Astérisque

JOSEPH OESTERLÉ

Nouvelles approches du « théorème » de Fermat

Astérisque, tome 161-162 (1988), Séminaire Bourbaki,
exp. nº 694, p. 165-186
<http://www.numdam.org/item?id=SB_1987-1988__30__165_0>

© Société mathématique de France, 1988, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
40ème année, 1987-88, n° 694

Février 1988

NOUVELLES APPROCHES DU "THÉORÈME" DE FERMAT

par Joseph OESTERLÉ

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Ce texte en latin, précédé de la mention : *Observatio Domini Petri de Fermat*, se trouve dans l'édition des oeuvres de Diophante que le fils de Fermat fait paraître en 1670, cinq ans après la mort de son père. Il reproduit selon toute vraisemblance une annotation portée par Fermat dans son propre exemplaire des oeuvres de Diophante (édition de Bachet), aujourd'hui perdu.

Fermat y affirme que pour $n \geq 3$ l'équation

$$x^n + y^n = z^n \tag{1}$$

n'a pas de solutions entières (avec $xyz \neq 0$). Cet énoncé est souvent appelé *le dernier* (ou *le grand*) *théorème de Fermat*. Il est démontré pour $n \leq 150000$ (cf. [T,W]), mais pas dans le cas général. On pourra consulter le livre de Ribenboim [R] comme guide bibliographique sur le sujet.

Pour $n \geq 4$, le genre $\frac{(n-1)(n-2)}{2}$ de la courbe de Fermat est supérieur à 2 et la conjecture de Mordell, démontrée par Faltings en 1983 ([Fa]), implique que (1) n'a qu'un nombre fini de solutions entières primitives.

Les nouvelles approches du théorème de Fermat que nous allons décrire ont pour point de départ commun une remarque de Hellegouarch ([He 1,2,3]), reprise et développée par Frey ([Fr]) :

Soient p un nombre premier ≥ 5 et a,b,c des entiers non nuls premiers entre eux tels que $a^p + b^p + c^p = 0$. Alors la courbe elliptique E sur $\mathbb{Q}$ d'équation

$$y^2 = x(x-a^p)(x+b^p) \tag{2}$$

(où a,b,c sont ordonnés de sorte que b soit pair et a congru à $-1 \bmod 4$) jouit de propriétés qui semblent trop miraculeuses pour que E puisse exister.

En voici quelques exemples :

a) Le discriminant minimal de E, égal à $\frac{(abc)^{2p}}{256}$, est très gros par rapport à son conducteur, égal au produit des nombres premiers qui divisent abc. Cela établit un lien entre le théorème de Fermat et une conjecture de Szpiro.

b) Les points de p-torsion de E sont non ramifiés en dehors de $2p$ et pas trop ramifiés en p. Cela permet de déduire le théorème de Fermat d'une très belle conjecture de Serre, disant que les représentations continues irréductibles de degré 2 et de déterminant impair de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ en caractéristique p doivent provenir de formes modulaires paraboliques modulo p dont on peut préciser le poids, le caractère et le niveau. Cette conjecture est un analogue modulo p de la "philosophie de Langlands". Outre le théorème de Fermat, la conjecture de Serre implique aussi la conjecture de Taniyama-Weil, permet de déterminer tous les schémas en groupes finis et plats de type (p,p) sur $\mathbb{Z}$, etc.

c) Un théorème de Ribet ([Ri]), qui résout partiellement les questions relatives au niveau dans la conjecture de Serre, implique que la courbe elliptique E ne peut être une courbe de Weil. Par conséquent :

THÉORÈME 1 (Ribet).- *La conjecture de Taniyama-Weil* (*cf.* II.4.D) *implique le théorème de Fermat.*

Il semble que Frey ait été le premier à deviner l'existence d'un lien entre ces deux conjectures. Indiquons que la conjecture de Taniyama-Weil n'est qu'un cas particulier des conjectures standard sur le comportement de certaines séries de Dirichlet associées aux variétés algébriques, et que l'on dispose de nombreuses évidences numériques en sa faveur.

I. LA CONJECTURE DE SZPIRO

1. Les courbes elliptiques $E_{a,b,c}$

Soient a,b,c des entiers non nuls premiers entre eux tels que

$$a + b + c = 0 . \tag{3}$$

Notons $E_{a,b,c}$ ou simplement E la courbe elliptique sur $\mathbb{Q}$ d'équation

$$y^2 = (x+b)(x-a)x . \tag{4}$$

Elle est isomorphe à la courbe elliptique d'équation $y^2 = (x-e_1)(x-e_2)(x-e_3)$ pour tout triplet (e_1,e_2,e_3) d'entiers tel que $a = e_2 - e_3$, $b = e_3 - e_1$, $c = e_1 - e_2$. En particulier, $E_{a,b,c}$ ne change pas si a,b,c sont permutés circulairement.

Supposons pour simplifier que l'on ait

$$a \equiv -1 \mod 4 \quad , \quad b \equiv 0 \mod 16 . \tag{5}$$

En effectuant le changement de variables $x = 4X$, $y = 8Y + 4X$, on obtient une nouvelle équation de E à coefficients entiers :

$$Y^2 + XY = X^3 + \frac{b-a-1}{4} X^2 - \frac{ab}{16} X \ . \tag{6}$$

Les invariants c_4, c_6, Δ associés à cette équation de Weierstrass sont (cf. [Ta])

$$c_4 = -(ab+ac+bc) \qquad c_6 = \frac{(b-a)(c-b)(a-c)}{2} \tag{7}$$

$$\Delta = \left(\frac{abc}{16}\right)^2 \ . \tag{8}$$

On a $\mathrm{pgcd}(c_4, \Delta) = 1$. Cela implique que (6) définit un modèle *minimal* de E et que E est une courbe elliptique *semi-stable* (*loc. cit.*) : elle a bonne réduction en un nombre premier ℓ si $\ell \nmid \frac{abc}{16}$, mauvaise réduction de type multiplicatif si $\ell \mid \frac{abc}{16}$. Si n est un entier non nul, notons $\mathrm{rad}\, n$ le produit des nombres premiers qui divisent n . Le conducteur de E est alors

$$N = \mathrm{rad}\, \frac{abc}{16} \ . \tag{9}$$

Remarque.- Lorsqu'aucun des trois triplets (a,b,c) , (b,c,a) , (c,a,b) ne vérifie (5), l'équation (4) est minimale et E n'est pas semi-stable en 2 .

2. La conjecture de Szpiro

Étant donnée une courbe elliptique E définie sur $\mathbb{Q}$, nous noterons Δ_E son discriminant minimal et N_E son conducteur : on a $N_E = \mathrm{rad}\, \Delta_E$ si E est semi-stable.

Dans un exposé à Hanovre en 1983, Szpiro formule la conjecture suivante, dont il démontre un analogue dans le cas des corps de fonctions :

CONJECTURE 1 (Szpiro, forme faible).- *Il existe* $\alpha > 0$ *et* $\beta > 0$ *tels que*

$$|\Delta_E| \leq \alpha\, N_E^{\beta} \tag{10?}$$

pour toute courbe elliptique semi-stable E *sur* $\mathbb{Q}$.

Cette conjecture a des conséquences arithmétiques étonnantes :

PROPOSITION 1.- *Admettons la conjecture* 1 *et posons* $\alpha' = 16\alpha^{1/2}$ et $\beta' = \beta/2$. *On a alors*

$$|abc| \leq \alpha' (\mathrm{rad}\, abc)^{\beta'} \tag{11?}$$

pour tout triplet (a,b,c) *d'entiers non nuls premiers entre eux tel que* $a+b+c = 0$ *et* $16 \mid abc$.

On peut permuter a,b,c de sorte que $a \equiv -1 \bmod 4$ et $b \equiv 0 \bmod 16$. L'inégalité (10?) appliquée à la courbe elliptique $E_{a,b,c}$ décrite au n° 1 implique alors (11?).

Remarque (Szpiro).- Sous les mêmes hypothèses, on a

(12?) $$\sup(|a|,|b|,|c|) \leq \alpha''(\mathrm{rad}\ abc)^{\beta''}$$

avec $\alpha'' = 2\alpha^{1/5}$ et $\beta'' = \beta/5$. Cela se déduit de l'inégalité (10?), appliquée aux trois courbes elliptiques obtenues en quotientant $E_{a,b,c}$ par ses sous-groupes d'ordre 2 . Ces courbes elliptiques sont semi-stables, ont le même conducteur que E et leurs discriminants minimaux sont, avec $b' = b/16$,

$$\Delta_1 = -a^4b'c \qquad \Delta_2 = -ab'^4c \qquad \Delta_3 = -ab'c^4 .$$

La relation (11?) signifie que a,b,c ne sont pas tous trois fortement factorisés. Si la conjecture 1 est vraie, l'expression $\dfrac{\log|abc|}{\log(\mathrm{rad}\ abc)}$, où a,b,c sont comme dans la prop. 1, est majorée. La plus grande valeur connue de cette expression est 4,1075... et provient d'un exemple de Xiao Gang :

$$3^{11}.5^4 + 7.11^6.43 = 2^{17}.17^3 .$$

COROLLAIRE.- *Admettons la conjecture* 1. *Alors, le théorème de Fermat est vrai pour les exposants assez grands.*

Si x,y,z sont des entiers tels que $x^n+y^n = z^n$, $xyz \neq 0$ et $\mathrm{pgcd}(x,y,z) = 1$, les entiers $a = x^n$, $b = y^n$ et $c = -z^n$ satisfont aux hypothèses de la prop. 1 et l'on a $\mathrm{rad}\ abc \leq |xyz|$, d'où $|xyz|^n \leq \alpha'|xyz|^{\beta'}$. Pour n assez grand, c'est absurde.

Dans la conjecture 1, on ne peut prendre $\beta = 6$. Considérons en effet les suites (a_n) , (b_n) , (c_n) définies par

$$a_0 = 16 \qquad b_0 = 1 \qquad c_0 = -17$$

$$a_{n+1} = 4a_nb_n \quad b_{n+1} = (a_n - b_n)^2 \quad c_{n+1} = -(a_n+b_n)^2$$

et posons $\lambda_n = |a_nb_nc_n|/(\mathrm{rad}(a_nb_nc_n))^3$. Pour tout $n \geq 0$, le triplet (a_n,b_n,c_n) vérifie les hypothèses de la prop. 1. On démontre facilement l'inégalité $\lambda_{n+1} \geq 4\lambda_n$ pour $n \geq 0$. On a donc $\lim_{n\to\infty} \lambda_n = +\infty$, de sorte que l'on ne peut prendre $\beta' = 3$ dans (11?), ni $\beta = 6$ dans (10?). (cf. [M] et [S,T] pour des résultats plus précis de ce type.)

En ce sens, la forme suivante de la conjecture de Szpiro est la plus optimiste possible.

CONJECTURE 2 (Szpiro, forme forte).- *Pour tout* $\varepsilon > 0$, *il existe* $C(\varepsilon) > 0$ *tel que*

(13?) $$|\Delta_E| \leq C(\varepsilon)\ N_E^{6+\varepsilon}$$

pour toute courbe elliptique semi-stable E *sur* $\mathbb{Q}$.

3. La conjecture abc

La conjecture abc est née d'une discussion entre Masser et l'auteur de cet exposé en 1985 :

CONJECTURE 3.- *Pour tout* $\varepsilon > 0$, *il existe* $C(\varepsilon) > 0$ *tel que*

(14?) $$\sup(|a|,|b|,|c|) \leq C(\varepsilon)(\mathrm{rad}\ abc)^{1+\varepsilon}$$

pour tout triplet (a,b,c) *d'entiers non nuls premiers entre eux vérifiant* $a+b+c=0$.

L'énoncé analogue où $1+\varepsilon$ est remplacé par $\frac{6}{5}+\varepsilon$ est impliqué par la conjecture 2. (Raisonner comme en haut de la page 6 pour se ramener au cas où $16|abc$, puis appliquer la remarque du n° 2.)

L'analogue de la conjecture 3 pour les corps de fonctions est connu, et très utile à l'étude des équations diophantiennes sur ces corps (cf. [Ms]). En voici un cas particulier :

THÉORÈME 2.- *Soient* k *un corps et* P,Q,R *trois polynômes non nuls de* $k[X]$, *premiers entre eux, tels que* $P+Q+R=0$, *dont l'un au moins a une dérivée* $\neq 0$. *Soit* s *le nombre de racines distinctes de* PQR *dans une clôture algébrique de* k . *On a alors*

(15) $$\sup(\deg P, \deg Q, \deg R) < s .$$

Posons $D = \begin{vmatrix} P & Q \\ P' & Q' \end{vmatrix}$. On a $D = \begin{vmatrix} R & P \\ R' & P' \end{vmatrix}$ et les hypothèses du théorème impliquent que le polynôme D est non nul. On a $\deg D < \deg P + \deg Q$. Par ailleurs, si $x \in \bar{k}$ est une racine de multiplicité m de P , de Q ou de R , c'est une racine de multiplicité $\geq m-1$ de D . On a donc $\deg D \geq \deg P + \deg Q + \deg R - s$. En comparant les inégalités obtenues, on trouve $\deg R < s$. On a de même $\deg P < s$ et $\deg Q < s$, d'où le théorème.

Démontrons que la conjecture 3 équivaut aux deux conjectures suivantes sur les courbes elliptiques :

CONJECTURE 4.- *Pour tout* $\varepsilon > 0$, *il existe* $C(\varepsilon) > 0$ *possédant la propriété suivante : pour toute courbe elliptique* E *sur* $\mathbb{Q}$, *les invariants* c_4 *et* c_6 *associés à un modèle minimal de* E (cf. [Ta]) *et le conducteur* N *de* E *vérifient*

(16?) $$\sup(|c_4|^3, |c_6|^2) \leq C(\varepsilon)\ N^{6+\varepsilon} .$$

CONJECTURE 4'.- *Même énoncé que la conjecture* 4, *mais en se restreignant aux courbes elliptiques* E *semi-stables.*

(On notera que la conjecture 4 implique la conjecture 2, même sans y supposer E semi-stable, en vertu de l'égalité $1728\ \Delta_E = c_4^3 - c_6^2$.)

Conjecture 4 $\Rightarrow$ Conjecture 4' : C'est clair.

Conjecture 4' $\Rightarrow$ Conjecture 3 : Admettons la conjecture 4'. On prouve alors

(14?) lorsque 16 divise abc par une démonstration analogue à celle de la prop. 1. Le cas où $4 \mid abc$, puis le cas général, s'en déduisent en choisissant b pair et en écrivant l'inégalité (14?) pour le triplet $(4ab\ ,\ (a-b)^2\ ,\ -(a+b)^2)$.

Conjecture 3 $\Longrightarrow$ Conjecture 4 (d'après les idées d'Hindry) : Admettons la conjecture 3. Soient E, c_4, c_6, N comme dans l'énoncé de la conjecture 4, et soit Δ le discriminant minimal de E. On a $c_4^3 - c_6^2 = 1728\Delta$. Posons $d = \mathrm{pgcd}(c_4^3\ ,\ c_6^2\ ,\ 1728\Delta)$, $a = c_4^3/d$, $b = c_6^2/d$, $c = -1728\Delta/d$. Appliquant (14?) à (a,b,c), on obtient :

$$\sup(|c_4|^3, |c_6|^2) \leq C(\varepsilon)\ M^{1+\varepsilon} \tag{17?}$$

où l'on a posé $M = d\ \mathrm{rad}(1728\ \Delta c_4^3 c_6^2/d^3)$. On vérifie place par place, en étudiant les divers types possibles de réduction de E, que M divise $6\,c_4\,c_6\,N$. On déduit alors facilement de (17?) que $|c_4|^3$ et $|c_6|^2$ sont majorés par $(C(\varepsilon)\,(6N)^{1+\varepsilon})^{6/(1-5\varepsilon)}$, ce qui prouve la conjecture 4.

4. Les théorèmes d'Hindry et Silverman ([H,S])

La conjecture de Szpiro suggère qu'un invariant d'une courbe elliptique E sur $\mathbb{Q}$ intéressant à considérer est le nombre

$$\beta_E = \frac{\log|\Delta_E|}{\log N_E}\ . \tag{18}$$

C'est effectivement le cas, comme le montrent les deux théorèmes suivants :

THÉORÈME 3 ([H,S], th. 0.3).- *La hauteur de Néron-Tate (relative au diviseur* (0) *) des points de* $E(\mathbb{Q})$ *qui ne sont pas de torsion est minorée par* $c(\beta_E)\ \log|\Delta_E|$ *où* $c(\beta_E) = (20\,\beta_E)^{-8}\ 10^{-1,1-4\beta_E}$.

THÉORÈME 4 ([H,S], th. 0.7).- *Le nombre de points entiers de* E *(dans un modèle minimal) est majoré par* $c^{(1+r)\beta_E}$, *où* c *est une constante indépendante de* E *et* r *le rang du* $\mathbb{Z}$*-module* $E(\mathbb{Q})$.

Remarques.- 1) Si les β_E sont majorés indépendamment de E, les théorèmes 3 et 4 répondent positivement à des conjectures de Lang ([La], p. 92 et 132). Tel est le cas en particulier si la conjecture abc est vraie.

2) Hindry et Silverman généralisent les théorèmes 3 et 4 au cas où $\mathbb{Q}$ est remplacé par un corps de nombres K. Ils posent dans ce cas $\beta_E = \dfrac{\log N_{K/\mathbb{Q}}(\Delta_E)}{\log N_{K/\mathbb{Q}}(N_E)}$ (avec $\beta_E = 1$ par convention si le dénominateur est nul). Ils majorent également $|E(K)_{\mathrm{tors}}|$ en fonction de β_E et $[K:\mathbb{Q}]$. (Pour $K = \mathbb{Q}$, on a mieux : Mazur ([Ma 2], th. 8) a démontré que $E(\mathbb{Q})$ a au plus 16 points de torsion.) Des résultats voisins ont été obtenus par Frey et explicités par Mme Flexor ([Fl]).

3) Supposons que le degré d'une paramétrisation de Weil (au sens de [Ma 1]) d'une courbe elliptique par $X_0(N)$ soit majoré par N^c, où c est une constante

absolue. Alors les β_E sont majorés pour les courbes elliptiques E sur $\mathbb{Q}$ qui sont de Weil (donc conjecturalement toutes).

5. D'autres conjectures

Je renvoie au séminaire de géométrie algébrique 1987 de Szpiro pour l'étude de diverses conjectures qui impliquent la conjecture 1 :

- énoncés du type "conjecture des petits points" de [Sz] ;
- versions effectives de la conjecture de Mordell ;
- analogues arithmétiques des inégalités de Bogomolov - Miyaoka - Yau.

Par ailleurs, Vojta a publié un livre ([Vo]) dans lequel il formule des conjectures très générales concernant les hauteurs des points de variétés algébriques définies sur les corps de nombres. Ces conjectures sont inspirées par des analogies avec la théorie de Nevanlinna. Elles impliquent la conjecture abc .

II. LA CONJECTURE DE SERRE

1. Représentations galoisiennes

Soient $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ son groupe de Galois et F un corps de caractéristique $\ell > 0$. Considérons une représentation

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F) .$$

Supposons que ρ soit *continue*, c'est-à-dire se factorise par $\mathrm{Gal}(K/\mathbb{Q})$, où K est une extension galoisienne finie de $\mathbb{Q}$. L'ensemble S des nombres premiers p en lesquels ρ est ramifiée est fini. À tout $p \notin S$ correspond un élément de Frobenius $\rho(\mathrm{Frob}_p)$ de $\mathrm{Im}\,\rho$, bien défini à conjugaison près. Posons

$$(19) \qquad \begin{cases} a_p = \mathrm{Tr}\,\rho(\mathrm{Frob}_p) \\ \omega(p) = \det \rho(\mathrm{Frob}_p) \end{cases} \qquad (\text{pour } p \notin S) .$$

PROPOSITION 2.- *La connaissance des* a_p *et des* $\omega(p)$ *pour presque tout* p *(ou même seulement pour un ensemble de nombres premiers* p *de densité* 1 *) détermine* ρ *à semi-simplification près.*

En effet, la connaissance de ces a_p et $\omega(p)$ détermine, d'après le théorème de Cebotarev, le polynôme caractéristique de la matrice $\rho(g)$ pour tout $g \in G_{\mathbb{Q}}$.

On définit le *conducteur* de ρ par une formule analogue à celle utilisée pour définir le conducteur d'Artin en caractéristique 0 , à cela près que l'on se restreint aux places premières à ℓ : pour tout nombre premier $p \neq \ell$, on choisit un prolongement à $\bar{\mathbb{Q}}$ de la valuation p-adique de $\mathbb{Q}$, on note $(G_i)_{i\geq 0}$ la suite des sous-groupes de ramification de $\mathrm{Im}\,\rho$ correspondants (égaux à $\{0\}$ pour i assez grand), d_i la dimension du sous-espace fixé par $\rho(G_i)$, et

l'on pose

$$n(p,\rho) = \sum_{i=0}^{\infty} [G_0:G_i]^{-1} (2-d_i) .$$

On a $n(p,\rho) = 0$ si et seulement si ρ est non ramifiée en p. Le conducteur de ρ est alors

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

Le caractère $\det\rho : G_{\mathbb{Q}} \longrightarrow F^\times$ est d'ordre premier à ℓ. Son conducteur (au sens usuel) divise ℓN : cela se voit en comparant les formules donnant les conducteurs de ρ et $\det\rho$. On en déduit, grâce à la théorie du corps de classes, qu'il existe un *caractère de Dirichlet* $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow F^\times$ et un élément h de $\mathbb{Z}/(\ell-1)\mathbb{Z}$ caractérisés par

(21) $$\det\rho(\mathrm{Frob}_p) = p^h\,\varepsilon(p) \qquad (p \not| \ell N) .$$

Si c est la conjugaison complexe relative à un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$, on a

(22) $$\det\rho(c) = (-1)^h\,\varepsilon(-1) .$$

Serre ([Se 3], § 2) associe à ρ un *poids* k qui est un entier ≥ 2 dont la classe modulo $\ell-1$ est $h+1$. La définition de k est trop technique pour être rappelée ici. Signalons simplement que ce poids ne dépend que de la restriction de ρ au groupe d'inertie en p (relatif à un prolongement à $\bar{\mathbb{Q}}$ de la valuation p-adique de $\mathbb{Q}$).

Exemple.- Soit E une courbe elliptique semi-stable définie sur $\mathbb{Q}$. Soient ℓ un nombre premier et $\rho_\ell : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_\ell)$ la représentation galoisienne fournie par les points de ℓ-torsion de E. Le déterminant de ρ_ℓ est le caractère cyclotomique $\chi_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_\ell^\times$ qui donne l'action de $G_{\mathbb{Q}}$ sur les racines ℓ-ièmes de l'unité : cela résulte des propriétés de l'accouplement de Weil. On a $\chi_\ell(\mathrm{Frob}_p) = p$ pour $p \neq \ell$ et $\chi_\ell(c) = -1$. Le caractère ε associé à ρ_ℓ est le caractère trivial. Le conducteur de ρ_ℓ divise celui de E. Il est égal au produit des nombres premiers $p \neq \ell$ dont l'exposant dans le discriminant minimal Δ de E n'est pas multiple de ℓ : cela résulte de l'étude de la courbe de Tate. Le poids de ρ_ℓ est déterminé par Serre ([Se 3], prop. 5) : il est égal à 2 ou $\ell+1$ suivant que l'exposant de ℓ dans Δ est ou non multiple de ℓ.

2. Représentations modulaires

Soient N un entier ≥ 1, k un entier ≥ 2 et $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ un caractère. Notons $\mathfrak{h}$ le demi-plan de Poincaré et $\Gamma_0(N)$ le sous-groupe de $SL_2(\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \bmod N$.

Rappelons la définition d'une *forme modulaire parabolique de type* (N,k,ε) : c'est une fonction holomorphe f sur $\mathfrak{h}$ telle que

(23) $$f\left(\frac{a\tau+b}{c\tau+d}\right) = \varepsilon(d)\,(c\tau+d)^k\, f(\tau)$$

pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ et $\tau \in \mathfrak{h}$, et qui tend vers 0 aux pointes. Une telle fonction admet un développement en série

(24) $$f = \sum_{n=1}^{\infty} a_n q^n \qquad (\text{avec } q = e^{2\pi i\tau}) .$$

Si f est non nulle, on a

(25) $$\varepsilon(-1) = (-1)^k .$$

L'ensemble $S(N,k,\varepsilon)$ des formes modulaires paraboliques de type (N,k,ε) est un espace vectoriel *de dimension finie* sur $\mathbb{C}$. À chaque nombre premier p tel que $p \nmid N$ correspond un *opérateur de Hecke* T_p dans $S(N,k,\varepsilon)$. Si $f = \Sigma\, a_n q^n$ est un élément de $S(N,k,\varepsilon)$, on a

(26) $$T_p f = \Sigma\, a_{np}\, q^n + \varepsilon(p)\, p^{k-1}\, \Sigma\, a_n\, q^{np} .$$

Les opérateurs de Hecke commutent entre eux. Soit $(a_p)_{p\nmid N}$ un *système de valeurs propres* des T_p, c'est-à-dire une famille de nombres complexes telle que l'intersection des $\mathrm{Ker}(T_p - a_p)$ ne soit pas $\{0\}$. L'anneau R engendré par les a_p et les $\varepsilon(p)$, pour $p \nmid N$, est alors un $\mathbb{Z}$-module de type fini. Soit $a \longmapsto \tilde{a}$ un homomorphisme de R dans un corps F de caractéristique $\ell > 0$. D'après un théorème de Deligne ([D,S], th. 6.7), il existe une représentation continue semi-simple :

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$$

non ramifiée en dehors de ℓN telle que

(27) $$\begin{cases} \mathrm{Tr}\,\rho(\mathrm{Frob}_p) = \tilde{a}_p \\ \det \rho(\mathrm{Frob}_p) = p^{k-1}\,\widetilde{\varepsilon(p)} \end{cases}$$

pour tout nombre premier p tel que $p \nmid \ell N$. Ces propriétés caractérisent ρ à conjugaison près (prop. 2). Il résulte des formules (22), (25), (27) que le caractère $\det \rho$ est *impair*, c'est-à-dire que l'on a

(28) $$\det \rho(c) = -1$$

si $c \in G_{\mathbb{Q}}$ est la conjugaison complexe associée à un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$.

DÉFINITION 1.- *Une représentation continue* $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$ *obtenue de cette façon est dite modulaire de type* (N,k,ε).

3. La conjecture de Serre

Soient ℓ un nombre premier, F un corps de caractéristique ℓ et $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$ une représentation continue de $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Supposons que ρ remplisse les deux conditions suivantes :

a) ρ est absolument irréductible ;

b) le caractère $\det \rho$ est impair, i.e. vérifie (28).

La condition b) équivaut à dire que la matrice $\rho(c)$ est conjuguée à la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Lorsque $\ell \neq 2$, une représentation irréductible qui remplit la condition b) est absolument irréductible.

CONJECTURE 5 (Serre, forme faible).- *Sous les hypothèses précédentes, il existe des entiers* $N \geq 1$, $k \geq 2$ *et un caractère* $\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ *tels que* ρ *soit modulaire de type* (N,k,ε_0) *au sens de la déf.* 1.

C'est l'énoncé (3.2.3?) de [Se 3].

Remarque 1.- Cette conjecture implique que ρ se relève en une représentation λ-adique en caractéristique 0 (*cf.* [D,S]), ce que l'on ne sait pas démontrer.

Reprenons les notations du début de ce numéro. Soient de plus N, k, et $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow F^\times$ le conducteur, le poids et le caractère associés à ρ (*cf.* n° 1). On peut choisir un sous-anneau R de $\mathbb{C}$, un homomorphisme $R \longrightarrow F$ et un caractère $\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow R^\times$ relevant ε et *de même ordre* que ε.

CONJECTURE 6 (Serre, forme forte).- *Avec les notations précédentes,* ρ *est modulaire de type* (N,k,ε_0), *sauf peut-être dans les deux cas suivants :*

a) *On a* $\ell = 2$ *et* ρ *est l'induite d'un caractère de* $G_{\mathbb{Q}(\sqrt{-1})}$.

b) *On a* $\ell = 3$ *et* ρ *est l'induite d'un caractère de* $G_{\mathbb{Q}(\sqrt{-3})}$.

C'est l'énoncé (3.2.4?) de [Se 3], à cela près que a) et b) n'y sont pas exclus. Serre trouve en avril 1987 des exemples qui montrent la nécessité d'exclure a) et b) ([Se 4]). Dans ces exemples, ρ provient d'un système de valeurs propres associé à des formes modulaires en caractéristique ℓ au sens de Katz ([Ka]) de type (N,k,ε), mais ce système n'est pas la réduction mod. ℓ d'un système de valeurs propres intervenant dans $S(N,k,\varepsilon_0)$. Ce phénomène ne se produit pas en dehors des cas a) et b) (Serre, Cours au Collège de France en 1987).

Pour les applications indiquées au numéro suivant, cette modification est sans importance.

Remarque 2.- La conjecture 6 se prête à des vérifications numériques. Mestre les a effectuées dans de nombreux cas particuliers. On en trouve quelques-uns dans [Se 3], § 5.

4. Applications

Les démonstrations sont seulement esquissées. Elles sont détaillées dans [Se 3], § 4.

A) *Le théorème de Fermat*

THÉORÈME 5.- *La conjecture* 6 *implique le théorème de Fermat.*

Si le théorème de Fermat est faux, il existe un nombre premier $\ell \geq 5$ et une solution primitive non triviale de l'équation $A^\ell + B^\ell + C^\ell = 0$. Quitte à

permuter A, B, C, on peut supposer que la courbe elliptique $E_{a,b,c}$ où $a = A^\ell$, $b = B^\ell$, $c = C^\ell$, est semi-stable (I, n° 1). Soit $\rho_\ell : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_\ell)$ la représentation définie par ses points de ℓ-torsion. Serre montre qu'elle est irréductible. Son déterminant est impair et les invariants (N,k,ε_0) associés sont $(2,2,1)$ (*cf.* n° 1, *exemple*). Cela contredit la conjecture 6 car $S(2,2,1)$ est réduit à 0.

La méthode ci-dessus s'applique à d'autres équations de type analogue (*cf.* [Se 3], 4.3).

B) *Discriminants des courbes elliptiques semi-stables*

THÉORÈME 6.- *Admettons la conjecture* 6. *Soit* E *une courbe elliptique semi-stable sur* $\mathbb{Q}$. *Si* $|\Delta_E|$ *est une puissance* m-*ième, on a* $m \leq 5$ *et* E *possède un point d'ordre* m *défini sur* $\mathbb{Q}$.

Le point crucial consiste à montrer que m ne peut être un nombre premier $\ell \geq 11$, ce que Serre déduit de la conjecture 6 appliquée à la représentation fournie par les points de ℓ-torsion de E. Les autres cas sont traités dans [M,O].

Le théorème 6 permet, modulo la conjecture 6, de déterminer la liste des courbes elliptiques sur $\mathbb{Q}$ de conducteur p premier et discriminant $\neq \pm p$. Outre les courbes de Setzer - Neumann d'équation $y^2 = x^3 - 2ux^2 + px$ (pour p de la forme $u^2 + 64$, avec le signe de u choisi de sorte que $u \equiv 1 \bmod 4$), il n'y en a que cinq, de conducteurs 11, 17, 17, 19 et 37.

C) *Schémas en groupes de type* (p,p) *sur* $\mathbb{Z}$

THÉORÈME 7.- *Admettons la conjecture* 6. *Soit* p *un nombre premier* ≥ 3. *Tout schéma en groupes fini et plat de type* (p,p) *sur* $\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$ *ou* $\mu_p \oplus \mu_p$.

À un tel schéma en groupes est associé une représentation $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_p)$. Lorsque ρ est irréductible, Serre montre que $\det \rho : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_p^\times$ est le caractère cyclotomique et que les invariants (N,k,ε_0) associés sont $(1,2,1)$. Cela contredit la conjecture 6 car on a $S(1,2,1) = \{0\}$. Pour ρ réductible, le théorème était connu auparavant, sans admettre la conjecture 6.

D) *La conjecture de Taniyama - Weil*

Soit N un entier ≥ 1. Soit $f = \sum_{n=1}^{\infty} a_n q^n$ une forme modulaire parabolique de type $(N,2,1)$ qui est une *newform* de niveau N au sens d'Atkin - Lehner ([A,L]) et dont les coefficients a_n appartiennent à $\mathbb{Z}$. Soit ω_f la forme différentielle sur la courbe modulaire $X_0(N)$ définie par $f(q)\frac{dq}{q}$. Il existe une courbe elliptique E sur $\mathbb{Q}$ et un morphisme $\varphi : X_0(N) \longrightarrow E$ défini sur $\mathbb{Q}$ tels que $\omega_f = \varphi^*\omega$ pour une forme différentielle ω sur E. Cela caractérise la courbe elliptique E à $\mathbb{Q}$-isogénie près. De plus :

a) La fonction L de Hasse-Weil de E est $\Sigma a_n n^{-s}$.

b) Le conducteur de E (i.e. celui des représentations ℓ-adiques associées à E) est N ([Ca]).

On dit qu'une telle courbe elliptique E est une *courbe de Weil* (faible dans la terminologie de [Ma 1]) associée à f.

Inversement, soit E une courbe elliptique sur $\mathbb{Q}$. Soient N son conducteur et $\sum_{n=1}^{\infty} a_n n^{-s}$ sa fonction L de Hasse-Weil. Si la fonction $f = \sum_{n=1}^{\infty} a_n q^n$ est une forme modulaire de type $(M,2,1)$ pour un entier M convenable, c'est une newform de niveau N et E est une courbe de Weil associée à f : en effet, il existe une newform $g = \Sigma b_n q^n$ de niveau M' divisant M telle que $a_p = b_p$ pour presque tout p. Les courbes de Weil associées à g et la courbe elliptique E ont alors des représentations ℓ-adiques associées isomorphes, donc sont $\mathbb{Q}$-isogènes ([Fa]). Cela implique l'égalité de leurs fonctions de Hasse-Weil et de leurs conducteurs. Vu les assertions a) et b) ci-dessus, on a $g=f$ et $N=M'$.

Weil ([We]) a démontré que pour que la courbe elliptique E soit une courbe de Weil, il faut et il suffit que les séries de Dirichlet $\sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$, pour χ caractère de Dirichlet de conducteur premier à N, admettent un prolongement holomorphe à $\mathbb{C}$ et vérifient un certain type d'équation fonctionnelle. Cela a motivé la conjecture suivante :

CONJECTURE 7 (Taniyama-Weil).- *Toute courbe elliptique sur $\mathbb{Q}$ est une courbe de Weil.*

THÉORÈME 8.- *La conjecture 6 implique la conjecture de Taniyama-Weil.*

Ce théorème a été suggéré à Serre par Colmez.

Principe de la démonstration : Soit E une courbe elliptique sur $\mathbb{Q}$. Soient N son conducteur et $\sum_{n=1}^{\infty} a_n n^{-s}$ sa fonction de Hasse-Weil. La conjecture 6 implique l'existence pour presque tout nombre premier ℓ d'un système $(a_{p,\ell})_{p \nmid N}$ de valeurs propres intervenant dans $S(N,2,1)$ et d'un prolongement v_ℓ à $\bar{\mathbb{Q}}$ de la valuation ℓ-adique de $\mathbb{Q}$ tels que $v_\ell(a_{p,\ell} - a_p) > 0$ pour $p \nmid N$. Comme il n'y a qu'un nombre fini de systèmes de valeurs propres intervenant dans $S(N,2,1)$, $(a_p)_{p \nmid N}$ doit en être un, et cela implique que E est une courbe de Weil.

Serre démontre de façon analogue les généralisations suivantes du th. 8 :

THÉORÈME 9.- *Admettons la conjecture 6. Alors toute variété abélienne A sur $\mathbb{Q}$ à multiplications réelles (cf. [Ri 1]) de dimension n est isomorphe à un quotient de la jacobienne de $X_0(N)$, où N est la racine n-ième du conducteur de A.*

THÉORÈME 10.- *Admettons la conjecture 6. Soit X une variété algébrique projective et lisse sur $\mathbb{Q}$. Soit m un entier impair tel que $H^m(X_{\mathbb{C}},\mathbb{C})$ soit de dimension 2 et de type de Hodge $(m,0)+(0,m)$. Alors les représentations*

ℓ-adiques de $G_{\mathbb{Q}}$ *dans* $H^m(X,\mathbb{Q}_\ell)$ *proviennent d'une forme parabolique de poids* $m+1$ *et caractère* 1 .

III. LE THÉORÈME DE MAZUR - RIBET

Dans ce paragraphe, nous notons $S(N)$ au lieu de $S(N,2,1)$ l'espace vectoriel des formes modulaires paraboliques de type $(N,2,1)$. Nous dirons qu'une représentation galoisienne est *modulaire de niveau* N si elle est modulaire de type $(N,2,1)$ au sens de la déf. 1 de II.2.

1. Énoncé du théorème

Soient F un corps de caractéristique $\ell \geq 3$, N un entier ≥ 1 , et $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$ une représentation continue *irréductible, modulaire de niveau* N . Une telle représentation est absolument irréductible, son déterminant est le caractère cyclotomique $\chi_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_\ell^\times$ (II,2), et elle peut se réaliser sur le sous-corps de F engendré par les traces des éléments de $\operatorname{Im}\rho$ ([D,S], lemme 6.13). Ce sous-corps est fini et nous supposerons dans la suite qu'il est égal à F .

Disons que ρ est *finie* en un nombre premier p s'il existe H , un schéma fini et plat en F-vectoriels sur $\mathbb{Z}_p$ tel que $\rho|_{\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)}$ soit isomorphe à la représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ dans $H(\bar{\mathbb{Q}}_p)$. Lorsque $p \neq \ell$, cela signifie simplement que ρ n'est pas ramifiée en p .

Exemple.- Si ρ est la représentation $G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_\ell)$ fournie par les points de ℓ-torsion d'une courbe elliptique semi-stable E sur $\mathbb{Q}$, ρ est finie en un nombre premier p si et seulement si l'exposant de p dans le discriminant minimal de E est multiple de ℓ .

THÉORÈME 11 (Mazur - Ribet).- *Soit* p *un nombre premier tel que* $p \| N$ (i.e. $p|N$ *et* $p^2 \nmid N$). *Supposons que la représentation* ρ *soit finie en* p *et que l'on ait* $p \not\equiv 1 \bmod \ell$ *ou* $\ell^2 \nmid N$. *Alors* ρ *est modulaire de niveau* N/p .

Cet énoncé est conjecturé par Serre dans [Se 2], même sans supposer $p \not\equiv 1 \bmod \ell$ ou $\ell^2 \nmid N$. Il est à rapprocher des questions relatives au niveau dans la conjecture 6. Le cas où $p \not\equiv 1 \bmod \ell$ est dû à Mazur ([Ma 3]). Le cas où $p \equiv 1 \bmod \ell$ et $\ell^2 \nmid N$ s'avère plus difficile et a été résolu par Ribet ([Ri 2]).

Nous indiquerons aux n°s 3 et suivants les idées principales de la démonstration du th. 11.

2. Conséquences

La première conséquence du th. 11 est le th. 1 : *la conjecture de Taniyama - Weil implique le théorème de Fermat.*

Supposons en effet que le théorème de Fermat soit faux. Considérons alors la représentation ρ_ℓ introduite dans la démonstration du th. 5. Elle est irréductible, et finie en p pour tout $p \neq 2$ (*cf.* n° 1, *exemple*). C'est la représentation définie par les points de ℓ-torsion d'une courbe elliptique semi-stable E sur $\mathbb{Q}$. Si E est une courbe de Weil, ρ_ℓ est modulaire de niveau N, où N est le conducteur de E. Comme N est sans facteurs carrés, une application répétée du th. 11 montre que ρ_ℓ est modulaire de niveau 2. C'est absurde car $S(2)$ est réduit à 0.

La conjecture de Taniyama-Weil implique de même les variantes du théorème de Fermat considérées dans [Se 3], 4.3. Le th. 11 permet aussi de démontrer la conclusion du th. 6 pour les courbes de Weil sans admettre la conjecture 6.

3. Représentations modulaires et algèbres de Hecke

Soit N un entier ≥ 1. À tout nombre premier p correspond un opérateur de Hecke dans $S(N)$, noté T_p si p ne divise pas N, U_p si p divise N : si $f = \Sigma\, a_n q^n$ est un élément de $S(N)$, on a

$$T_p f = \Sigma\, a_{np}\, q^n + p\,\Sigma\, a_n\, q^{np} \qquad (p \nmid N)$$

$$U_p f = \Sigma\, a_{np}\, q^n \qquad (p \mid N)\ .$$

L'algèbre de Hecke $\mathbb{T}(N)$ est le sous-anneau de $\mathrm{End}(S(N))$ engendré par ces endomorphismes. C'est un anneau *commutatif de rang fini* sur $\mathbb{Z}$. Soient m un idéal maximal de $\mathbb{T}(N)$, $k_m = \mathbb{T}(N)/m$ son corps résiduel et ℓ la caractéristique de k_m. En utilisant le fait que l'action de $\mathbb{T}(N)$ dans $S(N)$ est trigonalisable, on déduit du théorème de Deligne cité en II.1 qu'il existe une représentation continue semi-simple $\rho_m : G_{\mathbb{Q}} \longrightarrow GL_2(k_m)$ et une seule à conjugaison près, non ramifiée en dehors de ℓN, telle que l'on ait dans k_m

$$(29) \qquad \begin{cases} \mathrm{Tr}\, \rho_m(\mathrm{Frob}_p) = T_p \\ \det \rho_m(\mathrm{Frob}_p) = p \end{cases} \qquad \text{pour } p \nmid \ell N\ .$$

Pour qu'une représentation continue $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$, où F est un corps de caractéristique $\neq 0$, soit modulaire de niveau N, il faut et il suffit qu'il existe un idéal maximal m de $\mathbb{T}(N)$ tel que ρ et ρ_m soient isomorphes après extension des scalaires.

4. Réalisation géométrique de ρ_m

L'espace vectoriel $S(N)$ est canoniquement isomorphe à celui des formes différentielles holomorphes sur la variété des points complexes de la courbe modulaire $X_0(N)$. Les opérateurs de Hecke dans $S(N)$ proviennent de correspondances sur $X_0(N)$, définies sur $\mathbb{Q}$. Suivant que l'on emploie la fonctorialité

d'Albanese ou de Picard [1], on en déduit deux opérations de $\mathbb{T}(N)$ sur la jacobienne $J_0(N)$ de $X_0(N)$. (Elles coïncident en les T_p, mais pas en les U_p.) Nous choisirons de voir $J_0(N)$ comme $\mathrm{Pic}^0(X_0(N))$, de sorte que l'on a un isomorphisme $S(N) \approx \mathrm{Hom}_{\mathbb{Q}}(\mathrm{Lie}(J_0(N)^\vee), \mathbb{C})$, et choisirons de faire opérer $\mathbb{T}(N)$ sur $J_0(N)$ de façon compatible à cette identification. Il est clair que $\mathbb{T}(N)$ opère *fidèlement* sur $J_0(N)$.

Soit m un idéal maximal de $\mathbb{T}(N)$. Supposons que la représentation ρ_m associée soit *irréductible* et que le corps résiduel k_m de m soit *de caractéristique* $\neq 2$. L'espace V de la représentation ρ_m est un $k_m[G_{\mathbb{Q}}]$-module simple, de dimension 2 sur k_m. L'ensemble $J_0(N)(\bar{\mathbb{Q}})[m]$ des points de $J_0(N)(\bar{\mathbb{Q}})$ annulés par m est un $k_m[G_{\mathbb{Q}}]$-module de longueur finie.

PROPOSITION 3.- *Le semi-simplifié du* $k_m[G_{\mathbb{Q}}]$*-module* $J_0(N)(\bar{\mathbb{Q}})[m]$ *est isomorphe à* V^d *pour un entier* $d \geq 1$ *convenable. Si* ℓ *ne divise pas* N, *on a* $d = 1$.

C'est une généralisation facile de la prop. 14.2 de [Ma 2], où est traité le cas d'un niveau N premier. La première assertion se démontre par une comparaison de traces, en utilisant les relations de congruence d'Eichler - Shimura ; le fait que $\mathbb{T}(N)$ opère fidèlement sur $J_0(N)$ assure que d n'est pas nul. La seconde assertion, plus subtile, repose sur une étude des réductions mod ℓ de $X_0(N)$ et $J_0(N)$ et utilise de façon essentielle le fait que $\mathbb{T}(N)$ contient *tous* les opérateurs de Hecke.

Remarque.- Même lorsque ℓ divise N, on ne connaît pas d'exemple où $d \neq 1$.

5. Réduction modulo p de $J_0(N)$

Soient N un entier ≥ 1 et p un nombre premier tel que $p \| N$. Posons $M = N/p$. Dans ce numéro, nous dressons une liste de résultats sur $J = J_0(N)_{\mathbb{F}_p}$, la réduction modulo p du modèle de Néron de $J_0(N)$. Les ingrédients essentiels pour les démontrer sont la description de la fibre modulo p d'un modèle propre et plat de $X_0(N)$ sur $\mathbb{Z}$ donnée dans [D,R], et un théorème de spécialisation du foncteur de Picard démontré par Raynaud ([Ra], [Gr]).

a) La composante neutre de J est extension d'une variété abélienne A par un tore T.

b) La variété abélienne A est isomorphe à $J_0(M)_{\mathbb{F}_p} \times J_0(M)_{\mathbb{F}_p}$. Si r est un nombre premier tel que $r \nmid N$, l'élément T_r de $\mathbb{T}(N)$ stabilise chacun des facteurs de $A \approx J_0(M)_{\mathbb{F}_p} \times J_0(M)_{\mathbb{F}_p}$ et y opère comme l'élément T_r de $\mathbb{T}(M)$.

[1] Soit $D \subset C \times C'$ une correspondance entre deux courbes projectives et lisses C et C', et soient $p : D \longrightarrow C$ et $q : D \longrightarrow C'$ les projections associées. Nous disons par abus de langage, en considérant la notion de correspondance comme une généralisation de celle de morphisme, que les morphismes de variétés abéliennes $q_*p^* : J(C) \longrightarrow J(C')$ et $p_*q^* : J(C') \longrightarrow J(C)$ sont déduits de la correspondance D par fonctorialité d'Albanese et de Picard respectivement.

c) Le groupe Φ des composantes connexes sur $\bar{\mathbb{F}}_p$ de J est annulé par $T_r - (1+r)$ pour tout nombre premier r tel que $r \nmid N$.

d) Soit $\hat{T}$ le groupe des caractères sur $\bar{\mathbb{F}}_p$ du tore T. Le groupe $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ opère sur $\hat{T}$ via son quotient $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. L'élément de Frobenius Frob_p agit sur $\hat{T}$ comme l'opérateur de Hecke U_p et $\hat{T}$ est annulé par $U_p^2 - 1$.

Soient $\bar{\mathbb{Z}}_p$ la fermeture intégrale de $\mathbb{Z}_p$ dans $\bar{\mathbb{Q}}_p$ et $J_0(N)(\bar{\mathbb{Z}}_p)$ l'ensemble des points du modèle de Néron de $J_0(N)$ à valeurs dans $\bar{\mathbb{Z}}_p$. D'après [Gr], § 5.1, $T(\bar{\mathbb{F}}_p) = \mathrm{Hom}(\hat{T}, \bar{\mathbb{F}}_p^\times)$ se relève de façon naturelle en un sous-groupe de $J_0(N)(\bar{\mathbb{Z}}_p)$, isomorphe à $\mathrm{Hom}(\hat{T}, \bar{\mathbb{Z}}_p^\times)$ comme groupe à opérateurs dans $\mathbb{T}(N)$ et $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Par abus, nous noterons ce sous-groupe $T(\bar{\mathbb{Z}}_p)$.

6. Le théorème de Mazur : principe de la démonstration

Conservons les notations du n° 5. Soient de plus m un idéal maximal de $\mathbb{T}(N)$, k_m son corps résiduel, ℓ la caractéristique de k_m, ρ_m la représentation associée à m (cf. n° 3) et V l'espace de cette représentation. Si L est un $\mathbb{T}(N)$-module, $L[m]$ désigne l'ensemble des éléments de L annulés par m.

Lemme 1.- *Supposons* $\Phi[m] \neq 0$. *Alors* ρ_m *est réductible.*

En effet, d'après le n° 5, c) et la prop. 2, ρ_m est isomorphe à $1 \oplus \chi_\ell$, où $\chi_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_\ell^\times$ est le caractère cyclotomique.

Lemme 2.- *Supposons* $A(\bar{\mathbb{F}}_p)[m] \neq 0$. *Alors* ρ_m *est modulaire de niveau* N/p.

Cela résulte du n° 5, b) et de la prop. 2.

Choisissons un plongement de $\bar{\mathbb{Q}}$ dans $\bar{\mathbb{Q}}_p$, de sorte que $G_{\mathbb{Q}_p} = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ s'identifie à un sous-groupe de $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Lemme 3.- *Supposons que* V *soit isomorphe à un sous-*$k_m[G_{\mathbb{Q}_p}]$*-module de* $T(\bar{\mathbb{Z}}_p)$. *On a alors* $p \equiv 1 \bmod \ell$.

En effet, $G_{\mathbb{Q}_p}$ opère sur $\mathrm{Hom}(\hat{T}/m\hat{T}, \mu_\ell(\bar{\mathbb{Q}}_p))$ et *a fortiori* sur V suivant $\varepsilon\chi_\ell$, où χ_ℓ est le caractère cyclotomique et ε un caractère non ramifié de $G_{\mathbb{Q}_p}$ tel que $\varepsilon^2 = 1$ (n° 5, d)). Par suite, $\det \rho_m$ et χ_ℓ^2 coïncident sur $G_{\mathbb{Q}_p}$. Or $\det \rho_m$ est égal à χ_ℓ (formule (29)). On a donc $\chi_{\ell|G_{\mathbb{Q}_p}} = 1$, d'où $p \equiv 1 \bmod \ell$.

Le th. 11, sous l'hypothèse $p \not\equiv 1 \bmod \ell$, résulte d'après le n° 3 de la proposition suivante :

PROPOSITION 4.- *Supposons que l'on ait* $\ell \neq 2$, *que* ρ_m *soit irréductible, finie en* p *et ne soit pas modulaire de niveau* N/p. *Alors on a* $\hat{T} \neq m\hat{T}$ *et* $p \equiv 1 \bmod \ell$.

Nous ne traiterons que le cas où $p \neq \ell$; le cas où $p = \ell$, plus compliqué techniquement, est analogue dans son principe. D'après la prop. 3, V se réalise comme sous-$k_m[G_{\mathbb{Q}}]$-module de $J_0(N)(\bar{\mathbb{Q}})$. La représentation ρ_m n'est pas ramifiée en p (elle est finie en p , avec $p \neq \ell$). Cela permet, par la propriété universelle des modèles de Néron, de considérer la réduction de V modulo p . L'homomorphisme $V \longrightarrow J(\bar{\mathbb{F}}_p)$ obtenu est injectif car $p \neq \ell$. Son image est contenue dans $T(\bar{\mathbb{F}}_p)$ d'après les lemmes 1 et 2. Comme l'homomorphisme de réduction $T(\bar{\mathbb{Z}}_p)[\ell] \longrightarrow T(\bar{\mathbb{F}}_p)[\ell]$ est bijectif, V est isomorphe à un sous-$k_m[G_{\mathbb{Q}_p}]$-module de $T(\bar{\mathbb{Z}}_p)$. Il est alors clair que l'on a $\hat{T} \neq m\hat{T}$, et le lemme 3 montre que l'on a $p \equiv 1 \bmod \ell$.

Le lemme suivant ne sera utilisé qu'au n° 8.

Lemme 4.- *Supposons que* ρ_m *soit irréductible, que* $\hat{T}/m\hat{T}$ *soit de dimension* ≥ 2 *sur* k_m *et que* ℓ *ne divise pas* $2N$. *On a alors* $p \equiv 1 \bmod \ell$.

Le $k_m[G_{\mathbb{Q}_p}]$-module $J_0(N)(\bar{\mathbb{Q}}_p)[m] = J_0(N)(\bar{\mathbb{Q}})[m]$ est isomorphe à V d'après la prop. 3, donc de dimension 2 sur k_m . Il contient $T(\bar{\mathbb{Z}}_p)[m] = \mathrm{Hom}(\hat{T}/m\hat{T}, \mu_\ell(\bar{\mathbb{Q}}_p))$ qui est par hypothèse de dimension ≥ 2 sur k_m . On a donc $V = T(\bar{\mathbb{Z}}_p)[m]$ et le lemme 3 permet de conclure.

Remarque.- Si l'on a $\ell \neq 2$, $\ell \mid N$, $\ell^2 \nmid N$ et que ρ_m est irréductible et n'est pas modulaire de niveau N/ℓ , Ribet démontre que la conclusion de la prop. 3 reste valable. Il en est alors de même de celle du lemme 4.

7. Courbes de Shimura

Soient p,q deux nombres premiers distincts et $\mathcal{O}$ un ordre maximal d'un corps de quaternions sur $\mathbb{Q}$ ramifié seulement en p et q . Soit M un entier ≥ 1 premier à pq .

À ces données on associe une courbe projective lisse absolument irréductible X sur $\mathbb{Q}$, la *courbe de Shimura* : c'est le schéma grossier de modules qui classe les couples (A,C) , où A est une variété abélienne de dimension 2 sur laquelle opère $\mathcal{O}$, et C un sous-$\mathcal{O}$-module fini monogène d'ordre M^2 de A .

Pour tout nombre premier r ne divisant pas Mpq , on définit une correspondance T_r sur X par

$$T_r(A,C) = \sum_D (A/D\,,\,(C+D)/D)$$

où D parcourt l'ensemble des sous-$\mathcal{O}$-modules finis monogènes d'ordre r^2 de A . Pour tout nombre premier r tel que $r \mid M$, on définit une correspondance U_r sur X par la même formule que la précédente, mais où l'on ne retient que les D tels que $D \cap C = \{0\}$. Enfin on définit une involution U_p sur X par

$$U_p(A,C) = (A/A[\mathfrak{p}]\,,\,(C+A[\mathfrak{p}])/A[\mathfrak{p}])$$

(où $\mathfrak{p}$ est l'unique idéal maximal de $\mathcal{O}$ au-dessus de p) et de façon analogue une involution U_q sur X .

Les endomorphismes de la jacobienne $J(X)$ de X déduits par fonctorialité de Picard de ces correspondances sont encore notés T_r et U_r . Il sont appelés *opérateurs de Hecke* et engendrent un sous-anneau commutatif $\mathbb{T}(X)$ de $\mathrm{End}(J(X))$.

Cerednik et Drinfeld ont décrit la fibre spéciale d'un modèle propre et plat de X sur $\mathbb{Z}_q$. Cela a permis à Ribet, en utilisant le théorème de Raynaud déjà cité au n° 5, d'étudier la réduction $J(X)_{\mathbb{F}_q}$ modulo q du modèle de Néron de $J(X)$, et de mettre en évidence des liens étroits entre $J(X)_{\mathbb{F}_q}$ et $J_0(Mpq)_{\mathbb{F}_p}$. Voici ses résultats, qui précisent des résultats antérieurs de Jordan et Linné ([J,L]) :

a) La composante neutre de $J(X)_{\mathbb{F}_q}$ est un tore. Notons $\hat{T}_{X,q}$ le groupe des caractères de ce tore sur $\overline{\mathbb{F}}_q$.

b) Soit $\hat{T}_{Mpq,p}$ le groupe des caractères sur $\overline{\mathbb{F}}_p$ du sous-tore maximal de $J_0(Mpq)_{\mathbb{F}_p}$. Il existe un homomorphisme de groupes injectif

$$\alpha : \hat{T}_{X,q} \longrightarrow \hat{T}_{Mpq,p}$$

compatible à l'action des opérateurs de Hecke sur ces groupes. (*On dispose même d'un choix canonique de* α , une fois choisis des homomorphismes d'anneaux $\mathcal{O} \longrightarrow \overline{\mathbb{F}}_p$ et $\mathcal{O} \longrightarrow \overline{\mathbb{F}}_q$.) Cela implique que $\mathbb{T}(X)$ est un quotient de l'algèbre de Hecke de $\mathbb{T}(Mpq)$ via lequel $\mathbb{T}(Mpq)$ opère sur $J(X)$.

c) L'assertion b) peut être précisée : soient u,v les morphismes de dégénérescence de $X_0(Mpq)$ dans $X_0(Mp)$ déduits des applications $\tau \longmapsto \tau$ et $\tau \longmapsto q\tau$ du demi-plan de Poincaré dans lui-même. On a une suite exacte

$$0 \longrightarrow \hat{T}_{X,q} \xrightarrow{\alpha} \hat{T}_{Mpq,p} \xrightarrow{\beta} (\hat{T}_{Mp,p})^2 \longrightarrow 0$$

où β est l'homomorphisme déduit par fonctorialité de $(u,v) : X_0(Mpq) \longrightarrow X_0(Mp)^2$.

L'opération de $\mathbb{T}(Mpq)$ sur $(\hat{T}_{Mp,p})^2$ qui en résulte coïncide avec celle de $\mathbb{T}(Mp)$ en ce qui concerne les opérateurs de Hecke d'indice r premier, avec $r \neq q$. Par contre l'opérateur U_q de $\mathbb{T}(Mpq)$ opère matriciellement par

$$U_q = \begin{pmatrix} T_q & -1 \\ q & 0 \end{pmatrix} \tag{30}$$

où T_q est l'opérateur provenant de $\mathbb{T}(Mp)$.

d) Soient $\Phi_{X,q}$ le groupe des composantes connexes sur $\overline{\mathbb{F}}_q$ de $J(X)_{\mathbb{F}_q}$ et Ψ le conoyau de l'endomorphisme $U_q^2 - 1$ de $(\hat{T}_{Mp,p})^2$ (cf. c)). Il existe une application $\mathbb{T}(Mpq)$-linéaire $\Psi \longrightarrow \Phi_{X,q}$ dont le noyau et le conoyau sont annulés par $T_r - (1+r)$ pour tout nombre premier r tel que $r \nmid Mpq$.

Soient m un idéal maximal de $\mathbb{T}(Mpq)$, k_m son corps résiduel et $\rho_m : G_{\mathbb{Q}} \longrightarrow GL_2(k_m)$ la représentation associée.

Lemme 1.- Si ρ_m *n'est pas modulaire de niveau* Mp *, les espaces vectoriels* $\hat{T}_{X,q}/m\hat{T}_{X,q}$ *et* $\hat{T}_{Mpq,p}/m\hat{T}_{Mpq,p}$ *sont de même dimension sur* k_m .

Cela résulte de c) et de ce que, vu l'hypothèse faite, on a $(\hat{T}_{Mp,p})^2 = m(\hat{T}_{Mp,p})^2$.

Lemme 2.- Supposons que ρ_m *soit irréductible. Les conditions suivantes sont équivalentes :*

(i) *On a* $\Phi_{X,q} \neq m\,\Phi_{X,q}$.

(ii) *On a* $(\hat{T}_{Mp,p})^2 \neq m(\hat{T}_{Mp,p})^2$ *et* $U_q^2 - 1 \in m$.

Elles impliquent que ρ_m *est modulaire de niveau* Mp .

L'équivalence de (i) et (ii) est conséquence de d) (démonstration analogue à celle du lemme 1 du n° 5), et la relation $(\hat{T}_{Mp,p})^2 \neq m(T_{Mp,p})^2$ implique que ρ_m est modulaire de niveau Mp , d'après c) et la prop. 2.

8. Le théorème de Ribet : principe de la démonstration

Rappelons l'énoncé du théorème de Ribet (cf. n° 1) :

Soient F *un corps de caractéristique* $\ell \geq 3$, N *un entier* ≥ 1 *non multiple de* ℓ^2 , $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(F)$ *une représentation continue irréductible modulaire de niveau* N . *Soit* p *un nombre premier tel que* $p \,\|\, N$ *et* $p \equiv 1 \bmod \ell$. *Si* ρ *n'est pas ramifiée en* p *, elle est modulaire de niveau* $M = N/p$.

Indiquons les différentes étapes de la démonstration (par l'absurde) :

a) Quitte à diminuer N , on peut supposer que ρ n'est pas modulaire de niveau N' , avec N' un diviseur strict de N .

b) On peut supposer que ρ n'est pas modulaire de niveau Mq , avec q un nombre premier tel que $q \nmid \ell N$ et $q \not\equiv 1 \bmod \ell$, car sinon le théorème de Mazur (prop. 4) permettrait de conclure.

c) La représentation ρ est isomorphe (après extension des scalaires) à une représentation de la forme ρ_{m_0} , où m_0 est un idéal maximal de $\mathbb{T}(N)$ (n° 3). Puisqu'elle n'est pas modulaire de niveau M , on a, avec les notations du n° 7, $\hat{T}_{N,p} \neq m_0\,\hat{T}_{N,p}$ (prop. 4).

d) L'image de ρ_{m_0} contient une matrice conjuguée à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (cf. II.3), et l'on peut choisir, d'après le théorème de Cebotarev, un nombre premier q tel que $q \nmid \ell N$ et que la matrice $\rho_{m_0}(\mathrm{Frob}_q)$ soit conjuguée à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On a alors, d'après la formule (29)

$$T_q \equiv 0 \bmod m_0 \qquad q \equiv -1 \bmod m_0 \tag{31}$$

et en particulier $q \equiv -1 \bmod \ell$.

e) Sur le groupe $(\hat{T}_{N,p})^2$ opèrent d'une part l'algèbre de Hecke $\mathbb{T}(N)$, d'autre part l'algèbre de Hecke $\mathbb{T}(Nq)$ (de la façon décrite au n° 7, c)). Le sous-anneau R de $\mathrm{End}((\hat{T}_{N,p})^2)$ engendré par les images de $\mathbb{T}(N)$ et $\mathbb{T}(Nq)$ est commutatif et entier sur $\mathbb{T}(N)$: en effet il est engendré par l'image de $\mathbb{T}(N)$

et de l'opérateur U_q de $\mathbb{T}(Nq)$ qui, d'après le n° 7, c), commute à $\mathbb{T}(N)$ et satisfait l'équation de dépendance intégrale

$$U_q^2 - T_q U_q + q = 0 \ . \tag{32}$$

D'après c), l'idéal m_0 de $\mathbb{T}(N)$ appartient au support de $(\hat{T}_{N,p})^2$. Il est donc contenu dans un idéal maximal m_1 de R . Soit m l'image réciproque de m_1 dans $\mathbb{T}(Nq)$. C'est un idéal maximal de $\mathbb{T}(Nq)$ qui possède les propriétés suivantes :

- il contient $U_q^2 - 1$ (d'après (31) et (32)) ;
- il appartient au support du $\mathbb{T}(Nq)$-module $(\hat{T}_{N,q})^2$ (par construction) ;
- la représentation ρ_m qui lui est associée est isomorphe à ρ après extension des scalaires (prop. 2).

f) Soit X la courbe de Shimura considérée au n° 7. Employons les notations introduites au n° 7. Les propriétés de m décrites en e) impliquent que l'on a $\Phi_{X,q} \neq m\,\Phi_{X,q}$ (n° 7, *lemme* 2). On en déduit, parce que $\mathbb{T}(Mpq)$ opère dans $J(X)$ par son quotient $\mathbb{T}(X)$, que l'on a $\mathbb{T}(X) \neq m\mathbb{T}(X)$, et donc $J(X)(\bar{\mathbb{Q}})[m] \neq \{0\}$.

g) Le semi-simplifié du $k_m[G_{\mathbb{Q}}]$-module $J(X)(\bar{\mathbb{Q}})[m]$ est isomorphe à V^d , où V est l'espace de la représentation ρ_m et d un entier ≥ 0 : cela résulte, par une démonstration analogue à celle de la prop. 3, des relations d'Eichler-Shimura pour $J(X)$. On a $d \geq 1$ d'après f).

h) D'après g), $J(X)(\bar{\mathbb{Q}})[m]$ contient un sous-$k_m[G_{\mathbb{Q}}]$-module isomorphe à V . On peut prendre sa réduction modulo p parce que la représentation ρ_m n'est pas ramifiée en p , et ce sous-module se réduit injectivement modulo p parce que $\ell \neq p$. Ainsi $J(X)(\bar{\mathbb{F}}_p)[m]$ est de dimension ≥ 2 sur k_m .

i) Soit $\Phi_{X,p}$ le groupe des composantes connexes géométriques de $J(X)_{\mathbb{F}_p}$. Parce que ρ_m n'est pas modulaire de niveau Mq (cf. b)), on a $\Phi_{X,p} = m\,\Phi_{X,p}$ (n° 7, *lemme* 2 où l'on échange les rôles de p et q), d'où $\Phi_{X,p}[m] = 0$. Les points de $J(X)(\bar{\mathbb{F}}_p)[m]$ sont donc situés sur la composante neutre de $J(X)_{\mathbb{F}_p}$, c'est-à-dire appartiennent à $\mathrm{Hom}(\hat{T}_{X,p}/m\,\hat{T}_{X,p}, \bar{\mathbb{F}}_p^\times)$. Il résulte alors de h) que $\hat{T}_{X,p}/m\,\hat{T}_{X,p}$ est de dimension ≥ 2 sur k_m .

j) La dimension de $\hat{T}_{Nq,q}/m\hat{T}_{Nq,q}$ sur k_m est ≥ 2 : parce que ρ_m n'est pas modulaire de niveau Mq (cf. b)), cela résulte du lemme 1 du n° 7 où l'on échange les rôles de p et de q , et de i). Si $\ell \nmid N$, on en déduit, grâce au lemme 4 du n° 6, que l'on a $q \equiv 1 \mod \ell$, ce qui est absurde (cf. d)). Si $\ell \mid N$ et $\ell^2 \nmid N$, ρ_m n'est pas modulaire de niveau N/ℓ d'après a), et la remarque du n° 6 conduit à la même absurdité.

Cela achève la démonstration.

BIBLIOGRAPHIE

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

[Ca] H. CARAYOL - *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. ENS 19 (1986), 409-468.

[D,R] P. DELIGNE et M. RAPOPORT - *Les schémas de modules de courbes elliptiques*, Modular Functions of One Variable II, Lecture Notes in Math. 349 (1972), 143-316.

[D,S] P. DELIGNE et J.-P. SERRE - *Formes modulaires de poids* 1 , Ann. Sci. ENS 7 (1974), 507-530.

[Fa] G. FALTINGS - *Endlichkeitsätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349-366.

[Fl] M. FLEXOR - *Points de torsion des courbes elliptiques sur un corps de nombres fixé* (d'après les notes de G. Frey), preprint, 1987.

[Fr] G. FREY - *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Saraviensis, Ser. Math. 1 (1986), 1-40.

[Gr] A. GROTHENDIECK - SGA 7 I, Exposé IX, Lecture Notes in Math. 288.

[He 1] Y. HELLEGOUARCH - *Points d'ordre fini des courbes elliptiques*, C.R. Acad. Sc. Paris 273 (1971), 540-543.

[He 2] Y. HELLEGOUARCH - *Courbes elliptiques et équation de Fermat*, thèse, Besançon, 1972.

[He 3] Y. HELLEGOUARCH - *Points d'ordre* $2p^h$ *sur les courbes elliptiques*, Acta arithmetica 26 (1975), 253-263.

[H,S] M. HINDRY et J.H. SILVERMAN - *The canonical height and integral points on elliptic curves*, Invent. math. 93 (1988), 419-450.

[J,L] B. JORDAN et R. LIVNÉ - *On the Néron model of Jacobians of Shimura Curves*, Compositio Math. 60 (1986), 227-236.

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

[La] S. LANG - *Elliptic curves : Diophantine analysis*, Grundlehren der math. Wissenschaften, Vol. 231, Springer, 1978.

[Ms] R.C. MASON - *Diophantine equations over function fields*, London Math. Soc. Lecture Notes, Vol. 96, Cambridge, 1984.

[M] D.W. MASSER - *On Szpiro's conjecture*, preprint, 1986.

[Ma 1] B. MAZUR - *Courbes elliptiques et symboles modulaires*, Sém. Bourbaki, exposé n° 414, Lecture Notes in Math. 317, 1973.

[Ma 2] B. MAZUR - *Modular curves and the Eisenstein ideal*, Publ. math. de l'IHES 47 (1977), 33-186.

[Ma 3] B. MAZUR - Lettre à J.-F. Mestre, 16 août 1985.

[M,O] J.-F. MESTRE et J. OESTERLÉ - *Courbes de Weil semi-stables de discriminant une puissance* m-*ième*, à paraître.

[Ra] M. RAYNAUD - *Spécialisation du foncteur de Picard*, Publ. math. de l'IHES 38 (1970), 27-76.

[R] P. RIBENBOIM - 13 *lectures on Fermat's last theorem*, Springer-Verlag, 1979.

[Ri 1] K. RIBET - *Galois action on division points of abelian varieties with real multiplications*, Amer. J. of Math. 98 (1976), 751-804.

[Ri 2] K. RIBET - *On modular representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, preprint, 1987.

[Se 1] J.-P. SERRE - *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259-331 (= Oeuvres, t. III, 1-73).

[Se 2] J.-P. SERRE - Lettre à J.-F. Mestre, 13 août 1985. (Publiée dans Contemporary Mathematics 67 (1987), 263-268.)

[Se 3] J.-P. SERRE - *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\bar{\mathbb{Q}},\mathbb{Q})$, Duke Math. J. 54 (1987), 179-230.

[Se 4] J.-P. SERRE - Lettre à K. Ribet, 15 avril 1987.

[S,T] C.L. STEWART et R. TIJDEMAN - *On the Oesterlé - Masser conjecture*, Monatshefte für Mathematik 102 (1986), 251-257.

[Sz] L. SZPIRO - *La conjecture de Mordell* [*d'après Faltings*], Sém. Bourbaki 1983-84, exposé n° 619, Astérisque 121-122 (1985), 93-103.

[T,W] J.W. TANNER et S.S. WAGSTAFF - *New congruences for the Bernoulli Numbers*, Math. of Computation 48 (1987), 341-350.

[Ta] J. TATE - *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, Lecture Notes in Math. 476 (1975), 33-52.

[Vo] P. VOJTA - *Diophantine Approximation and Value Distribution Theory*, Lecture Notes in Math. 1239, 1987.

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

Joseph OESTERLÉ

Université de Paris 6
Institut Henri Poincaré
U.A. n° 763 du CNRS
11 rue Pierre et Marie Curie
F-75005 PARIS