ON SERRE'S MODULARITY CONJECTURE

JEAN-PIERRE WINTENBERGER

1. Introduction

Let $G_{\mathbb{Q}}$ be the Galois group of $\mathbb{Q}$, p a prime number, and $\overline{\mathbb{F}_p}$ the algebraic closure of $\mathbb{F}_p$. We are interested in what we call Serre's type Galois representations $\bar{\rho}$ *i.e.* continuous irreducible odd representations of $G_{\mathbb{Q}}$ with values in $\mathrm{GL}_2(\overline{\mathbb{F}_p})$: there is a finite extension F of $\mathbb{F}_p$ such that $\bar{\rho}$ factors through $\mathrm{GL}_2(F)$.

The conjecture states in a precise way that $\bar{\rho}$ arises from a "usual" (holomorphic) modular form ([10]) . For the oddness, let $c \in G_Q$ be the complex conjugation (defined up to conjugacy). $\bar{\rho}$ is odd if $\det(\bar{\rho}(c)) = -1$, *i.e.* if the eigenvalues of $\bar{\rho}(c)$ are 1 and -1. It is always the case if $p = 2$.

What means arise from a modular form ?

Let N be an interger ≥ 1. Let $\Gamma_0(N)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \bmod N$$

and $\Gamma_1(N)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \bmod N a \equiv 1\ bmodN.$$

Let k be an integer ≥ 1. Let $S_k(\Gamma_1(N))$ be the $\mathbb{C}$ vector space of parabolic forms for $\Gamma_1(N)$ of weight k (among the references : [7], [4]) . An element f of $S_k(\Gamma_1(N))$ is an holomorphic function on the Poincaré half plane $\mathcal{H}$ $\mathrm{im}(z) > 0$. It must satisfy the functional equations :

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. It must satisfy a condition of growth at each cusp. More precisely, for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, let $(f \mid [\gamma]_k)(z) = (cz+d)^{-k} f(\gamma(z))$, $\gamma(z) = \frac{az+b}{cz+d}$. One asks that $(f \mid [\gamma]_k)(z)$ have a Fourier expansion $\sum_{n\geq 1} a_n q^{n/h}$, $q^{1/h} = \exp(2\pi iz/h)$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ (h divides N and is 1 for the cusp ∞ *i.e.* if $\gamma \in \Gamma_1(N)$). When we speak of the q-expansion without more precision we mean the q-expansion at ∞. The quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$ by $\gamma \mapsto d \bmod N$. Then $S_k(\Gamma_1(N))$ carrries an action of $(\mathbb{Z}/N\mathbb{Z})^*$. that is noted $f \mapsto \langle (d) \rangle (f)$. One has a the decomposition $S_k(\Gamma_1(N)) = \sum_\eta S_k(\Gamma_0(N), \eta)$ into eigenspaces, η describing the characters of $(\mathbb{Z}/N\mathbb{Z})^*$. It is trivial if $\eta(-1) \neq (-1)^k$ as the functional equation shows (with $\gamma = -\mathrm{id}$).

The vector space $S_k(\Gamma_1(N))$ is finite dimensional. In fact, we have the projective smooth modular curve $X_1(N)$, which for $N \geq 5$ classify couples (E, P), E generalised elliptic curves, P point of order N, and coherent sheaves ω such that the elements of $S_k(\Gamma_1(N))$ are sections in $\Gamma(X_1(N), \omega^k)$ that vanish at the cusps. For every n prime to N, let T_n be the Hecke operator acting on $S_k(\Gamma_1(N))$ (and $S_k(\Gamma_0(N))$). The T_n and $\langle (d) \rangle$ commute and generate the Hecke algebra (ring) $\mathbb{T}_1(N)$. The T_n are semi-simple (they are normal linear transformation relatively to the Petersson scalar product). $\mathbb{T}_1(N)$ is a $\mathbb{Z}$-module of finite type. It is because, if $S_k(\Gamma_1(N))_{\mathbb{Z}}$ is the $\mathbb{Z}$-module of forms whose q-expansion is in $\mathbb{Z}$,

$$S_k(\Gamma_1(N)) = \mathbb{C} \otimes S_k(\Gamma_1(N))_{\mathbb{Z}}.$$

For that a theory of $X_1(N)$ over $\mathbb{Z}$ is needed (or one can also use the action of $\mathbb{T}_1(N)$ on the singular cohomology of $X_1(N)$).

Let d and M be such that dM divides N. Then $f(z) \mapsto f(dz)$ defines an injection of $S_k(\Gamma_1(M))$ in $S_k(\Gamma_1(N))$. Let $S_k^{\mathrm{new}}(\Gamma_1(N))$ be the orthogonal, for Petersson product, of the sum of the images of $S_k(\Gamma_1(M))$. Then, by Atkin-Lehner, $S_k^{\mathrm{new}}(\Gamma_1(N))$ has a basis f_i that are eigenvectors for $\mathbb{T}_1(N)$, each one appearing with multiplicity one. In fact, they are eigenforms for all Hecke operators T_n. If λ_n is the eigenvalue, one has $a_n(f_i) = \lambda_n a_1(f_i)$. It follows that $a_1(f_i) \neq 0$, and one can normalize f_i such that $a_1(f_i) = 1$. The f_i are the primitive forms. If f is primitive, $a_n(f) = \lambda_n$ generates over $\mathbb{Q}$ a number field E_f, the coefficient field. The $a_n(f)$ are integers. For n prime to N this is because $\mathbb{T}_1(N)$ is finitely generated as $\mathbb{Z}$-module. For p dividing n, we have formulas for a_p (th. 1.27 of [2]).

Let f be a primitive form. Let p be a prime number. Let $\iota_p : E_f \hookrightarrow \overline{\mathbb{Q}_p}$. Deligne if $k \geq 1$, and Deligne-Serre if $k = 1$, constructed a Galois representation $\rho_{f,\iota_p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$. It is unramified at ℓ if ℓ is prime to pN and is characterized by that for all ℓ prime to pN,

$$\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = \iota_p(a_\ell), \det(\rho(\sigma)) = \eta(\sigma)\chi_p(\sigma),$$

for all $\sigma \in G_{\mathbb{Q}}$, where we identify $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ with $(\mathbb{Z}/N\mathbb{Z})^*$. For $k \geq 2$, the representation is part of the p-adic etale cohomology of an algebraic variety over $\mathbb{Q}$. If $k = 1$, the construction of Deligne-Serre use congruences with Galois representations of weight ≥ 2. When $k = 1$, the image is finite.

The reduction $\bar{\rho}$ is well defined up to semisimplification. The Serre's type Galois representation $\bar{\rho}$ is said to arise from a modular if there exists (k, N) such that $\bar{\rho}$ is the reduction of ρ, $k \geq 2$. It implies that $\bar{\rho}$ is odd as $\eta(-1) = (-1)^k$.

Remark. The reduction may be reducible.

Serre's conjecture :

Theorem 1.1. *(Khare-W) Let $\bar{\rho}$ of Serre's type. Then there exist (k, N), $k \geq 2$, f a primitive form for $S_k(\Gamma_1(N))$ and ι_p such that $\bar{\rho}$ is isomorphic to the reduction of ρ_{f,ι_p}.*

Remarks. 1) If E is a elliptic curve over $\mathbb{Q}$, one knows by Wiles,.... that E is modular. By Wiles,..., there exists a primitive $f \in S_2(\Gamma_0(N))$ such that , for every p, the Galois representation $\rho_{E,p}$ on the Tate module of E is isomorphic to $\rho_{f,p}$ ([14]). It has coefficients in $\mathbb{Z}$. Then, $\bar{\rho}_{E,p}$ giving the action of $G_{\mathbb{Q}}$ on the points of order p of E is of Serre's type with $F = \mathbb{F}_p$. Wiles,... theorem implies Serre's conjecture for $\bar{\rho}_{E,p}$.

It follows that the L-function of E satisfies a functional equation analoguous to the functional equation of the Riemann ζ function and is the Mellin transform of f. The converse theorem of Weil implies that an L function that satisfies a functional equation with a precise suitable form is the Mellin transform of a modular form f. This makes perhaps natural that modular forms are linked with Galois representations.

2) There is non condition on $\bar{\rho}$. For ρ, there are conditions as the construction of Deligne for $k \geq 2$ gives ρ as a factor of the p-adic etale cohomology of variety X. First, ρ has to be unramified outside a finite set of primes. Furthermore, let $D_p \subset G_{\mathbb{Q}}$ be the decomposition group for a place above p. The restriction $\rho_{|D_p}$ of ρ to D_p satisfies the properties of p-adic Galois representations which satisfies a p-adic comparison theorem. With the terminology of Fontaine, $\rho_{|D_p}$ is potentially semistable. Fontaine and Mazur call geometric such representations, ramified outside a finite set of primes and potentially semistable ([9]). Fontaine and Mazur conjecture is that $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ odd irreducible and geometric is isomorphic to $\rho_{f,\iota_p} \otimes \chi_p^j$ for f of weight ≥ 1, ι_p an embedding of the coefficients of f in $\overline{\mathbb{Q}_p}$, $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ the cyclotomic character, and $j \in \mathbb{Z}$,

3) It is part of the conjectures in the subject that even geometric representations in $\mathrm{GL}_2(\overline{\mathbb{Q}_p})$ should have finite image and be associated to non-holomorphic Maass forms, eigenvectors for the Laplacian operator with eigenvalue $1/4$. One does not even know how to associate to such forms a Galois representation (one does not even know the algebraicity of the coefficients of these Maass forms).

2. The strong form of the conjecture.

In fact, Serre stated a more precise conjecture. Let $\bar{\rho}$ of Serre type. Serre defines $k(\bar{\rho})$ and $N(\bar{\rho})$ such that in the statement of the theorem we can further impose that $f \in S_{k(\bar{\rho})}(\Gamma_1(N(\bar{\rho})))$.

Theorem 2.1. *(Carayol, Edixhoven, Mazur, Ribet, ...) Let $\bar{\rho}$ be of Serre's type. Suppose that $\bar{\rho}$ arises from a modular form f of weight ≥ 2. Then, $\bar{\rho}$ arises from a modular form of weight $k(\bar{\rho})$ and level $N(\bar{\rho})$; furthermore $k(f) \geq k(\bar{\rho})$ and $N(\bar{\rho})$ devides $N(f)$.*

Le us define $N(\bar{\rho})$. It is the part prime to p of the Artin conductor of $\bar{\rho}$. Let ℓ be a prime $\neq p$ and $N(\bar{\rho})_\ell$ be the ℓ part of $N(\bar{\rho})$. One has $N(\bar{\rho})_\ell = 1$ if $\bar{\rho}$ is unramified at ℓ. Let G be the image of $\bar{\rho}(I_\ell)$ and let $G_0 \supset G_1 \supset \dots G_I \dots$ be the ramification filtration of G. The group G_0 is the inertia subgroup and G_i is the subgroup of $g \in G$ such that $v(\frac{\sigma\pi}{\pi} - 1) \geq i$, v and π are the valuation and a uniformizer of the subfield of $\overline{\mathbb{Q}}_\ell$ fixed by $\rho(I_\ell)$ $(v(\pi) = 1)$. Then $N(\bar{\rho})_\ell$ is ℓ to the power

$$\sum_{i=0}^{\infty} \frac{\dim(V/V_i)}{(G_0 : G_i)}$$

where $V_i = V^{G_i}$. This exponents equals the codimension of V^{I_ℓ} if and only if the action of I_ℓ is tame.

$k(\bar{\rho})$ only depends on the restriction of I_p to $\bar{\rho}$. For $p \neq 2$, we have $2 \leq k(\bar{\rho}) \leq p^2 - 1$ and there exist j such that $k(\bar{\rho} \otimes \overline{\chi_p}^j)$ is $\leq p + 1$. For $p = 2$, $k(\bar{\rho}) = 2, 4$.

A consequence of Serre's conjecture (in the strong form) is, for fixed p, the finiteness of the $\bar{\rho}$ of Serre's type with fixed conductor N.

We have : $S_k(\mathrm{SL}_2(\mathbb{Z})) = (0)$ for $k < 12$ and $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ is 1-dimensional generated by $\Delta = q\Pi_{n \geq 1}(1 - q^n)^{24}$. There is no $\bar{\rho}$ of Serre's type with $N(\bar{\rho}) = 1$ and $p \leq 7$, or $N(\bar{\rho}) = 1$ and $k(\bar{\rho}) < 12$. For $p > 7$, 691 is the only prime such that $\bar{\rho}_{\Delta,p}$ is reducible ([11]). It follows that there exists no $\bar{\rho}$ of Serre's type with $p = 691$ and $k(\bar{\rho}) = 12$. For $p \geq 11, p \neq 691$ and $k(\bar{\rho}) = 12$, the only Serre's type $\bar{\rho}$ is $\bar{\rho} \simeq \overline{\rho_\Delta}$ (which is induced if $p = 23$).

Let us define $k(\bar{\rho})$.

Let $\bar{\rho}_p$ be the restriction of $\bar{\rho}$ to D_p. Let $\bar{\rho}_{p,\mathrm{ss}}$ be the semisiplification of $\bar{\rho}_p$. We have $I_{p,\mathrm{w}} \subset I_p \subset D_p$, where $I_{p,\mathrm{w}}$ is the wild inertia subgroup (the pro p part of I_p). The action of I_p on $\bar{\rho}_{p,\mathrm{ss}}$ factors through $I_p/I_{p,\mathrm{w}} := I_{p,\mathrm{t}}$, and is given by 2 characters. Kummer's theory give an isomorphism of $I_{p,\mathrm{t}}$ with $\prod \mathbb{Z}_\ell$ for $\ell \neq p$. The action of Frobenius is by raising to the power p. The set of these characters of $I_{p,\mathrm{t}}$ appearing in $\bar{\rho}_p$ is stable by the Frobenius. It follows that either the characters are power of the cyclotomic character $\overline{\chi_p}$ (level 1) or $\{\phi, \phi^p\}$ for ϕ a character killed by raising to the power $p^2 - 1$ but not $p - 1$ (level 2). In the first case, $\bar{\rho}_p$ is not irreducible (wild inertia fix at least a line). In the second case $\bar{\rho}_p$ is irreducible as Frobenius permutes the two characters.

Let $\bar{\rho}_p$ be irreducible. The action of I_p is by two characters ϕ and ϕ^p that factorise by $\mathbb{F}_{p^2}^*$ and not by $\mathbb{F}_p^*$. Let ψ be the fundamental character of level 2 *i.e* the Kummer character of the extension $\mathbb{Q}_{p^2}(p^{1/(p^2-1)})/\mathbb{Q}_{p^2}$, where $\mathbb{Q}_{p^2}$ is the quadratic unramified extension of $\mathbb{Q}_p$. Then $\phi = \psi^{(a+pb)}$. with $0 \leq a, b \leq p - 1$, $a \neq b$ as ϕ is of level 2. After possibly changing ϕ by ϕ^p, we can impose that $0 \leq a < b \leq p - 1$. Then $k(\bar{\rho}) = 1 + pa + b$. We can take $j = -a$ and we get $\bar{\rho}'$ with $a' = 0$, $b' = b - a$. Then $k(\bar{\rho}') = 1 + a'$ and $2 \leq k(\bar{\rho}') \leq p$. We have $k(\bar{\rho}) = 2$ if and only if $a = 0$ and $b = 1$: then

$\bar{\rho}_p$ comes from a finite flat group scheme (the restriction to I_p comes from a Lubin-Tate). $k(\bar{\rho}) = 1 + p$ is impossible.

Let $\bar{\rho}_p$ be reducible and $p \neq 2$.

First suppose that the restriction to I_p of $\bar{\rho}_p$ is semisimple, sum of the two characters $\overline{\chi_p}^a$ and $\overline{\chi_p}^b$, $0 \leq a, b \leq p-2$. After possibly permuting the 2 characters, we can suppose that $a \leq b$. Then $k(\bar{\rho}) = 1 + pa + b$ if $(a, b) \neq (0, 0)$ and p if $(a, b) = (0, 0)$. If $a = 0$ we have $k(\bar{\rho}) = 1 + b$ if $b \neq 0$ and $2 \leq k(\bar{\rho}) \leq p - 1$. We have $2 \leq k(\bar{\rho} \otimes \overline{\chi_p}^j) \leq p$ for a j. When $k(\bar{\rho}) = 2$, $\bar{\rho}_p$ comes from a finite flat group scheme. If $a = b = 0$ Edixhoven choose $k = 1$ ([6]).

Let us suppose that wild inertia does not act trivially. Then the restriction of $\bar{\rho}$ to I_p is of the type :

$$\begin{pmatrix} \overline{\chi_p}^\beta & * \\ 0 & \overline{\chi_p}^\alpha \end{pmatrix}.$$

We choose $0 \leq \alpha \leq p-2$ and $1 \leq \beta \leq p-1$. We define $a = \inf(\alpha, \beta)$ and $b = \sup(\alpha, \beta)$. If $\beta \neq \alpha + 1$, we define $k = 1 + pa + b$. If $\beta = \alpha + 1$, let η be the star in the upper corner. It is a D_p 1-cocycle with coefficients in $\overline{\mathbb{F}_p}(\overline{\chi}_p)$, whose cohomology class, up to non zero scalar, describes the isomorphism class of $\bar{\rho}_p$. By Kummer's theory, it comes from $\gamma \in K^* \otimes \overline{\mathbb{F}_p}$ where K is the maximal unramified extension of $\mathbb{Q}_p$. The valuation gives a morphism $v : K^* \otimes \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$. We say that we are in the very ramified case if $v(\gamma)$ does not vanish. In the not very ramified case we have $k = 1 + pa + b$ and in the very ramified case we have $k = (a+1)(p+1)$. In particular , if $\alpha = 0$, which we can reach by a twist, we have $k = 1 + b$ in the not very ramified case (and $2 \leq k \leq p$) and in the very ramified case we have $k = p + 1$. This is the case when $\bar{\rho}_p$ is given by the points of order p of an elliptic curve which has semistable bad reduction at p and $v(q)$ is not divisible by p. When $k = 2$ ($\alpha = 0$, $\beta = 1$ and we are not in the case very ramified) the $\bar{\rho}$ comes from a finite flat group scheme.

If $p = 2$, then $k = 2$ either if $\bar{\rho}_p$ is irreducible or it is reducible and not very ramified. In the very ramified case, we have $k = 4$ (Edixhoven $k = 3$).

Remarks Edixhoven proved for $p \neq 2$ the weight part of the weak form of the Serre's conjecture implies the strong form (in his version which implies Serre's version).

We give some hints about these rules.

2.1. $\bar{\rho}$ comes from a semi-stable elliptic curve over $\mathbb{Q}$.

Let $\bar{\rho}$ comes from the kernel E_p of multiplication by p in a semistbale elliptic curve E over $\mathbb{Q}$.

Let us first suppose that E has good reduction at p. Let $\mathcal{E}$ its model over $\mathbb{Z}_p$. The multipication by p in the formal group of $\mathcal{E}$ is of the form : $[p](X) = pX + \sum_{i \geq 2} a_i X^i$ with

- $v(a_i) > 0$ for $i \leq p-1$,$v(a_p) = 0$ (case ordinary) ,
- $v(a_i) > 0$ for $i \leq p^2 - 1$, $v(a_p) = 0$ (case supersingular) .

In the ordinary case we have an exact sequence of finite flat group schemes over $\mathbb{Z}_p$: $0 \to C_1 \to \mathcal{E}_p \to C_2 \to 0$ with C_1 and C_2 of order p. Here C_1 is the kernel of the multiplication by p on the formal group $\widehat{\mathcal{E}}$ completion at the origin of $\mathcal{E}$. By Oort-Tate classification of finite flat group scheme of rank p, C_1 is isomorphic to μ_p over the rings of interger $\mathbb{Z}_{p,\mathrm{ur}}$ of the maximal unramified extension of $\mathbb{Z}_p$ (the only finite flat group schemes over $\mathbb{Z}_{p,\mathrm{ur}}$ are μ_p and $\mathbb{Z}/p\mathbb{Z}$). By Cartier duality, C_2 is etale (that implies that the action of I_p is trivial ; the converse is true for $p \neq 2$). If R is a local ring, we have a bijection of isomorphism classes of extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p in the category of finite flat commutative group schemes killed by p and elements of $(R)^*/(R^*)^p$. The bijection associates to an extension G, the μ_p-torsor which is is the inverse image of the point $\bar{1} \in \mathbb{Z}/p\mathbb{Z}(R)$. (Let $\alpha \in R^*$. Let R' an R algebra with $\mathrm{Spec}(R')$ connected. Then $G(R')$ is isomorphic to the p-torsion of $(R^*/\alpha^{\mathbb{Z}})$).

We are in the case not very ramified and $k(\bar{\rho}) = 2$.

In the supersingular case, let P be a point of order exactly p. The Newton polygon of $[p](X)$ implies that $v(x(P)) = 1/(p^2-1)$ $(v(p) = 1)$. It follows that for all $\sigma \in I_p$, we have that $v(x(\sigma(P)) - \psi(\sigma)x(P)) > 1/(p^2-1)$ and we can put on E_p a structure of $\mathbb{F}_{p^2}$-vector space of dimension 1 such that $\sigma(P) = \psi(\sigma)P$ for all points of order p. That means that I_p acts on E_p by $\{\psi, \psi^p\}$. We have $k(\bar{\rho}) = 2$.

Let us suppose that E has bad semistable reduction. Then, it is isomorphic to the Tate elliptic curve $\mathbb{G}_{\mathrm{m}}/q^{\mathbb{Z}}$, for $q \in \mathbb{Q}_p^*$ non unit . Then $\bar{\rho}_{E,p}$ is not very ramified if and only if $v(q)$ is divisible by p. Otherwise we are in the case of weight $p+1$. In the not very ramified case, a theorem of Mazur (level lowering) says that $\bar{\rho}_{E,p}$ arises from a modular form of weight 2 with p not dividing N (level lowering).

2.2. **Low weights.** By Scholl ([12]), if f is a primitive form $\in S_k(\Gamma_1(N))$, $k \geq 2$, and ι_p an embedding of its coefficient field E_f in $\overline{\mathbb{Q}_p}$, the Galois representation ρ_{f,ι_p} comes from a Grothendieck motive over $\mathbb{Q}$ with coefficients. More precisely, one has a smooth projective variety X over $\mathbb{Q}$ with an action of an Hecke algebra and a correspondence π on X with $\pi^2 = \pi$ and π commutes to the action of the Hecke algebra. The part $\pi_* H_*(X, \mathbb{Q})$ of the singular homology cut by the projector π is 2-dimensional over a quotient of the Hecke algebra which is isomorphic to E_f. The p-adic etale homology $\pi_* H_*(X, \mathbb{Q}_p)$ gives a Galois representation $\rho_{f,p}$, which composed with ι_p, gives ρ_{f,ι_p}.

The variety X is a desingularization of the symmetric $k-2$ product of the universal generalized elliptic curve over the modular curve with level N structure (one might have to replace N by a multiple, to get rid of problems of representability). The variety X has good reduction outside the primes dividing N. The Galois representation $\rho_{f,p}$ is unramified outside the primes dividing N et p. The trace, relatively to $\mathbb{Q}_p \otimes E_f$, of the image of Frob_ℓ for ℓ not dividing Np is $a_\ell(f)$.

Let us suppose that p does not divide N. One has a p-adic comparison theorem $\pi H_*(X, \mathbb{Q}_p) \otimes B_{\mathrm{crys}} = \pi H_*(X)_{\mathrm{dR}} \otimes B_{\mathrm{crys}}$. (Fontaine-Messing, Faltings, Tsuji,...) for the ring B_{crys} constructed by Fontaine.

We recall some facts about the theory of p-adic Galois representations ([8]).

Let E be the field of fractions of a complete discrete valuation ring with a perfect residue field k_E of characteristic p ; we suppose E of characteristic 0.Then E is a finite totally ramified extension of the field E_0 of fractions of the Witt vectors with coefficients in k_E. By Colmez and Fontaine ([1]), there is an equivalence of categories between the category of admissible filtered Dieudonné modules over E and a subcategory of G_E representations, the crystalline representations. As X has good reduction, the p-adic comparison theorem implies that the restriction of ρ_f to $G_{\mathbb{Q}_p}$ is crystalline (and a fortiori potentially semistable as mentionned in the introduction).

Let σ be the Frobenius of E_0. A filtered Dieudonné module is the data of a E_0-vector space D with a σ-linear endomorphism ϕ and a decreasing filtration Fil^j on $D_E := E \otimes_{E_0} D$ for $j \in Z$, which is exhaustive ($\cup \mathrm{Fil}^j = D$) and separated ($\cap \mathrm{Fil}^j = (0)$).

Let us suppose that D is finite dimensional and that ϕ is bijective. For $D' \subset D$ stable by ϕ, we call $t_{\mathrm{N}}(D')$ the valuation of the determinant of the restriction of ϕ to D' (it does not depend on the chosen basis). We let $t_{\mathrm{H}}(D')$ be $\sum_{j \in \mathbb{Z}} j \dim_E(\mathrm{gr}^j(D'_E))$ where the filtration on D'_E is the induced filtration.

The condition of admissibility is that : D is finite dimensional, ϕ is bijective, $t_{\mathrm{H}}(D') \leq t_{\mathrm{N}}(D')$ for all ϕ-stable D', and $t_{\mathrm{H}}(D) = t_{\mathrm{N}}(D)$.

The comparison theorem allows in principle to describe the Galois representation from the filtered Dieudonné module. $B = B_{\mathrm{crys}}$ is a filtered Dieudonné module, in fact an algebra in the category of filtered Dieudonné module (ϕ and the filtration are compatible with the structure of E_0-algebra). It also carries an action of G_E which commutes with the action of ϕ and respect the filtration. Then $V(D)$, the G_E representation associated by Colmez and Fontaine to D, is the $\mathbb{Q}_p$-vector space of $x \in B \otimes_{E_0} D$ which are fixed by ϕ and are in $\mathrm{Fil}^0(B \otimes_{E_0} D_E)$. But it is not obvious to extract concrete informations on $V(D)$ from D.

Exercise. B contains the completion P of the maximal unramified extension of E_0 with its natural action of Frobenius and non zero elements of P have degree 0 for the filtration. It also contains an inversible element t which satisfies : $\phi(t) = pt$, $\tau(t) = \chi_p(\tau)t$ for $\tau \in G_E$ where χ_p is the cyclotomic character, and the degree of t for the filtration is 1. Show that the crystalline characters $G_E \to \mathbb{Z}_p^*$ are exactly the characters whose restriction to inertia are χ_p^j for an interger j. Show that if $D = \mathbb{Q}_p e$, e of degree 0 for the filtration, $\phi(e) = \lambda e$, then $V(D)$ is unramified and the action of Frobenius is by λ^{-1}.

Let ι_p be an embedding of E_f into $\overline{\mathbb{Q}_p}$ and let K be the closure of its image. Then the filtered Dieudonné module associated to the restriction of ρ_{f,ι_p} has the following shape. (in fact we describe the dual ; we consider the Galois representation with coefficients in K). D is 2-dimensional over K. ϕ is a linear map $\phi : D \to D$ with characteristic polynomial $X^2 - \iota_p(a_p)X + \eta(p)p^{k-1}$ ([12]). The filtration :

$$(0) = \mathrm{Fil}^k(D) \subset \mathrm{Fil}^{k-1}(D) \subset \mathrm{Fil}^0(D) = D,$$

is by K-vector spaces, with $\Delta := \mathrm{Fil}^{k-1}(D)$ of dimension 1. The condition of admissibility is : if $\phi(\Delta) = \Delta$, the corresponding eigenvalue has valuation $k-1$. ϕ is the crystalline Frobenius ; the filtration is the Hodge filtration (one has an natural identification of Fil^{k-1} and $\mathbb{Q}_p \otimes \pi S_k(\Gamma_1(N))$).

Let us call V with the action of $G_{\mathbb{Q}_p}$ the underlying space of ρ_{f,ι_p} and $\bar{V}$ its semisimplified reduction.

The one dimensional over K quotients of V by $G_{\mathbb{Q}_p}$-stable lines corresponds to the subobjects of D, *i.e.* of lines L which are stable by ϕ and such that the corresponding eigenvalue λ is such that $v(\lambda)$ is equal to the degree of the filtration induced on L.

One says that we are in the ordinary case if $v(a_p) = 0$. Then V is not irreducible : it has a quotient of dimension 1 which is unramified. It corresponds to the eigenspace of ϕ for the unit root u of $X^2 - \iota_p(a_p)X + \eta(p)p^{k-1}$. The action of Frobenius on the quotient is by u^{-1}, on the subspace the action of I_p is by χ_p^{k-1}.

It implies that $k(\bar{\rho}) = k$ if $2 \leq k \leq p$ (we have use that, as we have supposed that p does not divide N, for $k = 2$ we are in the case not very ramified case). For $k = p+1$, we see that we have $k(\bar{\rho}) = p+1$ or 2 according that we are in the very ramified case or not.

Suppose $v(a_p) \neq 0$. Then, V is irreducible. Let us suppose that $2 \leq k \leq p$. Then, Fontaine-Laffaille theory establishes a bijection between O_K lattices of V stable by $G_{\mathbb{Q}_p}$ and O_K-lattices L of D which satisfy $\phi(\mathrm{Fil}^{k-1}L) \subset p^{k-1}L$ where the filtration on L the induced filtration. The filtered Dieudonné module reduction of L is $\overline{L} = L/\pi_K L$, with the induced filtration and the map $\phi : \overline{L} \to \overline{L}$ and $\phi_{k-1} : \mathrm{Fil}^{k-1}(\overline{L}) \to \overline{L}$ which is the reduction of $p^{1-k}\phi$. The ring B_{crys} has a subring A_{crys} which has a quotient which is isomorphic to $\overline{O}/p\overline{O}$ where $\overline{O}$ is the ring of integers of the algebraic closure of $\mathbb{Q}_p$. One puts a structure of filtered Dieudonné module on $\overline{L}$: if β is an element of $\overline{O}$ such that $\beta^p = p$, Fil^a is $\beta^a\overline{O}/p\overline{O}$. The map ϕ_a is defined by $\phi_a(\beta^a y) = y^p$. It is not difficult to prove that if we are not in the ordinary case, there is a basis e_0, e_1 of $\overline{L}$ such that $\phi(e_0) = e_1 \in \mathrm{Fil}^{k-1}$, $\phi_{k-1}(e_1) = \alpha e_0$, for $\alpha \in (k_K)^*$. The Galois representation $\overline{V}$ is described as $\mathrm{Hom}(\overline{L}, \overline{O}/p\overline{O})$ in the category of filtered Dieudonné module. It is straightforward that by the reduction of solutions x_0, x_1 of equations $x_0^p = x_1$, $x_1^p = p^{k-1}\alpha x_0$. One sees easily that the action is tame with characters $\psi^{k-1}, \psi^{p(k-1)}$. That proves that $k = k(\bar{\rho})$ in this case.

In the non ordinary case and for arbitrary Hodge weights, one needs Breuil's theory to describe the tame characters on $\bar{V}$.

3. The strategy.

We give the stategy of the proof of Khare of Serre's conjecture in the case of level $N = 1$ ($\bar{\rho}$ not ramified outside p).

Let p be a prime. We call $S(p)$ the statement : if $\bar{\rho} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is irreducible, odd, unramified outside p, $\bar{\rho}$ arises from a primitive modular $\in S_k(\mathrm{SL}_{\mathbb{Z}})$ for a $k \geq 2$.

Let $p \neq 2$. Let k an interger $2 \leq k \leq p+1$, we call $S(k,p)$ the statement : if $\bar{\rho} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is irreducible, odd, unramified outside p, and $k(\bar{\rho}) = k$, then $\bar{\rho}$ arises from a primitive modular $\in S_k(\mathrm{SL}_2(\mathbb{Z}))$.

The statement $S(k,p)$ for all k, $2 \leq k \leq p+1$, implies $S(p)$. This follows from the fact that if $\bar{\rho}$ arises from a modular form, then also $\bar{\rho} \otimes \overline{\chi_p}$. This follows from the existence of the operator θ on modular forms modulo p which on q-expansion is $q\frac{\mathrm{d}}{\mathrm{d}q}$. For $k \geq 2$, an eigenforms are in the image of the reduction map unless $p = 2$ (resp. 3) and $\bar{\rho}_f$ is induced from a character of $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(j)$) (Carayol). Systems of eigenvalues lift (lemma of Deligne-Serre).

The strategy is a recurrence on k (or p).

Two preliminary facts.

The restriction $\det(\bar{\rho})_{|I_p}$ of the determinant to the inertia I_p is $\overline{\chi_p}^{k(\bar{\rho})-1}$. This implies that, as $\bar{\rho}$ is not ramified outside p, $\det(\bar{\rho}) = \overline{\chi_p}^{k(\bar{\rho})-1}$. As $\bar{\rho}$ is odd, $k(\bar{\rho})$ is even. It suffices to prove $S(k,p)$ for even p.

Let H be a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}_p})$. Then, by Dickson, H is conjugate to

- a subgroup of the image of upper triangular matrices,
- $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ or $\mathrm{PSL}_2(\mathbb{F}_{p^r})$, for $r > 0$.
- A_4, S_4 if $p \neq 2$, A_5 or dihedral group of order $2r$ with $r > 1$ not divisible by p.

If the image of $\bar{\rho}$ irreducible is solvable, the projective image is up to conjugacy A_4, S_4 or dihedral. The representation $\bar{\rho}$ lift to a representation with finite image, first projective and then by a theorem of Tate as a linear representation. By Hecke in the dihedral case and Langlands and Tunnell in the A_4 and S_4 case, it arises from a modular form of weight 1. By multiplying its reduction by Hasse invariant, it arises from a modular form of weight p.

So we can suppose that the image of $\bar{\rho}$ is not solvable.

The following theorem of Tate (for $p = 2$) and Serre (for $p = 3$) imply $S(2)$ and $S(3)$.

Theorem 3.1. *Let $\bar{\rho}$ be a continuous representation of $G_{\mathbb{Q}}$ in $\mathrm{GL}_2(\overline{\mathbb{F}_2})$ (resp. $\mathrm{GL}_2(\overline{\mathbb{F}_3})$) and which is unramified outside 2 (resp. 3). Then $\bar{\rho}$ is reducible.*

The proof uses the structure of decomposition subgroups and lower bounds for discriminants.

Proposition 3.2. *$S(2,p)$ is true.*

Sketch of the proof. We have to prove that there is no $\bar{\rho}$ irreductible odd with $k(\bar{\rho}) = 2$ and $N(\bar{\rho}) = 1$. Let $\bar{\rho}$ be finite flat. Then, we have the statement (lifting with control of ramification : LCR) :

Theorem 3.3. *Let $p \neq 2$. Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}_p})$ which is odd and with nonsolvable image. Let us suppose that $2 \leq k(\bar{\rho}) \leq p+1$. Then $\bar{\rho}$ lifts to a $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ which is crystalline of Hodge-Tate weights $(0, k(\bar{\rho})-1)$ and with $N(\bar{\rho}) = N(\rho)$. There is a compatible system (ρ_ι) of $G_{\mathbb{Q}}$ representations such that $\rho = \rho_\iota$ for a ι.*

A geometric p-adic representation ρ has a conductor $N(\rho)$: the part prime to p of the conductor is given by the usual formula, the p-part is given by Fontaine's theory. The representation ρ is crystalline if and only if p does not divide $N(\rho)$. A 2-dimensional geometric $G_{\mathbb{Q}}$ representation which is of Hodge-Tate with weights $(0, k-1)$ with $k \geq 1$ will be called of weight k.

Let $k \geq 1$ and $N \geq 1$. A compatible system (ρ_ι) of 2-dimensional geometric representations of $G_{\mathbb{Q}}$ of weight k and conductor N is a family of geometric Galois representations ρ_ι of weight k and conductor N such that there exist a finite extension E of $\mathbb{Q}$, and for each prime ℓ and each embedding ι of E in $\overline{\mathbb{Q}}_\ell$, ρ_ι is a Galois representation $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$. For each ℓ that does not divide N, there is an integer $a_\ell \in E$ such that $\mathrm{tr}(\rho_\iota(\mathrm{Frob}_\ell)) = \iota(a_\ell)$ for each ι of characteristic $\neq \ell$.

In fact in the theorem, the compatibility is fully proved if $\ell \neq 2$.

If one member is reducible, then all are, as then there is a finite abelian extension K of $\mathbb{Q}$ such that $a_\ell = 1 + \ell^{k-1}$ for all ℓ that split in K and is outside a finite set.

To come back to $S(2,p)$, we have that ρ_ι, for ι an embedding in $\overline{\mathbb{Q}_3}$ is reducible by a theorem of Fontaine and Abrashkin.

We can also use the following theorem of Skinner and Wiles. Ordinary of weight $k \geq 2$ for a p-adic representation or a modulo p representation of D_p means that it has a free of rank 1 subrepresentation where the action of I_p is by χ_p^{k-1} and the quotient is unramified. p-adic ordinary representations are semistable and for $k > 2$ are crystalline. We say that a $G_{\mathbb{Q}}$ p-adic or mod. p representation is ordinary of its restriction to D_p is. The theorem of Skinner-Wiles that we use is:

Theorem 3.4. *Let $p \neq 2$. Let $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be a continuous irreducible representation which is geometric, odd and ordinary of weight $k \geq 2$. Suppose that $\bar{\rho}$ is either reducible or irreducible and modular. Suppose that $p-1$ does not divide $k-1$. Then ρ arises from a modular form of weight k.*

Such a statement will be called Lifting Modularity Theorem (LMT). The hypothesis $p-1$ divides $k-1$ ensures that the restriction of the two characters of the semisimplification of $\bar{\rho}$ to D_p are distinct. Skinner and Wiles have in fact a more general statement under this hypothesis.

To give an alternative proof of $S(2,p)$, we apply the theorem to ρ_ι the 3-adic representation as above. We also use the following proposition :

Proposition 3.5. *Let $p \neq 2$. Let ρ be a crystalline representation of D_p which is of weight k with $2 \leq k \leq p+1$. If $\bar{\rho}$ is reducible, it is ordinary, and ρ is also ordinary.*

The proposition follows from Fontaine-Laffaille theory for $2 \leq k \leq p$ and from Berger- Li-Zhu in the case of weight $p+1$. Berger-Li-Zhu prove that if $k = p+1$, either ρ is ordinary (and $k(\bar{\rho}) = 2$ or $p+1$) or it is not ordinary and the $\bar{\rho}_{|D_p}$ is irreducible and $k(\bar{\rho}) = 2$..

Proposition 3.6. *Let p and q be primes $\neq 2$ and let k be such that $2 \leq k \leq p+1$ and $2 \leq k \leq q+1$. If $S(k,p)$ is true, then also $S(k,q)$.*

Let $\bar{\rho}$ in characteristic q. We lift it and extend to a compatible system given by theorem 3.3. We consider ρ_p a p-adic member of the compatible system. We have $k(\rho_p) = k$ and $N(\rho_p) = 1$. We have the different cases :

- $\bar{\rho}_p$ is reducible. Then the restriction to D_p to ρ_p is ordinary, $p-1$ does not divide $k-1$ (k is even !), so the theorem of Skinner-Wiles 3.4 applies.
- $\bar{\rho}_p$ is irreducible. Then, by $S(k,p)$ it is modular, as $k(\bar{\rho}) = k$ if $k \leq p-1$ and if $k = p+1$, $k(\bar{\rho})$ is 2 or $p+1$ by Berger-Li-Zhu. In fact $k(\bar{\rho}) = 2$ and $\bar{\rho}_p$ irreducible is impossible by $S(2,p)$ that we already proved. If the restriction of ρ to D_p is reducible, we can apply theorem 3.4.

Let us suppose that the restriction of $\bar{\rho}$ to D_p is irreducible. We have $k \leq p-1$ and we claim that hypothesis 3) of the following LMT theorem is true.

Theorem 3.7. *Let $p \neq 2$. Let $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be a continuous irreducible representation which is geometric, odd and of weight $k \geq 2$. Suppose :*

1) $\bar{\rho}$ is irreducible and modular ;
2) $2 \leq k \leq p-1$ and ρ is crystalline ;
3) the restriction of ρ to $G_{\mathbb{Q}(\mu_p)}$ is irreducible ;
Then ρ arises from a modular form of weight k.

Proof of the claim : Suppose that the projective image H of $\bar{\rho}$ is dihedral of order $2r$, $r \geq 1$ prime to p. First r is odd as $\mathbb{Q}$ do not have 2 distinct quadratic extensions only ramified at p. The action of I_p is tame and factors through an element σ of order 2 of H. The normalisator of σ is the group of order 2 generated by σ. Hence the action of D_p in $\bar{\rho}_p$ is reducible.

Let $p' > p$. We see that $S(p')$ implies $S(p)$. To prove Serre's conjecture, it suffices to prove it for infinitely many p. We also see that if we know $S(p)$, we know $S(k,p')$ for $2 \leq k \leq p$. As $S(3)$ is true, we know $S(4,p)$ for all $p \geq 3$.

Proposition 3.8. *We have $S(6,p)$ for all $p \geq 5$.*

It suffices to prove $S(6,5)$. Let $\bar{\rho}$ of characteristic 5. A version of LCR gives a semistable lift ρ of weight 2 and conductor 5 : $\rho_{|D_5}$ is an extension of an unramified representation of dimension 1 by a dimension 1 representation on which I_5 acts by χ_5. The extension reduces to a very ramified extension. A theorem of Taylor implies that there exist a totally real field F such that the restriction of ρ to G_F comes from a Hilbert modular form for F of weight 2 unramified outside 5 and is Steinberg at primes above 5. That implies that the restriction of ρ to G_F is a factor of the Tate-module of a simple abelian variety B over F which has good reduction outside the primes above 5 and has bad semistable reduction at primes above 5. One has finite extension N of $\mathbb{Q}$ which is of degree the dimension of B and an embedding $N \hookrightarrow \mathrm{End}_{\mathbb{Q}}(B)$. By enlarging N , we can suppose that the factor is of multiplicity 1. Let B' be the Weil restriction from F to $\mathbb{Q}$ of B. Then ρ is a factor with multiplicity 1 of the Tate-module of B' by Frobenius theorem on induced representation.

By Faltings, ρ is a factor of the Tate module of a simple abelian variety B'' over $\mathbb{Q}$. Let L be the center of $\mathrm{End}_{\mathbb{Q}}(B'')$. By Faltings, ρ corresponds to an idempotent of $\mathbb{Q}_p \otimes L$. Then, B'' has good reduction outside 5 and has bad semistable reduction at 5. This follows from compatibility below. But by Brumer-Kramer (see also Schoof) such an abelian variety does not exist.

For the Galois representations associated to abelian varieties we have the following compatibility. Let F be a finite extension of $\mathbb{Q}_p$ and A a simple abelian variety over F. Let L be the center of $\mathrm{End}_{\mathbb{Q}}(A)$.

Let $W_\wp$ be the Weil group *i.e.* the inverse image in the decomposition group G_F of the subgroup generated by the Frobenius. We have an action of $W_\wp$ on the Tate modules $V_\ell(A)$, for $\ell \neq p$. Beware that this action is defined by restriction in the case A has potential good reduction, but it is not the case in general. We also have an action on the filtered Dieudonné module associated to the action of G_F on $V_p(A)$; the filtered Dieudonné module is a free $L \otimes \mathbb{Q}_{p,\mathrm{ur}}$-module. These actions are continuous in the sense that they are trivial on an open subgroup of inertia.

We have the following compatibility. Let $d = 2\mathrm{dim}(A)/[L : \mathbb{Q}]$. For each ι embedding of L in $\overline{\mathbb{Q}}_\ell$ (ℓ can be p), we get a representation ρ_ι of $W_\wp$ in $\mathrm{GL}_d(\overline{\mathbb{Q}}_q)$ by scalar extension $\mathbb{Q}_\ell \otimes L \to \overline{\mathbb{Q}}_\ell$ if $\ell \neq p$ and $\mathbb{Q}_{p,\mathrm{ur}} \otimes L \to \overline{\mathbb{Q}_p}$. The compatibility is that for each $\tau \in W_\wp$ the characteristic polynomial of τ acting on ρ_ι have coefficients in L that are independant of ℓ and p.

This implies that there is a finite extension E of L and a representation ρ_{W} of $W_\wp$ in $\mathrm{GL}_d(E)$ such that for each ι embedding of E in $\overline{\mathbb{Q}}_\ell$, the representation ρ_ι is isomorphic to the representation obtained from ρ_{W} by scalar extension $\iota : E \hookrightarrow \overline{\mathbb{Q}}_\ell$.

The abelian variety has semistable reduction if an only if ρ_{W} is trivial on the inertia group. In fact, one has the Weil-Deligne group whose finite dimensional representations are the data of a continuous representation of the Weil group and a nilpotent element N satisfying $\phi N \phi^{-1} = qN$ if the residue field of F has q elements and ϕ is any lifting of the Frobenius. We have a generalization of the above compatibility to the Weil-Deligne group. $N = 0$ if and only if A has potentially good reduction. $N = 0$ and the representation of the Weil group is trivial on inertia if and only if A has good reduction. The representation of the Weil-Deligne group defined by a Tate elliptic curve over F is trivial on W_{W} and N is a non trivial nilpotent.

The proof is by induction on p. We know $S(p)$ and we want to prove $S(P)$, with $p < P$. The induction hypothesis is that either $P = 7$ and $p = 5$, or $P > 7$ is not a Fermat prime and p is the biggest non Fermat prime $< P$ ($P \neq 2^* + 1$, $* = 2^*$).

First, suppose that $\bar\rho_{|D_P}$ is irreducible. We can suppose that $P < 2p - 1$ by the lemma below. We can also suppose that $k > p + 1$, as otherwise we already know Serre's conjecture, hence $k > 2$. We have $k < P + 1$, as the $P + 1$ case is ordinary. The couple (a, b), $0 \leq a < b \leq P - 1$, such that inertia acts by characters $\psi^{a+Pb}, \psi^{P(a+Pb)}$, ψ fundamental character of level 2, is such that $a = 0, b = k - 1 > 1$. (Recall that $k(\bar\rho) = b - a + 1 + a(P + 1)$). We consider twists by $\overline{\chi_P}, \overline{\chi_P}^2, \ldots$. Each time we twist we add $P + 1$ to the weight till we have made $P - b$ twists, and one of the characters is $\psi^{P-b+P^2} = \psi^{P-b+1}$. As $1 < P - b + 1 < P$, we have $k(\bar\rho \otimes \chi_P^{P-B}) = P - b + 2 = P - k + 3$. We have $P + 3 - k < P + 2 - p < p + 1$, so $\bar\rho \otimes \chi_P^{P-B}$ is modular, hence $\bar\rho$.

Let us see how the general proof works when $P = 7$. We can suppose that $k = 8$. We lift $\bar\rho$ and extend it to a compatible system (ρ_ι) of weight 2 and level 7. We consider a 3-adic member and its reduction $\bar\rho_3$. We have $k(\bar\rho_3) = 2$. If $\bar\rho_3$ is unramified at 7, $\bar\rho_3$ is reducible. and Skinner-Wiles implies that ρ_3 is modular and we are done. Let us suppose that $\bar\rho_3$ is ramified at 7 and irreducible. It cannot be induced. If it has solvable image it is modular and ρ_3 is modular by Skinner-Wiles. So we can suppose that it has non solvable image. Then we can lift it and extend it to a compatible system (ρ'_ι) of weight 2 and conductor 7 but whose Weil Deligne action at 7 is $(\omega_7^2 \oplus \mathrm{id}, 0)$ (note that ω_7^2 is of ordre 3).Then $k(\bar\rho') = 4$ or $k(\bar\rho' \otimes \ \overline{\chi}_7^2) = 6$ (Savitt). It follows that $\bar\rho'$ is modular or reducible. One check that one can apply a LMT theorem and conclude that (ρ'_ι) is modular.

Lemma 3.9. *Let $P > 7$ a non Fermat prime and let p the biggest non Fermat prime $< P$. Then there exist an odd prime ℓ dividing $P - 1$, such that the exact power ℓ^r of ℓ dividing $P - 1$ satisfy :*

$$P/p \leq \frac{2m+1}{m+1} - (\frac{m}{m+1})(\frac{1}{p}),$$

if $l^r = 2m + 1$.

For the proof, one proves that for $p > 100,000$, $P/p \leq 3/2 - 1/30$. We have Chebyshev type of estimates :

$$Ax/\log(x) < \pi(x) < Bx/\log(x),$$

for $x > x_0$. Let $a > C := B/A$. Let p_n the nth prime. The above inequalities implies that $p_{n+1} \leq ap_n$ for $p_{n+1} > \max(ax_0, a^{\frac{a}{a-C}})$. For $x > 100.000$, we have Chebyshev type of inequality for $A = 1, B = 1.131$. One applies it for $a = 1.2$, get $p_{n+1} \leq 1.2p_n$ for $p_{n+1} > 100.000$. There are no pair of successive Fermat primes after 3 and 5. One deduces that for $P > 100.000$, $P/p \leq (1.2)^2 < 1.4\bar{6} = 3/2 - 1/30$.

Let $\bar{\rho}$ of characteristic P with $2 \leq k(\bar{\rho}) \leq P+1$. We suppose that $k(\bar{\rho}) > p+1$. We suppose that $\bar{\rho}$ has non have solvable image. The weight $k(\bar{\rho})$ is > 2. We lift it to a compatible system (ρ_ι) of weight 2 and level P. The representation of the Weil-Deligne group WD_P is such that :

- if $k(\bar{\rho}) < P+1$, $N = 0$ and the restriction to I_P is $\omega_P^{k(\bar{\rho})-2} \oplus \mathrm{id}$, where ω_P is the Teichmuller representative of $\overline{\chi}_P$ (the coefficient field E of the compatible system has to contains the $P-1$ roots of unity) ;

- if $k(\bar{\rho}) = P+1$, the restriction to the Weil group is unramified and $N \neq 0$.

We consider ρ_ι where ι is of characteristic ℓ, ℓ as in the lemma : we call it ρ_ℓ. If $\bar{\rho}_\ell$ is reducible or dihedral we are done by Skinner-Wiles (one has to check that one can apply it). So we may suppose that $\bar{\rho}_\ell$ is ramified at P (as otherwise it is of weight 2 hence has solvable image). The action of I_P on ρ_ℓ is isomorphic to $\omega_P^{k(\bar{\rho})-2} \oplus \mathrm{id}$ if $k(\bar{\rho}) < P+1$ and unipotent if $k(\bar{\rho}) = P+1$.

The action of I_P on $\bar{\rho}_\ell$ is either isomorphic to $\overline{\omega_P}^{k(\bar{\rho})-2} \oplus \mathrm{id}$ with $\overline{\omega_P}^{k(\bar{\rho})-2} \neq 1$ or unipotent. Let i be an integer in $[m(P-1)/(2m+1), (m+1)(P-1)/(2m+1)]$ such that ω_P^i is congruent modulo the prime above ℓ defined by ι to $\omega_P^{k(\bar{\rho})-2}$. It is not difficult to prove that the reduction of the restriction of $\bar{\rho}_\ell$ to D_P lifts to a representation of D_P whose restriction to I_P is isomorphic to $\overline{\omega_P}^i \oplus \mathrm{id}$. A theorem LCR implies that as $\bar{\rho}_\ell$ is not reducible or dihedral, we can lift $\bar{\rho}_\ell$ to a compatible system $(\rho'_{\iota'})$ of weight 2 and level P with Weil-Deligne action isomorphic to $\overline{\omega_P}^i \oplus \mathrm{id}$.

Remark LCR theorem says that we do not have local global obstruction for the lift. It is motivated by the fact it is true for Galois representations associated to modular forms. For example, we have the following theorem of Carayol. Let η and η' characters of $G_{\mathbb{Q}}$ with values in $\overline{\mathbb{Z}_p}^*$ which have the same reduction. if $\bar{\rho}$ irreducible odd arises from $S_2(\Gamma_0(p), \eta)$, then it arises from $S_2(\Gamma_0(p), \eta')$ except for some induced particular $\bar{\rho}$ ($p = 3$ and $\bar{\rho}$ induced from $\mathbb{Q}(j)$ and $p = 2$ $\bar{\rho}$ induced from $\mathbb{Q}(i)$).

Choose a ι' of characteristic P and let ρ'_P be $\rho'_{\iota'}$. By Savitt, $\bar{\rho}'_P$ has weight $i+2$ or $\bar{\rho}'_P \otimes \overline{\chi_P}^{-i}$ has weight $P+1-i$. But the inequality of the above lemma is equivalent to $p+1 \geq \frac{m+1}{2m+1}(P-1)+2$ and we have $\frac{m+1}{2m+1}(P-1)+2 = (P+1) - \frac{m}{2m+1}(P-1)$. This implies that $2 \leq i, P+1-i \leq p+1$ and $\bar{\rho}'_P$ is either reducible or modular.

Remarks

The theorem of Savitt is motivated a theorem of Serre which says that if $\bar{\rho}$ arises from $S_2(\Gamma_0(p), \overline{\chi_p}^i)$, it also arises from $S_{i+2}(\mathrm{SL}_2(\mathbb{Z}))$ or $S_{p+1-i}(\mathrm{SL}_2(\mathbb{Z}))(\overline{\chi_p}^{-i})$.

What happens in case $k(\bar{\rho}) = 12$. We can suppose $P = 11$. Then, $\rho_{11}(\Delta)$ is congruent to $\rho_{11}(X_0(11))$. This follows that $S_2(\Gamma_0(11)$ is generated by $q\prod_{n\geq 1}(1-q^n)^2\prod_{n\geq 1}(1-q^{11n})^2$. We have $\ell^r = 5$, $X_0(11)$ has equation $y^2 + y = x^3 - x$, and $(0,0)$ is a point of order 5. So we can apply Skinner Wiles to ρ_5.

4. Lifting Modularity Theorem

We sketch the proof the following theorem which is an extension of a theorem of Wiles Taylor-Wiles (Diamond, Fujiwara, Taylor, Kisin,...) :

Theorem 4.1. *Let $p > 2$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be an odd Galois representation. One supposes that :*

- the restriction to $G_{\mathbb{Q}(\mu_p)}$ of "the reduction" $\bar{\rho}$ is irreducible (hence ρ is irreducible) ;

- $\bar{\rho}$ is modular ;

- ρ is unramified outside a finite set of primes ;

- $\rho_{|D_p}$ is crystalline of weight k (Hodge-Tate weights $(0, k-1)$) with $2 \leq k \leq p+1$.

Then ρ is modular.

Remark The case $k = p+1$ and the restriction of $\bar{\rho}$ to D_p is irreducible (hence $\bar{\rho}$ is of weight 2 is due to Kisin).

We introduce a solvable totally real field F. We prove that $\rho_{|G_F}$ is modular, *i.e.* arises from a cuspidal automorphic representation of $(D \otimes \mathbb{A}_F)^*$, D a suitable quaternion algebra of center F. Then, by Jacquet-Langlands correspondence and Arthur-Clozel solvable base change, we will know that ρ is modular.

One advantage of considering F is that we can suppose that $\rho_{|G_F}$ is unramified outside primes V_p over p and primes in a finite set Σ where at $v \in \Sigma$, the Weil-Deligne parameter of ρ_{D_v} is trivial on I_v and $N \neq 0$ (the representation $\rho_{|I_v}$ is tame and its image is unipotent). Furthermore, D is ramified exactly at infinity and primes in Σ (one imposes that $[F : \mathbb{Q}]$ and the cardinality of Σ are even). One supposes that F is unramified above p. One supposes that $\overline{\rho}_{|G_F}$ arises from π, that is discrete series of weight k at infinity, unramified outside Σ and unramified twist of Steinberg at primes in Σ. These latter conditions might imply to do level and weight lowering or raising.

One advantage to consider indefinite D is that spaces of modular forms with action of Hecke operators has combinatorial description. Let $(D \otimes_F \mathbb{A}_F^\infty)^*$ be the finite adeles. We fix a maximal order $\mathcal{O}_D$ of D. Let $U_v = (\mathcal{O}_D)_v^*$ and $U = \prod_v U_v$. Let E be an extension of $\mathbb{Q}_p$ which is sufficiently large and O be its ring of integers. Let $W := \otimes_{F \hookrightarrow E} \mathrm{Sym}^{k-2} O$ with the natural action of U through its quotient $\prod_{v \in V_p} U_v$, where V_p are the primes above p. Let ψ be the character $\det(\rho)\chi_p^{-1} = \chi_p^{k-2}$ where χ_p is the p-adic cyclotomic character. We also see ψ as a character of the finite ideles $(\mathbb{A}_F^\infty)^*$. We define the space of modular forms $S_{k,\psi}(U)$ with coefficients in O with central character ψ to be the space of functions

$$f : D^* \backslash (D \otimes_F \mathbb{A}_F^\infty)^* \to W$$

such that:

$$f(gu) = u^{-1} f(g)$$

$$f(gz) = \psi(z)f(g)$$

for all $g \in (D \otimes_F \mathbb{A}_F^\infty)^*, u \in U, z \in (\mathbb{A}_F^\infty)^*$.

For each finite place v of F we fix a uniformizer π_v of F_v. We consider the left action of $g \in (D \otimes_F \mathbb{A}_F^\infty)^*$ by right translation on the W-valued functions f on $(D \otimes \mathbb{A}_F^\infty)^*$ and denote this action by $g.f$ or gf. This induces an action of the double cosets $U \begin{pmatrix} \pi_v & 0 \\ 0 & \pi_v \end{pmatrix} U$ and $U \begin{pmatrix} \pi_v & 0 \\ 0 & 1 \end{pmatrix} U$ on $S_{k,\psi}(U)$ for $v \notin S$ (S is the set of places $V_\infty \cup V_p \cup \Sigma$). We denote these operators by S_v (which is simply multiplication by $\psi(\pi_v)$) and T_v respectively. They do not depend on the choice of π_v. We call $T_{k,\psi}(U)$ the Hecke algebra acting on $S_{k,\psi}(U)$ generated over O by the Hecke operators T_v and S_v at primes $v \notin S$.

By Jacquet-Langlands, $S_{k,\psi}(U)$ with its action of Hecke operators is (essentially) isomorphic of automorphic forms for $\mathrm{GL}_2(F)$ which are of weight k, unramifed outside Σ and for $v \in \Sigma$ it is unramified twist of Steinberg.

The automorphic representaton π defines a morphism $T_{k,\psi}(U) \to O$. By reduction it defines a maximal ideal m of $T_{k,\psi}(U)$. Let $T_{k,\psi}(U)_{\mathsf{m}}$ be the completion. By Deligne and Carayol, we get a Galois representation : $G_F \to \mathrm{GL}_2(T_\psi(U)_{\mathsf{m}})$ that lifts $\overline{\rho}$.

Let $\overline{R}_S^\psi$ be the ring representing deformations of $\overline{\rho}_{|G_F}$ that have determinant $\psi\chi_p$ and satisfies the following properties for $v \in S := V_\infty \cup V_p \cup \Sigma$: odd, crystalline of weight k and for $v \in \Sigma$ of the form $\begin{pmatrix} \gamma\chi_p & * \\ 0 & \gamma \end{pmatrix}$ with $\gamma^2\chi_p = \psi$.

We get a surjective map $\overline{R}_S^\psi \to T_\psi(U)_{\mathsf{m}}$. To get our theorem, we prove that this map is bijective after inverting p.

The existence of $\overline{R}_S^\psi$ as a complete noetherian local noetherian (CNLO) with residue field the residue field $\mathbb{F}$ of O is as follows. Let $G = G_{F,S}$. One can first consider the functor of continuous lifts in $G \to \mathrm{GL}_2(A)$, for A in CNLO. It is representable by a CNLO-algebra. It is almost obvious, but there is the continuity condition. One can use a representability theorem of Grothendieck which is a particular case of Schessinger criteria. One has to use that for any open subgroup G' of G, there are only finitely many continuous morphisms from G' to $\mathbb{Z}/p\mathbb{Z}$. The relative tangent space is the $\mathbb{F}$-vector space of 1-cocyles $Z^1(G, \mathrm{Ad})$ where Ad is the adjoint representation of $\bar{\rho}$.

A *deformation* of $\bar{\rho}$ is an equivalence set of lifts, two lifts being equivalent if they are conjugate by a matrix of the kernel $\mathrm{GL}_2(A)_1$ of the morphism $\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{F})$. As $\bar{\rho}$ is supposed to be irreducible the action of $\mathrm{PGL}(A)_1$ has no fixed points and Schlessinger criteria easily implies the representability. The relative tangent space is the $\mathbb{F}$-vector space $H^1(G, \mathrm{Ad})$.

Fixing the determinant is clearly a closed condition (for tangent spaces, as $p \neq 2$, replace Ad by trace 0 matrices Ad^0). The condition to be crystalline is closed. At least when $k \leq p-1$, it is because one can define a crystalline representation of weight $(0, k-1)$ with coefficients in a CNLO artinian algebra and the category is stable by direct sums, subobjects and quotients. For $v \in \Sigma$, we impose that the action is tame, the action of inertia is unipotent and the characteristic polynomial of a lift of Frobenius.

We want to prove that R is not to big and that T is not too small. In fact we have to do it allowing ramification at a finite set of auxiliary primes Q_n disjoint of S is allowed.

Let Q_n be a finite set of primes disjoint of S. We suppose :

- AUX1 $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues α_v and β_v and $\mathbb{N}(v) \equiv 1 \mathrm{mod}\, p^n$.

For $v \in Q_n$ let Δ_v the maximal p-quotient of k_v^* so by classfield theory it identifies to the maximal p-quotient of tame inertia at v. It is not difficult to see that the restriction to I_v of the universal representation in $\mathrm{GL}_2(\bar{R}^{\psi}_{S\cup Q_n})$ factors through Δ_v : the action of D_v is $\gamma_{\alpha_v} \oplus \gamma_{\beta_v}$ with γ_{α_v} having unramified reduction with the image of Frobenius α_v, idem for γ_{β_v} and the restriction γ_{α_v} and γ_{β_v} to I_v are inverse. Let $\Delta_n := \prod_{v\in Q_n} \Delta_v$. We have an action of Δ_v, hence of Δ_n on $\bar{R}^{\psi}_{S\cup Q_n}$ (by multiplication by $\gamma_{\alpha_v}(\sigma)$ where σ is a generator of tame inertia at v). The quotient of $\bar{R}^{\psi}_{S\cup Q_n}$ by the augmentation ideal is $\overline{R}^{\psi}_{S}$.

We have a compatible action of Hecke-algebras. The space $S_{k,\psi}(U_{Q_n})$ is defined in the same way as $S_{k,\psi}(U)$ but for $v \in Q_n$, one replaces $U_v = (O_D)_v^* \simeq \mathrm{GL}_2(O)$ by :

$$(U_{Q_n})_v = \{g \in \mathrm{GL}_2(\mathcal{O}_{F_v}) : g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mathrm{mod.}(\pi_v), ad^{-1} \to 1 \in \Delta_v\},$$

The natural action of $g \in \Delta_v$, denoted by $\langle g \rangle$, arises from the double coset

$$U_{Q_n} \begin{pmatrix} \tilde{g} & 0 \\ 0 & 1 \end{pmatrix} U_Q$$

where $\tilde{g}$ is a lift of g to $(\mathcal{O}_F)_v^*$. One also needs Γ_0 level.

$$\left(U_Q^0\right)_v = \{g \in \mathrm{GL}_2(\mathcal{O}_{F_v}) : g = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mathrm{mod.}(\pi_v)\}.$$

We have corresponding Hecke-algebras and maximal ideals m

We have the following proposition (at least for $p > 3$), otherwise more technical) :

Proposition 4.2. *$S_{k,\psi}(U_{Q_n})_{\mathsf{m}}$ is a free $O[\Delta_n]$-module of rank equal to the rank of $S_{k,\psi}(U^0_{Q_n})_{\mathsf{m}}$ as an O-module. $S_{k,\psi}(U^0_{Q_n})_{\mathsf{m}}$ is isomorphic to $S_{k,\psi}(U)_{\mathsf{m}}$.*

For the proof one uses the combinatorial description of spaces of modular forms. For U one of the open subgroups defined above, if $(D \otimes_F \mathbb{A}_F^{\infty})^*$ is the disjoint union of ${}_{i\in I}D^* t_i U(\mathbb{A}_F^{\infty})^*$ for a finite set I and with $t_i \in (D \otimes \mathbb{A}_F^{\infty})^*$, then $S_{k,\psi}(U)$ can be identified with

$$\oplus_{i\in I} W^{(U(\mathbb{A}_F^{\infty})^* \cap t_i^{-1} D^* t_i)/F^*} \tag{1}$$

via $f \to (f(t_i))_i$.

If $p > 3$, the groups appearing as exponent are of order prime to p (isotropy groups : one uses F unramified at p). The first part of the proposition follows. At least it follows that, for η a character of Δ_n, the rank of the part of $S_{k,\psi}(U_{Q_n})_{\mathsf{m}}$ on which the Δ_n acts with character η does not depend on η. This is because by replacing O by its residue field $\mathbb{F}$ one gets a space of modular form with coefficients in $\mathbb{F}$ which does not depend on η and which is the reduction of the spaces of modular forms with coefficients in O for the various η. This essentially gives a theorem of Carayol.

The fact that $S_{k,\psi}(U^0_{Q_n}) \simeq S_{k,\psi}(U)$ relies that there is no new at p modular forms for $\Gamma_0(p)$ that reduces to $\bar{\rho}$ as the eigenvalues of Frob_v are distinct and $\mathbb{N}(v) \equiv 1 \mathrm{mod}\ p$ and an Ihara lemma to get an isomorphism over O.

As the action of D_v in $\bar{\rho}$ is not irreducible, we consider for $v \in S$, the ring $\bar{R}_v^{\square,\psi}$ that represents lifts of $\bar{\rho}_{|D_v}$ with the current condition. We define $\bar{R}^{\square,\psi}_{S\cup Q_n}$ the ring that represents deformations of $\bar{\rho}$ of determinant $\psi\chi_p$ that locally at $v \in S$ satisfy the current conditions, are unramified outside Q_n and for $v \in S$ a choice of the basis B_v of the underlying space. Two such datas are isomorphic if $(\rho_{|D_v}, B_v)$ define isomorphic lifts. We write $\bar{R}_S^{\square,\mathrm{loc},\psi}$ the completed tensor product $\otimes_{v\in S}\bar{R}_v^{\square,\psi}$.

The ring $\bar{R}^{\square,\psi}_{S\cup Q_n}$ is naturally an $\bar{R}_S^{\square,\mathrm{loc},\psi}$-algebra. It is almost clear that $\bar{R}^{\square,\psi}_{S\cup Q_n}$ is a power series algebra over $\bar{R}^{\psi}_{S\cup Q_n}$ with $4s-1$ variables (s is the cardinality of S).

We let $R_n := \bar{R}^{\square,\psi}_{S\cup Q_n}$ and $M_n := R_n \otimes_{\bar{R}^{\psi}_{S\cup Q_n}} S_{k,\psi}(U_{Q_n})_{\mathsf{m}}$. We have structure of $O[[y_1,\ldots,y_{q_n+4s-1}]]$-algebra on R_n and an action of $O[[y_1,\ldots,y_{q_n+4s-1}]]$ on M_n that are compatible. The coinvariants by $(y_1,\ldots,y_{q_n+4s-1})$ are R and M respectively. The module M_n is finite free over the image of R_n in $\mathrm{End}_O(M_n)$.

We now have to bound the number of generators of R_n as a $\bar{R}_S^{\square,\mathrm{loc},\psi}$-module.

We write h^* for the dimension over $\mathbb{F}$ of H^*. For $v \in S \cup Q_n$, we choose $L_v \subset H^1(D_v, \mathrm{ad}^0)$ and $H^1_{\{L_v\}}(S \cup Q_n, \mathrm{ad}^0)$ are the elements of $H^1(S \cup Q_n, \mathrm{ad}^0)$ that at $v \in S \cup Q_n$ localizes to an element of L_v. We choose $L_v = 0$ for $v \in S$ and $L_v = H^1(D_v, \mathrm{ad}^0)$ for $v \in Q_n$.

Lemma 4.3. *The minimal number of generators of* $\bar{R}^{\square,\psi}_{S\cup Q_n}$ *as a* $\bar{R}_S^{\square,\mathrm{loc},\psi}$*-algebra is* $h^1_{\{L_v\}}(S \cup Q_n, \mathrm{ad}^0) + \sum_{v\in S} h^0(D_v, \mathrm{ad}) - 1$.

We have Wiles formula (we will use it with $V = Q_n$)

(2)
$$\frac{|H^1_{\{L_v\}}(S \cup V, \mathrm{Ad}^0)|}{|H^1_{\{L_v^\perp\}}(S \cup V, (\mathrm{Ad}^0)^*(1))|} = \frac{|H^0(G_F, \mathrm{Ad}^0)|}{|H^0(G_F, (\mathrm{Ad}^0)^*(1))|} \prod_{v\in S\cup V} \frac{|L_v|}{|H^0(D_v, \mathrm{Ad}^0)|}$$

We will be able to impose to Q_n the properties :
AUX2 : $q_n = h^1_{\{L_v^\perp\}}(S, (\mathrm{ad}^0)^*(1))$ and $H^1_{\{L_v^\perp\}}(S \cup Q_n, \mathrm{ad}^0)^*(1)) = 0$.
We write $q_n = q$.
In the Wiles formula, the terms $h^0(G_F)$ are trivial, the contribution of $v \in S$ is $-h^0(D_v, \mathrm{ad}^0)$ and the term for $v \in Q_n$ is 1. Finally, we have proved that

Lemma 4.4. *The minimal number of generators of $\bar{R}^{\square,\psi}_{S\cup Q_n}$ as a $\bar{R}^{\square,\mathrm{loc},\psi}_S$-algebra is $q + s - 1$.*

For the rings $\bar{R}^{\square,\psi}_v$ and $\bar{R}^{\square,\mathrm{loc},\psi}_S$, we have :

- $\bar{R}^{\square,\psi}_v$ is flat over $\mathcal{O}$,
- The relative to $\mathcal{O}$ dimension of each component of $\bar{R}^{\square,\psi}_v$ is :
  - 3 if $\ell \neq p$;
  - $3 + [F_v : \mathbb{Q}_p]$ if $\ell = p$;
  - 2 if v is an infinite place.
- $\bar{R}^{\square,\psi}_v[\frac{1}{p}]$ is regular.

It follows that the completed tensor product $\bar{R}^{\square,\mathrm{loc},\psi}_S$ is flat over $\mathcal{O}$, with each component of relative dimension $3|S|$, and $\bar{R}^{\square,\mathrm{loc},\psi}_S[\frac{1}{p}]$ is regular.

References

[1] P. Colmez et J.-M. Fontaine Construction des représentations p-adiques semi-stables Inven. Math. 140 (2000)
[2] H. Darmon, F. Diamond, R. Taylor. Fermat's last theorem.
[3] F. Diamond and J. Shurman. A first course in Modular Forms.
[4] F. Diamond and J. Im Modular forms and modular curves Seminar on Fermat's last theorem.
[5] B. Edixhoven Serre's conjecture Modular forms and Fermat's last theorem
[6] B. Edixhoven The weight in Serre's conjecture on modular forms Inventiones 109, 1992.
[7] Miyake Modular forms.
[8] J.-M. Fontaine and Y. Ouyang Theory of p-adic Galois Representations
[9] J.-M. Fontaine and B. Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), Ser. Number Theory, I, pages 41–78. Internat. Press, Cambridge, MA, 1995.
[10] J.-P. Serre. Sur les représentations modulaires de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). Duke 54 1987
[11] H.P.F. Swinnerton-Dyer. . On ℓ-adic representations and congruences for modular forms. Lecture Notes in Math. 350.
[12] T. Scholl. Motives for modular forms Inventiones 100.
[13] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2), 141(3), 553–572, 1995.
[14] A. Wiles. Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2), 141(3), 443–551, 1995.

E-mail address: wintenb@math.u-strasbg.fr

Université Louis Pasteur, Département de Mathématique, Membre de l'Institut Universitaire de France, 7, rue René Descartes, 67084, Strasbourg Cedex, France