ACTA ARITHMETICA
113.2 (2004)

Une généralisation du problème de Waring–Goldbach polynomial

par

Houda Aïssa (Tunis)

I. Introduction. Soit $\mathbb{F}_q$ le corps fini à q éléments, q étant impair, et $\mathbb{F}_q[X]$ l'anneau des polynômes à une variable sur le corps $\mathbb{F}_q$. Certaines analogies entre les propriétés arithmétiques de l'anneau $\mathbb{F}_q[X]$ et l'anneau $\mathbb{Z}$ des entiers relatifs ont été mises en évidence. En particulier, en ce qui concerne l'arithmétique additive, les problèmes de Waring [18] et de Goldbach [14] ont été étudiés et plus particulièrement le problème de Waring pour les carrés ([6]–[12]).

Dans [2], M. Car a établi une estimation asymptotique du nombre $\varrho(s, M)$ de représentations d'un polynôme $M \in \mathbb{F}_q[X]$ comme somme de s carrés de polynômes irréductibles :

$$M = P_1^2 + \ldots + P_s^2,$$

$P_1, \ldots, P_s$ étant des polynômes satisfaisant aux conditions de degré les plus restrictives possibles, à savoir pour tout $i = 1, \ldots, s$,

$$\deg P_i \le n \quad \text{si } \deg M \in \{2n, 2n-1\},$$

et cela pour $s \ge 5$.

D'autre part dans [5], M. Car a établi une estimation asymptotique du nombre $R(A_1, \ldots, A_s; M)$ de représentations d'un polynôme $M \in \mathbb{F}_q[X]$ comme somme

$$M = A_1 Y_1^2 + \ldots + A_s Y_s^2,$$

les polynômes $A_1, \ldots, A_s$ étant donnés premiers entre eux deux à deux, les polynômes $Y_1, \ldots, Y_s$ satisfaisant aux conditions de degré les plus restrictives possibles.

Une généralisation naturelle de ces deux problèmes est la suivante : étant donnés $A_1, \ldots, A_s$ polynômes de $\mathbb{F}_q[X]$, peut on représenter les polynômes $M \in \mathbb{F}_q[X]$ comme somme

$$M = A_1 P_1^2 + \ldots + A_s P_s^2, \tag{1}$$

2000 *Mathematics Subject Classification*: 11P55, 11E25.

$P_1, \dots, P_s$ étant des polynômes irréductibles de $\mathbb{F}_q[X]$ satisfaisant aux conditions de degré les plus restrictives possibles, à savoir, pour $i = 1, \dots, s$,

$$\deg P_i \le m_i? \tag{2}$$

Ici m_i est défini par

$$\deg M - \deg A_i = \begin{cases} 2m_i & \text{si } \deg M - \deg A_i \text{ est pair,} \\ 2m_i - 1 & \text{si } \deg M - \deg A_i \text{ est impair.} \end{cases}$$

Conformément à la terminologie de G. Effinger et D. Hayes [13], une représentation (1) satisfaisant la condition (2) est appelée une *représentation stricte*.

Comme le cas $\deg A_1 = \dots = \deg A_s = 0$ est semblable au cas $A_1 = \dots = A_s = 1$ déjà étudié dans [2], on supposera qu'au moins un polynôme parmi $A_1, \dots, A_s$ est non constant.

Comme il a déjà été noté dans [5], sans hypothèses supplémentaires sur les polynômes $A_1, \dots, A_s$, il existe une infinité de polynômes $M \in \mathbb{F}_q[X]$ n'admettant pas de représentation (1). Dans ce qui suit, nous supposerons les polynômes $A_1, \dots, A_s$ premiers entre eux deux à deux. Sous ces hypothèses nous obtenons le résultat suivant :

THÉORÈME. *Soient un entier $s \ge 5$ et $A_1, \dots, A_s$ des polynômes de $\mathbb{F}_q[X]$ premiers entre eux deux à deux. Alors* :

(i) *Si $q = 7$ ou $q > 9$ tout polynôme $M \in \mathbb{F}_q[X]$ de degré assez grand admet une représentation stricte comme somme*

$$M = A_1 P_1^2 + \dots + A_s P_s^2.$$

De plus, si $R_s(M)$ désigne le nombre de ces représentations on a

$$R_s(M) \gg (\deg M)^{-s} |M|^{s/2-1},$$

la constante intervenant dans le symbole $\gg$ ne dépendant que de q, s et $A_1, \dots, A_s$.

(ii) *Si $q = 5$ ou $q = 9$ et au moins quatre parmi $A_1, \dots, A_s$ ont des degrés de même parité, soient $A_{i_1}, \dots, A_{i_4}$, le résultat précédent reste valable pour les polynômes M tel que* $\deg M \equiv \deg A_{i_1} \bmod 2$.

La condition $s \ge 5$ est une condition technique. En fait, cette condition est nécessaire pour la convergence des séries singulières $\mathfrak{S}_s(M)$ (voir Proposition IV.9). Jusqu'à maintenant on n'a pas de démonstration pour le cas $s = 4$ et on ne peut pas donner de contre-exemple.

II. Notations et conventions. Nous reprenons ici — en les rappelant — les notations utilisées dans [3] et [5]. Dans cet article, le mot *polynôme* désignera un polynôme de $\mathbb{F}_q[X]$. On désigne par $\mathbb{M}$ l'ensemble des polynômes unitaires, par $\mathbb{M}_l$ l'ensemble des polynômes unitaires de degré l, par

I l'ensemble des polynômes irréductibles unitaires et par I^* l'ensemble des polynômes irréductibles quelconques. Si A et B sont des polynômes non nuls, on note (A, B) leur pgcd unitaire.

Soit H un polynôme non nul. On note $\deg H$ son degré, et $\mathcal{C}_H$ l'ensemble des polynômes de degré strictement inférieur au degré de H identifié à l'ensemble des classes de congruence modulo H. Le groupe multiplicatif des classes inversibles modulo H sera noté $\mathcal{C}_H^*$, l'ordre de ce groupe sera noté $\Phi(H)$. La fonction Φ ainsi définie a les mêmes propriétés que la fonction d'Euler classique. Sur le corps $\mathbb{K} = \mathbb{F}_q(X)$ des fractions rationnelles, on définit une valuation v par

$$v\left(\frac{A}{B}\right) = \deg B - \deg A$$

si A et B sont des polynômes non nuls. Le complété $\mathbb{K}_\infty$ de $\mathbb{K}$ pour cette valuation s'identifie au corps $\mathbb{F}_q((X^{-1}))$ des séries de Laurent en $1/X$ sur le corps $\mathbb{F}_q$, la valuation v se prolongeant aux éléments non nuls de $\mathbb{K}_\infty$ par

$$v\Big(\sum_{s=-\infty}^{\infty} a_s X^s\Big) = -\sup\{s \in \mathbb{Z};\, a_s \neq 0\}.$$

On associe à cette valuation la valeur absolue $|\ |_\infty$ définie par

$$|\alpha|_\infty = \begin{cases} q^{-v(\alpha)} & \text{si } \alpha \neq 0, \\ 0 & \text{si } \alpha = 0. \end{cases}$$

Nous noterons simplement $|\ |$ cette valeur absolue car le contexte nous permet de la distinguer de la valeur absolue classique sur le corps $\mathbb{R}$ des nombres réels ou le corps $\mathbb{C}$ des nombres complexes qu'on va utiliser.

Soit $u \in \mathbb{K}_\infty$; si $u = \sum_{s=-\infty}^{\infty} u_s X^s$, on pose $\mathrm{Res}(u) = u_{-1}$. De plus, pour tout non nul $u \in \mathbb{K}_\infty$, on pose $\mathrm{sgn}(u) = u_{-v(u)}$.

Si B est un sous-ensemble non vide de $\{1, \dots, s\}$, on désigne par $\#B$ le cardinal de B. D'autre part, si $\alpha_1, \dots, \alpha_s$ sont des éléments de $\mathbb{F}_q$, pour tout $x \in \mathbb{F}_q$ on note $r_B(\alpha_1, \dots, \alpha_s; x)$ le nombre de solutions $(x_i)_{i\in B} \in (\mathbb{F}_q^*)^{\#B}$ de l'equation

$$x = \sum_{i\in B} \alpha_i x_i^2.$$

Pour tout entier $j \geq 1$, on pose

$$\tau_j = \sum_{k=1}^{j} (q-1)\,\frac{q^k}{k}. \tag{II.1}$$

III. La méthode du cercle. Soit Ψ le caractère additif défini sur $\mathbb{F}_q$ par

$$\Psi(x) = \exp\left(\frac{2i\pi\,\mathrm{tr}(x)}{p}\right),$$

où tr est l'application trace de $\mathbb{F}_q$ dans $\mathbb{F}_p$. Au caractère non trivial Ψ, on associe le caractère additif non trivial E de $\mathbb{K}_\infty$ défini par

$$E(u) = \Psi(\mathrm{Res}(u)).$$

On désigne par $\mathcal{P}$ l'idéal de valuation, et, pour tout entier j, par $\mathcal{P}_j$ l'idéal

$$\{t \in \mathbb{K}_\infty;\, v(t) > j\}.$$

Les ensembles $\mathcal{P}_j$ sont des sous-groupes compacts du groupe additif localement compact $\mathbb{K}_\infty$. Désignons par dt la mesure de Haar sur $\mathbb{K}_\infty$ normalisée à 1 sur $\mathcal{P}$.

Nous rappelons ici quelques résultats établis dans [14] que nous utiliserons fréquemment par la suite.

Proposition III.1. (i) *Pour tout entier rationnel j, $\mathcal{P}_j$ a pour mesure q^{-j}.*

(ii) *Pour tout $H \in \mathbb{F}_q[T]$, $E(H) = 1$.*

(iii) *Soit H un polynôme non nul et soient A et B deux polynômes. Alors*,

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

(iv) *Pour tout $u \in \mathbb{K}_\infty$, on a*

$$v(u) \geq 2 \;\Rightarrow\; E(u) = 1.$$

(v) *Soient un entier $j \geq 0$, $u \in \mathbb{K}_\infty$ et $b \in \mathcal{P}$. Alors*,

$$\int_{b+\mathcal{P}_j} E(ut)\,dt = \begin{cases} q^{-j}E(ub) & \text{si } v(u) > -j, \\ 0 & \text{si } v(u) \leq -j. \end{cases} \tag{III.1}$$

(vi) *Soient G et H des polynômes, H n'étant pas nul. Alors*,

$$\sum_{R \in \mathcal{C}_H} E\left(\frac{G}{H}\,R\right) = \begin{cases} |H| & \text{si } H \text{ divise } G, \\ 0 & \text{si } H \text{ ne divise pas } G. \end{cases} \tag{III.2}$$

Soit un entier $s \geq 5$. Soient $A_1, \ldots, A_s$ des polynômes premiers entre eux, l'un d'entre eux au moins étant non constant. Pour $i = 1, \ldots, s$, soient

$$a_i = \deg A_i, \qquad \alpha_i = \mathrm{sgn}(A_i).$$

Sans perte de généralité on peut supposer que $a_1 \leq \ldots \leq a_s$. On a donc $a_s \neq 0$. Soit n un entier naturel tel que

$$n^{1/3} \geq 2\left(2q(\log q)^{-2} + \frac{1}{4}\right) + \frac{a_s}{2} + \frac{1}{2}, \tag{III.3}$$

$$n - 4n^{1/3} \geq \frac{3(a_s+1)}{2}. \tag{III.4}$$

Soit M un polynôme de degré $2n$ ou $2n-1$. Soit $R_s(A_1, \ldots, A_s; M)$ le nombre de solutions $(P_1, \ldots, P_s) \in (\mathbb{F}_q[X])^s$ de l'equation (1), vérifiant les conditions de degré (2).

On rappelle que pour tout $i = 1, \dots, s$,

$$\deg M - \deg A_i = \begin{cases} 2m_i & \text{si } \deg M - \deg A_i \text{ est pair,} \\ 2m_i - 1 & \text{si } \deg M - \deg A_i \text{ est impair.} \end{cases} \tag{III.5}$$

Soit $u(M)$, respectivement $v(M)$, l'ensemble des $i \in \{1, \dots, s\}$ tel que $\deg M \equiv a_i \bmod 2$, respectivement $\deg M \not\equiv a_i \bmod 2$. Pour $i = 1, \dots, s$, on note f_i l'application de $\mathcal{P}$ dans $\mathbb{C}$ définie par

$$f_i(t) = \sum_{\substack{P \in I^* \\ \deg P \le m_i}} E(tA_iP^2). \tag{III.6}$$

On pose

$$F(t) = \prod_{i=1}^{s} f_i(t). \tag{III.7}$$

Alors, d'après la relation (III.1) on a

$$R_s(A_1, \dots, A_s; M) = \int_{\mathcal{P}} F(t)E(-Mt)\,dt. \tag{III.8}$$

Pour alléger les notations, quand il n'y aura pas d'ambiguité, nous noterons

$$R_s(A_1, \dots, A_s; M) = R_s(M).$$

Définition 1. Soit un entier $l \ge 0$. On appelle *fraction de Farey* à l'ordre l toute fraction rationnelle G/H telle que :

(i) H est un polynôme unitaire de degré $\le l$,
(ii) G et H sont des polynômes premiers entre eux,
(iii) $\deg G < \deg H$.

Si G/H est une fraction de Farey à l'ordre l, on appelle *arc de Farey* à l'ordre l de centre G/H la boule

$$\mathcal{U}_{G/H,l} = \{t \in \mathcal{P};\ v(t - G/H) > l + \deg H\}.$$

On désigne par $\mathcal{F}_l$ l'ensemble des fractions de Farey à l'ordre l. On a alors :

Proposition III.2 ([14]). *Soit un entier $l \ge 0$. Lorsque G/H décrit $\mathcal{F}_l$, les arcs de Farey $\mathcal{U}_{G/H,l}$ forment une partition de $\mathcal{P}$.*

Une telle partition est appelée la *dissection de Farey* à l'ordre l.

Dans ce qui suit nous utiliserons deux dissections de Farey. La deuxième sera définie au chapitre VI. La première est une dissection de Farey à l'ordre

$$N = 2n - 4r, \tag{III.9}$$

où

$$r = [n^{1/3}]. \tag{III.10}$$

Nous noterons $\mathcal{U}_{G/H}$ l'arc de Farey $\mathcal{U}_{G/H,N}$. Les arcs de Farey $\mathcal{U}_{G/H}$ tels que $\deg H \le 4r$ seront dits *majeurs*. Soit $\mathcal{M}$ leur réunion. Les arcs restants

sont répartis en deux catégories définies comme suit : Posons, pour tout $i = 1, \dots, s$,

$$H_i^* = \frac{H}{(H, A_i)}, \qquad A_i^* = \frac{A_i}{(H, A_i)}. \tag{III.11}$$

Les arcs de Farey de centre G/H où $\deg H > 4r$ et où pour tout $i = 1, \dots, s$ $\deg H_i^* \le 4r$ seront dits *arcs médians*. Notons $\mathcal{M}_1'$ leur réunion. Sur les arcs majeurs comme sur les arcs médians, on a une bonne approximation des fonctions $f_i(t)$. Enfin les arcs de Farey de centre G/H pour lesquels existe $i \in \{1, \dots, s\}$ tel que $\deg H_i^* > 4r$ seront dits *arcs mineurs*. Notons $\mathcal{M}_2'$ leur réunion.

Soit

$$I_{G/H}(M) = \int\limits_{\mathcal{U}_{G/H}} F(t)E(-Mt)\,dt. \tag{III.12}$$

La somme

$$\int\limits_{\mathcal{M}} F(t)E(-Mt)\,dt = \sum_{\substack{H \in \mathbb{M} \\ \deg H \le 4r}} \sum_{G \in \mathcal{C}_H^*} I_{G/H}(M)$$

donnera de bonne approximation de $R_s(M)$. Le calcul de cette somme fait apparaître les premiers termes d'une série singulière $\mathfrak{S}_s(M)$ qui sera étudiée au paragraphe suivant.

Posons

$$R^+(M) = \int\limits_{\mathcal{M}} F(t)E(-Mt)\,dt, \tag{III.13}$$

$$R_1^-(M) = \int\limits_{\mathcal{M}_1'} F(t)E(-Mt)\,dt, \tag{III.14}$$

$$R_2^-(M) = \int\limits_{\mathcal{M}_2'} F(t)E(-Mt)\,dt. \tag{III.15}$$

Convenons que, sans indications supplémentaires, les constantes contenues dans les symboles $\ll$ et $\gg$ ne dépendront que de q, s et $A_1, \dots, A_s$ ou seront absolues.

IV. Les séries singulières. Dans ce paragraphe, M est un polynôme fixé. On pose, pour tout polynôme unitaire H et pour G premier à H

$$S(H, G) = \sum_{R \in \mathcal{C}_H^*} E\left(\frac{G}{H} R^2\right), \tag{IV.1}$$

$$T(H, G) = \prod_{i=1}^{s} S(H, GA_i). \tag{IV.2}$$

Si H est un polynôme non nul, on pose

$$A_s(H,M)=\Phi(H)^{-s}\sum_{G\in\mathcal{C}_H^*}T(H,G)E\Big(-M\,\frac{G}{H}\Big). \tag{IV.3}$$

PROPOSITION IV.1. *Soient $P_1,\dots,P_r$ des polynômes irréductibles unitaires et $k_1,\dots,k_r$ des entiers naturels. Alors, pour tout polynôme A, on a*

$$S\Big(\prod_{i=1}^r P_i^{k_i},A\Big)=\prod_{i=1}^r S\Big(P_i^{k_i},\,A\prod_{j=1,\,j\neq i}^r P_j^{k_j}\Big). \tag{IV.4}$$

Démonstration. C'est la proposition III.2 de [5].

PROPOSITION IV.2. *Soient P un polynôme irréductible, G un polynôme premier à P. Alors on a :*

(i) *Pour tout entier $l\geq 2$,*

$$S(P^l,G)=0. \tag{IV.5}$$

(ii)

$$|S(P,G)|\leq 1+|P|^{1/2}. \tag{IV.6}$$

(iii) *Si B est un polynôme non nul, $v=v_P(B)$, $B^*=B/P^v$ et si k est un entier ≥ 0,*

$$S(P^k,B)=\begin{cases}\Phi(P)^k & \text{si } k\leq v,\\ |P|^v S(P^{k-v},B^*) & \text{si } k>v.\end{cases} \tag{IV.7}$$

Démonstration. (i) et (ii) sont les propositions V.2 et V.3 de [2], et (iii) se démontre comme (iii) de la proposition de [5].

LEMME 1 ([4, lemme, p. 14]). *Pour tout réel $\theta>1$, pour tout réel $\varepsilon>0$, il existe une constante $a=a(q,\theta,\varepsilon)$ telle que, pour tout polynôme H sans facteur carré, on ait*

$$\theta^{\omega(H)}\leq a(q,\theta,\varepsilon)|H|^{\varepsilon}, \tag{IV.8}$$

où $\omega(H)$ est le nombre de facteurs irréductibles de H.

COROLLAIRE 1. *Soit ε un réel positif. Soient H un polynôme unitaire et A un polynôme quelconque. Alors, pour tout polynôme G premier à H, on a*

$$|S(H,GA)|\ll |H|^{1/2+\varepsilon}, \tag{IV.9}$$

où la constante intervenant dans le symbole $\ll$ ne dépend que de q, ε et A.

Démonstration. Le résultat se déduit à l'aide des relations (IV.4)–(IV.8).

PROPOSITION IV.3. *La fonction $H\mapsto A_s(H,M)$ est multiplicative.*

Démonstration. Immédiate.

PROPOSITION IV.4. *Soit H un polynôme avec facteur carré. Alors*

$$A_s(H, M) = 0. \tag{IV.10}$$

Démonstration. Soit P un polynôme irréductible tel que P^2 divise H. Puisque $A_1, \dots, A_s$ sont premiers entre eux, il existe $i \in \{1, \dots, s\}$ tel que P ne divise pas A_i. D'après les relations (IV.2) et (IV.5) on a $T(P^{v_P(H)}, G) = 0$, d'où avec (IV.3), $A_s(P^{v_P(H)}, M) = 0$ et par multiplicativité $A_s(H, M) = 0$.

Pour tout polynôme irréductible P, on pose

$$\Psi_s(P, M) = 1 + A_s(P, M). \tag{IV.11}$$

On désigne par $\mathcal{N}_s(P, M)$ le nombre de solutions $(M_1, \dots, M_s)$ de la congruence

$$M \equiv A_1 M_1^2 + \dots + A_s M_s^2 \pmod{P}$$

telles que $M_1, \dots, M_s$ soient non nuls modulo P.

PROPOSITION IV.5. *Soit P un polynôme irréductible. Alors on a*

$$\Phi(P)^s \Psi_s(P, M) = |P| \mathcal{N}_s(P, M). \tag{IV.12}$$

Démonstration. D'après (IV.1)–(IV.3) et (III.2),

$$\begin{aligned}
\Phi(P)^s A_s(P, M) &= \sum_{G \in \mathcal{C}_P^*} \prod_{i=1}^{s} \Big(\sum_{R \in \mathcal{C}_P^*} E\Big(\frac{G A_i}{P} R^2\Big)\Big) E\Big(-M \frac{G}{P}\Big) \\
&= \sum_{R_1, \dots, R_s \in \mathcal{C}_P^*} \sum_{G \in \mathcal{C}_P^*} E\Big(\frac{G}{P}(A_1 R_1^2 + \dots + A_s R_s^2 - M)\Big) \\
&= \sum_{R_1, \dots, R_s \in \mathcal{C}_P^*} \Big(\sum_{G \in \mathcal{C}_P} \Big(\frac{G}{P}(A_1 R_1^2 + \dots + A_s R_s^2 - M)\Big) - 1\Big) \\
&= |P| \mathcal{N}_s(P, M) - \Phi(P)^s.
\end{aligned}$$

L'étude des congruences modulo un polynôme irréductible P revient à étudier des équations dans un corps fini à $|P|$ éléments. Le résultat dont on a besoin est donné par la proposition suivante :

PROPOSITION IV.6. *Soit un entier $m \geq 3$. Soient $b_1, \dots, b_m$ des éléments non nuls du corps $\mathbb{F}_q$. Pour tout $b \in \mathbb{F}_q$, soit*

$$r_m^*(b) = r^*(b_1, \dots, b_m; b)$$

le nombre de solutions $(x_1, \dots, x_m) \in (\mathbb{F}_q^*)^m$ de l'équation

$$b = b_1 x_1^2 + \dots + b_m x_m^2.$$

Alors, on a

$$|q r_m^*(b) - (q-1)^m| \leq (q-1)(1 + \sqrt{q})^m. \tag{IV.13}$$

Démonstration. Pour $t \in \mathbb{F}_q$, posons

$$\sigma^*(t) = \sum_{x \in \mathbb{F}_q^*} \Psi(tx^2).$$

Alors on a

$$qr_m^*(b) = \sum_{t \in \mathbb{F}_q} \Psi(-tb) \prod_{i=1}^{m} \sigma^*(tb_i),$$

d'où

$$qr_m^*(b) = \sigma^*(0)^m + \sum_{t \in \mathbb{F}_q^*} \Psi(-tb) \prod_{i=1}^{m} \sigma^*(tb_i).$$

On déduit de la relation (5.9) de [16] que $|\sigma^*(tb_i)| \le 1 + \sqrt{q}$ pour tout t non nul, ce qui donne

$$|qr_m^*(b) - (q-1)^m| \le (q-1)(1+\sqrt{q})^m.$$

PROPOSITION IV.7. (i) *Pour $q \ge 5$ et $m \ge 4$, et tout $b \in \mathbb{F}_q$, on a*

$$r_m^*(b) > 0. \tag{IV.14}$$

(ii) *Pour $q = 7$ et $q > 9$, et tout $b \in \mathbb{F}_q$, on a*

$$r_3^*(b) > 0. \tag{IV.15}$$

Démonstration. (i) D'après (IV.13)

$$qr_m^*(b) \ge (q-1)^m - (q-1)(1+\sqrt{q})^m.$$

Si $q \ge 7$ et $m \ge 4$, le membre droit est > 0. Si $q = 5$, on montre directement que $r_4^*(b) > 0$, et par suite $r_m^*(b) > 0$ pour tout $m \ge 4$.

(ii) Si $q > 9$, on déduit de (IV.13) que $r_3^*(b) > 0$. Si $q = 7$, on le démontre directement.

COROLLAIRE 2. *Soit s un entier supérieur ou égal à 5 et P un polynôme irréductible. Alors*,

$$\Psi_s(P, M) \ge \Phi(P)^{-s}((|P|-1)^{s-1} - (|P|-1)(1+|P|^{1/2})^{s-1}). \tag{IV.16}$$

Démonstration. On remarque que si P ne divise aucun des polynômes $A_1, \dots, A_s$ alors

$$\mathcal{N}_s(P, M) = r_s^*(\overline{A}_1, \dots, \overline{A}_s; \overline{M}),$$

où pour tout polynôme Y de $\mathbb{F}_q[X]$, $\overline{Y}$ désigne la classe de Y modulo P. Si P divise l'un des polynômes $A_1, \dots, A_s$, soit par exemple A_s, on a

$$\mathcal{N}_s(P, M) = r_{s-1}^*(\overline{A}_1, \dots, \overline{A}_{s-1}; \overline{M}).$$

La relation (IV.16) se déduit alors de (IV.13).

PROPOSITION IV.8. *Soit P un polynôme irréductible. Alors on a*

$$|A_s(P,M)| \le \left(\frac{2|A_s|^{1/2}q}{q-1}\right)^s |P|^{1-s/2}. \tag{IV.17}$$

Démonstration. Conséquence des relations (IV.3), (IV.6) et (IV.7).

PROPOSITION IV.9. (i) *Pour $s \ge 5$, la série*

$$\mathfrak{S}_s(M) = \sum_{H\in\mathbb{M}} A_s(H,M) \tag{IV.18}$$

est absolument convergente, et on a

$$\mathfrak{S}_s(M) = \prod_{P\in I} \Psi_s(P,M). \tag{IV.19}$$

De plus, pour tout entier $t \ge 0$ et tout $\varepsilon \in]0,1/2[$, on a

$$\sum_{\substack{H\in\mathbb{M}\\ \deg H>t}} |A_s(H,M)| \ll q^{t(\varepsilon+2-s/2)}, \tag{IV.20}$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q, s, ε, $A_1,\dots,A_s$.

(ii) *Il existe des constantes $a_1 = a_1(q,s,A_1,\dots,A_s)$, $a_2 = a_2(q,s,A_1,\dots,A_s)$, strictement positives, telles que*

$$a_1 \le \mathfrak{S}_s(M) \le a_2. \tag{IV.21}$$

Démonstration. Soit H un polynôme sans facteur carré. D'après (IV.17),

$$(*)\quad |A_s(H,M)| \le \Phi(H)^{-s} \sum_{G\in\mathcal{C}_H^*} |T(H,G)| \le \left(\frac{2|A_s|^{1/2}q}{q-1}\right)^{s\omega(H)} |H|^{1-s/2}.$$

D'après le lemme précédent, pour tout nombre réel $\varepsilon > 0$,

$$(**)\qquad |A_s(H,M)| \le \Phi(H)^{-s} \sum_{G\in\mathcal{C}_H^*} |T(H,G)| \ll |H|^{\varepsilon+1-s/2},$$

la constante impliquée par $\ll$ ne dépendant que de $q,s,\varepsilon,A_1,\dots,A_s$. La relation (IV.20) s'en déduit. Ceci prouve que la série $\mathfrak{S}_s(M)$ est absolument convergente. La fonction $H \mapsto A_s(M,H)$ étant multiplicative, la somme $\mathfrak{S}_s(M)$ s'écrit comme produit eulérien absolument convergent, d'où (IV.19).

Les relations (IV.11) et (IV.17) nous donnent

$$1 - \left(\frac{2|A_s|^{1/2}q}{q-1}\right)^s |P|^{1-s/2} \le \Psi_s(P,M) \le 1 + \left(\frac{2|A_s|^{1/2}q}{q-1}\right)^s |P|^{1-s/2}.$$

Le produit

$$\prod_{P\in I} \left(1 + \left(\frac{2|A_s|^{1/2}q}{q-1}\right)^s |P|^{1-s/2}\right)$$

est convergent. Soit a_2 ce produit. On a ainsi la deuxième inégalité de (IV.21).

Soit

$$d = \frac{2s\log\left(\frac{2|A_s|^{1/2}q}{q-1}\right)}{(s-2)\log q}.$$

Si P est un polynôme irréductible tel que $\deg P > d$, on a $\Psi_s(P,M) > 0$. Le produit

$$\gamma_s(q,A_s) = \prod_{P\in I,\,\deg P>d}\left(1-\left(\frac{2|A_s|^{1/2}q}{q-1}\right)^s|P|^{1-s/2}\right)$$

est convergent et strictement positif. On a

$$\mathfrak{S}_s(M) \geq \gamma_s(q,A_s)\prod_{P\in I,\,\deg P\leq d}\Psi_s(P,M).$$

On pose

$$a_1 = \gamma_s(q,A_s)\prod_{P\in I,\,\deg P\leq d}\Phi(P)^{-s}((|P|-1)^{s-1}-(|P|-1)(1+|P|^{1/2})^{s-1})$$

et la relation (IV.16) nous donne alors la première inégalité de (IV.21).

V. Estimation de $f_i(t)$. On peut déduire l'estimation de $f_i(t)$ de l'estimation de $f(t)$ définie par

$$f(t) = \sum_{P\in I,\,\deg P\leq m} E(tAP^2), \tag{V.1}$$

où m est un entier non nul et A un polynôme non nul.

Les théorèmes de répartition des nombres premiers dans les progressions arithmétiques se généralisent aux polynômes de $\mathbb{F}_q[X]$. On a les théorèmes suivants établis dans [15].

THÉORÈME 1. *Soit, pour tout entier $k>0$, $\pi(k)$ le nombre de polynômes irréductibles unitaires de degré k de $\mathbb{F}_q[X]$. Alors,*

$$q^k - 2q^{k/2} \leq k\pi(k) \leq q^k.$$

THÉORÈME 2. *Soit, pour tout entier $k>0$, tout polynôme unitaire $H\neq 1$ et tout polynôme unitaire R premier à H, $\Pi(k,H,R)$ le nombre de polynômes unitaires irréductibles de degré k de $\mathbb{F}_q[X]$ congrus à R modulo H. Alors,*

$$\left|\Pi(k,H,R) - \frac{q^k}{k\Phi(H)}\right| \leq \deg H\,\frac{q^{k/2}}{k}.$$

THÉORÈME 3. *Soit, pour tout entier $k>0$, tout polynôme unitaire H, tout entier $l\geq 0$ tel que $l+\deg H\geq 1$, tout polynôme unitaire R premier*

à H, $\Pi(k,H,l,R)$ le nombre de polynômes unitaires irréductibles P de $\mathbb{F}_q[X]$ de degré k, congrus à R modulo H et tels que

$$\deg(X^{\deg P}R - X^{\deg R}P) < \deg P + \deg R - l.$$

Alors,

$$\left|\Pi(k,H,l,R) - \frac{q^{k-l}}{k\Phi(H)}\right| \le (l + \deg H + 1)\,\frac{q^{k/2}}{k}.$$

Ce dernier théorème correspond à une partition des polynômes unitaires irréductibles suivant les différents restes modulo H, et les différents systèmes $(a_{k-1},\dots,a_{k-l})$ possibles, pour les coefficients des l termes de plus haut degré.

LEMME 2. *Soit, pour tout polynôme A non nul, $D(A)$ le nombre de diviseurs unitaires de A. Alors, pour tout $\delta > 0$ il existe une constante $c_1 = c_1(\delta)$ telle que*

$$D(A) \le c_1|A|^{\delta}. \tag{V.2}$$

Démonstration. Semblable à celle du lemme V.1, chap. IV de [1].

Rappelons ici que l'on a divisé l'ideal $\mathcal{P}$ par une dissection de Farey à l'ordre $N = 2n - 4r$, les entiers n et r vérifiant les relations (III.3), (III.4) et (III.5). Soit A un polynôme non nul et soit a son degré.

PROPOSITION V.1. *Soit h un entier $< m$. Soit $t = u + G/H$ appartenant à un arc de Farey de centre G/H où $\deg H < h$. Alors*,

$$\left|f(t) - \frac{S(H,GA)}{\Phi(H)}\sum_{k=1}^{m}\frac{q^k}{k}\,\Gamma_k^{\mathrm{sgn}(A)}(u)\right| \ll r|H|\,\frac{q^{5m/2-v(u)}}{m} + \frac{q^h}{h}, \tag{V.3}$$

où pour tout $\alpha \in \mathbb{F}_q^*$,

$$\Gamma_k^{\alpha}(u) = \begin{cases} 1 & \text{si } v(u) > a + 2k + 1,\\ \Psi(\alpha\,\mathrm{sgn}(u)) & \text{si } v(u) = a + 2k + 1,\\ 0 & \text{si } v(u) \le a + 2k, \end{cases} \tag{V.4}$$

la constante intervenant dans le symbole $\ll$ ne dépendant que de q et A.

Démonstration. Dans ce qui suit, les constantes impliquées dans $\ll$ ne dépendront que de q et de A.

On a

$$f(t) = \sum_{\substack{P\in I\\ \deg P<h}} E(tAP^2) + \sum_{\substack{P\in I\\ h\le\deg P\le m}} E(tAP^2).$$

Posons

$$f'(t) = \sum_{\substack{P\in I\\ h\le\deg P\le m}} E(tAP^2).$$

Alors,

$$|f(t) - f'(t)| \ll q^h/h, \tag{1}$$

où la constante intervenant dans $\ll$ ne dépend que de q. On a

$$f'(t) = \sum_{k=h}^{m} \sum_{\substack{P\in I\\ \deg P=k}} E(tAP^2) = \sum_{k=h}^{m} g_k(t).$$

Soit $k \in \{h, \dots, m\}$. Soit $l = l(k) = 2k - v(u) + a + 1$. Sur l'ensemble des polynômes unitaires $\mathbb{M}$, on définit la relation d'equivalence $R_{H,l}$ comme suit : Pour tout $Y, Z \in \mathbb{M}$,

$$Y \equiv Z \bmod R_{H,l} \;\Leftrightarrow\; \begin{cases} \text{(i) } Y \equiv Z \bmod H, \\ \text{(ii) } \deg(YX^{\deg Z} - ZX^{\deg Y}) < \deg(YZ) - l. \end{cases}$$

D'après la proposition III.1, si $\deg Y = \deg Z = k$ alors

$$Y \equiv Z \bmod R_{H,l} \;\Rightarrow\; E(tAY^2) = E(tAZ^2). \tag{2}$$

Si $l \le 0$, les classes modulo $R_{H,l}$ sont les classes de congruences modulo H. Pour $l > 0$, soit $\mathcal{S} = \{R + T^w HY;\ R \in \mathcal{C}_H,\ Y \in \mathbb{M}_l,\ w = k - l - \deg H\}$. D'après [4, proposition IX.1], $\mathcal{S}$ est un système de représentants de l'ensemble des polynômes unitaires irréductibles de degré k modulo $R_{H,l}$.

Supposons $l \le 0$, i.e. $v(u) \ge 2k + a + 1$. Comme $\deg H < h \le \deg P$ alors $(P, H) = 1$. On a

$$\begin{aligned} g_k(t) &= \sum_{R\in\mathcal{C}_H^*} \sum_{\substack{P\in I,\,\deg P=k\\ P\equiv R \bmod H}} E\left(\left(u + \frac{G}{H}\right)AP^2\right) \\ &= \sum_{R\in\mathcal{C}_H^*} E\left(\frac{G}{H}\,AR^2\right) \sum_{\substack{P\in I,\,\deg P=k\\ P\equiv R \bmod H}} E(uAP^2). \end{aligned}$$

Pour $v(u) > 2k + a + 1$,

$$g_k(t) = \sum_{R\in\mathcal{C}_H^*} E\left(\frac{G}{H}\,AR^2\right) \Pi(k, H, R).$$

Pour $v(u) = 2k + a + 1$,

$$g_k(t) = \Psi(\operatorname{sgn}(uA)) \sum_{R\in\mathcal{C}_H^*} E\left(\frac{G}{H}\,AR^2\right) \Pi(k, H, R).$$

Supposons $l > 0$, i.e. $v(u) < 2k + a + 1$. D'après l'implication (2), on a

$$g_k(t) = \sum_{\substack{K\in\mathcal{S}\\ (H,K)=1}} E(tAK^2) \Pi(k, H, l, K).$$

Le théorème 3 donne alors

$$\left|g_k(t) - \frac{q^{k-l}}{k\Phi(H)} \sum_{\substack{K\in\mathcal{S}\\(H,K)=1}} E(tAK^2)\right| \le (l+\deg H+1)\,\frac{q^{k/2}}{k} \sum_{\substack{K\in\mathcal{S}\\(H,K)=1}} 1$$
$$\le (l+\deg H+1)\Phi(H)q^l\,\frac{q^{k/2}}{k}.$$

Calculons maintenant

$$\sum_{\substack{K\in\mathcal{S}\\(H,K)=1}} E(tAK^2) = \sum_{R\in\mathcal{C}_H^*} E\left(\frac{G}{H}\,AR^2\right) \sum_{Y\in\mathbb{M}_l} E(uA(X^wHY)^2).$$

Soit $Y\in\mathbb{M}_l$, $y\in\mathcal{P}$. On a

$$v(uA(X^wH)^2(Y^2-(Y+y)^2)) \ge 2,$$

d'où

$$\sum_{Y\in\mathbb{M}_l} E(uA(X^wHY)^2) = \sum_{Y\in\mathbb{M}_l} \int_{\mathcal{P}} E(uA(X^wH)^2(Y+y)^2)\,dy$$
$$= \int_{\substack{\mathrm{sgn}(y)=1\\v(y)=-l}} E(uA(X^wHy)^2)\,dy.$$

Soit y tel que $\mathrm{sgn}(y)=1$ et $v(y)=-l$. Alors $y^2=T^{2l}+z$ avec $v(z)>-2l$. Ainsi,

$$q^l \sum_{Y\in\mathbb{M}_l} E(uA(X^wHY)^2) = E(uA(X^wHX^l)^2) \int_{v(z)>-2l} E(uAX^{2w}H^2z)\,dz = 0,$$

puisque $v(uAX^{2w}H^2)\le 2l$. Avec le théorème 2, on conclut que

$$\left|f'(t) - \frac{S(H,GA)}{\Phi(H)} \sum_{k=h}^{m} \frac{q^k}{k}\,\Gamma_k^{\mathrm{sgn}(A)}(u)\right|$$
$$\le \deg H|S(H,GA)| \sum_{k=h}^{m} \frac{q^{k/2}}{k} + \Phi(H) \sum_{k=h}^{m} \frac{q^{k/2+l(k)}}{k}\,(l(k)+\deg H+1)$$
$$\ll \deg H\,\Phi(H)\,\frac{q^{m/2}}{m} + r\Phi(H)\,\frac{q^{5m/2-v(u)}}{m}$$
$$\ll r|H|\,\frac{q^{5m/2-v(u)}}{m},$$

d'où avec (2)

$$\left|f(t) - \frac{S(H,GA)}{\Phi(H)} \sum_{k=1}^{m} \frac{q^k}{k}\,\Gamma_k^{\mathrm{sgn}(A)}(u)\right| \ll r|H|\,\frac{q^{5m/2-v(u)}}{m} + \frac{q^h}{h}.$$

PROPOSITION V.2. *Soit $t = G/H + u$ appartenant à un arc de Farey de centre G/H où $\deg H \le 4r + a_i$. Alors,*

$$\left| f_i(t) - \frac{S(H, GA_i)}{\Phi(H)}\, f_i^*(u) \right| \ll r|H|\, \frac{q^{5m_i/2 - v(u)}}{m_i} + \frac{q^{4r}}{r}, \tag{V.5}$$

où

$$f_i^*(u) = \begin{cases} \tau_{m_i} & \text{si } v(u) \ge 2m_i + a_i + 2, \\ \tau_j & \text{si } v(u) = 2(j+1) + a_i \\ & \quad \text{avec } j \le m_i - 1, \\ \tau_{j-1} + \frac{q^j}{j}\sigma^*(\operatorname{sgn}(u)\alpha_i) & \text{si } v(u) = 2j + a_i + 1, \\ & \quad \text{avec } j \le m_i \end{cases} \tag{V.6}$$

et pour tout $t \in \mathbb{F}_q$,

$$\sigma^*(t) = \sum_{y \in \mathbb{F}_q^*} \Psi(ty^2).$$

Démonstration. On a

$$f_i(t) = \sum_{\substack{P \in I^* \\ \deg P \le m_i}} E(tA_iP^2) = \sum_{\alpha \in \mathbb{F}_q^*} \sum_{\substack{P \in I \\ \deg P \le m_i}} E(t\alpha^2 A_i P^2).$$

Compte tenu de l'inégalité (III.4) vérifiée par n, on a $4r + a_i + 1 \le m_i$, on peut donc appliquer la proposition précédente avec $A = A_i$, $h = 4r + a_i + 1$ et on a

$$\left| f_i(t) - \sum_{k=1}^{m_i} \frac{q^k}{k} \sum_{\alpha \in \mathbb{F}_q^*} \frac{S(H, G\alpha^2 A_i)}{\Phi(H)}\, \Gamma_k^{\alpha^2 \alpha_i}(u) \right| \ll 4r|H|\, \frac{q^{5m_i/2 - v(u)}}{m_i} + \frac{q^{4r}}{r}.$$

L'application $Y \mapsto \alpha Y$ étant une bijection de $\mathcal{C}_H^*$ sur $\mathcal{C}_H^*$, on a alors

$$\sum_{R \in \mathcal{C}_H^*} E\left(\frac{A_i G(\alpha R)^2}{H}\right) = \sum_{Y \in \mathcal{C}_H^*} E\left(\frac{A_i G Y^2}{H}\right),$$

d'où

$$S(H, G\alpha^2 A_i) = S(H, GA_i).$$

Posons

$$\lambda_k(u) = \sum_{\alpha \in \mathbb{F}_q^*} \Gamma_k^{\alpha^2 \alpha_i}(u).$$

Alors

$$\lambda_k(u) = \begin{cases} q - 1 & \text{si } v(u) > 2k + a_i + 1, \\ \sum_{\alpha \in \mathbb{F}_q^*} \Psi(\operatorname{sgn}(u)\alpha_i \alpha^2) & \text{si } v(u) = 2k + a_i + 1, \\ 0 & \text{si } v(u) \le 2k + a_i. \end{cases}$$

Ainsi

$$\left| f_i(t) - \frac{S(H, GA_i)}{\Phi(H)} \sum_{k=1}^{m_i} \frac{q^k}{k} \lambda_k(u) \right| \ll 4r|H| \, \frac{q^{5m_i/2 - v(u)}}{m_i} + \frac{q^{4r}}{r}.$$

Calculons maintenant $\sum_{k=1}^{m_i} \frac{q^k}{k} \lambda_k(u)$.

• Si $v(u) > a_i + 2m_i + 1$, on a pour tout k intervenant dans la somme ci-dessus, $v(u) > a_i + 2k + 1$, $\lambda_k(u) = q - 1$ et

$$\sum_{k=1}^{m_i} \frac{q^k}{k} \lambda_k(u) = \tau_{m_i}.$$

• Si $v(u) \leq a_i + 2m_i + 1$, il existe j tel que $a_i + 2j + 1 \leq v(u) \leq a_i + 2(j+1)$, alors

$$\sum_{k=1}^{m_i} \frac{q^k}{k} \lambda_k(u) = \sum_{k=1}^{j} \frac{q^k}{k} \lambda_k(u) + \sum_{k=j+1}^{m_i} \frac{q^k}{k} \lambda_k(u).$$

Or $\lambda_k(u) = 0$ pour $k = j+1, \ldots, m_i$. Ainsi

$$\sum_{k=1}^{m_i} \frac{q^k}{k} \lambda_k(u) = \sum_{k=1}^{j} \frac{q^k}{k} \lambda_k(u).$$

Pour $v(u) > a_i + 2j + 1$,

$$\sum_{k=1}^{j} \frac{q^k}{k} \lambda_k(u) = \tau_j.$$

Pour $v(u) = a_i + 2j + 1$,

$$\sum_{k=1}^{j} \frac{q^k}{k} \lambda_k(u) = \sum_{k=1}^{j-1} \frac{q^k}{k} \lambda_k(u) + \frac{q^j}{j} \lambda_j(u) = \tau_{j-1} + \frac{q^j}{j} \sigma^*(\mathrm{sgn}(u)\alpha_i).$$

On a le résultat annoncé en posant

$$f_i^*(u) = \sum_{k=1}^{m_i} \frac{q^k}{k} \lambda_k(u).$$

VI. Majoration de $R_2^-(M)$. La majoration de $R_2^-(M)$ nécessite l'introduction d'une fonction auxiliaire H que l'on va définir.

Soient $i < j$ des entiers pris parmi les s premiers entiers. On désigne par $Y(A_i, A_j)$ le nombre de solutions $(Y_i, Y_j, Z_i, Z_j) \in (\mathbb{F}_q[X])^4$ de l'equation

$$A_i Y_i^2 - A_i Z_i^2 = A_j Z_j^2 - A_j Y_j^2$$

telles que $\deg Y_i, \deg Z_i \leq m_i$ et $\deg Y_j, \deg Z_j \leq m_j$. On pose

$$N_j = a_j + m_j. \tag{VI.1}$$

On pose aussi, pour $t \in \mathcal{P}$, $k \in \{i, j\}$,

$$h_k(t) = \sum_{\deg Y \le m_k} E(tA_kY^2), \tag{VI.2}$$

$$H(t) = |h_i(t)|^2 |h_j(t)|^2; \tag{VI.3}$$

alors, d'après la proposition III.1,

$$Y(A_i, A_j) = \int_{\mathcal{P}} H(t)\, dt.$$

On fait une dissection de Farey de $\mathcal{P}$ à l'ordre N_j. On notera $\mathcal{V}_{G/K}$ l'arc de Farey $\mathcal{U}_{G/K,N_j}$. On appelle $\mathcal{P}_1$ la réunion des arcs de Farey $\mathcal{V}_{G/K}$ tels que $\deg K \le m_j$, $\mathcal{P}_2$ la réunion des arcs restants. On pose

$$Q_1 = \int_{\mathcal{P}_1} H(t)\, dt, \tag{VI.4}$$

$$Q_2 = \int_{\mathcal{P}_2} H(t)\, dt. \tag{VI.5}$$

Proposition VI.1. *Soit G/K une fraction de Farey telle que* $\deg K \le m_j$. *Posons*

$$J_{G/K} = \int_{\mathcal{V}_{G/K}} H(t)\, dt.$$

Alors

(i)

$$J_{G/K} \ge 0. \tag{VI.6}$$

(ii)

$$J_{G/K} \ll 2|K|^{-4} |C(K, GA_i)|^2 |C(K, GA_j)|^2 q^{2n}, \tag{VI.7}$$

où

$$C(K, G) = \sum_{R \in \mathcal{C}_K} E\Big(\frac{GR^2}{K}\Big).$$

Démonstration. Puisque H est une fonction positive, le (i) est évident.

Supposons que $2m_j + a_j > 2m_i + a_i$. Le corollaire VI.3 de [5] donne, pour $k = i, j$,

$$|h_k(t)|^2 = |K|^{-2} |h_k'(u)|^2 |C(K, GA_k)|^2,$$

avec

$$h_k'(u) = \begin{cases} q^{m_k+1} & \text{si } v(uA_k) \ge 2m_k + 2, \\ q^k & \text{si } v(uA_k) = 2k \le 2m_k, \\ q^k \sigma(\operatorname{sgn}(uA_k)) & \text{si } v(u) = 2k+1 \le 2m_k + 1. \end{cases}$$

On a donc

$$H(t) = |K|^{-4}|C(H, GA_i)|^2|C(H, GA_j)|^2 H'(u),$$

où $H'(u) = |h_i'(u)|^2|h_j'(u)|^2$. Comme $H'(u)$ dépend uniquement de $v(u)$ et $\operatorname{sgn}(u)$, on pose $H'(u) = \phi(v(u), \operatorname{sgn}(u))$. On a

$$J_{G/K} = |K|^{-4}|C(K, GA_i)|^2|C(K, GA_j)|^2 I,$$

avec

$$\begin{aligned} I &= \int\limits_{v(u)\geq 2m_j+a_j+2} H'(u)\,du + \sum_{l=N_j+\deg K+1}^{2m_j+a_j+1} \sum_{c\in\mathbb{F}_q^*} \phi(l,c) \int\limits_{v(u)>l} du \\ &= q^{2m_i-a_j+3} + \sum_{l=N_j+\deg K+1}^{2m_j+a_j+1} L_l, \end{aligned}$$

où

$$L_l = q^{-l} \sum_{c\in\mathbb{F}_q^*} \phi(l,c).$$

On déduit de la relation (5.9) de [16] que $|\sigma(\alpha)|^2 = |\sum_{t\in\mathbb{F}_q} \Psi(\alpha t^2)|^2 = q$ pour tout $\alpha \in \mathbb{F}_q^*$; alors $0 \leq \phi(l,c) \leq q^{2l}$, donc $I \leq 2q^{2m_j+a_j+3}$, d'où le résultat.

Si $2m_i + a_i > 2m_j + a_j$, on procède de façon identique.

Proposition VI.2. *On a*

$$0 \leq Q_1 \ll nq^{2n}. \tag{VI.8}$$

Démonstration. On a

$$Q_1 = \sum_{\deg K\leq m_j} \sum_{G\in\mathcal{C}_K^*} J_{G/K},$$

donc

$$Q_1 \ll q^{2n} \sum_{\deg K\leq m_j} |K|^{-4} \sum_{G\in\mathcal{C}_K^*} |C(K, GA_i)|^2|C(K, GA_j)|^2.$$

D'après les propositions III.2 et III.3 de [5], on a

$$|C(K, GA_i)| \leq |(K, A_i)|^{1/2}|K|^{1/2},$$

d'où

$$Q_1 \ll q^{2n} \sum_{\deg K\leq m_j} |K|^{-2}\Phi(K).$$

Comme $\sum_{\deg K\leq h} |K|^{-2}\Phi(K) \leq \sum_{\deg K\leq h} |K|^{-1} = h + 1$, alors $Q_1 \ll nq^{2n}$.

Proposition VI.3. *On a*

$$Q_2 \ll q^{2n}. \tag{VI.9}$$

Démonstration. Soit $t \in \mathcal{P}_2$. Alors t s'écrit $t = u + G/K$ avec $m_j < \deg K \le N_j$ et $v(u) \ge N_j + \deg K + 1 \ge 2m_j + a_j + 2$. On a donc

$$h_j(t) = \sum_{\deg Y \le m_j} E\left(\frac{GA_j}{K}\, Y^2\right).$$

• Si $\deg K \le m_i$, d'après le corollaire VI.3 de [5], on a

$$h_i(t) = |K|^{-1} h_i'(u) C(K, GA_i).$$

Alors,

$$0 \le |h_i(t)|^2 \le |K|^{-2} |h_i'(u)|^2 |C(K, GA_i)|^2 \le |K|^{-1} |(K, A_i)| q^{2m_i+2}.$$

Ainsi

$$0 \le |h_i(t)|^2 \le |A_i| q^{2m_i - m_j + 1}.$$

• Si $\deg K > m_i$,

$$h_i(t) = \sum_{\deg Y \le m_i} E\left(\frac{GA_i}{K}\, Y^2\right).$$

Majorons donc

$$S_k = \sum_{\deg Y \le m_k} E\left(\frac{GA_k}{K}\, Y^2\right).$$

Comme il a été démontré dans la preuve de la proposition VII.2 de [5] on a

$$|S_k|^2 \le q^{m_k+1} \# \left\{ Y;\, \deg Y < m_k,\, v\left(\left\{ \frac{GA_k}{K}\, Y \right\} > m_k + 1 \right) \right\}.$$

Si $\deg(K/(K, A_k)) \le m_k + 1$, on a

$$|S_k|^2 = q^{2m_k+2} |K|^{-1} |(K, A_k)| \le |A_k| q^{2m_k - m_j + 1}.$$

Si $\deg(K/(K, A_k)) > m_k + 1$, il vient

$$|S_k|^2 \le |K| \le q^{m_j + a_j},$$

soit dans tous les cas

$$|S_k|^2 \le |A_j| q^{2m_i - m_j + 1} \ll q^n,$$

d'où $|H(t)| \ll q^n$ et $\int_{\mathcal{P}_1} |H(t)|\, dt \ll q^n$.

Proposition VI.4. *On a*

$$Y(A_i, A_j) \ll n q^{2n}. \tag{VI.10}$$

Démonstration. On a $\int_{\mathcal{P}} H(t)\, dt = Y(A_i, A_j)$. Donc $Y(A_i, A_j) = Q_1 + Q_2$. On conclut avec les relations (VI.8) et (VI.9).

Proposition VI.5. *On a*

$$R_2^-(M) \ll \frac{q^{n(s-2)}}{n^s}\, (r n^7 \log n\, q^{-r/4}). \tag{VI.11}$$

Démonstration. Soit $t \in \mathcal{M}_2'$. Alors il existe une fraction de Farey G/H et un indice i tels que $t \in \mathcal{U}_{G/H}$, $4r < \deg H \le 2n-4r$ et $\deg H_i^* > 4r$. Comme $v(uA_iP^2) \ge 2$, alors

$$f_i(t) = \sum_{\substack{P\in I^*\\ \deg P\le m_i}} E(tA_iP^2) = \sum_{\substack{P\in I^*\\ \deg P\le m_i}} E\Big(\frac{GA_i}{H_i}\,P^2\Big)$$
$$= \sum_{\substack{P\in I^*\\ \deg P\le m_i}} E\Big(\frac{GA_i^*}{H_i^*}\,P^2\Big).$$

D'après la proposition VII.7 de [3], on a $|f_i(t)| \ll rn\log n\, q^{n-r/4}$. Comme $F(t) = \prod_{j=1}^{s} f_j(t)$, alors

$$|F(t)| \ll \Big(\prod_{j=1,\,j\ne i}^{s} |f_j(t)|\Big) rn\log n\, q^{n-r/4}.$$

Le théorème 1 nous donne $|f_j(t)| \ll q^n/n$. Ainsi

$$|F(t)| \ll |f_{i_1}(t)f_{i_2}(t)f_{i_3}(t)f_{i_4}(t)|rn\log n\, q^{n-r/4}\Big(\frac{q^n}{n}\Big)^{s-5}$$
$$\ll |f_{i_1}(t)f_{i_2}(t)f_{i_3}(t)f_{i_4}(t)|n^{6-s}r\log n\, q^{n(s-4)}q^{-r/4},$$

où i_1, i_2, i_3, i_4 sont des indices distincts et différents de i. Alors

$$\int_{\mathcal{M}_2'} |F(t)|\,dt \ll n^{6-s}r\log n\, q^{n(s-4)-r/4}\cdot L,$$

où

$$L = \int_{\mathcal{P}} |f_{i_1}(t)f_{i_2}(t)f_{i_3}(t)f_{i_4}(t)|\,dt.$$

L'inégalité de Cauchy–Schwarz donne

$$L^2 \le L_{1,2}\cdot L_{3,4}, \quad \text{où} \quad L_{j,k} = \int_{\mathcal{P}} |f_{i_j}(t)f_{i_k}(t)|^2\,dt.$$

Or

$$L_{j,k} = \int_{\mathcal{P}} \sum_{\substack{P,P',Q,Q'\in I^*\\ \deg P,\deg Q\le m_{i_j};\,\deg P',\deg Q'\le m_{i_k}}} E(t(A_{i_j}(P^2-Q^2)+A_{i_k}(P'^2-Q'^2))),$$
$$= Y^*(A_{i_j}, A_{i_k}),$$

où $Y^*(A_{i_j}, A_{i_k})$ est le nombre de solutions $(P, P', Q, Q') \in (I^*)^4$ de l'equation

$$A_{i_j}Y_{i_j}^2 - A_{i_j}Z_{i_j}^2 = A_{i_k}Z_{i_k}^2 - A_{i_k}Y_{i_k}^2$$

telles que $\deg P, \deg Q \le m_{i_j}$ et $\deg P', \deg Q' \le m_{i_k}$. De façon évidente on a $Y^*(A_{i_j}, A_{i_k}) \le Y(A_{i_j}, A_{i_k})$. On conclut à l'aide de la proposition VI.4.

VII. Approximation de $R(M)$. Nous reprenons les hypothèses du paragraphe IV. Notons aussi que pour tout $B \subset \{1,\dots,s\}$, on a

$$\prod_{i\in B}\tau_{m_i} = \prod_{i\in B}\tau_{m_i-1} + \sum_{\substack{I\cup J=B\\ I\cap J=\emptyset,\, J\neq\emptyset}} \prod_{i\in I}\tau_{m_i-1}\prod_{i\in J}\frac{q^{m_i}}{m_i}\,(q-1)^{\#J}.$$

Proposition VII.1. *Soit ε un réel positif. Soit G/H le centre d'un arc de Farey. Alors* :

(i) *Si G/H est le centre d'un arc majeur*,

$$\text{(VII.1)}\qquad \left|I_{G/H}(M) - \frac{T(H,G)}{\Phi(H)^s}\,E\Big(-M\,\frac{G}{H}\Big)(J_s(M)+j_s(H,M))\right| \ll |H|^{(\varepsilon-1/2)(s-1)-1}q^{n(s-5/2)}q^{8r},$$

où

$$\text{(VII.2)}\qquad J_s(M) = \begin{cases} |M|^{-1}\displaystyle\sum_{\substack{I\cup J=\{1,\dots,s\}\\ I\cap J=\emptyset,\, J\neq\emptyset}}\prod_{i\in I}\tau_{m_i-1}\prod_{i\in J}\frac{q^{m_i}}{m_i}\,r_J^*(\mathrm{sgn}(M)) & \\ \qquad\qquad \textit{si } \deg M \equiv a_i \bmod 2 \textit{ pour tout } i=1,\dots,s, & \\ |M|^{-1}q^{-1}\displaystyle\prod_{i\in u(M)}\tau_{m_i}\sum_{\substack{I\cup J=v(M)\\ I\cap J=\emptyset,\, J\neq\emptyset}}\prod_{i\in I}\tau_{m_i-1}\prod_{i\in J}\frac{q^{m_i}}{m_i}\,r_J^*(0) & \\ \quad + |M|^{-1}\displaystyle\prod_{i\in v(M)}\tau_{m_i-1}\sum_{\substack{I\cup J=u(M)\\ I\cap J=\emptyset,\, J\neq\emptyset}}\prod_{i\in I}\tau_{m_i-1}\prod_{i\in J}\frac{q^{m_i}}{m_i}\,r_J^*(\mathrm{sgn}(M)) \quad \textit{sinon}, & \end{cases}$$

et

$$\text{(VII.3)}\qquad |j_s(H,M)| \le \begin{cases} 0 & \textit{si } \deg M = 2n \\ & \textit{ou } \deg M = 2n-1 \textit{ et } \deg H < 4r, \\ |M|^{-1}\displaystyle\prod_{i=1}^{s}\tau_{m_i} & \textit{si } \deg M = 2n-1 \textit{ et } \deg H = 4r, \end{cases}$$

la constante intervenant dans le symbole $\ll$ ne dépendant que de q, s, ε et $A_1,\dots,A_s$.

(ii) *Si G/H est le centre d'un arc médian*,

$$\text{(VII.4)}\qquad |I_{G/H}(M)| \ll \frac{|T(H,G)|}{\Phi(H)^s}\,|H|^{-1}\,\frac{q^{n(s-2)}}{n^s}\,q^{4r}.$$

Démonstration. Soit $t = G/H + u$ appartenant à un arc de Farey $\mathcal{U}_{G/H}$ où $\deg H \le 4r + a_1$. Alors, avec (V.5),

$$F(t) = \prod_{i=1}^{s}\frac{S(H,GA_i)}{\Phi(H)}\,F^*(u) + e(t),$$

où

$$F^*(u)=\prod_{i=1}^{s} f_i^*(u), \qquad e(t)=\sum_{\substack{I\cup J=\{1,\dots,s\}\\ J\neq\emptyset}} \prod_{i\in I} \frac{S(H,GA_i)}{\Phi(H)}\, f_i^*(u)\cdot \prod_{j\in J} e_j(t)$$

et

$$e_i(t)\ll r|H|\,\frac{q^{5n/2-v(u)}}{n}+\frac{q^{4r}}{r}.$$

Or, d'après la proposition V.4 de [4] on a

$$\Phi(H)\gg |H|(\log\deg H)^{-1}.$$

Avec la relation (IV.9), on déduit que

$$\frac{|S(H,GA_i)|}{\Phi(H)}\ll (\log\deg H)|H|^{\varepsilon-1/2},$$

la constante intervenant dans $\ll$ ne dépendant que de q,ε et A_i. D'où

$$\begin{aligned} e(t) &\ll \sum_{\substack{I\cup J=\{1,\dots,s\}\\ J\neq\emptyset}} \left(r|H|^{\varepsilon-1/2}\,\frac{q^n}{n}\right)^{\#I}\left[\left(r|H|\,\frac{q^{5/2}n-v(u)}{n}\right)^{\#J}+\left(\frac{q^{4r}}{r}\right)^{\#J}\right]\\ &\ll \sum_{i=0}^{s-1}\left(r|H|^{\varepsilon-1/2}\,\frac{q^n}{n}\right)^{i}\left[\left(r|H|\,\frac{q^{5/2}n-v(u)}{n}\right)^{s-i}+\left(\frac{q^{4r}}{r}\right)^{s-i}\right]\\ &\ll \left(r|H|^{\varepsilon-1/2}\,\frac{q^n}{n}\right)^{s-1}\left[r|H|\,\frac{q^{5/2}n-v(u)}{n}+\frac{q^{4r}}{r}\right], \end{aligned}$$

où les constantes intervenant dans $\ll$ ne dépendent que de q, s, ε et $A_1,\dots,A_s$. Posons

$$K_s(M)=\int\limits_{v(u)>N+\deg H} F^*(u)E(-Mu)\,du.$$

Alors

$$\begin{aligned} &\left|I_{G/H}(M)-\frac{T(H,G)}{\Phi(H)^s}\,E\!\left(-M\,\frac{G}{H}\right)K_s(M)\right|\\ &\qquad\ll r^s|H|^{(\varepsilon-1/2)(s-1)+1}\,\frac{q^{n(s+3/2)}}{n^s}\int\limits_{v(u)>N+\deg H} q^{-v(u)}\,du\\ &\qquad\quad + r^{s-2}|H|^{(\varepsilon-1/2)(s-1)}\,\frac{q^{(s-1)n}}{n^{s-1}}\cdot\frac{q^{4r}}{r}\,q^{-N-\deg H}\\ &\qquad\ll r^s|H|^{(\varepsilon-1/2)(s-1)-1}\,\frac{q^{n(s-5/2)}}{n^s}\,q^{8r}, \end{aligned}$$

les constantes intervenant dans $\ll$ ne dépendant que de q,s,ε et $A_1,\dots,A_s$.

(i) Supposons que G/H soit le centre d'un arc majeur. Comme F^* ne dépend que de $v(u)$ et de $\operatorname{sgn}(u)$, on pose alors

$$F^*(u) = \phi(\operatorname{sgn}(u), v(u)).$$

On remarque que $F^*(u)$ est constante sur l'ensemble $\{u \in \mathcal{P};\ v(u) > 1+\lambda\}$, où

$$\lambda = \max\{2m_1 + a_1, \dots, 2m_s + a_s\}.$$

D'après (V.6),

$$K_s(M) = \prod_{i=1}^{s} \tau_{m_i} \int\limits_{v(u)>1+\lambda} E(-Mu)\,du + \sum_{j=1+N+\deg H}^{1+\lambda} \sum_{c\in\mathbb{F}_q^*} \phi(j,c) E(-McX^{-j}) \int\limits_{v(u)>j} E(-Mu)\,du,$$

d'où avec (III.1),

$$\begin{aligned} K_s(M) &= q^{-1-\lambda} \prod_{i=1}^{s} \tau_{m_i} + \sum_{j=1+\max(N+\deg H, \deg M)}^{1+\lambda} q^{-j} \sum_{c\in\mathbb{F}_q^*} \phi(j,c) E(-McX^{-j}) \\ &= J_s(M) + j_s(H,M), \end{aligned}$$

où

$$J_s(M) = q^{-1-\lambda} \prod_{i=1}^{s} \tau_{m_i} + \sum_{j=1+\deg M}^{1+\lambda} q^{-j} \sum_{c\in\mathbb{F}_q^*} \phi(j,c) E(-McX^{-j}),$$

$$j_s(H,M) = -\sum_{j=1+\deg M}^{\max(N+\deg H, \deg M)} q^{-j} \sum_{c\in\mathbb{F}_q^*} \phi(j,c) E(-McX^{-j}).$$

Calculons d'abord $J_s(M)$.

(a) Si $\lambda = \deg M$ alors pour tout $i \in \{1, \dots, s\}$, $\deg M = 2m_i + a_i$ et a_i est de même parité que $\deg M$. On applique la définition du caractère E. La relation (V.6) nous donne

$$J_s(M) = q^{-1-\lambda} \prod_{i=1}^{s} \tau_{m_i} + q^{-1-\lambda} \sum_{c\in\mathbb{F}_q^*} \Psi(-c\operatorname{sgn}(M)) \prod_{i=1}^{s} \left(\tau_{m_i-1} + \frac{q^{m_i}}{m_i}\, \sigma(\alpha_i c) \right),$$

d'où

$$J_s(M) = q^{-1-\lambda} \Bigg(\Big(\prod_{i=1}^{s} \tau_{m_i} - \prod_{i=1}^{s} \tau_{m_i-1} \Big) + \sum_{\substack{I\cup J=\{1,\dots,s\} \\ I\cap J=\emptyset,\ J\neq\emptyset}} \prod_{i\in I} \tau_{m_i-1} \prod_{i\in J} \frac{q^{m_i}}{m_i} \left(q r_J^*(\operatorname{sgn}(M)) - (q-1)^{\#J} \right) \Bigg),$$

donc

$$J_s(M) = q^{-\lambda} \sum_{\substack{I\cup J=\{1,\dots,s\}\\ I\cap J=\emptyset,\, J\neq\emptyset}} \prod_{i\in I} \tau_{m_i-1} \prod_{i\in J} \frac{q^{m_i}}{m_i}\, r_J^*(\mathrm{sgn}(M)),$$

ce qui est l'égalité cherchée.

(b) Si $\lambda > \deg M$ alors $\deg M = \lambda - 1$.

• Si $\deg M = 2m_i + a_i$ (i.e. $i \in u(M)$), pour $v(u) = 1+\lambda = 2m_i + a_i + 2$,

$$f_i^*(u) = \tau_{m_i},$$

et pour $v(u) = \lambda = 2m_i + a_i + 1$,

$$f_i^*(u) = \tau_{m_i-1} + \frac{q^{m_i}}{m_i}\,\sigma(\alpha_i c).$$

• Si $\deg M = 2m_i + a_i - 1$ (i.e. $i \in v(M)$), pour $v(u) = 1+\lambda = 2m_i + a_i + 1$,

$$f_i^*(u) = \tau_{m_i-1} + \frac{q^{m_i}}{m_i}\,\sigma(\alpha_i c),$$

et pour $v(u) = \lambda = 2m_i + a_i$,

$$f_i^*(u) = \tau_{m_i}.$$

D'où

$$\begin{aligned} J_s(M) = q^{-1-\lambda} \prod_{i=1}^{s} \tau_{m_i} &+ q^{-1-\lambda} \prod_{i\in u(M)} \tau_{m_i} \sum_{c\in\mathbb{F}_q^*} \prod_{i\in v(M)} \left(\tau_{m_i-1} + \frac{q^{m_i}}{m_i}\,\sigma(\alpha_i c)\right) \\ &+ q^{-\lambda} \prod_{i\in v(M)} \tau_{m_i-1} \sum_{c\in\mathbb{F}_q^*} \prod_{i\in u(M)} \left(\tau_{m_i-1} + \frac{q^{m_i}}{m_i}\,\sigma(\alpha_i c)\right) \\ &\times \Psi(-c\,\mathrm{sgn}(M)), \end{aligned}$$

donc

$$\begin{aligned} J_s(M) = q^{-1-\lambda} \prod_{i=1}^{s} \tau_{m_i} &+ q^{-1-\lambda} \prod_{i\in u(M)} \tau_{m_i} \Bigg((q-1) \prod_{i\in v(M)} \tau_{m_i-1} \\ &+ \sum_{\substack{I\cup J=v(M)\\ I\cap J=\emptyset,\, J\neq\emptyset}} \prod_{i\in I} \tau_{m_i-1} \prod_{i\in J} \frac{q^{m_i}}{m_i}\, q r_J^*(0) - \prod_{i\in v(M)} \tau_{m_i} + \prod_{i\in v(M)} \tau_{m_i-1} \Bigg) \\ &+ q^{-\lambda} \prod_{i\in v(M)} \tau_{m_i-1} \Bigg(- \prod_{i\in u(M)} \tau_{m_i-1} + \sum_{\substack{I\cup J=u(M)\\ I\cap J=\emptyset,\, J\neq\emptyset}} \prod_{i\in I} \tau_{m_i-1} \\ &\times \prod_{i\in J} \frac{q^{m_i}}{m_i}\, q r_J^*(\mathrm{sgn}(M)) - \prod_{i\in u(M)} \tau_{m_i} + \prod_{i\in u(M)} \tau_{m_i-1} \Bigg), \end{aligned}$$

par suite

$$J_s(M) = q^{-\lambda} \prod_{i\in u(M)} \tau_{m_i} \sum_{\substack{I\cup J=v(M)\\ I\cap J=\emptyset,\, J\neq\emptyset}} \prod_{i\in I} \tau_{m_i-1} \prod_{i\in J} \frac{q^{m_i}}{m_i}\, r_J^*(0) + q^{1-\lambda} \prod_{i\in v(M)} \tau_{m_i-1}$$
$$\times \sum_{\substack{I\cup J=u(M)\\ I\cap J=\emptyset,\, J\neq\emptyset}} \prod_{i\in I} \tau_{m_i-1} \prod_{i\in J} \frac{q^{m_i}}{m_i}\, r_J^*(\mathrm{sgn}(M)).$$

La majoration (VII.3) se déduit de (V.6).

(ii) Supposons que G/H soit le centre d'un arc médian. Puisque $v(u) \geq 2n+2 \geq \deg M + 2$, alors

$$|K_s(M)| \ll \frac{q^{ns}}{n^s}\, q^{-N-\deg H} \ll |H|^{-1}\, \frac{q^{n(s-2)}}{n^s}\, q^{4r}.$$

D'où la majoration de $I_{G/H}(M)$.

Corollaire 3. *Pour $s \geq 5$ et $\varepsilon > 0$, on a la relation*

$$\text{(VII.5)}\quad \Big| R^+(M) - J_s(M) \sum_{\substack{H\in\mathbb{M}\\ \deg H\leq 4r}} A_s(H,M) - \sum_{\substack{H\in\mathbb{M}\\ \deg H\leq 4r}} j_s(H,M) A_s(H,M) \Big| \ll q^{n(s-5/2)} q^{4r[(\varepsilon-1/2)(s-1)+3]},$$

la constante dans $\ll$ ne dépendant que de q, s, ε et $A_1, \dots, A_s$.

Proposition VII.2. *Pour tout réel $\varepsilon \in]0, 1/2[$ on a*

$$\text{(VII.6)}\qquad R_1^-(M) \ll \frac{q^{n(s-2)}}{n^s}\, q^{4r(\varepsilon+2-s/2)},$$

la constante dans $\ll$ ne dépendant que de q, s, ε et $A_1, \dots, A_s$.

Démonstration. Si G/H est le centre d'un arc médian alors $4r < \deg H \leq 4r + a_1$. D'après la relation (VII.4),

$$R_1^-(M) \ll \frac{q^{n(s-2)}}{n^s}\, q^{4r} \sum_{\substack{H\in\mathbb{M}\\ 4r<\deg H\leq 4r+a_1}} |H|^{-1} \Phi(H)^{-s} \sum_{G\in\mathcal{C}_H^*} |T(H,G)|.$$

D'après la majoration $(**)$ de la démonstration de la proposition IV.9 on a

$$R_1^-(M) \ll \frac{q^{n(s-2)}}{n^s}\, q^{4r} \sum_{\deg H>4r} |H|^{\varepsilon-s/2}$$
$$\ll \frac{q^{n(s-2)}}{n^s}\, q^{4r} \sum_{j=4r+1}^{\infty} q^{j(\varepsilon+1-s/2)} \ll \frac{q^{n(s-2)}}{n^s}\, q^{(\varepsilon+2-s/2)4r},$$

où les constantes intervenant dans le symbole $\ll$ ne dépendent que de q, s, ε et $A_1, \dots, A_s$.

LEMME 3. (i) *Si $q = 7$ ou $q > 9$, pour tout polynôme M de $\mathbb{F}_q[X]$, on a*

$$\frac{q^{n(s-2)}}{n^s} \ll J_s(M) \ll \frac{q^{n(s-2)}}{n^s}. \tag{VII.7}$$

Si $q = 5$ ou $q = 9$, et si au moins quatre polynômes $A_{i_1}, \dots, A_{i_4}$ parmi $A_1, \dots, A_s$ ont des degrés de même parité, le même résultat reste valable pour les polynômes M de degré $\deg M \equiv \deg A_{i_1} \bmod 2$.

(ii) *Pour* $\deg M = 2n-1$ *et* $\deg H = 4r$ *on a*

$$\frac{q^{n(s-2)}}{n^s} \ll j_s(H, M) \ll \frac{q^{n(s-2)}}{n^s}. \tag{VII.8}$$

Démonstration. (i) D'après la relation (IV.12) pour tout $b \in \mathbb{F}_q$, on a

$$qr_J^*(b) \le (q-1)^{\#J} + (q-1)(1+\sqrt{q})^{\#J} \le q(q-1)^{\#J}.$$

• On suppose que $\deg M \equiv a_i \bmod 2$ pour tout $i = 1, \dots, s$. La relation (VII.2) nous donne donc

$$\begin{aligned} J_s(M) &\le |M|^{-1} \sum_{i=1}^{s} \sum_{\substack{I \cup J = \{1,\dots,s\} \\ I \cap J = \emptyset,\ J \neq \emptyset}} \prod_{i \in I} \tau_{m_i - 1} \prod_{i \in J} (q-1)\, \frac{q^{m_i}}{m_i} \\ &\le |M|^{-1} \prod_{i=1}^{s} \tau_{m_i} \sum_{i=1}^{s} \sum_{\substack{I \cup J = \{1,\dots,s\} \\ I \cap J = \emptyset,\ J \neq \emptyset}} \prod_{i \in I} \frac{\tau_{m_i-1}}{\tau_{m_i}} \prod_{i \in J} \frac{(q-1)\frac{q^{m_i}}{m_i}}{\tau_{m_i}} \\ &\ll q^{-2n} \left(\frac{q^n}{n}\right)^s. \end{aligned}$$

La majoration s'en déduit.

Comme $s \ge 5$, l'ensemble d'indices $u(M)$ contient un ensemble J_0 a cinq éléments et $r_{J_0}^*(\mathrm{sgn}(M)) \ge 1$ d'après la relation (IV.14). Or $\tau_j \ge (q-1)q^j/j$, alors

$$J_s(M) \ge |M|^{-1} \prod_{i \in \{1,\dots,s\} \setminus J_0} \tau_{m_i - 1} \prod_{i \in J_0} \frac{q^{m_i}}{m_i} \gg q^{-2n} \left(\frac{q^n}{n}\right)^s.$$

• On suppose qu'il existe $j \in \{1, \dots, s\}$ tel que $\deg M \not\equiv a_j \bmod 2$. Alors $\#v(M) \ge 1$.

Si $q = 7$ ou $q > 9$, et si $\#v(M) \ge 3$, il existe $J_1 \subset v(M)$ à trois éléments. D'après la relation (IV.15), $r_{J_1}^*(0) \ge 1$. Dans ce cas,

$$J_s(M) \ge q^{-1}|M|^{-1} \prod_{i \in u(M)} \tau_{m_i} \prod_{i \in v(M) \setminus J_1} \tau_{m_i - 1} \prod_{i \in J_1} \frac{q^{m_i}}{m_i} \gg q^{-2n} \left(\frac{q^n}{n}\right)^s.$$

Si $q = 7$ ou $q > 9$ et si $\#v(M) \le 2$, alors $\#u(M) \ge s - 2 \ge 3$. Il existe $J_2 \subset u(M)$ à trois éléments et d'après la relation (IV.15), $r_{J_2}^*(\mathrm{sgn}(M)) \ge 1$.

Dans ce cas,

$$J_s(M) \geq |M|^{-1} \prod_{i\in v(M)} \tau_{m_i-1} \prod_{i\in u(M)\setminus J_2} \tau_{m_i-1} \prod_{i\in J_2} \frac{q^{m_i}}{m_i} \gg q^{-2n}\left(\frac{q^n}{n}\right)^s.$$

Si $q = 5$ ou $q = 9$, on a $\#u(M) \geq 4$, il existe donc $I \subset u(M)$ à quatre éléments tel que $r_I^*(\mathrm{sgn}(M)) \geq 1$. Alors

$$J_s(M) \geq |M|^{-1} \prod_{i\in v(M)} \tau_{m_i} \prod_{i\in u(M)\setminus I} \tau_{m_i-1} \prod_{i\in I} \frac{q^{m_i}}{m_i} \gg q^{-2n}\left(\frac{q^n}{n}\right)^s.$$

La majoration se démontre comme la majoration précédente.

(ii) Les relations (VII.8) sont évidentes.

Proposition VII.3. *Pour $s \geq 5$, on a*

$$|R_s(M) - J_s(M)\mathfrak{S}_s(M)| \ll \frac{q^{n(s-2)}}{n^s}\,(rn^7 \log n\, q^{-r/4}). \tag{VII.9}$$

Démonstration. On a

$$\begin{aligned}
&|R_s(M) - J_s(M)\mathfrak{S}_s(M)| \\
&\quad\leq \Big|R^+(M) - J_s(M) \sum_{\substack{H\in\mathbb{M}\\ \deg H\leq 4r}} A_s(H,M) - \sum_{\substack{H\in\mathbb{M}\\ \deg H\leq 4r}} j_s(H,M)A_s(H,M)\Big| \\
&\qquad + |J_s(M)| \sum_{\substack{H\in\mathbb{M}\\ \deg H>4r}} |A_s(H,M)| + \sum_{\substack{H\in\mathbb{M}\\ \deg H=4r}} |j_s(H,M)|\,|A_s(H,M)| \\
&\qquad + |R_1^-(M)| + |R_2^-(M)|.
\end{aligned}$$

Soit $\varepsilon \in]0, 1/4[$. Les relations (IV.20), (VI.11), (VII.5)–(VII.8) nous donnent

$$\begin{aligned}
|R_s(M) - J_s(M)\mathfrak{S}_s(M)| &\ll q^{n(s-5/2)} q^{4r[(\varepsilon-1/2)(s-1)+3]} + \frac{q^{n(s-2)}}{n^s}\, q^{4r(\varepsilon+2-s/2)} \\
&\quad + \frac{q^{n(s-2)}}{n^s}\,(rn^7 \log n\, q^{-r/4}) \\
&\ll \frac{q^{n(s-2)}}{n^s}\,(rn^7 \log n\, q^{-r/4}),
\end{aligned}$$

ce qui est le résultat annoncé.

Corollaire 4. *Sous les mêmes hypothèses du lemme* 3, *on a*

$$R_s(M) \gg (\deg M)^{-s} |M|^{s/2-1}.$$

Démonstration. D'après la proposition précédente on a

$$R_s(M) \gg J_s(M)\mathfrak{S}_s(M) - \frac{q^{n(s-2)}}{n^s}\,(rn^7 \log n\, q^{-r/4}).$$

D'après les relations (IV.21) et (VII.7) on a $J_s(M)\mathfrak{S}_s(M) > 0$ et

$$J_s(M)\mathfrak{S}_s(M) \gg (\deg M)^{-s} q^{\deg M(s/2-1)},$$

d'où le résultat annoncé.

Références

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

[2] M. Car, *Sommes de carrés de polynômes irréductibles dans* $\mathbb{F}_q[X]$, Acta Arith. 44 (1984), 307–321.

[3] —, *Sommes de carrés et d'irréductibles dans* $\mathbb{F}_q[X]$, Ann. Fac. Sci. Toulouse 3 (1981), 129–166.

[4] —, *Sommes de puissances et d'irréductibles dans* $\mathbb{F}_q[X]$, Acta Arith. 44 (1984), 7–34.

[5] —, *Quadratic forms on* $\mathbb{F}_q[T]$, J. Number Theory 61 (1996), 145–180.

[6] L. Carlitz, *On the representation of a polynomial on a Galois field as the sum of an even number of squares*, Trans. Amer. Math. Soc. 35 (1933), 397–410.

[7] —, *On the representation of a polynomial on a Galois field as the sum of an odd number of squares*, Duke Math. J. 1 (1935), 298–315.

[8] —, *Sums of squares of polynomials*, ibid. 3 (1937), 1–7.

[9] —, *The singular series for sums of squares of polynomials*, ibid. 14 (1947), 1105–1120.

[10] —, *A note on sums of three squares in* $GF[q,x]$, Math. Mag. 48 (1975), 109–110.

[11] E. Cohen, *Sums of an even number of squares in* $GF[p^n,x]$, *I*, Duke Math. J. 14 (1947), 251–267.

[12] —, *Sums of an even number of squares in* $GF[p^n,x]$, *II*, ibid. 14 (1947), 543–557.

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

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

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

[16] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, Cambridge, 1994.

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

[18] W. Webb, *Waring's problem in* $GF[q,x]$, Acta Arith. 22 (1972), 207–220.

Département de Mathématiques
Faculté des Sciences de Tunis
1060 Tunis, Tunisie
E-mail: anis.rezgui@fsb.rnu.tn

Reçu le 2.7.2002
et révisé le 24.6.2003 (4320)