0

.

Rang moyen de famille de courbes elliptiques et lois de Sato-Tate

Philippe MICHEL, Université d'Orsay

28 Janvier, 1995

Rang moyen de famille de courbes elliptiques et lois de Sato-Tate

Title (in english)

Average rank of families of elliptic curves and Sato-Tate laws

ABSTRACT: the goal of this note is to give some complements to an article of Fouvry and Pomykala: by an ad-hoc method, they bound on average the rang of elliptic curves over $\mathbf{Q}$ in polynomial families: $y^2 = x^3 + a(t)x + b(t)$ when t varies in $\mathbf{Z}$, under some generic conditions on the polynomials (over $\mathbf{Z}$) $a(t)$, $b(t)$. Here, by a more systematic treatment, we are able to relax most of them, keeping only the natural one (the family is not geometricaly trivial). However, this result, specialized to the case treated by Fouvry and Pomykala, yields a better bound; our method depends on the distribution of the number of point in families of elliptic curves over finite fields (known as "vertical" Sato-Tate law), which itself depends on the work of Deligne on the Weil conjectures.

Rang moyen de famille de courbes elliptiques et lois de Sato-Tate

Philippe MICHEL, Université d'Orsay

28 Janvier, 1995

1 Introduction

Dans cette note, on se propose de complèter et de généraliser et d'améliorer les résultats de Fouvry et Pomykala [5] qui majorent le rang en moyenne de familles polynômiales de courbes elliptiques. Rappelons que, pour ce faire, on a recours aux formules explicites de Weil et que cela nécessite de faire trois "grosses" hypothèses unanimement admises qui concernent, toutes trois les fonctions L attachées aux courbes elliptiques: il s' agit de conjectures de Taniama-Weil, Birch - Swinnerton-Dyer, et de l' hypothèse de Riemann généralisée , notées T-W, B-SD et GRH (voir [5] pour les énoncés précis). Les améliorations qui suivent proviennent de résultats plus profonds de la géométrie algébrique, relatifs à la distribution du nombre de points de familles de courbes elliptiques sur les corps finis(voir les propositions 1.1 1.2); ces proposition ne sont pas vraiment nouvelles et ont déjà été prouvées sous une forme un peu moins précise par Deligne, Katz et avant par Birch ([1, 4, 9]); en particulier l'emploi des caractères de $\mathbf{F}_p$ – permettant de compléter des sommes courtes – ne semble pas avoir été remarquée.

On considère $a_1(t), \ldots, a_4(t), a_6(t) \in \mathbf{Z}[t]$ cinq polynômes; pour $t \in \mathbf{Z}$ soit E_t la courbe elliptique d' équation

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t). \tag{1}$$

On note respectivement $\Delta(t)$ et $j(t)$, son discriminant "naïf", et son invariant: le premier est un polynôme à coefficients entiers et le second une fraction en t. On note $g_2(t)$ et $g_3(t)$, les deux polynômes rationnels qu'on obtient quand on met l'équation précédente sous forme de Weierstrass (voir le formulaire de Tate [3]):

$$y'^2 = 4x'^3 - g_2(t)x' - g_3(t),$$

On a alors

$$\Delta(t) = g_2(t)^3 - 27g_3(t)^2 \text{ et } j(t) = 1728g_2(t)^3/\Delta(t).$$

Enfin, on note N_t son conducteur.

On fait pour la suite l' hypothèse que *la fraction $j(t)$ est non constante.*

Pour $p \geq 5$ un nombre premier, soit $E_{p,t}$ la courbe projective correspondante dans $\mathbf{F}_p$. Le nombre de ses points à valeurs dans $\mathbf{F}_p$ de $E_{p,t}$ est de la forme

$$p + a_{p,t} + 1. \tag{2}$$

Si $p \not| N_{E_t}$, $E_{p,t}$ est une vraie courbe elliptique et (d' après Hasse)

$$a_{p,t} = \sqrt{p}(e^{i\theta_{p,t}} + e^{-i\theta_{p,t}}),\ \theta_{p,t} \in [0, \pi[. \tag{3}$$

Si $p|N_{E_t}$, $E_{p,t}$ est dégénérée et $a_{p,t} = 0, 1$ ou -1 suivant le type de mauvaise réduction. On remarque que pour tout nombre premier p,

$$p|N_{E_t} \Longrightarrow p|\Delta(t). \tag{4}$$

Nous montrerons les propositions suivantes:

Proposition 1.1 . — *Il existe un entier N tel que pour tout $p \not| N$, tout $k \geq 1$ et pour tout caractère additif de $\mathbf{F}_p$, ψ_p, on ait la majoration*

$$\Big| \sum_{\substack{t \in \mathbf{F}_p \\ \Delta(t) \neq 0}} \mathrm{sym}_k(\theta_{p,t})\psi_p(t) \Big| \leq (k+1)(c_\Delta - \delta_{\psi_p} - 1)\sqrt{p}.$$

où on a posé $\mathrm{sym}_k(\theta) := \sin((k+1)\theta)/\sin(\theta)$ *et* $c_\Delta = \#\{z \in \mathbf{C},\ \Delta(z) = 0\}$, δ_{ψ_p} *vaut* 0 *ou* 1 *suivant que le caractère ψ_p est trivial ou non.*

Cette proposition, pour ψ_p le caractère trivial, exprime que quand $p \to \infty$ les angles $\{\theta_{p,t}\}_{t \in \mathbf{F}_p, \Delta(t) \neq 0}$ sont équidistribués sur $[0, \pi[$ pour la mesure dite de Sato-Tate $\sin^2(\theta)d\theta$, le premier résultat de ce type est dû à Birch [1].

Dans le cas ou $k = 1$ et ψ_p trivial, $\mathrm{sym}_1(\theta_{p,t}) = a_{p,t}/\sqrt{p}$ et on peut améliorer substantiellement, la majoration précédente:

Proposition 1.2 . — *Il existe N tel que pour tout $p \not| N$, on a la majoration*

$$\Big| \sum_{\substack{t \in \mathbf{F}_p \\ \Delta(t) \neq 0}} \frac{a_{p,t}}{\sqrt{p}} \Big| \leq (c_\Delta + c'_\Delta - 2)\sqrt{p} + c_\Delta.$$

où $c_\Delta = \#\{z \in \mathbf{C},\ \Delta(z) = 0\}$, $c'_\Delta = \#\{z \in \mathbf{C},\ g_2(z) = g_3(z) = 0\}$.

Les preuves de ces deux propositions sont données aux section 3 et 4; indiquons d' abord leur conséquences sur l' article [5], qui traite du rang sur $\mathbf{Q}$ des courbes E_t (noté $\mathrm{rang}_{\mathbf{Q}}(E_t)$):

Théorème 1.3 . — *Soient $a_1(t), \dots, a_4(t)$, $a_6(t)$ cinq polynômes de $\mathbf{Z}[t]$ et E_t la famille de courbes elliptiques d'équation (1), $t \in \mathbf{Z}$.*

Supposons que toutes les courbes elliptiques de cette famille vérifient les hypothèses TW, B-SD et GRH et que son invariant $j(t)$, est une fraction non constante*, alors, quand $T \to +\infty$, on a la majoration*

$$\sum_{\substack{|t|\leq T \\ \Delta(t)\neq 0}} \mathrm{rang}_{\mathbf{Q}}(E_t) \leq (\deg \Delta + c_\Delta + c'_\Delta - 3/2)(1+o(1))2T. \tag{5}$$

où $\Delta(t)$ est le discriminant de la famille, et $c_\Delta = \#\{z \in \mathbf{C},\ \Delta(z) = 0\}$ et $c'_\Delta = \#\{z \in \mathbf{C},\ g_2(z) = g_3(z) = 0\}$.

Rappelons que Fouvry et Pomykala obtenaient la borne $(2\deg\Delta)(1+o(1))2T$, en faisant les hypothèses (génériques) suivantes

$$a_1 = a_2 = a_3 = 0 \text{ et donc } \Delta(t) = -2^4(4a_4(t)^3 + 27a_6^2(t))$$

$$\deg a_6(t) \geq 1.$$

$$a_6(t) \text{ est de discriminant non nul.}$$

$$\deg \Delta(t) = \max(3\deg a_4, 2\deg a_6).$$

$$\Delta(t) \text{ est de discriminant non nul.}$$

Sous ces hypothèses, on a $c'_\Delta = 0$ et $c_\Delta = \deg\Delta$, le Théorème 1.3 recouvre donc complètement celui de [5] et améliore même la majoration du rang moyen d'une constante 3/2. Il est possible d'obtenir des résultats similaires pour des familles de varietés abéliennes sur $\mathbf{Q}$, moyennant des conjectures standard: ce sera l'objet d'un futur article.

Je tiens à remercier vivement les professeurs Fouvry, Katz et Laumon pour leurs fructueux conseils, ainsi que le rapporteur, qui m'a suggéré une amélioration importante par rapport à la version précédente de cet article.

2 Preuve du Théorème 1.3

On rappelle la formule explicite de Weil sous la forme que lui ont donnée Fouvry et Pomykala: soit $\lambda \geq 1$ un paramètre, on pose $F_\lambda(x) := \max(0, 1 - |x/\lambda|)$, alors

$$\lambda \sum_{\substack{|t|\leq T \\ \Delta(t)\neq 0}} Rang(E_t) \ \leq (\deg\Delta)2T\log T - 2S_1(T) - 2S_2(T) + O(T), \tag{6}$$

avec

$$S_j(T) = \sum_{\substack{|t|\leq T \\ \Delta(t)\neq 0}} \sum_p b_{p^j,t}\frac{\log p}{p^j} F_\lambda(j\log p),\ j = 1, 2,$$

et $b_{p^n,t}$ définit par $b_{p^n,t} = 2\sqrt{p}^n \cos(n\theta_{p,t})$ si $p \not| N_{E_t}$, $b_{p^n,t} = a_{p,t}^n$ si $p|N_{E_t}$.

Il y avait dans [5], une légère imprécision qui ne remettait pas en cause ses théorèmes, en effet, il n'est pas vrai en général que la réduction mod p, de la courbe elliptique d'équation (1) est la courbe d'équation (1) dans $\mathbf{F}_p$; cela est vrai si E_t *a bonne réduction en* p: $p \not| N_t$. En particulier si $\Delta(t) \neq 0 \bmod p$. Soit N le nombre défini dans les propositions 1.1 et 1.2, en vertu de (3), la contribution à $S_j(T)$ des $p|N$ est un $O(T)$, on supposera donc que $p \not| N$. De plus, d'après (3), la contribution pour chaque p des $|t| \leq T$ tels que $\Delta(t) = 0 \pmod{p}$ est un $O(\deg \Delta T p^{j/2-1})$; il ne reste plus que les t tels que $\Delta(t) \neq 0 \pmod{p}$.

Pour chaque $p \not| N$, on découpe alors l'intervalle $[-T, T]$, en intervalles de longueur p, plus éventuellement un intervalle incomplet I_p de longueur $\leq p-1$:

$$(7) \qquad S_j(T) = \sum_{p \not| N} F_\lambda(j \log p) \frac{\log p}{p^j} \left[\frac{2T+1}{p}\right] \sum_{\substack{t \in \mathbf{F}_p \\ \Delta(t) \neq 0 \pmod{p}}} b_{p^j,t}$$

$$+ \sum_{p \not| N} F_\lambda(j \log p) \frac{\log p}{p^j} \sum_{\substack{t \in I_p \\ \Delta(t) \neq 0 \pmod{p}}} b_{p^j,t} + O(T + \mathrm{e}^\lambda);$$

Majoration de $S_1(T)$

On applique la Proposition 1.2, à la première partie de (7). Pour la seconde partie de (7), on complète la somme courte $\sum_{\substack{t \in I_p \\ \Delta(t) \neq 0 \pmod{p}}} a_{p,t}$ par transformation de Fourier à l'aide des caractères additifs de $\mathbf{F}_p$ (méthode de Polya-Vinogradov) et on applique la proposition 1.1. On obtient finalement la majoration

$$S_1(T) \leq (c_\Delta + c'_\Delta - 2)\frac{\lambda}{2}(1 + o(1))2T + O(T + \lambda\, \mathrm{e}^\lambda).$$

Majoration de $S_2(T)$

Dans [5], $S_2(T)$ était majoré par $2T\frac{\lambda}{2}(1 + o(1))$ grâce à la borne triviale (3)

$$|b_{p^2,t}| \leq 2p.$$

On gagne une constante $1/2$ en estimant $b_{p^2,t}$ en moyenne sur les t: d' après l'identité trigonométrique

$$\cos(2\theta) = -\frac{1}{2} + \frac{1}{2}\,\mathrm{sym}_2(\theta),$$

on déduit de la Proposition 1.1 ($k = 2,\ \psi_p = 1$), compte tenu de (4), que

$$\sum_{\substack{t \in \mathbf{F}_p \\ \Delta(t) \neq 0 \pmod{p}}} b_{p^2,t} = -p^2 + O(p^{3/2}) \text{ (au lieu de } \leq 2p^2);$$

on trouve finalement

$$S_2(T) = -T\frac{\lambda}{2}(1+o(1)) + O(T+e^{\lambda}),$$

et avec [5], on conclut la preuve du Théorème 1.3 en prenant $\lambda = (1 - \frac{1}{\log^{1/2} T})\log T$.

3 La proposition d'équidistribution

On rappelle ici la méthode ℓ-adique standard pour montrer la Proposition (cf [4, 6, 9, 8]). On commence par fixer ℓ un nombre premier.

Soit V le schéma sur $\mathbf{Z}$ défini par l'équation

$$V : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

et muni du morphisme de projection

$$\begin{array}{rccc} f: & V & \to & \mathbf{A}^1_{\frac{1}{6\ell}\mathbf{Z}} = Spec(\frac{1}{6\ell}\mathbf{Z}[t]) \\ & (x,y,t) & \to & t. \end{array}$$

On étudie ici la fibre $f^{-1}(t)$ quand t varie; l' objet qui décrira notre situation est le faisceau $\mathcal{F} := R^1 f_! \mathbf{Q}_\ell$: c'est un faisceau constructible sur $\mathbf{A}^1_{\frac{1}{6l}\mathbf{Z}}$ et on peut même préciser son ouvert de lissité (voir [6] 3. pour un énoncé général):

Soit $\Delta^1(t) = \Delta(t)/pgcd(\Delta(t), \Delta'(t))$, alors il existe $N \in \mathbf{N}^*$ tel que $\Delta^1(t)$ est unitaire dans $\frac{1}{6\ell N}\mathbf{Z}[t]$ et que $\mathcal{F}$ est lisse de rang 2 sur l'ouvert

$$U := Spec(\mathbf{Z}[t, \frac{1}{6\ell N \Delta^1(t)}]).$$

Par fonctorialité, on dispose donc pour chaque $p \not| 6\ell N$ d' un faisceau $\mathcal{F}_p$ lisse de rang 2 sur chaque fibre $U_p = U \otimes_{\frac{1}{6\ell N}\mathbf{Z}} \mathbf{F}_p$, c' est à dire une représentation du groupe de monodromie $\pi_1(U_p)$ (on omet la mention du point base) dans un $\mathbf{Q}_\ell$-espace vectoriel de dimension 2. Pour tout point de U_p à valeurs dans le corps $\mathbf{F}_p$ ($t \in \mathbf{F}_p,\ \Delta(t) \neq 0$) on a l'égalité

$$\mathrm{tr}(\mathrm{Frob}_{p,t} \,|\mathcal{F}_p) = a_{p,t};$$

quitte à prendre une extension finie, E_λ, de $\mathbf{Q}_\ell$, on peut considérer le twist de Tate $F_p(1/2)$, et

$$\mathrm{tr}(\mathrm{Frob}_{p,t} \,|\mathcal{F}_p(1/2)) = \frac{a_{p,t}}{\sqrt{p}};$$

(3) s' exprime alors en disant que $\mathcal{F}_p(1/2)$ est pur de poids 0 et de déterminant trivial (donc l'image par cette représentation, de $\pi_1(U_p)$ est contenue dans SL_2). On peut donc composer la représentation "qu' est" $\mathcal{F}_p(1/2)$ avec les représentations

irréductibles de SL_2, qui sont ces puissances symétriques; on obtient les faisceaux $Sym_k(\mathcal{F}_p)$ qui sont lisses, purs de poids 0, de rang $k+1$ et

$$t \in \mathbf{F}_p,\ \Delta(t) \neq 0,\ \mathrm{tr}(\mathrm{Frob}_{p,t}, Sym_k(\mathcal{F}_p)) = \mathrm{sym}_k(\theta_{p,t}).$$

Pour que le tableau soit complet, pour tout ψ_p caractère de $\mathbf{F}_p$, on dispose du faisceau sur $\mathbf{A}^1_{\mathbf{F}_p}$, $\mathcal{L}_{\psi_p}$, lisse, de rang 1, pur de poids 0, qui, si ψ_p est non trivial, est sauvagement ramifié en ∞ avec $\mathrm{Swan}_\infty = 1$ ([6] 4.8).

Alors par la formule des traces de Lefschetz-Grothendieck, on a

$$\sum_{\substack{t\in\mathbf{F}_p\\ \Delta(t)\neq 0}} \mathrm{sym}_k(\theta_{p,t})\psi_p(t) = \sum_{i=0}^{2} (-1)^i \,\mathrm{tr}(\mathrm{Frob}_p \,|H^i_c(\overline{U}_p, Sym_k(\mathcal{F}_p)\otimes\mathcal{L}_{\psi_p}));$$

comme la courbe $\overline{U}_p = U\otimes\overline{\mathbf{F}}_p$ est affine, $H^0_c(\overline{U_p}|-) = 0$, et d' après les théorèmes fondamentaux de Deligne, les valeurs propres de Frob_p agissant sur $H^i_c(\overline{U}_p, Sym_k(\mathcal{F}_p)\otimes \mathcal{L}_{\psi_p})$ sont des entiers algébriques dont tout les conjugués sont de valeur absolue $\leq p^{i/2}$; pour montrer la proposition 1.1, il suffit de montrer que $H^2_c(\overline{U}_p|-)$=0, et de calculer le caractéristique d' Euler des différents faisceaux.

Rappelons que la représentation $\mathcal{F}_p$ se restreint au groupe fondamental *géométrique* $\pi_1(\overline{U}_p)$, dont l' adhérence dans $Aut(\mathcal{F}_p)$ est appelée groupe de monodromie géométrique, et est noté $G^{geom}(\mathcal{F}_p)$. En $p=\infty$ on a également un faisceau $\mathcal{F}_{\mathbf{C}}$, pour $\pi_1(U\otimes\mathbf{C}) = \pi_1(\mathbf{C} - \{z\in\mathbf{C},\ \Delta(z)=0\})$. Pour tous ces faisceaux on dispose de théorèmes de "spécialisation de la monodromie":

Lemme 3.1 . — *(cf* [4] *1.5,* [6] *4.7,* [8] *8.18) Quitte à agrandir N, on a pour tout $p \not| 6\ell N$ les propriétés*

- *le faisceau $\mathcal{F}_p$ est modérément ramifié en tout point de $\mathbf{P}^1\otimes\overline{\mathbf{F}_p} - \overline{U_p}$,*
- *$G^{geom}(\mathcal{F}_p) = G^{geom}(\mathcal{F}_{\mathbf{C}})$.*

Les faisceaux $Sym_k(\mathcal{F}_p)$ étant modérément ramifiés partout, par la formule de Grothendieck-Ogg-Shafarevitch, on a

$$\begin{aligned}\chi_c(\overline{U_p}, Sym_k(\mathcal{F}_p)\otimes\mathcal{L}_{\psi_p}) = &\quad dim(Sym_k(\mathcal{F}_p)\otimes\mathcal{L}_{\psi_p})\chi_c(\overline{U_p}) + \mathrm{Swan}_\infty(Sym_k(\mathcal{F}_p)\otimes\mathcal{L}_{\psi_p})\\ = &\quad -(k+1)(c_\Delta - 1) + (k+1)\,\mathrm{Swan}_\infty(\mathcal{L}_{\psi_p})\\ = &\quad -(k+1)(c_\Delta - \delta_{\psi_p} - 1),\end{aligned}$$

Avec $\delta_{\psi_p} = 1$ ou 0 suivant que ψ_p est trivial ou non.

Compte tenu de l'interprétation des H^2_c en terme des coinvariants du faisceau, il suffit pour finir, de voir que les différents groupes de monodromie géométrique agissent irréductiblement. Par le lemme 3.3.5 de [4]: comme $j(t)$ *mod* p est non constant pour p assez grand, $G^{geom}(\mathcal{F}_p) = SL_2$ donc $G^{geom}(Sym_k(\mathcal{F}_p)) = Sym_k(SL_2)$ d'où

$$H^2_c(\overline{U_p}, Sym_k(\mathcal{F}_p)) = 0.$$

Pour montrer la nullité de H^2_c si ψ_p est non trivial, on peut, soit invoquer le lemme clef 4.8.7 de [6], soit remarquer que la propriété d'irréductibilité d'un faisceau (ici $Sym_k(\mathcal{F}_p)$) est conservée après tensorisation par un faisceau pur, de rang 1, (en l'occurence $\mathcal{L}_{\psi_p}$).

4 Preuve de la proposition 1.2

On rappelle que p est pris assez grand, en particulier, $p > 3$. Soit $\mathbf{F}_q$ une extension finie de $\mathbf{F}_p$ ($q = p^n$), contenant toutes les racines de $\Delta(t)$, on note $U_q := U_p \otimes \mathbf{F}_q$.

D'après la section précédente, le faisceau $\mathcal{F}(1/2)$ est géométriquement irréductible, pur de poids 0, ce qui entraine que

$$H^0_c(\overline{U}_p|\mathcal{F}(1/2)) = H^2_c(\overline{U}_p|\mathcal{F}(1/2)) = 0,$$

et que $H^1_c(\overline{U}_p|\mathcal{F}(1/2))$ (de dimension $2(c_\Delta - 1)$) est mixte de poids 1 (ie. toutes les valeurs propres de $\mathrm{Frob}_q = \mathrm{Frob}_p{}^n$ agissant sur $H^1_c(\overline{U}_p|\mathcal{F}(1/2))$, sont de module $\leq q^{1/2}$); le Lemme suivant calcule la somme des sous-espaces caractéristiques associés aux valeurs propres de module ≤ 1 (ie la partie de poids ≤ 0 de $H^1_c(\overline{U}_p|\mathcal{F}(1/2))$) , c'est une modification immédiate de [7] 7.1.2:

Lemme 4.1 . — *Soit $\mathcal{F}$ un E_λ-faisceau, lisse sur U_q, pur de poids w, géométriquement irréductible, on a un isomorphisme canonique de* $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$*-modules,*

$$\mathcal{F}^{I_\infty} \oplus \bigoplus_{x\in\mathbf{F}_q,\Delta(x)=0} \mathcal{F}^{I_{\overline{x}}} \tilde{\to} \text{la partie de poids} \leq w \text{ de } H^1_c(\overline{U}_p|\mathcal{F}).$$

On a noté $I_{\overline{x}}$ le groupe d'inertie d'une place $\overline{x}$ au dessus du point fermé $x \in U_q$.

Preuve. — Soit j, l'inclusion $j : U \hookrightarrow \mathbf{P}^1$, on a une suite exacte de faisceaux sur $\mathbf{P}^1 \otimes \mathbf{F}_q$,

$$0 \to j_!\mathcal{F} \to j_*\mathcal{F} \to \mathcal{F}^{I_\infty} \oplus \bigoplus_{x\in\mathbf{F}_q,\Delta(x)=0} \mathcal{F}^{I_{\overline{x}}} \to 0.$$

appliquant la suite exacte longue de cohomologie qui s'en déduit, et remarquant que

$$H^0(\mathbf{P}^1 \otimes \overline{\mathbf{F}}_q|j_*\mathcal{F}) = H^0(U_q \otimes \overline{\mathbf{F}}_q|\mathcal{F}) \simeq H^2_c(U_q \otimes \overline{\mathbf{F}}_q|\mathcal{F}^\vee(1)) = 0$$

(car $\mathcal{F}$ (et donc $\mathcal{F}^\vee$) est géométriquement irréductible (d'ailleurs $\mathcal{F} \simeq \mathcal{F}^\vee$)), on en déduit

$$0 \to \mathcal{F}^{I_\infty} \oplus \bigoplus_{x\in\mathbf{F}_q,\Delta(x)=0} \mathcal{F}^{I_{\overline{x}}} \to H^1_c(U_q \otimes \overline{\mathbf{F}}_q|\mathcal{F}) \to H^1(\mathbf{P}^1 \otimes \overline{\mathbf{F}}_q|j_*\mathcal{F}) \to 0.$$

Par les Théorèmes de Deligne [4], nous savons que

$$\mathcal{F}^{I_\infty} \oplus \bigoplus_{x\in\mathbf{F}_q,\Delta(x)=0} \mathcal{F}^{I_{\overline{x}}} \text{ est mixte de poids } \leq w.$$

$$H^1_c(U_q \otimes \overline{\mathbf{F}}_q|\mathcal{F}) \text{ est mixte de poids } \leq w+1.$$

$$H^1(\mathbf{P}^1 \otimes \overline{\mathbf{F}}_q|j_*\mathcal{F}) \text{ est pur de poids } w+1.$$

Cela démontre le Lemme.

□

Retournont au faisceau $\mathcal{F}(1/2)$ (ou plutôt sa restriction à U); la fibre de la famille E_t en un point $x \in \overline{\mathbf{F}}_p$ tel que $\Delta(x) = 0$ et $g_2(x) \neq 0$, est dégénérée de type multiplicatif, par conséquent l'action du groupe d'inertie I_x sur $\mathcal{F}(1/2)$, s'écrit dans une base convenable (formule de Picard-Lefschetz [2])

$$\gamma \in I_x \to \begin{pmatrix} 1 & t_\ell(\gamma) \\ 0 & 1 \end{pmatrix}$$

où $t_\ell : I_x \twoheadrightarrow I_x^{\mathrm{mod}} \simeq \prod_{l \neq p} \mathbf{Z}_l(1) \twoheadrightarrow \mathbf{Z}_\ell(1)$ est la surjection canonique. On en déduit la minoration $\dim_{E_\lambda} \mathcal{F}(1/2)^{I_x} = 1$, et donc

$$\dim_{E_\lambda}\{\textit{partie de poids} \leq 0 \textit{ de } H^1_c(U_q \otimes \overline{\mathbf{F}}_p|\mathcal{F}(1/2))\} \geq \#\{x \in \overline{\mathbf{F}}_p,\ \Delta(x) = 0,\ g_2(x) \neq 0\};$$

d'où finalement,

$$\begin{aligned} |\operatorname{tr}(\mathrm{Frob}_p, H^1_c(U_p \otimes \overline{\mathbf{F}}_p|\mathcal{F}(1/2)))| \quad &\leq (2(c_\Delta - 1) - \#\{x \in \overline{\mathbf{F}}_p,\ \Delta(x) = 0,\ g_2(x) \neq 0\})p^{1/2} \\ &\quad + \#\{x \in \overline{\mathbf{F}}_p,\ \Delta(x) = 0,\ g_2(x) \neq 0\} \\ &\leq (c_\Delta + c'_\Delta - 2)p^{1/2} + c_\Delta, \end{aligned}$$

si p est assez grand. Ce qui, d'après la formule de Lefschetz-Grothendieck, termine la preuve de la proposition.

Bibliographie

[1] B.J. BIRCH. — *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. 43 (1968),57-60.

[2] P. DELIGNE. — *La conjecture de Weil I* , Publ.Math.IHES 43 (1974), 273-308.

[3] P. DELIGNE. — *Courbes Elliptiques: Formulaire (d'après J.Tate)*, in Modular functions of one variable IV (1975), L.N.M. Springer-Verlag, 53-74.

[4] P. DELIGNE. — *La conjecture de Weil II*, Publ.Math.IHES 52 (1981), 313-428.

[5] E. FOUVRY et J. POMYKALA. — *Rang des courbes elliptiques et sommes d'exponentielles,* Mh. Math. 116 (1993), 111-125.

[6] N.M. KATZ. — *Sommes d'exponentielles,* Astérisque 79, Soc. Math. de France (1978).

[7] N.M. KATZ. — *Gauss Sums, Kloosterman Sums and Monodromy Groups,* Annals of Maths. Studies 116, PUP.

[8] N.M. KATZ. — *Exponential sums and Differential equations,* Annals of Maths. Studies 124, PUP.

[9] N.M. KATZ. — *Exponential sums over finite fields and Differential equations over the complex numbers : some interactions,* Bull. Am.. Math. Soc., Vol 23, n, p.269.

[10] J.-F. MESTRE. — *Formules explicites et minorations de conducteurs de variétés algébriques,* Comp. Math. 58, (1986), 209-232.

Philippe MICHEL
Mathématiques, Bât. 425
Université Paris-Sud
91405 ORSAY CEDEX