Jean-Marc Fontaine

MATHEMATICAL SCIENCES RESEARCH INSTITUTE

1000 CENTENNIAL DRIVE • BERKELEY, CA 94720

le 19 octobre 1986

Cher Serre,

Ce que tu me demandes est vrai, à ceci près que V est la représentation dual de celle que tu dis. Les conditions d'application de mon théorème avec Messing son

i) bonne réduction en p,

ii) $2m+1 < p-1$

(on n'a pas besoin de supposer la cohomologie de X sans p-torsion, ni de faire de restriction sur sa dimension ; mais bien sûr la condition (ii) interdit de calculer toute la cohomologie de X si sa dimension est trop grande).

Mais c'est beaucoup plus général, et comme l'hypothese $\dim V = 2$ ne me paraît pas très raisonnable, il me semble que tu aurais intérêt a considérer des morceaux de la cohomologie ; ceux-ci ont encore un type de Hodge, comme je vais essayer de te l'expliquer.

De facon précise, soit Y un schéma propre et lisse sur $\mathbb{Z}_p$ (je pourrai remplac $\mathbb{Z}_p$ par les vecteurs de Witt d'un corps parfait, à condition d'accepter que les Frobenius soient semi-linéaires et non linéaires). Soient Y_s (resp. Y_η) sa fibre spéciale (resp. générique) - si tu veux Y_η est l'extension des scalaires de $\mathbb{Q}$ a $\mathbb{Q}_p$ de ta variété X - et n un entier verifiant $0 \leq n < p-1$. Alors $H^n_{DR}(Y_s)$ a une structure naturelle de "φ-module filtré", i.e. c'est un $\mathbb{F}_p$-espace vectoriel M de dimension finie, muni d'une filtration (la filtration de Hodge) et d'un isomorphisme

$$\varphi : \mathrm{gr}.M \xrightarrow{\sim} M$$

(la construction la plus simple de φ, qui ne dépend que du relèvement mod p^2 de Y_s, est celle d'Illusie-Deligne).

L'anneau A = réduction modulo p de l'anneau des entiers de la clôture algébrique de $\mathbb{Q}_p$ a une structure naturelle de φ-module filtré (à ceci près que ce n'e pas de dimension finie sur $\mathbb{F}_p$ et que φ n'est pas injective). Si je pose

$$V = (H^n_{et}(\overline{Y}_\eta, Z/pZ)^* \quad ,$$

alors V s'identifie à $\mathrm{Hom}_{\varphi\text{-mod.fil.}}(H^n_{DR}(Y_s), A)$.

Dans cette identification les sous-$\mathbb{F}_p$-espaces vectoriels de V stables par $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ correspondent bijectivement aux sous-φ-modules filtrés de $M = H^n_{DR}(Y_s$ i.e. aux sous-$\mathbb{F}_p$-espaces vectoriels N de M qui ont la vertu que, lorsqu'on les munit de la filtration induite, l'application φ induit encore un isomorphism de $\mathrm{gr}.N$ sur N .

Soit W un tel sous-espace correspondant à $N \subset M$. Supposes que E est une extension finie de $\mathbb{F}_p$ qui se plonge dans $\mathrm{End}\, W$ et que $\dim_E V = 2$, ce qui permet de considérer W comme une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ de dimension 2 su E . Alors E se plonge dans les endomorphismes du φ-module filtré N , ce qui i plique en particulier, si je pose $d = [E:\mathbb{F}_p]$, qu'il existe deux entiers r et vérifiant $0 \leq r \leq s \leq n$ (et qui sont les entiers que tu appelles de la même façon dans le cas que tu considères, i.e. si $E = \mathbb{F}_p$, $W = V$, $n = 2m+1$) tels que

$$\dim_{\mathbb{F}_p} N \cap \mathrm{Fil}^i H^n_{DR}(Y_s) = \begin{cases} 2d & \text{si } i \leq r , \\ d & \text{si } r < i \leq s , \\ 0 & \text{si } i > s . \end{cases}$$

Ceci étant, si l'on écrit l'action de Galois sur W sous la forme $\rho_p = \chi^r \otimes \rho'_p$, où χ est le caractère cyclotomique, on a

i) si $r = s$, alors ρ'_p est non ramifiée ;

ii) si $r < s$, alors

a) si ρ_p est irréductible, l'action de l'inertie via ρ'_p est modérée et donné par les deux caractères ψ^{s-r} et $\psi'^{(s-r)}$, où ψ et ψ' sont les deux caractères fondamentaux de niveau 2 ;

b) sinon cette action est de la forme

$$\begin{pmatrix} \chi^{s-r} & * \\ 0 & 1 \end{pmatrix}$$

où $*$ est ou n'est pas triviale, mais est "peu ramifiee" si $s-r = 1$.

Bien sûr, dans cette dernière partie, il est essentiel que le corps résiduel soit $\mathbb{F}_p$, sinon il y a d'autres niveaux possibles que les niveaux 1 et 2.

Enfin si ta représentation est la restriction à $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ d'une représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, le déterminant de cette dernière est de la forme $\chi^{r+s}\eta$, où η est un caractère non ramifié en p ; si tu veux une représentation impaire, il faut supposer la parité de η opposée de celle de $r+s$.

Bien à toi

Jean-Marc Fontaine

P.S. J'imagine que tu as déjà eu des informations précises sur Rubin. Voila ce qu'il nous a expliqué :

Thm A : Soit E une courbe elliptique à multiplication complexe par un ordre dans un corps quadratique imaginaire K. On suppose E définie sur K et $L(E/K,1) \neq 0$. Alors $\text{Ш}(E/K)$ est fini et, plus précisément, si w_K désigne le nombre de racines de l'unité dans K,

si p divise l'ordre de Ш, alors p divise w_K.(ordre conjectural).

Thm B : Si de plus la dite courbe E est définie sur $\mathbb{Q}$, alors

$$\text{rang } E(\mathbb{Q}) \geqslant 2 \Rightarrow \operatorname{ord}_{s=1} L(E/\mathbb{Q},s) \geqslant 2 .$$

(Ce qui, combiné avec Coates-Wiles et Gross-Zagier, implique que si E est une courbe à multiplication complexe définie sur $\mathbb{Q}$ telle que $\operatorname{ord}_{s=1} L(E/\mathbb{Q},s) \leq 1$, alors l'ordre en question est égal au rang de Mordell-Weil.)

Le plus surprenant est qu'il ne semble y avoir rien de difficile dans la démonstration. Les choses vaches étaient déjà faites. La seule idée nouvelle consiste à transposer au cas elliptique le travail d'un certain Thaine sur les unités cyclotomiques !