore lift α to a homomorphism

$$\rho\colon G_{\mathbb{Q}} \longrightarrow G \subset \mathrm{GL}_2(\mathbb{F}_9).$$

Of course, the representation ρ thus obtained is not unique; it is only defined up to quadratic twist. As in Tate's theory (described in [43, Section 6]), we can use this twisting to make the invariants k and N of ρ as small as possible; in particular, we can choose ρ in such a way that $k = 2$ or 4, and that N is only divisible by those prime factors of the discriminant d which are not equal to 3 (i.e., $\ell = 2$ and 5 in the examples given above). Then the conjectures of Section 3 claim the existence of a cusp form $f = \sum a_n q^n$ of type $(N, k, 1)$, with coefficients in $\mathbb{F}_9$, which is a normalized eigenfunction of the Hecke operators, and such that $\rho \cong \rho_f$. The latter relation implies a strong link between the coefficients a_ℓ (for $\ell \nmid 3N$) and the decomposition of ℓ in the field K. More precisely, let $\mathrm{ord}(\ell)$ denote the *order* of the Frobenius element attached to ℓ in $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q}) \cong \mathfrak{A}_6$. We must have:

$$\begin{aligned} \mathrm{ord}(\ell) = 1 \text{ or } 3 &\Leftrightarrow a_\ell^2 = \left(\frac{\ell}{3}\right); \\ \mathrm{ord}(\ell) = 2 &\Leftrightarrow a_\ell = 0; \\ \mathrm{ord}(\ell) = 4 &\Leftrightarrow a_\ell^2 = -\left(\frac{\ell}{3}\right); \\ \mathrm{ord}(\ell) = 5 &\Leftrightarrow a_\ell^2 = -1. \end{aligned}$$

(Recall that the coefficients a_ℓ are elements of the field $\mathbb{F}_9$.)

In particular, if $\ell \neq 3$ does not divide the discriminant of $X^6 + aX + b$, the *number of solutions in* $\mathbb{F}_\ell$ of the congruence

$$x^6 + ax + b \equiv 0 \pmod{\ell}$$

must be 1 (respectively 2) if and only if a_ℓ is an element of order 8 of $\mathbb{F}_9^\times$ (respectively if $a_\ell = 0$).

The search for such a form f was done by J-F. Mestre in each of the cases $(a, b) = (24, -20), \ldots, (480, -400)$ given above, as well as a few others. The conductor N is then equal to $2^m 5^n$, where m and n depend on (a, b). Determining n is not hard: if the ramification is wild at 5 (which is the case in the examples), n is the exponent of 5 in $d^{1/2}$. On the other hand, determining m is a dyadic exercise that I have not performed; this forced Mestre to try the different possible levels: $2 \cdot 5^n$, $2^2 5^n$, $2^3 5^n, \ldots$, until he found a level with a form f of the desired type. His results are summarized in the following table:

a	b	$d^{1/2}$	$k =$ weight	level
24	-20	$2^3 3^3 5^3$	2	$2^3 5^3 = 1000$
30	25	$2^3 3^3 5^4$	2	≥ 20000?
240	400	$2^2 3^3 5^4$	2	$2^2 5^4 = 2500$
240	-400	$2^3 3^3 5^4$	2	$2^3 5^4 = 5000$
48	-80	$2^3 3^3 5^3$	2	$2^3 5^3 = 1000$
432	720	$2^2 3^5 5^3$	4	$2^2 5^3 = 500$
480	-400	$2^3 3^2 5^4$	2	$2^3 5^4 = 5000$

Note the case $a = 30$, $b = 25$, where no level ≤ 10000 works: it seems that the conductor N is of the form $2^m 5^4$, with $m \geq 5$, hence $N \geq 20000$, which is too big for the method employed (based on the Eichler-Selberg trace formula). In all the other cases, we find indeed a cusp form with the desired properties, as least for ℓ sufficiently small.

5.5 An example using the simple group $\mathrm{PSL}_2(\mathbb{F}_7)$ of order 168

The degree 7 extension of $\mathbb{Q}$ defined by the equation

(5.5.1) $$X^7 - 7X + 3 = 0$$

has Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$ (W. Trinks–cf. [25]). We will use it to construct a representation of $G_\mathbb{Q}$ in characteristic 7. The method is analogous to that of the previous section:

Let G be the subgroup of $\mathrm{GL}_2(\mathbb{F}_{49})$ defined by:

$$G = \{\pm 1, \pm i\} \cdot \mathrm{SL}_2(\mathbb{F}_7) = \mathrm{SL}_2(\mathbb{F}_7) \cup i \cdot \mathrm{SL}_2(\mathbb{F}_7),$$

where i is an element of order 4 of $\mathbb{F}_{49}^\times$. We have $\det G = \{\pm 1\}$, and the image of G in $\mathrm{PGL}_2(\mathbb{F}_{49})$ is $\mathrm{PGL}_2(\mathbb{F}_7)$. We get the exact sequence:

$$(*) \qquad \{1\} \longrightarrow \{\pm 1\} \longrightarrow G \longrightarrow \mathrm{PSL}_2(\mathbb{F}_7) \times \{\pm 1\} \longrightarrow \{1\}.$$

Let K be the field of degree 7 defined by (5.5.1), and let $\alpha^K: G_{\mathbb{Q}} \to \mathrm{PSL}_2(\mathbb{F}_7)$ be the corresponding homomorphism. On the other hand, let

$$\varepsilon\colon G_{\mathbb{Q}} \longrightarrow \{\pm 1\}$$

be the quadratic character associated with the field $\mathbb{Q}(\sqrt{-3})$. The pair (α^K, ε) defines a homomorphism

$$\alpha\colon G_{\mathbb{Q}} \longrightarrow \mathrm{PSL}_2(\mathbb{F}_7) \times \{\pm 1\}.$$

Let $\mathrm{obs}(\alpha) \in \mathrm{Br}_2(\mathbb{Q})$ be the obstruction to lifting α to a homomorphism

$$\rho\colon G_{\mathbb{Q}} \longrightarrow G \subset \mathrm{GL}_2(\mathbb{F}_{49}).$$

A calculation analogous to that of Lemma 6 shows that

$$\mathrm{obs}(\alpha) = w + (-1)(-3),$$

where w is the Witt invariant of the quadratic form $\mathrm{Tr}_{K/\mathbb{Q}}(x^2)$. According to [46, Section 3.3], we have $w = (-1)(-3)$, hence $\mathrm{obs}(\alpha) = 0$. This proves the existence of the representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_{49})$$

we are looking for. By construction, we have $\det \rho = \varepsilon$.

Once again, we choose ρ so that its conductor is as small as possible. The discriminant of the polynomial $X^7 - 7X + 3$ is $3^8\, 7^8$ and that of the field K is $3^6\, 7^8$. It follows that the conductor of ρ can be chosen to be 3^n, and a ramification calculation shows that $n = 3$. On the other hand, the study of the ramification at 7 shows that the action of the inertia at 7 is:

$$\text{either } \begin{pmatrix} \chi & * \\ 0 & \chi^{-1} \end{pmatrix}, \qquad \text{either } \begin{pmatrix} \chi^4 & * \\ 9 & \chi^{-4} \end{pmatrix},$$

where χ is the cyclotomic character.

After tensoring ρ by χ, or by χ^4, we get a new representation ρ' where the action of inertia at 7 is given by:

$$\begin{pmatrix} \chi^2 & * \\ 0 & 1 \end{pmatrix},$$

which leads to a weight k equal to 3, cf. Sections 2.3 and 2.4. We have

$$\det \rho' = \varepsilon \cdot \chi^2.$$

[Note that ρ' takes values in a group that is a little bigger than G: we have

$$\mathrm{Im}\, \rho' = \mathrm{GL}_2(\mathbb{F}_7) \cup i \cdot \mathrm{GL}_2(\mathbb{F}_7).]$$

The conjectures of Section 3 state that ρ' is of the form ρ_f, where $f = \sum a_n q^n$ is a cusp form of type $(3^3, 3, \varepsilon)$, with coefficients in $\mathbb{F}_{49}$, and which is a normalized eigenfunction for the Hecke operators. The link between the eigenvalues a_ℓ ($\ell \neq 3, 7$) and the decomposition of ℓ in K is the following:

if we write $\mathrm{ord}(\ell)$ for the *order* of the Frobenius automorphism attached to ℓ in $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{F}_7)$, we must have:

$$\begin{array}{llllll} \mathrm{ord}(\ell) = 1 \text{ or } 7 & \Leftrightarrow & a_\ell^2 & = & 4\ell^2\varepsilon(\ell) & \text{in } \mathbb{F}_7 \\ \mathrm{ord}(\ell) = 2 & \Leftrightarrow & a_\ell & = & 0 & \text{in } \mathbb{F}_7 \\ \mathrm{ord}(\ell) = 3 & \Leftrightarrow & a_\ell^2 & = & \ell^2\varepsilon(\ell) & \text{in } \mathbb{F}_7 \\ \mathrm{ord}(\ell) = 4 & \Leftrightarrow & a_\ell^2 & = & 2\ell^2\varepsilon(\ell) & \text{in } \mathbb{F}_7 \end{array}$$

with $\varepsilon(\ell) = \left(\dfrac{\ell}{3}\right)$.

Indeed, we can find a form f with these properties, at least for ℓ small enough. It is the reduction (mod 7) of a newform F in characteristic 0:

$$\begin{aligned} F &= q + \sum_{n\geq 2} A_n q^n \\ &= 9 + 3iq^2 - 5q^4 - 3iq^5 + 5q^7 - 3iq^8 + \dots \end{aligned}$$

This form has coefficients in $\mathbb{Z}[i]$. It can be computed easily, cf. above. The following table gives the values of $\mathrm{ord}(\ell)$ and A_ℓ for $\ell \leq 37$:

ℓ	2	5	11	13	17	19	23	29	31	37
$\mathrm{ord}(\ell)$	7	7	7	4	3	3	3	7	7	4
A_ℓ	$3i$	$-3i$	$-15i$	-10	$18i$	-16	$-12i$	$30i$	-1	20

(For example, for $\ell = 17$, we have $a_\ell^2 \equiv A_\ell^2 \equiv -2 \pmod 7$, $\varepsilon(\ell) = -1$, $\ell^2 \equiv 2 \pmod 7$, hence $a_\ell^2 = \ell^2\varepsilon(\ell)$ in $\mathbb{F}_7$, in accordance with the fact that $\mathrm{ord}(\ell) = 3$.)

Calculation of F. Let θ_1 be the theta function associated with the field $\mathbb{Q}(\sqrt{-3})$:

$$\theta_1 = \sum_{x,y\in\mathbb{Z}} q^{x^2+xy+y^2} = 1 + 6\left(q + q^3 + q^4 + 2q^7 + q^9 + \dots\right).$$

It is an Eisenstein series of weight 1, level 3 and character ε. If we set

$$\begin{aligned} \theta_2 &= \theta_1(3z) = 1 + 6\left(q^3 + q^9 + q^{12} + \dots\right) \\ \theta_3 &= \theta_1(9z) = 1 + 6\left(q^9 + q^{27} + q^{36} + \dots\right), \end{aligned}$$

we obtain forms of levels 3^2 and 3^3.

On the other hand, the series

$$g = q\prod_{n\geq 1}\left(1 - q^{3n}\right)^2\left(1 - q^{9n}\right)^2 = q - 2q^4 - q^7 + 5q^{13} + \dots$$

is the unique normalized cusp form of weight 2, level 3^3 and trivial character (it corresponds to the elliptic curve $y^2 + y = x^3 - 3$, of conductor 3^3).

The products $g\theta_1$, $g\theta_2$ and $g\theta_3$ are forms of weight 3, level 3^3 and character ε. They form a *basis* for the space of cusp forms of type $(3^3, 3, \varepsilon)$. The normalized eigenfunctions for the Hecke operators can be obtained, for instance, by diagonalizing the operator T_2. We find:

$$F = \frac{1}{2} i g\theta_1 - \frac{1}{2}(1+i) g\theta_2 + \frac{3}{2} g\theta_3 = q + 3iq^2 - 5q^4 + \dots,$$
$$\overline{F} = -\frac{1}{2} i g\theta_1 - \frac{1}{2}(1-i) g\theta_2 + \frac{3}{2} g\theta_3 = q - 3iq^2 - 5q^4 + \dots,$$
$$G = g\theta_2 = q + 4q^4 - 13q^7 + \dots$$

The series G is of (CM) type: it corresponds to a Hecke character for the field $\mathbb{Q}(\sqrt{-3})$.

The series F is the cusp form we are looking for.

References

[1] E. Artin. Zur Theorie der l-Reihen mit allgemeinen Gruppencharakteren. *Hamb. Abh.*, 8:292–306, 1930.

[2] A. Ash and G. Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.*, 365:192–220, 1986.

[3] A. O. L. Atkin and W. Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[4] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV.* Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin, 1975.

[5] S. Bloch. Algebraic cycles and values of L-functions. II. *Duke Math. J.*, 52(2):379–397, 1985.

[6] A. Brumer and K. Kramer. The rank of elliptic curves. *Duke Math. J.*, 44(4):715–743, 1977.

[7] J. P. Buhler. *Icosahedral Galois representations.* Lecture Notes in Mathematics, Vol. 654. Springer-Verlag, Berlin, 1978.

[8] H. Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[9] P. Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[10] P. Deligne. Valeurs de fonctions L et périodes d'intégrales. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 313–346. Amer. Math. Soc., Providence, R.I., 1979. With an appendix by N. Koblitz and A. Ogus.

[11] P. Deligne and J-P. Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[12] P. Dénes. Über die Diophantische Gleichung $x^l + y^l = cz^l$. *Acta Math.*, 88:241–251, 1952.

[13] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[14] G. Faltings, G. Wüstholz, F. Grunewald, N. Schappacher, and U. Stuhler. *Rational points*. Aspects of Mathematics, E6. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1992. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984, With an appendix by Wüstholz.

[15] J-M. Fontaine. Il n'y a pas de variété abélienne sur $\mathbf{Z}$. *Invent. Math.*, 81(3):515–538, 1985.

[16] G. Frey. Rationale Punkte auf Fermatkurven und getwisteten Modulkurven. *J. Reine Angew. Math.*, 331:185–191, 1982.

[17] G. Frey. Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1(1):1–40, 1986.

[18] A. Grothendieck. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.

[19] Y. Hellegouarch. Courbes elliptiques et équations de fermat. Thèse, Besançon, 1972.

[20] A. Hurwitz. über endliche gruppen linearer substitutionen, welche in der theorie der elliptischen transzendenten auftreten. *Math. Ann.*, 27:183–233, 1886.

[21] N. Jochnowitz. Congruences between systems of eigenvalues of modular forms. *Trans. Amer. Math. Soc.*, 270(1):269–285, 1982.

[22] N. Jochnowitz. A study of the local components of the Hecke algebra mod l. *Trans. Amer. Math. Soc.*, 270(1):253–267, 1982.

[23] N. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[24] N. Katz. A result on modular forms in characteristic p. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 53–61. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[25] S. LaMacchia. Polynomials with Galois group $\mathrm{P}SL(2,7)$. *Comm. Algebra*, 8(10):983–992, 1980.

[26] R. P. Langlands. *Base change for* $\mathrm{GL}(2)$, volume 96 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, N.J., 1980.

[27] W. Li. Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.

[28] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[29] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[30] J-F. Mestre. Courbes de Weil et courbes supersingulières. In *Seminar on number theory, 1984–1985 (Talence, 1984/1985)*, pages Exp. No. 23, 6. Univ. Bordeaux I, Talence, 1985.

[31] J-F. Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242, Nagoya, 1986. Nagoya Univ.

[32] I. Miyawaki. Elliptic curves of prime power conductor with $\mathbf{Q}$-rational points of finite order. *Osaka J. Math.*, 10:309–323, 1973.

[33] O. Neumann. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II. *Math. Nachr.*, 56:269–280, 1973.

[34] F. Oort and J. Tate. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)*, 3:1–21, 1970.

[35] M. Raynaud. Schémas en groupes de type $(p,\ldots,p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[36] K. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[37] C. Schoen. On the geometry of a special determinantal hypersurface associated to the Mumford-Horrocks vector bundle. *J. Reine Angew. Math.*, 364:85–111, 1986.

[38] J-P. Serre. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Sém. Delange-Pisot-Poitou 1969/1970, exposé 19.

[39] J-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[40] J-P. Serre. Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer). In *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, pages 319–338. Lecture Notes in Math., Vol. 317. Springer, Berlin, 1973.

[41] J-P. Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 191–268. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[42] J-P. Serre. Valeurs propres des opérateurs de Hecke modulo l. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, 1974)*, pages 109–117. Astérisque, Nos. 24–25. Soc. Math. France, Paris, 1975.

[43] J-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London, 1977.

[44] J-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, 1978. Troisième édition.

[45] J-P. Serre. *Corps locaux*. Hermann, Paris, 1980. Troisième édition.

[46] J-P. Serre. L'invariant de Witt de la forme $\mathrm{T}r(x^2)$. *Comment. Math. Helv.*, 59(4):651–676, 1984.

[47] J-P. Serre. Résumé des cours de 1984–1985. In *Annuaire du Collège de France*, pages 85–90. 1985.

[48] J-P. Serre. Lettre à J-F. Mestre. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 263–268. Amer. Math. Soc., Providence, RI, 1987.

[49] J-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[50] B. Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[51] G. Shimura. Class fields over real quadratic fields and Hecke operators. *Ann. of Math. (2)*, 95:130–190, 1972.

[52] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[53] J. Tunnell. Artin's conjecture for representations of octahedral type. *Bull. Amer. Math. Soc. (N.S.)*, 5(2):173–175, 1981.

[54] J. Vélu. Courbes modulaires et courbes de Fermat. In *Séminaire de Théorie des Nombres, 1975-1976 (Univ. Bordeaux I, Talence), Exp. No. 16*, page 10. Lab. Théorie des Nombres, Centre Nat. Recherche Sci., Talence, 1976.

[55] A. Weil. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.*, 168:149–156, 1967.