Le poids des polynômes irréductibles à coefficients dans un corps fini

Mireille Car, Christian Mauduit

Le poids des polynômes irréductibles à coefficients dans un corps fini
*The weight of irreducible polynomials over a finite field**

Mireille CAR

Aix-Marseille Université,

Institut de Mathématiques de Marseille CNRS, UMR 7373

CMI, 39 rue F. Joliot-Curie 13453 Marseille Cedex 13, France

Christian MAUDUIT

Aix-Marseille Université et Institut Universitaire de France,

Institut de Mathématiques de Marseille CNRS, UMR 7373

163 avenue de Luminy, Case 907, F-13288 Marseille Cedex 9, France

02/12/18

Résumé

Ce travail concerne le poids des polynômes irreductibles sur un corps fini, c'est-à-dire le nombre de coefficients non nuls de ces polynômes. Nous introduisons un analogue polynomial de la méthode de Vinogradov développée par Gallagher et Vaughan afin de majorer les sommes d'exponentielles associées. Cela nous permet d'une part d'étudier la répartition dans les progressions arithmétiques du poids des polynômes irréductibles et d'autre part de donner une estimation asymptotique (avec terme d'erreur) du nombre de polynômes irréductibles de degré fixé ayant un poids donné proche de la valeur moyenne.

*2010 AMS Classification 11T06, 11T23, 11T55.

Abstract

This work concerns the weight of irreducible polynomials over a finite field, i. e. the number of non-zero coefficients of these polynomials. We introduce a polynomial analog of the Vinogradov's method developed by Gallagher and Vaughan, which leads to upper bounds for associated exponential sums. This allows us to study the distribution in arithmetic progressions of the weight of irreducible polynomials and to provide an asymptotic estimate (with an error term) for the number of irreducible polynomials of a given degree whose weight is close to the expected value.

1 Introduction

1.1 Définitions et notations

Soit $\mathbb{F}$ un corps fini à q éléments et de caractéristisque p. On note $\mathbf{A}$ l'anneau $\mathbb{F}[T]$ des polynômes à une variable sur le corps $\mathbb{F}$, $\mathbf{M}$ l'ensemble des polynômes unitaires de $\mathbf{A}$ et $\mathbf{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbf{A}$. Pour tout nombre entier n positif, on note $\mathbf{M}_n$ l'ensemble des polynômes unitaires de degré n, $\mathbf{I}_n$ l'ensemble des polynômes irréductibles unitaires de degré n et Π_n le nombre de polynômes irréductibles unitaires de degré n.

Définition 1 Le *poids* $w(X)$ d'un polynôme $X \in \mathbf{A}$ est le nombre de ses coefficients non nuls.

On note $\mathbf{K}$ le corps $\mathbb{F}(T)$ des fractions rationnelles à coefficients dans $\mathbb{F}$. La valuation à l'infini sur $\mathbf{K}$ est l'application v_∞ de $\mathbf{K}$ dans $\mathbb{Z} \cup \{\infty\}$ définie par $v_\infty(0) = \infty$ et $v_\infty(G/H) = \deg H - \deg G$ si G et H sont des polynômes non nuls. Le complété de $\mathbf{K}$ pour la valuation v_∞ est le corps $\mathbf{K}_\infty = \mathbb{F}((T^{-1}))$ des séries de Laurent formelles $y = \sum_{n=-\infty}^{+\infty} y_n T^n$, $y_n \in F$, les coefficients y_n étant tous nuls pour n assez grand. On prolonge v_∞ à $\mathbf{K}_\infty$ en posant pour $y \neq 0$, $v_\infty(y) = -\sup\{n \in \mathbb{Z} \mid y_n \neq 0\}$. Soit $\mathcal{P}$ l'idéal de valuation de $\mathbf{K}_\infty$. Tout $y \in \mathbf{K}_\infty$ s'écrit de façon unique comme somme $y = [y] + \{y\}$ avec $[y] \in \mathbf{A}$ et $\{y\} \in \mathcal{P}$ ($[y]$ et $\{y\}$ peuvent être considérés comme les parties entière et fractionnaire de y). Soit $\psi : \mathbb{F} \mapsto \mathbb{C}$ le caractère non trivial du groupe additif de $\mathbb{F}$ défini par

$$\psi(x) = \exp(2\pi i \frac{j(\mathrm{tr}(x))}{p}),$$

j étant la bijection naturelle de $\mathbb{F}_p$ sur $\{0, 1, \ldots, p-1\}$. On associe à ψ un caractère additif non trivial de $\mathbf{K}_\infty$ en posant pour tout $y = \sum_{n=-\infty}^{+\infty} y_n T^n$ élément de $\mathbf{K}_\infty$, $E(y) = \psi(\mathrm{Res}(y))$ où $\mathrm{Res}(y) = y_{-1}$. Ce caractère est trivial sur l'anneau $\mathbf{A}$. Dans la suite de ce travail nous utiliserons souvent la conséquence immédiate suivante de cette propriété : si $(A, B, H) \in \mathbf{A}^3$ avec $H \neq 0$, alors

$$A \equiv B \pmod{H} \Rightarrow E(\frac{A}{H}) = E(\frac{B}{H}).$$

Si $Q \in \mathbf{A}$ est un polynôme de degré strictement positif, on note

$$\mathcal{C}_Q = \{X \in \mathbf{A} | \deg X < \deg Q\}$$

l'ensemble des restes de la division euclidienne par Q, où l'on convient que $\deg 0 = -\infty$. En particulier, pour tout nombre entier $n \geq 0$, $\mathcal{C}_{T^n}$ désigne l'ensemble des polynômes de $\mathbf{A}$ de degré $< n$. La valeur absolue d'un polynôme $X \in \mathbf{A}$ est définie par

$$\langle X \rangle = \begin{cases} q^{\deg X} & \text{si } X \neq 0, \\ 0 & \text{si } X = 0. \end{cases}$$

On définit les analogues polynomiaux de la fonction μ de Möbius et de la fonction Λ de Von Mangolt. La fonction μ est définie sur $\mathbf{M}$ par $\mu(X) = 0$ si $X \in \mathbf{M}$ a un facteur carré et $\mu(X) = (-1)^r$ si X est le produit de r polynômes irréductibles unitaires deux à deux distincts. La fonction Λ est définie sur $\mathbf{M}$ par $\Lambda(X) = 0$ si $X \in \mathbf{M}$ a au moins deux facteurs irréductibles unitaires distincts et $\Lambda(X) = \deg P$ si X est puissance du polynôme irréductible unitaire P.

Si H et G sont des polynômes non nuls, on note (H, G) le plus grand commun diviseur unitaire de H et G et, pour tout nombre complexe t, on note $e(t) = \exp(2\pi i t)$.

1.2 Présentation des résultats

Ce travail a pour objet l'étude de la répartition de la fonction poids sur l'ensemble des polynômes irréductibles de $\mathbb{F}[T]$. Très peu de résultats sont connus dans ce domaine et la plupart des questions concernant l'existence de polynômes ayant un poids fixé sont ouvertes (voir par exemple [1]).

Il résulte d'un travail dû à Drmota et Gutenbrunner (voir [9]) que la fonction poids vérifie un théorème central limite sur les polynômes irréductibles : on a pour tous y nombre réel fixé et n nombre entier tendant vers $+\infty$,

$$\frac{\mathrm{Card}(\{P \in \mathbf{I}, \deg P < n, w(X) \leq n\mu(q) + y\sqrt{n}\sigma(q)\})}{\mathrm{Card}(\{P \in \mathbf{I}, \deg P < n\})} = \Phi(y) + o(1),$$

avec

$$\mu(q) = \frac{q-1}{q}, \sigma(q) = \frac{(q-1)^{1/2}}{q}$$

et $\Phi(y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-t^2/2} \mathrm{d}t$ la loi de distribution normale.

Dans cet article nous étudions le comportement local de la fonction poids sur l'ensemble des polynômes irréductibles de $\mathbb{F}[T]$ et nous démontrons le théorème suivant :

Théorème 1 *Si $q \neq 2$, on a pour tout nombre entier $k \in [2, N+1]$*

$$\mathrm{Card}(\{P \in \mathbf{I}_N,\ w(P) = k\}) = \frac{\Pi_N}{\sqrt{2\pi}\sigma(q)\sqrt{N-1}} \exp(-\frac{1}{2}\frac{(\mu(q)(N-1) - k + 2)^2}{\sigma(q)^2(N-1)})$$

$$+O(\frac{\Pi_N q^2}{N}).$$

Si $q = 2$, pour tout polynôme irréductible P de degré > 1, $w(P)$ est impair et on a pour tout nombre entier k impair de l'intervalle $[2, N+1]$,

$$\mathrm{Card}(\{P \in \mathbf{I}_N,\ w(P) = k\}) = \frac{4\Pi_N}{\sqrt{2\pi}\sqrt{N-1}} \exp(-\frac{(N+3-2k)^2}{2(N-1)}) + O(\frac{\Pi_N}{N}).$$

Les constantes impliquées par les symboles O ci-dessus sont absolues.

Observons que le théorème 1 permet d'estimer le nombre de polynômes irréductibles unitaires de $\mathbb{F}_q[T]$ de degré N et de poids k lorsque $|k - \mu(q)(N-1) + 2| \leq \delta(N)$ avec $\delta(N) = o((N \log N)^{1/2})$. Pour démontrer ce théorème nous estimerons pour tous nombres entiers N et $k \geq 2$ la quantité

$$b(N,k) = \mathrm{Card}(\{P \in \mathbf{I}_N,\ w(P) = k\})$$

$$= \sum_{P \in \mathbf{I}_N} \int_{-1/2}^{1/2} e(\alpha(w(P) - k)\mathrm{d}\alpha = \int_{-1/2}^{1/2} g(\alpha)\mathrm{d}\alpha,$$

où

$$g(\alpha) = \sum_{P \in \mathbf{I}_N} e(w(P) - k).$$

Nous obtiendrons une valeur approchée de $g(\alpha)$ lorsque α est proche de 0 (plus précisément pour $|\alpha| \leq (N-1)^{\eta - 1/2}/2\pi\sigma(q)$ dans le cas où $q > 2$)

et lorsque α est proche de 0 ou 1/2 lorsque $q = 2$). Pour les autres valeurs de α nous utiliserons seulement une majoration de $|g(\alpha)|$. L'expression de cette majoration fera apparaître le nombre $\|\alpha\|$ égal à la distance de α à l'ensemble $\mathbb{Z}$ et dans le cas où $q = 2$, le nombre $\|\alpha\|_{1/2}$ égal à la distance de α à l'ensemble $\frac{1}{2}\mathbb{Z}$. L'obtention de cette majoration constituera la partie la plus importante de notre travail et sera achevée à la section 7, où nous établirons le théorème

Théorème 2 *Pour tout nombre entier $N \geq 128$ on a*

$$|\sum_{P \in \mathbf{I}_N} e(w(P))| \leq A(q) N^2 q^{N(1-3C(q,\alpha)/64)},$$

avec

$$A(q) = \frac{3}{8} q^{3C(q,\alpha)/4} (\frac{2}{q^2} + \frac{2(q-1)^2}{q(q^{1/3}-1)} + \frac{1}{2})^{1/4} + 1$$

et

$$C(q,\alpha) = \begin{cases} 4\|\alpha\|^2/q\log(q) \text{ si } q > 2, \\ 2\|\alpha\|_{1/2}^2/\log(2) \text{ si } q = 2. \end{cases}$$

Nous déduirons de ce théorème le corollaire

Corollaire *Si q est un nombre entier > 2, alors pour tout nombre entier $m > 0$ et pour tout nombre entier rationnel a on a*

$$|\mathrm{Card}(\{P \in \mathbf{I}_N; w(P) \equiv a \pmod m\}) - \frac{\Pi_N}{m}| \leq A(q) N^2 q^{N(1-3/256m^2 q\log q)}.$$

Si $q = 2$, alors pour tout nombre entier $m > 0$ impair et pour tout nombre entier rationnel a on a

$$|\mathrm{Card}(\{P \in \mathbf{I}_N; w(P) \equiv a \pmod m\}) - \frac{\Pi_N}{m}| \leq A(2) N^2 2^{N(1-3/512m^2\log 2)}.$$

La fonction w étant complètement T-additive au sens de [9] (ou [8]), ces résultats peuvent être considérés comme l'analogue dans $\mathbb{F}[T]$ de résultats obtenus par Drmota, Martin, Mauduit et Rivat dans le cas de nombres entiers (voir [10], [18], [19], [20], [21] et [23]). Le théorème de Weil [31, Appendice 5] permet habituellement d'obtenir de très bonnes majorations pour les sommes de caractères du type

$$\sum_{P \in \mathbf{I_N}} E(\alpha P)$$

($\alpha \in \mathbf{K}_\infty$) portant sur les polynômes irréductibles de $\mathbb{F}[T]$. De nombreux résultats ont été obtenus grâce à cet outil (voir par exemple [13], [28], [11,

chapitres 5 et 6], [15] et [6]. Pour obtenir la majoration du théorème 2, nous utiliserons une autre démarche car il s'agit ici d'estimer des sommes d'exponentielles du type

$$\sum_{P \in \mathbf{I_N}} e(\alpha w(P)).$$

Nous montrerons que la méthode introduite par Mauduit et Rivat dans [23] et [24] peut être adaptée à $\mathbf{I}$. Pour cela nous introduirons dans la section 4 un analogue polynomial de la méthode de Vinogradov développée par Vaughan dans [30] (voir également [16, section 13.4]) dans le prolongement des travaux antérieurs de Gallagher ([12]) et de Vaughan ([29]) (voir [27] pour un survol concernant ce type de méthodes). A notre connaissance, c'est la première fois que cette approche est utilisée dans le cadre polynomial.

2 Lemmes techniques

Tout d'abord rappelons sans démonstration le résultat fondamental suivant (voir [13]).

Proposition 2.1 *Pour tous $y \in \mathbf{K}_\infty$ et $N \in \mathbb{N}$, on a*

$$\sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} E(yX) = \begin{cases} q^N & si \quad v_\infty(\{y\}) > N, \\ 0 & sinon. \end{cases} \tag{2.1}$$

On en déduit les corollaires

Corollaire 2.2 *Pour tout $(H, G) \in \mathbf{A}^2$ avec $H \neq 0$, on a*

$$\sum_{X \in \mathcal{C}_H} E(\frac{GX}{H}) = \begin{cases} \langle H \rangle & si \quad G \equiv 0 \pmod{H}, \\ 0 & sinon. \end{cases} \tag{2.2}$$

Corollaire 2.3 *Pour tous $j \in \mathbb{N}$ et $H \in \mathbf{A}$ avec $H \neq 0$, on a*

$$|\sum_{L \in \mathbf{M}_j} E(\frac{AL}{H})| = \begin{cases} q^j \text{ si } v_\infty(\{A/H\}) > j, \\ 0 \text{ sinon.} \end{cases} \tag{2.3}$$

Preuve. On a

$$|\sum_{L\in\mathbf{M}_j} E(\frac{AL}{H})| = |\sum_{Y\in\mathcal{C}_{T^j}} E(\frac{A(T^j+Y)}{H})| = |\sum_{Y\in\mathcal{C}_{T^j}} E(\frac{Y}{H})|.$$

□

Pour tous $j \in \mathbb{N}$ et $(H, A, B) \in \mathbf{A}^3$ avec $H \neq 0$, on pose

$$S(H, A, B, j) = \sum_{X\in\mathcal{C}_H} |\sum_{L\in\mathbf{M}_j} E(\frac{(AX+B)L}{H})|. \tag{2.4}$$

Proposition 2.4 *Pour tous $j \in \mathbb{N}$ et $(H, A, B) \in \mathbf{A}^3$ avec $H \neq 0$, on a*

$$S(H, A, B, j) \leq \max(q^j\langle(A, H)\rangle, \langle H\rangle). \tag{2.5}$$

Preuve. Pour tout $X \in \mathcal{C}_H$, on note

$$s(X) = \sum_{L\in\mathbf{M}_j} E(\frac{(AX+B)L}{H}).$$

On a

$$s(X) = \sum_{Y\in\mathcal{C}_{T^j}} E(\frac{(AX+B)(T^j+Y)}{H}) = E(\frac{(AX+B)T^j}{H}) \sum_{Y\in\mathcal{C}_{T^j}} E(\frac{(AX+B)Y}{H})$$

et, d'après la proposition 2.1,

$$|s(X)| = |\sum_{Y\in\mathcal{C}_{T^j}} E(\frac{(AX+B)Y}{H})| = \sum_{Y\in\mathcal{C}_{T^j}} E(\frac{(AX+B)Y}{H}).$$

Donc

$$S(H, A, B, j) = \sum_{X\in\mathcal{C}_H} |s(X)| = \sum_{X\in\mathcal{C}_H} \sum_{Y\in\mathcal{C}_{T^j}} E(\frac{(AX+B)Y}{H}).$$

En inversant l'ordre des sommations puis en appliquant le corollaire 2.2 à la somme intérieure, on obtient

$$S(H, A, B, j) = \langle H\rangle \sum_{\substack{Y\in\mathcal{C}_{T^j} \\ H|AY}} E(\frac{BY}{H}).$$

Si l'on pose $H = (A,H)H_1,\ A = (A,H)A_1$, on remarque que $H|AY \Leftrightarrow H_1|Y$ et donc

$$S(H,A,B,j) = \langle H\rangle \sum_{\substack{Z\in\mathbf{A}\\ \deg Z<j-\deg H_1}} E(\frac{BZ}{(A,H)}),$$

d'où, avec la proposition 2.1,

$$S(H,A,B,j) = \begin{cases} \langle H\rangle \text{ si } j \le \deg H_1, \\ q^j\langle (A,H)\rangle \text{ si } j > \deg H_1 \text{ et } v_\infty(\{\frac{B}{(A,H)}\}) > j - \deg H_1, \\ 0 \text{ si } j > \deg H_1 \text{ et } v_\infty(\{\frac{B}{(A,H)}\}) \le j - \deg H_1. \end{cases}$$

□

Proposition 2.5 *Soient g une application de $\mathbf{A}$ dans $\mathbb{C}$, M et N des nombres entiers strictement positifs. Alors on a*

(2.6)
$$\sum_{\substack{H\in\mathbf{M}\\ \deg H\le M}} \sum_{\substack{G\in\mathcal{C}_H\\ (G,H)=1}} |\sum_{X\in\mathcal{C}_{T^N}} g(X)E(\frac{GX}{H})|^2 \le \max(q^N, q^{2M}) \sum_{X\in\mathcal{C}_{T^N}} |g(X)|^2.$$

Preuve. Le groupe additif $\mathbf{K}_\infty$ est localement compact. Notons dt la mesure de Haar sur ce groupe normalisée à 1 sur l'idéal de valuation $\mathcal{P}$. Les deux propriétés suivantes de cette mesure dt ont été établies par Hayes dans [13]

(i) pour tout $n \in \mathbb{Z}$ on a

$$\int_{\mathcal{P}^n} \mathrm{d}t = q^{-n}; \qquad (P_1)$$

(ii) pour tout $X \in \mathbf{A}$, on a

$$\int_{\mathcal{P}} E(Xt)\mathrm{d}t = \begin{cases} 1 \text{ si } X = 0, \\ 0 \text{ si } X \ne 0. \end{cases} \qquad (P_2)$$

Soit

$$I = \int_{\mathcal{P}} V(t)\mathrm{d}t \text{ avec } V(t) = |\sum_{X\in\mathcal{C}_{T^N}} g(X)E(tX)|^2. \qquad (\dagger)$$

Nous allons calculer I de deux façons différentes et déduire de ces calculs la majoration (2.6). D'après (†),

$$I = \int_{\mathcal{P}} \sum_{X \in \mathcal{C}_{T^N}} \sum_{Y \in \mathcal{C}_{T^N}} g(X)\overline{g(Y)}E(tX)E(-tY)\mathrm{d}t$$

$$= \sum_{X \in \mathcal{C}_{T^N}} \sum_{Y \in \mathcal{C}_{T^N}} g(X)\overline{g(Y)} \int_{\mathcal{P}} E(t(X-Y))\mathrm{d}t$$

et la propriété (P_2) nous donne

$$I = \sum_{X \in \mathcal{C}_{T^N}} |g(X)|^2. \qquad (\ddagger)$$

Nous utilisons maintenant une dissection de Farey à l'ordre M de $\mathcal{P}$. Une fraction de Farey à l'ordre M est une fraction rationnelle G/H où H est un polynôme unitaire de degré $\leq M$ et où $G \in \mathcal{C}_H^\star$, $\mathcal{C}_H^\star$ désignant l'ensemble des polynômes de $\mathcal{C}_H$ premiers à H. Notons $\mathcal{F}_M$ l'ensemble des fractions de Farey à l'ordre M. Si $G/H \in \mathcal{F}_M$, l'arc de Farey de centre G/H est la boule

$$\mathcal{A}_{G/H} = \{t \in \mathcal{P} \mid v_\infty(t - \frac{G}{H}) > M + \deg H\}.$$

D'après [13, Theorem 4-3], les arcs de Farey $\left(\mathcal{A}_{G/H}\right)_{G/H \in \mathcal{F}_M}$ forment une partition de $\mathcal{P}$. On a donc

$$I = \sum_{G/H \in \mathcal{F}_M} I_{G/H} \text{ avec } I_{G/H} = \int_{v_\infty(u) > M + \deg H} V(\frac{G}{H} + u)\mathrm{d}u. \qquad (P_3)$$

Soient G/H une fraction rationnelle et $u \in \mathcal{P}$. Si $v_\infty(u) > N$, pour tout $X \in \mathbf{A}$ tel que $\deg X < N$, on a $E(uX) = 1$, d'où $E((\frac{G}{H} + u)X) = E(\frac{G}{H}X)$. Il s'en suit l'implication

$$v_\infty(u) > N \Rightarrow V(\frac{G}{H} + u) = V(\frac{G}{H}).$$

On a donc

$$I_{G/H} \geq \int_{v_\infty(u) > \max(N, M + \deg H)} V(\frac{G}{H})\mathrm{d}u = V(\frac{G}{H})q^{-\max(N, M+\deg H)}$$

d'après (P_1). Par suite, on a $\max(q^N, q^{2M})I \geq \sum_{G/H \in \mathcal{F}_M} V(\frac{G}{H})$ et on conclut avec (‡).

□

Lemme 2.6 *Pour tout $\alpha \in \mathbb{R}$ et tout nombre réel $b > 0$, on a*

$$|1 + (b-1)e(\alpha)| \leq b(1 - \frac{8(b-1)}{b^2}\|\alpha\|^2). \tag{2.7}$$

Preuve. Voir le lemme 1 de [25].

□

Proposition 2.7 *Si l'on note, pour tous $\alpha \in \mathbb{R}$, $H \in \mathbf{A}$ et j nombre entier strictement positif,*

$$\phi_j = \phi_j(\alpha, H) = \sum_{a \in \mathbb{F}} e(\alpha w(a)) E(-\frac{aH}{T^j}), \tag{2.8}$$

alors on a

$$\phi_j \leq q(1 - c(q, \alpha)), \tag{2.9}$$

où

$$c(q,\alpha) = \begin{cases} 4\|\alpha\|^2/q \text{ si } q > 2, \\ 2\|\alpha\|_{1/2}^2 \text{ si } q = 2. \end{cases} \tag{2.10}$$

Preuve. On a

$$\phi_j = 1 + \sum_{\substack{a \in \mathbb{F} \\ a \neq 0}} e(\alpha) E(-\frac{Ha}{T^j}) = 1 - e(\alpha) + e(\alpha) \sum_{a \in \mathbb{F}} E(-\frac{Ha}{T^j})$$

et on applique la proposition 2.1.

- Si $v_\infty(\{H/T^j\}) > 1$, on a $\phi_j = 1 - e(\alpha) + qe(\alpha) = 1 + (q-1)e(\alpha)$ d'où, avec (2.7), $|\phi_j| \leq q(1 - \frac{8(q-1)}{q^2}\|\alpha\|^2)$.

- Si $v_\infty(\{H/T^j\}) \leq 1$, alors $\phi_j = 1 - e(\alpha)$ et on distingue deux cas. Si $q > 2$, on a trivialement $|\phi_j| \leq 2 \leq q - 1 \leq q(1 - \frac{4}{q}\|\alpha\|^2)$. Si $q = 2$, on a $\phi_j = 1 - e(\alpha) = 1 + e(\alpha + \frac{1}{2})$, d'où, avec (2.7), $|\phi_j| \leq 2(1 - 2\|\alpha + \frac{1}{2}\|^2)$.

On a donc

$$|\phi_j| \leq q(1 - \frac{4}{q}\|\alpha\|^2) \text{ si } q > 2$$

et

$$|\phi_j| \leq 2(1 - 2\min(\|\alpha\|^2, \|\alpha + \frac{1}{2}\|^2) \text{ si } q = 2.$$

□

3 Transformées de Fourier

Dans ce paragraphe α est un nombre réel fixé. Si $X \in \mathbf{A}$ s'écrit $X = \sum_{i=0}^{\infty} x_i T^i$, alors $w(X) = \sum_{i=0}^{\infty} w(x_i)$. Soient ℓ et m des nombres entiers tels que $0 \leq \ell < m$. Pour tout $X \in \mathbf{A}$ écrit comme ci-dessus, on définit les sommes tronquées $w_m(X), w_{\ell,m}(X)$ et $r_{\ell,m}(X)$ par

(3.1)
$$w_m(X) = \sum_{n=0}^{m-1} w(x_n), \quad w_{\ell,m}(X) = \sum_{n=\ell}^{m-1} w(x_n), \quad r_{\ell,m}(X) = \sum_{n=\ell}^{m-1} x_n T^{n-\ell}.$$

On observe que si $X \in \mathcal{C}_{T^m}$, alors $w(X) = w_m(X)$ et on pose pour tout $X \in \mathbf{A}$,

$$f_m(X) = e(\alpha w_m(X)), \quad f_{\ell,m}(X) = e(\alpha w_{\ell,m}(X)) \tag{3.2}$$

et pour tout $t \in \mathbf{K}_\infty$,

$$\widehat{f_m}(t) = q^{-m} \sum_{X \in \mathcal{C}_{T^m}} f_m(X) E(-\frac{tX}{T^m}), \tag{3.3}$$

$$\widehat{f_{\ell,m}}(t) = q^{-m} \sum_{X \in \mathcal{C}_{T^m}} f_{\ell,m}(X) E(-\frac{tX}{T^m}). \tag{3.4}$$

Bien qu'élémentaire la proposition suivante sera très utilisée dans la suite de ce travail.

Proposition 3.1 *Pour tous $(k, \ell, m) \in \mathbb{N}^3$ tel que $0 \leq k \leq \ell < m$ et $(X, Y) \in \mathbf{A}^2$, on a*

$$f_{\ell,m}(T^k X) = f_{\ell-k,m-k}(X), \tag{3.5}$$

$$f_m(X + T^\ell Y) = f_{\ell,m}(X + T^\ell Y) f_\ell(X), \tag{3.6}$$

ainsi que l'implication

$$r_{k,m}(X) = r_{k,m}(Y) \Rightarrow f_{\ell,m}(X) = f_{\ell,m}(Y). \tag{3.7}$$

Preuve. On a $w_{\ell,m}(T^kX) = w_{\ell-k,m-k}(X)$, d'où (3.5). On a aussi $w_m(X + T^\ell Y) = w_\ell(X) + w_{\ell,m}(X + T^\ell Y)$, d'où (3.6). On a $w_{\ell,m}(X) = w_{m-\ell}(r_{\ell,m}(X))$ et l'implication $r_{k,m}(X) = r_{k,m}(Y) \Rightarrow r_{\ell,m}(X) = r_{\ell,m}(Y)$, d'où l'implication (3.7).

□

Proposition 3.2 *Si k et m sont des nombres entiers tels que $0 \leq k < m$ alors, pour tous $X \in \mathbf{A}$ et $U \in \mathcal{C}_{T^{m-k}}$, on a*

$$\sum_{G \in \mathcal{C}_{T^{m-k}}} E\left(G(\frac{X}{T^m} - \frac{U}{T^{m-k}})\right) = \begin{cases} q^{m-k} \text{ si } r_{k,m}(X) = U, \\ 0 \text{ sinon.} \end{cases}$$

Preuve. D'après la proposition 2.1, la somme ci-dessus vaut 0 ou q^{m-k} et vaut q^{m-k} si et seulement si $v_\infty(\{\frac{X}{T^m} - \frac{U}{T^{m-k}}\}) > m - k$. Il suffit donc de montrer l'équivalence

$$v_\infty(\{\frac{X}{T^m} - \frac{U}{T^{m-k}}\}) > (m-k) \Leftrightarrow r_{k,m}(X) = U.$$

Or $r_{k,m}(X) = U$ si et seulement si il existe $Y \in \mathbf{A}$ tel que $\deg(X - YT^m - UT^k) < k$ c'est à dire tel que $v_\infty(Y + \frac{U}{T^{m-k}} - \frac{X}{T^m}) > m - k$, soit $v_\infty(\{\frac{X}{T^m} - \frac{U}{T^{m-k}}\}) > m - k$.

□

Proposition 3.3 *Pour tout $(\ell, m) \in \mathbb{N}^2$ tel que $0 \leq \ell < m$, on a*

$$\sum_{H \in \mathcal{C}_{T^m}} |\widehat{f_{\ell,m}}(H)|^2 = 1. \tag{3.8}$$

Preuve. On a

$$q^{2m} \sum_{H \in \mathcal{C}_{T^m}} |\widehat{f_m}(H)|^2 = \sum_{H \in \mathcal{C}_{T^m}} \sum_{X \in \mathcal{C}_{T^m}} \sum_{Y \in \mathcal{C}_{T^m}} f_{\ell,m}(X)\overline{f_{\ell,m}(Y)} E(\frac{(Y-X)H}{T^m})$$

$$= \sum_{X \in \mathcal{C}_{T^m}} \sum_{Y \in \mathcal{C}_{T^m}} f_{\ell,m}(X)\overline{f_{\ell,m}(Y)} \sum_{H \in \mathcal{C}_{T^m}} E(\frac{(Y-X)H}{T^m}),$$

d'où, avec le corollaire 2.2,

$$q^m \sum_{H \in \mathcal{C}_{T^m}} |\widehat{f_{\ell,m}}(H)|^2 = \sum_{X \in \mathcal{C}_{T^m}} |f_{\ell,m}(X)|^2 = q^m.$$

□

Proposition 3.4 *Pour tout nombre entier $m \geq 0$ et tout $t \in \mathbf{K}_\infty$ on a*

$$|\widehat{f_m}(t)| \leq q^{-C(q,\alpha)m}, \tag{3.9}$$

avec

$$C(q,\alpha) = \frac{c(q,\alpha)}{\log(q)}. \tag{3.10}$$

Preuve. Pour $m = 0$, il n'y a rien à démontrer. Si $m > 0$, on observe que $\widehat{f_m}(t) = \widehat{f_m}([t])$ et que la fonction $\widehat{f_m}$ coïncide sur $\mathbf{A}$ avec la fonction F_m définie à la section 4 de [8]. La proposition 4.2 de [8] nous donne alors

$$q^m|\widehat{f_m}(t)| = \prod_{i=1}^{m} \phi_j(\alpha, [t]).$$

La majoration (2.9) nous donne $|\widehat{f_m}(t)| \leq (1 - c(q,\alpha))^m$ et nous concluons en observant que $1 - c(q,\alpha) \leq q^{-\frac{c(q,\alpha)}{\log q}}$.

□

Notons que

$$C(q,\alpha) \leq \begin{cases} \frac{1}{q\log(q)} < 1/3 \text{ si } q \geq 3 \\ \frac{1}{8\log 2} < 1/4 \text{ si } q = 2. \end{cases} \tag{3.11}$$

Proposition 3.5 *Si ℓ, m et s sont des nombres entiers strictement positifs tels que $0 < \ell + s < m$, alors*

$$\sum_{G \in \mathcal{C}_{T^s}} \sum_{H \in \mathcal{C}_{T^m}} |\widehat{f_{\ell,m}}(H)|^2 |\widehat{f_{\ell,m}}(G+H)|^2 \leq q^{-2C(q,\alpha)(m-\ell-s)}. \tag{3.12}$$

Preuve. Soit $\mathfrak{S}$ la somme à majorer. On a $\mathfrak{S} = \sum_{H \in \mathcal{C}_{T^m}} |\widehat{f_{\ell,m}}(H)|^2 \sigma(H)$ où, pour tout $H \in \mathcal{C}_{T^m}$, $\sigma(H) = \sum_{G \in \mathcal{C}_{T^s}} |\widehat{f_{\ell,m}}(G+H)|^2$. D'après (3.4), on a

$$q^{2m}\sigma(H) = \sum_{G \in \mathcal{C}_{T^s}} \sum_{X \in \mathcal{C}_{T^m}} \sum_{Y \in \mathcal{C}_{T^m}} f_{\ell,m}(X)\overline{f_{\ell,m}(Y)} E(\frac{(Y-X)(G+H)}{T^m}).$$

En inversant l'ordre des sommations et en appliquant la proposition 2.1 on obtient

$$q^{2m}\sigma(H) = q^s \sum_{\substack{(X,Y)\in\mathcal{C}_{T^m}\times\mathcal{C}_{T^m}\\ \deg(X-Y)<m-s}} f_{\ell,m}(X)\overline{f_{\ell,m}(Y)}E(\frac{(Y-X)H}{T^m}),$$

d'où

$$q^{2m-s}\sigma(H) = \sum_{U\in\mathcal{C}_{T^{m-s}}}\sum_{V\in\mathcal{C}_{T^{m-s}}}\sum_{Z\in\mathcal{C}_{T^s}} f_{\ell,m}(U+ZT^{m-s})\overline{f_{\ell,m}(V+ZT^{m-s})}E(\frac{(V-U)H}{T^m}).$$

Comme $\ell < m-s$, on a pour tout $(U,Z)\in\mathcal{C}_{T^{m-s}}\times\mathcal{C}_{T^s}$,

$$w_{\ell,m}(U+ZT^{m-s}) = w_{\ell,m-s}(U) + w_s(Z),$$

d'où, pour tout $(U,V,Z)\in\mathcal{C}_{T^{m-s}}\times\mathcal{C}_{T^{m-s}}\times\mathcal{C}_{T^s}$,

$$f_{\ell,m}(U+ZT^{m-s})\overline{f_{\ell,m}(V+ZT^{m-s})} = f_{\ell,m-s}(U)\overline{f_{\ell,m-s}(V)}.$$

Il s'en suit que

$$q^{2m}\sigma(H) = q^{2s}\sum_{U\in\mathcal{C}_{T^{m-s}}}\sum_{V\in\mathcal{C}_{T^{m-s}}} f_{\ell,m-s}(U)\overline{f_{\ell,m-s}(V)}E(\frac{(V-U)H}{T^m})$$

et, puisque

$$\sum_{U\in\mathcal{C}_{T^{m-s}}} f_{\ell,m-s}(U)E(-\frac{UH}{T^m}) = q^{m-s}\widehat{f_{\ell,m-s}}(HT^{-s}),$$

on obtient $\sigma(H) = |\widehat{f_{\ell,m-s}}(HT^{-s})|^2$. La proposition 4.5 de [8] jointe à la proposition 2.1 nous donne

$$\sigma(H) = \begin{cases} |\widehat{f_{m-s-\ell}}(HT^{-s})|^2 \text{ si } v_\infty(\{[HT^{-s}]T^{s-m}\}) > \ell, \\ 0 \text{ sinon.} \end{cases}$$

Or $H\in\mathcal{C}_{T^m}$ vérifie $v_\infty(\{[HT^{-s}]T^{s-m}\}) > \ell$ si et seulement si $H\in\mathcal{C}_{T^{m-\ell}}$ et on a donc

$$\mathfrak{S} = \sum_{H\in\mathcal{C}_{T^{m-\ell}}} |\widehat{f_{\ell,m}}(H)|^2\widehat{f_{m-s-\ell}}(HT^{-s})|^2,$$

d'où avec (3.9) et en posant $C = C(q, \alpha)$, $\mathfrak{S} \leq q^{-2C(m-\ell-s)} \sum_{H \in \mathcal{C}_{T^{m-\ell}}} |\widehat{f_{\ell,m}}(H)|^2$. Si $H \in \mathcal{C}_{T^{m-\ell}}$, alors $v_\infty(\{H/T^m\}) > \ell$ et d'après la proposition 4.5 de [8] jointe à la proposition 2.1, on a $\widehat{f_{\ell,m}}(H) = \widehat{f_{m-\ell}}(H)$, d'où

$$\mathfrak{S} \leq q^{-2C(m-\ell-s)} \sum_{H \in \mathcal{C}_{T^{m-\ell}}} |\widehat{f_{m-\ell}}(H)|^2.$$

D'après la proposition 4.4 de [8] avec $\delta = 0$ et la proposition 4.2 de [8], on a $\sum_{H \in \mathcal{C}_{T^{m-\ell}}} |\widehat{f_{m-\ell}}(H)|^2 = 1$, ce qui termine la preuve.

□

4 La méthode de Vaughan dans $\mathbb{F}[T]$

Nous établissons ici une identité qui peut être vue comme l'analogue polynomial du lemme de Vaughan et nous en déduirons un lemme qui est la clef de la preuve.

Lemme 4.1 *Pour tout $A \in \mathbf{M}$, on a*

$$\sum_{\substack{D \in \mathbf{M} \\ D|A}} \mu(D) = \begin{cases} 1 & \text{si} \quad \deg A = 0, \\ 0 & \text{si} \quad \deg A > 0; \end{cases} \tag{4.1}$$

$$\sum_{\substack{D \in \mathbf{M} \\ D|A}} \Lambda(D) = \deg A \tag{4.2}$$

Preuve. Si $A = 1$, il n'y a rien à démontrer. On suppose $A \neq 1$. Soit $A = P_1^{a_1} \dots P_r^{a_r}$ la factorisation de A en produit de polynômes irréductibles unitaires $P_1, \dots, P_r$ deux à deux distincts. Les diviseurs unitaires de A sont de la forme $D = P_1^{b_1} \dots P_r^{b_r}$ avec $0 \leq b_i \leq a_i$. Pour un tel D, s'il existe un indice i pour lequel $b_i > 1$, $\mu(D) = 0$. Par suite

$$\sum_{\substack{D \in \mathbf{M} \\ D|A}} \mu(D) = \sum_{\substack{D \in \mathbf{M} \\ D|P_1 \dots P_r}} \mu(D) = \sum_{j=0}^{r} (-1)^j \binom{r}{j} = 0.$$

D'autre part, pour un tel diviseur D, s'il existe deux indices distincts i et j pour lesquels $b_i > 0$ et $b_j > 0$, $\Lambda(D) = 0$. Par suite

$$\sum_{\substack{D\in M\\ D|A}} \Lambda(D) = \sum_{i=1}^{r}\sum_{j=1}^{a_i} \deg P_i = \sum_{i=1}^{r} a_i \deg P_i = \deg A.$$

□

Lemme 4.2 *Pour tout polynôme unitaire A et tout nombre entier $j > 0$ tels que $\deg A \geq j$ on a*

$$\Lambda(A) = \lambda_1(A) - \lambda_2(A) + \lambda_3(A) \tag{4.3}$$

avec

$$\lambda_1(A) = \sum_{\substack{(D,X)\in\mathbf{M}\times\mathbf{M}\\ DX=A\\ \deg D<j}} \mu(D)\deg X, \tag{4.4}$$

$$\lambda_2(A) = \sum_{\substack{(D,H,X)\in\mathbf{M}\times\mathbf{M}\times\mathbf{M}\\ DHX=A\\ \deg D<j,\deg X<j}} \mu(D)\Lambda(X), \tag{4.5}$$

$$\lambda_3(A) = \sum_{\substack{(D,H,X)\in\mathbf{M}\times\mathbf{M}\times\mathbf{M}\\ DHX=A\\ \deg D\geq j,\deg X\geq j}} \mu(D)\Lambda(X), \tag{4.6}$$

Preuve. Pour tout $A \in \mathbf{M}$, on pose

$$\lambda(A) = \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY|A\\ \deg Y\geq j}} \mu(D)\Lambda(Y) = \sum_{\substack{Y\in\mathbf{M},\ Y|A\\ \deg Y\geq j}} \Lambda(Y) \sum_{\substack{D\in\mathbf{M}\\ D|(A/Y)}} \mu(D)$$

$$= \sum_{\substack{Y\in\mathbf{M},\ A/Y=1\\ \deg Y\geq j}} \Lambda(Y) = \begin{cases} \Lambda(A) \text{ si } \deg A \geq j \\ 0 \text{ sinon} \end{cases}$$

d'après (4.1). Si l'on suppose que $\deg A \geq j$, on a donc

$$\Lambda(A) = \lambda(A) = \lambda'(A) + \lambda''(A) \qquad (\dagger)$$

avec

$$\lambda'(A) = \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY|A\\ \deg D<j,\ \deg Y\geq j}} \mu(D)\Lambda(Y) \text{ et } \lambda''(A) = \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY|A\\ \deg D\geq j,\ \deg Y\geq j}} \mu(D)\Lambda(Y).$$

Observons que $\lambda''(A) = \lambda_3(A)$ et traitons $\lambda'(A)$. On a

$$\lambda'(A) = \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY|A\\ \deg D<j}} \mu(D)\Lambda(Y) - \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY|A\\ \deg D<j,\ \deg Y<j}} \mu(D)\Lambda(Y).$$

La deuxième somme ci-dessus est égale à $\lambda_2(A)$ et il nous reste donc à montrer que la première somme que nous noterons σ est égale à $\lambda_1(A)$. En posant $HY = X$ dans la somme σ on obtient

$$\sigma = \sum_{\substack{(D,X)\in\mathbf{M}\times\mathbf{M}\\ DX=A\\ \deg D<j}} \mu(D) \sum_{\substack{(H,Y)\in\mathbf{M}\times\mathbf{M}\\ HY=X}} \Lambda(Y)$$

$$= \sum_{\substack{(D,X)\in\mathbf{M}\times\mathbf{M}\\ DX=A\\ \deg D<j}} \mu(D) \sum_{\substack{Y\in\mathbf{M}\\ Y|X}} \Lambda(Y) = \sum_{\substack{(D,X)\in\mathbf{M}\times\mathbf{A}\\ DX=A\\ \deg D<j}} \mu(D)\deg X$$

d'après (4.2).

□

Nous sommes en mesure de prouver le lemme fondamental suivant qui est l'analogue de la méthode de Vaughan pour $\mathbb{F}_q[T]$.

Proposition 4.3 *Soient un nombre réel $B > 0$, un nombre entier $N \geq 4$ et g une application de $\mathbf{A}$ dans $\mathbb{C}$. On suppose que quel que soit le nombre entier $M \in [1, N]$, quelles que soient les applications $a : X \mapsto a_X$ et $b : X \mapsto b_X$ de $\mathbf{A}$ dans l'ensemble des nombres complexes de module au plus 1, on a*

(i) pour $M \leq N/4$:

$$\sum_{X \in \mathbf{M}_M} | \sum_{H \in \mathbf{M}_{N-M}} g(HX)| \leq B \tag{4.7}$$

(sommes de type I),

(ii) pour $N/4 \leq M \leq 3N/4$:

$$\left| \sum_{H \in \mathbf{M}_M} \sum_{X \in \mathbf{M}_{N-M}} a_H b_X g(HX) \right| \leq B \tag{4.8}$$

(sommes de type II).
Alors on a

$$\left| \sum_{X \in \mathbf{M}_N} \Lambda(X) g(X) \right| \leq \frac{3BN^2}{4}. \tag{4.9}$$

Preuve. Notons $\mathfrak{S}$ la somme à majorer et

$$u = \lceil N/4 \rceil. \tag{$\dagger$}$$

Le lemme 4.2 nous donne $\mathfrak{S} = S_1 - S_2 + S_3$, avec

$$S_1 = \sum_{\substack{(D,X) \in \mathbf{M} \times \mathbf{M} \\ \deg D < u \\ DX \in \mathbf{M}_N}} \mu(D) \deg(X) g(DX),$$

$$S_2 = \sum_{\substack{(D,H,Y) \in \mathbf{M} \times \mathbf{M} \times \mathbf{M} \\ \deg D < u,\ \deg Y < u \\ DHY \in \mathbf{M}_N}} \mu(D) \Lambda(Y) g(DHY),$$

$$S_3 = \sum_{\substack{(D,H,Y)\in\mathbf{M}\times\mathbf{M}\times\mathbf{M}\\ \deg D\geq u,\ \deg Y\geq u\\ DHY\in\mathbf{M}_N}} \mu(D)\Lambda(Y)g(DHY).$$

(I) Majoration de $|S_1|$. On a

$$|S_1| = |\sum_{i=0}^{u-1}\sum_{D\in\mathbf{M}_i}\mu(D)(N-i)\sum_{X\in\mathbf{M}_{N-i}} g(DX)|$$

$$\leq \sum_{i=0}^{u-1}\sum_{D\in\mathbf{M}_i}(N-i)|\sum_{X\in\mathbf{M}_{N-i}} g(DX)| = \sum_{i=0}^{u-1}(N-i)\sum_{D\in\mathbf{M}_i}|\sum_{X\in\mathbf{M}_{N-i}} g(DX)|.$$

La majoration (4.7) nous donne

$$|S_1| \leq \frac{Bu(2N-u+1)}{2}.$$

(II) Majoration de $|S_2|$. Si l'on pose $DY = X$ dans l'expression de S_2, on a

$$S_2 = \sum_{\substack{X\in\mathbf{M}\\ \deg X<2u-1}} \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY=X\\ \deg D<u,\ \deg Y<u}} \mu(D)\Lambda(Y)\sum_{H\in\mathbf{M}_{N-\deg X}} g(HX),$$

d'où

$$|S_2| \leq \sum_{\substack{X\in\mathbf{M}\\ \deg X<2u-1}} \sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY=X\\ \deg D<u,\ \deg Y<u}} \Lambda(Y)|\sum_{H\in\mathbf{M}_{N-\deg X}} g(HX)|.$$

Pour tout $X\in\mathbf{M}$, on a

$$\sum_{\substack{(D,Y)\in\mathbf{M}\times\mathbf{M}\\ DY=X\\ \deg D<u,\deg Y<u}} \Lambda(Y) \leq \sum_{\substack{Y\in\mathbf{M}\\ Y|X}} \Lambda(Y) = \deg X$$

d'après (4.2). On en déduit la majoration

$$|S_2| \leq \sum_{\substack{X\in\mathbf{M}\\ \deg X<2u-1}} \deg X| \sum_{H\in\mathbf{M}_{N-\deg X}} g(HX)|$$

$$\leq \sum_{i=0}^{2u-2} i \max_{0\leq i\leq 2u-2} \sum_{X\in\mathbf{M}_i} | \sum_{H\in\mathbf{M}_{N-i}} g(HX)|$$

$$= (u-1)(2u-1) \max_{0\leq i\leq 2u-2} \sum_{X\in\mathbf{M}_i} | \sum_{H\in\mathbf{M}_{N-i}} g(HX)|.$$

Si le maximum est atteint pour un $i < u$, la majoration (4.7) donne

$$|S_2| \leq (u-1)(2u-1)B.$$

Sinon, le maximum est atteint pour un $i \in [u, 2u-2]$ donc tel que $N/4 \leq i \leq 3N/4$. Posons pour $X \in \mathbf{M}_i$

$$\Sigma(X) = \sum_{H\in\mathbf{M}_{N-i}} g(HX) \quad \text{et} \quad a(X) = \begin{cases} \frac{|\Sigma(X)|}{\Sigma(X)} \text{ si } \Sigma(X) \neq 0, \\ 1 \text{ si } \Sigma(X) \neq 0. \end{cases}$$

Alors,

$$\sum_{X\in\mathbf{M}_i} |\Sigma(X)| = \sum_{X\in\mathbf{M}_i} a(X)\Sigma(X) = \sum_{X\in\mathbf{M}_i} \sum_{H\in\mathbf{M}_{N-i}} a(X)g(HX)$$

et la majoration (4.8) nous donne

$$\sum_{X\in\mathbf{M}_i} | \sum_{H\in\mathbf{M}_{N-i}} g(HX)| = \sum_{X\in\mathbf{M}_i} |\Sigma(X)| \leq B,$$

d'où $|S_2| \leq (u-1)(2u-1)B$.

- (III) Majoration de $|S_3|$. Écrivons S_3 sous la forme

$$S_3 = (N-u) \sum_{i=u}^{N-u} \sum_{D\in\mathbf{M}_i} \mu(D) \sum_{X\in\mathbf{M}_{N-i}} b(X)g(DX),$$

avec

$$b(X) = \frac{1}{N-u} \sum_{\substack{Y\in\mathbf{M}\\ Y|X,\ \deg Y\geq u}} \Lambda(Y).$$

Pour tout $i \in [u, N-u]$ on a $N/4 \leq u \leq i \leq N-u \leq 3N/4$ et pour tout $X \in \mathbf{M}_{N-i}$ on a d'après (4.2)

$$0 \leq b(X) \leq \frac{1}{N-u} \sum_{\substack{Y \in \mathbf{M} \\ Y|X}} \Lambda(Y) = \frac{\deg X}{N-u} \leq 1.$$

La majoration (4.8) nous donne $|S_3| \leq (N-u)(N-2u+1)B$.

- (IV) Majoration de $|S|$. En additionnant ces trois majorations, on obtient

$$|\mathfrak{S}| \leq B(\frac{u(2N-u+1)}{2} + (u-1)(2u-1) + (N-u)(N-2u+1)).$$

Pour tout nombre entier $N \geq 7$ la fonction

$$u \mapsto \frac{u(2N-u+1)}{2} + (u-1)(2u-1) + (N-u)(N-2u+1)$$

est décroissante sur l'intervalle $[\frac{N}{4}, \frac{N+3}{4}]$. Son maximum sur cet intervalle est donc égal a $\frac{23N^2+4N}{32}$, ce qui implique que, pour $N \geq 8$, on a $|\mathfrak{S}| \leq \frac{3BN^2}{4}$.

□

5 Sommes de type I

Si α est un nombre réel, μ et ν des nombres entiers tels que

$$0 < \mu \leq \nu/2, \tag{5.1}$$

on pose

$$S_{\mu,\nu} = \sum_{H \in \mathbf{M}_\mu} | \sum_{X \in \mathbf{M}_\nu} e(\alpha w(HX))|. \tag{5.2}$$

Le but de cette section est de majorer la somme $S_{\mu,\nu}$. Cette majoration résultera de la majoration de la somme

$$S'_{\mu,\nu} = \sum_{H \in \mathbf{M}_\mu} \frac{1}{\langle H \rangle} \sum_{R \in \mathcal{C}_H} |\widehat{f_{\mu+\nu}}(\frac{R}{H} T^{\mu+\nu})|. \tag{5.3}$$

comme le montre la proposition suivante.

Proposition 5.1 *Pour tout* $(\mu,\nu)\in\mathbb{N}^2$, *on a*

$$S_{\mu,\nu}\leq q^{\mu+\nu}S'_{\mu,\nu}. \tag{5.4}$$

Preuve. Posons pour $H\in\mathbf{M}_\mu$, $\sigma_H=\sum_{X\in\mathbf{M}_\nu} e(\alpha w(HX))$. Le corollaire 2.2 permet d'écrire σ_H sous la forme

$$\sigma_H=\sum_{L\in\mathbf{M}_{\mu+\nu}}\frac{e(\alpha w(L))}{\langle H\rangle}\sum_{R\in\mathcal{C}_H}E(\frac{LR}{H}),$$

d'où

$$\begin{aligned}\langle H\rangle\sigma_H&=\sum_{Y\in\mathcal{C}_{T^{\mu+\nu}}}e(\alpha w((T^{\mu+\nu}+Y)))\sum_{R\in\mathcal{C}_H}E(\frac{R(T^{\mu+\nu}+Y)}{H})\\&=e(\alpha)\sum_{Y\in\mathcal{C}_{T^{\mu+\nu}}}e(\alpha w(Y))\sum_{R\in\mathcal{C}_H}E(\frac{R(T^{\mu+\nu}+Y)}{H})\\&=e(\alpha)\sum_{R\in\mathcal{C}_H}E(\frac{RT^{\mu+\nu}}{H})\sum_{Y\in\mathcal{C}_{T^{\mu+\nu}}}e(\alpha w(Y))E(\frac{RY}{H}),\end{aligned}$$

ce qui donne avec (3.1), (3.2) et (3.3)

$$\langle H\rangle\sigma_H=q^{\mu+\nu}e(\alpha)\sum_{R\in\mathcal{C}_H}E(\frac{RT^{\mu+\nu}}{H})\widehat{f_{\mu+\nu}}(-\frac{R}{H}T^{\mu+\nu}),$$

d'où

$$\langle H\rangle|\sigma_H|\leq q^{\mu+\nu}\sum_{R\in\mathcal{C}_H}|\widehat{f_{\mu+\nu}}(-\frac{R}{H})T^{\mu+\nu})|.$$

On obtient avec (5.2)

$$S_{\mu,\nu}=\sum_{H\in\mathbf{M}_\mu}|\sigma_H|\leq\sum_{H\in\mathbf{M}_\mu}\frac{q^{\mu+\nu}}{\langle H\rangle}\sum_{R\in\mathcal{C}_H}|\widehat{f_{\mu+\nu}}((-\frac{R}{H})T^{\mu+\nu})|.$$

□

Proposition 5.2 *Pour tout* $(\mu,\nu)\in\mathbb{N}^2$ *tel que* $0<\mu\leq\nu/2$, *on a*

$$S'_{\mu,\nu}\leq\mu q^{-C(q,\alpha)(\mu+\nu)/3}. \tag{5.5}$$

Preuve. Dans la somme $S'_{\mu,\nu}$ on divise la somme intérieure en sommes partielles suivant les valeurs de $D = (H, R)$. Il vient

$$S'_{\mu,\nu} = \sum_{\substack{D\in\mathbf{M}\\ \deg D\le\mu}} \sum_{H\in\mathbf{M}_{\mu-\deg D}} \frac{1}{\langle HD\rangle} \sum_{\substack{G\in\mathcal{C}_H\\ (G,H)=1}} |\widehat{f_{\mu+\nu}}(\frac{G}{H}T^{\mu+\nu}|. \tag{5.6}$$

Pour tout polynôme unitaire D tel que $\deg D \le \mu$, on pose

$$\kappa(D) = 2(\mu - \deg D). \tag{5.7}$$

D'après (5.1), on a

$$\kappa(D) \le 2\mu \le \frac{2}{3}(\mu+\nu). \tag{5.8}$$

Soient $t \in \mathbf{K}_\infty$ et un nombre entier $\kappa < \mu+\nu$. En écrivant $X \in \mathcal{C}_{T^{\mu+\nu}}$ comme somme $X = U + VT^\kappa$ avec $U \in \mathcal{C}_{T^\kappa}$ et $V \in \mathcal{C}_{T^{\mu+\nu-\kappa}}$ on obtient avec (3.2) et (3.3)

$$q^{\mu+\nu}\widehat{f_{\mu+\nu}}(t) = \sum_{U\in\mathcal{C}_{T^\kappa}} \sum_{V\in\mathcal{C}_{T^{\mu+\nu-\kappa}}} e(\alpha w(U+VT^\kappa))E(-t\frac{U+VT^\kappa}{T^{\mu+\nu}})$$

$$= \sum_{U\in\mathcal{C}_{T^\kappa}} \sum_{V\in\mathcal{C}_{T^{\mu+\nu-\kappa}}} e(\alpha(w(U)+w(V)))E(-t\frac{U}{T^{\mu+\nu}} - t\frac{V}{T^{\mu+\nu-\kappa}}),$$

ce qui nous donne

$$\widehat{f_{\mu+\nu}}(t) = \frac{1}{q^{\mu+\nu-\kappa}} \sum_{V\in\mathcal{C}_{T^{\mu+\nu-\kappa}}} e(\alpha w(V))E(-t\frac{V}{T^{\mu+\nu-\kappa}})\frac{1}{q^\kappa}\sum_{U\in\mathcal{C}_{T^\kappa}} e(\alpha w(U))E(-t\frac{U}{T^{\mu+\nu}}),$$

soit

$$\widehat{f_{\mu+\nu}}(t) = \widehat{f_{\mu+\nu-\kappa}}(t)\frac{1}{q^\kappa}\sum_{U\in\mathcal{C}_{T^\kappa}} e(\alpha w(U))E(-t\frac{U}{T^{\mu+\nu}}).$$

Si nous portons cette égalité dans la somme (5.6) en prenant $\kappa = \kappa(D)$ et $t = -\frac{G}{H}T^{\mu+\nu}$, nous obtenons

$$S'_{\mu,\nu} = \sum_{\substack{D\in\mathbf{M}\\ \deg D\le\mu}} \frac{1}{\langle D\rangle} \sum_{H\in\mathbf{M}_{\mu-\deg D}} \frac{1}{\langle H\rangle} \sum_{\substack{G\in\mathcal{C}_H\\ (G,H)=1}} |\widehat{f_{\mu+\nu-\kappa(D)}}(\frac{G}{H}T^{\mu+\nu})|$$

$$\times \frac{1}{q^{\kappa(D)}} |\sum_{U\in\mathcal{C}_{T^{\kappa(D)}}} e(\alpha w(U))E(-\frac{GU}{H})|.$$

D'après la proposition 3.4 et la majoration (5.8), on a $|\widehat{f_{\mu+\nu-\kappa(D)}}(\frac{G}{H}T^{\mu+\nu})| \le q^{-C(\mu+\nu-\kappa(D))} \le q^{-C(\mu+\nu)/3}$, où l'on a posé $C = C(q,\alpha)$. Par suite

$$S'_{\mu,\nu} \le q^{-C(\mu+\nu)/3} \sum_{\substack{D\in\mathbf{M}\\ \deg D\le\mu}} \frac{1}{\langle D\rangle q^{\kappa(D)}} \sum_{H\in\mathbf{M}_{\mu-\deg D}} \frac{1}{\langle H\rangle} T(D,H),$$

avec

$$T(D,H) = \sum_{\substack{G\in\mathcal{C}_H\\ (G,H)=1}} |\sum_{U\in\mathcal{C}_{T^{\kappa(D)}}} e(\alpha w(U))E(\frac{GU}{H})|.$$

On a donc

$$S'_{\mu,\nu} \le q^{-C(\mu+\nu)/3} \sum_{\substack{D\in\mathbf{M}\\ \deg D\le\mu}} \frac{1}{\langle D\rangle q^{\kappa(D)}} S''(\mu,D) \tag{5.9}$$

avec

$$S''(\mu,D) = \sum_{H\in\mathbf{M}_{\mu-\deg D}} \frac{1}{\langle H\rangle} \sum_{\substack{G\in\mathcal{C}_H\\ (G,H)=1}} |\sum_{U\in\mathcal{C}_{T^{\kappa(D)}}} e(\alpha w(U))E(\frac{GU}{H})|. \tag{5.10}$$

L'inégalité de Cauchy-Schwarz nous donne $S''(\mu,D)^2 \le AB$ avec

$$A = \sum_{H\in\mathbf{M}_{\mu-\deg D}} \frac{1}{\langle H\rangle^2} \mathrm{Card}(\{G\in\mathcal{C}_H; (G,H)=1\})$$

et

$$B = \sum_{H \in \mathbf{M}_{\mu - \deg D}} \sum_{\substack{G \in \mathcal{C}_H \\ (G,H)=1}} \left| \sum_{U \in \mathcal{C}_{T^{\kappa(D)}}} e(\alpha w(U)) E(\frac{GU}{H}) \right|^2$$

qui vérifient $A \leq \sum_{H \in \mathbf{M}_{\mu - \deg D}} \frac{1}{\langle H \rangle} = 1$ et

$$B \leq \sum_{\substack{H \in \mathbf{M} \\ \deg H \leq \mu - \deg D}} \sum_{\substack{G \in \mathcal{C}_H \\ (G,H)=1}} \left| \sum_{U \in \mathcal{C}_{T^{\kappa(D)}}} e(\alpha w(U)) E(\frac{GU}{H}) \right|^2 .$$

La proposition 2.5, où l'on remplace M par $\mu - \deg D$, N par $\kappa(D)$ et où l'on prend pour fonction g la fonction $U \to e(\alpha w(U))$, nous donne $B \leq \max(q^{2(\mu - \deg D)}, q^{\kappa(D)}) q^{\kappa(D)}$ d'où, avec (5.7), $B \leq q^{2\kappa(D)}$. Par suite, $S''(\mu, D) \leq q^{\kappa(D)}$, d'où, avec (5.9),

$$S'_{\mu,\nu} \leq q^{-C(\mu+\nu)/3} \sum_{\substack{D \in \mathbf{M} \\ \deg D \leq \mu}} \frac{1}{\langle D \rangle} = \mu q^{-C(\mu+\nu)/3}.$$

□

Proposition 5.3 *Pour tout $(\mu, \nu) \in \mathbb{N}^2$ tel que $0 < \mu \leq \nu/2$, on a*

$$S_{\mu,\nu} \leq \mu q^{(1 - C(q,\alpha)/3)(\mu+\nu)}. \tag{5.11}$$

Preuve. Cela résulte immédiatement de (5.4) et (5.5).

□

6 Sommes de type II

Soient α un nombre réel, $X \mapsto a_X$ et $X \mapsto b_X$ des applications de $\mathbf{A}$ dans l'ensemble des nombres complexes de module au plus 1. On se donne des nombres entiers $\mu \leq \nu$ et on pose

$$T_{\mu,\nu} = \sum_{H \in \mathbf{M}_\mu} \sum_{Y \in \mathbf{M}_\nu} a_H b_Y e(\alpha w(XY)). \tag{6.1}$$

Le but de cette section est la majoration de la somme $T_{\mu,\nu}$ qui sera obtenue lorsque $\mu \geq 32$. On pose

$$f(X) = e(\alpha w(X)). \tag{6.2}$$

On considère un nombre entier r tel que

$$4 < 4r < \nu \tag{6.3}$$

et on pose

$$\begin{cases} m = \mu + 2r, \\ s = 2r \\ \ell = \mu - 2r. \end{cases} \tag{6.4}$$

Proposition 6.1 *On a*

$$|T_{\mu,\nu}|^2 \leq q^{2(\mu+\nu)-r} + q^{\mu+\nu-r} \sum_{\substack{R \in \mathcal{C}_{T^r} \\ R \neq 0}} T_1(R) \tag{6.5}$$

où

$$T_1(R) = \sum_{H \in \mathbf{M}_\mu} \sum_{Y \in \mathbf{M}_\nu} b_{Y+R} \overline{b_Y} f(H(Y+R)) \overline{f(HY)}. \tag{6.6}$$

Preuve. L'inégalité de Cauchy-Schwarz appliquée à (6.1) nous donne

$$|T_{\mu,\nu}|^2 \leq q^\mu \sum_{H \in \mathbf{M}_\mu} |s_H|^2, \tag{†}$$

où

$$s_H = \sum_{X \in \mathbf{M}_\nu} b_X f(HX). \tag{‡}$$

Fixons $H \in \mathbf{M}_\mu$. Pour $R \in \mathcal{C}_{T^r}$ et $X \in \mathbf{M}_\nu$, on a d'après (6.3), $\deg R < \nu = \deg X$. L'application $X \mapsto X + R$ est une permutation de $\mathbf{M}_\nu$ et donc

$$s_H = \sum_{X \in \mathbf{M}_\nu} b_{X+R} f(H(X+R)).$$

On a donc

$$\mathrm{Card}(\mathcal{C}_{T^r})s_H = \sum_{R\in\mathcal{C}_{T^r}} \sum_{X\in\mathbf{M}_\nu} b_{X+R} f(H(X+R)),$$

d'où

$$q^r s_H = \sum_{X\in\mathbf{M}_\nu} \sum_{R\in\mathcal{C}_{T^r}} b_{X+R} f(H(X+R)).$$

L'inégalité de Cauchy-Schwarz nous donne alors

$$q^{2r}|s_H|^2 \le q^\nu \sum_{X\in\mathbf{M}_\nu} \sum_{R_1\in\mathcal{C}_{T^r}} \sum_{R_2\in\mathcal{C}_{T^r}} b_{X+R_1} f(H(X+R_1))\overline{b_{X+R_2} f(H(X+R_2))}.$$

En posant $R = R_1 - R_2$ et $Y = X + R_2$ on obtient

$$q^{2r}|s_H|^2 \le q^\nu \sum_{Y\in\mathbf{M}_\nu} \sum_{R_1\in\mathcal{C}_{T^r}} \sum_{R\in\mathcal{C}_{T^r}} b_{Y+R} f(H(Y+R))\overline{b_Y f(HY)},$$

soit

$$q^r|s_H|^2 \le q^\nu \sum_{Y\in\mathbf{M}_\nu} \sum_{R\in\mathcal{C}_{T^r}} b_{Y+R}\overline{b_Y} f(H(Y+R))\overline{f(HY)}.$$

En reportant cette majoration dans (†) et en inversant l'ordre des sommations, on obtient

$$q^r|T_{\mu,\nu}|^2 \le q^{\mu+\nu} \sum_{R\in\mathcal{C}_{T^r}} \sum_{H\in\mathbf{M}_\mu} \sum_{Y\in\mathbf{M}_\nu} b_{Y+R}\overline{b_Y} f(H(Y+R))\overline{f(HY)}.$$

□

Proposition 6.2 *On a*

$$|T_{\mu,\nu}|^4 \le 2(2q^{4(\mu+\nu)-2r} + q^{3(\mu+\nu)-3r} \sum_{\substack{R\in\mathcal{C}_{T^r}\\ R\neq 0}} \sum_{\substack{S\in\mathcal{C}_{T^s}\\ S\neq 0}} T_2(R,S)), \tag{6.7}$$

avec

$$T_2(R,S) = \sum_{X\in\mathbf{M}_\mu} \sum_{Y\in\mathbf{M}_\nu} \Phi_{\ell,m}(X,Y,R,S), \tag{6.8}$$

où

$$\Phi_{\ell,m}(X,Y,R,S) = f_{\ell,m}((X+T^\ell S)(Y+R))f_{\ell,m}(XY)$$

$$\times\overline{f_{\ell,m}((X+T^\ell S)Y)f_{\ell,m}(X(Y+R))}, \tag{6.9}$$

$f_{\ell,m}$ étant définie par (3.2).

Preuve. Si l'on pose

$$T^\star = \sum_{\substack{R\in\mathcal{C}_{T^r}\\ R\neq 0}} T_1(R),$$

il résulte de (6.5) que l'on a

$$|T_{\mu,\nu}|^4 \leq 2(q^{4(\mu+\nu)-2r} + q^{2(\mu+\nu-r)}|T^\star|^2). \tag{6.10}$$

L'inégalité de Cauchy-Schwarz appliquée à la somme $T^\star$ donne

$$|T^\star|^2 \leq (q^r-1)\sum_{\substack{R\in\mathcal{C}_{T^r}\\ R\neq 0}} |T_1(R)|^2. \tag{6.11}$$

Soit $R\in\mathcal{C}_{T^r}$ non nul. Si l'on pose, pour tout $H\in\mathbf{M}_\mu$ et $Y\in\mathbf{M}_\nu$

$$HY = \sum_{i=0}^{\infty} u_i T^i,\ HR = \sum_{i=0}^{\infty} v_i T^i, \text{ avec } u_i \text{ et } v_i \text{ dans } \mathbb{F} \text{ pour tout } i\in\mathbb{N},$$

on a

$$f(H(Y+R))\overline{f(HY)} = e(\alpha w(H(Y+R))-\alpha w(HY)) = e(\alpha(\sum_{i=0}^{\infty} w(u_i+v_i)-\sum_{i=0}^{\infty} w(u_i))).$$

Comme $\deg(HR) < \mu+r < m$, on a $v_i = 0$ pour $i\geq m$ et par suite,

$$f(H(Y+R))\overline{f(HY)} = e(\alpha(\sum_{i=0}^{m-1} w(u_i+v_i) + \sum_{i=m}^{\infty} w(u_i) - \sum_{i=0}^{\infty} w(u_i)))$$

$$= e(\alpha(\sum_{i=0}^{m-1} w(u_i+u_i) - \sum_{i=0}^{m-1} w(u_i)) = f_m(H(Y+R))\overline{f_m(HY)},$$

f_m étant défini par (3.2). Avec (6.6) on obtient

$$T_1(R) = \sum_{H\in\mathbf{M}_\mu} \sum_{Y\in\mathbf{M}_\nu} b_{Y+R}\overline{b_Y} f_m(H(Y+R))\overline{f_m(HY)},$$

d'où

$$T_1(R) = \sum_{Y\in\mathbf{M}_\nu} b_{Y+R}\overline{b_Y} U(Y) \tag{6.12}$$

avec

$$U(Y) = \sum_{H\in\mathbf{M}_\mu} f_m(H(Y+R))\overline{f_m(HY)}. \tag{6.13}$$

L'inégalité de Cauchy-Schwarz appliquée à la somme (6.12) donne

$$|T_1(R)|^2 \le q^\nu \sum_{Y\in\mathbf{M}_\nu} |U(Y)|^2. \tag{6.14}$$

Pour tout $S \in \mathcal{C}_{T^s}$, on a $\deg(T^\ell S) \le (\ell+s)-1 \le \mu-1$, d'où $(H+T^\ell S) \in \mathbf{M}_\mu$ pour tout $H \in \mathbf{M}_\mu$. L'application $H \mapsto H + T^\ell S$ étant une permutation de $\mathbf{M}_\mu$, on obtient comme pour la proposition précédente,

$$q^s U(Y) = \sum_{H\in\mathbf{M}_\mu} \sum_{S\in\mathcal{C}_{T^s}} f_m((H+T^\ell S)(Y+R))\overline{f_m((H+T^\ell S)Y)}.$$

L'inégalité de Cauchy-Schwarz nous donne alors

$$q^{2s}|U(Y)|^2 \le q^\mu \sum_{H\in\mathbf{M}_\mu} \sum_{S_1\in\mathcal{C}_{T^s}} \sum_{S_2\in\mathcal{C}_{T^s}} f_m((H+T^\ell S_1)(Y+R))\overline{f_m((H+T^\ell S_1)Y)}$$

$$\times\overline{f_m((H+T^\ell S_2)(Y+R))} f_m((H+T^\ell S_2)Y).$$

Les changements de variable $S = S_1 - S_2$ et $K = H + T^\ell S_2$ montrent que

$$q^{2s}|U(Y)|^2 \leq q^{\mu} \sum_{K\in\mathbf{M}_\mu} \sum_{S_1\in\mathcal{C}_{T^s}} \sum_{S\in\mathcal{C}_{T^s}} \Phi(K,Y,R,S),$$

où

$$\Phi(K,Y,R,S) = f_m((K+T^\ell S)(Y+R))f_m(KY)\overline{f_m((K+T^\ell S)Y)f_m(K(Y+R))},$$

d'où

$$|U(Y)|^2 \leq q^{\mu-s} \sum_{K\in\mathbf{M}_\mu} \sum_{S\in\mathcal{C}_{T^s}} \Phi(K,Y,R,S).$$

Comme $\Phi(K,Y,R,0) = 1$, (6.14) nous donne

$$|T_1(R)|^2 \leq q^{2(\mu+\nu)-s} + q^{\mu+\nu-s} \sum_{Y\in\mathbf{M}_\nu} \sum_{K\in\mathbf{M}_\mu} \sum_{\substack{S\in\mathcal{C}_{T^s}\\ S\neq 0}} \Phi(K,Y,R,S).$$

Avec (6.11), il vient

$$|T^\star|^2 \leq q^{2(\mu+\nu+r)-s} + q^{\mu+\nu+r-s} \sum_{\substack{R\in\mathcal{C}_{T^r}\\ R\neq 0}} \sum_{Y\in\mathbf{M}_\nu} \sum_{K\in\mathbf{M}_\mu} \sum_{\substack{S\in\mathcal{C}_{T^s}\\ S\neq 0}} \Phi(K,Y,R,S).$$

Montrons que Φ vérifie (6.9) ce qui, avec (6.4) et (6.10) nous permettra de conclure. La proposition 3.1 nous donne

$$f_m((K+T^\ell S)(Y+R)) = f_{\ell,m}((K+T^\ell S)(Y+R))f_\ell((K+T^\ell S)(Y+R))$$

$= f_{\ell,m}((K+T^\ell S)(Y+R))f_\ell(K(Y+R))$. De même $f_m((K+T^\ell S)Y) = f_{\ell,m}((K+T^\ell S)Y)f_\ell(KY)$ et par suite $\Phi(K,Y,R,S) =$
$f_{\ell,m}((K+T^\ell S)(Y+R))f_{\ell,m}(KY)\overline{f_{\ell,m}(K(Y+R))f_{\ell,m}((K+T^\ell S)Y)}$.

□

Si k est un nombre entier tel que $r \leq k < \ell$, on pose

(6.15) $$g = f_{\ell-k,m-k}.$$

Proposition 6.3 *Pour $R \in \mathcal{C}_{T^r}$ et $S \in \mathcal{C}_{T^s}$ non nuls, on a*

$$T_2(R,S) = T_3(R,S) + T_4(R,S), \tag{6.16}$$

avec

$$T_3(R,S) = \sum_{(G,G_1,H_1)\in(\mathcal{C}_{T^{m-k}})^3} \hat{g}(G-G_1)\overline{\hat{g}(H_1+G)}\hat{g}(H_1)\overline{\hat{g}(-G_1)} \times \sum_{X\in\mathbf{M}_\mu}\sum_{Y\in\mathbf{M}_\nu} E(-\frac{GXR}{T^m} + \frac{(G_1+H_1)SY}{T^{m-\ell}}) \tag{6.17}$$

et

$$T_4(R,S) = \sum_{\substack{(G,H)\in(\mathcal{C}_{T^{m-k}})^2 \\ G\neq -H}} \sum_{(G_1,H_1)\in(\mathcal{C}_{T^{m-k}})^2} \hat{g}(G-G_1)\overline{\hat{g}(H_1-H)}\hat{g}(H_1)\overline{\hat{g}(-G_1)} \times \sum_{X\in\mathbf{M}_\mu}\sum_{Y\in\mathbf{M}_\nu} E(\frac{(G+H)XY + HXR + (G_1+H_1)T^\ell SY}{T^m}). \tag{6.18}$$

Preuve. Soient $(X,Y,R,S) \in \mathbf{M}_\mu \times \mathbf{M}_\nu \times \mathcal{C}_{T^r} \times \mathcal{C}_{T^s}$ et $(U,V) \in \mathcal{C}_{T^{m-k}}^2$ tels que $r_{k,m}(XY) = U$ et $r_{k,m}(X(Y+R)) = V$, les fonctions $r_{k,m}$ étant celles définies par (3.1). Alors il existe $(B,W) \in \mathbf{A} \times \mathcal{C}_{T^k}$ tel que

$$XY = BT^m + UT^k + W.$$

Si $U' = r_{k,m}(XY + T^\ell SY)$ et $U'' = r_{k,m}(T^k U + T^\ell SY)$, alors il existe $(B',W') \in \mathbf{A} \times \mathcal{C}_{T^k}$ et $(B'',W'') \in \mathbf{A} \times \mathcal{C}_{T^k}$ tels que

$$XY + T^\ell SY = B'T^m + U'T^k + W' \text{ et } T^kU + T^\ell SY = B''T^m + U''T^k + W'',$$

d'où $(B - B' + B'')T^m - (U' - U'')T^k = W' - W'' - W$, ce qui entraîne $B - B' + B'' = U' - U'' = W' - W'' - W = 0$. On a donc $r_{k,m}(XY + T^\ell SY) = r_{k,m}(T^kU + T^\ell SY)$. La proposition 3.1 nous donne $f_{\ell,m}(XY + T^\ell SY) = f_{\ell,m}(T^kU + T^\ell SY) = f_{\ell-k,m-k}(U + T^{\ell-k}SY)) = g(U + T^{\ell-k}SY)$. De la même façon, $f_{\ell,m}(X(Y+R) + T^\ell S(Y+R)) = g((V + T^{\ell-k}S(Y+R)))$, $f_{\ell,m}(XY) = g(U)$ et $f_{\ell,m}(X(Y+R)) = g(V)$. D'après (6.8) et (6.9), on a

$$T_2(R,S)=\sum_{X\in\mathbf{M}_\mu}\sum_{Y\in\mathbf{M}_\nu}\sum_{\substack{U\in\mathcal{C}_{T^{m-k}}\\ r_{k,m}(XY)=U}}\sum_{\substack{V\in\mathcal{C}_{T^{m-k}}\\ r_{k,m}(X(Y+R))=V}} g(U)g(V+T^{\ell-k}S(Y+R))$$

$$\times\overline{g(V)g(U+T^{\ell-k}SY)}.$$

La proposition 3.2 nous donne alors

$$q^{2(m-k)}T_2(R,S)=\sum_{X\in\mathbf{M}_\mu}\sum_{Y\in\mathbf{M}_\nu}\sum_{U\in\mathcal{C}_{T^{m-k}}}\sum_{G\in\mathcal{C}_{T^{m-k}}}E((\frac{XY}{T^m}-\frac{U}{T^{m-k}})G)$$

$$\sum_{V\in\mathcal{C}_{T^{m-k}}}\sum_{H\in\mathcal{C}_{T^{m-k}}}E((\frac{X(Y+R)}{T^m}-\frac{V}{T^{m-k}})H)$$

$$\times g(U)g(V+T^{\ell-k}S(Y+R))\overline{g(V)g(U+T^{\ell-k}SY)}.$$

Si $U\in\mathcal{C}_{T^{m-k}}$ et $U_1\in\mathcal{C}_{T^{m-k}}$ sont tels que $U+T^{\ell-k}SY\equiv U_1 \pmod{T^{m-k}}$, alors

$$g(U+T^{\ell-k}SY)=f_{\ell-k,m-k}(U+T^{\ell-k}SY)=f_{\ell-k,m-k}(U_1)=g(U_1).$$

De même, si $V\in\mathcal{C}_{T^{m-k}}$ et $V_1\in\mathcal{C}_{T^{m-k}}$ sont tels que $V+T^{\ell-k}S(Y+R)\equiv V_1 \pmod{T^{m-k}}$, alors $g(V+T^{\ell-k}S(Y+R))=g(V_1)$. En faisant appel au corollaire 2.2 on obtient

$$q^{4(m-k)}T_2(R,S)=\sum_{X\in\mathbf{M}_\mu}\sum_{Y\in\mathbf{M}_\nu}\sum_{U\in\mathcal{C}_{T^{m-k}}}\sum_{V\in\mathcal{C}_{T^{m-k}}}$$

$$\sum_{U_1\in\mathcal{C}_{T^{m-k}}}\sum_{V_1\in\mathcal{C}_{T^{m-k}}}\sum_{G\in\mathcal{C}_{T^{m-k}}}E((\frac{XY}{T^m}-\frac{U}{T^{m-k}})G)\sum_{H\in\mathcal{C}_{T^{m-k}}}E((\frac{X(Y+R)}{T^m}-\frac{V}{T^{m-k}})H)$$

$$\sum_{G_1\in\mathcal{C}_{T^{m-k}}}E(\frac{(U+T^{\ell-k}SY-U_1)G_1}{T^{m-k}})\sum_{H_1\in\mathcal{C}_{T^{m-k}}}E(\frac{(V+T^{\ell-k}S(Y+R)-V_1)H_1}{T^{m-k}})$$

$$\times g(U)g(V_1)\overline{g(V)g(U_1)}.$$

En utilisant les transformées de Fourier de $g=f_{l-k,m-k}$, on obtient

$$T_2(R,S)=\sum_{X\in\mathbf{M}_\mu}\sum_{Y\in\mathbf{M}_\nu}\sum_{(G,H)\in(\mathcal{C}_{T^{m-k}})^2}\sum_{(G_1,H_1)\in(\mathcal{C}_{T^{m-k}})^2}\hat{g}(G-G_1)\hat{g}(H_1)$$

$$\times\overline{\hat{g}(H_1-H)\hat{g}(-G_1)}E\left(\frac{H_1SR}{T^{m-\ell}}+\frac{(G+H)XY+HXR+(G_1+H_1)T^\ell SY}{T^m}\right).$$

On inverse maintenant l'ordre de sommation et on divise la somme en deux parties $T_2(R,S)=T_3(R,S)+T_4(R,S)$ où $T_3(R,S)$ contient les couples (G,H) tels que $G+H=0$ et où $T_4(R,S)$ contient les couples (G,H) tels que $G+H\neq 0$.

□

Proposition 6.4 *Pour $R\in\mathcal{C}_{T^r}$ et $S\in\mathcal{C}_{T^s}$ non nuls, on a*

$$|T_4(R,S)|\leq \max(1,q^{\nu-m})q^{\mu+3(m-k)}. \tag{6.19}$$

Preuve. D'après (6.18),

$$|T_4(R,S)|\leq \sum_{\substack{(G,H)\in(\mathcal{C}_{T^{m-k}})^2\\ G\neq -H}}\ \sum_{(G_1,H_1)\in(\mathcal{C}_{T^{m-k}})^2}|\hat{g}(G-G_1)\hat{g}(H_1-H)\hat{g}(H_1)\hat{g}(-G_1)|$$

$$\times|a(G,H,G_1,H_1)| \tag{$\dagger$}$$

où

$$a(G,H,G_1,H_1)=\sum_{Y\in\mathbf{M}_\nu}\sum_{X\in\mathbf{M}_\mu}E(\frac{(G+H)XY+HXR+(G_1+H_1)T^\ell SY}{T^m}).$$

On a

$$|a(G,H,G_1,H_1)|\leq\sum_{Y\in\mathbf{M}_\nu}|\sum_{X\in\mathbf{M}_\mu}E(\frac{(G+H)XY+HXR}{T^m})|$$

$$\leq\sum_{Y\in\mathcal{C}_{T^\nu}}|\sum_{X\in\mathbf{M}_\mu}E(\frac{(G+H)XY+HXR}{T^m})|$$

$$=\sum_{Y_1\in\mathcal{C}_{T^{\nu-m}}}\sum_{Y_2\in\mathcal{C}_{T^m}}|\sum_{X\in\mathbf{M}_\mu}E(\frac{(G+H)X(Y_1T^m+Y_2)+HXR}{T^m})|,$$

où l'on convient que $\mathcal{C}_{T^{\nu-m}}=\{0\}$ lorsque $\nu<m$. Donc,

$$|a(G,H,G_1,H_1)| \leq \max(1,q^{\nu-m}) \sum_{Y_2 \in \mathcal{C}_{T^m}} |\sum_{X \in \mathbf{M}_\mu} E(\frac{(G+H)XY_2+HXR}{T^m})|$$

et la proposition 2.4 nous donne alors

$$|a(G,H,G_1,H_1)| \leq \max(1,q^{\nu-m}) \max(q^\mu \langle (G+H,T^m)\rangle, q^m).$$

Comme $(G,H) \in \mathcal{C}_{T^{m-k}} \times \mathcal{C}_{T^{m-k}}$, on a $\deg((G+H,T^m)) < m-k$, d'où

$$|a(G,H,G_1,H_1)| \leq \max(1,q^{\nu-m}) \max(q^{\mu+m-k}, q^m).$$

Comme $k < \ell$, on a avec (6.4), $\mu - k > 2r \geq 2$, d'où $q^{\mu+m-k} \geq q^{m+3}$ et

$$|a(G,H,G_1,H_1)| \leq \max(1,q^{\nu-m}) q^{\mu+m-k} = \beta. \qquad (\ddagger)$$

Avec (†) et (‡) il vient

$$|T_4(R,S)| \leq \beta \sum_{\substack{(G,H) \in (\mathcal{C}_{T^{m-k}})^2 \\ G \neq -H}} \sum_{(G_1,H_1) \in (\mathcal{C}_{T^{m-k}})^2} |\hat{g}(G-G_1)\hat{g}(H_1-H)\hat{g}(H_1)\hat{g}(-G_1)|$$

$$\leq \beta \sum_{(G,H) \in (\mathcal{C}_{T^{m-k}})^2} \left(\sum_{G_1 \in \mathcal{C}_{T^{m-k}}} |\hat{g}(G-G_1)\hat{g}(-G_1)| \right) \left(\sum_{H_1 \in \mathcal{C}_{T^{m-k}}} |\hat{g}((H_1-H)\hat{g}(H_1)| \right).$$

L'inégalité de Cauchy-Schwarz nous donne pour $G \in \mathcal{C}_{T^{m-k}}$,

$$\sum_{G_1 \in \mathcal{C}_{T^{m-k}}} |\hat{g}(G-G_1)\hat{g}(-G_1)| \leq (\sum_{\Gamma \in \mathcal{C}_{T^{m-k}}} |\hat{g}(G+\Gamma)|^2)^{1/2} (\sum_{\Gamma \in \mathcal{C}_{T^{m-k}}} |\hat{g}(\Gamma)|^2)^{1/2},$$

d'où, avec la proposition 3.3,

$$\sum_{G_1 \in \mathcal{C}_{T^{m-k}}} |\hat{g}(G-G_1)\hat{g}(-G_1)| \leq 1.$$

La deuxième somme se majore de même et il s'en suit la majoration

$$|T_4(R,S)| \leq \beta q^{2(m-k)}.$$

On conclut avec (‡).

□

Proposition 6.5 *Pour $R \in \mathcal{C}_{T^r}$ et $S \in \mathcal{C}_{T^s}$ non nuls, on a*

$$|T_3(R,S)| \leq q^{\mu+\nu+\ell-k-2C(q,\alpha)(2r+\deg R)} q^{v_T(S)}, \tag{6.20}$$

$v_T(S)$ désignant la valuation T-adique de S.

Preuve. On a

$$|T_3(R,S)| \leq \sum_{(G,G_1,H_1)\in(\mathcal{C}_{T^{m-k}})^3} |\hat{g}(G-G_1)\hat{g}(H_1+G)\hat{g}(H_1)\hat{g}(-G_1)|$$

$$\times|\sum_{X\in\mathbf{M}_\mu} E(\frac{GXR}{T^m})||\sum_{Y\in\mathbf{M}_\nu} E(\frac{(G_1+H_1)SY}{T^{m-\ell}})|.$$

D'après le corollaire 2.3,

$$|T_3(R,S)| \leq q^{\mu+\nu} \sum_{\substack{G\in\mathcal{C}_{T^{m-k}} \\ v_\infty(\{\frac{GR}{T^m}\})>\mu}} \sum_{\substack{(G_1,H_1)\in(\mathcal{C}_{T^{m-k}})^2 \\ v_\infty(\{\frac{(G_1+H_1)S}{T^{m-\ell}}\})>\nu}} |\hat{g}(G-G_1)|$$

$$\times|\hat{g}(H_1+G)\hat{g}(H_1)\hat{g}(-G_1)|.$$

Si $G \in \mathcal{C}_{T^{m-k}}$, alors $v_\infty(\frac{GR}{T^m}) \geq k-r+2 > 0$. Comme $m-k > m-\ell = 4r > \mu - r$, on a en posant $H = G_1 + H_1$,

$$|T_3(R,S)| \leq q^{\mu+\nu} \sum_{\substack{G\in\mathcal{C}_{T^{2r-\deg R}} \\ \deg(GR)<m-\mu}} \sum_{\substack{H\in\mathcal{C}_{T^{m-k}} \\ v_\infty(\{\frac{HS}{T^{m-\ell}}\})>\nu}} a(G,H), \qquad (\dagger)$$

où

$$a(G,H) = \sum_{H_1\in\mathcal{C}_{T^m}} |\hat{g}(G-H+H_1)\hat{g}(H_1+G)\hat{g}(H_1-H)\hat{g}(H_1)|.$$

L'inégalité de Cauchy-Schwarz nous donne

$$a(G,H) \leq \left(\sum_{H_1\in\mathcal{C}_{T^{m-k}}} |\hat{g}(G-H+H_1)\hat{g}(H_1-H)|^2\right)^{1/2} \left(\sum_{H_1\in\mathcal{C}_{T^{m-k}}} |\hat{g}(G+H_1)\hat{g}(H_1)|^2\right)^{1/2},$$

soit

$$a(G,H) \le b(G) = \sum_{H_1 \in \mathcal{C}_{T^{m-k}}} |\hat{g}(G+H_1)\hat{g}(H_1)|^2.$$

On porte cette majoration dans (†). Avec (6.4), il vient

$$|T_3(R,S)| \le n(S) q^{\mu+\nu} \sum_{G \in \mathcal{C}_{T^{2r-\deg R}}} b(G),$$

où $n(S) = \mathrm{Card}(\{H \in \mathcal{C}_{T^{m-k}} \mid v_\infty(\{\frac{HS}{T^{m-\ell}}\}) \ge \nu\})$. D'après (6.3) et (6.4), on a $m - \ell < \nu$ et donc

$$n(S) = \mathrm{Card}(\{H \in \mathcal{C}_{T^{m-k}}; T^{m-\ell} | HS\}).$$

Avec (6.4) on a $v_T(S) \le \deg S < s < m - \ell$, d'où

$$n(S) = \mathrm{Card}(\{H \in \mathcal{C}_{T^{m-k}}; T^{m-\ell-v_T(S)} | H\}) = q^{\ell-k+v_T(S)},$$

ce qui nous donne

$$|T_3(R,S)| \le q^{\mu+\nu+\ell-k+v_T(S)} T_5(R), \qquad (\ddagger)$$

où $T_5(R) = \sum_{G \in \mathcal{C}_{T^{2r-\deg R}}} b(G)$ et, avec (6.15),

$$T_5(R) = \sum_{G \in \mathcal{C}_{T^{2r-\deg R}}} \sum_{H \in \mathcal{C}_{T^{m-k}}} |\widehat{f_{\ell-k,m-k}}(G+H)\widehat{f_{\ell-k,m-k}}(H)|^2.$$

On a $2r - \deg R + \ell - k = m - k - \deg R \le m - k$. La proposition 3.5 nous donne alors

$$T_5(R) \le q^{-2C(m-\ell-2r+\deg R)} = q^{-2C(2r+\deg R)},$$

où l'on a posé $C = C(q,\alpha)$ et on conclut avec (‡).

□

Proposition 6.6 *Si $\mu \ge 32$, alors*

$$|T_{\mu,\nu}| \le a(q) \mu^{1/4} q^{\mu+\nu-3C(q,\alpha)\mu/64}, \qquad (6.21)$$

où

$$a(q) = \frac{1}{2}\left(\frac{2}{q} + 4\frac{(q-1)^2}{q^{1/3}-1} + q\right)^{1/4}. \qquad (6.22)$$

Preuve. On choisit

$$r = [\frac{\mu}{16}] \text{ et } k = \ell - [\gamma r], \tag{6.23}$$

avec

$$\gamma = 3C(q, \alpha). \tag{6.24}$$

La condition (6.3) est réalisée et on a, d'après (6.7) et (6.16),

$$|T_{\mu,\nu}|^4 \leq 4q^{4(\mu+\nu)-2r} + 2q^{3(\mu+\nu)}(\mathfrak{S}_3 + \mathfrak{S}_4),$$

où

$$\mathfrak{S}_3 = \frac{1}{q^{r+s}} \sum_{\substack{(R,S)\in\mathcal{C}_{T^r}\times\mathcal{C}_{T^s} \\ RS\neq 0}} T_3(R,S) \text{ et } \mathfrak{S}_4 = \frac{1}{q^{r+s}} \sum_{\substack{(R,S)\in\mathcal{C}_{T^r}\times\mathcal{C}_{T^s} \\ RS\neq 0}} T_4(R,S).$$

Avec (6.19), puis (6.4) et (6.23), on voit que

$$\mathfrak{S}_4 \leq q^{\mu+3(m-k)}q^{\nu}\max(q^{-\nu}, q^{-m}) \leq q^{\mu+\nu+3(4r+[\gamma r])}\max(q^{-\nu}, q^{-\mu-2r}).$$

D'après (3.11), (6.23) et (6.24), on a $2\gamma r + 12r \leq 14r \leq \mu \leq \nu$, d'où $12r + 3\gamma r - \nu \leq -\gamma r$. On a aussi $10r + 3\gamma r - \mu \leq -\gamma r$, d'où

$$\mathfrak{S}_4 \leq q^{\mu+\nu-\gamma r}. \tag{6.25}$$

Si l'on pose $C = C(q, \alpha)$, la proposition précédente nous donne

$$\mathfrak{S}_3 \leq q^{\mu+\nu+\ell-k-4Cr}AB,$$

avec

$$A = q^{-r} \sum_{\substack{R\in\mathcal{C}_{T^r} \\ R\neq 0}} q^{-2C\deg R} = q - r\sum_{i=0}^{r-1}(q-1)q^{(1-2C)i} \leq \frac{q-1}{q^{1-2C}-1}q^{-2Cr}$$

et

$$B = q^{-s} \sum_{\substack{S \in \mathcal{C}_{T^s} \\ S \neq 0}} q^{v_T(S)} = q^{-s} \sum_{i=0}^{s-1} q^i (q^{s-i} - q^{s-i-1}) = \frac{s(q-1)}{q} = \frac{2r(q-1)}{q}.$$

La remarque (3.11) montre que $A \leq \frac{q-1}{q^{1/3}-1} q^{-2Cr}$, d'où l'on déduit la majoration

$$\mathfrak{S}_3 \leq \frac{2r(q-1)^2}{q(q^{1/3}-1)} q^{\mu+\nu+(\gamma-6C)r}. \tag{6.26}$$

Avec (6.25), (6.26) et (6.24) on obtient

$$|T_{\mu,\nu}|^4 \leq q^{4(\mu+\nu)}(4q^{-2r} + \frac{4r(q-1)^2}{q(q^{1/3}-1)} q^{-3Cr} + 2q^{-3Cr})$$

$$\leq r q^{4(\mu+\nu)-3Cr}(4\frac{q^{3Cr-2r}}{r} + 4\frac{(q-1)^2}{q(q^{1/3}-1)} + \frac{2}{r}).$$

En remplaçant r par sa valeur fixée par (6.23) dans le premier facteur, en le minorant par 2 dans le deuxième facteur et en utilisant encore une fois la remarque (3.11) on obtient la majoration

$$|T_{\mu,\nu}|^4 \leq \frac{\mu}{16} q^{4(\mu+\nu)-3C\mu/16}(\frac{2}{q} + 4\frac{(q-1)^2}{q^{1/3}-1} + q)$$

qui nous permet de conclure.

□

7 Démonstration du théorème 2

Proposition 7.1 *Pour tout nombre entier $N \geq 128$, on a*

$$\left| \sum_{X \in \mathbf{M}_{\mathbb{N}}} \Lambda(X) e(\alpha w(X)) \right| \leq \frac{3a(q)N^3}{4} q^{(1-3C(q,\alpha)/256)N}. \tag{7.1}$$

Preuve. Soit μ un nombre entier, $\mu \in [1, N]$, $\nu = N - \mu$, a et b des applications de $\mathbf{A}$ dans l'ensemble des nombres complexes de module au plus 1. Pour

démontrer la proposition 7.3, nous allons estimer les sommes de type I et II et appliquer la proposition 4.3.

(I) Si $\mu \leq N/4$ on a $\mu \leq \nu/2$ et la proposition 5.3 nous donne

$$\sum_{H \in \mathbf{M}_\mu} | \sum_{X \in \mathbf{M}_{N-\mu}} e(\alpha w(HX))| \leq \mu q^{(1-C(q,\alpha)/3)(\mu+\nu)} \leq b_1,$$

avec $b_1 = \frac{N}{4} q^{(1-C(q,\alpha)/3)N}$.

(II) Si $N/4 \leq \mu \leq 3N/4$, alors

- si $\mu \leq N - \mu$, la condition sur N nous permet d'appliquer la proposition 6.6 et on obtient

$$| \sum_{H \in \mathbf{M}_\mu} \sum_{Y \in \mathbf{M}_{N-\mu}} a_H b_Y e(\alpha w(HY))| \leq a(q) \mu^{1/4} q^{\mu+\nu-3C(q,\alpha)\mu/64} \leq b_2$$

avec $b_2 = a(q)(\frac{N}{2})^{1/4} q^{N(1-3C(q,\alpha)/256)}$.

- si $\mu > N - \mu$, on applique encore la proposition 6.6. mais en inversant les rôles joués par μ et ν.

La proposition 4.3 où l'on prend $g(X) = e(\alpha w(X))$ et

$$B = a(q) N q^{N(1-3C(q,\alpha)/256)} \tag{7.2}$$

donne alors

$$\left| \sum_{X \in \mathbf{M}_\mathbb{N}} \Lambda(X) e(\alpha w(X)) \right| \leq \frac{3a(q)N^3}{4} q^{N(1-3C(q,\alpha)/256)}.$$

□

Théorème 7.2 *Pour $N \geq 128$ on a*

$$\sum_{P \in \mathbf{I_N}} e(\alpha w(P)) \leq A(q) N^2 q^{N(1-3C(q,\alpha)/256)}, \tag{7.3}$$

avec

$$A(q) = \frac{3a(q)}{4} + 1. \tag{7.4}$$

Preuve. On a

$$|N\sum_{P\in\mathbf{I}_N} e(\alpha w(P))-\sum_{X\in\mathbf{M}_N}\Lambda(X)e(\alpha w(X))| = |\sum_{\substack{P\in\mathbf{I}\\ \deg P|N\\ \deg P\neq N}} \deg P e(\alpha w(P^{N/\deg P})|$$

$$\leq \sum_{k|N,k<N} k\Pi_k \leq q^{N/2}$$

d'après [17, Corollary 3.21]. Il résulte de la proposition 7.1 et de la remarque (3.11) que

$$\sum_{P\in\mathbf{I}_N} e(\alpha w(P)) \leq \frac{3}{4}a(q)N^2q^{N(1-3C(q,\alpha)/256)} + \frac{q^{N/2}}{N}$$

$$\leq (\frac{3}{4}a(q) + \frac{q^{-127N/256}}{N^3})N^2q^{N(1-3C(q,\alpha)/256)} \leq (\frac{3}{4}a(q)+1)N^2q^{N(1-3C(q,\alpha)/256)}.$$

□

Corollaire 7.3 *(I) Si $q > 2$, pour tout nombre entier strictement positif m et pour tout nombre entier rationnel a, on a*

$$|\mathrm{Card}(\{P\in\mathbf{I}_N; w(P)\equiv a \pmod m\}) - \frac{\Pi_N}{m}| \leq A(q)N^2q^{N(1-3/256m^2q\log q)}.$$

Si $q = 2$, pour tout nombre entier strictement positif impair m et pour tout nombre entier rationnel a on a

$$|\mathrm{Card}(\{P\in\mathbf{I}_N; w(P)\equiv a \pmod m\}) - \frac{\Pi_N}{m}| \leq N^2q^{N(1-3/512m^2\log 2)}.$$

Preuve. Notons $\pi(m,a,N)$ le nombre de polynômes irréductibles unitaires P de degré N tels que $w(P)\equiv a(\mathrm{mod}\ m)$. Alors,

$$\pi(m,a,N) = \sum_{P\in\mathbf{I}_N}\frac{1}{m}\sum_{k=0}^{m-1} e(\frac{k(w(P)-a)}{m}),$$

d'où, pour $N \geq 128$,

$$m\pi(m,a,N) = \sum_{k=0}^{m-1} e(\frac{-ka}{m})\sum_{P\in\mathbf{I}_N} e(\frac{kw(P)}{m}) = \Pi_N + \sum_{k=1}^{m-1} e(\frac{-ka}{m})\sum_{P\in\mathbf{I}_N} e(\frac{kw(P)}{m}).$$

On a

$$\sum_{P\in\mathbf{I}_N} e(\frac{kw(P)}{m}) \leq A(q)N^2 q^{N(1-3C(q,k/m)/256)}.$$

Si $q>2$, pour tout $k\in\{1,\dots,m-1\}$, on a $C(q,k/m)=4\|k/m\|^2/q\log q \geq 4/m^2 q\log q$, d'où

$$|m\pi(m,a,N)-\Pi_N| \leq (m-1)A(q)N^2 q^{N(1-3/256/m^2 q\log q)}.$$

Si $q=2$ et si m est impair, la même méthode conduit à

$$|m\pi(m,a,N)-\Pi_N| \leq (m-1)A(2)N^2 2^{N(1-3/512m^2\log 2)}.$$

□

8 Démonstration du théorème 1

Rappelons que

$$\mu(q)=\frac{q-1}{q},\ \sigma(q)=\frac{(q-1)^{1/2}}{q} \tag{8.1}$$

Pour tout polynôme $A=a_0+a_1T+\cdots+a_NT^N$ de degré N appartenant à $\mathbf{A}$, posons $x_j(A)=a_j$ pour $j\in\{0,\dots N\}$.

Si $P=a_0+a_1T+\cdots+a_{N-1}T^{N-1}+T^N$ est un polynôme irréductible de $\mathbf{A}$, on a $w(P)=w'(P)+2$, où l'on a posé pour tout polynôme $X\in\mathbf{A}$ de degré N

$$w'(X)=\sum_{j=1}^{N-1} w(x_j(X)). \tag{8.2}$$

Dans ce qui suit nous démontrons la propositon suivante dont le théorème 1 est une conséquence.

Proposition 8.1 *Soit η un nombre réel tel que $0<\eta<\frac{1}{12}$. On a uniformément pour $t\in[-N^\eta,N^\eta]$*

$$\varphi_{\mathbf{I}}(t)=\exp(-\frac{t^2}{2})(1+O(\frac{q^{3/2}t^3}{\sqrt{N}}))+O(q^{3/2}N^{-(1/12-\eta)N^{1/6}})). \tag{8.3}$$

où l'on a posé pour tout nombre réel t,

$$\varphi_{\mathbf{I}}(t) = \frac{1}{\Pi_N} \sum_{P \in \mathbf{I}_N} e(\frac{t(w'(P) - \mu(q)(N-1))}{2\pi\sigma(q)\sqrt{N-1}}), \tag{8.4}$$

les constantes impliquées par le symbole O étant absolues.

Nous interprétons $\varphi_{\mathbf{I}}$ comme la fonction caractéristique de la variable aléatoire

$$Y_{\mathbf{I}} : P \to \frac{w'(P) - \mu(q)(N-1)}{\sigma(q)\sqrt{N-1}}$$

définie sur l'espace $\mathbf{I}_N$ muni de la mesure uniforme. Nous définissons pour tout nombre réel t,

$$\varphi_{\mathbf{M}}(t) = q^{-N} \sum_{H \in \mathbf{M}_N} e(\frac{t(w'(H) - \mu(q)(N-1))}{2\pi\sigma(q)\sqrt{N-1}}) \tag{8.5}$$

et nous interprétons $\varphi_{\mathbf{M}}$ comme a fonction caractéristique de la variable aléatoire

$$Y_{\mathbf{M}} : H \to \frac{w'(H) - \mu(q)(N-1)}{\sigma(q)\sqrt{N-1}}$$

définie sur l'espace $\mathbf{M}_N$. Notre stratégie est la suivante. Nous commençons par démontrer au lemme 8.2 [1] que $\varphi_{\mathbf{M}}$ est bien approchée par la fonction caractéristique de la loi centrée réduite puis nous appliquons une variante de la méthode des moments pour montrer que pour $t \in [-N^\eta, N^\eta]$ $\varphi_{\mathbf{I}}(t)$ est bien approché par $\varphi_{\mathbf{M}}(t)$. La méthode des moments classique consiste à montrer la convergence en loi de $Y_{\mathbf{I}}$ vers la loi normale centrée réduite en montrant que pour tout $d \in \mathbb{N}$ fixé on a

$$\mathbf{E}(Y_{\mathbf{I}}^d) = \mathbf{E}(Y_{\mathbf{M}}^d) + o(1) \tag{8.6}$$

(voir par exemple [2, Theorem 30.2]). Cette approche utilisée par Bassily et Katai dans [3] ne s'appliquant pas directement à notre situation, nous utiliserons la variante développée par Drmota, Mauduit et Rivat dans [10] (voir aussi [20]). Celle-ci consiste à établir au lemme 8.4 une version uniforme de (8.6) qui permet grâce à la formule de Taylor, d'obtenir au corollaire 8.6 la majoration recherchée. Dans ce qui suit, les constantes contenues dans les symboles O sont absolues et on suppose que $N \geq 128$.

1. Ce lemme est formulé dans le plan complexe afin de nous permettre de majorer la quatité Γ_D définie par (8.17) dans la démonstration du lemme 8.5.

Lemme 8.2 *On a uniformément pour tout nombre complexe t tel que $|t| \leq N^{1/2}$*

$$\varphi_{\mathbf{M}}(t) = \exp(-\frac{t^2}{2})(1 + O(q^{3/2}N^{-1/2}|t|^3). \tag{8.7}$$

Preuve : On a

$$\varphi_{\mathbf{M}}(t) = \exp(-\frac{\mu(q)it\sqrt{N-1}}{\sigma(q)})\Theta(\frac{t}{\sigma(q)\sqrt{N-1}}), \tag{$\dagger$}$$

où pour tout nombre complexe z,

$$\Theta(z) = q^{-N} \sum_{H \in \mathbf{M}_N} e^{izw'(H)}$$

$$= q^{-N} \sum_{(a_0,\ldots,a_{N-1}) \in F} e^{iz(w(a_1)+\cdots+w(a_{N-1}))} = (\frac{1 + (q-1)e^{iz}}{q})^{N-1}.$$

Un développement de Taylor à l'ordre 3 au voisinage de 0 nous donne

$$\log(\frac{1 + (q-1)e^{iz}}{q}) = \mu(q)iz - \frac{\sigma(q)^2 z^2}{2} + O(|z|^3),$$

d'où l'on déduit

$$\Theta(z) = \exp((N-1)(\mu(q)iz - \frac{\sigma(q)^2 z^2}{2}))(1 + O(N|z|^3)).$$

On porte ce résultat dans ($\dagger$) en remplaçant z par $\frac{t}{\sigma(q)\sqrt{N-1}}$.

□

Pour approcher $\varphi_{\mathbf{I}}(t)$ par $\varphi_{\mathbf{M}}(t)$ nous aurons besoin du lemme crucial suivant.

Lemme 8.3 *Soit r un nombre entier tel que $1 \leq r < N$. Si $j_1, j_2, \ldots, j_r$ sont des nombres entiers vérifiant $0 < j_1 < j_2 < \cdots < j_r < N$ et si $(a_1, \ldots, a_r) \in \mathbb{F}^r$, on a*

$$|\frac{\pi(N, \vec{j}, \vec{a})}{\Pi_N} - \frac{1}{q^r}| \leq 4\frac{q^{1/4}N}{q^{N/(r+3)}}, \tag{8.8}$$

où $\pi(N, \vec{j}, \vec{a}) = \mathrm{Card}(\{P \in \mathbf{I}_N, x_{j_1}(P) = a_1, \ldots, x_{j_r}(P) = a_r\})$.

Preuve : Ce lemme résulte de [26, Theorem 1], où Pollack démontre que [2]

$$|\pi(N,\vec{j},\vec{a}) - \Pi_N q^{-r}| \leq q^{N-[N/2]/2} + q^{N-1-[N/(r+1)]}$$

et dont on déduit

$$|\frac{\pi(N,\vec{j},\vec{a})}{\Pi_N} - q^{-r}| \leq 2q^{1/4}\frac{q^N}{\Pi_N}q^{-N/(r+3)}.$$

De l'égalité bien connue $q^N = \sum_{d|N} d\Pi_d$ (voir par exemple [17, Corollary 3.21]), on déduit la minoration $N\Pi_N \geq q^N - \frac{q}{q-1}q^{N/2}$ qui nous donne

$$|\frac{\pi(N,\vec{j},\vec{a})}{\Pi_N} - q^{-r}| \leq 4\frac{q^{1/4}N}{q^{N/(r+3)}}.$$

□

Posons, pour tout nombre entier strictement positif d,

$$\Phi_{d,\mathbf{I}}(N) = \frac{1}{\Pi_N}\sum_{P\in\mathbf{I}_N}(w'(P) - \mu(q)(N-1))^d \tag{8.9}$$

et

$$\Phi_{d,\mathbf{M}}(N) = q^{-N}\sum_{H\in\mathbf{M}_N}(w'(H) - \mu(q)(N-1))^d. \tag{8.10}$$

Nous approchons $\Phi_{d,\mathbf{I}}(N)$ par $\Phi_{d,\mathbf{M}}(N)$.

Lemme 8.4 *On a pour* $1 \leq d < N$

$$|\Phi_{d,\mathbf{I}}(N - \Phi_{d,\mathbf{M}}(N)| \leq 4q^{1/4}N(q(N-1))^d q^{-N/(d+3)}. \tag{8.11}$$

Preuve : On a

$$\Phi_{d,\mathbf{M}}(N) = q^{-N}\sum_{H\in\mathbf{M}_N}(\sum_{j=1}^{N-1}(w(x_j(H)) - \mu(q)))^d,$$

2. Ce résultat n'est intéressant que lorsque $r(r+1) < N$. Mentionnons que Ha a étendu dans [14] ce résultat au cas $r < \delta N$ pour $\delta \leq \delta_0(q)$ en adaptant la méthode développée par Bourgain dans [4] et [5].

d'où

$$\Phi_{d,\mathbf{M}}(N) = q^{-N} \sum_{H\in\mathbf{M}_N} \sum_{r=1}^{d} \sum_{0<j_1<\cdots<j_r<N}$$

$$\sum_{\substack{d_1,\dots,d_r>0\\ d_1+\cdots+d_r=d}} \frac{d!}{d_1!\dots d_r!}(w(x_{j_1}(H))-\mu(q))^{d_1}\dots(w(x_{j_r}(H))-\mu(q))^{d_r},$$

d'où, après inversion de l'ordre des sommations

$$\Phi_{d,\mathbf{M}}(N) = \sum_{r=1}^{d} \sum_{0<j_1<\cdots<j_r<N} \sum_{\substack{d_1,\dots,d_r>0\\ d_1+\cdots+d_r=d}} \frac{d!}{d_1!\dots d_r!}\Psi_{\mathbf{M}}(\vec{j},\vec{d}), \tag{8.12}$$

où pour $\vec{j} = (j_1,\dots,j_r)$,

$$\Psi_{\mathbf{M}}(\vec{j},\vec{d}) = q^{-N} \sum_{H\in\mathbf{M}_N} (w(x_{j_1}(H))-\mu(q))^{d_1}\dots(w(x_{j_r}(H))-\mu(q))^{d_r}. \tag{8.13}$$

De la même façon on obtient que

$$\Phi_{d,\mathbf{I}}(N) = \sum_{r=1}^{d} \sum_{0<j_1<\cdots<j_r<N} \sum_{\substack{d_1,\dots,d_r>0\\ d_1+\cdots+d_r=d}} \frac{d!}{d_1!\dots d_r!}\Psi_{\mathbf{I}}(\vec{j},\vec{d}), \tag{8.14}$$

où

$$\Psi_{\mathbf{I}}(\vec{j},\vec{d}) = \frac{1}{\Pi_N} \sum_{P\in\mathbf{I}_N} (w(x_{j_1}(P))-\mu(q))^{d_1}\dots(w(x_{j_r}(P))-\mu(q))^{d_r}. \tag{8.15}$$

Pour $0 < j_1 < \cdots < j_r < N$ et pour $0 < d_1,\dots,0 < d_r$, on a

$$\Psi_{\mathbf{M}}(\vec{j},\vec{d}) = q^{-r} \sum_{(a_{j_1},\dots,a_{j_r})\in\mathbb{F}^r} (w(a_{j_1})-\mu(q))^{d_1}\dots(w(a_{j_r})-\mu(q))^{d_r}$$

et

$$\Psi_{\mathbf{I}}(\vec{j},\vec{d}) = \frac{1}{\Pi_N} \sum_{(a_{j_1},\dots,a_{j_r})\in\mathbb{F}^r} (w(a_{j_1})-\mu(q))^{d_1}\dots(w(a_{j_r})-\mu(q))^{d_r}$$

$$\times \mathrm{Card}(\{P\in\mathbf{I}_N, x_{j_1}(P)=a_{j_1},\dots,x_{j_r}(P)=a_{j_r}\}).$$

Le lemme précédent nous donne

$$|\Psi_{\mathbf{I}}(\vec{j},\vec{d}) - \Psi_{\mathbf{M}}(\vec{j},\vec{d})| \leq \frac{4Nq^{r+1/4}}{q^{N/(r+3)}},$$

d'où

$$|\Phi_{d,\mathbf{I}}(N) - \Phi_{d,\mathbf{M}}(N)| \leq 4Nq^{1/4} \sum_{r=1}^{d} \sum_{1<j_1<\dots<j_r<N} \sum_{\substack{d_1,\dots,d_r>0 \\ d_1+\dots+d_r=d}} \frac{d!}{d_1!\dots d_r!} \frac{q^r}{q^{N/(r+3)}}$$

$$\leq 4q^{1/4}N(q(N-1))^d q^{-N/(d+3)}.$$

□

Lemme 8.5 *Soit η un nombre réel tel que $0<\eta<1/12$. On a uniformément pour $t\in[-N^\eta,N^\eta]$:*

$$|\varphi_{\mathbf{I}}(t) - \varphi_{\mathbf{M}}(t)| = O(q^{3/2}N^{-(1/12-\eta)N^{1/6}}). \tag{8.16}$$

Preuve. Soit $D = D(N) = 2\lceil N^{1/6}\rceil$. Il résulte de la formule de Taylor que pour tout nombre réel y on a

$$|\exp(iy) - \sum_{d=0}^{D-1} \frac{(iy)^d}{d!}| \leq \frac{|y|^D}{D!} = \frac{y^D}{D!}.$$

Par suite, pour tout nombre réel x on a

$$|\frac{1}{\Pi_N}\sum_{P\in\mathbf{I}_N} e(x(w'(P)-\mu(q)(N-1)) - \frac{1}{\Pi_N}\sum_{P\in\mathbf{I}_N}\sum_{d=0}^{D-1} \frac{(2i\pi x(w'(P)-\mu(q)(N-1)))^d}{d!}|$$

$$\leq \frac{1}{\Pi_N} \sum_{P \in \mathbf{I}_N} \frac{(2\pi x(w'(P) - \mu(q)(N-1))))^D}{D!}.$$

On prend $x = t/2\pi\sigma(q)\sqrt{N-1}$ et on inverse les sommations. Avec (8.4) et (8.9) on obtient

$$|\varphi_{\mathbf{I}}(t) - \sum_{d=0}^{D-1} \frac{t^d \Phi_{d,\mathbf{I}}(N)}{(\sigma(q)\sqrt{N-1})^d d!}| \leq \frac{|t|^D \Phi_{D,\mathbf{I}}(N)}{(\sigma(q)\sqrt{N-1})^D D!}.$$

De la même façon on obtient

$$|\varphi_{\mathbf{M}}(t) - \sum_{d=0}^{D-1} \frac{t^d \Phi_{d,\mathbf{M}}(N)}{(\sigma(q)\sqrt{N-1})^d d!}| \leq \frac{|t|^D \Phi_{D,\mathbf{M}}(N)}{(\sigma(q)\sqrt{N-1})^D D!},$$

d'où

$$|\varphi_{\mathbf{I}}(t) - \varphi_{\mathbf{M}}(t)| \leq \sum_{d=1}^{D-1} \frac{|t|^d |\Phi_{d,\mathbf{I}}(N) - \Phi_{d,\mathbf{M}}(N)|}{(\sigma(q)\sqrt{N-1})^d d!} + \frac{|t|^D \Phi_{D,\mathbf{I}}(N)}{(\sigma(q)\sqrt{N-1})^D D!} + \frac{|t|^D \Phi_{D,\mathbf{M}}(N)}{(\sigma(q)\sqrt{N-1})^D D!}$$

$$= \sum_{d=1}^{D} \frac{|t|^d |\Phi_{d,\mathbf{I}}(N) - \Phi_{d,\mathbf{M}}(N)|}{(\sigma(q)\sqrt{N-1})^d d!} + 2\frac{|t|^D \Phi_{D,\mathbf{M}}(N)}{(\sigma(q)\sqrt{N-1})^D D!}.$$

Posons

$$\Gamma(D) = \frac{\Phi_{D,\mathbf{M}}(N)}{(\sigma(q)\sqrt{N-1})^D D!}. \tag{8.17}$$

Le lemme précédent nous donne alors

$$|\varphi_{\mathbf{I}}(t) - \varphi_{\mathbf{M}}(t)| \leq 2|t|^\eta \Gamma(D) + 4q^{1/4} N \sum_{d=1}^{D} \frac{(|t| q N^{1/2})^d}{\sigma(q)^d q^{N/(d+3)} d!},$$

d'où,

$$|\varphi_{\mathbf{I}}(t) - \varphi_{\mathbf{M}}(t)| \leq 2N^{\eta D}\Gamma(D) + 4q^{1/4} N^{1+\eta D} q^{-N/(D+3)} (\mathfrak{S}_1 + \mathfrak{S}_2) \tag{8.18}$$

où

$$\mathfrak{S}_1 = \sum_{d=1}^{D/2} \frac{(qN^{1/2})^d}{\sigma(q)^d d!} \quad \mathfrak{S}_2 = \sum_{d=1+[D/2]}^{D} \frac{(qN^{1/2})^d}{\sigma(q)^d d!}.$$

On a donc

$$\mathfrak{S}_1 \leq \sum_{d=1}^{D/2} (\frac{qN^{1/2}}{\sigma(q)})^d \leq 2(\frac{qN^{1/2}}{\sigma(q)})^{D/2}$$

et

$$\mathfrak{S}_2 \leq \frac{1}{(1+[D/2])!} \sum_{d=1+[D/2]}^{D} (\frac{qN^{1/2}}{\sigma(q)})^D \leq 2\frac{(qN^{1/2})^D}{\sigma(q)^D(1+[D/2])(D/2)!}.$$

La formule de Stirling nous donne

$$\mathfrak{S}_2 \leq \sqrt{\frac{2}{\pi}} \frac{(qN^{1/2})^D \exp(D/2)}{\sigma(q)^D(1+[D/2])(D/2)^{(1+D)/2}} \leq \frac{4}{\sqrt{\pi}D^{3/2}} \left(\frac{2eq^2N}{\sigma(q)^2D}\right)^{D/2}$$

et puisque $D = 2\lceil N^{1/6} \rceil$, on obtient

$$\mathfrak{S}_1 + \mathfrak{S}_2 = O\left(D^{-3/2}\left(\frac{2eq^4N}{D}\right)^{D/2}\right). \tag{8.19}$$

Pour majorer $\Gamma(D))$ rappelons que d'après (8.5) et (8.10), pour tout nombre complexe u,

$$\varphi_{\mathbf{M}}(-iu) = \sum_{k=0}^{\infty} \frac{u^k \Phi_{k,\mathbf{I}}(N)}{(\sigma(q)\sqrt{N-1})^k k!}.$$

La formule de Cauchy nous donne

$$\Gamma(D) = \frac{1}{2\pi i} \int_{|u|=\sqrt{D}} \frac{\varphi_{\mathbf{M}}(-iu)}{t^{D+1}} \mathrm{d}u$$

et le Lemme 8.2 nous donne alors

$$|\Gamma(D)| \leq \frac{\exp(D/2)}{D^{D/2}}(1 + O\left((qD)^{3/2}N^{-1/2}\right))$$
$$\leq \frac{\exp(D/2)}{D^{D/2}}(1 + q^{3/2}O(N^{-1/4})) = O(q^{3/2}\frac{\exp(D/2)}{D^{D/2}}).$$

Observons maintenant que, puisque $D = 2\lceil N^{1/6} \rceil$, on a pour N assez grand $q^{1/4-N/(D+3)+2D} \leq 2^{1/4-N/(D+3)+2D}$ et donc

$$q^{1/4} N q^{-N/(D+3)} \left(\frac{2eq^4 N}{D} \right)^{D/2} = o(1),$$

d'où avec (8.18) et (8.19)

$$|\varphi_{\mathbf{I}}(t) - \varphi_{\mathbf{M}}(t)| = O(q^{3/2} N^{\eta D} \frac{\exp(D/2)}{D^{D/2}}).$$

Pour tout nombre réel $K > 0$, la fonction ρ qui à tout nombre réel $x > 0$ associe $\rho(x) = (\frac{K}{x})^x$ est décroissante sur l'intervalle $[\frac{K}{e}, +\infty[$. Comme pour tout $N \geq 1$, on a $D/2 \geq N^{1/6} \geq \frac{N^{2\eta}}{2}$, il en résulte (en prenant $K = \frac{N^\eta e}{2}$ dans la remarque précédente) que

$$N^{\eta D} \frac{\exp(D/2)}{D^{D/2}} = (\frac{N^{2\eta} e}{2D/2})^{D/2} \leq (\frac{N^{2\eta} e}{2N^{1/6}})^{N^{1/6}} = (N^{2\eta - 1/6} \frac{e}{2})^{N^{1/6}},$$

d'où

$$N^{\eta D} \frac{\exp(D/2)}{D^{D/2}} = O(N^{(\eta - 1/12) N^{1/6}}).$$

□

La proposition 8.1 découle alors des lemmes 8.2 et 8.5.

Nous pouvons maintenant démontrer le Théorème 1. Il nous faut distinguer le cas $q = 2$ du cas $q \neq 2$. Nous commencerons par ce dernier cas qui est plus simple. Posons pour tout nombre entier $k \geq 2$

$$b(N, k) = \mathrm{Card}(\{P \in \mathbf{I}_N,\ w(P) = k\}). \tag{8.20}$$

On a avec (8.2)

$$b(N, k) = \sum_{P \in \mathbf{I}_N} \int_{-1/2}^{1/2} e(\alpha(w'(P) - k + 2)) d\alpha = \int_{-1/2}^{1/2} g(\alpha) d\alpha$$

où

$$g(\alpha) = \sum_{P \in \mathbf{I}_N} e(\alpha(w'(P) - k + 2)). \tag{8.21}$$

On pose $v = (N-1)^{\eta - 1/2} / 2\pi\sigma(q)$ et on écrit

(8.22) $$b(N,k) = \beta(N,k) + \beta'(N,k),$$

où

(8.23) $$\beta(N,k) = \int_{|\alpha|\leq v} g(\alpha)d\alpha$$

et

(8.24) $$\beta'(N,k) = \int_{v<|\alpha|\leq 1/2} g(\alpha)d\alpha.$$

Le théorème 7.2 joint aux relations (3.10) et (2.10) nous donne

$$|g(\alpha)| = |\sum_{P\in\mathbf{I}_N} e(\alpha(w(P)-k))| = |\sum_{P\in\mathbf{I}_N} e(\alpha w(P))| \leq$$

$$A(q)N^2 q^{N(1-B(q)\|\alpha\|^2)},$$

où $B(q) = \frac{3}{64q\log q}$. Si l'on pose

(8.25) $$B_1(q) = \frac{B(q)}{4\pi^2\sigma(q)^2} = \frac{3q}{256\pi^2(q-1)\log q},$$

il vient avec (8.24), $|\beta'(N,k)| \leq A(q)N^2q^Nq^{-B_1(q)N(N-1)^{2\eta-1}} \leq A(q)N^2q^Nq^{-B_1(q)(N-1)^{2\eta}}$, soit

(8.26). $$\beta'(N,k) = O(A(q)\Pi_N N^3 q^{-B_1(q)N^{-2\eta}}).$$

Pour traiter $\beta(N,k)$ observons que

$$g(\alpha) = \sum_{P\in\mathbf{I}_N} e(\alpha(w'(P)-\mu(q)(N-1)))e(\alpha(\mu(N-1)-k+2)),$$

d'où, avec (8.4),

$$g(\alpha) = \Pi_N\varphi_{\mathbf{I}}(2\pi\sigma(q)\alpha\sqrt{N-1})e(\alpha(\mu(q)(N-1)-k+2))$$

et le changement de variable $t = 2\pi\sigma(q)\alpha\sqrt{N-1}$ nous donne

$$\beta(N,k)=\frac{\Pi_N}{2\pi\sigma(q)\sqrt{N-1}}\int_{-(N-1)^\eta}^{(N-1)^\eta}\varphi_{\mathbf{I}}(t)e(\frac{t(\mu(q)(N-1)-k+2)}{2\pi\sigma(q)\sqrt{N-1}})dt.$$

Avec (8.3) il vient

(8.27)
$$\frac{2\pi\sigma(q)\sqrt{N-1}\beta(N,k)}{\Pi_N}=J_1(N)+O(\frac{q^{3/2}}{\sqrt{N}}J_2(N))+O(q^{3/2}N^{\eta-(1/12-\eta)N^{1/6}}),$$

où

$$J_1(N)=\int_{-(N-1)^\eta}^{(N-1)^\eta}\exp(-\frac{t^2}{2})\exp(i\frac{t(\mu(q)(N-1)-k+2)}{\sigma(q)\sqrt{N-1}})dt$$

et

$$J_2(N)=\int_{-(N-1)^\eta}^{(N-1)^\eta}\exp(-\frac{t^2}{2})|t|^3dt\leq 4\int_0^\infty u\exp(-u)du=4.$$

On a

$$|J_1(N)-\int_\infty^{+\infty}\exp(-\frac{t^2}{2})\exp(i\frac{t(\mu(q)(N-1)-k+2)}{\sigma(q)\sqrt{N-1}})dt|\leq 2\int_{(N-1)^\eta}^{+\infty}\exp(-\frac{t^2}{2})dt,$$

d'où

$$|J_1(N)-\sqrt{2\pi}\exp(-\frac{1}{2}(\frac{\mu(q)(N-1)-k+2}{\sigma(q)\sqrt{N-1}})^2)|\leq\frac{2}{(N-1)^\eta}\exp(-\frac{(N-1)^{2\eta}}{2})$$

et avec (8.27) on a

$$\beta(N,k)=\frac{\Pi_N}{\sqrt{2\pi}\sigma(q)\sqrt{N-1}}\exp(-\frac{1}{2}(\frac{\mu(q)(N-1)-k+2}{\sigma(q)\sqrt{N-1}})^2)+O(\Pi_N\frac{q^2}{N}).)$$

Avec (8.22), (8.26), (7.4) et (6.22) on a

$$b(N,k)=\frac{\Pi_N}{\sqrt{2\pi}\sigma(q)\sqrt{N-1}}\exp(-\frac{1}{2}(\frac{\mu(q)(N-1)-k+2}{\sigma(q)\sqrt{N-1}})^2)+O(\Pi_N\frac{q^2}{N})),$$

ce qui démontre la première partie du théorème 1.

Lorsque $q = 2$, on observe que tout polynôme irréductible est de poids impair. On suppose donc que k est impair et on écrit

$$b(N,k) = \beta_-(N,k) + \beta_0(N,k) + \beta_+(N,k) + \beta_-^{'}(N,k) + \beta_+^{'}(N,k)$$

avec

$$\beta_0(N,k) = \int_{|\alpha|\leq v} g(\alpha)d\alpha,$$

$$\beta_-(N,k) = \int_{-1/2}^{-1/2+v} g(\alpha)d\alpha,\ \beta_+(N,k) = \int_{1/2-v}^{1/2} g(\alpha)d\alpha$$

et

$$\beta_-^{'}(N,k) = \int_{-1/2+v}^{-v} g(\alpha)d\alpha,\ \beta_+^{'}(N,k) = \int_{v}^{1/2-v} g(\alpha)d\alpha.$$

Le théorème 7.2 nous donne ici $|g(\alpha)| \leq A(2)N^2 2^{N(1-3\|\alpha\|_{1/2}^2/256\log(2))}$, d'où

$$|\beta_-^{'}(N,k)|+|\beta_+^{'}(N,k)| \leq A(2)N^2 2^{N(1-3\|\alpha\|_{1/2}^2/256\log(2))} = O(\Pi_N N^3 q^{-3N^{2\eta}/256\log(2)}).$$

Observons que comme pour tout $P \in \mathbf{I}_N,\ w(P) - k$ est pair, il résulte de (8.21) que pour tout nombre réel α, on a $g(\alpha - 1/2) = g(\alpha) = g(\alpha + 1/2)$. Donc,

$$\beta_-(N,k) = \int_0^v g(\alpha - 1/2)d\alpha = \int_0^v g(\alpha)d\alpha$$

et de même

$$\beta_+(N,k) = \int_{-v}^0 g(\alpha + 1/2)d\alpha = \int_0^v g(\alpha)d\alpha.$$

Donc $\beta_-(N,k) + \beta_0(N,k) + \beta_+(N,k) = 2\beta_0(N,k)$ et on termine la preuve comme dans le cas $q \neq 2$.

□

Références

[1] O. Ahmadi, *Weights of irreducible polynomials*, Handbook of finite fields, ed. G. L. Mullen, D. Panario, Discrete Mathematics and its Applications (2013), 70-72.

[2] P. Billingsley, *Probalility and Measure*, Wiley series in probability and mathematical statistics (1995).

[3] N.L. Bassily, I. Kátai, *Distribution of the values of q-additive functions on polynomial sequences*, Acta Math. Hung. **68** (1995), 353-361.

[4] J. Bourgain, *Prescribing the binary digits of the primes*, Israel J. Math. **194** (2013), no. 2, 935-955.

[5] J. Bourgain, *Prescribing the binary digits of the primes, II*, Israel J. Math. **206** (2015), no. 1, 165-182.

[6] M. Car, *Distribution des polynômes irréductibles dans* $\mathbb{F}_q[T]$, Acta Arith. **88** (1999), 141-153.

[7] S. D. Cohen, *Prescribed coefficients*, Handbook of finite fields, ed. G. L. Mullen, D. Panario, Discrete Mathematics and its Applications (2013), 73-79.

[8] M. Car, C. Mauduit, *Fonctions complètement Q-additives pour les carrés*, Bull. Soc Math. France **144** (2016), 775-817.

[9] M. Drmota, G. Gutenbrunner, *The joint distribution of Q-additive functions on polynomials over finite fields*, J. Theor. Nombres Bordeaux **17** (2005), 125-150.

[10] M. Drmota, C. Mauduit, J. Rivat, *Primes with an average sum of digits*, Compositio Math. **145** (2009) 271-292.00000

[11] G. Effinger, D.R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field*, Oxford Mathematical Monographs (1991).

[12] P. X. Gallagher, *Bombieri's mean value theorem*, Mathematika **15** (1968) 1-6.

[13] D. R. Hayes, *The expression of a polynomial as the sum of three irreducibles,* Acta Arith **11** (1966), 461-488.

[14] J. Ha, *Irreducible polynomials with several prescribed coefficients*, Finite Fields Appl. **40** (2016), 10-25.

[15] C.H. Hsu, *The distribution of irreducible polynomials in* $\mathbb{F}_q[T]$, J. Number Theory **61** (1996), 85-96.

[16] H. Iwaniec, E. Kowalski, *Analytic number theory*, vol. 53 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI, 2004.

[17] R. Lidl, H. Niederreiter, *Finite Fields*, Introduction to finite fields and their applications, Cambridge University Press (1986).

[18] B. Martin, C. Mauduit, J. Rivat, *Théorème des nombres premiers pour les fonctions digitales*, Acta Arithmetica **165** (2014), 11-45.

[19] B. Martin, C. Mauduit, J. Rivat, *Fonctions digitales le long des nombres premiers*, Acta Arithmetica **170** (2015),175-197.

[20] B. Martin, C. Mauduit, J. Rivat, *Propriétés locales des chiffres des nombres premiers*, J. Inst. Math. Jussieu (à paraître).

[21] B. Martin, C. Mauduit, J. Rivat, *Nombres premiers avec contraintes digitales multiples*, Bull. Soc. Math. France (à paraître).

[22] C. Mauduit, J. Rivat, *La somme des chiffres des carrés*, Acta Math., **203** (2009), 107-148.

[23] C. Mauduit, J. Rivat, *Sur un problème de Gelfond : la somme des chiffres des nombres premiers*, Ann. of Math. **171** (2010), 1591-1646.

[24] C. Mauduit, J. Rivat, *Prime numbers along Rudin-Shapiro sequences*, Journal of the European Mathematical Society **17** (2015), 2595-2642.

[25] C. Mauduit, A. Sárközy, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith **81**, $n\,°2$, (1997), 145-173

[26] P. Pollack, *Irreducible polynomials with several prescribed coefficients*, Finite Fields Appl. **22** (2013), 70-78.

[27] O. Ramaré, *Prime numbers : emergence and victories of bilinear forms decomposition*, European Math. Soc. newsletter **90** (2013), 18–28.

[28] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Math. **95** (1972).

[29] R. C. Vaughan, *Mean value theorems in prime number theory*, J. London Math. Soc. **10** (1975) 153-162.

[30] R. C. Vaughan, *On the distribution of αp modulo 1*, Mathematika **24** (1977) 135-141.

[31] A. Weil, *Basic NumberTheory*, 3rd Ed., Springer, Berlin (1974).