Mathematics Subject Classification (1991):11G05, 11G40, 11K99

TITLE:Sur les zéros de fonctions L sur les corps de fonctions

AUTHOR: Philippe MICHEL

Département de Mathematiques, Université Paris-Sud, Bât. 425, 91405 Orsay; (e-mail : michel@math.u-psud.fr).

ABSTRACT: A la différence du cas des corps de nombres, on sait prouver depuis les travaux de Grothendieck et de Deligne que les fonctions L de courbes elliptiques sur les corps de fonctions possèdent des propriétés extrêmement agréables: prolongement analytique, hypothèse de Riemann (alors que pour leurs analogues sur les corps de nombres, on ne dispose bien souvent que de conjectures) il est tentant de pousser plus loin et d'essayer d'étudier les propriétés "fines" des ces fonctions L... Dans cet article nous nous intéressons à la distribution des zéros de la fonction $L(s,E)$ d'une courbe elliptique E définie sur $\mathbf{F}_q(X)$ non géométriquement triviale: nous montrons que quand n_E le degré du conducteur de E croit, les zéros de $L(s,E)$ (après une normalisation convenable) ont tendance à devenir uniformement distribués sur le cercle unité avec une discrépance en $O(\log^{-1} n_E)$. Il semble que l'on soit loin de la vérité (on s'attendrait plutôt à ce que la discrépance soit en $O(n_E^{\varepsilon-1})$). Inspirés par des travaux antérieurs de Brumer, Fouvry-Pomykala et l'auteur, nous considérons le problème en moyenne pour une famille très générale de courbes elliptiques et obtenons "presque surement" une discrépance en $O(n_E^{\varepsilon-1})$.

Sur les zéros de fonctions L sur les corps de fonctions

Philippe MICHEL, Université d'Orsay

September 11, 2001

Département de Mathematiques, Université Paris-Sud, Bât. 425, 91405 Orsay; (e-mail : michel@math.u-psud.fr).

Mathematics Subject Classification (1991):11G05, 11G40, 11K99

Notations

- K désigne le corps $\mathbf{F}_q(X)$ corps de fonctions de $\mathbf{P}^1_{\mathbf{F}_q}$ et $\mathcal{Z}$ l'anneau $\mathbf{F}_q[X]$.
- pour tout $t \in \mathcal{Z}$, on pose $|t| := q^{\deg t}$.
- Pour chaque place p de $\mathbf{P}^1_{\mathbf{F}_q}$, on note $\mathbf{F}_p$ son corps résiduel (c'est le corps fini à $|p|$ éléments si $p \neq \infty$) et d_p le degré de $\mathbf{F}_p$ sur $\mathbf{F}_q$ (c'est aussi le degré du polynôme irréductible unitaire p).

1 Introduction

Soit E/K une courbe elliptique définie sur K. On désigne par $N_E = \prod_p p^{f_p}$ son conducteur et on note n_E son degré: $n_E = \sum_p d_p f_p$. Une fonction L est naturellement attachée à E; rappelons sa définition: Pour toute place p de K, on définit l'entier $a_p = |p| + 1 - |E_p|$ où $|E_p|$ est le nombre de points à valeur dans $\mathbf{F}_p$ de la réduction modulo p de E; si p ne divise pas N_E (E a bonne réduction en p) Hasse a montré que a_p s'écrit sous la forme $\alpha_p + \overline{\alpha}_p,\ \alpha_p \in \mathbf{C}$ avec $|\alpha_p| = |p|^{1/2}$; en revanche, si $p|N_E$, a_p vaut $0, 1, -1$ suivant que la réduction modulo p est additive, multiplicative deployée ou non deployée. La fonction $L(s, E)$ est alors définie par

$$L(s,E) = \prod_{p|N_E} (1 - \frac{a_p}{p^s})^{-1} \prod_{p\nmid N_E} (1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}})^{-1}.$$

De manière plus savante, $L(s, E)$ est la fonction L associée à la représentation galoisienne ℓ-adique de $Gal(K^{sep}/K)$ sur le dual du module de Tate de E:

$$L(s,E) = \prod_p \det(I - q^{-s}\mathrm{Frob}_p|\mathbf{V}_\ell(E)^{\vee I_{\overline{p}}})^{-1}.$$

(en cas de bonne réduction, $\mathbf{V}_\ell(E)^{\vee I_{\overline{p}}} = \mathbf{V}_\ell(E)^\vee$).

À la différence du cas des courbes elliptiques sur un corps de nombres, on sait que cette fonction a des propriétés extrêmement agréables (cf.[Mi2], [Sch]):

- la fonction $L(s,E)$ est une fraction rationnelle en q^{-s}, de degré $n_E - 4$ qui s'écrit
$$L(s,E) = \frac{P_1(q^{-s})}{P_0(q^{-s})P_2(q^{-s})},$$
et $P_j(X) \in \mathbf{Q}[X]$ avec $P_j(0) = 1$. $\mathbf{V}_\ell(E)$ définit un $\mathbf{Q}_\ell$-module sur $\mathbf{P}^1_{\overline{\mathbf{F}}_q}$ lisse hors des places de mauvaises réduction de E, et on a
$$P_j(X) = \det(I_d - X\mathrm{Frob}_q, H^j(\mathbf{P}^1_{\overline{\mathbf{F}}_q}, \mathbf{V}_\ell(E)^\vee)).$$
D'autre part P_0, P_2 sont de même degré qui vaut 0 ou 2, ce dernier cas se produisant si et seulement si l'invariant $j_E \in K$ est constant ($j_E \in \mathbf{F}_q$) alors, $n_E = 0$ et $P_1(X) = 1$.
- $L(s,E)$ vérifie l'equation fonctionnelle
$$L(2-s,E) = \pm q^{(1-s)(n_E-4)}L(s,E).$$
- Pour $j = 0,1,2$ les zéros de $P_j(X)$ sont de la forme $q^{-(j+1)/2}\zeta$, $|\zeta| = 1$.

Dans ce travail, nous nous intéressons à la répartition des complexes $\{\zeta\}_E$ correspondant aux $n_E - 4$ zéros (comptés avec leur multiplicité) de $L(s,E) = P_1(q^{-s})$ dans le cercle unité quand le degré n_E du conducteur grandit et l'invariant j_E est non constant (la courbe elliptique est donc non géométriquement constante). Remarquons d'abord que l'équation fonctionnelle implique que les complexes $\{\zeta\}_E$ sont répartis symétriquement par rapport à l'axe réel: si $q^{-1}\zeta$ est un zéro de $P_1(X)$ avec une certaine multiplicité $q^{-1}\overline{\zeta}$ l'est aussi avec la même multiplicité.

Le premier résultat qui a motivé ce travail est que les complexes $\{\zeta\}_E$ deviennent uniformément distribués sur le cercle unité quand $n_E \to \infty$. Une autre manière d'énoncer les résultats est de représenter les complexes z par leur argument $\theta \in]-\pi,\pi]$: $\zeta = \mathrm{e}^{i\theta}$, on définit ainsi l'ensemble $\{\theta\}_E$ des angles associés à E. Dans cet énoncé et pour toute la suite, on fera la convention que dans toute somme de la forme $\sum_{\theta\in\{\theta\}_E} f(\theta)$, l'angle θ est compté avec la multiplicité du zéro qui lui correspond.

Théorème 1.1 *Soit E une courbe elliptique sur K d'invariant j non constant. Soit un intervalle $I \subset [-\pi,\pi]$; notons χ_I sa fonction caractéristique et $|I|$ sa longueur, alors on a l'égalité*
$$\frac{1}{n_E-4}\sum_{\theta\in\{\theta\}_E}\chi_I(\theta) - \frac{1}{2\pi}|I| = O(\frac{\log q}{\log n_E}).$$
La constante implicite dans le terme de droite est absolue et en particulier ne dépend pas de l'intervalle I choisi. En d'autre termes, quand $n_E \to \infty$, l'ensemble de angles $\{\theta\}_E$ devient uniformément distribué sur $[-\pi,\pi]$

Remarque. — Cet énoncé est en fait valable plus généralement pour l'ensemble des angles des zéros de la fonction L associée à une variété abélienne définie sur K et dont la $K/\mathbf{F}_q$-trace est nulle (la constante implicite ne dépend alors que de la dimension de la variété abélienne).

Ainsi, le nombre de zéros de $L(s,E)$ contenus dans tout intervalle I de longueur $\gg \log^{-1} n_E$ a le bon ordre de grandeur (en particulier, la multiplicité de $\theta = 0$ — rappelons qu'elle majore le rang de E — est un $O(n_E \log^{-1} n_E)$ on retrouve ainsi le résultat de [Br]). Nous définissons la discrépance de l'ensemble $\{\theta\}_E$

$$\mathrm{discr}(\{\theta\}_E) = \max_{I\subset[-\pi,\pi]} \Big|\frac{1}{n_E-4}\sum_{\theta\in\{\theta\}_E} \chi_I(\theta) - \frac{|I|}{\pi}\Big|.$$

On a donc la majoration $\mathrm{discr}(\{\theta\}_E) = O(\log^{-1} n_E)$.

Cette majoration, très générale, semble grossière: on dispose de $n_E - 4$ angles répartis dans $[-\pi,\pi]$ on pourrait s'attendre à un meilleur espacement de ces angles et à une discrépance beaucoup plus petite. Nous montrons que c'est le cas en moyenne (nous inspirant des travaux sur $\mathbf{Q}$ de Fouvry-Pomykala [F-P] et [Mi1]):

On considère une famille de courbes elliptiques $(E_t)_{t\in\mathbf{P}^1_K}$ définie sur K par l'équation

(1) $$E_T:\ y^2 = x^3 + a(T)x + b(T),\ a(T),\ b(T) \in \mathcal{Z}[T]$$

On note $\Delta(T) = 4a^3(T) + 27b^2(T)$ son discriminant et on suppose que la famille n'est pas géométriquement triviale ($j_{E_T} = j(T) \notin K$). D'autre part, on fait l'hypothèse que $a(T)$ et $b(T)$ sont premiers entre eux (ce qui implique que la courbe générique E_T définie sur $K(T)$ est semi-stable). Alors on a une estimation en moyenne de la répartition des angles $\{\theta\}_{E_t}$, $t \in \mathcal{Z}$:

Théorème 1.2 *Soit $(E_t)_{t\in\mathbf{P}^1_K}$ la famille de courbes elliptiques définie par (1), on suppose $j(T) \notin K$ et $(a(T), b(T)) = 1$. Alors, pour tout $\varepsilon > 0$, pour tout entier positif l et pour tout intervalle $I \subset [-\pi,\pi]$ on a pour $x \to +\infty$*

$$\sum_{\substack{t\in\mathcal{Z},\ |t|\le q^x \\ \Delta(t)\neq 0,\ j(t)\notin\mathbf{F}_q}} \Big|\frac{1}{(n_{E_t}-4)}\sum_{\theta\in\{\theta\}_{E_t}} \chi_I(\theta) - \frac{|I|}{2\pi}\Big|^{2l} \ll x^{\varepsilon-2l} q^{x+1},$$

où la constante implicite du symbole de Vinogradov ne dépend que de q, l, ε et du degré de Δ, en particulier elle est indépendante *de l'intervalle I choisi* [1].

En vue de la majoration $n_{E_t} \le \deg\Delta(t) \le \deg\Delta.x$ ce théorème donne le bon ordre de grandeur du nombre de zéros de $L(s,E_t)$ contenus dans tout intervalle I de longueur $\gg n_{E_t}^{\varepsilon-1}$ pour presque toutes les courbes elliptiques E_t avec $|t| \le q^x$ (en effet l'ensemble des $t \in \mathcal{Z}$ tels que $j(t) \in \mathbf{F}_q$ est fini). Par un argument élémentaire, on obtient alors une majoration en moyenne de la discrépance:

[1] Dans la suite, nous considérerons q fixé pour eviter d'avoir à écrire les dépendances en la caractéristique.

Corollaire 1.3 *Pour tout $\varepsilon > 0$, on a la majoration*

$$\sum_{\substack{t\in\mathcal{Z},\ |t|\le q^x\\ \Delta(t)\neq 0,\ j(t)\notin\mathbf{F}_q}} \mathrm{discr}(\{\theta\}_{E_t}) \ll_\varepsilon x^{\varepsilon-1}q^{x+1}.$$

En particulier pour tout $\varepsilon > 0$, le nombre de courbes E_t avec $|t| \le q^x$ et $\mathrm{discr}(\{\theta\}_{E_t}) > n_{E_t}^{\varepsilon-1}$ *est un $o_\varepsilon(q^{x+1})$.*

Remerciements: Ce travail doit beaucoup aux conseils et aux encouragements de E. Fouvry, qu'il en soit remercié ! Je remercie également H. Iwaniec de son invitation, de sa chaleureuse hospitalité et de ses commentaires lors de mon séjour à l'Université de Rutgers où ce travail à commencé d'être rédigé.

2 La formule explicite

La formule explicite que nous utilisons est conséquence directe de la formule des traces de Lefschetz et de l'équation fonctionnelle de $L(s,E)$ (elle a été employée par Brumer sous cette forme pour majorer le rang de E [Br], étendant ainsi aux corps de fonctions des travaux antérieurs de Mestre sur $\mathbf{Q}$ [Me]): pour simplifier les notations on posera pour tout $m \ge 1$ et pour tout p

$$\mathrm{tr}(\mathrm{Frob}_p^m, E) = \mathrm{tr}(\mathrm{Frob}_p^m, \mathbf{V}_\ell(E)^{\vee, I_{\overline{p}}})\ ).$$

Lemme 2.1 *Soit E/K une courbe elliptique d'invariant j non constant et f un polynôme trigonométrique pair de longueur Y:*

$$f(\theta) = c_0 + 2\sum_{d=1}^{Y} c_d\cos(d\theta).$$

On a l'égalité

$$\sum_{\theta\in\{\theta\}_E} f(\theta) = \qquad c_0(n_E-4) - 2\sum_{m\ge 1}\sum_p \frac{c_{md_p}d_p}{|p|^m}\mathrm{tr}(\mathrm{Frob}_p^m, E)$$

La somme $\sum_{\theta\in\{\theta\}_E} f(\theta)$ porte sur les ordonnées des zéros s de $L(s,E)$, écrits sous la forme $s = 1 + \mathrm{i}\theta/\log q,\ \theta \in]-\pi,\pi]$.

Nous rappelons la version "corps de fonctions" du théorème des nombres premiers:

$$(2) \qquad \sum_{p,d_p=n} 1 = \frac{q^n}{n} + O(q^{n/2}).$$

qui s'obtient immédiatement à partir de l'identité suivante par inversion de Möebius:

$$\sum_{p, d_p | n} d_p = q^n. \tag{3}$$

Rappelons également la majoration de Hasse:

$$|\mathrm{tr}(\mathrm{Frob}_p^m, E)| \leq 2|p|^{m/2}, \tag{4}$$

qui est aussi valable aussi bien aux places de bonne que de mauvaise réduction (dans ce dernier cas le terme est majoré par 1).

Le théorème 1.1, est conséquence de la majoration effective de la discrépance d'un ensemble $\{\theta\} \subset [-\pi, \pi]$ ([K-N] (2.42))

Théorème 2.2 *(**Erdös-Turan**) Soit $\{\theta\}$ un ensemble fini $\subset [-\pi, \pi]$ de cardinal N, alors pour tout $Y \geq 1$, on a la majoration*

$$\mathrm{Disc}(\{\theta\}) \ll \frac{1}{Y} + \frac{1}{N} \sum_{1 \leq d \leq Y} |\sum_{\theta \in \{\theta\}} \mathrm{e}^{\imath d\theta}|.$$

Dans le cas présent, posons

$$\sum_{1 \leq d \leq Y} \frac{1}{d} |\sum_{\theta \in \{\theta\}_E} \mathrm{e}^{\imath d\theta}| := \sum_{1 \leq d \leq Y} \frac{c_d}{d} \sum_{\theta \in \{\theta\}_E} \mathrm{e}^{\imath d\theta}, \text{ avec } |c_d| = 1.$$

Compte-tenu de la propriété de symétrie de l'ensemble $\{\zeta\}_E$ on a la majoration

$$\mathrm{Disc}(\{\theta\}_E) \leq \frac{1}{Y} + \frac{1}{n_E - 4} \sum_{\theta \in \{\theta\}_E} f_Y(\theta),$$

où

$$f_Y(\theta) = \sum_{1 \leq d \leq Y} \frac{c_d}{d} \cos(d\theta).$$

Appliquant la formule explicite on a

$$\sum_{\theta \in \{\theta\}_E} f_Y(\theta) = - \sum_{m \geq 1} \sum_{p} \frac{c_{md_p} d_p}{md_p |p|^m} \mathrm{tr}(\mathrm{Frob}_p^m, E),$$

Par (4), (2), le terme de droite est majoré par $O_k(q^{Y/2})$. On choisit alors $Y = \log n_E / \log q$ pour conclure.

3 Preuve du Théorème 1.2

3.1 Premières réductions

Cette fois-ci, nous procédons directement à partir de la fonction caractérisitique $\chi_I(\theta)$ d'un intervalle $I \subset [-\pi, \pi[$. Par symétrie on peut supposer I de la forme $[-a, a[$ et on notera $\chi_a := \chi_I$. Soit $X > 1/\pi$ et $\chi_{a,X}$ une fonction $\in \mathcal{C}^\infty([-\pi, \pi])$, paire, décroissante sur $[0, \pi]$ telle que

$$\begin{aligned}
\chi_{a,X}(\theta) &= 1 \quad \text{pour} \quad 0 \le \theta \le a \\
\chi_{a,X}(\theta) &= 0 \quad \text{pour} \quad \theta \ge a + 1/X \ (\text{si } a + 1/X \le \pi) \\
\chi_{a,X}(\theta) &= 1 \quad \text{pour} \quad \theta \in [-\pi, \pi] \ (\text{si } a + 1/X > \pi)
\end{aligned}$$

et dont les dérivées succéssives vérifient $|\chi_{a,X}^{(j)}(\theta)| \ll_j X^j$ pour tout $j \ge 1$. Par intégration par partie, on voit que les coefficients de Fourier c_n définis par

$$\chi_{a,X}(\theta) = c_0 + 2 \sum_{n \ge 1} c_n \cos(n\theta)$$

vérifient les majorations

$$c_n = O_j(\frac{X^j}{n^{j+1}}), \text{ et } c_n = O(\frac{1}{n} + \frac{1}{X}) \ \forall \ n, j \ge 1; \text{ en particulier } c_n = O(\frac{1}{n}).$$

Pour $Y > X$ un paramètre à fixer, on considère enfin la série tronquée

$$f_Y(\theta) = c_0 + 2 \sum_{1 \le n \le Y} c_n \cos(n\theta)$$

de sorte que pour tout $k \ge 0$ on a

$$\chi_{a,X}(\theta) - f_Y(\theta) = O_k((X/Y)^k).$$

On a alors la majoration

$$\sum_{\substack{t \in \mathcal{Z}, |t| \le q^x \\ \Delta(t) \neq 0, \ j(t) \notin \mathbf{F}_q}} \Big| \sum_{\theta \in \{\theta\}_{E_t}} \chi_{a,X}(\theta) - c_0(n_{E_t} - 4) \Big|^{2l} \ll$$

$$\sum_{\substack{t \in \mathcal{Z}, |t| \le q^x \\ \Delta(t) \neq 0, \ j(t) \notin \mathbf{F}_q}} \Big| \sum_{\theta \in \{\theta\}_{E_t}} f_Y(\theta) - c_0(n_{E_t} - 4) \Big|^{2l} + O_{k,l}(q^{x+1}(x\frac{X^k}{Y^k})^{2l})$$

Appliquant la formule explicite à chacune des sommes $\sum_{\theta \in \{\theta\}_{E_t}} f_Y(\theta)$, on constate avec (4) et (2) que la contribution des termes des la forme $\sum_{p,m \ge 3} \dots$ est un $O(1)$ qui fournit en sommant sur les t un $O_{k,l}(q^{x+1})$.

Par l'inégalité $(a+b)^{2l} \leq 2^{2l}(a^{2l}+b^{2l})$, on est réduit à majorer deux sommes:

$$S_1 := \sum_{\substack{t\in\mathcal{Z}\\ \Delta(t)\neq 0}} |\sum_p \frac{d_p c_{d_p}}{|p|}\mathrm{tr}(\mathrm{Frob}_p, E_t)|^{2l},$$

$$S_2 := \sum_{\substack{t\in\mathcal{Z}\\ \Delta(t)\neq 0}} |\sum_p \frac{d_p c_{2d_p}}{|p|^2}\mathrm{tr}(\mathrm{Frob}_p^2, E_t)|^{2l},$$

à ce point, on a ajouté les termes correspondant aux $t \in \mathcal{Z}$ tels que $j(t) \in \mathbf{F}_q$ qui sont en nombre fini, leur contribution est en $O(q^{2lY/2}\log^{2l} Y)$.

3.2 Majoration de S_2

On utilise simplement la borne triviale (4) et $c_n = O_k(n^{-1})$: on obtient

$$S_2 \ll_k q^{x+1}(\sum_{\substack{p\\ |p|\leq q^{Y/2}}} \frac{1}{|p|^2}2|p|)^{2l} \ll_{k,l} q^{x+1}\log^{2l} Y. \qquad (5)$$

3.3 Majoration de S_1

Nous utilisons maintenant l'hypothèse que $a(T)$ et $b(T)$ sont premiers entre eux: il existe donc $u(T), v(\mathrm{T}) \in \mathcal{Z}[T]$ et $c \in \mathcal{Z}$ tels que $u(T)a(T)+b(T)v(T) = c$, par conséquent si $p \neq \infty$ et $p \not| c$ alors $p \not|\mathrm{pgcd}(a(t), b(t))$ et l'équation de $E_t : y^2 = x^3 + a(t)x + b(t)$ est minimale en p. La réduction en p de E_t est la courbe elliptique sur $\mathbf{F}_p$ d'équation $E_{\bar{t}} = y^2 = x^3 + a(\bar{t})x + b(\bar{t})$ ($\bar{t}$ désigne la classe de t modulo p). En particulier, on a l'égalité $\mathrm{tr}(\mathrm{Frob}_p, E_t) = \mathrm{tr}(\mathrm{Frob}_p, E_{\bar{t}})$: la fonction $\mathrm{tr}(\mathrm{Frob}_p, E_t)$ ne dépend que de la classe de $t \pmod p$. Dans la suite on note $q_1, \ldots, q_m$ l'ensemble des diviseurs premiers de c (avec ∞, $q_1, \ldots, q_m$ constituent les "mauvaises" places).

Notons alors que par (4), la contribution des $q_i|c$ dans S_1 et S_2 est majorée trivialement par $O_c(q^{x+1})$. Dans toute la suite les p (indicés ou non) qui interviendront seront "bons" (ie. seront $\neq \infty$ et ne diviseront pas c).

Dans l'expression de S_1, on ouvre le terme à la puissance $2l$ et on intervertit les sommations; on voit alors que S_1 se décompose en $O_l(1)$ sommes de la forme

$$S_1(\alpha_1, \ldots, \alpha_j) := \sum_{p_1} \cdots \sum_{p_j} \prod_{i=1}^{j} \frac{(c_{d_{p_i}} d_{p_i})^{\alpha_i}}{|p_i|^{\alpha_i}} S(p_1, \ldots, p_j; \alpha_1, \ldots, \alpha_j),$$

avec $1 \leq j \leq 2l$; les α_i sont des entiers ≥ 1 vérifant $\sum_i \alpha_i = 2l$ et dans la somme précédente les p_i sont tous "bons", distincts deux à deux et vérifient $d_{p_i} \leq Y$; enfin on a posé

$$S_1(p_1, \ldots, p_j; \alpha_1, \ldots, \alpha_j) := \sum_{\substack{|t|\leq q^x\\ \Delta(t)\neq 0}} \prod_i \mathrm{tr}(\mathrm{Frob}_{p_i}, E_t)^{\alpha_i}.$$

Application du théorème chinois

On suppose $x \geq 2lY$ de sorte pour tout j-uple $(p_1, \ldots, p_j)$ avec $d_{p_i} \leq Y$ on a $x \geq \sum_i d_{p_i}$; on découpe alors l'ensemble $\{t \in \mathcal{Z},\ |t| \leq q^x\}$ en $q^{x+1}/|p_1 \ldots p_j|$ sous-ensembles de cardinal $|p_1 \ldots p_j|$ contenant une fois et une seule chaque classe de congruence de $\mathcal{Z}/p_1 \ldots p_j\mathcal{Z}$, comme les p_i sont supposés "bons", la fonction $\prod_{i=1}^j \operatorname{tr}(\operatorname{Frob}_{p_i}, E_t)^{\alpha_i})$ ne dépend que de la classe de t modulo $p_1 \ldots p_j$. D'après le théorème chinois (rappelons que les p_i sont deux à deux distincts), la somme $S_1(p_1, \ldots, p_j; \alpha_1, \ldots, \alpha_j)$ vaut

$$S_1(p_1, \ldots, p_j; \alpha_1, \ldots, \alpha_j) = \frac{q^{x+1}}{|p_1 \ldots p_j|} \prod_i S(p_i, \alpha_i),$$

avec

$$S(p, \alpha) = \sum_{\bar{t} \in \mathbf{A}^1(\mathbf{F}_p)} \operatorname{tr}(\operatorname{Frob}_p, E_{\bar{t}})^{\alpha}.$$

Pour $\alpha = 1$ on utilise la majoration de [Mi1] Prop. 1.2:

$$|S(p, 1)| \leq 2(\deg \Delta - 1)|p| + 2 \deg \Delta |p|^{1/2},$$

alors que pour $\alpha \geq 2$ on utilise simplement la majoration triviale (4)

$$|S(p, \alpha)| \leq 2^{\alpha} |p|^{1+\alpha/2}$$

On en déduit la majoration :

$$|S_1(p_1, \ldots, p_j; \alpha_1, \ldots, \alpha_j)| \ll_l \deg \Delta^j q^{x+1} \prod_{\substack{i=1 \\ \alpha_i \geq 2}}^{j} |p_i|^{\alpha_i/2}.$$

On déduit de cette dernière majoration et de la majoration $c_n = O_k(n^{-1})$ que $S_1(\alpha_1, \ldots, \alpha_j)$ est un

$$O_{k,l}((\deg \Delta)^j \sum_{\substack{p_1, \ldots, p_j \\ |p_i| \leq q^Y}} \frac{1}{|p_1| \ldots |p_j|}),$$

et finalement la majoration de S_1:

$$|S_1| \ll_{k,l} (\deg \Delta)^{2l} q^{x+1} \log^{2l} Y. \tag{6}$$

finalement, par (6) et (5) pour $Y \leq x/2l$ on obtient:

$$\sum_{\substack{|t| \leq q^x \\ \Delta(t) \neq 0,\ j(t) \notin \mathbf{F}_q}} |\sum_{\theta \in \{\theta\}_{E_t}} f_Y(\theta) - c_0(n_{E_t} - 4)|^{2l} = O(q^{x+1} \log^{2l} Y)$$

et par conséquant,

$$\sum_{\substack{t\in\mathcal{Z},\ |t|\le q^x\\ \Delta(t)\neq 0,\ j(t)\notin\mathbf{F}_q}} \Big|\sum_{\theta\in\{\theta\}_{E_t}} \chi_{a,X}(\theta)-c_0(n_{E_t}-4)\Big|^{2l} \ll q^{x+1}(\log^{2l}Y+x^{2l}(X/Y)^{2l(k+1)}).$$

On choisit $Y=x/2l$, $X=x^{1-\varepsilon}$ et k assez grand. Utilisant alors que $c_0=\frac{2a}{2\pi}+O(1/X)$ et l'encadrement suivant valable

$$\text{pour } \frac{1}{X}\le a\le \pi-\frac{1}{X},\ \text{on a } \chi_{a-\frac{1}{X},X}\le\chi_a\le\chi_{a,X},$$

on en tire que pour tout intervalle I de la forme $[-a,a]$, ($a\in[0,\pi]$) on a la majoration

$$(7)\quad \sum_{\substack{t\in\mathcal{Z},\ |t|\le q^x\\ \Delta(t)\neq 0,\ j(t)\notin\mathbf{F}_q}} \Big|\sum_{\theta\in\{\theta\}_{E_t}} \chi_I(\theta)-\frac{|I|}{2\pi}(n_{E_t}-4)\Big|^{2l} \ll q^{x+1}(x^{\varepsilon}+x^{2l}X^{-2l})=O(q^{x+1}x^{\varepsilon}),$$

uniformement por $a\in[0,\pi]$; puis par différence l'inégalité précédente est valable pour tout intervalle $I\subset[-\pi,\pi]$.

3.4 Minoration du conducteur.

Pour obtenir un théorème d'équirépartition à partir de l 'inégalité (7) il est nécessaire d'introduire dans la somme précédente le poids $1/(n_{E_t}-4)^{2l}$. On le fait simplement grâce à la proposition suivante qui permet de minorer le conducteur n_{E_t} à un très petit nombre d'exceptions près.

Proposition 3.1 *Le cardinal de l'ensemble des $t\in\mathcal{Z}$ vérifiant $2x/3<\deg t\le x$ et*

$$n_{E_t}\le\frac{1}{6}\max(\frac{1}{3},\frac{2\deg\Delta}{3}-1)x-3,$$

est majoré par $O((\deg\Delta)^{m+1}x^m)$ (rappelons que m est le nombre de diviseurs premiers de c).

Preuve. — L'analogue de la conjecture de Szpiro est vraie dans le cadre des corps de fonction (voir par exemple [Si] p. 287), on a:

$$n_{E_t}\ge\frac{1}{6}\deg\Delta_{min}(E_t)-2;$$

où $\Delta_{min}(E_t):=\sum_p f_{p,min}(E_t)d_p\{p\}$ désigne le diviseur positif, discriminant minimal de E_t, il suffit donc de minorer ce dernier.

Supposons d'abord $\deg\Delta=1$ alors on a nécessairement $3\deg a=2\deg b\ge 6$ ($j(T)$ est non constant), alors pour $\deg t\ge 2x/3$, on a la minoration ([Si] 3.35 p. 286)

$$\deg\Delta_{min}(E_t)\ge f_{\infty,min}(E_t)\ge 3\deg a(t)-1=3\deg_K a.\deg t-1\ge 4x-1.$$

Si $\deg \Delta \geq 2$, d'après l'hypothèse $(a(T), b(T)) = 1$, l'équation de E_t est minimale en tout p ne divisant pas c et $\neq \infty$, en particulier les valuations en p de $\Delta(t)$ et de $\Delta_{min}(E_t)$ coïncident. On a donc

$$\deg \Delta_{min}(E_t) \geq \sum_{\substack{p^{f_p} \| \Delta(t) \\ p \nmid c}} f_p d_p.$$

D'autre part, on a $\deg \Delta(t) \geq \frac{2 \deg \Delta}{3}.x$ pour $2x/3 < \deg t \leq x$, il suffit donc de montrer que le cardinal de ensemble des t vérifiant les deux conditions

$$2x/3 < \deg t \leq x, \text{ et } \sum_{\substack{q^{f_q} || \Delta(t) \\ q \neq \infty, q | c}} f_q d_q > x,$$

est majoré par $O((\deg \Delta)^m x^m)$.

Ce nombre est majoré trivialement par

$$(8) \qquad \sum_{n_1 \geq 1} \cdots \sum_{\substack{n_l \geq 1 \\ x \leq n_1 d_{q_1} + \ldots + n_m d_{q_m} \leq \deg \Delta . x}} |\{t, \ 2x/3 < \deg t \leq x, \ q_1^{n_1} \ldots q_m^{n_m} | \Delta(t)\}|.$$

Pour n assez grand, le nombre de solutions dans $\mathcal{Z}/q^n\mathcal{Z}$ de l'équation $\Delta(\bar{t}) = 0 \pmod{q^n}$ est majoré par $\deg \Delta$, ainsi la quantité (8) est majorée à une constante multiplicative près dépendant de c, par

$$\sum_{n_1 \geq 1} \cdots \sum_{\substack{n_m \geq 1 \\ x \leq n_1 d_{q_1} + \ldots + n_m d_{q_m} \leq \deg \Delta . x}} \max(1, \frac{\deg \Delta q^{x+1}}{q^{d_{q_1} n_1 + \ldots + d_{q_m} n_m}}) \ll (\deg \Delta)^{m+1} x^m.$$

□

Nous pouvons maintenant terminer la preuve du Théorème 1.1: dans la somme

$$\sum_{\substack{t \in \mathcal{Z}, \ |t| \leq q^x \\ \Delta(t) \neq 0, \ j(t) \notin \mathbf{F}_q}} \frac{1}{(n_{E_t} - 4)^{2l}} | \sum_{\theta \in \{\theta\}_{E_t}} \chi_I(\theta) - \frac{|I|}{2\pi}(n_{E_t} - 4)|^{2l},$$

la contribution des t tels que $n_{E_t} \ll x$ est majorée trivialement par $O(q^{2x/3} + x^m)$, les autres termes sont traités par (7) et par la minoration $n_{E_t} \gg x$.

3.5 Preuve du Corollaire

Pour $j = 1, \ldots x$, on considère les x sous-intervalles centrés à l'origine $I_j = [-\pi j/x, \pi j/x]$ et alors pour tout intervalle $I = [-a, a]$, on a la majoration

$$|\frac{1}{(n_{E_t} - 4)} \sum_{\theta \in \{\theta\}_{E_t}} \chi_I(\theta) - \frac{|I|}{2\pi}| \leq$$

$$\max_{j=1,\ldots,x} |\frac{1}{(n_{E_t} - 4)} \sum_{\theta \in \{\theta\}_{E_t}} \chi_{I_j}(\theta) - \frac{|I_j|}{2\pi}| + 2.2\pi/x$$

dont on déduit

$$\mathrm{discr}(\{\theta\}_{E_t}) \leq \max_{j=1,\ldots,x} \Big| \frac{1}{(n_{E_t}-4)} \sum_{\theta\in\{\theta\}_{E_t}} \chi_{I_j}(\theta) - \frac{|I_j|}{2\pi} \Big| + 2.2\pi/x;$$

Pour tout entier $l \geq 1$, on a la majoration

$$\max_{j=1,\ldots,x} \Big| \frac{1}{(n_{E_t}-4)} \sum_{\theta\in\{\theta\}_{E_t}} \chi_{I_j}(\theta) - \frac{|I_j|}{2\pi} \Big|$$

$$\leq \Big(\sum_{j=1}^{x} \Big| \frac{1}{(n_{E_t}-4)} \sum_{\theta\in\{\theta\}_{E_t}} \chi_{I_j}(\theta) - \frac{|I_j|}{2\pi} \Big|^{2l} \Big)^{1/2l}$$

ce qui donne après application de l'inégalité de Hölder et du Théorème 1.2, la majoration

$$\sum_{\substack{t\in\mathcal{Z} \\ \Delta(t)\neq 0,\ j(t)\notin\mathbf{F}_q}} \mathrm{discr}(\{\theta\}_{E_t}) \ll q^{x+1}\frac{1}{x}$$

$$+q^{(x+1)(1-\frac{1}{2l})} \Big(\sum_{j=1}^{x} \sum_{t} \Big| \frac{1}{(n_{E_t}-4)} \sum_{\theta\in\{\theta\}_{E_t}} \chi_{I_j}(\theta) - \frac{|I_j|}{2\pi} \Big|^{2l} \Big)^{1/2l}$$

$$\ll_{l,\varepsilon} q^{x+1}(\frac{1}{x} + x^{\varepsilon-1+1/(2l)})$$

Il ne reste plus qu'à choisir l assez grand pour conclure.

Remarque. — En utilisant le théorème 2.2 on pourrait montrer la majoration

$$\mathrm{discr}(\bigcup_{\substack{|t|\leq q^x \\ \Delta(t)\neq 0,\ j(t)\notin\mathbf{F}_q}} \{\theta\}_{E_t}) = O(\frac{\log x}{x}).$$

Références

[Br] A. BRUMER. — *The average rank of elliptic curves I*, Invent.Math. 109, (1992) , 445–472.

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

[K-N] L. KUIPERS, H. NIEDERREITER. — *Uniform distribution of sequences,* Pure and Applied Mathematics. Wiley-Interscience Pub. XIV, (1974).

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

[Mi1] P. MICHEL. — *Rang moyen de famille de courbes elliptiques et lois de Sato-Tate.* Mh. Math. 120, (1995) 127–136.

[Mi2] P. MICHEL. — *Le rang de familles de variétés abéliennes.* J. Alg. Geom. 6, (1997) 201–234.

[Sch] P. SCHNEIDER. — *Zur Vermütung von Birch and Swinnerton-Dyer uber globalen Funktionen körpern*, Math. Ann. 260, 495–510 (1982).

[Si] J. H. SILVERMAN. — *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag Berlin Heidelberg New-York (1994).