ACTA ARITHMETICA
LXV.3 (1993)

Sommes de cubes dans l'anneau $\mathbb{F}_{2^h}[X]$

par

Mireille Car (Marseille) et Jorgen Cherly (Brest)

Soit $\mathbb{F}_q$ le corps fini à q éléments. Le problème de Waring peut se poser dans l'anneau $\mathbb{F}_q[X]$. Sous sa forme la plus générale, il s'apparente à ce qui est appelé problème de Waring "facile" en arithmétique classique. Les résultats de L. N. Vaserstein (cf. [10], [11]) apportent une réponse à ce type de problème. Il est intéressant de poser le problème de Waring dans l'anneau $\mathbb{F}_q[X]$ avec les conditions de degré les plus restrictives possibles. On a alors un problème qui s'apparente au problème de Waring "difficile" de l'arithmétique classique. Pour le résoudre, on adapte à $\mathbb{F}_q[X]$ la méthode de Hardy et Littlewood, dite méthode du cercle. C'est ce qui a été fait dans [9] pour des exposants $k < p$, où p est la caractéristique du corps $\mathbb{F}_q$. Cette restriction provient du fait suivant. On majore des sommes de caractères par la méthode de Weyl. Celle-ci, basée sur des différentiations successives introduit le facteur $k!$ qui est nul et conduit donc à la majoration triviale pour $k \geq p$. J. Cherly (cf. [4], [5]) a pu s'affranchir de cette difficulté dans le cas de l'exposant 3 pour l'anneau $\mathbb{F}_2[X]$. Son point de départ est une remarque de R. C. Vaughan qui a montré, dans le problème de Waring classique, que l'on pouvait retrouver la majoration de Weyl des sommes trigonométriques cubiques sur les "arcs mineurs" en utilisant la formule sommatoire de Poisson qui traditionnellement n'était utilisée que dans le traitement des "arcs majeurs" (cf. [12]). L'utilisation de la formule sommatoire de Poisson est le seul point commun entre le travail de J. Cherly et la remarque de R. C. Vaughan, le problème posé par la caractéristique 2 étant trop crucial pour qu'une analogie entre les deux méthodes soit possible. Le premier pas ayant été fait, il était facile de généraliser le travail de J. Cherly à un anneau $\mathbb{F}_q[X]$, où q est une puissance de 2. L'utilisation d'une méthode légèrement différente et une étude plus fine de certaines sommes de Gauss ont permis d'obtenir une meilleure majoration des sommes de caractères (cf. [2]). Nous appliquons ici cette majoration à l'étude du problème de Waring pour les cubes dans l'anneau $\mathbb{F}_{2^h}[X]$.

Soit q une puissance de 2. Soit un entier $s \geq 1$. Suivant la terminologie introduite par G. Effinger et D. Hayes, cf. [6], on dira qu'un polynôme $M \in \mathbb{F}_q[X]$ admet une *représentation stricte en somme de s cubes* s'il existe dans $\mathbb{F}_q[X]$ des polynômes $M_1, \ldots, M_s$ vérifiant les conditions suivantes :

$$M = M_1^3 + \ldots + M_s^3\,, \tag{1}$$

$$\deg M_i \leq n \quad \text{si } 3n-2 \leq \deg M \leq 3n\,. \tag{2}$$

On impose là les conditions de degré les plus restrictives possibles.

On voit aisément que si $q \in \{2,4\}$, certains polynômes de $\mathbb{F}_q[X]$ n'admettent pas des représentations strictes en sommes de cubes. En effet, dans le corps $\mathbb{F}_4$, seuls 0 ou 1 sont sommes de cubes. Si $M \in \mathbb{F}_2[X]$ est une somme de cubes de $\mathbb{F}_2[X]$, M est congru à 0 ou 1 modulo X^2+X+1 qui est le seul polynôme irréductible de degré 2. Si $M \in \mathbb{F}_4[X]$ est somme de cubes de $\mathbb{F}_4[X]$, M est congru à 0 ou 1 modulo les polynômes de degré 1 de $\mathbb{F}_4[X]$. Enfin, si $M \in \mathbb{F}_4[X]$ est de degré divisible par 3 et admet une représentation stricte en somme de cubes, le coefficient du terme de plus haut degré de M est une somme de cubes, il est donc égal à 1. On se limitera donc, et ce sera là la seule limitation, aux polynômes M vérifiant ces conditions nécessaires évidentes.

On définit le sous-ensemble $\mathcal{M}_q$ de $\mathbb{F}_q[X]$ de la façon suivante :

(i) $\mathcal{M}_q = \mathbb{F}_q[X]$ pour $q \geq 8$,

(ii) $\mathcal{M}_2$ est l'ensemble des polynômes M de $\mathbb{F}_2[X]$ congrus à 0 ou 1 modulo X^2+X+1,

(iii) $\mathcal{M}_4$ est l'ensemble des polynômes M de $\mathbb{F}_4[X]$ congrus à 0 ou 1 modulo les polynômes de degré 1 vérifiant l'une ou l'autre des conditions suivantes :

(a) le degré de M n'est pas divisible par 3,

(b) le degré de M est divisible par 3 et le polynôme M est unitaire.

On désigne par $G(q,3)$ le plus petit des entiers s, s'il en existe, tels que tout polynôme M de $\mathcal{M}_q$, de degré suffisamment grand, admette une représentation stricte en somme de s cubes.

Dans ce qui suit, on démontre le théorème suivant :

Théorème. *On a la majoration* $G(q,3) \leq 11$.

La démonstration de ce théorème fournit une estimation asymptotique du nombre $R_s(M)$ de solutions $(M_1, \ldots, M_s) \in \mathbb{F}_q[X]^s$ de l'équation (1) astreintes aux conditions de degré (2).

Ce travail est divisé en trois parties. La deuxième partie est consacrée à l'étude des séries singulières, la troisième partie à la majoration de $G(q,3)$ par la méthode du cercle. Dans la première partie, nous rappelons les définitions et notations introduites en [2] ainsi que les principaux outils de la

méthode du cercle dans $\mathbb{F}_q[X]$, nous introduisons les notations dont nous aurons besoin et nous établissons quelques résultats sur les sommes de cubes dans un corps de caractéristique 2 qui nous seront utiles.

I. Résultats auxiliaires

I.1. *Notations et conventions.* Dans ce qui suit, le mot polynôme désignera un élément de $\mathbb{A} = \mathbb{F}_q[X]$. L'ensemble des polynômes unitaires sera noté $\mathcal{U}$, l'ensemble des polynômes irréductibles unitaires sera noté $\mathcal{I}$.

Soit H un polynôme non nul. L'ensemble des polynômes de degré strictement inférieur à $\deg H$ identifié à l'ensemble des classes de congruence modulo H sera noté $\boldsymbol{C}_H$, l'ensemble des polynômes de $\boldsymbol{C}_H$ inversibles modulo H sera noté $\boldsymbol{C}_H^*$.

A la valuation à l'infini $\nu = \nu_\infty$ est associée la valeur absolue $|\ |_\infty$ définie par

$$|a|_\infty = q^{-\nu(a)} \quad \text{si } a \neq 0, \qquad |0|_\infty = 0\,.$$

Nous noterons $|\ |$ cette valeur absolue car le contexte permet de la distinguer aisément de la valeur absolue de $\mathbb{R}$ qui sera aussi utilisée.

Soit $\mathbb{K}_\infty$ le complété de $\mathbb{K}$ pour cette valeur absolue. Il s'identifie au corps $\mathbb{F}_q((X^{-1}))$ des séries de Laurent formelles en $\frac{1}{X}$ à coefficients dans $\mathbb{F}_q$. Si

$$u = \sum_{s=-\infty}^{\infty} u_s X^s$$

est un élément non nul de $\mathbb{K}_\infty$, on pose

$$\operatorname{sgn}(u) = u_{-\nu(u)}\,.$$

Si B est un ensemble fini, on note $\#B$ le nombre d'éléments de B.

I.2. *Sommes de cubes dans un corps fini de caractéristique* 2. Soit Q une puissance de 2. Soit $a \in \mathbb{F}_Q$. Pour tout entier $s \geq 1$, on désigne par $r_Q(a,s)$ le nombre de solutions $(a_1,\dots,a_s) \in \mathbb{F}_Q^s$ de l'équation

$$a = a_1^3 + \ldots + a_s^3\,. \tag{I.1}$$

On pose pour tout $a \in \mathbb{F}_Q$,

$$\psi_Q(a) = (-1)^{t_Q(a)}\,, \tag{I.2}$$

où t_Q désigne la trace de l'extension $\mathbb{F}_Q|\mathbb{F}_2$ et on pose aussi,

$$\tau_Q(a) = \sum_{b \in \mathbb{F}_Q} \psi_Q(ab^3)\,. \tag{I.3}$$

PROPOSITION I.1. *Soit $a \in \mathbb{F}_Q$. Alors, pour tout entier $s \geq 1$, on a*

$$r_Q(a,s) = \frac{1}{Q} \sum_{b \in \mathbb{F}_Q} \tau_Q(b)^s \psi_Q(ab)\,. \tag{I.4}$$

Démonstration. Immédiate, le caractère ψ_Q étant non trivial.

PROPOSITION I.2. *Soit a un élément non nul du corps $\mathbb{F}_Q$. Alors, on a*

$$|\tau_Q(a)| = \begin{cases} 0 & \text{si } Q \not\equiv 1 \bmod 3, \\ Q^{1/2} & \text{si } Q \equiv 1 \bmod 3 \text{ et si } a \text{ n'est pas un cube dans } \mathbb{F}_Q, \\ 2Q^{1/2} & \text{si } Q \equiv 1 \bmod 3 \text{ et si } a \text{ est un cube dans } \mathbb{F}_Q. \end{cases} \tag{I.5}$$

Démonstration. Si $Q \not\equiv 1 \bmod 3$, l'application $x \mapsto x^3$ est une bijection de $\mathbb{F}_Q$ sur lui-même, d'où

$$\tau_Q(a) = \sum_{x \in \mathbb{F}_Q} \psi_Q(ax^3) = \sum_{y \in \mathbb{F}_Q} \psi_Q(ay) = 0\,.$$

On suppose que 3 divise $Q-1$. On a

$$\tau_Q(a)^2 = \sum_{y,z \in \mathbb{F}_Q} \psi_Q(a(y+z)^3 + z^3) = \sum_{y \in \mathbb{F}_Q} \psi_Q(ay^3)\sigma_Q(ay, ay^2)\,,$$

où, pour $\alpha \in \mathbb{F}_Q$, $\beta \in \mathbb{F}_Q$,

$$\sigma_Q(\alpha,\beta) = \sum_{x \in \mathbb{F}_Q} \psi_Q(\alpha y^2 + \beta y)\,.$$

Le lemme I.9 de [2] nous donne alors

$$\tau_Q(a)^2 = \sum_{\substack{y \in \mathbb{F}_Q \\ ay = a^2 y^4}} \psi_Q(ay^3) Q\,.$$

Si a n'est pas un cube dans $\mathbb{F}_Q$, l'équation $y = ay^4$ n'admet que la solution triviale $y = 0$. Si a est un cube dans $\mathbb{F}_Q$, il existe trois éléments b_1, b_2, b_3 dans $\mathbb{F}_Q^*$ tels que $a = b_1^3 = b_2^3 = b_3^3$ et l'équation $y = ay^4$ admet les quatre solutions 0, b_1^{-1}, b_2^{-1}, b_3^{-1}. Par suite,

- si a n'est pas un cube, $\tau_Q(a)^2 = Q$,
- si a est un cube, $\tau_Q(a)^2 = Q(1 + 3\psi_Q(1))$.

Puisque 3 divise $Q-1$, Q est une puissance paire de 2 et $\psi_Q(1) = (-1)^{t_Q(1)} = 1$. Si a est un cube dans $\mathbb{F}_Q$, $\tau_Q(a)^2 = 4Q$.

PROPOSITION I.3. *Soient $a \in \mathbb{F}_Q$ et un entier $s \geq 1$. Alors,*

(i) *si $Q \not\equiv 1 \bmod 3$, on a $r_Q(a,s) = Q^{s-1}$,*
(ii) *si $Q \equiv 1 \bmod 3$, on a $r_Q(a,s) \geq Q^{s-1} - \frac{Q-1}{3}(2+2^s)Q^{s/2-1}$,*

(iii) *si* $Q = 4$, *on a*

$$r_Q(a,s) = 0 \qquad si\ a \notin \{0,1\}\,,$$
$$4r_Q(0,s) = 2\cdot 4^s + 2\cdot(-2)^s\,,$$
$$4r_Q(1,s) = 2\cdot 4^s - 2\cdot(-2)^s\,.$$

Démonstration. Avec (I.3), (I.1) et (I.2), on a

$$Qr_Q(a,s) = Q^s + \sum_{x\in\mathbb{F}_Q^*} \tau_Q(x)^s\psi_Q(ax)\,.$$

Avec la proposition précédente (i) est immédiat. On suppose $Q \not\equiv 1 \bmod 3$. Il y a $(Q-1)/3$ cubes dans $\mathbb{F}_Q^*$, d'où

$$\Big|\sum_{x\in\mathbb{F}_Q^*} \tau_Q(x)^s\psi_Q(ax)\Big| \le \Big(Q-1-\frac{Q-1}{3}\Big)Q^{s/2} + \frac{Q-1}{3}(2Q^{1/2})^s\,,$$

et

$$Qr_Q(a,s) \ge Q^s - Q^{s/2}\frac{Q-1}{3}(2+2^s)\,.$$

Lorsque $Q = 4$, le membre de droite de cette inégalité est négatif. Une étude directe donne le résultat annoncé.

I.3. *Le caractère* E *et la mesure de Haar* dt. On définit un caractère E de $\mathbb{K}_\infty$ en posant

$$E\Big(\sum_{s=-\infty}^{\infty} u_s X^s\Big) = \psi(u_{-1})\,, \tag{I.6}$$

où ψ est le caractère ψ_q défini ci-dessus.

Le caractère ψ de $\mathbb{F}_q$ étant non trivial, il en est de même du caractère E.

On désigne par $\mathcal{P}$ l'idéal de valuation de $\mathbb{K}_\infty$. C'est un sous-groupe compact de $\mathbb{K}_\infty$, groupe additif localement compact. On désigne par dt la mesure de Haar sur $\mathbb{K}_\infty$ normalisée à 1 sur l'idéal de valuation $\mathcal{P}$.

La proposition suivante donne l'égalité fondamentale de la méthode du cercle.

Proposition I.4. *Pour* $u \in \mathbb{K}_\infty$, *on a*

$$\int_{\mathcal{P}} E(ut)\,dt = \begin{cases} 1 & si\ \nu(u) > 0,\\ 0 & sinon. \end{cases} \tag{I.7}$$

Démonstration. C'est le cas $j = 0$ du théorème 3.5 de [7].

II. Les séries singulières. Soit un entier $s \geq 1$. Soit M un polynôme non nul. Pour tout polynôme H, on pose

$$A_s(M,H) = |H|^{-s} \sum_{G \in \boldsymbol{C}_H^*} S(H,G)^s E\left(\frac{GM}{H}\right), \tag{II.1}$$

où

$$S(H,G) = \sum_{R \in \boldsymbol{C}_H} E\left(\frac{GR^3}{H}\right). \tag{II.2}$$

On remarque que $S(H,G)$ est la somme $S(H,G,0)$ définie au paragraphe II de [2].

Dans ce qui suit, on s'intéresse aux séries singulières

$$B_s(M) = \sum_{H \in \mathcal{U}} A_s(M,H). \tag{II.3}$$

On montre que ces séries sont absolument convergentes pour $s \geq 7$ et que si $M \in \mathcal{M}_q$, elles sont minorées par une fonction de q et de s strictement positive.

Proposition II.1. *Il existe des constantes $a_1(q,s)$, $a_2(q,s)$ telles que pour tout polynôme unitaire H, on ait*

$$|A_s(M,H)| \leq a_1(q,s)|H|^{1-s/3}, \tag{II.4}$$

et, pour $s \geq 7$, pour tout entier $m > 0$, on ait

$$\sum_{\substack{H \in \mathcal{U} \\ \deg H \geq m}} |A_s(M,H)| \leq a_2(q,s) q^{m(2-s/3)}. \tag{II.5}$$

Pour $s \geq 7$, la série $B_s(M)$ est absolument convergente.

Démonstration. Les propositions II.4 et II.11 de [2] donnent l'existence d'une constante $\alpha_1(q)$ telle que

$$|S(H,G,0)| \leq \alpha_1(q)|H|^{2/3},$$

pour tout couple de polynômes (H,G), où G est premier à H. On a donc (II.4) avec $a_1(q,s) = \alpha_1(q)^s$. On en déduit que pour tout entier $k \geq 0$, on a

$$\sum_{\substack{H \in \mathcal{U} \\ \deg H = k}} |A_s(M,H)| \leq a_1(q,s) q^{k(2-s/3)},$$

d'où, pour $s \geq 7$,

$$\sum_{\substack{H \in \mathcal{U} \\ \deg H \geq m}} |A_s(M,H)| \leq a_1(q,s) q^{m(2-s/3)} (1 - q^{2-s/3})^{-1},$$

ce qui donne (II.5) avec $a_2(q,s) = a_1(q,s)(1-q^{2-s/3})^{-1}$, ainsi que la convergence absolue de $B_s(M)$.

Pour $s \geq 7$, la somme $B_s(M)$ se développe en produit eulérien absolument convergent. Pour cela, on pose pour tout polynôme irréductible unitaire P,

$$\Lambda_s(M,P) = \sum_{j=0}^{\infty} A_s(M,P^j)\,. \tag{II.6}$$

La majoration (II.4) nous donne la convergence de cette série pour $s \geq 7$. En fait, on pourrait définir $\Lambda_s(M,P)$ pour tout s car on peut montrer que $A_s(M,P^j)$ est nul sauf pour un nombre fini d'indices j.

Proposition II.2. *Si H_1 et H_2 sont des polynômes premiers entre eux, on a*

$$A_s(M,H_1H_2) = A_s(M,H_1)A_s(M,H_2)\,. \tag{II.7}$$

Démonstration. On procède comme pour le problème de Waring classique (cf. [1], chapitre IV, paragraphe 8) en utilisant les propriétés bien connues du caractère E (cf. [2], [3], [6], [7]).

Proposition II.3. *Pour $s \geq 7$, il existe une constante $a_3(q,s)$ telle que pour tout polynôme irréductible P, on ait*

$$|\Lambda_s(M,P) - 1| \leq a_3(q,s)|P|^{1-s/3}\,. \tag{II.8}$$

Démonstration. Les relations (II.4) et (II.7) donnent

$$|\Lambda_s(M,P) - 1| \leq a_1(q,s)|P|^{1-s/3}(1-|P|^{1-s/3})^{-1} \leq a_3(q,s)|P|^{1-s/3}\,,$$

avec $a_3(q,s) = a_1(q,s)(1-q^{1-s/3})^{-1}$.

Corollaire II.4. *Pour $s \geq 7$, on a*

$$B_s(M) = \prod_{P \in \mathcal{I}} \Lambda_s(M,P)\,, \tag{II.9}$$

ce dernier produit étant absolument convergent.

Démonstration. La convergence absolue du produit ci-dessus s'obtient comme la convergence absolue de la série $B_s(M)$ à l'aide de la majoration (II.4). L'égalité (II.9) se déduit alors de la relation (II.7).

La majoration (II.8) permet de majorer $B_s(M)$. Pour minorer $B_s(M)$ nous aurons besoin de deux résultats supplémentaires.

Pour tout polynôme irréductible P, pour tout entier $k \geq 1$, on désigne par $\varrho(M,s,P^k)$ le nombre de solutions $(M_1,\ldots,M_s) \in \boldsymbol{C}_{P^k} \times \ldots \times \boldsymbol{C}_{P^k}$ de la congruence

$$M \equiv M_1^3 + \ldots + M_s^3 \bmod P^k\,.$$

PROPOSITION II.5. *Pour tout entier $s \geq 1$, on a*

$$|P|^{k(1-s)}\varrho(M,s,P^k) = \sum_{j=0}^{k} A_s(M,P^j)\,. \tag{II.10}$$

Démonstration. Comme pour le théorème 8.11 de [1].

PROPOSITION II.6. *Si $M \in \mathcal{M}_q$, pour tout entier $s \geq 4$, pour tout polynôme irréductible P, on a*

$$\Lambda_s(M,P) \geq |P|^{1-s}\,. \tag{II.11}$$

Démonstration. Comme pour le théorème 8.13 de [1], on peut montrer que si $T \in \mathbb{A}$ est tel que la congruence $T \equiv Y^3 \bmod P$ admet une solution Y non divisible par P, alors, pour tout entier $k \geq 1$, la congruence $T \equiv Z^3 \bmod P^k$ admet une solution Z non divisible par P. La proposition I.3 montre que pour $|P| \geq 8$, la congruence

$$A \equiv A_1^3 + A_2^3 + A_3^3 \bmod P$$

est résoluble pour tout $A \in \mathbb{A}$, et donc que pour $s \geq 4$, pour tout $A \in \mathbb{A}$, la congruence

$$A \equiv A_1^3 + \ldots + A_s^3 \bmod P$$

admet une solution $(A_1,\ldots,A_s)$ où les A_i ne sont pas tous divisibles par P. Si $|P| = 4$, si $A \in \mathcal{M}_q$, A est congru à 0 ou 1 modulo P et pour $s \geq 4$, la congruence

$$A \equiv A_1^3 + \ldots + A_s^3 \bmod P$$

admet une solution où l'un des A_i est égal à 1 modulo P.

On a supposé $M \in \mathcal{M}_q$, $s \geq 4$. La congruence

$$M \equiv M_1^3 + \ldots + M_s^3 \bmod P$$

admet une solution $(M_1,\ldots,M_s)$ avec par exemple M_s non divisible par P. Soit un entier $k \geq 1$. Soient $(H_1,\ldots,H_{s-1}) \in \boldsymbol{C}_{P^k} \times \ldots \times \boldsymbol{C}_{P^k}$ tels que

$$H_i \equiv M_i \bmod P\,. \tag{i}$$

Alors,

$$M + H_1^3 + \ldots + H_{s-1}^3 \equiv M_s^3 \bmod P$$

et il existe Z non divisible par P tel que

$$M + H_1^3 + \ldots + H_{s-1}^3 \equiv Z^3 \bmod P^k\,. \tag{ii}$$

La congruence

$$M \equiv Z_1^3 + \ldots + Z_s^3 \bmod P^k$$

admet au moins toutes les solutions $(H_1,\ldots,H_{s-1},Z)$ vérifiant (i) et (ii). On a donc

$$\varrho(M,s,P^k) \geq |P|^{(k-1)(s-1)}$$

et (II.10) nous donne

$$\sum_{j=0}^{k} A_s(M, P^j) \geq |P|^{1-s}\,.$$

On conclut avec (II.6).

PROPOSITION II.7. *Soit un entier* $s \geq 7$. *Alors, il existe une constante* $a_4(q,s) > 0$ *telle que pour tout polynôme* $M \in \mathcal{M}_q$, *on ait*

$$a_4(q,s) \leq B_s(M) \leq a_2(q,s)\,. \tag{II.12}$$

Démonstration. La relation (II.8) donne la minoration

$$\Lambda_s(M,P) \geq 1 - a_3(q,s)|P|^{1-s/3}\,. \tag{i}$$

Soit

$$\delta(q,s) = \frac{3\log(2a_3(q,s))}{(s-3)\log q}\,. \tag{ii}$$

Si $\deg P \geq \delta(q,s)$, le deuxième membre de (i) est strictement positif. On pose

$$a_4(q,s) = \Big\{ \prod_{\substack{P\in\mathcal{I}\\ \deg P<\delta(q,s)}} |P|^{1-s} \Big\} \Big\{ \prod_{\substack{P\in\mathcal{I}\\ \deg P\geq\delta(q,s)}} (1 - a_3(q,s)|P|^{1-s/3}) \Big\}\,.$$

Alors, $a_4(q,s) > 0$ et les relations (II.9) et (II.11) nous donnent $B_s(M) \geq a_4(q,s)$. La majoration se déduit immédiatement de (II.4) et (II.5).

III. Majoration de $G(q,3)$**.** Soit M un polynôme non nul. Suivant la méthode du cercle, on exprime le nombre $R_s(M)$ de représentations strictes de M en somme de s cubes à l'aide d'une intégrale. On procède comme suit. Soit n l'entier déterminé par la condition

$$3n - 2 \leq \deg M \leq 3n\,. \tag{III.1}$$

Soit f l'application de $\mathcal{P}$ dans $\mathbb{Z}$ définie par

$$f(t) = \sum_{\substack{A\in\mathbb{A}\\ \deg A\leq n}} E(tA^3)\,. \tag{III.2}$$

PROPOSITION III.1. *Soit un entier* $s \geq 1$. *Alors, on a*

$$R_s(M) = \int_{\mathcal{P}} f^s(t)E(Mt)\,dt\,. \tag{III.3}$$

Démonstration. Immédiate avec (I.7).

On désigne par $\mathcal{F}_n$ l'ensemble des *fractions de Farey* à l'ordre n, c'est-à-dire, l'ensemble des fractions rationnelles G/H telles que $G \in \boldsymbol{C}_H^*$ et

$\deg H \le n$. Si G/H est un élément de $\mathcal{F}_n$, on appelle *arc de Farey de centre* G/H l'ensemble $\mathcal{U}_{G/H}$ ainsi défini :

$$t \in \mathcal{U}_{G/H} \;\Leftrightarrow\; \nu\left(t - \frac{G}{H}\right) > n + \deg H\,. \tag{III.4}$$

Proposition III.2. *Lorsque G/H décrit $\mathcal{F}_n$, les arcs de Farey $\mathcal{U}_{G/H}$ forment une partition de $\mathcal{P}$.*

Démonstration. C'est le théorème 4.3 de [7].

Dans [2] on a montré que l'on a une bonne approximation de $f(t)$ pour les $t \in \mathcal{P}$ proches d'une fraction G/H de $\mathcal{F}_n$. Ces points sont ceux qui vérifient $\nu(t - G/H) > 2n + \deg H$. Ils correspondent aux arcs majeurs d'une dissection de Farey classique. Pour les autres t on a seulement une majoration de $f(t)$.

Si $G/H \in \mathcal{F}_n$, on appelle *arc majeur de centre* G/H la boule $\mathcal{A}_{G/H}$ définie par la condition

$$t \in \mathcal{A}_{G/H} \;\Leftrightarrow\; \nu\left(t - \frac{G}{H}\right) > 2n + \deg H\,. \tag{III.5}$$

Notons $\mathcal{P}^+$ la réunion des arcs majeurs et $\mathcal{P}^-$ le complémentaire de $\mathcal{P}^+$ dans $\mathcal{P}$. Posons

$$R_s^+(M) = \int\limits_{\mathcal{P}^+} f^s(t)E(Mt)\,dt\,, \tag{III.6}$$

$$R_s^-(M) = \int\limits_{\mathcal{P}^-} f^s(t)E(Mt)\,dt\,. \tag{III.7}$$

Proposition III.3. *On a*

$$R_s^+(M) = \sum_{G/H \in \mathcal{F}_n} |H|^{-s} S^s(H,G) E\left(M\frac{G}{H}\right) J_{H,s}(M)\,, \tag{III.8}$$

où

$$J_{H,s}(M) = \int\limits_{\nu(u) > 2n + \deg H} f^s(u)E(Mu)\,du\,. \tag{III.9}$$

Démonstration. D'après le corollaire IV.3 de [2], si $t \in \mathcal{A}_{G/H}$,

$$f(t) = |H|^{-1} S(H,G) f\left(t + \frac{G}{H}\right),$$

d'où (III.9).

PROPOSITION III.4. *On a*

(III.10)
$$J_{H,s}(M) = \begin{cases} q^{n(s-3)} r(\mathrm{sgn}(M), s) & \text{si } \deg M = 3n, \\ q^{n(s-3)}(r(0,s)-1) & \text{si } \deg M \neq 3n \\ & \quad \text{et si } \deg H \leq \deg M - 2n, \\ q^{n(s-3)} r(0,s) & \text{si } \deg M \neq 3n \\ & \quad \text{et si } \deg H = n, \\ q^{n(s-3)}(r(0,s)+q-1) & \text{si } \deg M = 3n-2 \\ & \quad \text{et } \deg H = n-1, \end{cases}$$

$r(a,s)$ désignant le nombre $r_q(a,s)$ de solutions $(a_1,\dots,a_s) \in \mathbb{F}_q^s$ de l'équation

(I.1) $$a = a_1^3 + \dots + a_s^3 .$$

Démonstration. Le corollaire IV.3 de [2] donne les valeurs de $f(u)$ pour $\nu(u) > 2n$.

(i) $$f(u) = \begin{cases} q^{n+1} & \text{si } \nu(u) > 3n+1, \\ q^m & \text{si } 2n+1 \leq \nu(u) \leq 3n,\ \nu(u) \in \{3m, 3m-1\}, \\ q^m \tau(\mathrm{sgn}(u)) & \text{si } \nu(u) = 3m+1 \leq 3n+1. \end{cases}$$

Une démonstration analogue à celle de la proposition IV.3 de [3] conduit alors au résultat annoncé.

On remarque que l'on peut écrire

(III.11) $$J_{H,s}(M) = q^{n(s-3)} \Theta_q(s, M, H) ,$$

et que l'on a

(III.12) $$\Theta_q(s,M,H) = \Theta_q(s,M,1) = \begin{cases} r(\mathrm{sgn}(M), s) & \text{si } \deg M = 3n, \\ r(0,s) - 1 & \text{si } \deg M \neq 3n, \end{cases}$$

si $\deg H \leq n-2$.

On supposera maintenant $s \geq 7$. La proposition I.3 conduit aux remarques suivantes :

Remarques III.5. Si $q \not\equiv 1 \bmod 3$,
$$63 \leq q^{s-1} - 1 \leq \Theta_q(s,M,H) < q^{s-1} + q - 1 .$$
Si $q \equiv 1 \bmod 3$ et si $q \geq 16$,
$$0 < q^{s-1} - \frac{q-1}{3}(2 + 2^s) q^{s/2-1} - 1 \leq \Theta_q(s,M,H) \leq 3q^{s-1} + q - 1 .$$
Si $q = 4$, si $\deg M = 3n$ et si $\mathrm{sgn}(M) = 1$,
$$2^{13} + 2^5 - 1 \leq \Theta_q(s,M,H) \leq 2(4^{s-1} + 2^{s-2}) .$$
Si $q = 4$, si $\deg M \neq 3n$,
$$2^{11} - 2^5 - 1 \leq \Theta_q(s,M,H) \leq 3 + 2(4^{s-1} + 2^{s-2}) .$$

Si $q = 4$, si $\deg M = 3n$ et si $\mathrm{sgn}(M) \neq 1$,

$$\Theta_q(s, M, H) = 0\,.$$

Proposition III.6. *On a*

$$|R_s^+(M) - \Theta_q(s, M, 1)q^{n(s-3)}B_s(M)| \leq a_5(q, s)q^{n(2s/3-1)}\,, \tag{III.13}$$

avec

$$a_5(q, s) = q^{s/3-2}a_2(q, s)(3q^{s-1} + q - 1)\,. \tag{III.14}$$

Démonstration. Avec (III.8) et (II.1), on a

$$R_s^+(M) = \sum_{\substack{H\in\mathcal{U}\\ \deg H\leq n}} A_s(M, H)J_{H,s}(M)\,,$$

puis avec (III.11) et (III.12),

$$R_s^+(M) = q^{n(s-3)} \sum_{\substack{H\in\mathcal{U}\\ \deg H\leq n}} A_s(M, H)\Theta_q(s, M, H)\,,$$

$$R_s^+(M) = q^{n(s-3)}\Theta_q(s, M, 1) \sum_{\substack{H\in\mathcal{U}\\ \deg H\leq n-2}} A_s(M, H) + q^{n(s-3)} \sum_{\substack{H\in\mathcal{U}\\ n-1\leq\deg H\leq n}} A_s(M, H)\Theta_q(s, M, H)\,.$$

Les remarques III.5 permettent de majorer $\Theta_q(s, M, H)$. Dans tous les cas, on a

$$\Theta_q(s, M, H) \leq 3q^{s-1} + q - 1\,,$$

d'où, avec (II.3) et (II.5),

$$|R_s^+(M) - q^{n(s-3)}\Theta_q(s, M, 1)B_s(M)| \leq (3q^{s-1} + q - 1)q^{n(s-3)}a_2(q, s)q^{(n-1)(2-s/3)}\,.$$

C'est là le résultat annoncé.

On majore R_s^- par la méthode de Hua (cf. [8]). Nous utiliserons un lemme préliminaire.

Lemme III.7. *Pour tout polynôme non nul A, soit $d(A)$ le nombre de diviseurs de A. Alors, pour tout nombre réel $\varepsilon > 0$, il existe une constante $a_6(q, \varepsilon)$ telle que*

$$d(A) \leq a_6(q, \varepsilon)|A|^{\varepsilon}\,. \tag{III.15}$$

Démonstration. Comme pour la majoration du nombre de diviseurs d'un entier. Voir par exemple le lemme 5.1, chapitre VIII, de [1].

PROPOSITION III.8. *Soit un nombre réel* $\varepsilon > 0$. *Alors, il existe une constante* $a_7(q,\varepsilon)$ *telle que*

$$\int_{\mathcal{P}} f(t)^4\,dt \le a_7(q,\varepsilon)q^{n(2+\varepsilon)}\,. \tag{III.16}$$

Démonstration. Comme pour la proposition II.4 de [2], on démontre que

$$f(t)^2 \in \{0, g(t)\}\,, \quad \text{où} \quad g(t) = \sum_{A,B\in\mathbb{A}_n} E(t(A^2B+AB^2))\,.$$

Avec (I.7), on en déduit la majoration

$$\int_{\mathcal{P}} f(t)^4\,dt \le \#\{(A,B,Y,Z)\in\mathbb{A}_n^4 \mid A^2B+AB^2 = Y^2Z+YZ^2\}\,,$$

d'où

$$\int_{\mathcal{P}} f(t)^4\,dt \le \sum_{A,B\in\mathbb{A}_n^*} d(A^2B+AB^2) + 3(q^{n+1}-1)\,. \tag{i}$$

On conclut avec le lemme précédent.

PROPOSITION III.9. *Soit un nombre réel* $\varepsilon > 0$. *Alors, il existe une constante* $a_8(q,s,\varepsilon)$ *telle que*

$$|R_s^-(M)| \le a_8(q,s,\varepsilon)q^{n(5s/6-4/3+\varepsilon)}\,. \tag{III.17}$$

Démonstration. Si $t\in\mathcal{P}^-$, il existe $G/H\in\mathcal{F}_n$ tel que $n+\deg H < \nu(t-G/H)\le 2n+\deg H$. Soit $\delta=\varepsilon/(s-3)$. La proposition IV.4 de [2] nous donne l'existence d'une constante $\beta(q,s,\delta)$ telle que

$$|f(t)| \le \beta(q,s,\delta)q^{n(5/6+\delta)}\,,$$

d'où

$$\int_{\mathcal{P}^-} |f(t)^s E(Mt)|\,dt \le (\beta(q,s,\delta)q^{n(5/6+\delta)})^{s-4}\int_{\mathcal{P}^-}|f(t)|^4\,dt\,,$$

$$\int_{\mathcal{P}^-} |f(t)^s E(Mt)|\,dt \le (\beta(q,s,\delta)q^{n(5/6+\delta)})^{s-4}\int_{\mathcal{P}}|f(t)|^4\,dt\,.$$

La proposition précédente donne alors la majoration annoncée avec

$$a_8(q,s,\varepsilon) = a_7\Big(q,\frac{\varepsilon}{s-3}\Big)\beta\Big(q,s,\frac{\varepsilon}{s-3}\Big)^{(s-4)}\,.$$

COROLLAIRE III.10. *Soit* $\varepsilon>0$. *Alors, on a*

$$|R_s(M) - \Theta_q(s,M,1)q^{n(s-3)}B_s(M)| \le a_9(q,s,\varepsilon)q^{n(5s/6-4/3+\varepsilon)}\,, \tag{III.18}$$

avec

$$a_9(q,s,\varepsilon) = a_8(q,s,\varepsilon) + a_5(q,s)\,. \tag{III.19}$$

Démonstration. Immédiate.

Nous pouvons conclure.

PROPOSITION III.11. *Soit un entier $s \geq 11$. Alors, tout polynôme de $\mathcal{M}_q$, de degré suffisamment élevé, admet une représentation stricte en somme de s cubes.*

Démonstration. Pour $s \geq 11$, la relation (III.18) conduit à une relation de la forme

$$\text{(i)} \qquad R_s(M) = \Theta_q(s, M, 1) B_s(M) q^{n(s-3)} + o(q^{n(s-3)}) .$$

Les remarques III.5 montrent l'existence d'une constante $a_{10}(q, s) > 0$ telle que

$$\text{(ii)} \qquad \Theta_q(s, M, 1) \geq a_{10}(q, s) \quad \text{pour tout } M \in \mathcal{M}_q .$$

La proposition II.7 donne l'existence d'une constante $a_4(q, s) > 0$ telle que

$$\text{(iii)} \qquad B_s(M) \geq a_4(q, s) \quad \text{pour tout } M \in \mathcal{M}_q .$$

La relation (i) montre que pour $s \geq 11$, pour $M \in \mathcal{M}_q$, de degré $3n-1$, $3n$ ou $3n+1$, assez grand, on a $R_s(M) > 0$. Le polynôme M admet alors une représentation stricte en somme de s cubes.

Références

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Math. Surveys 10, Amer. Math. Soc., 1963.

[2] M. Car, *Sommes d'exponentielles dans $\mathbb{F}_{2^h}((X^{-1}))$*, Acta Arith. 62 (1992), 303–328.

[3] —, *Sommes de carrés dans $\mathbb{F}[X]$*, Dissertationes Math. 215 (1983).

[4] J. Cherly, *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à 2 éléments, et application au problème de Waring*, thèse soutenue à l'Université de Bordeaux I, 1989.

[5] —, *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à 2 éléments, et application au problème de Waring*, Astérisque 200 (1991), 198–199.

[6] G. Effinger and D. Hayes, *Additive Number Theory of Polynomials over a Finite Field*, Oxford University Press, 1991.

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

[8] L. K. Hua, *On Waring's problem*, Quart. J. Math. Oxford 9 (1938), 199–202.

[9] R. M. Kubota, *Waring's problem for $\mathbb{F}_q[X]$*, Dissertationes Math. 215 (1983).

[10] L. N. Vaserstein, *Waring's problem for commutative rings*, J. Number Theory 26 (1987), 299–307.

[11] —, *Waring's problem for algebras over fields*, ibid. 26 (1987), 286–298.

[12] R. C. Vaughan, *Some remarks on Weyl sums*, in: Topics in Classical Number Theory, Budapest 1981, Colloq. Math. Soc. János Bolyai 34, Vol. II, North-Holland, 1984, 1585–1602.

LABORATOIRE DE MATHÉMATIQUES
FACULTÉ DES SCIENCES DE SAINT-JÉRÔME
AVENUE ESCADRILLE NORMANDIE-NIEMEN
13397 MARSEILLE CEDEX 13
FRANCE

UNIVERSITÉ DE BRETAGNE OCCIDENTALE
6, AVENUE LE GORGEU
29287 BREST CEDEX
FRANCE

Reçu le 16.11.1992 (2333)