Autour de la conjecture ε de Serre

M. Tibouchi

29 novembre 2006

Résumé

On se propose de présenter, à un niveau aussi élémentaire que possible, un certain nombre des idées intervenant dans la preuve par Mazur et Ribet de la conjecture ε de Serre, ingrédient important de la preuve par Wiles du grand théorème de Fermat. Bien que sans rapport direct avec d'autres résultats plus récents que l'auteur a pu étudier au cours de son stage de M2, on espère que ce sujet fournit une illustration concrète et motivée, dans des situations simples, de thèmes tels que celui du lien entre la mauvaise réduction de représentations galoisiennes attachées à une variété et les singularités de ses modèles locaux.

1 La courbe elliptique de Frey

Une idée essentielle qui a mené à la démonstration du grand théorème de Fermat est celle d'un lien, suggéré par Gerhard Frey au milieu des années 1980 [4], entre ce théorème et un certain nombre de conjectures au sujet de la modularité des courbes elliptiques. Une large part de cet exposé va consister à expliciter ce lien.

Supposons donnée une solution non triviale (a, b, c) en nombres entiers de l'équation de Fermat :

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

avec p premier fixé $\geqslant 5$, et sans perte de généralité $a \equiv -1 \pmod 4$ et b pair. On considère alors la courbe algébrique d'équation :

$$E_{A,B,C} : y^2 = x(x - A)(x + B) \quad \text{avec } (A, B, C) = (a^p, b^p, c^p) \tag{1}$$

(ou plutôt son adhérence dans le plan projectif). Une telle courbe de degré trois sans point double a la propriété qu'une droite qui la coupe en deux points la recoupe exactement en un troisième, ce qui permet[1] de munir l'ensemble des points (par exemple à coordonnées dans $\mathbf{C}$, noté $E_{A,B,C}(\mathbf{C})$) de la courbe d'une

[1]Précisément, pour former la somme de deux points M et N, on construit le troisième point d'intersection P de la droite (MN) avec la courbe, et $M+N$ est alors le troisième point d'intersection de la droite (OP) avec la courbe, où O est l'origine qu'on a choisie. La définition et la commutativité sont claires, l'associativité un peu moins.

loi de groupe (une fois qu'on a choisi une origine, ici le point à l'infini O). La courbe $E_{A,B,C}$, munie de sa loi de groupe, est ce que l'on appelle une courbe elliptique.

La théorie classique des fonctions elliptiques (ou éventuellement des arguments plus généraux faciles sur les groupes de Lie commutatifs[2]) montre qu'il existe un isomorphisme de groupes (et même de groupes de Lie complexes) entre $E_{A,B,C}(\mathbf{C})$ et un quotient de la forme $\mathbf{C}/\Lambda_E$, ou $\Lambda_E = \mathbf{Z} \oplus \omega_E \mathbf{Z}$ est un certain réseau de $\mathbf{C}$. En particulier, l'ensemble des points $P \in E_{A,B,C}(\mathbf{C})$ tels que $nP = O$ pour un certain $n \geqslant 1$ est un sous-groupe $E_{A,B,C}[n]$ vérifiant :

$$E_{A,B,C}[n] \cong \frac{1}{n}\Lambda_E/\Lambda_E \cong (\mathbf{Z}/n\mathbf{Z})^2$$

Remarquons alors que la loi de groupe est définie sur $\mathbf{Q}$, au sens où les coordonnées de la somme de deux points sont une fraction rationnelle à coefficients dans $\mathbf{Q}$ des coordonnées des points. Il en résulte que les points de ce sous-groupe $E_{A,B,C}[n]$ sont à coefficients algébriques. On peut donc considérer l'action du groupe de Galois $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) = G_{\mathbf{Q}}$ sur $E_{A,B,C}[n]$, qui est compatible avec la loi de groupe, toujours parce que cette dernière est définie sur $\mathbf{Q}$. Toute la construction que l'on vient d'effectuer aboutit donc à une *représentation galoisienne* :

$$\rho_n : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(E_{A,B,C}[n]) = \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$$

L'observation de Frey est que cette représentation galoisienne, pour $n = p$, possède des propriétés surprenantes, qui contredisent notamment une certaine conjecture formulée par Serre dans l'article [7] (sous le nom «conjecture» et pas seulement «question»). Tâchons tout d'abord de détailler ces propriétés surprenantes, qui sont de nature locale.

2 Réduction des courbes elliptiques et conducteur

Soit k un corps quelconque, et $E : y^2 = x^3 + ax + b$ une cubique plane sur k. C'est une courbe elliptique dès qu'elle est sans point double, ce qui revient à la non-nullité du discriminant $16(4a^3 + 27b^2)$. Réciproquement, en caractéristique différente de 2 et 3, toute courbe elliptique a une équation de cette forme (il faut admettre une forme un peu plus générale en caractéristiques 2 et 3).

Dans le cas où le discriminant s'annule, on peut séparer deux cas : celui où la courbe a des tangentes distinctes au point double (le cas *semi-stable*), et celui

[2]En effet, $E_{A,B,C}(\mathbf{C})$ est un groupe de Lie commutatif compact de dimension complexe 1. L'application exponentielle $\exp_E : \mathbf{C} \to E_{A,B,C}(\mathbf{C})$ est donc un morphisme de groupes, qui est un isomorphisme local en 0, donc partout. Son image est donc un sous-groupe ouvert, et par conséquent fermé, de $E_{A,B,C}(\mathbf{C})$, qui est connexe (par exemple parce que la fonction coordonnée y est un revêtement à deux feuillets $E_{A,B,C} \to \mathbf{P}^1$ ramifié en quatre points, et les feuillets se recollent aux points de ramification). Donc $\exp_E$ est surjectif, et son noyau est par ailleurs un sous-groupe discret (par isomorphisme local en 0) et visiblement cocompact de $\mathbf{C}$, c'est-à-dire un réseau.

où il y a une tangente double. L'ensemble des points de la courbe autre que le point double forme alors un groupe, qui est isomorphe à une forme du groupe multiplicatif de k (c'est-à-dire un groupe algébrique qui devient isomorphe au groupe multiplicatif après extension des scalaires convenable) dans le premier cas, et au groupe additif dans le second.

Considérons maintenant une courbe elliptique $E/\mathbf{Q}$. On peut en donner une équation à coefficients dans $\mathbf{Z}$, et la question a alors un sens de savoir ce que devient E quand on la réduit modulo un nombre premier p. La courbe réduite $\tilde{E}$ peut rester une courbe elliptique, ou bien acquérir un point double, à tangentes distinctes ou non. La situation ne dépend toutefois pas seulement de E, mais de l'équation particulière dont on est parti. Il faudrait disposer d'un modèle privilégié $E_{\mathbf{Z}_{(p)}}$ de E sur le localisé $\mathbf{Z}_{(p)}$ en (p) de $\mathbf{Z}$ pour s'affranchir de ce problème : il se trouve qu'un tel modèle existe bien et correspond à une équation de Weierstrass «minimale» qui se calcule explicitement, par un algorithme dû à Tate [8]. Selon la nature de la réduction de $E_{\mathbf{Z}_{(p)}}$ modulo p, on dira que E a *bonne réduction*, *réduction multiplicative* ou *réduction additive* en p. Notons $\Delta_p \in \mathbf{Z}_{(p)}$ le discriminant de $E_{\mathbf{Z}_{(p)}}$. Alors :

$$\Delta(E) = \prod_p p^{v_p(\Delta_p)}$$

est appelé *discriminant minimal* de E. C'est une mesure de la mauvaise réduction de E, et il se trouve que c'est effectivement le discriminant de E pour une certaine équation de Weierstrass, mais c'est un fait particulier au corps $\mathbf{Q}$ (il ne subsiste pas dans un corps de nombre de nombre de classes plus grand que 1). On pose en outre :

$$a_p = p + 1 - E_{\mathbf{Z}_{(p)}}(\mathbf{F}_p)$$

Une autre mesure de la mauvaise réduction est le *conducteur* $N(E)$. C'est un entier naturel que l'on ne définira pas précisément (voir par exemple [9]), mais qui vérifie pour tout p premier :

$$\begin{cases} v_p(N(E)) &= 0 & \text{si } E \text{ a bonne réduction en } p \\ v_p(N(E)) &= 1 & \text{si } E \text{ a réduction multiplicative en } p \\ v_p(N(E)) &\geqslant 2 & \text{si } E \text{ a réduction additive en } p, \text{ avec égalité si } p > 3 \end{cases}$$

Lorsque le conducteur est sans diviseur carré, c'est-à-dire que E a bonne réduction ou au pire réduction multiplicative en chaque nombre premier, on dit que E est *semi-stable*.

Un calcul élémentaire montre alors que, si $E_{A,B,C}$ est la courbe définie en (1), on a :

$$\Delta(E_{A,B,C}) = 2^{-8}(abc)^{2p} \tag{2}$$

$$N(E_{A,B,C}) = \prod_{\ell | abc} \ell \tag{3}$$

En particulier, $E_{A,B,C}$ est semi-stable.

3 Propriétés de la représentation galoisienne associée

Soit ℓ un nombre premier $\geqslant 5$ et ρ_ℓ la représentation galoisienne donnée par les points de ℓ-torsion de la courbe $E_{A,B,C}$. Serre montre dans [7] que ρ_ℓ est absolument irréductible, et par ailleurs :

$$\det \circ \rho_\ell : G_{\mathbf{Q}} \longrightarrow \mathbf{F}_\ell^*$$

est juste le caractère cyclotomique, qui donne l'action de Galois sur les racines ℓ-ièmes de l'unité. Ce dernier point résulte de l'existence de «l'accouplement de Weil»[3]. En particulier, la représentation ρ_ℓ est impaire, au sens où, si $c \in G_{\mathbf{Q}}$ est la conjugaison complexe pour un certain plongement de $\bar{\mathbf{Q}}$ dans $\mathbf{C}$, $\det(\rho_\ell(c)) = -1$.

Venons-en par ailleurs aux propriétés locales de ρ_ℓ. Pour p un nombre premier, fixons v une place de $\bar{\mathbf{Q}}$ au-dessus de p, et notons D_v et I_v le groupe de décomposition et le groupe d'inertie correspondants (qui fixent respectivement les $x \in \bar{\mathbf{Q}}$ tels que $v(x) \geqslant 0$ et $v(x) > 0$). Rappelons que D_v agit naturellement sur le corps résiduel $\kappa(v) \cong \bar{\mathbf{F}}_p$, et que l'on a une suite exacte :

$$1 \to I_v \to D_v \to \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p) \to 1$$

On peut en particulier choisir un relèvement Frob_v à D_v du Frobenius de $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$. On dit que ρ_ℓ est non-ramifié en p lorsque l'image de I_v est triviale (ce qui revient à dire que p est non-ramifié dans l'extension finie $K_\ell/\mathbf{Q}$, où K_ℓ est le corps fixé par $\mathrm{Ker}\,\rho_\ell$). On peut alors définir $\rho_\ell(\mathrm{Frob}_v)$, qui ne dépend du choix de v qu'à conjugaison près.

Il existe une relation entre la ramification de ρ_ℓ et la mauvaise réduction de $E_{A,B,C}$. Tout d'abord, le critère de Néron-Ogg-Shafarevitch [9] affirme que $E_{A,B,C}$ a bonne réduction en $p \neq \ell$ si et seulement si la représentation :

$$\rho_{\ell^\infty} : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) = \mathrm{Aut}(\varprojlim E[\ell^n])$$

est non-ramifiée. Il en résulte que si p ne divise pas $\ell N(E_{A,B,C})$, ρ_ℓ est *a fortiori* non-ramifiée en p. De plus, on a alors[4] :

$$\mathrm{Tr}\,\rho_\ell(\mathrm{Frob}_v) \equiv a_p \pmod{\ell}$$

Mais plus généralement, on sait décrire en termes «géométriques» à quelle condition ρ_ℓ est non-ramifiée en $p \neq \ell$: Serre remarque qu'une conséquence

[3] Ou si l'on préfère, de la dualité de Poincaré. En effet, le module galoisien $E[\ell]$ est, à dualité près, $H^1_{\text{ét}}(E_{\bar{\mathbf{Q}}}, \mathbf{Z}/\ell\mathbf{Z})$, comme on le voit en écrivant la suite exacte longue de cohomologie associée à la suite exacte courte de faisceaux étales $0 \to \mu_\ell \to \mathbf{G}_m \to \mathbf{G}_m \to 0$, et en se rappelant que E est sa propre jacobienne. L'accouplement de Weil est alors le cup-produit intervenant dans la dualité de Poincaré.

[4] Dans l'interprétation cohomologique, cette égalité est simplement la formule de Lefschetz appliquée à la courbe réduite modulo p.

facile de la théorie de la courbe de Tate est que ρ_ℓ est non-ramifiée en $p \neq \ell$ si et seulement si :

$$v_p(\Delta(E_{A,B,C})) \equiv 0 \pmod{\ell}$$

En effet, comme $E_{A,B,C}$ a réduction au plus multiplicative mod p, elle est isomorphe, comme variété analytique en groupes sur $\mathbf{Q}_p^{\mathrm{nr}}$, à une courbe de Tate [9], i.e., il existe un paramètre $q \in \mathbf{Q}_p^{\mathrm{nr}}$ et un isomorphisme Galois-équivariant :

$$\bar{\mathbf{Q}}_p^*/q^{\mathbf{Z}} \longrightarrow E_{A,B,C}(\bar{\mathbf{Q}}_p)$$

Dire que ρ_ℓ est non ramifiée en p (ou, si l'on préfère, en restriction à $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ pour un certain plongement $\bar{\mathbf{Q}} \subset \bar{\mathbf{Q}}_p$) revient à dire que les points de $E_{A,B,C}[\ell]$ sont définis sur $\mathbf{Q}_p^{\mathrm{nr}}$, donc que q a ses racines ℓ-ièmes dans $\mathbf{Q}_p^{\mathrm{nr}}$. La condition est ainsi que la valuation de q soit multiple de ℓ : or cette valuation est la même que celle du discriminant.

Dans le cas qui nous intéresse, on en déduit, d'après les formules (2), que ρ_p est non-ramifiée en dehors de $2p$. De plus, la ramification en p n'est pas méchante : on peut montrer [7] que ρ_p est *finie* en p, i.e. sa restriction à $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ provient d'un schéma en groupes fini et plat de type (p,p) sur $\mathbf{Z}_p$. On tient là une propriété surprenante de ρ_p que l'on évoquait au début : elle est très peu ramifiée.

On conjecture en fait qu'il n'existe pas de représentation galoisienne de dimension 2 sur $\mathbf{F}_p$ qui soit absolument irréductible, impaire, non-ramifiée en dehors de $2p$ et finie en p, mais ce n'est pas encore prouvé à ma connaissance. En revanche, Ribet a pu montrer qu'il n'existait pas de telle représentation qui soit en outre *modulaire*.

4 Questions de modularité

Soit $X_0(N)$ la courbe modulaire de niveau N. Sur $\mathbf{C}$, il s'agit de la surface de Riemann qui compactifie naturellement l'espace $\Gamma_0(N) \setminus \mathcal{H}$, où :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}$$

agit sur le demi-plan de Poincaré $\mathcal{H}$ par homographies. Ce n'est autre que l'espace de modules des courbes elliptiques (généralisées) munies d'un sous-groupe d'ordre N. Cette interprétation modulaire assure que $X_0(N)$ est bien définie sur $\mathbf{Q}$ (en fait $\mathrm{Spec}\,\mathbf{Z}[1/N]$), et Katz et Mazur [5] ont montré comment en donner une définition convenable sur $\mathrm{Spec}\,\mathbf{Z}$.

On appelle forme modulaire parabolique de poids 2 toute forme différentielle holomorphe sur $X_0(N)(\mathbf{C})$. L'espace $S(N)$ de ces formes modulaires est donc un $\mathbf{C}$-espace vectoriel de dimension $g(N)$, le genre de $X_0(N)$. Il est muni de l'action d'une famille d'opérateurs T_n, $n \geqslant 1$, appelés opérateurs de Hecke, qui ont une interprétation géométrique (ils proviennent de correspondances algébriques sur la jacobienne) et peuvent être définis en termes du développement de Fourier des formes modulaires.

La conjecture de Taniyama-Shimura-Weil, que Wiles a montré [10] dans le cas semi-stable, énonce que toute courbe elliptique $E/\mathbf{Q}$ est modulaire, au sens où il existe une forme modulaire $f \in S(N(E))$, valeur propre pour les opérateurs de Hecke, telle que pour tout p premier ne divisant pas $N(E)$, $T_p(f) = a_p f$. Elle équivaut à l'énoncé que E est un quotient de la jacobienne $J_0(N)$. Si E est modulaire, alors les représentations galoisiennes ρ_n qui lui sont attachées sont modulaires de niveau $N(E)$, au sens suivant.

Soit $\mathbf{T}$ le sous-anneau (commutatif) de $\mathrm{End}_{\mathbf{C}}(S(N))$ engendré par les opérateurs de Hecke. C'est un $\mathbf{Z}$-module libre de rang $g(N)$, et si m est un idéal maximal de $\mathbf{T}$, alors $\mathbf{T}/m$ est en particulier un corps fini k_m, d'une certaine caractéristique ℓ. Un théorème classique de Deligne associe à une telle donnée une représentation galoisienne (bien déterminée d'après le théorème de Čebotarev) :

$$\rho_m : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(k_m)$$

telle que $\det \circ \rho_m$ est le caractère cyclotomique χ_ℓ, qui soit non-ramifiée en dehors de ℓN, et telle que :

$$\mathrm{Tr}\, \rho_m(\mathrm{Frob}_v) = T_p \pmod m \quad \text{pour tout } p \text{ ne divisant pas } \ell N$$

On dit alors qu'une représentation galoisienne :

$$\rho_m : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F})$$

sur un corps fini $\mathbf{F}$ est modulaire de niveau N si elle est isomorphe à une représentation ρ_m.

5 Les résultats de Mazur et Ribet

Le théorème de Fermat découle alors de la conjecture de Taniyama-Shimura-Weil dans le cas démontré par Wiles *via* le résultat suivant, qui est un cas particulier des conjectures énoncées par Serre dans [7] :

Théorème 1 (Mazur-Ribet). *Soit p un nombre premier impair $\geqslant 3$, $\rho : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbf{F}}_p)$ une représentation galoisienne irréductible et modulaire de niveau N, et ℓ un nombre premier divisant exactement N. Si $\ell \neq p$ et ρ est non-ramifiée en ℓ, ou bien si $\ell = p$ et ρ est finie en p, alors ρ est modulaire de niveau N/ℓ.*

En effet, comme la courbe $E_{A,B,C}$ est semi-stable, la représentation ρ_p sur les points de p-torsion est modulaire de niveau $N(E_{A,B,C}) = \prod_{\ell | abc} \ell$. Comme pour chaque ℓ impair différent de p, ρ_p est non ramifiée en ℓ, on peut diviser le niveau par ℓ, et ρ_p est donc modulaire de niveau $2p$. En outre, la représentation est finie en p, donc elle est même modulaire de niveau 2. Mais $X_0(2)$ étant de genre 0, on a $S(2) = 0$, donc il n'existe aucune représentation modulaire de niveau 2. Ainsi, ρ_p n'existe pas et le théorème de Fermat est démontré.

On se propose pour finir de donner des indications sur la preuve [3] d'une partie de ce théorème, due à Mazur, qui correspond au cas où ℓ n'est pas congru

à 0 ou 1 (mod p). Mazur a également traité le cas $\ell = p$, qui présente quelques complications techniques, et Ribet a montré par la suite [6] comment traiter le cas assez différent où $\ell \cong 1 \pmod{p}$.

On se donne donc $\rho : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbf{F}}_p)$ une représentation galoisienne irréductible et modulaire de niveau N, et ℓ un nombre premier divisant exactement N, non congru à 0 ou 1 (mod p). On pose $M = N/\ell$, et l'on suppose par l'absure que ρ *n'est pas* modulaire de niveau M.

On note $X_0(N) = X_0(N)_{\mathbf{Z}_{(\ell)}}$ le modèle de $X_0(N)_{\mathbf{Q}}$ sur $\mathbf{Z}_{(\ell)}$ construit par Katz et Mazur [5] comme espace de modules, et $J_0(N) = J_0(N)_{\mathbf{Z}_{(\ell)}}$ le modèle de Néron sur $\mathbf{Z}_{(\ell)}$ de la jacobienne $J_0(N)_{\mathbf{Q}}$ de $X_0(N)_{\mathbf{Q}}$. C'est en fait vraiment la «jacobienne» de $X_0(N)$ (i.e. la composante de degré 0 du schéma de Picard relatif sur $\operatorname{Spec} \mathbf{Z}_{(\ell)}$). On note enfin $X_0(N)_{\mathbf{F}_\ell}$ et $J_0(N)_{\mathbf{F}_\ell}$ les fibres spéciales, et on définit les mêmes objets au niveau M. D'après Katz et Mazur [5] (et avant eux Deligne et Rapoport [2]), $X_0(N)_{\mathbf{F}_\ell}$ s'écrit comme réunion de deux composantes irréductibles isomorphes à la courbe lisse $X_0(M)_{\mathbf{F}_\ell}$, qui s'intersectent transversalement aux points «supersinguliers» (i.e. aux points qui, dans l'interprétation modulaire, correspondent à des courbes elliptiques E sur $\mathbf{F}_\ell$ telles que $E[\ell](\bar{\mathbf{F}}_\ell) = 0$). Le morphisme de normalisation $X_0(M)_{\mathbf{F}_\ell} \amalg X_0(M)_{\mathbf{F}_\ell} \to X_0(N)_{\mathbf{F}_\ell}$ induit une suite exacte de groupes algébriques sur $\mathbf{F}_\ell$:

$$0 \to T_0(N)_{\mathbf{F}_\ell} \to J_0(N)^0_{\mathbf{F}_\ell} \to J_0(M)^2_{\mathbf{F}_\ell} \to 0$$

où $J_0(N)^0_{\mathbf{F}_\ell}$ est la composante neutre de $J_0(N)_{\mathbf{F}_\ell}$, et $T_0(N)_{\mathbf{F}_\ell}$ est un tore dont le groupe des caractères s'identifie au groupe des diviseurs de degré 0 sur $X_0(M)_{\mathbf{F}_\ell}$ supportés aux points supersinguliers.

L'algèbre de Hecke $\mathbf{T}$ de niveau N, engendrée par les opérateurs de Hecke sur $S(N)$ (ou $\mathrm{End}(J_0(N)_{\mathbf{Q}})$) agit également, par universalité du modèle de Néron, sur $J_0(N)_{\mathbf{Z}_{(\ell)}}$ (et cette action peut d'ailleurs être décrite par des correspondances directement sur $\mathbf{Z}_{(\ell)}$), de manière compatible à la suite exacte précédente. Cela étant, dire que ρ est modulaire de niveau N revient à dire, si l'on précise comment est construite la représentation ρ_m évoquée au paragraphe précédent, qu'il existe un idéal maximal m de $\mathbf{T}$, un plongement de $k = \mathbf{T}/m$ dans $\bar{\mathbf{F}}_p$, un entier $d \geqslant 1$ et un k-espace vectoriel V de dimension 2 muni d'une action de $G_{\mathbf{Q}}$ tels que $\rho = V \otimes_k \bar{\mathbf{F}}_p$, et que $J_0(N)(\bar{\mathbf{Q}})[m]$ (le noyau de m) soit isomorphe à V^d comme $k[G_{\mathbf{Q}}]$-module.

La représentation ρ (donc V) étant non ramifiée en ℓ par hypothèse, il existe un schéma en groupes (ou en fait k-espaces vectoriels) fini étale W sur $\mathbf{Z}_{(\ell)}$ tel que V soit isomorphe, comme $k[G_{\mathbf{Q}}]$-module, à $W(\bar{\mathbf{Q}})$. Si l'on choisit une injection $G_{\mathbf{Q}}$-équivariante $V \hookrightarrow J_0(N)(\bar{\mathbf{Q}})[m]$, elle se prolonge en une immersion $W_{\mathbf{Q}} \hookrightarrow J_0(N)_{\mathbf{Q}}$, et même, par propriété de Néron, en un morphisme $W \to J_0(N)$ (encore injectif car $J_0(N)[p]$, donc $J_0(N)[m]$, sont étales). On peut montrer de plus (en étudiant l'action de l'algèbre de Hecke sur le quotient fini étale $J_0(N)/J_0(N)^0$) que l'image de $W_{\mathbf{F}_\ell}$ tombe dans la composante neutre $J_0(N)^0_{\mathbf{F}_\ell}$. Mais comme ρ n'est pas modulaire de niveau M, l'image dans $J_0(M)^2_{\mathbf{F}_\ell}$ est nécessairement triviale. Il en résulte que l'image de $W_{\mathbf{F}_\ell}$ est en fait dans $T_0(N)_{\mathbf{F}_\ell}$.

Cela fournit des informations importantes sur $\rho(\mathrm{Frob}_\ell)$. En effet, vu son ac-

tion sur les courbes elliptiques supersingulières [8], le Frobenius Frob_ℓ agit sur le groupe $T_0(N)_{\mathbf{F}_\ell}(\bar{\mathbf{F}}_\ell)$ par $-\ell w_\ell$, où w_ℓ est l'involution d'Atkin-Lehner de niveau ℓ. Mais il agit également comme ℓT_ℓ, donc c'est une homothétie. Ainsi $\ell = \det(\rho(\mathrm{Frob}_\ell)) = \rho(\mathrm{Frob}_\ell^2) = \ell^2$, ce qui contredit l'hypothèse selon laquelle $\ell \not\equiv 0$ ou $1 \pmod{p}$. □

Références

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

[2] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math. **349** (1973), 143–316.

[3] B. Edixhoven, *Serre's conjectures*, Modular forms and Fermat's last theorem (G. Cornell, J. H. Silverman, and G. Stevens, eds.), 1997, pp. 209–242.

[4] G. Frey, *Links between solutions of $A-B=C$ and elliptic curves*, J. Indian. Math. Soc. **51** (1987), 117–145.

[5] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. Math. Studies, vol. 108, Princeton University Press, 1985.

[6] K. A. Ribet, *From the Taniyama-Shimura conjecture to Fermat's last theorem*, Ann. Faculté Sci. Toulouse **11** (1990), no. 1, 116–139.

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

[8] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag, 1986.

[9] ———, *A survey of the arithmetic of elliptic curves*, Modular forms and Fermat's last theorem (G. Cornell, J. H. Silverman, and G. Stevens, eds.), 1997, pp. 17–41.

[10] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443–551.