SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Travaux de Wiles (et Taylor, ...), partie I

Séminaire N. Bourbaki, 1994-1995, exp. n° 803, p. 319-332.

<http://www.numdam.org/item?id=SB_1994-1995__37__319_0>

Séminaire BOURBAKI
47ème année, 1994-95, n° 803

Juin 1995

TRAVAUX DE WILES (ET TAYLOR,...), PARTIE I

par **Jean-Pierre SERRE**

Le théorème qui fait l'objet de cet exposé, et de celui d'Oesterlé, est le suivant :

THÉORÈME (Wiles [37], complété par Taylor-Wiles [34]).— *Toute courbe elliptique sur* $\mathbf{Q}$ *qui est semi-stable est modulaire.*

(Pour les définitions de "semi-stable" et de "modulaire", voir § 1.)

En d'autres termes :

La conjecture de Taniyama-Weil est vraie pour les courbes elliptiques semi-stables sur $\mathbf{Q}$.

(En fait, la semi-stabilité en 3 et 5 suffit, d'après Diamond [10].)

La démonstration est longue, et utilise des méthodes très diverses, dues notamment à Faltings, Langlands, Mazur, Ribet,... On se bornera à en expliquer la stratégie générale. Pour la vérification(*) des points techniques (qui sont essentiels, bien entendu), le lecteur devra se reporter à [34] et [37] ; on recommande aussi l'exposé qu'en donnent Darmon, Diamond et Taylor, cf. [7].

1. LA CONJECTURE DE TANIYAMA-WEIL

1.1. Énoncés

À tout entier $N \geq 1$ est associée une certaine courbe $X_0(N)$ sur $\mathbf{Q}$, dont on trouvera la définition par exemple dans [32]. C'est une courbe *modulaire* au sens suivant : ses points (les "pointes" mises à part) paramètrent les isogénies cycliques de degré N entre courbes elliptiques.

La jacobienne $J_0(N)$ de $X_0(N)$ est une variété abélienne, définie sur $\mathbf{Q}$. La forme la plus simple de la conjecture de Taniyama-Weil est :

(*) vérification que le rédacteur ne prétend pas avoir entièrement faite.

Conjecture 1.— *Toute courbe elliptique sur* $\mathbf{Q}$ *est* $\mathbf{Q}$*-isogène à un quotient de* $J_0(N)$*, pour* N *convenable.*

Ou, ce qui est équivalent :

Conjecture 1′.— *Pour toute courbe elliptique* E *sur* $\mathbf{Q}$*, il existe un entier* $N \geq 1$ *et un* $\mathbf{Q}$*-morphisme non constant* $X_0(N) \to E$.

Cet énoncé peut être précisé en termes du *conducteur* $N(E)$ de la courbe E. Rappelons quelques propriétés de $N(E)$ (pour une définition générale, voir [27]) :

On a :

$$N(E) = \prod p^{n(p,E)},$$

où p parcourt l'ensemble des nombres premiers, et où :

$n(p,E) = 0$ si E a bonne réduction en p,

$n(p,E) = 1$ si E a mauvaise réduction de type multiplicatif (cubique à point double à tangentes distinctes),

$n(p,E) \geq 2$ sinon (et même $n(p,E) = 2$ sauf si $p = 2$ ou 3).

On dit que E est *semi-stable en* p si $n(p,E) = 0$ ou 1 ; on dit que E est *semi-stable* si elle est semi-stable en tout nombre premier, *i.e.* si son conducteur est sans facteur carré. (Pour une interprétation en termes de modèles de Néron et une généralisation aux variétés abéliennes, voir par exemple [2].)

La forme plus précise de la conjecture de Taniyama-Weil est :

Conjecture 2.— *L'entier* N *de la conjecture* 1′ *peut être pris égal à* $N(E)$.

En fait, on sait (Carayol [3]) que ces divers énoncés sont *équivalents.* De plus, le conducteur $N(E)$ est le plus petit (au sens multiplicatif) des N intervenant dans la conjecture 1′.

Une autre formulation est :

Conjecture 2′.— *Il existe une forme parabolique primitive* ("newform", au sens d'Atkin-Lehner [1]) $f = \sum a_n q^n$*, de poids* 2 *et de niveau* $N(E)$*, telle que la série de Dirichlet* $L(f,s) = \sum a_n n^{-s}$ *soit égale à la fonction* L *associée à* E (au sens de [27]).

En particulier, on a :

$a_p = 0$, si $n(p,E) = 2$;

$a_p = \pm 1$, si $n(p,E) = 1$;

$a_p = 1 + p - |E(\mathbf{F}_p)|$ = Trace du Frobenius de E en p, si $n(p,E) = 0$.

Exemple.— La courbe elliptique d'équation $y^2 - y = x^3 - x^2$ est de conducteur 11. Elle est liée par une isogénie de degré 5 à $J_0(11)$, qui est de dimension 1. La forme primitive correspondante est :

$$f = q \prod_{n=1}^{\infty} (1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + q^6 + \cdots$$

1.2. Historique de la conjecture de Taniyama-Weil

Le point de départ est un travail d'Eichler [13], publié en 1954, qui démontre (au moins dans un cas particulier) que la fonction L de $X_0(N)$ est essentiellement la même qu'un produit de fonctions L attachées par Hecke aux formes paraboliques de poids 2 et de niveau N. Quelques années plus tard, ceci est clarifié et généralisé par Shimura [31], et complété sur un point important ("bonne réduction en dehors de N") par Igusa [17].

En 1955, dans un recueil de problèmes distribué aux participants du colloque de Tokyo-Nikko [33], Taniyama propose une réciproque :

"Let C be an elliptic curve over an algebraic number field k, and $L_C(s)$ denote the L function of C over k, namely $\zeta_C(s) = \zeta_k(s)\zeta_k(s-1)/L_C(s)$, is the zeta function of C over k. If a conjecture of Hasse is true for $\zeta_C(s)$, then the Fourier series obtained from $L_C(s)$ by the inverse Mellin-transformation must be an automorphic form of dimension -2, of some special type (cf. Hecke). If so, it is very plausible that this form is an elliptic differential of the field of that automorphic functions. The problem is to ask if it is possible to prove Hasse's conjecture for C, by going back this considerations, and by finding a suitable automorphic form from which $L_C(s)$ may be obtained."

Ce texte ne semble guère avoir eu d'écho, à cause de sa distribution limitée et de sa rédaction imprécise (par exemple : qu'est-ce que le "field of automorphic functions" lorsque k n'est pas totalement réel ?).

La situation change en 1967, avec la publication du mémoire de Weil [36] donnant une caractérisation des séries de Dirichlet provenant de formes modulaires. Non que Weil insiste sur la conjecture en question : il se borne à la mentionner comme un "Übungsaufgabe" pour le lecteur que cela peut intéresser. Mais il lui apporte deux compléments essentiels :

a) Il montre que toute fonction L, dont les "tordues" par des caractères ont des prolongements analytiques satisfaisant à des équations fonctionnelles de type raisonnable, provient d'une forme modulaire.

b) Il suggère la forme précise appelée plus haut "conjecture 2", mettant en jeu le conducteur. Du coup, cela permet toute une série de vérifications : courbes à

multiplication complexe, courbes à petit conducteur (exemple : pourquoi ne trouve-t-on pas de courbe elliptique de conducteur < 11 ? Parce que $X_0(N)$ est de genre 0 pour $N < 11$).

Ces résultats ont eu une profonde influence, d'autant plus qu'ils arrivaient en même temps que la théorie des motifs de Grothendieck et la philosophie de Langlands : visiblement, une belle synthèse restait (et reste encore) à faire !

(Le lecteur qui s'intéresse aux relations entre les idées de Weil et celles de Langlands aura intérêt à lire les commentaires sur [36], rédigés par Weil lui-même, dans le troisième volume de ses *Oeuvres.*)

1.3. Terminologie

Elle a varié, au fil des années et des modes :

Une courbe elliptique sur $\mathbf{Q}$ pour laquelle la conjecture 1′ est vraie a été longtemps appelée une courbe "de Weil". On dit maintenant que c'est une courbe elliptique "modulaire".

Le terme de "conjecture de Weil" a été d'abord utilisé pour désigner l'ensemble des conjectures du n° 1.1 ; c'était un peu fâcheux, vu le risque de confusion avec d'autres conjectures de Weil. On est passé de là à "conjecture de Taniyama-Weil" ; c'est la terminologie utilisée ici. Plus récemment, on trouve "conjecture de Shimura-Taniyama-Weil", ou même "conjecture de Shimura-Taniyama", le nom de Shimura étant ajouté en hommage à son étude des quotients de $J_0(N)$. Le lecteur choisira. L'essentiel est qu'il sache qu'il s'agit du même énoncé.

1.4. Quelques applications du théorème de Wiles

a) La plus spectaculaire – et celle qui semble avoir motivé Wiles – est le *théorème de Fermat.* On sait en effet, grâce à Ribet [25], que :

"Taniyama-Weil dans le cas semi-stable $\Longrightarrow$ Fermat".

La démonstration de cette implication utilise une construction de Hellegouarch et Frey, cf. [15]. Elle a été exposée au Séminaire Bourbaki 1987/88 par Oesterlé [23]. Je n'y reviens pas.

Je profite quand même de l'occasion pour rectifier une assertion de [30], fin du n° 4.2 : "La relation existant entre solutions de l'équation de Fermat... figure déjà dans un travail de Hurwitz...". C'est faux, comme me l'a signalé N. Schappacher : il n'y a rien de tel dans Hurwitz. *Mea culpa.*

b) Le même genre d'argument s'applique à des équations voisines de celle de Fermat. Par exemple cf. [30], n° 4.3), si L est un nombre premier appartenant à l'ensemble $\{3,5,7,11,13,17,19,19,23,29,53,59\}$ et si p est un nombre premier > 7, l'équation $x^p + y^p = L^\alpha \cdot z^p$ n'a pas de solution avec $x, y, z \in \mathbf{Z}$, $xyz \neq 0$, α entier ≥ 0.

D'autres exemples sont donnés dans Darmon [6].

c) Lorsqu'on applique la méthode de Goldfeld et Gross-Zagier à la détermination des corps imaginaires quadratiques de petit nombre de classes, on a besoin de savoir que certaines courbes elliptiques (par exemple les courbes $y^2 - y = x^3 - 7x + 6$ et $y^2 - y = x^3 - x + 6$, de conducteurs 5077 et 16811) sont modulaires, cf. [24]. C'était assez pénible. C'est maintenant un cas particulier du théorème de Wiles.

d) Le fait de savoir qu'une courbe est modulaire permet de définir l'ordre de sa fonction L au point $s = 1$, et du coup d'énoncer (et parfois de démontrer) les conjectures de Birch et Swinnerton-Dyer.

2. REPRÉSENTATIONS GALOISIENNES MODULAIRES

Commençons par rappeler quelques résultats connus.

2.1. Représentations galoisiennes de degré 2 en caractéristique ℓ

Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$. Si K est une sous-extension de $\overline{\mathbf{Q}}$, on note G_K le groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$.

Soit ℓ un nombre premier. Vu les applications que nous avons en vue, *on supposera* $\ell \neq 2$ (bien que le cas $\ell = 2$ pose des problèmes fort intéressants, cf. [30], n° 5.2). Soit $\mathbf{F}$ une clôture algébrique de $\mathbf{F}_\ell$. Une *représentation de* $G_\mathbf{Q}$ *de degré* 2 *à coefficients dans* $\mathbf{F}$ est un homomorphisme continu

$$\rho : G_\mathbf{Q} \longrightarrow \mathbf{GL}_2(\mathbf{F}).$$

Son image est finie ; elle est donc contenue dans $\mathbf{GL}_2(F')$, où F' est une extension finie de $\mathbf{F}_\ell$ (le cas le plus important pour la suite est celui où $F' = \mathbf{F}_\ell$).

On note $\det\rho$ le déterminant de ρ. On dit que ρ est *impaire* si $\det\rho(c) = -1$, où c est la conjugaison complexe (pour un plongement quelconque de $\overline{\mathbf{Q}}$ dans $\mathbf{C}$).

Une telle représentation n'est ramifiée qu'en un nombre fini de nombres premiers. Pour presque tout p, on peut donc parler de l'élément de Frobenius $\rho(\mathrm{Frob}_p)$, défini à conjugaison près dans $\mathbf{GL}_2(\mathbf{F})$; en particulier, $\mathrm{Tr}\,\rho(\mathrm{Frob}_p)$ et $\det\rho(\mathrm{Frob}_p)$

sont des éléments bien déterminés de $\mathbf{F}$ et de $\mathbf{F}^*$ respectivement. Si ρ est semi-simple, la connaissance des $\operatorname{Tr}\rho(\mathrm{Frob}_p)$, pour presque tout p, détermine ρ à conjugaison près.

Les formes modulaires ($\mathrm{mod}\,\ell$) fournissent de telles représentations, d'après un théorème de Deligne (cf. [8], [9]). De façon plus précise (voir [9] pour les détails), si f est une forme modulaire ($\mathrm{mod}\,\ell$) de type (N, k, ε), qui est fonction propre des opérateurs de Hecke T_p (pour $p \nmid \ell N$), il existe une représentation ρ semi-simple qui est *associée* à f au sens que :

$$(*) \qquad \operatorname{Tr}\rho(\mathrm{Frob}_p) = a_p \quad \text{pour tout} \quad p \quad \text{assez grand},$$

où a_p est la valeur propre de T_p correspondant à f.

Cette représentation est unique, à conjugaison près. Elle est non ramifiée en tout p ne divisant pas ℓN. De plus, pour un tel p, la formule $(*)$ est vraie et l'on a :

$$(**) \qquad \det\rho(\mathrm{Frob}_p) = \varepsilon(p)\, p^{k-1}.$$

On peut reformuler $(**)$ en disant que le caractère $\det\rho$ est égal au produit du caractère ε par χ^{k-1}, où χ est le caractère cyclotomique, cf. [30], § 1. Comme $\varepsilon(-1) = (-1)^k$, on a $\det\rho(c) = -1$, *i.e.* ρ est impaire.

Remarque.— Ce qui précède est vrai que l'on interprète le terme de "forme modulaire $\mathrm{mod}\,\ell$" au sens "réduction en caractéristique ℓ de formes modulaires en caractéristique 0", ou, lorsque $(\ell, N) = 1$, au sens de Katz [18].

2.2. Les conjectures de [30]

Convenons de dire qu'une représentation $\rho : G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F})$ est *modulaire* si elle peut être obtenue à partir d'une forme modulaire ($\mathrm{mod}\,\ell$) par la méthode que l'on vient d'indiquer.

Conjecture 3 ([29], [30]).— *Toute représentation irréductible impaire*

$$\rho : G_{\mathbf{Q}} \longrightarrow \mathbf{GL}_2(\mathbf{F})$$

est modulaire.

De même que pour Taniyama-Weil, il est essentiel d'avoir une forme plus précise de la conjecture qui fournisse explicitement un triplet (N, k, ε) permettant d'obtenir la représentation ρ donnée. On trouvera dans [30] la définition d'un tel triplet, que nous noterons $(N(\rho), k(\rho), \varepsilon(\rho))$. Le poids $k(\rho)$ ne dépend que de la ramification de ρ

en ℓ, tandis que le niveau $N(\rho)$, qui est premier à ℓ, ne dépend que de la ramification en dehors de ℓ (c'est essentiellement le *conducteur d'Artin* de ρ). La forme précisée de la conjecture 3 est alors :

Conjecture 4.— *Si ρ satisfait aux hypothèses de la conjecture 3, et si $\ell \neq 3$, ou si $\ell = 3$ et la restriction de ρ à $G_{\mathbf{Q}(\sqrt{-3})}$ est irréductible, alors ρ est associée à une forme modulaire de type $(N(\rho), k(\rho), \varepsilon(\rho))$.*

Remarques.— 1) Si l'on utilise la définition des formes modulaires mod ℓ de Katz, le cas "$\ell = 3$ et la restriction de ρ à $G_{\mathbf{Q}(\sqrt{-3})}$ est réductible" n'est plus exceptionnel.

2) On sait maintenant, grâce aux travaux de Ribet et d'autres (cf. [4], [5], [10], [11], [12], [16], [25], [26], [37]) que les conjectures 3 et 4 sont *équivalentes*. De façon plus précise, *si une représentation ρ est modulaire, elle l'est pour $(N(\rho), k(\rho), \varepsilon(\rho))$* – avec la même exception que ci-dessus. C'est là un résultat difficile, qui joue un rôle important dans la démonstration de Wiles (cf. l'exposé d'Oesterlé).

3) Les conjectures ci-dessus, utilisées pour une suite de ℓ tendant vers l'infini, entraînent (facilement) la conjecture de Taniyama-Weil, cf. [30], n° 4.6. La méthode de Wiles est différente : au lieu de faire varier ℓ, il le remplace par ℓ^n, avec $n \to \infty$, cf. plus loin. C'est assez naturel : l'anneau $\mathbf{Z}_\ell = \varprojlim \mathbf{Z}/\ell^n\mathbf{Z}$ a une structure plus simple que le produit des $\mathbf{F}_\ell$ pour ℓ variable.

Un exemple

THÉORÈME 1 ([30], prop. 11).— *Si $\ell = 3$, et si ρ prend ses valeurs dans $\mathbf{GL}_2(\mathbf{F}_3)$, la conjecture 3 est vraie pour ρ.*

Rappelons la démonstration, qui est une simple application de la *théorie de Langlands* [20], complétée par Tunnell [35] :

On utilise le fait que $\mathbf{GL}_2(\mathbf{F}_3)$ se relève dans $\mathbf{GL}_2(\mathbf{Z}[\sqrt{-2}])$. La représentation $\rho : G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_3)$ donne ainsi une représentation

$$\rho_0 : G_{\mathbf{Q}} \longrightarrow \mathbf{GL}_2(\mathbf{Z}[\sqrt{-2}]) \longrightarrow \mathbf{GL}_2(\mathbf{C}).$$

D'après Langlands et Tunnell (*loc. cit.*), la fonction L de ρ_0 est associée, au sens de [9], à une forme modulaire de poids 1. La réduction de cette forme en caractéristique 3 convient. (Si l'on désire une forme de poids 2, et non de poids 1, on multiplie par une série d'Eisenstein convenable, par exemple $\theta = \sum_{x,y \in \mathbf{Z}} q^{x^2+xy+y^2}$ $= 1 + 6(q + q^3 + \cdots)$.)

2.3. Représentations galoisiennes dans des anneaux locaux

Le cas d'un corps ne suffit pas. On a besoin d'anneaux locaux complets. En fait, il suffira (dans le présent exposé, mais pas dans celui d'Oesterlé) du cas de l'anneau des entiers d'une extension finie de $\mathbf{Q}_\ell$. Soit donc A un tel anneau, soit $\mathfrak{m}$ son idéal maximal, et choisissons un plongement de $A/\mathfrak{m}$ dans $\mathbf{F} = \overline{\mathbf{F}}_\ell$, cf. n° 2.1. On s'intéresse à des homomorphismes continus $\rho : G_\mathbf{Q} \to \mathbf{GL}_2(A)$.

Par réduction (mod $\mathfrak{m}$), un tel homomorphisme définit une représentation en caractéristique ℓ

$$\overline{\rho} : G_\mathbf{Q} \longrightarrow \mathbf{GL}_2(\mathbf{F}).$$

Ici encore, la théorie de Deligne (cf. [3], [8], [19]) fournit de telles représentations, à partir de formes modulaires. L'une des façons d'énoncer le résultat est d'introduire, pour tout couple (N, k), l'espace $S_1(N, k)$ des formes paraboliques de poids k sur $\Gamma_1(N)$, ainsi que la $\mathbf{Z}$-sous-algèbre $\mathbf{T}$ de $\mathrm{End}(S_1(N, k))$ engendrée par les opérateurs de Hecke T_n, pour n premier à ℓN. On dit alors que ρ est *modulaire* de type (N, k) s'il existe un homomorphisme $a : \mathbf{T} \to A$ tel que, pour tout $p \nmid \ell N$, ρ soit non ramifiée en p et $\mathrm{Tr}\,\rho(\mathrm{Frob}_p) = a(T_p)$; on a $\det \rho(\mathrm{Frob}_p) = a(R_p)\, p^{k-1}$, où R_p désigne l'opérateur "losange" $\langle p \rangle$, qui appartient à $\mathbf{T}$.

Une représentation est dite *modulaire* si elle l'est pour un couple (N, k) convenable.

Exemple : représentation ℓ-adique associée à une courbe elliptique

Soit E une courbe elliptique sur $\mathbf{Q}$, et soit $T_\ell(E) = \varprojlim E[\ell^n]$ son module de Tate. C'est un $\mathbf{Z}_\ell$-module libre de rang 2, muni d'une action de $G_\mathbf{Q}$. Si l'on identifie $T_\ell(E)$ à $\mathbf{Z}_\ell \times \mathbf{Z}_\ell$, on en déduit une représentation

$$\rho_{E,\ell} : G_\mathbf{Q} \longrightarrow \mathbf{GL}_2(\mathbf{Z}_\ell).$$

THÉORÈME 2.— *Pour que la représentation $\rho_{E,\ell}$ soit modulaire au sens ci-dessus, il faut et il suffit que E soit modulaire au sens du* n° 1.3 (autrement dit, la conjecture de Taniyama-Weil est vraie pour E).

L'implication "E-modulaire $\Longrightarrow$ $\rho_{E,\ell}$ modulaire" est facile. Pour l'implication réciproque, on remarque que, si $\rho_{E,\ell}$ est modulaire de type (N, k), on a $k = 2$, et le caractère correspondant $\varepsilon : p \mapsto a(R_p)$ est égal à 1 (cela résulte du fait que $\det \rho_{E,\ell}$ est égal au ℓ-ième caractère cyclotomique χ_ℓ). On déduit de là qu'il existe un $G_\mathbf{Q}$-homomorphisme non trivial de $T_\ell(E)$ dans $T_\ell(J_0(N))$, et il en résulte

que E est $\mathbf{Q}$-isogène à un quotient de $J_0(N)$ d'après un théorème de Faltings [14] (ex "conjecture de Tate").

2.4. Un cas particulier du théorème principal de Wiles

Je me borne à un cas simple, mais suffisant pour la suite ; le lecteur trouvera des énoncés plus généraux dans [7], [10] et [37].

On considère une représentation ℓ-adique $\rho : G_{\mathbf{Q}} \to \mathbf{GL}_2(A)$ du type du n° 2.3 (avec $\ell \neq 2$, bien entendu). On fait les hypothèses suivantes :

(0) ρ est non ramifiée en dehors d'un ensemble fini de nombres premiers.

(1) La réduction (mod $\mathfrak{m}$) $\overline{\rho}$ de ρ est modulaire au sens du n° 2.2.

(2) La représentation $\overline{\rho}$ est irréductible ; si $\ell = 3$, sa restriction à $G_{\mathbf{Q}(\sqrt{-3})}$ est irréductible.

(3) Le déterminant de ρ est égal au caractère cyclotomique χ_ℓ.

(4) La représentation ρ est semi-stable en ℓ (au sens de l'exposé d'Oesterlé) et, pour tout $p \neq \ell$, l'image par ρ du groupe d'inertie en p est un groupe unipotent, *i.e.* est conjuguée d'un sous-groupe de $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

THÉORÈME 3 (Wiles [37]).— *Si les conditions ci-dessus sont réalisées, ρ est modulaire au sens du* n° 2.3.

La démonstration de ce résultat fait l'objet de l'exposé d'Oesterlé. Indiquons seulement son point de départ, qui consiste à comparer *déformations universelles* de $\overline{\rho}$ (au sens de Mazur [22]) et *déformations de Hecke* ; tout revient alors à montrer que ces déformations coïncident.

COROLLAIRE.— *Soit E une courbe elliptique semi-stable sur $\mathbf{Q}$. S'il existe $\ell \geq 3$ tel que la représentation $\overline{\rho}_{E,\ell}$ associée à E et ℓ soit modulaire au sens du* n° 2.2 *et vérifie* (2) *ci-dessus, alors E est modulaire.*

Cela résulte du th. 2, et du fait que $\rho_{E,\ell}$ a les propriétés (0), (3) et (4).

On verra au § 3 comment cet énoncé, appliqué avec $\ell = 3$ ou 5, entraîne la conjecture de Taniyama-Weil dans le cas semi-stable.

3. FIN DE LA DÉMONSTRATION

Dans tout ce qui suit, E désigne une courbe elliptique semi-stable sur $\mathbf{Q}$. On se propose de montrer que E est modulaire.

3.1. La représentation $\overline{\rho}_{E,\ell}$

Soit ℓ premier ≥ 3, et soit $E[\ell]$ le groupe des points de ℓ-division de E. L'action de $G_{\mathbf{Q}}$ sur $E[\ell]$ définit une représentation :

$$G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}\, E[\ell] \simeq \mathbf{GL}_2(\mathbf{F}_\ell).$$

Par extension des scalaires de $\mathbf{F}_\ell$ à $\mathbf{F} = \overline{\mathbf{F}}_\ell$, cela donne la représentation $\overline{\rho}_{E,\ell}$ du n° 2.4.

PROPOSITION 1.— *Deux cas seulement sont possibles* :

a) $G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_\ell)$ *est surjectif.*

b) *L'image de* $G_{\mathbf{Q}}$ *dans* $\mathbf{GL}_2(\mathbf{F}_\ell)$ *est contenue dans un sous-groupe de Borel.*

(Le cas b) signifie que $E(\overline{\mathbf{Q}})$ contient un sous-groupe d'ordre ℓ stable par $G_{\mathbf{Q}}$.)

Pour $\ell \geq 7$, ceci est démontré dans [28], prop. 21. Des arguments analogues s'appliquent à $\ell = 3$ et 5. Indiquons par exemple comment on traite le cas où $\ell = 3$. Soit G l'image de $G_{\mathbf{Q}}$ dans $\mathbf{GL}_2(\mathbf{F}_3)$ et soit PG son image dans $\mathbf{PGL}_2(\mathbf{F}_3) = S_4$. Supposons que ni a), ni b) ne soient vrais. Alors PG est distinct de S_4, et ne fixe aucun point ; comme PG n'est pas contenu dans A_4 (à cause de la surjectivité du déterminant de la représentation), il en résulte que PG est, soit le groupe diédral D_4 d'ordre 8, soit un sous-groupe d'indice 2 de D_4. Mais le fait que E soit semi-stable entraîne que, pour tout $p \neq 3$, le groupe d'inertie de p dans PG est trivial. On obtient alors une extension galoisienne de $\mathbf{Q}$ de groupe de Galois PG, qui est non ramifiée en dehors de 3. Or il est facile de voir qu'une telle extension n'existe, ni quand $PG = D_4$, ni quand PG est d'indice 2 dans D_4.

Remarques

1) Le cas b) n'est possible que si la courbe E, ou une courbe ℓ-isogène à E, possède un point d'ordre ℓ rationnel sur $\mathbf{Q}$ ([28], *loc. cit.*).

2) Il résulte d'un théorème de Mazur (cf. [21]) que le cas b) ne se produit *que pour une valeur de* ℓ ($\ell \geq 3$) *au plus*, et que cette valeur est ≤ 7.

3.2. Le cas a) pour $\ell = 3$

PROPOSITION 2.— *Supposons que, pour $\ell = 3$, on soit dans le cas* a) *de la prop.* 1. *du* n° 3.1. *Alors E est modulaire.*

En effet, la représentation $G_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{F}_3)$ est modulaire (th. 1), et surjective. D'où le résultat, d'après le corollaire au th. 3.

3.3. Le cas b) pour $\ell = 3$

Supposons maintenant que l'on soit dans le cas b) pour $\ell = 3$. D'après la remarque 2) du n° 3.1, on est alors dans le cas a) pour tout $\ell > 3$, et en particulier pour $\ell = 5$. La représentation $\overline{\rho}_{E,5}$ a donc une image isomorphe à $\mathbf{GL}_2(\mathbf{F}_5)$. De plus :

PROPOSITION 3.— *$\overline{\rho}_{E,5}$ est modulaire.*

Soit X la courbe qui paramètre les courbes elliptiques E' munies d'un isomorphisme $E'[5] \simeq E[5]$ compatible avec les isomorphismes de Weil :

$$\wedge^2 E[5] \simeq \mu_5 \qquad \text{et} \qquad \wedge^2 E'[5] \simeq \mu_5.$$

On vérifie par descente galoisienne que X est une courbe affine lisse absolument irréductible sur $\mathbf{Q}$. Sa compactification lisse $\overline{X}$ est $\mathbf{C}$-isomorphe à la courbe modulaire $X(5)$, qui est de genre 0. De plus, $\overline{X}$ *est isomorphe à la droite projective* $\mathbf{P}_1$. Cela peut se voir de deux façons : soit en construisant par descente un fibré inversible de degré impair sur $\overline{X}$, soit en remarquant que X a un point $\mathbf{Q}$-rationnel, à savoir le point P_0 correspondant à $E' = E$ et à l'application identique $E[5] \to E[5]$.

Choisissons maintenant une suite de points rationnels P_n de X, correspondant à des courbes elliptiques E_n, ayant les propriétés suivantes :

(i) *Le groupe de Galois des points de 3-division de E_n est* $\mathbf{GL}_2(\mathbf{F}_3)$.

(ii) *Les P_n tendent 5-adiquement vers le point P_0 correspondant à E.*

Une telle suite de points existe ; cela résulte du théorème d'irréductibilité de Hilbert (applicable parce que $\overline{X} \simeq \mathbf{P}_1$) compte tenu de ce que (i) est vrai pour un point générique de $\overline{X}$.

Si $p \neq 5$, les courbes E_n sont semi-stables en p : cela provient de ce que $E_n[5]$ est isomorphe à $E[5]$, car la semi-stabilité en p se "lit" sur les points de division par 5. Cet argument ne s'applique pas pour $p = 5$: certaines des E_n peuvent ne pas être semi-stables en 5. Mais, pour $n \to \infty$, les E_n tendent 5-adiquement vers E (en un sens évident), et comme E est semi-stable en 5, il en est de même des E_n pour n assez grand.

Ainsi, on peut choisir un n tel que E_n soit semi-stable. Vu (i), on peut appliquer la prop. 2 à E_n. Donc E_n est modulaire, et il en est *a fortiori* de même de $\overline{\rho}_{E_n,5}$. Comme $\overline{\rho}_{E,5}$ est isomorphe à $\overline{\rho}_{E_n,5}$, cela démontre la proposition.

COROLLAIRE.— *La courbe E est modulaire.*

Cela résulte de la proposition, combinée au corollaire au th. 3.

Ce corollaire, joint à la prop. 2, achève la démonstration de la conjecture de Taniyama-Weil dans le cas semi-stable.

BIBLIOGRAPHIE

[1] A.O.L. ATKIN et J. LEHNER - *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134-160.

[2] S. BOSCH, W. LÜTKEBOHMERT et M. RAYNAUD - *Néron Models*, Springer-Verlag, 1990.

[3] H. CARAYOL - *Sur les formes modulaires p-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. E.N.S. **19** (1986), 409-468.

[4] H. CARAYOL - *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. **59** (1989), 785-801.

[5] R.F. COLEMAN et J.F. VOLOCH - *Companion forms and Kodaira-Spencer theory*, Invent. math. **110** (1992), 263-281.

[6] H. DARMON - *The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$*, Intern. Math. Research Notices (1993), 263-274.

[7] H. DARMON, F. DIAMOND et R. TAYLOR - *Fermat's Last Theorem*, Current Developments in Math. 1995, International Press, Cambridge MA.

[8] P. DELIGNE - *Formes modulaires et représentations ℓ-adiques*, Sém. Bourbaki 1968/69, Exposé 355, Lect. Notes in Math. **179** (1971), 139-172.

[9] P. DELIGNE et J.-P. SERRE - *Formes modulaires de poids* 1, Ann. Sci. E.N.S. **7** (1974), 507-530 (= J.-P. Serre, *Oe.* 101).

[10] F. DIAMOND - *On deformation rings and Hecke rings*, Ann. of Math., à paraître.

[11] F. DIAMOND - *The refined conjecture of Serre*, Conference on Elliptic Curves, Hong-Kong 1993, International Press, Cambridge MA (1995), 22-37.

[12] B. EDIXHOVEN - *The weight in Serre's conjectures on modular forms*, Invent. math. **109** (1992), 563-594.

[13] M. EICHLER - *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Archiv der Mat. **5** (1954), 355-366.

[14] G. FALTINGS - *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. math. **73** (1983), 349-366 ; *Erratum, ibid.* **75** (1984), 381.

[15] G. FREY - *Links between solutions of* $A - B = C$ *and elliptic curves*, Lect. Notes in Math. **1380** (1989), 31-62.

[16] B.H. GROSS - *A tameness criterion for Galois representations associated to modular forms* mod p, Duke Math. J. **61** (1990), 445-517.

[17] J.-I. IGUSA - *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. **81** (1959), 561-577.

[18] N. KATZ - *p-adic properties of modular schemes and modular forms*, Lect. Notes in Math. **350** (1973), 69-190.

[19] R.P. LANGLANDS - *Modular forms and* ℓ*-adic representations*, Lect. Notes in Math. **349** (1973), 361-500.

[20] R.P. LANGLANDS - *Base change for* GL(2), Ann. of Math. Studies **96**, Princeton Univ. Press, Princeton, 1980.

[21] B. MAZUR - *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33-186.

[22] B. MAZUR - *Deforming Galois representations*, in : Galois groups over $\mathbf{Q}$, Y. Ihara, K. Ribet, J.-P. Serre, edit., Springer-Verlag, 1989, 385-437.

[23] J. OESTERLÉ - *Nouvelles approches du "théorème" de Fermat*, Sém. Bourbaki 1987/88, exposé 694, Astérisque **161-162**, S.M.F. (1988), 165-186.

[24] J. OESTERLÉ - *Le problème de Gauss sur le nombre de classes*, L'Ens. Math. **34** (1988), 43-67 (noter que $h(-43) = h(-67) = 1$).

[25] K.A. RIBET - *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. math. **100** (1990), 431-476.

[26] K.A. RIBET - *Report on* mod ℓ *representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Proc. Symp. Pure Math. **55**, A.M.S. (1994), vol. 2, 639-676.

[27] J.-P. SERRE - *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Sém. Delange-Pisot-Poitou 1969/1970, exposé 19 (= *Oe.* 87).

[28] J.-P. SERRE - *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. math. **15** (1972), 259-331 (= *Oe.* 94).

[29] J.-P. SERRE - *Lettre à J.-F. Mestre*, Contemp. Math. **67**, A.M.S. (1987), 263-268.

[30] J.-P. SERRE - *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179-230.

[31] G. SHIMURA - *Correspondances modulaires et les fonctions* ζ *de courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1-28.

[32] G. SHIMURA - *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan **11**, Princeton Univ. Press, 1971.

[33] Y. TANIYAMA - *Problem* 12, in : "Some unsolved problems in mathematics", polycopié, Tokyo-Nikko, 1955.

[34] R. TAYLOR et A. WILES - *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553-572.

[35] J. TUNNELL - *Artin's conjecture for representations of octahedral type*, Bull. A.M.S. **5** (1981), 173-175.

[36] A. WEIL - *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149-156 (= *Oe. Sci.* [1967a]).

[37] A. WILES - *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443-551.

Jean-Pierre SERRE

Collège de France
3, rue d'Ulm
75005 PARIS