

Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

RÉPARTITION DES FONCTIONS COMPLÈTEMENT Q -ADDITIVES LE LONG DES CARRÉS DE POLYNÔMES SUR UN CORPS FINI

Mireille Car & Christian Mauduit

Tome 144
Fascicule 4

2016

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du Centre national de la recherche scientifique
pages 775-817

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 4, tome 144, décembre 2016

Comité de rédaction

Emmanuel BREUILLARD

Yann BUGEAUD

Jean-François DAT

Charles FAVRE

Marc HERZLICH

O'Grady KIERAN

Raphaël KRIKORIAN

Julien MARCHÉ

Emmanuel RUSS

Christophe SABOT

Wilhelm SCHLAG

Pascal HUBERT (dir.)

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
smf@smf.univ-mrs.fr

Hindustan Book Agency
O-131, The Shopping Mall
Arjun Marg, DLF Phase 1
Gurgaon 122002, Haryana
Inde

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 43 € (\$ 64)
Abonnement Europe : 178 €, hors Europe : 194 € (\$ 291)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Nathalie Christiaën

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
revues@smf.ens.fr • <http://smf.emath.fr/>

© Société Mathématique de France 2016

Tous droits réservés (article L 122-4 du Code de la propriété intellectuelle). Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'éditeur est illicite. Cette représentation ou reproduction par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L 335-2 et suivants du CPI.

ISSN 0037-9484

Directeur de la publication : Stéphane SEURET

RÉPARTITION DES FONCTIONS COMPLÈTEMENT Q -ADDITIVES LE LONG DES CARRÉS DE POLYNÔMES SUR UN CORPS FINI

PAR MIREILLE CAR & CHRISTIAN MAUDUIT

RÉSUMÉ. — Soit F un corps fini à q éléments (q impair), $Q \in F[T]$ et f une fonction complètement Q -additive à valeurs entières. L'objet de ce travail est l'étude des sommes d'exponentielles $\sum_{\substack{X \in F[T] \\ \deg X < N}} \exp(2\pi i \alpha f(X^2))$ pour $\alpha \in \mathbb{R}$. Nous en déduisons en particulier une condition nécessaire et suffisante portant sur f pour que, pour tout $(a, m) \in \mathbb{N} \times \mathbb{N}^*$, on ait $\text{card}\{X \in \mathbf{A} \mid \deg X < N, f(X^2) \equiv a \pmod{m}\} = \frac{q^N}{m} + O(q^{(1-h)N})$, avec $0 < h < 1$.

ABSTRACT (*Repartition of completely Q -additive functions along squares of polynomials over a finite field*)

Let F be a finite field with q elements (q odd), $Q \in F[T]$ and f an integer valued completely Q -additive function. The goal of this work is to study the exponential sums $\sum_{\substack{X \in F[T] \\ \deg X < N}} \exp(2\pi i \alpha f(X^2))$ for $\alpha \in \mathbb{R}$. In particular, this study provides a necessary and sufficient condition on f under which, for any $(a, m) \in \mathbb{N} \times \mathbb{N}^*$, we have $\text{card}\{X \in \mathbf{A} \mid \deg X < N, f(X^2) \equiv a \pmod{m}\} = \frac{q^N}{m} + O(q^{(1-h)N})$, with $0 < h < 1$.

Texte reçu le 19 février 2015, révisé le 5 janvier 2016 accepté le 9 février 2016.

MIREILLE CAR, Université d'Aix-Marseille, Institut de Mathématiques de Marseille CNRS, UMR 7373, CMI, 39 rue F. Joliot-Curie 13453 Marseille Cedex 13, France

CHRISTIAN MAUDUIT, Université d'Aix-Marseille 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

Classification mathématique par sujets (2000). — 11 T 55.

Mots clefs. — Polynômes sur un corps fini, fonctions Q -additives, sommes d'exponentielles. Recherche effectuée avec le soutien de l'Agence Nationale de La Recherche, projet ANR-10-BLAN 0103 MUNUM et de Ciéncia sem Fronteiras, projet PVE 407308/2013-0.

1. Introduction et notations

Soit F un corps fini à q éléments et de caractéristique p . On note \mathbf{A} l'anneau $F[T]$ des polynômes à une variable sur le corps F , \mathbf{M} l'ensemble des polynômes unitaires de $F[T]$ et \mathbf{I} l'ensemble des polynômes irréductibles unitaires de $F[T]$. Si X et Y sont des polynômes non nuls, on note $\tau(X)$ le nombre de diviseurs unitaires de X et (X, Y) le plus grand commun diviseur unitaire de X et Y . Dans tout cet article, $Q \in \mathbf{A}$ est un polynôme de degré $d > 0$ et on note $\mathcal{C}_Q = \{X \in \mathbf{A} \mid \deg X < \deg Q\}$ l'ensemble des restes de la division euclidienne par Q où l'on convient que $\deg 0 = -\infty$. Tout polynôme $X \in \mathbf{A}$ admet une unique représentation comme somme

$$(1.1) \quad X = \sum_{n=0}^{\infty} X_n Q^n,$$

où $X_n \in \mathcal{C}_Q$ pour tout $n \in \mathbb{N}$, appelée représentation de X en base Q . La suite $(X_n)_{n \in \mathbb{N}}$ dont tous les termes sont nuls à partir d'un certain rang est la suite des chiffres de X en base Q . La valeur absolue d'un polynôme $X \in \mathbf{A}$ est définie par

$$(1.2) \quad \langle X \rangle = \begin{cases} q^{\deg X} & \text{si } X \neq 0, \\ 0 & \text{si } X = 0 \end{cases}$$

et on note $|\mathcal{X}|$ le nombre d'éléments de tout ensemble fini \mathcal{X} .

DÉFINITION. — *Une application f de \mathbf{A} dans un groupe additif \mathbf{B} est dite complètement Q -additive si pour tout $Y \in \mathbf{A}$ et tout $R \in \mathcal{C}_Q$, on a $f(YQ+R) = f(Y) + f(R)$.*

Observons qu'une fonction complètement Q -additive f à valeurs dans un groupe \mathbf{B} est déterminée par les valeurs prises par f sur l'ensemble des chiffres \mathcal{C}_Q . En effet, si (1.1) est la représentation de X en base Q , alors $f(X) = \sum_{n=0}^{\infty} f(X_n)$.

Drmota et Gutenbrunner ont étudié dans [7] la distribution des fonctions Q -additives sur \mathbf{A} et montré des résultats analogues à ceux obtenus par Bassily-Kátai, Kim et Drmota dans le cas des nombres entiers (voir [1], [12] et [5]). Madritsch et Thuswaldner ont étudié dans [14] le cas plus général des sommes de Weyl polynomiales associées aux fonctions Q -additives. Lorsque \mathbf{B} est égal à l'anneau $\mathbf{A} = F[T]$, la fonction « somme des chiffres en base Q » définie pour tout $X \in A$ écrit sous la forme (1.1) par $s(X) = \sum_{n \geq 0} X_n$, constitue un exemple typique de fonction Q -additive sur \mathbf{A} . Dans [3] nous avons étudié son comportement sur les puissances k -ièmes des éléments de \mathbf{A} . Dans cet article nous nous intéressons au cas plus difficile à traiter des fonctions Q -additives à valeurs réelles.

Un exemple simple de fonctions complètement Q -additives à valeurs entières est fourni par les fonctions de poids Q -adique $w_Q^{(\ell)}$, ℓ étant un paramètre réel, définies par

$$(1.3) \quad w_Q^{(\ell)}(X) = \sum_{n=0}^{\infty} \langle X_n \rangle^{\ell}$$

pour tout $X \in \mathbf{A}$ dont la représentation en base Q est donnée par (1.1). En particulier, $w_Q^{(0)}(X)$ est le nombre de chiffres de X différents de 0.

Drmota et Gutenbrunner ont montré dans [7] l'existence d'un théorème central limite pour les fonctions complètement Q -additives à valeurs réelles sur les puissances k -ièmes des éléments de \mathbf{A} :

THÉORÈME. — *Pour toute fonction complètement Q -additive $f : \mathbf{A} \rightarrow \mathbb{R}$ et pour tout nombre entier $k > 0$, on a pour y nombre réel et n nombre entier tendant vers $+\infty$,*

$$\frac{1}{q^n} |\{X \in \mathbf{A} \mid \deg X < n, f(X^k) \leq \frac{kn}{\deg Q} \mu_f + y \sqrt{\frac{nk}{\deg Q} \sigma_f}\}| = \Phi(y) + o(1),$$

avec $\mu_f = q^{-\deg Q} \sum_{x \in \mathcal{C}_Q} f(x)$, $\sigma_f^2 = q^{-\deg Q} \sum_{x \in \mathcal{C}_Q} f(x)^2$ et $\Phi(y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^y e^{-t^2/2} dt$, la loi de distribution normale.

Dans ce qui suit, on suppose que f une fonction complètement Q -additive à valeurs entières définie sur \mathbf{A} de caractéristique p impaire et on s'intéresse à la répartition des valeurs prises par $f(X^2)$, X décrivant l'anneau \mathbf{A} . Lorsque la caractéristique de \mathbf{A} est égale à 2, les carrés de \mathbf{A} ont des propriétés particulières qui peuvent conduire à des représentations Q -adiques très atypiques. Par exemple, si $p = 2$ et $Q = T^2$, la fonction complètement Q -additive f définie sur $\mathcal{C}_Q = \{x_0 + x_1 T, (x_0, x_1) \in \mathbb{F}^2\}$ par

$$f(x_0 + x_1 T) = \begin{cases} 0 & \text{si } x_1 = 0, \\ 1 & \text{si } x_1 \neq 0 \end{cases}$$

est nulle sur les carrés de \mathbf{A} .

Le but de cet article est de montrer que la méthode introduite par Mauduit et Rivat dans [17] (voir également [9] et [20] pour des généralisations) peut être adaptée à \mathbf{A} afin d'étudier le comportement de $f(X^2)$ lorsque $p \neq 2$. Notons que l'étude du comportement de $f(X^k)$ pour $k \geq 3$ semble hors d'atteinte par les techniques connues à ce jour (sauf lorsque k est une puissance de p).

La situation est rendue plus complexe que dans le cas des nombres entiers par l'existence d'obstructions de nature arithmétique propres à \mathbf{A} et qui n'apparaissaient pas dans le cas des nombres entiers. Plus précisément, nous allons identifier une classe de fonctions complètement Q -additives pour lesquelles,

pour tout nombre entier $k > 0$, la suite $(\frac{k}{p}f(X^2))_{X \in \mathbf{A}}$ a un comportement pathologique.

Par exemple, dans le cas où $\mathbf{A} = \mathbb{F}_3[T]$, $Q = T$ et f est l'application de A dans \mathbb{R} définie par $f(0) = 0$, $f(1) = 1$, $f(2) = 2$, on a

$$|\{X \in \mathbb{F}_3[T] \mid \deg X < n, f(X^2) \equiv a \pmod{3}\}| = \begin{cases} 3^{n-1} & \text{si } a = 0, \\ 2 \times 3^{n-1} & \text{si } a = 1, \\ 0 & \text{si } a = 2 \end{cases}$$

et f n'est donc pas équidistribuée sur les carrés.

À toute forme linéaire $\lambda : F^d \rightarrow F$, on associe l'application λ^* de \mathcal{C}_Q dans \mathbb{F}_p définie par $\lambda^*(\sum_{i=0}^{d-1} x_i Y^i) = \text{tr}(\lambda(x_0, \dots, x_{d-1}))$, où tr désigne la trace de F sur \mathbb{F}_p .

DÉFINITION. — *On dit qu'une application w de \mathcal{C}_Q dans \mathbb{Z} est dans la classe \mathcal{L} s'il existe une forme linéaire $\lambda : F^d \rightarrow F$ telle que pour tout $X \in \mathcal{C}_Q$, $\lambda^*(X)$ soit la classe de $w(X)$ modulo p . Les fonctions Q -additives f pour lesquelles $f|_{\mathcal{C}_Q}$ décrit \mathcal{L} sont dites dégénérées et on note \mathcal{D} l'ensemble de ces fonctions.*

Théorème 1.1. — *Soit f une fonction complètement Q -additive à valeurs entières dégénérée. Alors il existe une constante $\gamma(q, Q, f) > 0$ ne dépendant que de q, Q et f telle que pour tout nombre entier k et tout nombre entier $N > \deg Q$, on a*

$$\left| \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} \exp\left(2\pi i \frac{k}{p} f(X^2)\right) \right| \geq \gamma(q, Q, f) q^N.$$

Le principal théorème établi dans cet article est le suivant :

Théorème 1.2. — *Soit f une fonction complètement Q -additive à valeurs entières non dégénérée. Alors, pour tout nombre réel α non entier, il existe un nombre réel $0 < a(q, Q, f, \alpha) < 1$ et un nombre entier $N(q, Q, f, \alpha)$ ne dépendant que de q, Q, f et α tel que pour tout nombre entier $N \geq N(q, Q, f, \alpha)$ on a*

$$\left| \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} \exp(2\pi i \alpha f(X^2)) \right| \leq b(q, Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1-a(q, Q, f, \alpha))},$$

$\omega(Q)$ désignant le nombres de polynômes irréductibles distincts divisant Q et $b(q, Q) > 0$ étant une constante ne dépendant que de q et de Q .

On déduit de ce théorème le corollaire ci dessous :

COROLLAIRE 1.3. — *Soit f une fonction complètement Q -additive à valeurs entières non dégénérée. Alors, pour tout nombre entier $m > 0$, il existe un nombre réel $0 < h(q, Q, f, m) < 1$, tel que pour tout nombre entier rationnel a , on a*

$$|\{X \in \mathbf{A} \mid \deg X < n, f(X^2) \equiv a \pmod{m}\}| = \frac{q^n}{m} + O(q^{n(1-h(q, Q, f, m))}),$$

les constantes impliquées par le symbole O ne dépendant que de q, Q, f et m .

La preuve du théorème 1.1 sera donnée à la section 3. Pour obtenir la majoration du théorème 1.2 prouvée à la section 6, nous majorerons les sommes

$$\Sigma_f(N) = \sum_{\substack{X \in \mathbf{A} \\ \nu \deg Q \leq \deg X < N}} \exp(2\pi i \alpha f(X^2)),$$

où $\nu = \nu(N)$ est le nombre entier déterminé par la condition $\nu \deg Q < N \leq (\nu + 1) \deg Q$. Ceci sera fait à la section 5. Les outils nécessaires à ces preuves seront établis aux sections 2 et 4. Ce sont essentiellement des majorations de sommes de caractères faisant intervenir le caractère E défini à la section 2.1.

Remarque. — Dans [18], Mauduit et Rivat on introduit une nouvelle méthode permettant d'étudier la répartition de la somme des chiffres des nombres premiers (voir [6], [8], [15], [16], [19] pour des généralisation de ce résultat). Il serait intéressant de savoir si cette méthode peut être adaptée à l'étude du comportement des fonctions complètement Q -additives sur l'ensemble des polynômes irréductibles de \mathbf{A} .

Pour $\alpha \in \mathbb{R}$, on pose $e(\alpha) = \exp(2\pi i \alpha)$ et on note $\|\alpha\|$ la distance de α au nombre entier le plus proche. Pour alléger l'écriture, nous ne préciserons pas la dépendance des constantes à q et, dans les estimations de sommes de caractères, nous identifierons un élément x de \mathbb{F}_p à son image $j(x)$, j étant la bijection naturelle de \mathbb{F}_p sur $\{0, 1, \dots, p-1\}$.

2. Rappels et lemmes techniques concernant le caractère exponentiel E

2.1. Le caractère E . — On note \mathbf{K} le corps $F(T)$. La valuation à l'infini sur le corps \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 $\mathbf{K}_\infty = F((T^{-1}))$ des séries de Laurent formelles $y = \sum_{n=-\infty}^{+\infty} y_n T^n$, où $y_n \in F$ et les coefficients y_n sont tous nuls pour n assez grand. On prolonge v_∞ à \mathbf{K}_∞ en posant pour $y \neq 0$,

$$v_\infty(y) = -\sup\{n \in \mathbb{Z} \mid y_n \neq 0\}.$$

Si \mathcal{P} est l'idéal de valuation de \mathbf{K}_∞ , alors tout $y \in \mathbf{K}_\infty$ s'écrit de façon unique comme somme $y = [y] + \{y\}$, avec $[y] \in \mathbf{A}$ et $\{y\} \in \mathcal{P}$ (où $[y]$ et $\{y\}$ peuvent

être vus comme les parties entière et fractionnaire de y). Soit $\psi : F \mapsto \mathbb{C}$ le caractère non trivial du groupe additif de F défini par

$$\psi(x) = e\left(\frac{j(\text{tr}(x))}{p}\right).$$

On associe à ψ un caractère additif non trivial de \mathbf{K}_∞ en posant pour tout $y = \sum_{n=-\infty}^{+\infty} y_n T^n \in \mathbf{K}_\infty : E(y) = \psi(\text{Res}(y))$, où $\text{Res}(y) = y_{-1}$ (voir par exemple [4], [10] ou [21]). Ce caractère est trivial sur l'anneau \mathbf{A} . Dans la suite de ce travail nous utiliserons souvent une conséquence immédiate de cette propriété à savoir, l'implication : Si A, B, H sont dans \mathbf{A} avec $H \neq 0$, alors

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

2.2. Sommes associées au caractère E . — Tout d'abord rappelons sans démonstration le résultat fondamental suivant (voir [11]).

PROPOSITION 2.1. — Soit, pour $y \in \mathbf{K}_\infty$ et N un nombre entier naturel,

$$(2.1) \quad S(y, N) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} E(yX).$$

Alors, on a

$$(2.2) \quad S(y, N) = \begin{cases} q^N & \text{si } v_\infty(\{y\}) > N, \\ 0 & \text{sinon.} \end{cases}$$

On en déduit le corollaire :

COROLLAIRE 2.2. — Soit $H \in \mathbf{A}$ un polynôme non nul et soit $G \in \mathbf{A}$. Alors, on a

$$(2.3) \quad \sum_{X \in \mathcal{C}_H} E\left(\frac{GX}{H}\right) = \begin{cases} \langle H \rangle & \text{si } G \equiv 0 \pmod{H}, \\ 0 & \text{sinon.} \end{cases}$$

PROPOSITION 2.3. — Pour tout $H \in \mathbf{A}$ non nul, on désigne par $v_Q(H)$ le plus grand nombre entier m tel que Q^m divise H . Soient m, n et ℓ des nombres entiers tels que $0 \leq m \leq n \leq \ell$ et soit $\theta \in \mathbb{R}$. Alors, on a

$$(2.4) \quad \begin{aligned} & \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ m \leq v_Q(D) \leq n}} \langle D \rangle^{1/2} \langle Q \rangle^{\theta v_Q(D)} \\ & \leq (n - m + 1) \tau(Q^{\ell-m}) \left(\frac{\langle Q \rangle}{q}\right)^{\ell/2} \max\left((\langle Q \rangle^\theta q^{1/2})^m, (\langle Q \rangle^\theta q^{1/2})^n\right). \end{aligned}$$

Démonstration. — Analogue à celle du lemme 19 de [17]. □

LEMME 2.4. — Pour tout $u \in \mathbb{R}$, on a

$$(2.5) \quad |1 + e(u)| \leq 2 - 4\|u\|^2.$$

Démonstration. — On a $|1 + e(u)|^2 = 4(1 - \sin(\pi u)^2) \leq 4(1 - 4\|u\|^2)$, d'où $|1 + e(u)| \leq 2(1 - 2\|u\|^2)$. \square

PROPOSITION 2.5. — Soit w une application de \mathcal{C}_Q dans \mathbb{Z} n'appartenant pas à la classe \mathcal{L} . Pour $\alpha \in \mathbb{R}$ et $H \in \mathcal{C}_Q$, soit

$$(2.6) \quad \phi = \phi_1(Q, w, \alpha, H) = \sum_{X \in \mathcal{C}_Q} e(\alpha w(X)) E\left(-\frac{HX}{Q}\right).$$

Si $\alpha \in \mathbb{R} \setminus \mathbb{Z}$, alors il existe une constante $0 < c_{Q, w, \alpha} \leq 1$ telle que pour tout $H \in \mathcal{C}_Q$, on a

$$(2.7) \quad |\phi_1(Q, w, \alpha, H)| \leq \langle Q \rangle - c_{Q, w, \alpha}.$$

Démonstration. — Posons $d = \deg Q$. Dans le corps \mathbf{K}_∞ , $\frac{H}{Q}$ se développe en série de Laurent

$$\frac{H}{Q} = \sum_{i \leq -1} \frac{a_i}{T^i}.$$

Pour tout $X = \sum_{j=0}^{d-1} x_j T^j$ appartenant à \mathcal{C}_Q , on a

$$\begin{aligned} E\left(-\frac{HX}{Q}\right) &= \psi(-(a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1})) \\ &= e\left(\frac{\text{tr}(-(a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1}))}{p}\right), \end{aligned}$$

d'où

$$e(\alpha w(X)) E\left(-\frac{HX}{Q}\right) = e(\alpha w(X)) - \frac{\text{tr}(a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1})}{p}.$$

Notons $L_H(X) = a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1}$. Soit α un nombre réel non entier. Si α n'est pas un nombre rationnel de la forme ℓ/p , ℓ premier à p alors, pour tout chiffre $X \in \mathcal{C}_Q$ non nul, on a $(\alpha w(X) - \frac{\text{tr}(L_H(X))}{p}) \notin \mathbb{Z}$. Si $\alpha = \ell/p$, ℓ étant premier à p , comme $w \notin \mathcal{L}$, il existe $X \in \mathcal{C}_Q$ non nul tel que $(w(X) - \text{tr}(L_H(X))) \notin \mathbb{Z}$. Dans l'un ou l'autre cas on peut choisir $X_H \in \mathcal{C}_Q - \{0\}$ maximisant $\|\alpha w(X) - \frac{\text{tr}(L_H(X))}{p}\|$. On pose $\Delta_{Q, w, \alpha, H} = \|\alpha w(X_H) - \frac{\text{tr}(L_H(X_H))}{p}\|$ et $\delta_{Q, w, \alpha} = \min_{H \in \mathcal{C}_Q} \Delta_{w, \alpha, H}$ et on note que $\delta_{Q, w, \alpha} > 0$. La somme $\phi = \phi_1(Q, w, \alpha, H)$ s'écrit

$$\phi = 1 + e\left(\alpha w(X_H) - \frac{\text{tr}(L_H(X_H))}{p}\right) + \sum_{\substack{X \in \mathcal{C}_Q \\ X \notin \{0, X_H\}}} e(\alpha w(X)) E\left(-\frac{HX}{Q}\right),$$

d'où

$$|\phi| \leq |1 + e(\alpha w(X_H) - \frac{\text{tr}(L_H(X_H))}{p})| + \langle Q \rangle - 2.$$

Avec (2.5), il vient

$$\begin{aligned} |\phi| &\leq \langle Q \rangle - 4\|\alpha w(X_H) - \frac{\text{tr}(L_H(X_H))}{p}\|^2 \\ &= \langle Q \rangle - 4\Delta_{Q,w,\alpha,H} \leq \langle Q \rangle - 4\delta_{Q,w,\alpha}^2. \end{aligned}$$

□

Pour des commodités d'écriture, posons $c_{Q,w,\alpha} = 0$ dans le cas où $\alpha \in \mathbb{Z}$.

PROPOSITION 2.6. — *Soit w une application de \mathcal{C}_Q dans \mathbb{Z} n'appartenant pas à la classe \mathcal{L} . Soient $\alpha \in \mathbb{R}$ et $H \in \mathbf{A}$ avec $\deg Q > 0$ et, pour tout nombre entier $j > 0$,*

$$(2.8) \quad \phi_j = \phi_j(Q, w, \alpha, H) = \sum_{R \in \mathcal{C}_Q} e(\alpha w(R)) E\left(-\frac{HR}{Q^j}\right).$$

Alors on a

$$(2.9) \quad \phi_j \leq \langle Q \rangle - c_{Q,w,\alpha}.$$

Démonstration. — Soit $H = \sum_{k=0}^m H_k Q^k$, $H_k \in \mathcal{C}_Q$ le développement de H en base Q . Le caractère E étant trivial sur \mathbf{A} , on a

$$E\left(\frac{HR}{Q^j}\right) = E\left(\sum_{k=0}^{\min(m,j-1)} \frac{H_k R}{Q^{j-k}}\right) = \prod_{k=0}^{\min(m,j-1)} E\left(\frac{H_k R}{Q^{j-k}}\right).$$

Pour $0 \leq k \leq j-2$, on a $v_\infty\left(\frac{H_k R}{Q^{j-k}}\right) \geq 2$, d'où $E\left(\frac{H_k R}{Q^{j-k}}\right) = 1$. Par suite,

$$\phi_j = \sum_{R \in \mathcal{C}_Q} e(\alpha w(R)) E\left(-\frac{H_j R}{Q}\right) = \phi_1(w, \alpha, Q, H_j)$$

et la proposition précédente nous donne $\phi_j \leq \langle Q \rangle - c_{Q,w,\alpha}$. □

2.3. Sommes de Gauss quadratiques associées au caractère E . — Pour $H \in \mathbf{A}$ non nul et $(A, B) \in \mathbf{A}^2$, soit

$$(2.10) \quad \Gamma(H; A, B) = \sum_{X \in \mathcal{C}_H} E\left(\frac{AX^2 + BX}{H}\right).$$

PROPOSITION 2.7. — *Soit $(H, A, B) \in \mathbf{A}^3$ avec $H \neq 0$. Alors, on a*

- (1) $\Gamma(H; A, B) = \langle (A, H) \rangle \Gamma\left(\frac{H}{(A, H)}, \frac{A}{(A, H)}, \frac{B}{(A, H)}\right)$ si (A, H) divise B ;
- (2) $\Gamma(H; A, B) = 0$ si (A, H) ne divise pas B .

Démonstration. — On pose $H = H_1(A, H)$, $A = A_1(A, H)$. Tout $X \in \mathcal{C}_H$ s'écrivant de façon unique $X = Y + ZH_1$ avec $Y \in \mathcal{C}_{H_1}$ et $Z \in \mathcal{C}_{(A, H)}$, on a

$$\begin{aligned}\Gamma(H; A, B) &= \sum_{Y \in \mathcal{C}_{H_1}} \sum_{Z \in \mathcal{C}_{(A, H)}} E\left(\frac{A_1(Y + ZH_1)^2}{H_1} + \frac{B(Y + ZH_1)}{H_1(A, H)}\right) \\ &= \sum_{Y \in \mathcal{C}_{H_1}} E\left(\frac{A_1 Y^2}{H_1} + \frac{BY}{H_1(A, H)}\right) \sum_{Z \in \mathcal{C}_{(A, H)}} E\left(\frac{BZ}{(A, H)}\right).\end{aligned}$$

Le corollaire 2.2 nous donne alors

$$\Gamma(H; A, B) = \left(\sum_{Y \in \mathcal{C}_{H_1}} E\left(\frac{A_1 Y^2}{H_1} + \frac{BY}{H_1(A, H)}\right) \right) \times \begin{cases} \langle(A, H) \rangle \text{ si } (A, H) | B, \\ 0 \text{ sinon,} \end{cases}$$

ce qui prouve (2). Si (A, H) divise B , on pose $B = B_1(A, H)$. On a alors

$$\Gamma(H; A, B) = \langle(A, H) \rangle \sum_{Y \in \mathcal{C}_{H_1}} E\left(\frac{A_1 Y^2}{H_1} + \frac{B_1 Y}{H_1}\right) = \langle(A, H) \rangle \Gamma(H_1; A_1, B_1).$$

□

PROPOSITION 2.8. — Soit $(H, A, B) \in \mathbf{A}^3$ avec $H \neq 0$. Alors, on a

$$(2.11) \quad |\Gamma(H; A, B)| \leq \langle(A, H) \rangle^{1/2} \langle H \rangle^{1/2}.$$

Démonstration. — Si (A, H) ne divise pas B , la relation (2.11) est triviale d'après la proposition 2.7 (2). On suppose que (A, H) divise B . Comme ci-dessus, on pose $H = H_1(A, H)$, $A = A_1(A, H)$, $B = B_1(A, H)$. Les polynômes A_1 et H_1 étant premiers entre eux, il existe $C_1 \in \mathcal{C}_{H_1}$ tel que $B_1 \equiv 2A_1C_1 \pmod{H_1}$. Par suite,

$$\Gamma(H_1; A_1, B_1) = \sum_{Y \in \mathcal{C}_{H_1}} E\left(\frac{A_1(Y^2 + 2C_1Y)}{H_1}\right) = \sum_{Y \in \mathcal{C}_{H_1}} E\left(\frac{A_1(Y + C_1)^2}{H_1}\right) E\left(-\frac{C_1^2}{H_1}\right).$$

L'application $Y \rightarrow Y + C_1$ étant une permutation de l'ensemble \mathcal{C}_{H_1} , on a $\Gamma(H_1; A_1, B_1) = E\left(-\frac{C_1^2}{H_1}\right) \Gamma(H_1; A_1, 0)$, d'où $|\Gamma(H_1; A_1, B_1)| = |\Gamma(H_1; A_1, 0)|$. Les propositions III.2 et III.3 de [2] nous donnent $|\Gamma(H_1; A_1, 0)| = \langle H_1 \rangle^{1/2}$, d'où, d'après la proposition 2.7 (1),

$$|\Gamma(H; A, B)| = \langle(A, H) \rangle \langle H_1 \rangle^{1/2} = \langle(A, H) \rangle^{1/2} \langle H \rangle^{1/2}.$$

□

3. Démonstration du théorème 1.1

Soit λ une application linéaire non nulle de F^d dans F , λ^* l'application de \mathcal{C}_Q dans \mathbb{F}_p définie par

$$\lambda^*\left(\sum_{i=0}^{d-1} x_i T^i\right) = \text{tr}(\lambda(x_0, x_1, \dots, x_{d-1}))$$

et f^* la fonction complètement Q -additive à valeurs dans \mathbb{F}_p prolongeant λ^* à l'anneau \mathbf{A} .

PROPOSITION 3.1. — *Les applications λ^* et f^* sont \mathbb{F}_p -linéaires et*

$$\text{Ker}f^* = \text{Ker}\lambda^* + (Q-1),$$

$(Q-1)$ désignant l'idéal de \mathbf{A} engendré par le polynôme $Q-1$.

Démonstration. — La linéarité de λ^* est évidente et on vérifie facilement celle de f^* . L'inclusion $\text{Ker}\lambda^* \subset \text{Ker}f^*$ est également évidente et pour montrer l'inclusion $(Q-1) \subset \text{Ker}f^*$, on remarque que si $X = \sum_{m=0}^{\infty} X_m Q^m$ est la représentation en base Q de $X \in \mathbf{A}$, alors $X(Q-1) = -X_0 + \sum_{m=0}^{\infty} (X_m - X_{m+1})Q$ et par suite

$$\begin{aligned} f^*(X(Q-1)) &= \lambda^*(-X_0) + \sum_{m=0}^{\infty} \lambda^*(X_m - X_{m+1}) \\ &= -\lambda^*(X_0) + \sum_{m=0}^{\infty} (\lambda^*(X_m) - \lambda^*(X_{m+1})) = 0. \end{aligned}$$

Montrons maintenant l'inclusion inverse. Soit $Y \in \text{Ker}f$. On fait la division euclidienne de Y par $Q-1$: $Y = R + X(Q-1)$, avec $R \in \mathcal{C}_{Q-1}$ et $X \in \mathbf{A}$. On a vu que $X(Q-1) \in \text{Ker}f^*$. Il s'en suit que $R \in \text{Ker}f^*$. Comme $\deg R < \deg(Q-1) = \deg Q$, on a $f(R) = \lambda(R)$, c'est à dire $R \in \text{Ker}\lambda^*$. \square

On pose pour tout nombre entier N strictement positif et tout $a \in \mathbb{F}_p$,

$$(3.1) \quad U_N(a) = |\{X \in \mathbf{A} ; \deg X < N \text{ et } f^*(X^2) = a\}|.$$

La proposition suivante permet de relier le calcul de $U_N(a)$ à des résultats connus concernant les formes quadratiques sur les corps finis.

PROPOSITION 3.2. — *Soient (u_1, \dots, u_d) l'élément non nul de F^d tel que pour $(x_0, \dots, x_{d-1}) \in F^d$, $\lambda(x_0, \dots, x_{d-1}) = u_1 x_0 + \dots + u_d x_{d-1}$ et $(z_{-m})_{m \geq 1}$ la suite d'éléments de F définie par*

$$\frac{Y_{\lambda}}{Q-1} = \sum_{m=1}^{\infty} z_{-m} T^{-m},$$

où $Y_\lambda = [(Q-1)(u_1T^{-1} + u_2T^{-2} + \cdots + u_dT^{-d})]$. Soit φ la forme quadratique à d variables définie sur F^d par

$$\varphi(x_0, \dots, x_{d-1}) = \sum_{k=0}^{2d-2} z_{-k-1} \left(\sum_{i+j=k} x_i x_j \right).$$

Alors,

- (i) la forme φ n'est pas nulle ;
- (ii) pour tout $a \in \mathbb{F}_p$ et tout nombre entier $N > d$, on a

$$U_N(a) = q^{N-d} |\{(x_0, \dots, x_{d-1}) \in F^d ; \operatorname{tr}(\varphi(x_0, \dots, x_{d-1})) = a\}|.$$

Démonstration. — Posons $D = Q - 1$. La forme linéaire λ n'étant pas nulle, elle est surjective. La trace l'étant aussi, λ^* est surjective et il existe $R \in \mathcal{C}_Q$ tel que $\lambda^*(R) = a$. Comme

$$\operatorname{Ker} f^* = \operatorname{Ker} \lambda^* + (Q-1) = \operatorname{Ker} \lambda^* + (D),$$

on en déduit

$$U_N(a) = \sum_{A \in \operatorname{Ker} \lambda^*} |\{X \in \mathbf{A} ; \deg X < N \text{ et } X^2 \equiv R + A \pmod{D}\}|.$$

Supposons $N > d$. La division euclidienne par D nous donne l'égalité

$$|\{X \in \mathbf{A} ; \deg X < N \text{ et } X^2 \equiv R + A \pmod{D}\}| = q^{N-d} v(R, A),$$

où

$$v(R, A) = |\{X \in \mathcal{C}_D ; X^2 \equiv R + A \pmod{D}\}|.$$

Si $A \in \operatorname{Ker} \lambda^*$, on a par orthogonalité,

$$v(R, A) = \sum_{X \in \mathcal{C}_D} \frac{1}{\langle D \rangle} \sum_{Y \in \mathcal{C}_D} E\left(\frac{(X^2 - R - A)Y}{D}\right),$$

d'où avec (3.1)

$$(3.2) \quad q^{2d-N} U_N(a) = \sum_{Y \in \mathcal{C}_D} E\left(-\frac{RY}{D}\right) \sum_{X \in \mathcal{C}_D} E\left(\frac{X^2 Y}{D}\right) \sigma_Y,$$

où $\sigma_Y = \sum_{A \in \operatorname{Ker} \lambda^*} E\left(-\frac{AY}{D}\right)$. Pour tout $Y \in \mathcal{C}_D$, l'application $A \mapsto E\left(-\frac{AY}{D}\right)$ est un caractère du groupe additif $\operatorname{Ker} \lambda^*$ et la somme σ_Y vaut donc 0 ou $|\operatorname{Ker} \lambda^*| = q^d/p$. D'autre part,

$$\sum_{Y \in \mathcal{C}_D} \sum_{A \in \operatorname{Ker} \lambda^*} E\left(-\frac{AY}{D}\right) = \sum_{A \in \operatorname{Ker} \lambda^*} \sum_{Y \in \mathcal{C}_D} E\left(-\frac{AY}{D}\right) = q^d$$

et donc il y a exactement $q^d/|\operatorname{Ker} \lambda^*| = p$ polynômes $Y \in \mathcal{C}_D$ pour lesquels la somme σ_Y est non nulle. Déterminons ces polynômes.

Comme $Y_\lambda = [D(u_1T^{-1} + u_2T^{-2} + \dots + u_dT^{-d})]$, on a $v_\infty(\frac{Y_\lambda}{D} - (u_1T^{-1} + u_2T^{-2} + \dots + u_dT^{-d})) > d$. Donc, pour tout $A \in \mathcal{C}_D$ et tout $b \in \mathbb{F}_p$ on a $v_\infty(b(\frac{Y_\lambda}{D} - (u_1T^{-1} + u_2T^{-2} + \dots + u_dT^{-d}))A) > 1$ d'où

$$E(b \frac{Y_\lambda A}{D}) = E(b(u_1T^{-1} + u_2T^{-2} + \dots + u_dT^{-d})A).$$

Si $A = \sum_{i=0}^{d-1} a_i T^i$, alors

$$(3.3) \quad E(b \frac{Y_\lambda A}{D}) = e\left(\frac{\text{tr}(b(u_1a_0 + \dots + u_da_{d-1}))}{p}\right) = e\left(\frac{b\text{tr}(u_1a_0 + \dots + u_da_{d-1})}{p}\right).$$

En particulier, on a $E(\frac{bY_\lambda A}{D}) = 1$ pour tout $(b, A) \in \mathbb{F}_p \times \text{Ker } \lambda^*$. Par suite, pour tout $b \in \mathbb{F}_p$, la somme σ_{bY_λ} est non nulle. Les p polynômes $Y \in \mathcal{C}_D$ pour lesquels $\sigma_Y \neq 0$ sont donc les polynômes bY_λ , b décrivant \mathbb{F}_p . Avec (3.2) il vient

$$(3.4) \quad pq^{d-N} U_N(a) = \sum_{b \in \mathbb{F}_p} E\left(-\frac{bRY_\lambda}{D}\right) \sum_{X \in \mathcal{C}_D} E\left(\frac{bX^2Y_\lambda}{D}\right) = \sum_{X \in \mathcal{C}_D} \Theta_X,$$

où

$$(3.5) \quad \Theta_X = \sum_{b \in \mathbb{F}_p} E\left(b\left(\frac{Y_\lambda(X^2 - R)}{D}\right)\right).$$

Les sommes Θ_X valent 0 ou p . Posons $R = \rho_0 + \rho_1T + \dots + \rho_{2d-2}T^{2d-2}$ avec $\rho_d = \rho_{d+1} = \dots = \rho_{2d-2} = 0$. Pour $X = \sum_{i=0}^{d-1} x_i T^i$ appartenant à \mathcal{C}_D , on a d'après (3.3)

$$E(bY_\lambda(X^2 - R)/D)) = e\left(\text{tr}\left(\sum_{k=0}^{2d-2} z_{-k-1} \left(\sum_{i+j=k} x_i x_j - \rho_k\right)\right)/p\right).$$

D'après (3.5), on a

$$\Theta_X = p \Leftrightarrow \text{tr}\left(\sum_{k=0}^{2d-2} z_{-k-1} \left(\sum_{i+j=k} x_i x_j - \rho_k\right)\right) = 0,$$

soit en posant

$$\varphi(x_0, \dots, x_{d-1}) = \sum_{k=0}^{2d-2} z_{-k-1} \left(\sum_{i+j=k} x_i x_j\right) \text{ et } b(a) = \sum_{k=0}^{d-1} z_{-k-1} \rho_k,$$

$$\Theta_X = p \Leftrightarrow \text{tr}(\varphi(x_0, \dots, x_{d-1}) - b(a)) = 0.$$

Comme

$$\begin{aligned} \sum_{m=1}^{\infty} z_{-m} T^{-m} &= \frac{Y_{\lambda}}{D} \\ &= u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d} \\ &\quad + \frac{\{D(u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d})\}}{D}, \end{aligned}$$

on a $z_{-m} = u_m$ pour $m = 1, \dots, d$. Cela montre d'une part que la forme φ n'est pas nulle et que d'autre part $b(a) = \sum_{k=0}^{d-1} u_{-k-1} \rho_k = \lambda(\rho_0, \dots, \rho_{d-1})$. On a donc $\text{tr}(b(a)) = a$ d'où, d'après (3.4), $q^{d-N} U_N(a) = |\{(x_0, \dots, x_{d-1}) \in F^d, \text{tr}(\varphi(x_0, \dots, x_{d-1}) = a)\}|$, ce qui est le résultat annoncé. \square

Nous pouvons maintenant démontrer le théorème 1.1.

Preuve du théorème 1.1. — Posons

$$S_k(N) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} \text{e}\left(\frac{k}{p} f(X^2)\right).$$

La fonction f étant à valeurs entières, on peut supposer $0 \leq k < p$. Si $k = 0$, alors $S_k(N) = q^N$. Il reste à prouver la proposition dans le cas où $0 < k < p$, ce que l'on supposera maintenant. Comme $f \in \mathcal{D}$, on a $w = f|_{\mathcal{C}_Q} \in \mathcal{L}$. Il existe λ , application linéaire non nulle de F^d dans F telle que pour tout $X \in \mathcal{C}_Q$, $\lambda^*(X)$ soit la classe de $w(X)$ modulo p . Par Q -additivité, pour tout $X \in \mathbf{A}$, la classe de $f(X)$ modulo p est $f^*(X)$. Donc,

$$S_k(N) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} \text{e}\left(\frac{k}{p} f(X^2)\right) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} \text{e}\left(\frac{k}{p} f^*(X^2)\right) = \sum_{a \in \mathbb{F}_p} \text{e}\left(\frac{ak}{p}\right) U_N(a).$$

Si l'on suppose $N > d$, il s'en suit que $S_k(N) = q^{N-d} \sum_{a \in \mathbb{F}_p} \text{e}\left(\frac{ak}{p}\right) u(a)$. La forme φ_{λ} n'est pas nulle. Soit $r \in [1, d]$ son rang et δ son discriminant. Elle est équivalente à une forme diagonale $\phi(y_1, \dots, y_d) = y_1^2 + \cdots + y_{r-1}^2 + a_r y_r^2$ où a_r est un élément non nul de F . Par suite, pour tout $a \in \mathbb{F}_p$, on a

$$u(a) = q^{d-r} \nu(a),$$

où $\nu(a) = |\{(y_1, \dots, y_r) \in F^r, \text{tr}(\theta(y_1, \dots, y_r)) = a\}|$ et $\theta(y_1, \dots, y_r) = y_1^2 + \cdots + y_{r-1}^2 + a_r y_r^2$. On a donc

$$\nu(a) = \sum_{\substack{x \in F \\ \text{tr}(x)=a}} n_{\theta}(x),$$

où $n_{\theta}(x) = |\{(y_1, \dots, y_r) \in F^r, \theta(y_1, \dots, y_r) = x\}|$. Les propositions 6.26 et 6.27 de [13] nous donnent les valeurs des nombres $n_{\theta}(x)$. Pour cela, notons η le caractère quadratique du corps F et remarquons que $|\text{Ker}(\text{tr})| = q/p$.

Supposons d'abord r pair. La proposition 6.26 de [13] nous donne

$$n_\theta(x) = q^{r-1} + v(x)q^{(r-2)/2}\eta((-1)^{r/2}\delta) \text{ avec } v(x) = \begin{cases} -1 & \text{si } x \neq 0, \\ q-1 & \text{si } x = 0. \end{cases}$$

Si $a \neq 0$, les $x \in F$ intervenant dans la somme $\nu(a)$ sont non nuls. Si $a = 0$, 0 intervient dans la somme $\nu(a)$ et il y a exactement $\frac{q}{p} - 1$ éléments x non nuls intervenant dans $\nu(a)$. D'où,

$$\begin{aligned} S_k(N) &= q^{N-r} \left(\frac{q}{p} (q^{r-1} - q^{(r-2)/2} \eta((-1)^{r/2}\delta)) \sum_{\substack{a \in \mathbb{F}_p \\ a \neq 0}} e\left(\frac{ak}{p}\right) \right. \\ &\quad \left. + \left(\frac{q}{p} - 1\right) (q^{r-1} - q^{(r-2)/2} \eta((-1)^{r/2}\delta)) \right. \\ &\quad \left. + q^{r-1} + (q-1)q^{(r-2)/2} \eta((-1)^{r/2}\delta) \right) \\ &= q^{N-r} \left(\frac{q}{p} (q^{r-1} - q^{(r-2)/2} \eta((-1)^{r/2}\delta)) \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) + q^{r/2} \eta((-1)^{r/2}\delta) \right) \\ &= q^{N-r/2} \eta((-1)^{r/2}\delta), \end{aligned}$$

ce qui donne le résultat annoncé lorsque r est pair.

Supposons maintenant r impair. La proposition 6.27 de [13] nous donne

$$n_\theta(x) = q^{r-1} + q^{(r-1)/2} \eta((-1)^{(r-1)/2} x \delta),$$

d'où

$$\begin{aligned} S_k(N) &= q^{N-r} \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) \left(\frac{q^r}{p} + q^{(r-1)/2} \eta((-1)^{(r-1)/2} \delta) \sum_{\substack{x \in F \\ \text{tr}(x)=a}} \eta(x) \right), \\ &= q^{N-(r+1)/2} \eta((-1)^{(r-1)/2} \delta) \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) \sum_{\substack{x \in F \\ \text{tr}(x)=a}} \eta(x). \end{aligned}$$

Posons $\sigma = \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) \sum_{\substack{x \in F \\ \text{tr}(x)=a}} \eta(x)$. On a

$$\begin{aligned} \sigma &= \frac{q}{p} \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) + \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) \sum_{\substack{x \in F \\ \text{tr}(x)=a}} \eta(x) \\ &= \sum_{a \in \mathbb{F}_p} e\left(\frac{ak}{p}\right) \sum_{\substack{x \in F \\ \text{tr}(x)=a}} (1 + \eta(x)) = \sum_{\substack{x \in F \\ \text{tr}(x)=a}} e\left(\frac{\text{tr}(x)k}{p}\right) (1 + \eta(x)) \end{aligned}$$

$$= \sum_{\substack{x \in F \\ \text{tr}(x)=a}} \text{e}\left(\frac{\text{tr}(x)k}{p}\right) |\{y \in F; y^2 = x\}| = \sum_{y \in F} \text{e}\left(\frac{\text{tr}(y^2)k}{p}\right) = \sum_{y \in F} \psi(ky^2),$$

ψ étant le caractère additif de F défini dans la section 2.1. On a $|\sigma| = q^{1/2}$ (voir par exemple [13, Théorème 5.15]) et il s'en suit que $|S_k(N)| = q^{N-r/2}$, ce qui donne le résultat annoncé lorsque r est impair. \square

4. Transformées de Fourier associées aux fonctions complètement Q -additives tronquées

Dans ce paragraphe ainsi que dans les paragraphes suivants on suppose que $f \notin \mathcal{D}$ et on définit les fonctions Q -additives tronquées de la manière suivante. Soient λ et μ des nombres entiers tels que $0 \leq \mu \leq \lambda$. Pour tout $X \in \mathbf{A}$ dont la représentation en base Q est donnée par (1.1), on définit $f_\lambda(X)$ et $f_{\mu,\lambda}(X)$ par

$$(4.1) \quad f_\lambda(X) = \sum_{n=0}^{\lambda-1} f(X_n), \quad f_{\mu,\lambda}(X) = \sum_{n=\mu}^{\lambda-1} f(X_n).$$

Soit $\alpha \in \mathbb{R}$, fixé. On pose pour tout $H \in \mathbf{A}$,

$$(4.2) \quad F_\lambda(H) = F_\lambda^{(f)}(\alpha, H) = \langle Q \rangle^{-\lambda} \sum_{X \in \mathcal{C}_{Q^\lambda}} \text{e}(\alpha f_\lambda(X)) E\left(-\frac{HX}{Q^\lambda}\right),$$

et

$$(4.3) \quad F_{\mu,\lambda}(H) = F_{\mu,\lambda}^{(f)}(\alpha, H) = \langle Q \rangle^{-\lambda} \sum_{X \in \mathcal{C}_{Q^\lambda}} \text{e}(\alpha f_{\mu,\lambda}(X)) E\left(-\frac{HX}{Q^\lambda}\right).$$

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

PROPOSITION 4.1. — *Soit un nombre entier $\lambda \geq 0$.*

- (i) *Si $X \in \mathcal{C}_{Q^\lambda}$, alors $f_\lambda(X) = f(X)$.*
- (ii) *Si $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathcal{C}_Q$, alors $f_{\lambda+1}(QX + Y) = f_\lambda(X) + f(Y) = f(X) + f(Y)$.*
- (iii) *Si $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathbf{A}$, alors $f_\lambda(X + YQ^\lambda) = f(X) = f_\lambda(X)$.*
- (iv) *Si μ est un nombre entier tel que $\mu < \lambda$, si $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$ et si $Z \in \mathcal{C}_{Q^\mu}$, alors $f_{\mu,\lambda}(YQ^\mu + Z) = f(Y) = f_{\lambda-\mu}(Y)$.*
- (v) *Si $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathbf{A}$, alors $F_\lambda(X + YQ^\lambda) = F_\lambda(X)$.*
- (vi) *Si $X \in \mathbf{A}$ et $Y \in \mathbf{A}$ sont congrus modulo Q^λ , alors, $F_\lambda(X) = F_\lambda(Y)$.*
- (vii) *Si μ est un nombre entier tel que $\mu < \lambda$, si $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$ et si $Z \in \mathcal{C}_{Q^\mu}$, alors $F_{\mu,\lambda}(YQ^\mu + Z) = F_{\lambda-\mu}(Y)$.*

Démonstration. — Les points (i), (iii), et (iv) sont évidents; (v) et (vii) décourent de (4.2) et (4.3), (iii) et de la définition du caractère E ; (vi) est une conséquence de (v). Pour démontrer (ii), il suffit de vérifier que pour $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathcal{C}_Q$ on a $f_{\lambda+1}(QX+Y) = f(QX+Y) = f(X)+f(Y) = f(X)+f(Y) = f_\lambda(X)+f(Y)$. \square

PROPOSITION 4.2. — *On a $F_0(H) = 1$ et, pour tout nombre entier $\lambda \geq 1$,*

$$\langle Q \rangle^\lambda F_\lambda(H) = \prod_{j=1}^{\lambda} \phi_j(Q, f, \alpha, H),$$

les fonctions ϕ_j étant définies par (2.8).

Démonstration. — Utilisant la proposition 4.1-(ii), la preuve est analogue à celle de la relation (17) de [17]. \square

PROPOSITION 4.3. — *Soient un nombre entier $\lambda > 0$ et $H \in \mathbf{A}$. Alors, on a*

$$(4.4) \quad |F_\lambda(H)| \leq \langle Q \rangle^{-C(Q, f, \alpha)\lambda},$$

avec

$$(4.5) \quad C(Q, f, \alpha) = \frac{c_{Q, f, \alpha}}{\langle Q \rangle \deg Q \log q},$$

où $c_{Q, f, \alpha}$ est défini dans la Proposition 2.5.

Démonstration. — La proposition précédente donne le résultat quand $\lambda = 0$. Lorsque $\lambda > 0$, la proposition 4.2 jointe à la majoration (2.9) donne

$$|F_\lambda(H)| = \langle Q \rangle^{-\lambda} \prod_{j=1}^{\lambda} |\phi_j(Q, f, \alpha, H)| \leq \left(1 - \frac{c_{Q, f, \alpha}}{\langle Q \rangle}\right)^\lambda.$$

Soit $C = C(Q, f, \alpha) = c_{Q, f, \alpha}/\langle Q \rangle \log \langle Q \rangle$. Alors, $C \log \langle Q \rangle \leq \log \left(\frac{1}{1 - c_{Q, f, \alpha}/\langle Q \rangle}\right)$, d'où $1 - c_{Q, f, \alpha}/\langle Q \rangle \leq \langle Q \rangle^{-C}$. \square

PROPOSITION 4.4. — *Soient $A \in \mathbf{A}$ et δ et λ des nombres entiers tels que $0 \leq \delta \leq \lambda$. Alors, on a*

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A \pmod{Q^\delta}}} |F_\lambda(X)|^2 = |F_\delta(A)|^2.$$

Démonstration. — Utilisant la proposition 4.1-(ii), la preuve est analogue à celle du lemme 19 de [18]. \square

PROPOSITION 4.5. — Soient λ et μ des nombres entiers tels que $0 \leq \mu < \lambda$. Alors, pour tout $H \in \mathbf{A}$, on a

$$\langle Q \rangle^\mu F_{\mu, \lambda}(H) = F_{\lambda-\mu}(H) S\left(\frac{H}{Q^\lambda}, \mu \deg Q\right),$$

où S est définie par (2.1).

Démonstration. — Utilisant la proposition 4.1-(iv), la preuve est analogue à celle à celle du lemme 10 de [17]. \square

PROPOSITION 4.6. — Soient λ et μ des nombres entiers tel que $0 \leq \mu < \lambda$. Alors, on a

$$\sum_{X \in \mathcal{C}_{Q^\lambda}} |F_{\mu, \lambda}(X)| = \sum_{R \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(R)| \leq \langle Q \rangle^{\lambda-\mu}.$$

Démonstration. — Ici on fait la division euclidienne par $Q^{\lambda-\mu}$ des polynômes $X \in \mathcal{C}_{Q^\lambda}$. Avec la proposition précédente, il vient

$$\begin{aligned} \langle Q \rangle^\mu \sum_{X \in \mathcal{C}_{Q^\lambda}} |F_{\mu, \lambda}(X)| &= \sum_{\substack{R \in \mathcal{C}_{Q^{\lambda-\mu}} \\ L \in \mathcal{C}_{Q^\mu}}} |F_{\lambda-\mu}(R + LQ^{\lambda-\mu})| |S\left(\frac{R + LQ^{\lambda-\mu}}{Q^\lambda}, \mu \deg Q\right)| \\ &= \sum_{\substack{R \in \mathcal{C}_{Q^{\lambda-\mu}} \\ L \in \mathcal{C}_{Q^\mu}}} |F_{\lambda-\mu}(R + LQ^{\lambda-\mu})| |S\left(\frac{R + LQ^{\lambda-\mu}}{Q^\lambda}, \mu \deg Q\right)| \end{aligned}$$

puisque d'après la proposition 2.1, les sommes $S\left(\frac{R + LQ^{\lambda-\mu}}{Q^\lambda}, \mu \deg Q\right)$ sont positives ou nulles. La partie (v) de la proposition 4.1 nous donne ensuite

$$\langle Q \rangle^\mu \sum_{X \in \mathcal{C}_{Q^\lambda}} |F_{\mu, \lambda}(X)| = \sum_{R \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(R)| \sum_{L \in \mathcal{C}_{Q^\mu}} S\left(\frac{R + LQ^{\lambda-\mu}}{Q^\lambda}, \mu \deg Q\right).$$

Or,

$$\begin{aligned} \sum_{L \in \mathcal{C}_{Q^\mu}} S\left(\frac{R + LQ^{\lambda-\mu}}{Q^\lambda}, \mu \deg Q\right) &= \sum_{L \in \mathcal{C}_{Q^\mu}} \sum_{Y \in \mathcal{C}_{Q^\mu}} E\left(\left(\frac{R}{Q^\lambda} + \frac{L}{Q^\mu}\right)Y\right) \\ &= \sum_{Y \in \mathcal{C}_{Q^\mu}} E\left(\frac{RY}{Q^\lambda}\right) \sum_{L \in \mathcal{C}_{Q^\mu}} E\left(\frac{LY}{Q^\mu}\right) = \langle Q \rangle^\mu \end{aligned}$$

d'après le corollaire 2.2. En reportant cette égalité dans la somme précédente, on obtient

$$\sum_{X \in \mathcal{C}_{Q^\lambda}} |F_{\mu, \lambda}(X)| = \sum_{R \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(R)|$$

et on majore trivialement $|F_{\lambda-\mu}(R)|$ par 1. \square

PROPOSITION 4.7. — Soient λ, δ et μ des nombres entiers tels que $1 \leq \mu < \lambda, \lambda - \mu \leq \delta \leq \lambda$. Si $A \in \mathbf{A}$, alors on a

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A \pmod{Q^\delta}}} |F_{\mu, \lambda}(X)| = \begin{cases} |F_{\lambda-\mu}(A)| & \text{si } v_\infty(\{A/Q^\delta\}) > (\mu + \delta - \lambda) \deg Q, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. — Soit $R \in \mathcal{C}_{Q^\delta}$ congru à A modulo Q^δ . Alors A et R sont congrus modulo $Q^{\lambda-\mu}$. Les polynômes $X \in \mathcal{C}_{Q^\lambda}$ congrus à A modulo Q^δ sont de la forme $X = R + LQ^\delta$ avec $L \in \mathcal{C}_{Q^{\lambda-\delta}}$; ils sont congrus à R modulo $Q^{\lambda-\mu}$ et vérifient, d'après la proposition 4.5, la relation

$$\langle Q \rangle^\mu F_{\mu, \lambda}(X) = F_{\lambda-\mu}(R) S\left(\frac{R + LQ^\delta}{Q^\lambda}, \mu \deg Q\right).$$

La positivité des sommes $S\left(\frac{R + LQ^\delta}{Q^\lambda}, \mu \deg Q\right)$ jointe à la proposition 4.1-(vi) permet d'écrire

$$\langle Q \rangle^\mu \sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A \pmod{Q^\delta}}} |F_{\mu, \lambda}(X)| = |F_{\lambda-\mu}(A)| \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} S\left(\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}}, \mu \deg Q\right).$$

Par ailleurs, d'après le corollaire 2.2,

$$\begin{aligned} \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} S\left(\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}}, \mu \deg Q\right) &= \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} \sum_{X \in \mathcal{C}_{Q^\mu}} E\left(\left(\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}}\right) X\right) \\ &= \sum_{X \in \mathcal{C}_{Q^\mu}} E\left(\frac{RX}{Q^\lambda}\right) \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} E\left(\frac{LX}{Q^{\lambda-\delta}}\right) = \langle Q \rangle^{\lambda-\delta} \sum_{\substack{X \in \mathcal{C}_{Q^\mu} \\ X \equiv 0 \pmod{Q^{\lambda-\delta}}}} E\left(\frac{RX}{Q^\lambda}\right). \end{aligned}$$

La proposition 2.1 donne alors

$$\begin{aligned} \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} S\left(\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}}, \mu \deg Q\right) \\ = \langle Q \rangle^{\lambda-\delta} \times \begin{cases} \langle Q \rangle^{\mu+\delta-\lambda} & \text{si } v_\infty(R/Q^\delta) > (\mu + \delta - \lambda) \deg Q, \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

On a donc

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A \pmod{Q^\delta}}} |F_{\mu, \lambda}(X)| = |F_{\lambda-\mu}(A)| \times \begin{cases} 1 & \text{si } v_\infty(R/Q^\delta) > (\mu + \delta - \lambda) \deg Q, \\ 0 & \text{sinon} \end{cases}$$

et on conclut en observant que $v_\infty(R/Q^\delta) = v_\infty(\{A/Q^\delta\})$. \square

PROPOSITION 4.8. — Soient λ, δ et μ des nombres entiers tels que $1 \leq \mu < \lambda$ et $\delta \leq \lambda - \mu$. Si $(A, L) \in \mathbf{A}^2$, alors on a

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A \pmod{Q^\delta}}} |F_{\mu, \lambda}(X)F_{\lambda-\mu}(X+L)| \leq |F_\delta(A)| |F_\delta(A+L)|.$$

Démonstration. — Notons B la somme à majorer et $R \in \mathcal{C}_{Q^\delta}$ le reste de A modulo Q^δ . Les polynômes $X \in \mathcal{C}_{Q^\lambda}$ congrus à R modulo Q^δ sont de la forme $X = Y + ZQ^{\lambda-\mu}$ avec $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$, $Y \equiv R \pmod{Q^\delta}$ et $Z \in \mathcal{C}_{Q^\mu}$. D'après les propositions 4.5 et 4.1-(v), on obtient comme ci-dessus

$$\langle Q \rangle^\mu B = \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R \pmod{Q^\delta}}} |F_{\lambda-\mu}(Y)| |F_{\lambda-\mu}(L+Y)| \sum_{Z \in \mathcal{C}_{Q^\mu}} S\left(\frac{Y}{Q^\lambda} + \frac{Z}{Q^\mu}\right), \mu \deg Q.$$

Mais, pour tout $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$, on a

$$\begin{aligned} \sum_{Z \in \mathcal{C}_{Q^\mu}} S\left(\frac{Y}{Q^\lambda} + \frac{Z}{Q^\mu}\right), \mu \deg Q &= \sum_{Z \in \mathcal{C}_{Q^\mu}} \sum_{W \in \mathcal{C}_{Q^\mu}} E\left(\left(\frac{Y}{Q^\lambda} + \frac{Z}{Q^\mu}\right)W\right) \\ &= \sum_{W \in \mathcal{C}_{Q^\mu}} E\left(\frac{YW}{Q^\lambda}\right) \sum_{Z \in \mathcal{C}_{Q^\mu}} E\left(\frac{ZW}{Q^\mu}\right) = \langle Q \rangle^\mu \end{aligned}$$

d'après le corollaire 2.2. On a donc,

$$B = \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R \pmod{Q^\delta}}} |F_{\lambda-\mu}(Y)| |F_{\lambda-\mu}(L+Y)|.$$

L'inégalité de Cauchy-Schwarz donne

$$B^2 \leq \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R \pmod{Q^\delta}}} |F_{\lambda-\mu}(Y)|^2 \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R \pmod{Q^\delta}}} |F_{\lambda-\mu}(L+Y)|^2.$$

Notons V le reste de L modulo $Q^{\lambda-\mu}$. Pour tout $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$, on a avec la proposition 4.1-(vi) $F_{\lambda-\mu}(L+Y) = F_{\lambda-\mu}(V+Y)$, d'où

$$\begin{aligned} \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R \pmod{Q^\delta}}} |F_{\lambda-\mu}(L+Y)|^2 &= \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R \pmod{Q^\delta}}} |F_{\lambda-\mu}(V+Y)|^2 \\ &= \sum_{\substack{Z \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Z \equiv V+R \pmod{Q^\delta}}} |F_{\lambda-\mu}(Z)|^2. \end{aligned}$$

La proposition 4.4 donne alors $B^2 \leq |F_\delta(R)|^2 |F_\delta(V+R)|^2$. On conclut en remarquant que puisque $R \equiv A \pmod{Q^\delta}$ et $V+R \equiv L+A \pmod{Q^\delta}$, on a $F_\delta(R) = F_\delta(A)$, $F_\delta(R+V) = F_\delta(A+L)$. \square

PROPOSITION 4.9. — *Soient λ, δ et μ des nombres entiers tels que $1 \leq \mu < \lambda$, $\lambda - \mu \leq \delta \leq \lambda$. Si $A \in \mathbf{A}$, alors on a*

$$\sum_{\substack{X, Y \in \mathcal{C}_{Q^\lambda} \\ X - Y \equiv A \pmod{Q^\delta}}} |F_{\mu, \lambda}(X) F_{\mu, \lambda}(Y)| \leq \begin{cases} 1 \text{ si } v_\infty(\{A/Q^\delta\}) > (\mu + \delta - \lambda) \deg Q, \\ 0 \text{ sinon.} \end{cases}$$

Démonstration. — Posons

$$B' = \sum_{\substack{X, Y \in \mathcal{C}_{Q^\lambda} \\ X - Y \equiv A \pmod{Q^\delta}}} |F_{\mu, \lambda}(X) F_{\mu, \lambda}(Y)|.$$

Soit $A' \in \mathcal{C}_{Q^\delta}$ congru à A modulo Q^δ . Alors

$$B' = \sum_{Y \in \mathcal{C}_{Q^\lambda}} |F_{\mu, \lambda}(Y)| \sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A' + Y \pmod{Q^\delta}}} |F_{\mu, \lambda}(X)|.$$

D'après la proposition 4.7,

$$B' = \sum_{\substack{Y \in \mathcal{C}_{Q^\lambda} \\ v_\infty(\{\frac{Y+A'}{Q^\delta}\}) > (\mu + \delta - \lambda) \deg Q}} |F_{\mu, \lambda}(Y)| |F_{\lambda-\mu}(Y+A')|.$$

Soit $Y \in \mathcal{C}_{Q^\lambda}$. Ecrivons Y comme somme $Y = R + ZQ^\delta$ avec $R \in \mathcal{C}_{Q^\delta}$ et $Z \in \mathcal{C}_{Q^{\lambda-\delta}}$. Comme $\delta \geq \lambda - \mu$, on a $Y + A' \equiv R + A' \pmod{Q^{\lambda-\mu}}$. D'après la proposition 4.1-(vi), on a $F_{\lambda-\mu}(Y+A') = F_{\lambda-\mu}(R+A')$. D'autre part, $v_\infty(\{\frac{Y+A'}{Q^\delta}\}) = v_\infty(\{\frac{R+A'}{Q^\delta}\})$ et on a

$$v_\infty(\{\frac{A+Y}{Q^\delta}\}) > (\mu + \delta - \lambda) \deg Q \Leftrightarrow \deg(R+A') < (\lambda - \mu) \deg Q.$$

En posant $S = R + A'$ on peut écrire

$$\begin{aligned} B' &= \sum_{S \in \mathcal{C}_{Q^{\lambda-\mu}}} \sum_{Z \in \mathcal{C}_{Q^{\lambda-\delta}}} |F_{\mu, \lambda}(S - A' + ZQ^\delta)| |F_{\lambda-\mu}(S)| \\ &= \sum_{S \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(S)| \sum_{Z \in \mathcal{C}_{Q^{\lambda-\delta}}} |F_{\mu, \lambda}(S - A' + ZQ^\delta)|. \end{aligned}$$

Lorsque Z décrit l'ensemble $\mathcal{C}_{Q^{\lambda-\delta}}$, le polynôme $S - A' + ZQ^\delta$ décrit l'ensemble des polynômes $X \in \mathcal{C}_{Q^\lambda}$ congrus à $S - A'$ modulo Q^δ . Par suite,

$$B' = \sum_{S \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(S)| \sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv S - A' \pmod{Q^\delta}}} |F_{\mu,\lambda}(X)|.$$

La proposition 4.7 nous donne pour $S \in \mathcal{C}_{Q^{\lambda-\mu}}$ fixé,

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv S - A' \pmod{Q^\delta}}} |F_{\mu,\lambda}(X)| = \begin{cases} |F_{\lambda-\mu}(S - A')| & \text{si } v_\infty(\{\frac{S-A'}{Q^\delta}\}) > (\mu + \delta - \lambda) \deg Q, \\ 0 & \text{sinon.} \end{cases}$$

Par ailleurs on a

$$\begin{aligned} v_\infty(\{\frac{S-A'}{Q^\delta}\}) &> (\mu + \delta - \lambda) \deg Q \\ \Leftrightarrow \deg(S - A') &< (\lambda - \mu) \deg Q \Leftrightarrow \deg(A') < (\lambda - \mu) \deg Q. \end{aligned}$$

Donc, si $\deg A' \geq (\lambda - \mu) \deg Q$, alors $B' = 0$ et si $\deg A' < (\lambda - \mu) \deg Q$, alors

$$C = \sum_{S \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(S)| |F_{\lambda-\mu}(S - A')|$$

et la proposition 4.8 donne $B' \leq |F_0(0)| |F_0(-A')| = 1$. \square

5. Majoration de la somme $\Sigma_f(N)$

Le nombre réel α étant toujours fixé. Soient un nombre entier $N > 0$ et $\mathcal{X} = \mathcal{X}(N)$ l'ensemble des polynômes $X \in \mathbf{A}$ tels que

$$(5.1) \quad \nu \deg Q \leq \deg X < N,$$

où $\nu = \nu(N)$ est le nombre entier déterminé par la condition

$$(5.2) \quad \nu \deg Q < N \leq (\nu + 1) \deg Q.$$

Observons que l'ensemble \mathcal{X} a au plus q^N éléments. Posons

$$(5.3) \quad \Sigma(N) = \sum_{X \in \mathcal{X}} e(\alpha f(X^2)).$$

Nous supposerons N assez grand pour que $\nu(N) \geq 30 \deg Q$. Soient des nombres entiers r et m tels que

$$(5.4) \quad \begin{cases} \text{(i)} & 1 < r \leq \frac{\nu-3}{5 \deg Q-1} ; \\ \text{(ii)} & m < \nu - r ; \\ \text{(iii)} & m < \nu + r + 3 - 2r \deg Q ; \\ \text{(iv)} & 2m > \nu + r(1 + \deg Q). \end{cases}$$

Observons qu'à l'exception du cas $\deg Q = 1$, la condition (iii) implique la condition (ii). Observons aussi que la condition (i) assure la compatibilité des conditions (ii) et (iv) et celle des conditions (iii) et (iv). On pose

$$(5.5) \quad \ell = \nu + r + 1.$$

5.1. Utilisation des fonctions tronquées. — La proposition suivante est un analogue polynomial de l'inégalité de Van der Corput (Voir [7, Lemme 3.2]).

PROPOSITION 5.1. — *On a*

$$(5.6) \quad |\Sigma(N)|^2 \leq q^N \max_{R \in \mathcal{C}_{Q^r}} \left| \sum_{X \in \mathcal{X}} e(\alpha(f((X+R)^2)) - f(X^2)) \right|.$$

Démonstration. — Soit $R \in \mathcal{C}_{Q^r}$. Puisque $r < \nu$, l'application $X \mapsto X+R$ est une permutation de l'ensemble \mathcal{X} . On a donc

$$\sum_{X \in \mathcal{X}} e(\alpha f(X^2)) = \sum_{X \in \mathcal{X}} e(\alpha f((X+R)^2)).$$

Par suite,

$$\begin{aligned} \langle Q \rangle^r \Sigma(N) &= \langle Q \rangle^r \sum_{X \in \mathcal{X}} e(\alpha f(X^2)) = \sum_{R \in \mathcal{C}_{Q^r}} \sum_{X \in \mathcal{X}} e(\alpha f((X+R)^2)) \\ &= \sum_{X \in \mathcal{X}} \sum_{R \in \mathcal{C}_{Q^r}} e(\alpha f((X+R)^2)). \end{aligned}$$

L'inégalité de Cauchy-Schwarz donne

$$\begin{aligned} \langle Q \rangle^{2r} |\Sigma(N)|^2 &\leq |\mathcal{X}| \sum_{X \in \mathcal{X}} \left| \sum_{R \in \mathcal{C}_{Q^r}} e(\alpha f((X+R)^2)) \right|^2 \\ &\leq q^N \sum_{X \in \mathcal{X}} \sum_{\substack{R_1 \in \mathcal{C}_{Q^r} \\ R_2 \in \mathcal{C}_{Q^r}}} e(\alpha(f((X+R_1)^2) - f((X+R_2)^2))) \\ &= q^N \sum_{\substack{R_1 \in \mathcal{C}_{Q^r} \\ R_2 \in \mathcal{C}_{Q^r}}} \sum_{X \in \mathcal{X}} e(\alpha(f((X+R_1)^2) - f((X+R_2)^2))). \end{aligned}$$

L'application $X \mapsto Y = X+R_2$ étant une permutation de \mathcal{X} et l'application $R_1 \mapsto R = R_1 - R_2$ une permutation de \mathcal{C}_{Q^r} , on en déduit

$$\begin{aligned} \langle Q \rangle^{2r} |\Sigma(N)|^2 &\leq q^N \sum_{\substack{R_2 \in \mathcal{C}_{Q^r} \\ R \in \mathcal{C}_{Q^r}}} \sum_{Y \in \mathcal{X}} e(\alpha(f((Y+R)^2) - f(Y^2))), \\ &\leq q^N \langle Q \rangle^{2r} \max_{R \in \mathcal{C}_{Q^r}} \left| \sum_{Y \in \mathcal{X}} e(\alpha(f((Y+R)^2) - f(Y^2))) \right|. \quad \square \end{aligned}$$

On en déduit

PROPOSITION 5.2. — *On a*

$$(5.7) \quad |\Sigma(N)|^2 \leq q^N \max_{R \in \mathcal{C}_{Q^r}} (|T(N, r, R)|),$$

où

$$(5.8) \quad T = T(N, r, R) = \sum_{X \in \mathcal{X}} e(\alpha(f_\ell((X + R)^2) - f_\ell(X^2))),$$

f_ℓ étant la fonction tronquée introduite à la section 4.

Démonstration. — Soient $X \in \mathcal{X}$ et $R \in \mathcal{C}_{Q^r}$. On a $\deg X < N \leq (\nu+1) \deg Q$, d'où

$$\deg(XR) \leq (\nu + r + 1) \deg Q - 2 = \ell \deg Q - 2.$$

D'après 5.4 (i) on a $r \leq \nu + 1$ ce qui, compte tenu de (5.5), implique $2r \leq \ell$. Il en résulte $\deg(R^2) \leq 2r \deg Q - 2 \leq \ell \deg Q - 2$ et par suite,

$$\deg((X + R)^2 - X^2) \leq \ell \deg Q - 2.$$

Si $X^2 = \sum_{n=0}^{\infty} Y_n Q^n$ et $(X + R)^2 = \sum_{n=0}^{\infty} Z_n Q^n$ sont les représentations respectives de X^2 et $(X + R)^2$ en base Q , on a $Y_j = Z_j$ pour tout nombre entier $j \geq \ell$, d'où, avec (4.1), $f((X + R)^2) - f_\ell((X + R)^2) = f(X^2) - f_\ell(X^2)$ ou encore $f((X + R)^2) - f(X^2) = f_\ell((X + R)^2) - f_\ell(X^2)$ et on conclut grâce à (5.6). \square

En appliquant une deuxième fois l'inégalité de Van der Corput, on obtient

PROPOSITION 5.3. — *Soit $R \in \mathcal{C}_{Q^r}$. Alors*

$$(5.9) \quad T^2(N, r, R) \leq q^N \max_{S \in \mathcal{C}_{Q^r}} U(N, r, m, R, S),$$

où

$$(5.10) \quad U(N, r, m, R, S) = \left| \sum_{X \in \mathcal{X}} e(\alpha(f_{m,\ell}((X + R + SQ^m)^2) - f_{m,\ell}((X + R)^2) - f_{m,\ell}((X + SQ^m)^2) + f_{m,\ell}(X^2))) \right|.$$

Démonstration. — Soit $S \in \mathcal{C}_{Q^r}$. Alors, avec (5.4-(ii)), $\deg(SQ^m) < (m + r) \deg Q < \nu \deg Q$. L'application $X \mapsto X + SQ^m$ est donc une permutation de l'ensemble \mathcal{X} . De ce fait,

$$T = \sum_{X \in \mathcal{X}} e(\alpha(f_\ell((X + R + SQ^m)^2) - f_\ell((X + SQ^m)^2))).$$

Par suite, on a

$$\langle Q \rangle^r T = \sum_{S \in \mathcal{C}_{Q^r}} \sum_{X \in \mathcal{X}} e(\alpha(f_\ell((X + R + SQ^m)^2) - f_\ell((X + SQ^m)^2)))$$

$$= \sum_{X \in \mathcal{X}} \sum_{S \in \mathcal{C}_{Q^r}} e(\alpha(f_\ell((X + R + SQ^m)^2) - f_\ell((X + SQ^m)^2)))$$

et l'inégalité de Cauchy-Schwarz donne

$$\begin{aligned} \langle Q \rangle^{2r} |T|^2 &\leq q^N \sum_{X \in \mathcal{X}} \left| \sum_{S \in \mathcal{C}_{Q^r}} e(\alpha(f_\ell((X + R + SQ^m)^2) - f_\ell((X + SQ^m)^2))) \right|^2 \\ &= q^N \sum_{X \in \mathcal{X}} \sum_{\substack{S_1 \in \mathcal{C}_{Q^r} \\ S_2 \in \mathcal{C}_{Q^r}}} e(\theta_X(S_1) - \theta_X(S_2)), \end{aligned}$$

où pour $S \in \mathcal{C}_{Q^r}$, $\theta_X(S) = \alpha(f_\ell((X + R + SQ^m)^2) - f_\ell((X + SQ^m)^2))$. En inversant l'ordre des sommes on obtient

$$\langle Q \rangle^{2r} |T|^2 \leq q^N \sum_{\substack{S_1 \in \mathcal{C}_{Q^r} \\ S_2 \in \mathcal{C}_{Q^r}}} \sum_{X \in \mathcal{X}} e(\theta_X(S_1) - \theta_X(S_2)).$$

Les applications $X \mapsto Y = X + S_2 Q^m$ et $S_1 \mapsto S = S_1 - S_2$ sont des permutations de \mathcal{X} et \mathcal{C}_{Q^r} respectivement. Donc,

$$\langle Q \rangle^{2r} |T|^2 \leq q^N \sum_{\substack{S_2 \in \mathcal{C}_{Q^r} \\ S \in \mathcal{C}_{Q^r}}} \sum_{Y \in \mathcal{X}} e(\theta_{Y - S_2 Q^m}(S_2 + S) - \theta_{Y - S_2 Q^m}(S_2)),$$

d'où

$$\begin{aligned} \langle Q \rangle^{2r} |T|^2 &\leq q^N \sum_{S_2 \in \mathcal{C}_{Q^r}} \sum_{S \in \mathcal{C}_{Q^r}} \sum_{Y \in \mathcal{X}} e(\alpha(f_\ell((Y + R + SQ^m)^2) - f_\ell((Y + SQ^m)^2) \\ &\quad - f_\ell((Y + R)^2) + f_\ell(Y^2))), \end{aligned}$$

ce qui nous donne

$$|T|^2 \leq q^N \max_{S \in \mathcal{C}_{Q^r}} U'(N, r, m, R, S),$$

avec

$$U' = U'(N, r, m, R, S) = \left| \sum_{Y \in \mathcal{X}} e(\alpha(f_\ell((Y + R + SQ^m)^2) - f_\ell((Y + SQ^m)^2) - f_\ell((Y + R)^2) + f_\ell(Y^2))) \right|.$$

Montrons que $U' = U$, où U est défini par (5.10). Soient $Z \in \mathcal{X}$ et $S \in \mathcal{C}_{Q^r}$. Si $Z^2 = \sum_{n=0}^{\infty} V_n Q^n$ et $(Z + SQ^m)^2 = \sum_{n=0}^{\infty} W_n Q^n$ sont les représentations respectives de Z^2 et $(Z + SQ^m)^2$ en base Q , alors $V_j = W_j$ pour tout nombre entier $j < m$, d'où $f_m((Z + SQ^m)^2) = f_m(Z^2)$. D'autre part, $f_\ell(Z^2) = f_m(Z^2) + f_{m,\ell}(Z^2)$ et $f_\ell((Z + SQ^m)^2) = f_m((Z + SQ^m)^2) + f_{m,\ell}((Z + SQ^m)^2)$. Il s'en suit que

$$f_\ell((Z + SQ^m)^2) - f_\ell(Z^2) = f_{m,\ell}((Z + SQ^m)^2) - f_{m,\ell}(Z^2).$$

On reporte cette égalité dans la formule définissant U' en prenant Z égal à $Y+R$ puis à Y et on obtient $U' = U$. \square

5.2. Majoration de $U(N, r, m, R, S)$

PROPOSITION 5.4. — Pour tout $(R, S) \in \mathcal{C}_{Q^r}^2$, on a

$$(5.11) \quad \langle Q \rangle^\ell U(N, r, m, R, S) = \left| \sum_{L \in \mathcal{C}_{Q^m}} \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) \sum_{(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4} F_{m, \ell}(A) F_{m, \ell}(-B) F_{m, \ell}(-G) F_{m, \ell}(H) \Lambda(L) \right|,$$

où

$$(5.12) \quad \Lambda(L) = \Lambda(N, r, R, S, L, A, B, G, H) = \sum_{M \in \mathcal{C}_{Q^\ell}} E\left(\frac{(M+R+SQ^m)^2 A + (M+R)^2 B + (M+SQ^m)^2 G + M^2 H + LM}{Q^\ell}\right).$$

Démonstration. — On pose $U = U(N, r, m, R, S)$ et pour $X \in \mathcal{X}, Y \in \mathcal{C}_{Q^\ell}, \rho \in \{0, 1\}$ et $\sigma \in \{0, 1\}$,

$$\Theta = \Theta(X, Y, \rho, \sigma) = \sum_{Z \in \mathcal{C}_{Q^\ell}} E\left(\frac{((X+\rho R+\sigma SQ^m)^2 - Y)Z}{Q^\ell}\right).$$

D'après le corollaire 2.2, on a

$$\Theta = \begin{cases} \langle Q \rangle^\ell \text{ si } Y \equiv (X+\rho R+\sigma SQ^m)^2 \pmod{Q^\ell}, \\ 0 \quad \text{sinon,} \end{cases}$$

d'où $\Theta = \overline{\Theta}$ et

$$\langle Q \rangle^{-\ell} e(\alpha f_{m, \ell}(Y)) \Theta = \begin{cases} e(\alpha f_{m, \ell}(Y)) \text{ si } Y \equiv (X+\rho R+\sigma SQ^m)^2 \pmod{Q^\ell}, \\ 0 \quad \text{sinon.} \end{cases}$$

D'autre part, d'après la proposition 4.1-(iv), si $Y \equiv (X+\rho R+\sigma SQ^m)^2 \pmod{Q^\ell}$, alors $f_{m, \ell}(Y) = f_{m, \ell}((X+\rho R+\sigma SQ^m)^2)$. Par suite, pour $X \in \mathcal{X}$ et $(\rho, \sigma) \in \{0, 1\}^2$, on a

$$e(\alpha f_{m, \ell}((X+\rho R+\sigma SQ^m)^2)) = \sum_{Y \in \mathcal{C}_{Q^\ell}} \langle Q \rangle^{-\ell} e(\alpha f_{m, \ell}(Y)) \Theta(X, Y, \rho, \sigma).$$

On porte cette relation dans l'égalité (5.10). Il vient

$$\begin{aligned} \langle Q \rangle^{4\ell} U = & \left| \sum_{X \in \mathcal{X}} \sum_{(Y, Y', V, V') \in (\mathcal{C}_{Q^\ell})^4} \right. \\ & \times e(\alpha f_{m,\ell}(Y)) \Theta(X, Y, 1, 1) e(-\alpha f_{m,\ell}(Y')) \Theta(X, Y', 1, 0) \\ & \left. \times e(-\alpha f_{m,\ell}(V)) \Theta(X, V, 0, 1) e(\alpha f_{m,\ell}(V')) \Theta(X, V', 0, 0) \right|. \end{aligned}$$

On inverse l'ordre des sommes après avoir remplacé les $\Theta(X, \cdot, \rho, \sigma)$ par leurs valeurs et on obtient :

$$\begin{aligned} \langle Q \rangle^{4\ell} U = & \left| \sum_{Y, A \in \mathcal{C}_{Q^\ell}} e(\alpha f_{m,\ell}(Y)) E\left(\frac{-YA}{Q^\ell}\right) \sum_{Y', B \in \mathcal{C}_{Q^\ell}} e(-\alpha f_{m,\ell}(Y')) E\left(\frac{-Y'B}{Q^\ell}\right) \right. \\ & \times \left. \sum_{V, G \in \mathcal{C}_{Q^\ell}} e(-\alpha f_{m,\ell}(V)) E\left(\frac{-VG}{Q^\ell}\right) \sum_{V', H \in \mathcal{C}_{Q^\ell}} e(\alpha f_{m,\ell}(V')) E\left(\frac{-V'H}{Q^\ell}\right) \times \Psi \right|, \end{aligned}$$

où

$$\begin{aligned} \Psi = \Psi(A, B, G, H) = & \\ \sum_{X \in \mathcal{X}} E\left(\frac{(X + R + SQ^m)^2 A + (X + R)^2 B + (X + SQ^m)^2 G + X^2 H}{Q^\ell} \right). \end{aligned}$$

Avec (4.3), on a

$$(5.13) \quad U = \left| \sum_{A \in \mathcal{C}_{Q^\ell}} F_{m,\ell}(A) \sum_{B \in \mathcal{C}_{Q^\ell}} F_{m,\ell}(-B) \sum_{G \in \mathcal{C}_{Q^\ell}} F_{m,\ell}(-G) \sum_{H \in \mathcal{C}_{Q^\ell}} F_{m,\ell}(H) \Psi \right|.$$

Il nous reste à transformer la somme $\Psi(A, B, G, H)$. Pour cela, on répartit les $X \in \mathcal{X}$ dans les différentes classes modulo Q^ℓ . On a

$$\begin{aligned} \Psi(A, B, G, H) = & \\ \sum_{M \in \mathcal{C}_{Q^\ell}} \sum_{\substack{X \in \mathcal{X} \\ X \equiv M \pmod{Q^\ell}}} E\left(\frac{(X + R + SQ^m)^2 A + (X + R)^2 B + (X + SQ^m)^2 G + X^2 H}{Q^\ell} \right) \\ = & \sum_{M \in \mathcal{C}_{Q^\ell}} \sum_{\substack{X \in \mathcal{X} \\ X \equiv M \pmod{Q^\ell}}} E\left(\frac{(M + R + SQ^m)^2 A + (M + R)^2 B + (M + SQ^m)^2 G + M^2 H}{Q^\ell} \right). \end{aligned}$$

Le corollaire 2.2 nous donne alors

$$\langle Q \rangle^\ell \Psi(A, B, G, H) = \sum_{M \in \mathcal{C}_{Q^\ell}} \sum_{X \in \mathcal{X}} \sum_{L \in \mathcal{C}_{Q^\ell}} E\left(\frac{L(M - X)}{Q^\ell} \right)$$

$$\begin{aligned}
& \times E\left(\frac{(M+R+SQ^m)^2A + (M+R)^2B + (M+SQ^m)^2G + M^2H}{Q^\ell}\right) \\
& = \sum_{L \in \mathcal{C}_{Q^\ell}} \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) \\
& \times \sum_{M \in \mathcal{C}_{Q^\ell}} E\left(\frac{(M+R+SQ^m)^2A + (M+R)^2B + (M+SQ^m)^2G + M^2H + LM}{Q^\ell}\right).
\end{aligned}$$

En reportant cette valeur dans (5.13) on obtient (5.11), ce qui achève la preuve de la proposition 5.4. \square

LEMME 5.5. — *On a*

$$\sum_{L \in \mathcal{C}_{Q^\ell}} \left| \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) \right| \leq 2\left(1 - \frac{1}{q}\right) \langle Q \rangle^\ell.$$

Démonstration. — Posons pour tout $L \in \mathcal{C}_{Q^\ell}$, $\sigma_L = \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right)$. On a

$$\sigma_L = \sum_{\substack{X \in \mathbf{A} \\ \nu \deg Q \leq \deg X < N}} E\left(\frac{LX}{Q^\ell}\right) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} E\left(\frac{LX}{Q^\ell}\right) - \sum_{\substack{X \in \mathbf{A} \\ \deg X \geq \nu \deg Q}} E\left(\frac{LX}{Q^\ell}\right).$$

La proposition 2.1 donne la valeur de σ_L en fonction de $v_\infty(L/Q^\ell) = \ell \deg Q - \deg L$:

$$\sigma_L = \begin{cases} q^N - q^{\nu \deg Q} & \text{si } \deg L < \ell \deg Q - N, \\ -q^{\nu \deg Q} & \text{si } \ell \deg Q - N \leq \deg L < (\ell - \nu) \deg Q, \\ 0 & \text{si } \deg L \geq (\ell - \nu) \deg Q. \end{cases}$$

Par suite,

$$\begin{aligned}
\sum_{L \in \mathcal{C}_{Q^\ell}} \left| \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) \right| &= \sum_{\substack{L \in \mathbf{A} \\ \deg L < \ell \deg Q - N}} (q^N - \langle Q \rangle^\nu) + \sum_{\substack{L \in \mathbf{A} \\ \ell \deg Q - N \leq \deg L < (\ell - \nu) \deg Q}} \langle Q \rangle^\nu \\
&= \langle Q \rangle^\ell q^{-N} (q^N - \langle Q \rangle^\nu) + (\langle Q \rangle^{\ell - \nu} - \langle Q \rangle^\ell q^{-N}) \langle Q \rangle^\nu \\
&= 2\langle Q \rangle^\ell (1 - \langle Q \rangle^\nu q^{-N}) \leq 2\left(1 - \frac{1}{q}\right) \langle Q \rangle^\ell. \quad \square
\end{aligned}$$

PROPOSITION 5.6. — *Pour tout $(R, S) \in (\mathcal{C}_{Q^r})^2$ on a*

$$(5.14) \quad U(N, r, m, R, S) \leq 2\left(1 - \frac{1}{q}\right) \langle Q \rangle^{\ell/2} \max_{L \in \mathcal{C}_{Q^{\ell-r}}} \left(\sum_{\substack{D \in \mathbf{M} \\ D \mid Q^\ell}} \langle D \rangle^{1/2} W(L, D) \right),$$

avec

$$(5.15) \quad W(L, D) = \sum_{(A, B, G, H) \in \mathcal{G}(L, D)} |F_{m, \ell}(A) F_{m, \ell}(-B) F_{m, \ell}(-G) F_{m, \ell}(H)|,$$

$\mathcal{G}(L, D)$ désignant l'ensemble des $(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4$ vérifiant les conditions

$$(5.16) \quad \begin{cases} (i) & (A + B + G + H, Q^\ell) = D; \\ (ii) & L + 2R(A + B) + 2SQ^m(A + G) \equiv 0 \pmod{D}. \end{cases}$$

Démonstration. — Si $(R, S) \in (\mathcal{C}_{Q^r})^2$, on pose $U = U(N, r, m, R, S)$ et pour $L \in \mathcal{C}_{Q^\ell}$

$$u(L) = \sum_{(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4} F_{m, \ell}(A) F_{m, \ell}(-B) F_{m, \ell}(-G) F_{m, \ell}(H) \Lambda(L).$$

Alors, avec (5.11),

$$\begin{aligned} \langle Q \rangle^\ell U &= \left| \sum_{L \in \mathcal{C}_{Q^m}} \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) u(L) \right| \leq \sum_{L \in \mathcal{C}_{Q^m}} |u(L)| \left| \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) \right| \\ &\leq \max_{L \in \mathcal{C}_{Q^m}} |u(L)| \sum_{L \in \mathcal{C}_{Q^m}} \left| \sum_{X \in \mathcal{X}} E\left(-\frac{LX}{Q^\ell}\right) \right|, \end{aligned}$$

d'où, d'après le lemme 5.5,

$$U \leq 2\left(1 - \frac{1}{q}\right) \max_{L \in \mathcal{C}_{Q^m}} |u(L)|.$$

Avec (5.12) et Γ défini par (2.10), on a

$$\begin{aligned} |u(L)| &\leq \sum_{(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4} |F_{m, \ell}(A) F_{m, \ell}(-B) F_{m, \ell}(-G) F_{m, \ell}(H)| \\ &\quad \times |\Gamma(Q^\ell, A + B + G + H, L + 2R(A + B) + 2SQ^m(A + G))|. \end{aligned}$$

On divise la somme ci-dessus en sommes partielles, suivant les valeurs de $D = (A + B + G + H, Q^\ell)$. La Proposition 2.7 jointe à la majoration (2.11) nous donnent alors

$$\begin{aligned} |u(L)| &\leq \sum_{\substack{D \in \mathbf{M} \\ D \mid Q^\ell}} \sum_{\substack{(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4 \\ (A + B + G + H, Q^\ell) = D \\ D \mid (L + 2R(A + B) + 2SQ^m(A + G))}} |F_{m, \ell}(A) F_{m, \ell}(-B) F_{m, \ell}(-G) F_{m, \ell}(H)| \langle D \rangle^{1/2} \langle Q \rangle^{\ell/2}, \end{aligned}$$

ce qui donne le résultat annoncé. \square

Soit, pour $R \in \mathcal{C}_{Q^r}$, $S \in \mathcal{C}_{Q^r}$ et $L \in \mathcal{C}_{Q^\ell}$,

$$(5.17) \quad V = V(R, S, L) = \sum_{\substack{D \in \mathbf{M} \\ D \mid Q^\ell}} \langle D \rangle^{1/2} W(L, D).$$

On pose

$$(5.18) \quad \rho = \rho(Q) = r \deg Q - 1$$

et

$$(5.19) \quad \Delta = \Delta(Q) = \ell - m + \rho(Q).$$

La condition (5.4-(ii)) jointe à (5.5) entraîne $\Delta > 0$. La condition (5.4-(iv)) entraîne $r \deg Q - 1 < 2m - \nu - r - 1$, d'où $\rho(Q) < 2m - \nu - r - 1$ et, avec (5.19) et (5.5), $\Delta < m$. On divise V en trois sommes partielles suivant les valeurs de $v_Q(D)$: $V = V_1 + V_2 + V_3$, avec

$$(5.20) \quad V_1 = V_1(R, S, L) = \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ v_Q(D) < \Delta}} \langle D \rangle^{1/2} W(L, D),$$

$$(5.21) \quad V_2 = V_2(R, S, L) = \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ \Delta \leq v_Q(D) < m}} \langle D \rangle^{1/2} W(L, D),$$

$$(5.22) \quad V_3 = V_3(R, S, L) = \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ v_Q(D) \geq m}} \langle D \rangle^{1/2} W(L, D).$$

On fixe momentanément les polynômes R, S et L et on majore ces trois sommes.

5.3. Majoration de V_1, V_2 et V_3 . — La majoration de V_1 est facile.

PROPOSITION 5.7. — Pour tout $(R, S) \in (\mathcal{C}_{Q^r})^2$ et $L \in \mathcal{C}_{Q^\ell}$ on a

$$(5.23) \quad V_1(R, S, L) \leq \Delta \tau(Q^\ell) \langle Q \rangle^{4(\ell-m)} \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} q^{(\Delta-1)/2}.$$

Démonstration. — On majore les sommes $W(L, D)$ intervenant dans V_1 en remplaçant la condition $(A, B, G, H) \in \mathcal{G}(L, D)$ par la condition moins restrictive $(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4$. Cela donne

$$V_1 \leq \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ v_Q(D) < \Delta}} \langle D \rangle^{1/2} \sum_{(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4} |F_{m, \ell}(A) F_{m, \ell}(B) F_{m, \ell}(G) F_{m, \ell}(H)|,$$

d'où, avec la proposition 4.6,

$$V_1 \leq \langle Q \rangle^{4(\ell-m)} \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ v_Q(D) < \Delta}} \langle D \rangle^{1/2}.$$

On applique alors la proposition 2.3 avec $m = \theta = 0$ et $n = \Delta - 1$ et il vient

$$\sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ \omega_Q(D) < \Delta}} \langle D \rangle^{1/2} \leq \Delta \tau(Q^\ell) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} \max(1, q^{(\Delta-1)/2}). \quad \square$$

Les majorations de V_2 et V_3 demandent quelques notations supplémentaires.

D'après (5.15), si D est un polynôme unitaire divisant Q^ℓ tel que $\mathcal{G}(L, D) = \emptyset$, $W(L, D) = 0$ et n'intervient pas dans les sommes V_i . On n'a donc à considérer que les polynômes D pour lesquels $\mathcal{G}(L, D) \neq \emptyset$. Pour tout polynôme unitaire D divisant Q^ℓ , on pose

$$(5.24) \quad \tilde{D} = (D, R).$$

Les facteurs irréductibles de \tilde{D} sont facteurs irréductibles de Q . Soit P l'un de ces facteurs. Alors $P^{v_P(\tilde{D})}$ divise (D, R) , donc divise R . On a donc $v_P(\tilde{D}) \deg P \leq \deg R < r \deg Q$, ou encore avec (5.18), $v_P(\tilde{D}) \leq \rho$. Par suite,

$$(5.25) \quad \tilde{D} = \prod_{\substack{P \in \mathbf{I} \\ P|D}} P^{v_P(\tilde{D})} \quad | \quad \prod_{\substack{P \in \mathbf{I} \\ P|Q}} P^\rho \quad | \quad Q^\rho.$$

Avec (5.4-(ii)) et (5.4-(iv)) on a $\rho < m$, d'où $\tilde{D}|Q^m$. D'après (5.16), si $(A, B, G, H) \in \mathcal{G}(L, D)$, alors $D|Q^\ell$ et $L + 2R(A + B) + 2SQ^m(A + G) \equiv 0 \pmod{D}$, d'où, avec (5.24), $L + 2SQ^m(A + G) \equiv 0 \pmod{\tilde{D}}$, ce qui implique que \tilde{D} divise L . Les polynômes D tels que $\mathcal{G}(L, D) \neq \emptyset$ sont tels que \tilde{D} divise L . Quand cette condition est réalisée, on pose

$$(5.26) \quad 2R = R'\tilde{D}, \quad 2SQ^\rho = S'\tilde{D}, \quad L = L'\tilde{D}, \quad D = D'\tilde{D}.$$

La deuxième des conditions (5.16) s'écrit alors

$$L'\tilde{D} + R'\tilde{D}(A + B) + S'\tilde{D}(A + G) \equiv 0 \pmod{D'\tilde{D}},$$

d'où

$$(5.27) \quad L' + R'(A + B) + S'Q^{m-\rho}(A + G) \equiv 0 \pmod{D'}.$$

Les polynômes R' et D' sont premiers entre eux. Soit $R'' \in \mathcal{C}_{D'}$, inverse de R' modulo D' . Posons

$$(5.28) \quad L'' = R''L', \quad S'' = R''S' = \frac{2R''SQ^\rho}{(D, R)}.$$

La condition (5.27) devient

$$(5.29) \quad L'' + A + B + S''Q^{m-\rho}(A + G) \equiv 0 \pmod{D'}.$$

On peut maintenant majorer V_2 et V_3 :

PROPOSITION 5.8. — Pour tout $(R, S) \in (\mathcal{C}_{Q^\ell})^2$ et $L \in \mathcal{C}_{Q^\ell}$, on a

$$V_2(R, S, L) \leq (m - \Delta)\tau(Q^{\ell-\Delta}) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} q^{(m-1)/2}.$$

Démonstration. — Soit $D \in \mathbf{M}$ divisant Q^ℓ et tel que $\Delta \leq v_Q(D) < m$. Nous supposerons que \tilde{D} divise L . Soit $\delta = v_Q(D)$. D'après (5.19), on a

$$v_Q(D' \tilde{D}) = v_Q(D) \geq \Delta = \ell - m + \rho,$$

et d'après (5.25), $v_Q(\tilde{D}) \leq \rho$. Donc $v_Q(D') \geq \delta - \rho \geq \ell - m$. On majore la somme $W(L, D)$ en remplaçant les conditions (5.16) par les conditions moins restrictives

$$A + B + G + H \equiv 0 \pmod{Q^{\delta-\rho}}; \quad L'' + A + B \equiv 0 \pmod{Q^{\delta-\rho}}$$

impliquées par (5.16-(i)) et (5.29). On obtient avec (5.21) et (5.15)

$$\begin{aligned} V_2 &\leq \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ \Delta \leq v_Q(D) < m}} \langle D \rangle^{1/2} \\ &\times \sum_{\substack{(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4 \\ A+B+G+H \equiv 0 \pmod{Q^{\delta-\rho}} \\ A+B \equiv -L'' \pmod{Q^{\delta-\rho}}}} |F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell} - (G)F_{m,\ell}(H)|, \end{aligned}$$

d'où

$$\begin{aligned} V_2 &\leq \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ \Delta \leq v_Q(D) < m}} \langle D \rangle^{1/2} \sum_{\substack{(A, B) \in (\mathcal{C}_{Q^\ell})^2 \\ A+B \equiv -L'' \pmod{Q^{\delta-\rho}}}} |F_{m,\ell}(A)F_{m,\ell}(-B)| \\ &\times \sum_{\substack{(G, H) \in (\mathcal{C}_{Q^\ell})^2 \\ G+H \equiv L'' \pmod{Q^{\delta-\rho}}}} |F_{m,\ell}(-G)F_{m,\ell}(H)|. \end{aligned}$$

Comme $\ell - m \leq \delta - \rho$, on peut appliquer la proposition 4.9 aux deux dernières sommes. On obtient

$$V_2 \leq \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ \Delta \leq v_Q(D) < m}} \langle D \rangle^{1/2},$$

d'où, avec la proposition 2.3,

$$V_2 \leq (m - \Delta)\tau(Q^{\ell-\Delta}) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} \max(q^{\Delta/2}, q^{(m-1)/2}). \quad \square$$

Pour majorer V_3 , on majore d'abord les $W(L, D)$ intervenant dans V_3 .

PROPOSITION 5.9. — Soit D un diviseur unitaire de Q^ℓ tel que \tilde{D} divise L et tel que $\delta = v_Q(D) \geq m$. Alors, on a

$$W(L, D) \leq \begin{cases} \langle Q \rangle^{-2C(Q, f, \alpha)(\delta - m - 2\rho(Q))} & \text{si } \delta - m - 2\rho(Q) > 0, \\ 1 & \text{sinon.} \end{cases}$$

Démonstration. — Soit $(A, B, G, H) \in \mathcal{G}(L, D)$. Avec (5.29) on a

$$L'' + A + B + S''Q^{m-\rho}(A + G) \equiv 0 \pmod{D'}$$

et avec (5.16-(i)) on a

$$A + B + G + H \equiv 0 \pmod{D}.$$

Comme $v_Q(D') \geq \delta - \rho$, on en déduit

$$\begin{cases} L'' + A + B + S''Q^{m-\rho}(A + G) \equiv 0 \pmod{Q^{\delta-\rho}} \\ A + B + G + H \equiv 0 \pmod{Q^{\delta-\rho}}, \end{cases}$$

système équivalent au système (\mathcal{E}) suivant

$$\begin{cases} L'' + A + B + S''Q^{m-\rho}(A + G) \equiv 0 \pmod{Q^{\delta-\rho}} \\ G + H - S''Q^{m-\rho}(A + G) - L'' \equiv 0 \pmod{Q^{\delta-\rho}}. \end{cases}$$

On majore $W = W(L, D)$ en remplaçant la condition $(A, B, G, H) \in \mathcal{G}(L, D)$ par la condition moins restrictive $(A, B, G, H) \in (\mathcal{C}_{Q^\ell})^4$ et vérifie (\mathcal{E}) . On obtient

$$\begin{aligned} W \leq \sum_{(A, G) \in (\mathcal{C}_{Q^\ell})^2} & |F_{m, \ell}(A)F_{m, \ell}(-G)| \sum_{\substack{B \in \mathcal{C}_{Q^\ell} \\ -B \equiv L'' + A + S''Q^{m-\rho}(A + G) \pmod{Q^{\delta-\rho}}}} & |F_{m, \ell}(-B)| \\ & \times \sum_{\substack{H \in \mathcal{C}_{Q^\ell} \\ H \equiv L'' - G + S''Q^{m-\rho}(A + G) \pmod{Q^{\delta-\rho}}}} & |F_{m, \ell}(H)|. \end{aligned}$$

Avec (5.4-(iv)), (5.5) et (5.18), on a $\delta - \rho \geq m - \rho \geq \ell - m$. En appliquant la proposition 4.7 aux deux dernières sommes on obtient que la somme

$$\sum_{\substack{B \in \mathcal{C}_{Q^\ell} \\ -B \equiv L'' + A + S''Q^{m-\rho}(A + G) \pmod{Q^{\delta-\rho}}}} |F_{m, \ell}(-B)|$$

vaut $|F_{\ell-m}(L'' + A + S''Q^{m-\rho}(A + G))|$ si $v_\infty(\{\frac{L'' + A + S''Q^{m-\rho}(A + G)}{Q^{\delta-\rho}}\}) > (m + \delta - \rho - \ell) \deg Q$ et 0 sinon ainsi que la majoration

$$\sum_{\substack{H \in \mathcal{C}_{Q^\ell} \\ H \equiv L'' - G + S''Q^{m-\rho}(A + G) \pmod{Q^{\delta-\rho}}}} |F_{m, \ell}(H)| \leq |F_{\ell-m}(L'' - G + S''Q^{m-\rho}(A + G))|.$$

On définit le sous ensemble \mathcal{H} de $(\mathcal{C}_{Q^\ell})^2$ par la condition

$$(A, G) \in \mathcal{H} \Leftrightarrow v_\infty\left(\left\{\frac{L'' + A + S''Q^{m-\rho}(A+G)}{Q^{\delta-\rho}}\right\}\right) > (m + \delta - \rho - \ell) \deg Q.$$

Alors,

$$W \leq \sum_{(A, G) \in \mathcal{H}} |F_{m, \ell}(A)F_{m, \ell}(-G)|$$

$$\times |F_{\ell-m}(L'' + A + S''Q^{m-\rho}(A+G))| |F_{\ell-m}(L'' - G + S''Q^{m-\rho}(A+G))|.$$

Fixons $A \in \mathcal{C}_{Q^\ell}$ et montrons que les $G \in \mathcal{C}_{Q^\ell}$ tels que $(A, G) \in \mathcal{H}$ sont dans une même classe de congruence modulo $Q^{\delta-m-2\rho}$. En effet, supposons que $(A, G) \in \mathcal{H}$ et $(A, G') \in \mathcal{H}$. Alors on a

$$v_\infty\left(\left\{\frac{S''(G - G')}{Q^{\delta-m}}\right\}\right) > (m + \delta - \rho - \ell) \deg Q.$$

Avec (5.4-(iv)) on a $2m > r(\deg Q + 1) + \nu$, d'où $m + \delta - \rho - \ell > \delta - m$. Par suite $S''(G - G') \equiv 0 \pmod{Q^{\delta-m}}$ d'où, avec (5.28), $\frac{R''SQ^\rho}{(D, R)}(G - G') \equiv 0 \pmod{Q^{\delta-m}}$. Le polynôme R'' étant l'inverse de R' modulo D' , il est donc premier à tout diviseur de D' . En particulier, il est premier à Q et donc inversible modulo $Q^{\delta-m}$, d'où $SQ^\rho(G - G') \equiv 0 \pmod{Q^{\delta-m}}$. Par ailleurs, si P est un facteur irréductible de (S, Q) , on $v_P(S) \deg P \leq \deg S < r \deg Q$, d'où avec (5.18), $v_P(S) \leq \rho$. On a donc $\prod_{P \mid (S, Q)} P^{v_P(S)} \mid Q^\rho$, d'où

$$Q^{2\rho}(G - G') \equiv 0 \pmod{Q^{\delta-m}} \text{ et } G' \equiv G \pmod{Q^{\delta-m-2\rho}}.$$

Pour tout $A \in \mathcal{C}_{Q^\ell}$, notons $G_0(A)$ l'élément de $\mathcal{C}_{Q^{\delta-m-2\rho}}$ tel que pour tout $G \in \mathcal{C}_{Q^\ell}$ on a

$$(A, G) \in \mathcal{H} \Rightarrow G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}.$$

On majore $W = W(L, D)$ en remplaçant la condition $(A, H) \in \mathcal{H}$ par la condition $G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}$. On obtient

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} \sum_{\substack{G \in \mathcal{C}_{Q^\ell} \\ G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}}} |F_{m, \ell}(A)|$$

$$\times |F_{\ell-m}(L'' + A + S''Q^{m-\rho}(A+G))| |F_{m, \ell}(-G)| |F_{\ell-m}(L'' - G + S''Q^{m-\rho}(A+G))|$$

Avec (5.4-(iv)) on a $m - \rho > \ell - m$ et la proposition 4.1-(vi) nous donne

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} \sum_{\substack{G \in \mathcal{C}_{Q^\ell} \\ G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}}} |F_{m, \ell}(A)F_{\ell-m}(L'' + A)| |F_{m, \ell}(-G)| |F_{\ell-m}(L'' - G)|,$$

soit

$$\begin{aligned} W &\leq \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L'' + A)| \\ &\quad \times \sum_{\substack{G \in \mathcal{C}_{Q^\ell} \\ G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}}} |F_{m,\ell}(-G)F_{\ell-m}(L'' - G)|. \end{aligned}$$

(I) Supposons d'abord que $\gamma = \delta - m - 2\rho > 0$. On a alors $\gamma < \ell - m$ et $m < \ell$. On applique la proposition 4.8 à la somme intérieure et on obtient

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L'' + A)| |F_\gamma(-G_0(A))F_\gamma(L'' - G_0(A))|.$$

La proposition 4.3 donne alors

$$W \leq \langle Q \rangle^{-2C\gamma} \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L'' + A)|$$

où $C = C(Q, f, \alpha)$ et les propositions 4.8 et 4.2 nous donnent

$$W \leq \langle Q \rangle^{-2C\gamma} |F_0(0)F_0(L'')| = \langle Q \rangle^{-2C\gamma}.$$

(II) Supposons maintenant que $\gamma = \delta - m - 2\rho \leq 0$. Dans ce cas, la condition de congruence dans la somme majorant W n'apportant aucune restriction, on majore W trivialement et on obtient

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L'' + A)| \sum_{G \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(-G)F_{\ell-m}(L'' - G)|$$

et la proposition 4.8 nous donne $W \leq 1$. □

PROPOSITION 5.10. — Pour tout $(R, S) \in (\mathcal{C}_{Q^r})^2$ et $L \in \mathcal{C}_{Q^\ell}$, on a

$$(5.30) \quad V_3(R, S, L) \leq (\ell - m + 1) \tau(Q^{\ell-m}) \langle Q \rangle^{\ell/2} \langle Q \rangle^{-C'(Q, f, \alpha)(\ell - m - 2\rho(Q))},$$

avec

$$(5.31) \quad C'(Q, f, \alpha) = \min(2C(Q, f, \alpha), \frac{1}{2 \deg Q}).$$

Démonstration. — Observons d'abord que la condition (5.4-(iii)) entraîne la relation $m + 2\rho < \ell$. D'après (5.22) et la proposition 5.9, on a

$$V_3 \leq \sum_{\substack{D \in \mathbf{M} \\ D \mid Q^\ell \\ m \leq v_Q(D) \leq m + 2\rho}} \langle D \rangle^{1/2} + \sum_{\substack{D \in \mathbf{M} \\ D \mid Q^\ell \\ m + 2\rho < v_Q(D)}} \langle D \rangle^{1/2} \langle Q \rangle^{2(m + 2\rho - v_Q(D))C},$$

où l'on a posé $C = C(Q, f, \alpha)$. Comme $\tau(Q^{\ell-m-2\rho-1}) \leq \tau(Q^{\ell-m})$, la proposition 2.3 donne

$$V_3 \leq \tau(Q^{\ell-m}) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} \left((2\rho+1)q^{\rho+m/2} + (\ell-m-2\rho)\langle Q \rangle^{2(m+2\rho)C} \right. \\ \left. \times \max \left((\langle Q \rangle^{-2C\|\alpha\|^2} q^{1/2})^{m+2\rho+1}, (\langle Q \rangle^{-2C\|\alpha\|^2} q^{1/2})^\ell \right) \right).$$

Si $\langle Q \rangle^{-2C} q^{1/2} < 1$, on a

$$V_3 \leq \tau(Q^{\ell-m}) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} \left((2\rho+1)q^{\rho+m/2} + (\ell-m-2\rho)q^{(m+1+2\rho)/2} \langle Q \rangle^{-2C} \right),$$

d'où

$$V_3 \leq \tau(Q^{\ell-m}) \langle Q \rangle^{\ell/2} (\ell-m+1) q^{\rho+m/2-\ell/2}.$$

Si $\langle Q \rangle^{-2C} q^{1/2} \geq 1$, on a

$$V_3 \leq \tau(Q^{\ell-m}) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} \left((2\rho+1)q^{\rho+m/2} + (\ell-m-2\rho)q^{\ell/2} \langle Q \rangle^{2(m+2\rho-\ell)C} \right), \\ \leq \tau(Q^{\ell-m}) \langle Q \rangle^{\ell/2} \left((2\rho+1)q^{\rho+\frac{m-\ell}{2}} + (\ell-m-2\rho) \langle Q \rangle^{-2C(\ell-m-2\rho)} \right).$$

Si on pose $C' = C'(Q, f, \alpha)$, on a

$$V_3 \leq \tau(Q^{\ell-m}) \langle Q \rangle^{\ell/2} (\ell-m+1) \langle Q \rangle^{-C'(\ell-m-2\rho)}.$$

□

PROPOSITION 5.11. — *On a*

$$(5.32) \quad V(R, S, L) \leq m\tau(Q^\ell) \langle Q \rangle^{\ell/2} \left(q^{-1} \langle Q \rangle^{4\nu+9r/2-(4+1/2 \deg Q)m+4} \right. \\ \left. + q^{-1-r/2} \langle Q \rangle^{-(\nu-m)/2 \deg Q} + \langle Q \rangle^{-C'(Q, f, \alpha)(\ell-m-2\rho)} \right).$$

Démonstration. — La proposition 5.7 nous donne

$$V_1 \leq \Delta \tau(Q^\ell) \langle Q \rangle^{4(\ell-m)} \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} q^{(\Delta-1)/2},$$

d'où, avec (5.19), (5.18), (5.4) et (5.5),

$$V_1 \leq m\tau(Q^\ell) \langle Q \rangle^{\ell/2} \langle Q \rangle^{4(\nu+r+1-m)+r/2} q^{-1-m/2}, \\ \leq \frac{m}{q} \tau(Q^\ell) \langle Q \rangle^{\ell/2} \langle Q \rangle^{4\nu+9r/2-m(4+1/2 \deg Q)+4}.$$

La proposition 5.8 nous donne

$$V_2 \leq m\tau(Q^{\ell-\Delta}) \left(\frac{\langle Q \rangle}{q} \right)^{\ell/2} q^{(m-1)/2},$$

d'où, avec (5.5),

$$V_2 \leq \frac{m}{q} \tau(Q^\ell) \langle Q \rangle^{\ell/2} q^{-r/2} \langle Q \rangle^{-(\nu-m)/2 \deg Q}.$$

D'après la proposition 5.10, on a

$$V_3 \leq (\ell - m + 1) \tau(Q^{\ell-m}) \langle Q \rangle^{\ell/2} \langle Q \rangle^{-C'(Q, f, \alpha)(\ell-m-2\rho)},$$

d'où, avec (5.18), (5.4) et (5.5),

$$V_3 \leq m \tau(Q^\ell) \langle Q \rangle^{\ell/2} \langle Q \rangle^{-C'(Q, f, \alpha)(\ell-m-2\rho)}.$$

Les majorations de V_1 , V_2 , V_3 jointes aux relations (5.17), (5.20), (5.21), (5.22), nous donnent

$$\begin{aligned} V \leq m \tau(Q^\ell) \langle Q \rangle^{\ell/2} & \left(q^{-1} \langle Q \rangle^{4\nu+9r/2-m(4+1/2 \deg Q)+4} \right. \\ & \left. + q^{-1-r/2} \langle Q \rangle^{-(\nu-m)/2 \deg Q} + \langle Q \rangle^{-C'(Q, f, \alpha)(\ell-m-2\rho)} \right). \quad \square \end{aligned}$$

5.4. Fin de la majoration. — On est maintenant en mesure de démontrer la proposition suivante :

PROPOSITION 5.12. — *On suppose $\alpha \in \mathbb{R} \setminus \mathbb{Z}$ et on pose*

$$(5.33) \quad \eta(Q) = \left(\frac{4q^{99/100} \exp(\frac{1}{48 \deg Q})(1 - \frac{1}{q})(1 + \frac{2}{q}) \tau(Q) \langle Q \rangle^5}{(\deg Q)^{\omega(Q)+1}} \right)^{1/4}$$

et

$$(5.34) \quad \xi(Q, f, \alpha) = \frac{11}{15} \min \left(\frac{1}{48(\deg Q)^2 + 11 \deg Q - 1}, \frac{1}{16(\deg Q)^2 + 7 \deg Q + \frac{1+8 \deg Q}{C(Q, f, \alpha)} - 1} \right),$$

où $C(Q, f, \alpha)$ est définie par (4.5). Alors, pour $\nu(N) > 100/\xi(Q, f, \alpha)$, on a

$$(5.35) \quad |\Sigma(N)| \leq \eta(Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1 - \frac{99}{400} \xi(Q, f, \alpha))}.$$

Démonstration. — On pose $C' = C'(Q, f, \alpha)$ défini par (5.31). On va imposer des conditions supplémentaires aux paramètres r et m afin que les conditions suivantes soient réalisées :

$$(5.36) \quad \begin{cases} (4\nu + 13r/2) - m(4 + 1/2 \deg Q) \leq 0, \\ (m - \nu - r)/2 \deg Q + 2r - 4 \leq 0, \\ C'(m - \nu - r - 3) + 2r(1 + C' \deg Q) - 4 \leq 0. \end{cases}$$

Ces conditions réalisées, on déduit des relations (5.14), (5.17) et (5.32) que pour $R \in \mathcal{C}_Q$ et $S \in \mathcal{C}_{Q^r}$,

$$\begin{aligned} U = U(N, r, m, R, S) \leq 2(1 - \frac{1}{q}) m \tau(Q^\ell) \langle Q \rangle^\ell & \left(q^{-1} \langle Q \rangle^{4\nu+9r/2-(4+1/2 \deg Q)m+4} \right. \\ & \left. + q^{-1-r/2} \langle Q \rangle^{-(\nu-m)/2 \deg Q} + \langle Q \rangle^{-C'(\ell-m-2\rho)} \right), \end{aligned}$$

d'où, avec (5.5), (5.18) et (5.36),

$$(5.37) \quad U \leq 2\left(1 - \frac{1}{q}\right)\left(\frac{2}{q} + 1\right)m\tau(Q^\ell)\langle Q \rangle^{\nu-r+5}.$$

Compte tenu de (5.31), les conditions (5.36) sont réalisées dès que les conditions

$$(5.38) \quad \begin{cases} (8\nu + 13r) \deg Q \leq m(8 \deg Q + 1), \\ m \leq \nu + r - \frac{2r}{C'} - 2r \deg Q + 8 \deg Q \end{cases}$$

le sont.

On se donne un paramètre $\xi \in]0, 1]$ et on impose

$$(5.39) \quad 1 < r \leq \xi\nu.$$

Les conditions (5.38) sont satisfaites si

$$\nu \left(\frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8 \deg Q}} \right) \leq m \leq \nu(1 + \xi - \frac{2\xi}{C'} - 2\xi \deg Q).$$

On exigera donc que ξ vérifie la condition

$$(5.40) \quad \frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8 \deg Q}} \leq 1 + \xi - 2\xi \deg Q - \frac{2\xi}{C'}$$

et que l'intervalle

$$J_{\xi, \nu} = [\nu \frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8 \deg Q}}, \nu(1 + \xi - 2\xi \deg Q - \frac{2\xi}{C'})]$$

contienne des nombres entiers m tels que $r \leq \xi\nu$ et m vérifient les conditions (5.4). On prend

$$(5.41) \quad \xi = \xi(Q, f, \alpha) = \frac{\frac{11}{15}}{16(\deg Q)^2 + 7 \deg Q + \frac{2+16 \deg Q}{C'} - 1}.$$

et la condition (5.40) est vérifiée. Observons que, $C' = C'(Q, f, \alpha)$ étant défini par (5.31), $\xi(Q, f, \alpha)$ vérifie (5.34). On suppose que N est assez grand pour que $\nu = \nu(N) > 100/\xi$. Alors on a $\nu > 30 \deg Q$ et

$$(5.42) \quad \nu \geq \frac{1}{1 + \xi - 2\xi \deg Q - \frac{2\xi}{C'} - \frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8 \deg Q}}}.$$

L'intervalle $J_{\xi, \nu}$ contient alors des nombres entiers. Si $r \leq \xi\nu$, alors $\frac{1-3/\nu}{5 \deg Q-1} > \frac{1-1/10 \deg Q}{5 \deg Q-1} > \xi$, d'où $r \leq \xi\nu < \frac{\nu-3}{5 \deg Q-1}$, ce qui est la relation (5.4-(i)). Soit un nombre entier $m \in J_{\xi, \nu}$. Alors

$$m \leq \nu(1 + \xi - 2\xi \deg Q - 2\xi/C') \leq \nu(1 + \xi - 6\xi \deg Q),$$

d'où, d'une part $m \leq \nu(1 - 5\xi) < \nu - r$ et d'autre part,

$$m \leq \nu(1 + \xi(1 - 2 \deg Q)) \leq \nu + r(1 - 2 \deg Q) < \nu + r(1 - 2 \deg Q) + 3.$$

Les relations (5.4-(ii)) et (5.4-(iii)) sont vérifiées. Avec (5.41), on a

$$\xi < \frac{1 - 1/8 \deg Q}{(1 + \deg Q)(1 + 1/8 \deg Q)},$$

d'où

$$2m > \nu(1 + \xi(1 + \deg Q)) \geq \nu + r(1 + \deg Q)$$

et (5.4)-(iv) est vérifiée. Par suite, (5.37) est vérifiée. Majorons $\tau(Q^\ell)$. On a

$$\tau(Q^\ell) = \prod_{\substack{P \in \mathbf{I} \\ P|Q}} (\ell v_P(Q) + 1) \leq \prod_{\substack{P \in \mathbf{I} \\ P|Q}} (\ell v_P(Q) + \ell) = \ell^{\omega(Q)} \tau(Q).$$

Avec (5.5) puis (5.39), on a $\ell^{\omega(Q)} = (\nu + r + 1)^{\omega(Q)} \leq \nu^{\omega(Q)}(1 + \xi + \frac{1}{\nu})^{\omega(Q)}$. Comme $\nu = \nu(N) \geq 100/\xi$, on a

$$\begin{aligned} \ell^{\omega(Q)} &\leq \nu^{\omega(Q)}(1 + 2\xi)^{\omega(Q)} \\ &= \nu^{\omega(Q)} \exp(\omega(Q) \log(1 + \frac{101}{100}\xi)) \leq \nu^{\omega(Q)} \exp(\frac{101}{100}\xi \deg Q). \end{aligned}$$

Avec (5.41) et (5.31), on a $\ell^{\omega(Q)} \leq \nu^{\omega(Q)} \exp(\frac{1}{48 \deg Q})$, d'où

$$(5.43) \quad \tau(Q^\ell) \leq \exp(\frac{1}{48 \deg Q}) \tau(Q) \nu^{\omega(Q)}.$$

Avec (5.4) on a $m \leq \nu + r - 6r \deg Q + 8 \deg Q \leq \nu + r < 2\nu$, d'où, avec (5.37), (5.42) et (5.43),

$$U \leq \kappa(Q) \tau(Q) \nu^{\omega(Q)+1} \langle Q \rangle^{\nu-r+5},$$

où $\kappa(Q) = 4 \exp(\frac{1}{48 \deg Q})(1 - \frac{1}{q})(1 + \frac{2}{q})$. La proposition 5.3 nous donne

$$T(N, R, S)^2 \leq \kappa(Q) \tau(Q) q^N \nu^{\omega(Q)+1} \langle Q \rangle^{\nu-r+5},$$

puis, la proposition 5.2 nous donne

$$|\Sigma(N)|^4 \leq \kappa(Q) \tau(Q) q^{3N} \nu^{\omega(Q)+1} \langle Q \rangle^{\nu-r+5},$$

d'où, en majorant ν par $N/\deg Q$,

$$|\Sigma(N)| \leq (\kappa(Q) \tau(Q) \langle Q \rangle^5)^{1/4} \left(\frac{N}{\deg Q} \right)^{\frac{\omega(Q)+1}{4}} q^N \langle Q \rangle^{-r/4}.$$

L'intervalle $[\frac{99}{100}\xi\nu, \xi\nu]$ contient des nombres entiers. On prend r dans cet intervalle et on obtient la majoration

$$|\Sigma(N)| \leq (\kappa(Q) \tau(Q) \langle Q \rangle^5)^{1/4} \left(\frac{N}{\deg Q} \right)^{\frac{\omega(Q)+1}{4}} q^{N(1 - \frac{99}{400}\xi) + \frac{99}{400}}. \quad \square$$

6. Démonstration du théorème 1.2

PROPOSITION 6.1. — *Si N est un nombre entier, $N > 100 \deg Q/\xi(Q, f, \alpha)$, alors on a*

$$\left| \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e(\alpha f(X^2)) \right| \leq \eta(Q) \left(1 + \frac{\langle Q \rangle^{1-99\xi/400}}{\langle Q \rangle^{1-99\xi/400} - 1} \right) N^{\frac{\omega(Q)+1}{4}} q^{N(1-99\xi/400)} + \langle Q \rangle^{[100/\xi]} - \eta(Q) N^{\frac{\omega(Q)+1}{4}} \frac{\langle Q \rangle^{([100/\xi]+1)(1-99\xi/400)}}{\langle Q \rangle^{1-99\xi/400} - 1},$$

où $\xi = \xi(Q, f, \alpha)$.

Démonstration. — Posons $\mathfrak{S}(N) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e(\alpha f(X^2))$. Avec (5.1), (5.2) et

(5.3), on a $\mathfrak{S}(N) = 1 + \sum_{j=1}^{\nu(N)} \Sigma(j \deg Q) + \Sigma(N)$ et la proposition 5.12 nous donne

$$|\mathfrak{S}(N)| \leq 1 + \sum_{j=1}^{[100/\xi]} |\Sigma(j \deg Q)| + \eta(Q) \left(\sum_{j=1+[100/\xi]}^{\nu(N)} (j \deg Q)^{\frac{\omega(Q)+1}{4}} q^{j \deg Q (1-99\xi/400)} + N^{\frac{\omega(Q)+1}{4}} q^{N(1-99\xi/400)} \right).$$

On majore la première somme en majorant trivialement $|\Sigma(j \deg Q)|$ par $q^{j \deg Q} - q^{(j-1) \deg Q}$ et la deuxième somme en majorant $(j \deg Q)^{\frac{\omega(Q)+1}{4}}$ par $N^{\frac{\omega(Q)+1}{4}}$. On obtient

$$|\mathfrak{S}(N)| \leq \langle Q \rangle^{[100/\xi]} + \eta(Q) N^{\frac{\omega(Q)+1}{4}} \left(\sum_{j=1+[100/\xi]}^{\nu(N)} \langle Q \rangle^{j(1-99\xi/400)} + q^{N(1-99\xi/400)} \right),$$

d'où

$$|\mathfrak{S}(N)| \leq \langle Q \rangle^{[100/\xi]} + \eta(Q) N^{\frac{\omega(Q)+1}{4}} \left(\frac{\langle Q \rangle^{(\nu(N)+1)(1-99\xi/400)} - \langle Q \rangle^{(1+[100/\xi])(1-99\xi/400)}}{\langle Q \rangle^{(1-99\xi/400)} - 1} + q^{N(1-99\xi/400)} \right).$$

Avec (5.2), on obtient

$$|\mathfrak{S}(N)| \leq \langle Q \rangle^{[100/\xi]} + \eta(Q) \left(1 + \frac{\langle Q \rangle^{1-99\xi/400}}{\langle Q \rangle^{1-99\xi/400} - 1} \right) N^{\frac{\omega(Q)+1}{4}} q^{N(1-99\xi/400)} - \eta(Q) N^{\frac{\omega(Q)+1}{4}} \frac{\langle Q \rangle^{([100/\xi]+1)(1-99\xi/400)}}{\langle Q \rangle^{1-99\xi/400} - 1}. \quad \square$$

COROLLAIRE 6.2. — Soit α un nombre réel non entier. Alors il existe un nombre entier $N(Q, f, \alpha)$ tel que pour tout nombre entier $N \geq N(Q, f, \alpha)$ on a

$$\left| \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e(\alpha f(X^2)) \right| \leq \beta(Q, f, \alpha) N^{\frac{\omega(Q)+1}{4}} q^{N(1-99\xi/400)},$$

où $\xi = \xi(Q, f, \alpha)$ et

$$(6.1) \quad \beta(Q, f, \alpha) = \eta(Q) \left(1 + \frac{\langle Q \rangle^{1-99\xi/400}}{\langle Q \rangle^{1-99\xi/400} - 1} \right).$$

Démonstration. — Pour $N \geq n(Q, \xi) = n(Q, \xi(Q, f, \alpha))$, on a

$$\eta(Q) N^{\frac{\omega(Q)+1}{4}} \frac{\langle Q \rangle^{([100/\xi]+1)(1-99\xi/400)}}{\langle Q \rangle^{1-99\xi/400} - 1} > \langle Q \rangle^{[100/\xi]}.$$

On prend $N(Q, f, \alpha) = \max(n(Q, \xi(Q, f, \alpha)), 1 + 100 \deg Q / \xi(Q, f, \alpha))$. \square

Preuve du théorème 1.2. — Nous pouvons maintenant démontrer le théorème 1.2 avec

$$(6.2) \quad a(Q, f, \alpha) = \frac{363}{2000} \min\left(\frac{1}{48(\deg Q)^2 + 11 \deg Q - 1}, \frac{C(Q, f, \alpha)}{C(Q, f, \alpha)(16(\deg Q)^2 + 7 \deg Q - 1) + 1 + 8 \deg Q}\right)$$

et

$$(6.3) \quad b(Q) = \eta(Q) \left(1 + \frac{\langle Q \rangle^{1-363/2000(48(\deg Q)^2+11 \deg Q-1)}}{\langle Q \rangle^{1-99/400(48(\deg Q)^2+11 \deg Q-1)} - 1} \right).$$

Posons $a = a(Q, f, \alpha)$ et minorons d'abord $\xi = C(Q, f, \alpha)$. On a

$$\frac{1}{48(\deg Q)^2 + 11 \deg Q - 1} \geq \frac{2000}{363} a$$

ainsi que

$$\frac{1}{16(\deg Q)^2 + 7 \deg Q + \frac{1+8 \deg Q}{C(Q, f, \alpha)-1}} \geq \frac{2000}{363} a.$$

D'après (5.34), on a $\xi(Q, f, \alpha) \geq \frac{2000}{363} a$, d'où $1 - 99\xi/400 \leq 1 - a$. D'autre part, la fonction $t \rightarrow \frac{\langle Q \rangle^t}{\langle Q \rangle^t - 1}$ étant décroissante sur l'ensemble des nombres réels, on a avec (5.34)

$$\frac{\langle Q \rangle^{1-99\xi/400}}{\langle Q \rangle^{1-99\xi/400} - 1} \leq \frac{\langle Q \rangle^{1-363/2000(48(\deg Q)^2+11 \deg Q-1)}}{\langle Q \rangle^{1-363/2000(48(\deg Q)^2+11 \deg Q-1)} - 1},$$

d'où, avec (6.1)

$$\beta(Q, f, \alpha) \leq \eta(Q) \left(1 + \frac{\langle Q \rangle^{1-363/2000(48(\deg Q)^2+7\deg Q-1)}}{\langle Q \rangle^{1-363/2000(48(\deg Q)^2+7\deg Q-1)} - 1} \right),$$

soit $\beta(Q, f, \alpha) \leq b(Q)$. D'après le corollaire 6.2, pour tout nombre entier $N \geq N(Q, f, \alpha)$, on a donc

$$\left| \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e(\alpha f(X^2)) \right| \leq b(Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1-a)}. \quad \square$$

Terminons cette section par la preuve du corollaire 1.3. Si m est un nombre entier strictement positif et $a \in \{0, 1, \dots, m-1\}$, on pose

$$\begin{aligned} z(m, a, N) &= \text{Card}\{X \in \mathbf{A} \mid \deg X < n, f(X^2) \equiv a \pmod{m}\} \\ &= \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} \frac{1}{m} \sum_{h=0}^{m-1} e\left(\frac{h(f(X^2) - a)}{m}\right). \end{aligned}$$

En inversant l'ordre des sommes on obtient

$$\begin{aligned} mz(m, a, N) &= \sum_{h=0}^{m-1} e\left(\frac{-ha}{m}\right) \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e\left(\frac{hf(X^2)}{m}\right) \\ &= q^N + \sum_{h=1}^{m-1} e\left(\frac{-ha}{m}\right) \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e\left(\frac{h}{m} f(X^2)\right). \end{aligned}$$

Le théorème 1.2 nous donne alors

$$\begin{aligned} |mz(m, a, N) - q^N| &\leq \sum_{h=1}^{m-1} b(Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1-a(Q, f, h/m))} \\ &\leq (m-1) b(Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1-\eta(Q, f, m))}, \end{aligned}$$

avec $\eta(Q, f, m) = \min_{1 \leq h \leq m-1} \{a(Q, f, h/m)\}$, d'où le résultat annoncé.

Remerciements. — Nous remercions vivement le rapporteur pour sa relecture très attentive et pour ses nombreuses suggestions.

BIBLIOGRAPHIE

- [1] N. L. BASSILY & I. KÁTAI – « Distribution of the values of q -additive functions on polynomial sequences », *Acta Math. Hungar.* **68** (1995), p. 353–361.
- [2] M. CAR – « Quadratic forms on $\mathbf{F}_q[T]$ », *J. Number Theory* **61** (1996), p. 145–180.
- [3] M. CAR & C. MAUDUIT – « Sur les puissances des polynômes sur un corps fini », *Unif. Distrib. Theory* **8** (2013), p. 171–182.
- [4] L. CARLITZ – « Diophantine approximation in fields of characteristic p », *Trans. Amer. Math. Soc.* **72** (1952), p. 187–208.
- [5] M. DRMOTA – « The joint distribution of q -additive functions », *Acta Arith.* **100** (2001), p. 17–39.
- [6] ———, « Subsequences of automatic sequences and uniform distribution », in *Uniform distribution and quasi-Monte Carlo methods*, Radon Ser. Comput. Appl. Math., vol. 15, De Gruyter, Berlin, 2014, p. 87–104.
- [7] M. DRMOTA & G. GUTENBRUNNER – « The joint distribution of Q -additive functions on polynomials over finite fields », *J. Théor. Nombres Bordeaux* **17** (2005), p. 125–150.
- [8] M. DRMOTA, C. MAUDUIT & J. RIVAT – « Primes with an average sum of digits », *Compos. Math.* **145** (2009), p. 271–292.
- [9] M. DRMOTA & J. F. MORGENBESSER – « Generalized Thue-Morse sequences of squares », *Israel J. Math.* **190** (2012), p. 157–193.
- [10] G. W. EFFINGER & D. R. HAYES – *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs, The Clarendon Press, Oxford Univ. Press, New York, 1991.
- [11] D. R. HAYES – « The expression of a polynomial as a sum of three irreducibles », *Acta Arith.* **11** (1966), p. 461–488.
- [12] D.-H. KIM – « On the joint distribution of q -additive functions in residue classes », *J. Number Theory* **74** (1999), p. 307–336.
- [13] R. LIDL & H. NIEDERREITER – *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company, Reading, MA, 1983.
- [14] M. G. MADRITSCH & J. M. THUSWALDNER – « Weyl sums in $\mathbf{F}_q[x]$ with digital restrictions », *Finite Fields Appl.* **14** (2008), p. 877–896.
- [15] B. MARTIN, C. MAUDUIT & J. RIVAT – « Théorème des nombres premiers pour les fonctions digitales », *Acta Arith.* **165** (2014), p. 11–45.
- [16] ———, « Fonctions digitales le long des nombres premiers », *Acta Arith.* **170** (2015), p. 175–197.
- [17] C. MAUDUIT & J. RIVAT – « La somme des chiffres des carrés », *Acta Math.* **203** (2009), p. 107–148.

- [18] _____, « Sur un problème de Gelfond : la somme des chiffres des nombres premiers », *Ann. of Math.* **171** (2010), p. 1591–1646.
- [19] _____, « Prime numbers along Rudin-Shapiro sequences », *J. Eur. Math. Soc. (JEMS)* **17** (2015), p. 2595–2642.
- [20] _____, « Rudin-Shapiro sequences along squares », prépublication.
- [21] G. RHIN – « Répartition modulo 1 dans un corps de séries formelles sur un corps fini », *Dissertationes Math. (Rozprawy Mat.)* **95** (1972).

