ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

MIREILLE CAR

Sommes de carrés et d'irréductibles dans $IF_q[X]$

Annales de la faculté des sciences de Toulouse 5^e série, tome 3, n° 2 (1981), p. 129-166

<http://www.numdam.org/item?id=AFST_1981_5_3_2_129_0>

© Université Paul Sabatier, 1981, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (http://picard.ups-tlse.fr/~annales/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Annales Faculté des Sciences Toulouse
Vol III, 1981, P. 129 à 166

SOMMES DE CARRES ET D'IRREDUCTIBLES DANS $\mathbb{F}_q[X]$

Mireille Car *(1)*

(1) Laboratoire de Mathématiques, Faculté des Sciences et Techniques de Saint Jérôme, rue Henri Poincaré, 13397 Marseille Cédex 4 - France.

Résumé : Soit $\mathbb{F}_q$ le corps fini à q éléments, q étant un entier impair. Par une méthode analogue à la «méthode du cercle» on démontre que pour tout polynôme M de $\mathbb{F}_q[X]$ de degré suffisamment grand, l'équation

(E) $$M = P_1 + P_2 + A^2$$

admet une solution (P_1,P_2,A) où P_1 et P_2 sont des polynômes irréductibles de $\mathbb{F}_q[X]$, A un polynôme de $\mathbb{F}_q[X]$, ces polynômes vérifiant les conditions de degré les plus restrictives possibles. Cette méthode donne une évaluation asymptotique du nombre de ces solutions. Ces résultats restent valables si l'on exige en plus que le polynôme A soit irréductible.

Summary : Let $\mathbb{F}_q$ be a finite field with q elements, q being odd. By a method similar to the «circle method» one can prove that for every polynomial M in $\mathbb{F}_q[X]$, if the degree of M is large enough, the equation

(E) $$M = P_1 + P_2 + A^2$$

has solutions (P_1,P_2,A) where P_1 and P_2 are irreducibles polynomials in $\mathbb{F}_q[X]$ and A is a polynomial in $\mathbb{F}_q[X]$, the degrees of these polynomials satisfying the most restrictive conditions which are possible. This method gives an asymptotic estimate for the number of these solutions. These results remain true even if one asks the polynomial A to be irreducible.

I. - INTRODUCTION

Soit $\mathbb{F}_q$ le corps fini à q éléments, q étant un entier impair. Certaines analogies entre les propriétés arithmétiques de l'anneau $\mathbb{F}_q[X]$ des polynômes à une variables sur le corps $\mathbb{F}_q$ et l'anneau $\mathbb{Z}$ des entiers relatifs ont été mises en évidence, notamment en ce qui concerne l'arithmétique additive, les problèmes de Goldbach ([11]) et de Waring ([2], [15]) ont été étudiés, et plus particulièrement le problème de Waring pour les carrés ([3], [4], [5], [6], [7], [8], [9]). Il est actuellement connu que tout polynôme de $\mathbb{F}_q[X]$ est représentable comme somme de trois carrés ([7]), sans que l'on ait une limitation du degré des polynômes intervenant dans la représentation, et que tout polynôme M de $\mathbb{F}_q[X]$ de degré «assez élevé» est représentable comme somme de trois polynômes irréductibles de $\mathbb{F}_q[X]$ de degré au plus égal au degré du polynôme M ([11]).

Nous étudions ici la représentation d'un polynôme de $\mathbb{F}_q[X]$ comme somme d'un carré et de deux polynômes irréductibles. Un premier résultat a été établi dans [16] où l'on démontre le théorème suivant.

THEOREME. *Si* k *est un entier strictement inférieur à la caractéristique du corps* $\mathbb{F}_q$, *si* n *est un entier suffisamment grand, tout polynôme* K *de* $\mathbb{F}_q[X]$ *de degré* nk *est représentable comme somme*

$$K = a_1P_1 + a_2P_2 + a_3A^k,$$

P_1, P_2 *étant des polynômes irréductibles unitaires de degré* nk, A *un polynôme unitaire de degré* n, a_1, a_2, a_3 *des éléments de* $\mathbb{F}_q$ *dont la somme est égale au coefficient du terme de degré* nk *du polynôme* K.

Il est possible d'obtenir de telles représentations pour des polynômes de degré non multiple de k, et même d'avoir des représentations de la forme

$$K = P_1 + P_2 + A^k,$$

les polynômes P_1, P_2 et A n'étant plus unitaires, mais satisfaisant toujours aux conditions de degré les plus restrictives possibles ; on peut aussi exiger que le polynôme A intervenant dans une telle représentation soit irréductible. C'est ce que nous faisons ici dans le cas où k = 2, où nous établissons essentiellement le théorème suivant :

THEOREME. *Il existe un entier* n_0, *ne dépendant que de* q, *tel que, pour tout entier* $n \geqslant n_0$, *pour tout polynôme* M *de* $\mathbb{F}_q[X]$ *de degré* 2n *ou* 2n−1, *l'équation*

$$(E) \qquad M = P_1 + P_2 + A^2$$

admette une solution (P_1,P_2,A) *où* P_1 *et* P_2 *sont des polynômes irréductibles de* $\mathbb{F}_q[X]$ *de degré égal au degré de* M, *où* A *est*

(i) soit un polynôme de $\mathbb{F}_q[X]$ *de degré strictement inférieur à* n,

(ii) soit un polynôme de $\mathbb{F}_q[X]$ *tel que* A^2 *soit de degré au plus égal au degré de* M,

(iii) soit un polynôme irréductible de $\mathbb{F}_q[X]$ *de degré strictement inférieur à* n,

(iv) soit un polynôme irréductible de $\mathbb{F}_q[X]$ *tel que* A^2 *soit de degré au plus égal au degré de* M.

On peut remarquer que les conditions (i) et (ii) sont équivalentes lorsque le polynôme M est de degré impair, ainsi que les conditions (iii) et (iv). On remarque aussi que l'existence d'une solution satisfaisant à la condition (iii) entraîne l'existence de solutions satisfaisant aux autres conditions. Toutefois nous démontrerons de façon indépendante les quatre parties du théorème car la démonstration fournit une évaluation asymptotique du nombre de solutions de l'équation (E), et ce nombre varie suivant les conditions exigées.

II. - NOTATIONS

Nous reprenons les notations introduites dans [11] et nous en introduisons de nouvelles qui nous permettront d'alléger les calculs.

Soit H un polynôme de $\mathbb{F}_q[X]$, son degré sera noté d^oH, le coefficient de son terme de plus haut degré sgn(H) ; l'ensemble des polynômes de degré strictement inférieur au degré de H, identifié à l'ensemble des classes de congruence modulo H, sera noté C_H, et le groupe multiplicatif des classes inversibles modulo H sera noté 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.

On désigne par U l'ensemble des polynômes unitaires. Sur U on définit la fonction de Möbius μ par :

$$\mu(H) = \begin{cases} 1 & \text{si } H = 1, \\ 0 & \text{si H est divisible par le carré d'un polynôme irréductible,} \\ (-1)^r & \text{si H est produit de r polynômes irréductibles distincts.} \end{cases}$$

L'ensemble des polynômes irréductibles sera noté I, l'ensemble des polynômes de degré m sera noté D_m, l'ensemble des polynômes de degré strictement inférieur à m sera noté F_m, l'ensemble des polynômes irréductibles de degré m sera noté I_m.

Si A, B et H sont des polynômes, la relation A divise B, (respectivement A ne divise pas B) sera notée $A|B$, (respectivement $A\not|B$); la relation A est congrue à B modulo H sera notée $A \equiv B \pmod H$, le plus grand commun diviseur unitaire des polynômes A et B sera noté (A,B).

Sur le corps $\mathbb{F}_q(X)$ des fractions rationnelles on définit une valuation ν par

$$\nu(A/B) = d^oB - d^oA$$

si A et B sont des polynômes non nuls. Le complété de $\mathbb{F}_q(X)$ pour cette valuation s'identifie au corps $\mathbf{K}$ des séries de Laurent formelles en 1/X à coefficients dans le corps $\mathbb{F}_q$, la valuation ν se prolongeant à $\mathbf{K}$ par

$$\nu\Big(\sum_{s\in\mathbb{Z}} a_s X^s\Big) = -\operatorname{Sup}\{r\in\mathbf{Z} \mid a_r \neq 0\}.$$

A cette valuation ν est associée la valeur absolue $|\ |_\nu$ définie par

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

Nous noterons simplement $|\ |$ cette valeur absolue, bien que ce dernier symbole soit aussi utilisé pour désigner la valeur absolue classique sur le corps $\mathbb{R}$ des réels ou le corps $\mathbb{C}$ des complexes, mais il y a peu de risques de confusion.

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

$$\{t\in\mathbf{K} \mid \nu(t) > j\}.$$

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

Soit e un caractére non principal du groupe additif de $\mathbb{F}_q$. On définit un caractère non principal E du groupe additif de $\mathbf{K}$ en posant

$$E\Big(\sum_{s\in\mathbb{Z}} a_s X^s\Big) = e(a_{-1}).$$

L'ensemble des éléments non nuls de $\mathbb{F}_q$, respectivement de $\mathbb{F}_q[X]$, respectivement de $\mathbf{K}$, sera noté $\mathbb{F}_q^*$, respectivement $\mathbb{F}_q[X]^*$, respectivement $\mathbf{K}^*$.

Si y est nombre réel, on notera [y] la partie entière de y.

III. - SOMMES DE CARACTERES

Les cinq propositions suivantes ont été établies dans [11] ou se démontrent par des méthodes analogues.

PROPOSITION III-1. *Pour tout entier relatif* j, $\mathscr{P}_j$ *a pour mesure* q^{-j}.

PROPOSITION III-2. *(i) Pour tout polynôme* A, E(A) = 1.
(ii) Pour tout polynôme H *non nul, si* A *et* B *sont des polynômes congrus modulo* H, E(A/H) = E(B/H).
(iii) Si $u \in \mathscr{P}^2$, E(u) = 1.

PROPOSITION III-3. *Soient un entier* $j \geqslant 0$, $u \in \mathbf{K}$ *et* $b \in \mathscr{P}$. *Alors*

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

PROPOSITION III-4. *Soient* $u \in \mathbf{K}$, $\{u\}$ *la partie fractionnaire de* u *et* j *un entier naturel. Alors,*

$$\sum_{B \in F_j} E(uB) = \begin{cases} q^j & si \quad \nu(\{u\}) > j, \\ 0 & si \quad \nu(\{u\}) < j. \end{cases} \tag{III-2}$$

De cette proposition on déduit un corollaire très souvent utilisé par la suite :

COROLLAIRE. *Si* G *et* H *sont des polynômes premiers entre eux,*

$$\sum_{R \in C_H} E(\frac{G}{H} R) = 0 ; \tag{III-3}$$

ainsi que la première «formule de changement de variable» :

PROPOSITION III-5. *Soient un entier* $j \geqslant 0$, $u \in \mathscr{P}$ *et* $a \in \mathbf{K}$ *tels que* $j \geqslant \nu(a) \geqslant -\nu(u)$. *Alors,*

$$\sum_{B \in F_j} E(auB) = \frac{1}{|a|} \sum_{B \in F_{j-\nu(a)}} E(uB). \tag{III-4}$$

Les deux propositions suivantes sont à la base de la deuxième «formule de changement de variable».

PROPOSITION III-6. *Soient* $j \in \mathbb{Z}$ *et* $a \in \mathbf{K}^*$. *Si* f *est une application localement sommable de* $\mathbf{K}$ *dans* $\mathbb{C}$, *alors,*

$$\int_{\mathscr{P}_j} f(at)dt = \frac{1}{|a|} \int_{\mathscr{P}_{j+\nu(a)}} f(t)dt. \tag{III-5}$$

Démonstration. C'est une conséquence de l'unicité, à constante multiplicative près, de la mesure de Haar sur $\mathbf{K}$.

PROPOSITION III-7. *Soient un entier* $j \geqslant 0$ *et* $a \in \mathbf{K}$ *tels que* $\nu(a) \geqslant j$. *Alors,*

$$\sum_{B \in F_j} E(aB^2) = \int_{\mathscr{P}_{-j}} E(at^2)dt \,. \tag{III-6}$$

Démonstration. L'égalité (III-6) est triviale si $j = 0$. Supposons $j \neq 0$. Soit $m \in \{0,...,j-1\}$. Alors,

$$\int_{\nu(t)=-m} E(at^2)dt = \sum_{B \in D_m} \int_{B+\mathscr{P}} E(at^2)dt = \sum_{B \in D_m} E(aB^2) \int_{\mathscr{P}} E(2atB+at^2)dt \,.$$

Si $B \in D_m$ et si $t \in \mathscr{P}$,

$$\nu(at^2) > \nu(at) \geqslant \nu(atB) > \nu(a) - m \geqslant \nu(a) - j + 1 \,,$$

et,

$$E(2atB + at^2) = 1 \,.$$

Donc,

$$1 + \sum_{m=0}^{j-1} \sum_{B \in D_m} E(aB^2) = 1 + \sum_{m=0}^{j-1} \int_{\nu(t)=-m} E(at^2)dt = \int_{\mathscr{P}_{-j}} E(at^2)dt \,.$$

Donnons maintenant la deuxième «formule de changement de variable».

PROPOSITION III-7. *Soient un entier* $j \geqslant 0$, H *un polynôme tel que* $d^oH \leqslant j$ *et* u *un élément de* $\mathscr{P}$ *tel que* $\nu(u) \geqslant j + d^oH$. *Alors,*

$$\sum_{B \in F_{j-d^oH}} E(uH^2B^2) = \frac{1}{|H|} \sum_{B \in F_j} E(uB^2) \,. \tag{III-7}$$

Démonstration. On a $\nu(uH^2) \geqslant j - d^oH$, d'où, avec (III-6),

$$\sum_{B \in F_{j-d^oH}} E(uH^2B^2) = \int_{\mathscr{P}_{-j+d^oH}} E(uH^2t^2)dt,$$

puis, avec (III-5) et à nouveau (III-6),

$$\sum_{B \in F_{j-d^oH}} E(uH^2B^2) = \frac{1}{|H|} \int_{\mathscr{P}_{-j}} E(ut^2)dt = \frac{1}{|H|} \sum_{B \in F_j} E(uB^2) \,.$$

Terminons ce paragraphe par la dernière «formule de changement de variable» et son corollaire.

PROPOSITION III-8. *Soient un entier* $m \geqslant 0$ *et* $u \in \mathscr{P}$ *tels que* $\nu(u) > m$. *Alors,*

$$\sum_{B \in D_m} E(uB^2) = q^{-m} \sum_{b \in \mathbf{F}_q^*} E(ub^2X^{2m}) \sum_{V \in F_{2m}} E(uV) \,. \tag{III-8}$$

Démonstration. Si $B \in D_m$, il existe $b \in \mathbb{F}_q^*$ et $V \in F_{2m}$ tels que

$$B^2 = b^2X^{2m} + V,$$

donc tels que,

$$E(uB^2) = E(ub^2X^{2m})E(uV),$$

et il existe exactement q^m polynômes W de F_{2m} tels que

$$d^o(B^2 - b^2X^{2m} - W) < m,$$

et, pour de tels polynômes,

$$E(uV) = E(uW).$$

D'autre part, soient $b \in \mathbb{F}_q^*$ et $V \in F_{2m}$. Alors, il existe un et un seul polynôme B tel que

$$d^o(B^2 - b^2X^{2m} - V) < m.$$

En effet, une telle relation détermine le degré de B égal à 2m et le coefficient du terme de plus haut degré de B qui doit être égal à b ; elle exige de plus, que les coefficients $b_0,\ldots,b_{m-1}$, b du polynôme B et les coefficients $v_0,\ldots,v_{2m-1}$ du polynôme V soient liés par les relations

$$v_{2m-1} = 2bb_{m-1},$$

et, pour $j \in \{m-2,\ldots,1,0\}$,

$$v_{m+j} = 2bb_j + \sum_{\substack{r+s=m+j \\ j<r<m \\ j<s<m}} b_r b_s,$$

ce qui détermine $b_{m-1},\ldots,b_1,b_0$ de façon unique.

COROLLAIRE. *Sous les mêmes hypothèses,*

$$\text{(III-9)} \qquad \sum_{B \in D_m} E(uB^2) = \begin{cases} q^m(q-1) & \text{si } \nu(u) > 2m+1, \\ 0 & \text{si } \nu(u) \leqslant 2m, \\ q^m \sum_{b \in \mathbb{F}_q^*} e(ab^2) & \text{si } \nu(u) = 2m+1 \\ & \text{et si } a \in \mathbb{F}_q^* \text{ est tel que } \nu(u-aX^{-\nu(u)}) > \nu(u). \end{cases}$$

Démonstration. La première assertion est immédiate avec (III-2). Les deux autres assertions sont des conséquences de (III-2) et de (III-8).

IV. - LA METHODE DU CERCLE

Soit n un entier tel que

$$\text{(IV-1)} \qquad n > 33\frac{\log n}{\log q} \quad \text{et} \quad 2n > \left(33\frac{\log n}{\log q}\right)^2 \left(2q(\log(q))^{-2} + \frac{1}{4}\right).$$

Soit M un polynôme de degré 2n ou 2n−1. Soient $i \in \{n, n+1\}$, f_i, f_i^* et g les applications de $\mathscr{P}$ dans $\mathbb{C}$ définies par

$$\text{(IV-2)} \qquad f_i(t) = \sum_{A \in F_i} E(tA^2),$$

$$\text{(IV-3)} \qquad f_i^*(t) = \sum_{P \in F_i \cap I} E(tP^2),$$

$$\text{(IV-4)} \qquad g(t) = \sum_{P \in I_{d^oM}} E(tP).$$

Soient

$$\text{(IV-5)} \qquad R_i(M) = \int_{\mathscr{P}} f_i(t) g^2(t) E(-Mt)dt,$$

$$\text{(IV-6)} \qquad R_i^*(M) = \int_{\mathscr{P}} f_i^*(t) g^2(t) E(-Mt)dt.$$

Alors, d'après (III-1), $R_i(M)$, respectivement $R_i^*(M)$ est égal au nombre de solutions de l'équation

$$M = P_1 + P_2 + A^2$$

où P_1 et P_2 sont des polynômes irréductibles de degré d^oM, où A est un polynôme de degré strictement inférieur à i, respectivement un polynôme irréductible de degré strictement inférieur à i.

Les intégrales $R_n(M)$ et $R_n^*(M)$ nous donneront le nombre de solutions de l'équation (E) satisfaisant aux conditions (i) et (iii), et les intégrales $R_{n+1}(M)$ et $R_{n+1}^*(M)$ nous donneront, pour des polynômes M de degré pair, le nombre de solutions de l'équation (E) satisfaisant aux conditions (ii) et (iv).

Posons

$$\text{(IV-7)} \qquad s = \left[33\frac{\log(n)}{\log(q)}\right].$$

(IV-8) $$N = 2(n-s).$$

On appelle fraction de Farey à l'ordre N toute fraction rationnelle G/H telle que

(i) H est un polynôme unitaire de degré au plus N,
(ii) $G \in C_H^*$.

Si G/H est une fraction de Farey à l'ordre N, la boule

$$U_{G/H} = \left\{ t \in \mathscr{P} \mid \nu(t - \frac{G}{H}) > d^oH + N \right\}$$

est appelée arc de Farey de centre G/H.

Lorsque G/H parcourt l'ensemble des fractions de Farey à l'ordre N, les arcs de Farey $U_{G/H}$ forment une partition de $\mathscr{P}$. C'est le théorème 4-3 de [11].

Sur les arcs de Farey $U_{G/H}$ tels que $d^oH \leqslant 2s$ on saura calculer $f_i(t)$ et on aura une bonne approximation de g(t) et de $f_i^*(t)$; ces arcs seront dits majeurs. Soit $\mathfrak{a}$ leur réunion et $\mathfrak{a}'$ la réunion des arcs restants.

Si G/H est une fraction de Farey à l'ordre N, soient

(IV-9) $$I_{G/H}(M) = \int_{U_{G/H}} f_i(t) g^2(t) E(-Mt)dt,$$

et

(IV-10) $$I^*_{G/H}(M) = \int_{U_{G/H}} f_i^*(t) g^2(t) E(-Mt)dt.$$

Les sommes

$$\int_{\mathfrak{a}} f_i(t) g^2(t) E(-Mt)dt = \sum_{\substack{H \in U \\ d^oH \leqslant 2s}} \sum_{G \in C_H^*} I_{G/H}(M)$$

$$\int_{\mathfrak{a}} f_i^*(t) g^2(t) E(-Mt)dt = \sum_{\substack{H \in U \\ d^oH \leqslant 2s}} \sum_{G \in C_H^*} I^*_{G/H}(M)$$

donneront de bonnes approximations de $R_i(M)$ et $R_i^*(M)$; leurs calculs nous donneront les premiers termes des séries singulières $\mathfrak{S}(M)$ et $\mathfrak{S}(M)^*$ qui seront étudiées au paragraphe suivant.

Lorsque t décrit $\mathfrak{a}'$ on a une majoration de $f_i(t)$ et de $f_i^*(t)$; si la majoration de $f_i(t)$ est assez simple, il n'en est pas de même de celle de $f_i^*(t)$ qui nécessitera l'utilisation d'un crible, ce qui sera fait au paragraphe VII, et la majoration de sommes doubles, ce qui sera fait au paragraphe VI.

V. - LES SERIES SINGULIERES $\mathfrak{S}(M)$ ET $\mathfrak{S}(M)^*$

Dans ce paragraphe M est un polynôme de $\mathbb{F}_q[X]$ fixé.

Si G et H sont des polynômes premiers entre eux, soient

$$S(G,H) = \sum_{A \in C_H} E(\frac{G}{H}A^2), \tag{V-1}$$

$$S^*(G,H) = \sum_{A \in C_H^*} E(\frac{G}{H}A^2). \tag{V-2}$$

Si H est un polynôme non nul, soient

$$C(M,H) = \sum_{G \in C_H^*} S(G,H)E(-M\frac{G}{H}), \tag{V-3}$$

$$C^*(M,H) = \sum_{G \in C_H^*} S^*(G,H)E(-M\frac{G}{H}). \tag{V-4}$$

Les deux propositions suivantes se démontrent comme les théorèmes 8-4 et 8-8 de [1], avec quelques simplifications pour la dernière proposition permettant d'avoir une égalité au lieu d'une majoration.

PROPOSITION V-1. *Les fonctions* $H \to C(M,H)$ *et* $H \to C^*(M,H)$ *sont multiplicatives.*

PROPOSITION V-2. *Si* G *et* H *sont des polynômes premiers entre eux,*

$$|S(G,H)| = |H|^{1/2}. \tag{V-5}$$

Si P est un polynôme irréductible ne divisant pas M, on définit le symbole de Legendre $(\frac{M}{P})$ par

$$(\frac{M}{P}) = \begin{cases} 1 \text{ si M est carré modulo P,} \\ -1 \text{ si M n'est pas carré modulo P.} \end{cases}$$

PROPOSITION V-3. *Soit* P *un polynôme irréductible. Alors,*

$$\text{si } P|M,\ C(M,P) = 0 \text{ et } C^*(M,P) = 1 - |P|, \tag{V-6}$$

$$\text{si } P\nmid M,\ C(M,P) = (\frac{M}{P})|P| \text{ et } C^*(M,P) = 1 + (\frac{M}{P})|P|. \tag{V-7}$$

Démonstration. Soit u(M) le nombre de solutions de la congruence

$$M \equiv L^2 \pmod{P}.$$

Alors,

$$C(M,P) = \sum_{G \in C_P^*} \sum_{A \in C_P} E((A^2-M)G/P) = u(M)\Phi(P) - (|P| - u(M)),$$

$$C(M,P) = (u(M)-1)\,|P|.$$

La somme C*(M,P) se traite de la même façon.

COROLLAIRE 1. *Si* P *est un polynôme irréductible,*

$$|C^*(M,P)| \leqslant 1 + |P|. \tag{V-8}$$

COROLLAIRE 2. *Si* H *est un polynôme sans facteur carré,*

$$|C(M,H)| \leqslant |H|, \tag{V-9}$$

$$|C^*(M,H)| \leqslant |H|^2 \Phi(H)^{-1}. \tag{V-10}$$

Démonstration. (V-9) est immédiate. Si H est sans facteur carré,

$$|C^*(M,H)| = \prod_{\substack{P \in I \cap U \\ P \mid H}} |C^*(M,P)| \leqslant \prod_{\substack{P \in I \cap U \\ P \mid H}} (1 + |P|) = \prod_{\substack{P \in I \cap U \\ P \mid H}} (|P|^2-1)/(|P|-1),$$

$$|C^*(M,H)| \leqslant \prod_{\substack{P \in I \cap U \\ P \mid H}} (|P|^2/(|P|-1) = |H|^2 / \Phi(H).$$

PROPOSITION V-4. *Il existe une constante* C_1 *ne dépendant que de* q, *telle que, pour tout polynôme* H *de degré au moins égal à* 2,

$$\Phi(H) \geqslant C_1 |H| (\log(d^oH))^{-1}. \tag{V-11}$$

Démonstration. Comme pour le théorème 5-1, chapitre I de [12].

PROPOSITION V-5. *La série*

$$\mathcal{G}(M) = \sum_{H \in U} \frac{\mu^2(H)\, C(M,H)}{|H|\,\Phi^2(H)} \tag{V-12}$$

est absolument convergente ; de plus il existe une constante $C_2 > 0$, *ne dépendant que de* q, *telle que, pour tout entier* $T \geqslant 2$,

(V-13) $$\sum_{\substack{H\in U\\ d^oH\geqslant T}} \left|\frac{\mu^2(H)\,C(M,H)}{|H|\,\Phi^2(H)}\right| \leqslant C_2\, q^{-T/2}.$$

D'autre part,

(V-14) $$\mathfrak{S}(M) = \prod_{\substack{P\in I\cap U\\ P\nmid M}} \left(1+\left(\frac{M}{P}\right)(|P|-1)^{-2}\right),$$

et il existe une constante $C_3 > 0$, *ne dépendant que de* q *telle que*

(V-15) $$\mathfrak{S}(M) \geqslant C_3.$$

Démonstration. Si le polynôme H est sans facteur carré, et de degré supérieur à T, d'après (V-9) et (V-11),

$$|C(M,H)\,|H|^{-1}\,\Phi(H)^{-2}| \leqslant \Phi(H)^{-2} \leqslant C_1^{-2}(\log(d^oH))^2\,|H|^{-2},$$

d'où,

$$\sum_{\substack{H\in U\\ d^oH\geqslant T}} \left|\frac{\mu^2(M)\,C(M,H)}{|H|\,\Phi^2(H)}\right| \leqslant C_1^{-2}\sum_{h=T}^{\infty}(\log h)^2\,q^{-h} \leqslant C_2\,q^{-T/2},$$

C_2 ne dépendant que de q.

La série $\mathfrak{S}(M)$ est absolument convergente et s'écrit comme produit eulérien

$$\mathfrak{S}(M) = \prod_{P\in I\cap U}\left(1+\frac{C(M,P)}{|P|\,(|P|-1)^2}\right),$$

et (V-14) se déduit de la proposition V-3. Enfin,

$$\mathfrak{S}(M) \geqslant \prod_{\substack{P\in I\cap U\\ P\nmid M}}(1-(|P|-1)^{-2}) \geqslant \prod_{P\in I\cap U}(1-(|P|-1)^{-2}) \geqslant \prod_{j=1}^{\infty}(1-(q^j-1)^{-2})^{q^j},$$

ce dernier produit est strictement positif ; notons le C_3.

PROPOSITION V-6. *La série*

(V-16) $$\mathfrak{S}(M)^* = \sum_{H\in U}\frac{\mu^2(H)\,C^*(M,H)}{|H|\,\Phi^2(H)}$$

est absolument convergente ; de plus, il existe une constante $C_4 > 0$, *ne dépendant que de* q, *telle que, pour tout entier* $T \geqslant 2$,

$$\text{(V-17)} \qquad \sum_{\substack{H\in U \\ d^oH \geqslant T}} \left|\frac{\mu^2(H)\, C^*(M,H)}{|H|\,\Phi^2(H)}\right| \leqslant C_4\, q^{-T/2}.$$

D'autre part,

$$\text{(V-18)} \qquad \mathfrak{S}(M)^* = \left(\prod_{\substack{P\in I\cap U \\ P\mid M}} \left(1-\frac{1}{\Phi(P)^2}\right)\right)\left(\prod_{\substack{P\in I\cap U \\ P\nmid M}} \left(1+\frac{1+\left(\frac{M}{P}\right)|P|}{\Phi(P)^3}\right)\right)$$

et,

$$\text{(V-19)} \qquad \mathfrak{S}(M)^* \geqslant C_3.$$

Démonstration. Si le polynôme H est sans facteur carré et de degré au moins égal à T, d'après (V-10) et (V-11),

$$|C^*(M,H)\Phi(H)^{-3}| \leqslant C_1^{-4}(\log(d^oH))^4\,|H|^{-2},$$

et (V-17) se démontre comme (V-13). En écrivant $\mathfrak{S}(M)^*$ comme produit eulérien et en utilisant la proposition V-3 on obtient (V-18). Enfin

$$\mathfrak{S}(M)^* \geqslant \left(\prod_{\substack{P\in I\cap U \\ P\mid M}} (1-\Phi(P)^{-2})\right)\left(\prod_{\substack{P\in I\cap U \\ P\nmid M}} 1+\frac{1-|P|}{\Phi(P)^3}\right) \geqslant C_3.$$

VI. - MAJORATION DE SOMMES DE CARACTERES

Dans ce paragraphe G et H sont des polynômes premiers entre eux.

PROPOSITION VI-1. *Soit* r *un entier naturel. Alors,*

$$\text{(VI-1)} \qquad \left|\sum_{A\in F_r} E\left(\frac{G}{H}A^2\right)\right| \leqslant \operatorname{Sup}\left(q^r\,|H|^{-1/2},\,|H|^{1/2}\right).$$

Démonstration. On majore cette par la méthode de Weyl déjà utilisée dans [15]. Désignons par S cette somme. Alors,

$$|S|^2 = \sum_{A_1\in F_r}\ \sum_{A_2\in F_r} E\left(\frac{G}{H}(A_1^2-A_2^2)\right) = \sum_{A\in F_r}\ \sum_{B\in F_r} E\left(\frac{G}{H}(2AB+A^2)\right),$$

$$|S|^2 \leqslant \sum_{A\in F_r}\left|\sum_{B\in F_r} E\left(\frac{G}{H}(2AB+A^2)\right)\right| = \sum_{A\in F_r}\left|\sum_{B\in F_r} E\left(2\frac{G}{H}AB\right)\right|,$$

d'où, avec (III-3),

$$|S|^2 \leqslant q^r \sum_{A \in F_r} v(A) \qquad \text{où} \qquad v(A) = \begin{cases} 1 \text{ si } \nu(\{GA/H\}) > r, \\ 0 \text{ si } \nu(\{GA/H\}) \leqslant r. \end{cases}$$

Si $d^oH \leqslant r$, $v(A) = 1$ si et seulement si A est congru à 0 modulo H.
Si $d^oH \leqslant r$,

$$|S|^2 \leqslant q^r q^{r-d^oH}.$$

Si $d^oH > r$,

$$|S|^2 \leqslant q^r \sum_{A \in C_H} v(A) = q^r \sum_{\substack{R \in C_H \\ d^oR < d^oH - r}} 1 = |H|.$$

Dans les deux cas,

$$|S|^2 \leqslant \text{Sup}\left(\frac{q^{2r}}{|H|}, |H|\right).$$

PROPOSITION VI-2. *Soient* a *et* b *des entiers strictement positifs, A une partie de* F_a, *B une partie de* F_b *et*

$$S(A,B) = \sum_{A \in A} \sum_{B \in B} E\left(\frac{G}{H} A^2 B^2\right).$$

Alors,

$$\text{(VI-2)} \qquad |S(A,B)| \leqslant q^{a+b} \,\text{Sup}(|H|^{-1/8}, q^{-(a+b)/4} |H|^{1/8}, \text{Inf}(q^{-a/8}, q^{-b/8})).$$

Démonstration. L'inégalité de Schwarz donne

$$|S(A,B)|^2 \leqslant q^a \sum_{A \in A} \Big| \sum_{B \in B} E\left(\frac{G}{H} A^2 B^2\right) \Big|^2 \leqslant q^a \sum_{A \in F_a} \Big| \sum_{B \in B} E\left(\frac{G}{H} A^2 B^2\right) \Big|^2,$$

$$|S(A,B)|^2 \leqslant q^a \sum_{B_1 \in B} \sum_{B_2 \in B} S_{B_1,B_2},$$

où, pour $B_1 \in F_b$, $B_2 \in F_b$,

$$S_{B_1,B_2} = \sum_{A \in F_a} E\left(\frac{G}{H} A^2 (B_1^2 - B_2^2)\right).$$

Alors, comme pour la majoration précédente,

$$|S_{B_1,B_2}|^2 \leqslant \sum_{A \in F_a} \Big| \sum_{T \in F_a} E\left(2 \frac{G}{H} (B_1^2 - B_2^2) AT\right) \Big|,$$

(III-1) permet d'écrire

$$|S_{B_1,B_2}|^2 \leqslant \sum_{A\in F_a} \sum_{T\in F_a} E\,(2\frac{G}{H}(B_1^2-B_2^2)AT)\,,$$

d'où,

$$|S(A,B)|^4 \leqslant q^{2a+2b} \sum_{B_1\in F_b} \sum_{B_2\in F_b} \sum_{A\in F_a} \sum_{T\in F_a} E\,(2\frac{G}{H}(B_1^2-B_2^2)AT),$$

puis, en procédant comme pour la proposition (VI-1),

$$|S(A,B)|^4 \leqslant q^{2a+2b} \sum_{A\in F_a} \sum_{T\in F_a} \sum_{B\in F_b} \sum_{V\in F_b} E\,(4\frac{GATBV}{H})\,.$$

Soit, pour tout polynôme R

$$\epsilon(R) = \begin{cases} 1 & \text{si} \quad \nu(\{GR/H\}) > b\,, \\ 0 & \text{si} \quad \nu(\{GR/H\}) \leqslant b\,, \end{cases}$$

et $\delta(R)$ le nombre de solutions $(A,T,B)\in F_a \times F_a \times F_b$ de l'équation

$$R = ATB\,.$$

Alors, d'après (III-1)

$$|S(A,B)|^4 \leqslant q^{2a+3b} \sum_{R\in F_{2a+b-2}} \epsilon(R)\delta(R)\,,$$

d'où,

$$|S(A,B)|^8 \leqslant q^{4a+6b} \Big(\sum_{R\in F_{2a+b-2}} \delta(R)^2\Big)\Big(\sum_{R\in F_{2a+b-2}} \epsilon(R)\Big)\,.$$

Posons

$$e(a,b) = \sum_{R\in F_{2a+b-2}} \epsilon(R)\,.$$

Si $d^oH \leqslant b$,

$$e(a,b) = q^{2a+b-2-d^oH}\,,$$

si $b < d^oH \leqslant 2a+b-2$,

$$e(a,b) = \sum_{R\in C_H} \sum_{L\in F_{2a+b-2-d^oH}} \epsilon(LH+R) = q^{2a+b-2-d^oH} \sum_{R\in C_H} \epsilon(R)$$

$$e(a,b) = q^{2a+b-2-d^oH}\, q^{d^oH-b} = q^{2a-2},$$

si $d^oH > 2a+b-2$,

$$e(a,b) \leqslant \sum_{R \in C_H} \epsilon(R) = q^{d^oH-b}.$$

Dans tous les cas,

$$e(a,b) \leqslant \text{Sup}\left(\frac{q^{2a+b-2}}{|H|}, q^{2a-2}, |H|\, q^{-b}\right).$$

D'autre part,

$$\sum_{R \in F_{2a+b-2}} \delta(R)^2 = q^{2a+b},$$

d'où,

$$|S(A,B)|^8 \leqslant q^{8a+8b}\, \text{Sup}\left(\frac{q^{-2}}{|H|}, q^{-2-b}, |H|\, q^{-(2a+2b)}\right).$$

De la même façon on aurait,

$$|S(A,B)|^8 \leqslant q^{8a+8b}\, \text{Sup}\left(\frac{q^{-2}}{|H|}, q^{-2-a}, |H|\, q^{-(2a+2b)}\right).$$

PROPOSITION VI-3. *Soient* m, a *et* b *des entiers strictement positifs, A un ensemble de polynômes* A *tels que* $a \leqslant d^oA < a+m$, *B un ensemble de polynômes* B *tels que* $b \leqslant d^oB < b+m$. *Soit*

$$T(A,B) = \sum_{A \in A} \sum_{\substack{B \in B \\ d^o(AB) < a+b+m}} E\left(\frac{G}{H} A^2 B^2\right).$$

Alors,

(VI-3) $|T(A,B)| \leqslant 2mq^{a+b+m}\, \text{Sup}(|H|^{-1/8}, q^{(a+b+m)/4}\, |H|^{1/8}, q^{-(a+b+m)/16})$.

Démonstration. Désignons par T l'ensemble des couples d'entiers (α,β) tels que

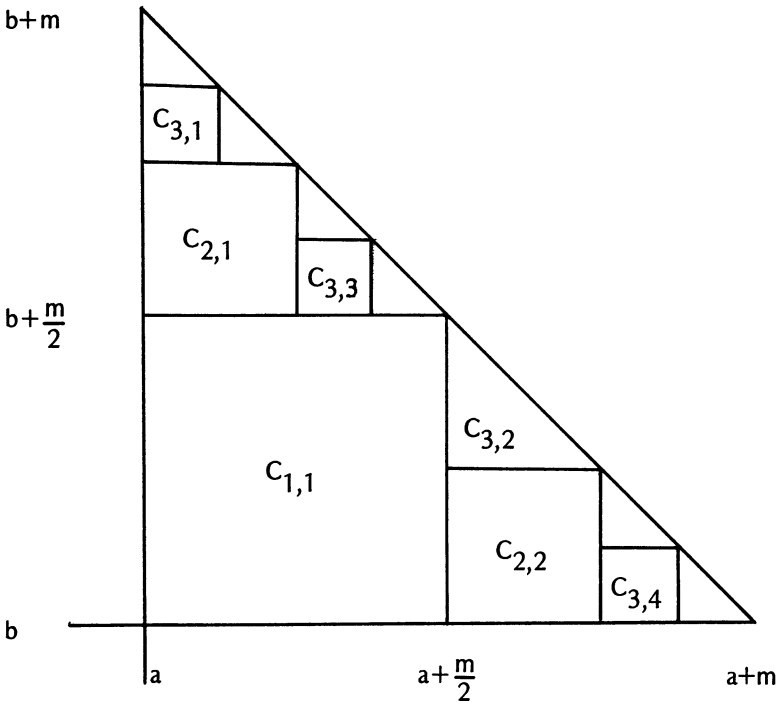
$$a \leqslant \alpha < a+m \quad , \quad b \leqslant \beta < a+b+m-\alpha.$$

Partageons l'ensemble T en ensembles élémentaires $C_{i,j}$ définis de la façon suivante :

$$C_{1,1} = [a, a+\tfrac{m}{2}[\times [\, b, b+\tfrac{m}{2}[\cap \mathbb{Z} \times \mathbb{Z}.$$

Si i est un entier compris entre 2 et $h = [\log m / \log 2] + 1$, j varie de 1 à 2^{i-1} et, si

$$j - 1 = \sum_{r=0}^{i-2} d_{j,r}\, 2^r \quad , \quad d_{j,r} \in \{0,1\} \ ,$$



$$C_{i,j} = [a_{i,j} \, , \, a_{i,j} + m2^{-i} [\ \times \ [b_{i,j} \, , \, b_{i,j} + m2^{-i} [\cap \mathbb{Z} \times \mathbb{Z} \ ,$$

où,

$$a_{i,j} = a + m \sum_{r=0}^{i-2} d_{j,r}\, 2^{-r-1} \quad , \quad b_{i,j} = b + m \sum_{r=0}^{i-2} e_{j,r}\, 2^{-r-1} \ ,$$

les coefficients $d_{j,r}$ et $e_{j,r}$ étant liés par la relation

$$d_{j,r} + e_{j,r} = 1 \ .$$

De ce fait, lorsque j varie de 1 à 2^{i-1}, on a

(*) $$a_{i,j} + b_{i,j} + m\, 2^{1-i} = a + b + m \ .$$

Le plus grand des nombres $a_{i,j} + m2^{-i}$ est $a + m - m2^{-h}$, le plus grand des nombres $b_{i,j} + m2^{-i}$ est $b + m - m2^{-h}$ et il n'existe pas d'entier dans les intervalles $[a + m - m2^{-h} \, , \, a + m [$ et

$[b + m - m2^{-h}, b + m[$.

Les ensembles $C_{i,j}$ $(1 \leqslant i \leqslant h,\ 1 \leqslant j \leqslant 1^{i-1})$ forment donc une partition de T, et, si pour $i \in \{1,...,h\}$, pour $j \in \{1,...,2^{i-1}\}$,

$$S_{i,j} = \sum_{(\alpha,\beta) \in C_{i,j}} \sum_{\substack{A \in \mathcal{A} \\ d^oA = \alpha}} \sum_{\substack{B \in \mathcal{B} \\ d^oB = \beta}} E\left(\frac{G}{H} A^2 B^2\right)$$

$$T(\mathcal{A},\mathcal{B}) = \sum_{i=1}^{h} \sum_{j=1}^{2^{i-1}} S_{i,j} \ .$$

La proposition précédente permet de majorer chacune des sommes $S_{i,j}$. Compte tenu de l'égalité (*), on obtient

$$|S_{i,j}| \leqslant q^{a+b+m} \operatorname{Sup}(|H|^{-1/8}, q^{-(a+b+m)/4}|H|^{1/8}, q^{-(a+b+m)/16}) ;$$

et il y a

$$\sum_{i=1}^{h} 2^{i-1} = 2^h - 1 < 2m$$

sommes $S_{i,j}$.

PROPOSITION VI-4. *Soient* m, a, b *et* c *des entiers strictement positifs tels que* $b \leqslant c$, *$\mathcal{A}$ un ensemble de polynômes* A *tels que* $a \leqslant d^oA < a+m$ *et $\mathcal{B}$ un ensemble de polynômes* B *tels que* $b \leqslant d^oB < c+m$. *Soit*

$$U(\mathcal{A},\mathcal{B}) = \sum_{A \in \mathcal{A}} \sum_{\substack{B \in \mathcal{B} \\ d^o(AB) < a+c+m}} E\left(\frac{G}{H} A^2 B^2\right) .$$

Alors,

(VI-4) $|U(\mathcal{A},\mathcal{B})| \leqslant (2m+1)q^{a+c+m} \operatorname{Sup}(|H|^{1/8}, q^{-(a+c+m)/4}|H|^{1/8}, q^{-(a+c+m)/16})$.

Démonstration. On partage la somme $U(\mathcal{A},\mathcal{B})$ en deux sommes U_1 et U_2 où

$$U_1 = \sum_{A \in \mathcal{A}} \sum_{B \in \mathcal{B} \cap F_c} E\left(\frac{G}{H} A^2 B^2\right) \quad \text{et} \quad U_2 = \sum_{A \in \mathcal{A}} \sum_{\substack{B \in \mathcal{B} \\ c \leqslant d^oB < a+c+m-d^oA}} E\left(\frac{G}{H} A^2 B^2\right) .$$

Avec (VI-1) et (VI-3) il vient

$$|U_1| \leqslant q^{a+m+c} \operatorname{Sup}(|H|^{-1/8}, q^{-(a+c+m)/4}|H|^{1/8}, \operatorname{Inf}(q^{-(a+m)/8}, q^{-c/8})) ,$$

$$|U_2| \leqslant 2mq^{a+c+m} \operatorname{Sup}(|H|^{-1/8}, q^{-(a+c+m)/4}|H|^{1/8}, q^{-(a+s+m)/16}) ,$$

d'où la majoration (VI-4).

VII. - MAJORATION DE LA SOMME $\sum_{P \in \mathfrak{J} \cap F_m} E(\frac{G}{H}P^2)$

Dans ce paragraphe m et r sont des entiers strictement positifs tels que

$$m \geqslant \mathrm{Sup}(8r+1,\ 2r^2(2q(\log q)^{-2} + \frac{1}{4}))\ ,$$

H est un polynôme tel que $d^oH \in [4r, 2m-4r]$ et G est un polynôme premier à H. Soit

$$S = \sum_{P \in I \cap F_m} E(\frac{G}{H}P^2)\ . \tag{VII-1}$$

Pour majorer la somme S nous utilisons un crible semblable à celui utilisé pour majorer des sommes analogues portant sur des nombres premiers. (Voir [10] par exemple). Soit

$$B = \prod_{\substack{P \in I \cap U \\ d^oP < m/2}} P. \tag{VII-2}$$

Soient D l'ensemble des diviseurs unitaires de B, D' l'ensemble des polynômes D de D dont tous les diviseurs irréductibles sont de degré strictement inférieur à 2r et soit D'' le complémentaire de D' dans D.

Si j est un entier naturel, F_j^* désignera l'ensemble des polynômes non nuls de F_j.

PROPOSITION VII-1.

$$\Big|S - \sum_{\substack{D \in D \\ d^oD < m}} \mu(D) \sum_{A \in F^*_{m-d^oD}} E(\frac{G}{H}D^2A^2)\Big| \leqslant q^{(m+1)/2}\ . \tag{VII-3}$$

Démonstration. Si $u \in F_m$ est premier à B, les facteurs irréductibles de U sont de degré au moins égal à m/2 et U est irréductible. Donc,

$$\sum_{\substack{P \in I \\ m/2 \leqslant d^oP < m}} E(\frac{G}{H}P^2) = \sum_{\substack{U \in F_m \\ (U,B)=1}} E(\frac{G}{H}U^2),$$

et, avec l'identité de Möbius,

$$\sum_{\substack{U \in F_m \\ (U,B)=1}} E(\frac{G}{H}U^2) = \sum_{\substack{D \in D \\ d^oD<m}} \mu(D) \sum_{\substack{U \in F_m^* \\ D|U}} E(\frac{G}{H}U^2) = \sum_{\substack{D \in D \\ d^oD<m}} \mu(D) \sum_{A \in F^*_{m-d^oD}} E(\frac{G}{H}A^2D^2)$$

d'autre part,

$$\Big| \sum_{\substack{P \in I \\ d^oP < m/2}} E\left(\frac{G}{H} P^2\right) \Big| \leqslant q^{(m+1)/2},$$

d'où la majoration (VII-3).

Si D est un polynôme de D de degré strictement inférieur à m, soit

$$S_D = \sum_{A \in F^*_{m-d^oD}} E\left(\frac{G}{H} A^2 D^2\right). \tag{VII-4}$$

Désignons par D_0 , respectivement D_1 l'ensemble des polynômes D de D tels que $\mu(D) = 1$, respectivement $\mu(D) = -1$.

PROPOSITION VII-2. *Pour* $j \in \{0,1\}$,

$$\Big| \sum_{\substack{D \in D_j \\ d^oD < r}} S_D \Big| \leqslant r q^{m-r} + q^r. \tag{VII-5}$$

Démonstration. Soit $D \in D_j \cap F_r$. Posons

$$H' = H/(H,D^2) \quad , \quad G' = GD^2/(H,D^2).$$

Les polynômes H' et G' sont premiers entre eux et

$$S_D = \sum_{A \in F^*_{m-d^oD}} E\left(\frac{G'}{H'} A^2\right)$$

Avec (VI-1) on a

$$|S_D| \leqslant 1 + \mathrm{Sup}(q^{m-d^oD} |H'|^{-1/2}, |H'|^{1/2}).$$

D'autre part,

$$d^oH' \leqslant d^oH \leqslant 2m-4r \quad \text{et} \quad d^oH' \geqslant d^oH - 2d^oD \geqslant 2r,$$

donc,

$$|S_D| \leqslant 1 + q^{m-r-d^oD},$$

et,

$$\Big| \sum_{D \in D_j \cap F_r} S_D \Big| \leqslant \sum_{D \in D \cap F_r} \left(\frac{q^{m-r}}{|D|} + 1\right) \leqslant q^r + q^{m-r} \sum_{h=0}^{r-1} 1 .$$

PROPOSITION VII-3. *Pour* $j \in \{0,1\}$,

$$\text{(VII-6)} \qquad \Big| \sum_{\substack{D \in D_j \\ r < d^o D < m-r}} S_D \Big| \leqslant 2mq^{m-r/2}.$$

Démonstration. La proposition VI-4 s'applique ici et donne

$$\Big| \sum_{\substack{D \in D_j \\ r < d^o D < m-r}} S_D \Big| \leqslant (2m-4r+1)q^m \operatorname{Sup}(|H|^{-1/8}, |H|^{1/8} q^{-m/4}, q^{-m/16}).$$

Les inégalités vérifiées par m, r et d^oH donnent alors (VII-6).

PROPOSITION VII-4. *Soit, pour tout entier* $k > 0$, $h(k)$ *le nombre de polynômes de D' de degré strictement inférieur à* k. *Alors,*

$$\text{(VII-7)} \qquad h(k) \leqslant q^{k(1-(1/2r))} + 2qr/\log^2 q.$$

Démonstration. Si $D \in D'$, D est sans facteur carré et tous ses facteurs irréductibles sont de degré strictement inférieur à 2r. Soit

$$v = 1 - (1/2r).$$

Alors,

$$h(k) \leqslant \sum_{D \in D' \cap F_k} \leqslant \sum_{D \in D' \cap F_k} (q^k/|D|)^v \leqslant q^{kv} \prod_{P \in I \cap F_{2r}} (1 + |P|^{-v}),$$

$$\log(h(k)/q^{kv}) \leqslant \sum_{P \in I \cap F_{2r}} \log(1+|P|^{-v}) \leqslant \sum_{P \in I \cap F_{2r}} |P|^{-v} \leqslant \sum_{j=1}^{2r-1} q^{(1-v)j},$$

$$\log(h(k)/q^{kv}) \leqslant \frac{q^{(1-v)2r}}{(1-v)\log q} = 2rq/\log q.$$

La majoration de h(k) s'en déduit.

PROPOSITION VII-5. *Pour* $j \in \{0,1\}$,

$$\text{(VII-8)} \qquad \Big| \sum_{\substack{D \in D' \cap D_j \\ m-r \leqslant d^o D < m}} S_D \Big| \leqslant q^{1/2}(q-1)rq^{2rq(\log q)^{-2}} q^{m(1-(1/2r))}.$$

Démonstration. Désignons cette somme par T_j'. Alors,

$$T_j' = \sum_{\substack{D\in D_j\cap D' \\ m-r\leqslant d^oD<m}} \sum_{\substack{A\in F_m^* \\ d^o(AD)<m}} E\left(\frac{G}{H}A^2D^2\right) = \sum_{A\in F_r^*} \sum_{\substack{D\in D_j\cap D' \\ m-r\leqslant d^oD<m-d^oA}} E\left(\frac{G}{H}A^2D^2\right),$$

$$|T_j'| \leqslant \sum_{A\in F_r^*} h(m-d^oA) ;$$

la majoration précédente nous donne

$$|T_j'| \leqslant q^{2rq(\log q)^{-2}} q^{(r-m)/2r} q^m \sum_{A\in F_r^*} |A|^{-1},$$

d'où (VII-8).

PROPOSITION VII-6. *Pour* $j\in\{0,1\}$,

$$\text{(VII-9)} \qquad \Big|\sum_{\substack{D\in D_j\cap D'' \\ m-r\leqslant d^oD<m}} S_D\Big| \leqslant r(q-1)(4m+2)(1+\log m)q^{m-r/4}.$$

D

Démonstration. Soit T_j'' cette somme. Comme précédemment,

$$\text{(VII-10)} \qquad T_j'' = \sum_{A\in F_r^*} \sum_{\substack{D\in D_j\cap D'' \\ m-r\leqslant d^oD<m-d^oA}} E\left(\frac{G}{H}A^2D^2\right).$$

Si $D\in D''$, D a $\omega(D)$ facteurs irréductibles unitaires P tels que $d^oP > 2r$, avec $\omega(D) < m/2r$.

Soit $K=[m/2r]$, et, pour $k=1,2,\ldots,K$, soit

$$\text{(VII-11)} \qquad T_{j,k}'' = \sum_{A\in F_r^*} \sum_{\substack{D\in D_j\cap D'' \\ \omega(D)=k \\ m-r\leqslant d^oD<m-d^oA}} E\left(\frac{G}{H}A^2D^2\right).$$

Posons pour $A\in F_r$,

$$\Theta_{j,k}(A) = \sum_{\substack{P\in I \\ 2r\leqslant d^oP<m/2}} \sum_{\substack{V\in \overline{D}_j \\ m-r\leqslant d^o(VP)<m-d^oA \\ \omega(V)=k-1}} E\left(\frac{G}{H}A^2P^2V^2\right),$$

où,

$$\overline{D}_j = \begin{cases} D_1 & \text{si} \quad j=0, \\ D_0 & \text{si} \quad j=1. \end{cases}$$

Alors,

$$T''_{j,k} = \frac{1}{k} \sum_{A \in F_r^*} \Theta_{j,k}(A) . \tag{VII-12}$$

La somme $\Theta_{j,k}(A)$ s'écrit comme différence $\Theta^{(1)} - \Theta^{(2)}$ des deux sommes

$$\Theta^{(1)} = \sum_{\substack{P \in I \\ 2r \leqslant d^o P < m/2}} \sum_{\substack{V \in \bar{D}_j \\ d^o(VP) < m - d^o A \\ \omega(V) = k-1}} E\left(\frac{G}{H} A^2 P^2 V^2\right),$$

et

$$\Theta^{(2)} = \sum_{\substack{P \in D \\ 2r \leqslant d^o P < m/2}} \sum_{\substack{V \in \bar{D}_j \\ d^p(VP) < m - r \\ \omega(V) = k-1}} E\left(\frac{G}{H} A^2 P^2 V^2\right).$$

La proposition VI-4 donne une majoration de ces sommes ; si

$$H' = H/(H, A^2) \qquad \text{et} \qquad G' = GA^2 / (H, A^2),$$

$$|\Theta^{(1)}| \leqslant (2m+1) q^{m - d^o A} \operatorname{Sup}\left(|H'|^{-1/8}, |H'|^{1/8} q^{-(m-d^o A)/4}, q^{-(m-d^o A)/16} \right),$$

$$|\Theta^{(2)}| \leqslant (2m+1) q^{m-r} \operatorname{Sup}\left(|H'|^{-1/8}, |H'|^{1/8} q^{-(m-r)/4}, q^{-(m-r)/16} \right),$$

d'où,

$$|\Theta^{(1)} - \Theta^{(2)}| \leqslant (4m+2) q^{m - d^o A} q^{-r/4},$$

et, avec (VII-10), (VII-11) et (VII-12)

$$|T''_j| \leqslant (4m+2)\, q^m q^{-r/4} \left(\sum_{k=1}^{K} \frac{1}{k} \right) \left(\sum_{A \in F_r^*} \frac{1}{|A|} \right).$$

PROPOSITION VII-7. *Il existe une constante* $C_5 > 0$, *ne dépendant que de* q *telle que, pour tout entier* $r > 0$, *pour tout entier* $m \geqslant \operatorname{Sup}(8r+1, 2r^2(2q(\log q)^{-2} + 1/4))$, *si* H *est un polynôme tel que* $d^o H \in [4r, 2m-4r]$, *si* G *est un polynôme premier à* H,

$$\left| \sum_{P \in I \cap F_m} E\left(\frac{G}{H} P^2\right) \right| \leqslant C_5\, rm \log(m) q^{m - r/4}. \tag{VII-13}$$

Démonstration. Avec (VII-3), (VII-4), (VII-5), (VII-6), (VII-8) et (VII-9), on a

$$|S| \leqslant q^{(m+1)/2} + \sum_{j=0}^{1} (rq^{m-r} + q^r + 2mq^{m-r/2} +$$

$$q^{1/2}(q-1)rq^{2qr(\log q)^{-2}} q^{m(1-(1/2r))} + (q-1)r(4m+2)(1+\log m)q^{m-r/4}) ;$$

d'où (VII-13).

VIII. - EVALUATION DE $f_i(t)$

PROPOSITION VIII-1. *Soit* $u \in \mathscr{P}$ *de valuation* $\nu(u) \geqslant i$. *Alors*

(i) *si* $\nu(u) > 2i-1$, $f_i(u) = q^i$;

(ii) *si* $\nu(u) = 2k$ *avec* $k < i$, $f_i(u) = q^k$;

(iii) *si* $\nu(u) = 2k+1$ *avec* $k < i$, *si* a *est l'élément de* $\mathbb{F}_q^*$ *tel que* $\nu(u-aX^{-2k-1}) > 2k+1$,

$$f_i(u) = q^k \sum_{b \in \mathbb{F}_q} e(ab^2).$$

Démonstration. (i) est immédiat. Pour avoir (ii) et (iii) on écrit

$$f_i(u) = 1 + \sum_{m=0}^{i-1} \sum_{A \in D_m} E(uA^2)$$

et on applique le corollaire de la proposition III-8. Si $\nu(u) = 2k$,

$$f_i(u) = 1 + \sum_{m=0}^{k-1} q^m(q-1) = q^k ;$$

si $\nu(u) = 2k+1$, et si $a \in \mathbb{F}_q^*$ est tel que $\nu(u-aX^{-2k-1}) > 2k+1$,

$$f_i(u) = 1 + \sum_{m=0}^{k-1} q^m(q-1) + q^k \sum_{b \in \mathbb{F}_q^*} e(ab^2) = q^k \sum_{b \in \mathbb{F}_q} e(ab^2).$$

On remarque que, pour $a \in \mathbb{F}_q^*$, pour tout entier $k \geqslant i$, pour $v \in \mathscr{P}_k$, $f(v+aX^{-k})$ ne dépend que de a et de k. Posons

$$f(v+aX^{-k}) = \varphi(a,k). \tag{VIII-1}$$

PROPOSITION VIII-2. *Soit* $t = \frac{G}{H} + u$ *appartenant à l'arc de Farey* $U_{G/H}$ *où* $d^oH \leqslant i$. *Alors,*

$$f_i(t) = |H|^{-1} S(G,H) f_i(u). \tag{VIII-2}$$

Démonstration. On a

$$f_i\left(\frac{G}{H}+u\right)=\sum_{R\in C_H}\ \sum_{L\in F_{i-d^oH}} E\left(\left(\frac{G}{H}+u\right)(R+LH)^2\right)=$$

$$\sum_{R\in C_H} E\left(\frac{G}{H}R^2\right)\ \sum_{L\in F_{i-d^oH}} E(u(R^2+2RHL+L^2H^2)),$$

Si $R\in C_H$ et si $L\in F_{i-d^oH}$,

$$\nu(uR^2) > N-i+2 \geqslant 2 \qquad \text{et} \qquad \nu(uLRH) > N-i+2 \geqslant 2,$$

d'où, avec (III-7) et (V-1),

$$f_i\left(\frac{G}{H}+u\right)=\sum_{R\in C_H} E\left(\frac{G}{H}R^2\right)\ \sum_{L\in F_{i-d^oH}} E(uL^2H^2)=S(G,H)\,|H|^{-1}\sum_{L\in F_i} E(uL^2).$$

PROPOSITION VIII-3. *Soit* G/H *une fraction de Farey telle que* $2s < d^oH \leqslant N$. *Alors, si* $t\in U_{G/H}$,

(VIII-3) $$|f_i(t)| \leqslant q^{i-s}.$$

Démonstration. Lorsque $d^oH \leqslant i$, les deux propositions précédentes donnent

$$|f_i(t)| \leqslant |S(G,H)|\,|H|^{-1} q^i,$$

et, (VIII-3) se déduit de (V-5).

Lorsque $d^oH > i$, $\nu\left(t-\frac{G}{H}\right) > 2(n-s) + d^oH \geqslant 2n+1$, et,

$$f_i(t) = f_i(G/H);$$

(VIII-3) se déduit alors de (VI-1).

IX. - APPROXIMATION DE g(t) SUR LES ARCS MAJEURS

Les théorèmes de répartition des nombres premiers dans les progressions arithmétiques se généralisent aux polynômes irréductibles de $\mathbf{F}_q[X]$. On a les théorèmes suivants conséquences de résultats établis dans [13] et [14].

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

$$q^m - 2q^{m/2} \leqslant m\pi(m) \leqslant q^m.$$

THEOREME B. *Soit, pour tout entier* $m > 0$, *pour tout polynôme unitaire* H, *pour tout polynôme* K *premier à* H, $\Pi(m,H,K)$ *le nombre de polynômes irréductibles de degré* m *congrus à* K *modulo* H. *Alors,*

$$|\Pi(m,H,K) - \frac{q^m(q-1)}{m\Phi(H)}| \leqslant (d^oH + 1)q^{m/2}.$$

THEOREME C. *Soit, pour tout entier* $m > 0$, *pour tout entier* $k \geqslant 0$, *pour tout polynôme unitaire* H, *pour tout polynôme* K *premier à* H, $\Pi(m,H,k,K)$ *le nombre de polynômes irréductibles* P *de degré* m, *congrus à* K *modulo* H *et tels que*

$$d^o(X^{d^oP}K - X^{d^oK}P) < d^oP + d^oK - k.$$

Alors,

$$|\Pi(m,H,k,K) - \frac{q^{m-k}}{m\Phi(H)}| \leqslant (k + d^oH + 1)q^{m/2}.$$

Ce dernier théorème correspond à une partition des polynômes irréductibles suivant les différents restes modulo H, et les différents systèmes $(a_m, \ldots, a_{m-k+1})$ possibles pour les coefficients des k termes de plus haut degré. Définissons d'une autre façon une telle partition.

DEFINITION. *Soit* H *un polynôme non nul. Les polynômes* A *et* B *sont dits équivalents modulo* R_H *si*

1) A et B sont congrus modulo H,

2) $d^o(A-B) < N$.

La proposition suivante nous donne un système de représentants des classes modulo R_H.

PROPOSITION IX-1. *Soit* H *un polynôme non nul de degré* $d^oH \leqslant 2s$, *soit* $w = N - d^oH$, *et, pour tout entier* $m \geqslant N$, *soit* A_m *l'ensemble des polynômes*

$$A = W^wHB + R$$

où B *décrit* D_{m-N}, *où* R *parcourt l'ensemble des restes modulo* H. *Alors, la réunion des classes modulo* H *et des différents ensembles* A_m *où* $m \geqslant N$ *constitue un système de représentants des classes d'équivalence modulo* R_H.

Démonstration. Remarquons que des polynômes A et B de degré différents supérieurs ou égaux à N sont distincts modulo R_H et que des polynômes A et B de degrés strictement inférieur à N congrus modulo H sont congrus modulo R_H.

Soit un entier $m \geqslant N$. Les polynômes de A_m sont de degré m. Soient

$$A = X^w HB + R \qquad \text{et} \qquad A' = X^w HB' + R'$$

des polynômes de A_m. S'ils sont équivalents modulo R_H, alors $R = R'$ et $d^o(A-A') < N$, les polynômes $X^w HB$ et $X^w HB'$ ont mêmes $m - N + 1$ premiers coefficients, il en est de même des polynômes HB et HB' qui sont de degré $m - w$, et par suite, $d^o(HB - HB') < m - w - (m-N) = d^oH$, d'où $B = B'$. Chaque ensemble A_m contient au plus un représentant de chaque classe modulo R_H, de plus,

$$\mathrm{Card}(A_m) = (q-1)q^m \mid H \mid .$$

Or, les polynômes de D_m se répartissent en exactement $(q-1)q^{m-N} \mid H \mid$ classes d'équivalence modulo R_H. A_m est donc un système complet de représentants modulo R_H des polynômes de degré m.

PROPOSITION IX-2. *Soit* t *appartenant à l'arc de Farey* $U_{G/H}$. *Alors si* A *et* A' *sont des polynômes équivalents modulo* R_H,

$$E(tA) = E(tA').$$

Démonstration. Immédiate.

PROPOSITION IX-3. *Soit* $t = \dfrac{G}{H} + u$ *appartenant à l'arc majeur* $U_{G/H}$. *Alors,*

$$\text{(IX-1)} \qquad \mid g(t) - \frac{\mu(H)}{\Phi(H)} G(\nu(u)) \mid \leqslant (q-1)(4s+1)q^{n+4s},$$

où

$$\text{(IX-2)} \qquad G(\nu(u)) = \begin{cases} (q-1) \mid M \mid (d^oM)^{-1} & si \quad \nu(u) > d^oM + 1, \\ - \mid M \mid (d^oM)^{-1} & si \quad \nu(u) = d^oM + 1, \\ 0 & si \quad \nu(u) \leqslant d^oM . \end{cases}$$

Démonstration. Posons $d^oM = m$. Utilisons le système de représentants des classes modulo R_H donné par la proposition IX-1. Si $A \in A_m$, notons provisoirement P(m;H,A) le nombre de polynômes irréductibles de degré m équivalents à A modulo R_H. Alors,

$$g(t) = \sum_{P \in I_m} E(tP) = \sum_{A \in A_m} E(tA)\, P(m;H,A) .$$

Si A et H ne sont pas premiers entre eux, et si P est un polynôme irréductible congru à A modulo H, P divise H ; ceci ne pouvant se produire pour des polynômes P de degré $m \geqslant 2n-1 > d^oH$,

$$g(t) = \sum_{\substack{A \in A_m \\ (A,H)=1}} E(tA)\, P(m,H,A)\,.$$

Si les polynômes A et P de degré m sont équivalents modulo R_H, ils sont congrus modulo H, et,

$$d^o(X^{d^oA}P - X^{d^oP}A) < m + N = d^oA + d^oP - (m-N)\,;$$

le nombre P(m;H,A) est donc le nombre $\Pi(m;H,m-N,A)$ intervenant au théorème C ; d'où,

$$\left| g(t) - \frac{q^N}{m\Phi(H)} \sum_{\substack{A \in A_m \\ (A,H)=1}} E(At) \right| \leqslant (q-1)\, q^{m-N}\, \Phi(H)(m-N+d^oH+1)q^{m/2}.$$

Utilisons la définition de A_m et le fait que $d^oH \leqslant 2s$,

$$\left| g(t) - \frac{q^N}{m\Phi(H)} \sum_{R \in C_H^*} E\left(\frac{G}{H}R\right) E(uR) \sum_{B \in D_{m-N}} E(uX^wHB) \right| \leqslant (q-1)(4s+1)q^{n+4s}.$$

Si $R \in C_H$, $\nu(uR) > 1$ et $E(uR) = 1$; de plus, comme pour le théorème 3-1, chapitre VI de [12], on a

$$\sum_{R \in C_H^*} E\left(\frac{G}{H}R\right) = \mu(H)\,,$$

d'où,

$$\text{(IX-3)} \qquad \left| g(t) - \frac{q^N \mu(H)}{m\Phi(H)} \sum_{B \in D_{m-N}} E(uX^wHB) \right| \leqslant (q-1)(4s+1)q^{n+4s}\,.$$

On a

$$m+1-N > m-N > -N = \nu(X^wH) > -\nu(u)\,.$$

La «première formule de changement de variable» donne

$$\sum_{B \in D_{m-N}} E(uX^wHB) = \frac{1}{|X^wH|} \sum_{B \in D_m} E(uB) = \begin{cases} (q-1)q^{m-N} & \text{si} \quad \nu(u) > m+1, \\ -q^{m-N} & \text{si} \quad \nu(u) = m+1, \\ 0 & \text{si} \quad \nu(u) \leqslant m\,. \end{cases}$$

La valeur de cette somme ne dépend que de la valuation de u. On pose

$$G(\nu(u)) = \frac{1}{m} \sum_{B \in D_m} E(uB),$$

d'où (IX-2) ; (IX-1) se déduit alors de (IX-3).

COROLLAIRE. *Sous les mêmes hypothèses,*

$$|g^2(t) - \frac{\mu^2(H)}{\Phi^2(H)} G^2(\nu(u))| \leqslant 2(q-1)^2(4s+1)q^{3n+4s}(d^oM)^{-1}. \tag{IX-4}$$

Démonstration. Le théorème A nous donne la majoration triviale

$$|g(t)| \leqslant (q-1)q^m/m ;$$

on conclut avec (IX-1) et (IX-2).

X. - EVALUATION DE $f_i^*(t)$

L'étude de f_i^* sur les arcs majeurs est semblable à celle de la fonction g. Nous avons besoin d'une équivalence $R_{i,H}$ donnant une partition de l'ensemble des polynômes irréductibles plus fine que celle donnée par la relation R_H.

DEFINITION. *Soit* H *un polynôme non nul. Les polynômes* A *et* B *seront dits équivalents modulo* $R_{i,H}$ *si*

1) A *et* B *sont congrus modulo* H,
2) $d^oA < i-s$ *et* $d^oB < i-s$ *ou* $d^oA \geqslant i-s$ *et* $d^o(A-B) < 2i-2s-d^oA$.

La proposition suivante donne, pour un polynôme H appartenant à F_{2s+1}, un système de représentants des classes modulo $R_{i,H}$.

PROPOSITION X-1. *Soit* H *un polynôme de degré au plus* 2s. *Soient, pour tout entier* $r \in \{i-s,\ldots,i-1\}$,

$$w(i,r) = 2(i-s) - r - d^oH,$$

et $A_i(r)$ *l'ensemble des polynômes*

$$A = X^{w(i,r)}HB + R$$

où R *décrit* C_H, *où* B *décrit* $D_{2(r+s-i)}$. *Alors, la réunion de* C_H *et des ensembles* $A_i(R)$ $(i-s \leqslant r < i)$ *constitue un système de représentants des classes modulo* $R_{i,H}$ *des polynômes de* F_i.

Démonstration. Comme pour la proposition IX-1.

PROPOSITION X-2. *Soit* t *appartenant à l'arc majeur* $U_{G/H}$. *Si* A *et* B *sont des polynômes équivalents modulo* $R_{i,H}$, *alors,*

$$E(tA^2) = E(tB^2).$$

Démonstration. Immédiate.

DEFINITIONS. *Pour tout entier* $k \geqslant 2$, *soit*

$$\sigma_k = (q-1)\sum_{r=1}^{k-1} q^r/r, \tag{X-1}$$

et soit Ψ_i *l'application de* $\mathscr{P}_N$ *dans* $\mathbb{C}$ *définies par*

$$\Psi_i(u) = \begin{cases} \sigma_i \quad si \quad \nu(u) > 2i-1, \\ \sigma_k \quad si \quad \nu(u) = 2k \quad avec \quad k < i, \\ \sigma_k + q^k \Big(\sum_{b \in \mathbb{F}_q^*} e(ab^2)\Big)/k \quad si \\ \nu(u) = 2k+1 \ avec \ k < i \ et \ si \ a \ est \\ l'élément \ de \ \mathbb{F}_q^* \ tel \ que \ \nu(u - aX^{-\nu(u)}) > \nu(u). \end{cases} \tag{X-2}$$

On remarque que si $u = aX^{-\nu(u)} + v$ avec $a \in \mathbb{F}_q^*$ et $\nu(v) > \nu(u)$, $\Psi_i(u)$ ne dépend que de a et de $\nu(u)$. Posons

$$\Psi_i(u) = \varphi_i^*(a, \nu(u)). \tag{X-3}$$

PROPOSITION X-3. *Il existe une constante* $C_6 > 0$, *ne dépendant que de* q, *telle que, si* $t = G/H + u$ *appartient à l'arc majeur* $U_{G/H}$,

$$\left| f_i^*(t) - \frac{S^*(G,H)}{\Phi(H)} \Psi(u) \right| \leqslant C_6 \, s \, q^{4s} q^{i/2}. \tag{X-4}$$

Démonstration. On a

$$f_i^*(t) = \sum_{r=1}^{i-1} S_r(t) \qquad \text{où} \qquad S_r(t) = \sum_{P \in I_r} E(tP^2). \tag{X-5}$$

Utilisons le système de représentants des classes modulo $R_{i,H}$ donné par la proposition X-1. Si $r \in \{i-s,\ldots,i-1\}$, si $A \in A_i(r)$, notons $P_i(r,H,A)$ le nombre de polynômes irréductibles de degré r équivalents à A modulo $R_{i,H}$ si $r \in \{1,\ldots,i-s-1\}$, si $R \in C_H$, notons $p_i(r,H,R)$ le nombre de

polynômes irréductibles de degré r équivalents à R modulo $R_{i,H}$. Alors, pour $r \in \{i-s,\dots,i-1\}$,

$$S_r(t) = \sum_{\substack{A \in A_i(r) \\ (A,H)=1}} E(tA^2)P_i(r;H,A),$$

pour $r \in \{d^oH+1,\dots,i-s+1\}$,

$$S_r(t) = \sum_{R \in C_H^*} E(tR^2)p_i(r;H,R),$$

et, pour $r \in \{1,\dots,d^oH\}$,

$$S_r(t) = \sum_{R \in C_H} E(tR^2)p_i(r;H,R).$$

Si A et H sont premiers entre eux, $P_i(r;H,A)$ est égal au nombre $\Pi(r;H,2r-2i+2s,A)$ du théorème C, si R et H sont premiers entre eux, $p_i(r;H,R)$ est égal au nombre $\Pi(r;H,R)$ du théorème B. Donc en procédant comme pour la fonction g, on obtient pour $r \in \{i-s,\dots,i-1\}$,

$$|S_r(t) - \sum_{R \in C_H^*} E\left(\frac{G}{H}R^2\right) \sum_{B \in D_{2(r+s-i)}} E(u(R+X^{w(i,r)}HB)^2) \frac{q^{2i-2s-r}}{r\Phi(H)}| \leqslant$$

$$(q-1)\Phi(H)q^{2(r+s-i)}q^{r/2}(2r-2i+2s+d^oH+1) \leqslant 4s(q-1)q^{2(r+2s-i)}q^{r/2}.$$

Si $R \in C_H$, si $B \in D_{2(r+s-i)}$,

$$E(u(R + X^{w(i,r)}HB)^2) = E(uX^{2w(i,r)}H^2B^2),$$

la deuxième «formule de changement de variable» donne alors,

$$(X\text{-}6) \qquad |S_r(t) - \frac{1}{r\Phi(H)} \sum_{R \in C_H^*} E\left(\frac{G}{H}R^2\right) \sum_{B \in D_r} E(uB^2)| \leqslant 4s(q-1)q^{2(r+2s-i)}q^{r/2}.$$

De la même façon, pour $r \in \{d^oH+1,\dots,i-s-1\}$,

$$(X\text{-}7) \qquad |S_r(t) - \frac{(q-1)q^r}{r\Phi(H)} \sum_{R \in C_H^*} E\left(\frac{G}{H}R^2\right)| \leqslant (2s+1)q^{2s}q^{r/2},$$

et, pour $r \in \{1,\dots,d^oH\}$,

$$(X\text{-}8) \qquad |S_r(t) - \frac{(q-1)q^r}{r\Phi(H)} \sum_{R \in C_H^*} E\left(\frac{G}{H}R^2\right)| \leqslant (2s+1)q^{2s}q^{r/2} + \Delta_r(H),$$

où $\Delta_r(H)$ désigne le nombre de diviseurs irréductibles de H de degré r. On remarque que si $r \in \{1,\ldots,i-s-1\}$,

$$\sum_{B \in D_r} E(uB^2) = \mathrm{Card}(D_r) = (q-1)q^r ,$$

donc, avec (X-5), (X-6), (X-7), (X-8), le corollaire de la proposition III-8, les définitions (X-1) et (X-2), en majorant la somme des $\Delta_r(H)$ par d^oH, on obtient

$$| f_i^*(t) - \Phi(H)^{-1} \sum_{R \in C_H^*} E\left(\frac{G}{H}R^2\right)\Psi_i(u) | \leqslant C_6\, s\, q^{4s} q^{i/2} ,$$

C_6 étant une constante qui ne dépend que de q.

Sur $\mathfrak{a}'$ on a simplement une majoration de $f_i^*(t)$.

PROPOSITION X-4. *Il existe une constante* $C_7 > 0$, *ne dépendant que de* q, *telle que, si* $t \in \mathfrak{a}'$,

$$| f_i^*(t) | \leqslant C_7\, i s \log(i) q^i q^{-s/8} . \tag{X-9}$$

Démonstration. Si $t \in \mathfrak{a}'$, il existe un arc de Farey $U_{G/H}$ tel que $t \in U_{G/H}$ et $2s < d^oH \leqslant 2n-2s < 2(n+1)-2s$. Alors, si $A \in F_i$,

$$E(tA^2) = E\left(\frac{G}{H}A^2\right) .$$

Donc,

$$f_i^*(t) = \sum_{P \in I \cap F_i} E\left(\frac{G}{H}P^2\right) ,$$

comme $i \in \{n, n+1\}$, et que n vérifie la condition (IV-1), on peut appliquer la proposition VII-7 avec $r = [s/2]$, ce qui nous donne le résultat annoncé.

XI. - APPROXIMATION DE $R_i(M)$ ET DE $R_i^*(M)$

Posons

$$J_i(M) = \int_{\mathfrak{a}} f_i(t) g^2(t) E(-Mt)dt \quad ; \quad J_i'(M) = \int_{\mathfrak{a}'} f_i(t) g^2(t) E(-Mt)dt .$$

$$J_i^*(M) = \int_{\mathfrak{a}} f_i^*(t) g^2(t) E(-Mt)dt \quad ; \quad J_i'^*M) = \int_{\mathfrak{a}'} f_i^*(t) g^2(t) E(-Mt)dt.$$

PROPOSITION XI-1. *On a les majorations :*

$$|J'_i(M)| \leqslant (q-1)\,|M|\,q^{i-s}(d^oM)^{-1}, \tag{XI-1}$$

$$|J'^*_i(M)| \leqslant C_7(q-1)is(\log i)q^i q^{-s/8}\,|M|\,(d^oM)^{-1}. \tag{XI-2}$$

Démonstration. Si $t \in \mathcal{A}'$, $|f_i(t)| \leqslant q^{i-s}$, d'où,

$$|J'_i(M)| \leqslant q^{i-s}\int_{\mathcal{A}'} |g^2(t)|\,dt \leqslant q^{i-s}\int_{\mathcal{P}} |g^2(t)|\,dt = q^{i-s}\,\mathrm{Card}(I_{d^oM});$$

(XI-1) se déduit alors du théorème A.

De même, si $t \in \mathcal{A}'$,

$$|f^*_i(t)| \leqslant C_7\, is\,(\log i)\, q^i q^{-s/8},$$

et une majoration analogue conduit à (XI-2).

PROPOSITION XI-2. *Soient*

$$K_n(M) = (q-2)q^n\,|M|\,(d^oM)^{-2}, \tag{XI-3}$$

$$K^*_n(M) = (q-2)\sigma_n\,|M|\,(d^oM)^{-2}, \tag{XI-4}$$

et, si M *est de degré pair, soient*

$$K_{n+1}(M) = (q^2-2q+\rho(M))q^n\,|M|\,(d^oM)^{-2}, \tag{XI-5}$$

$$K^*_{n+1}(M) = ((q-2)\sigma_n + q^n(q-3+\rho(M)+\frac{2}{q})/n)\,|M|\,(d^oM)^{-2}, \tag{XI-6}$$

où,

$$\rho(M) = \begin{cases} 2 & \textit{si} \quad \mathrm{sgn}(M) \quad \textit{est carré dans } \mathbb{F}_q, \\ 0 & \textit{si} \quad \mathrm{sgn}(M) \quad \textit{n'est pas carré dans } \mathbb{F}_q. \end{cases}$$

Alors, si $i \in \{n,n+1\}$, *pour tout arc majeur* $U_{G/H}$,

$$|I_{i,G/H}(M) - K_i(M)\frac{\mu^2(H)S(G,H)}{|H|\,\Phi(H)}E(-M\frac{G}{H})| \leqslant C_8\, sq^{n+i+6s}(d^oM)^{-1}, \tag{XI-7}$$

(XI-8) $$|I^*_{i,G/H}(M) - K^*_i(M)\frac{\mu^2(H)S^*(G,H)}{\Phi^3(H)}E(-M\frac{G}{H})| \leqslant C_9\, sq^{2n+6s}q^{i/2}(d^oM)^{-2},$$

C_8 *et* C_9 *étant des constantes qui ne dépendent que de* q.

Démonstration. Soit $t = \frac{G}{H} + u$ appartenant à l'arc majeur $U_{G/H}$. Alors, avec (VIII-2), (IX-4), (IX-2), (X-1) et (X-2),

$$|f_i(t)g^2(t) - \frac{\mu^2(H)S(G,H)}{|H|\Phi^2(H)}f_i(u)G^2(\nu(u))| \leqslant 2(q-1)^2(4s+1)q^{3n+4s+i}(d^oM)^{-1}$$

$$|f^*_i(t)g^2(t) - \frac{\mu^2(H)S^*(G,H)}{\Phi^3(H)}\Psi_i(u)G^2(\nu(u))| \leqslant C_6\, sq^{4s}q^{i/2}(q-1)^2|M|^2(d^oM)^{-2}.$$

Posons

(XI-9) $$K_i(M) = \int_{\nu(u) > N+d^oH} f_i(u)G^2(\nu(u))E(-Mu)du,$$

(XI-10) $$K^*_i(M) = \int_{\nu(u) > N+d^oH} \Psi_i(u)G^2(\nu(u))E(-Mu)du.$$

Alors,

$$|I_{i,G/H}(M) - K_i(M)\frac{\mu^2(H)S(G,H)}{|H|\Phi^2(H)}E(-M\frac{G}{H})| \leqslant C_8\, sq^{n+i+6s}(d^oM)^{-1},$$

$$|I^*_{i,G/H}(M) - K^*(M)\frac{\mu^2(H)S^*(G,H)}{\Phi^3(H)}E(-M\frac{G}{H})| \leqslant C_9\, sq^{2n+6s}q^{i/2}(d^oM)^{-2},$$

C_8 et C_9 étant des constantes qui ne dépendent que de q. Pour avoir la proposition il suffit de montrer que $K_i(M)$ et $K^*_i(M)$ définis par les relations (XI-9) et (XI-10) vérifient les égalités (XI-3), (XI-4), (XI-5) et (XI-6).

On a vue que $G(\nu(u))$ est nul si $d^oM \geqslant \nu(u)$. D'autre part, si $\nu(u) > d^oM$, $\nu(u) > 2n-1$, et, d'après la proposition VIII-1 et la définition (X-2),

$$f_n(u) = q^n \quad \text{et} \quad \Psi_n(u) = \sigma_n .$$

En remplaçant $G(\nu(u))$ par sa valeur on obtient

$$K_n(M) = q^n\left(\left(\frac{|M|(q-1)}{d^oM}\right)^2 \int_{\mathscr{P}_{d^oM+1}} E(-Mu)du + \left(\frac{|M|}{d^oM}\right)^2 \sum_{b\in \mathbf{IF}_q^*} \int_{\mathscr{P}_{d^oM+1}} E(-M(u+bX^{-d^oM-1}))du\right),$$

$$K_n(M) = \frac{q^{n-1}|M|}{(d^oM)^2}\left((q-1)^2 + \sum_{b\in \mathbf{IF}_q^*} e(-b\,\mathrm{sgn}(M))\right) = \frac{q^{n-1}|M|}{(d^oM)^2}\left((q-1)^2-1\right),$$

$$K_n(M) = \frac{q^n|M|}{(d^oM)^2}(q-2);$$

et, de la même façon,

$$K_n^*(M) = \frac{\sigma_n|M|}{(d^oM)^2}(q-2).$$

Le cas $i = n+1$ ne nous intéresse que si $d^oM = 2n$; on a alors, avec la proposition VIII-1,

$$K_{n+1}(M) = \frac{q^{n+1}|M|^2(q-1)^2}{(d^oM)^2} \int_{\mathscr{P}_{2n+1}} E(-Mu)du + \sum_{b\in \mathbf{IF}_q^*} \int_{\mathscr{P}_{2n+1}} \varphi(b,2n+1)G^2(2n+1)E(-M(u+bX^{-2n-1}))du,$$

en remplaçant $\varphi(b,2n+1)$ et $G(2n+1)$ par les valeurs on obtient

$$K_{n+1}(M) = \frac{q^n(q-1)^2|M|}{(d^oM)^2} + \sum_{b\in \mathbf{IF}_q^*} q^n \sum_{c\in \mathbf{IF}_q} e(bc^2)\frac{|M|q^{-1}}{(d^oM)^2}\, e(-b\,\mathrm{sgn}(M)),$$

$$K_{n+1}(M) = \frac{q^n|M|}{(d^oM)^2}\left((q-1)^2 + q^{-1}\sum_{c\in \mathbf{IF}_q}\sum_{b\in \mathbf{IF}_q^*} e(b(c^2-\mathrm{sgn}(M))\right).$$

Soit $\rho(M)$ le nombre d'éléments $c \in \mathbf{IF}_q$ tels que $\mathrm{sgn}(M) = c^2$. Alors,

$$K_{n+1}(M) = \frac{q^n|M|}{(d^oM)^2}\left((q-1)^2 + q^{-1}(\rho(M)(q-1) - (q-\rho(M))\right),$$

$$K_{n+1}(M) = \frac{q^n|M|}{(d^oM)^2}\left(q^2 - 2q + \rho(M)\right).$$

Avec la définition (X-4) il vient

$$K^*_{n+1}(M) = \frac{\sigma_{n+1}\,|M|^2\,(q-1)^2}{(d^oM)^2} \int_{\mathscr{P}_{2n+1}} E(-Mu)du +$$

$$\sum_{b\in \mathbf{IF}_q^*} \int_{\mathscr{P}_{2n+1}} \varphi^*(b,2n+1)G^2(2n+1)E(-M(u+bX^{-2n-1}))du,$$

d'où,

$$K^*_{n+1}(M) = \frac{\sigma_{n+1}\,|M|\,(q-1)^2 q^{-1}}{(d^oM)^2} + \sum_{b\in \mathbf{IF}_q^*} (\sigma_n + \frac{q^n}{n} \sum_{c\in \mathbf{IF}_q^*} e(bc^2)) \frac{|M|\,q^{-1}}{(d^oM)^2} e(-\mathrm{sgn}(M)b),$$

$$K^*_{n+1}(M) = \frac{|M|\,q^{-1}}{(d^oM)^2} (\sigma_{n+1}(q-1)^2 + \sigma_n \sum_{b\in \mathbf{IF}_q^*} e(-b\mathrm{sgn}(M) + \frac{q^n}{n} \sum_{\substack{b\in \mathbf{IF}_q^* \\ c\in \mathbf{IF}_q^*}} e(b(c^2-\mathrm{sgn}(M))$$

$$K^*_{n+1}(M) = \frac{|M|\,q^{-1}}{(d^oM)^2} (\sigma_{n+1}(q-1)^2 - \sigma_n + q^n(\rho(M)(q-1) - (q-1-\rho(M)))),$$

$$K^*_{n+1}(M) = \frac{|M|}{(d^oM)^2}(\sigma_n(q-2) + q^n(q-3+\rho(M)+2/q))/n).$$

On a les minorations :

(XI-7) $$K_{n+1}(M) \geqslant (q-2)q^{n+1}\,|M|\,(d^oM)^{-2},$$

(XI-8) $$K^*_n(M) \geqslant (q-2)(q-1)q^{-1}\,q^n\,|M|\,n^{-1}\,(d^oM)^{-2},$$

(XI-9) $$K^*_{n+1}(M) \geqslant (q-2)q^{-2}\,q^{n+1}\,|M|\,n^{-1}(d^oM)^{-2}.$$

PROPOSITION XI-3. *Il existe des constantes* C_{10} *et* C_{11} *, ne dépendant que de* q, *telles que, pour tout polynôme* M *de degré* 2n *ou* 2n−1,

(XI-14) $$|R_n(M) - K_n(M)\mathcal{G}(M)| \leqslant C_{10}\,K_n(M)n^{-32},$$

(XI-15) $$|R^*_n(M) - K^*_n(M)\mathcal{G}(M)^*| \leqslant C_{11}\,K_n(M)n^{-1},$$

et, pour tout polynôme M *de degré* 2n,

(XI-16) $$|R_{n+1}(M) - K_{n+1}(M)\,\mathcal{G}(M)| \leqslant C_{10}\,K_{n+1}(M)n^{-32},$$

(XI-17) $$|R^*_{n+1}(M) - K^*_{n+1}(M)\mathcal{G}(M)^*| \leqslant C_{11}\,K^*_{n+1}(M)n^{-1}.$$

Démonstration. Avec la proposition précédente, (XI-1) et (V-13) on a

$$|R_i(M) - K_i(M)\,\mathcal{G}(M)| \leqslant K_i(M)C_2q^{-s} + (q-1)\,|M|\,q^{i-s}(d^oM)^{-1} +$$

$$C_8 s\frac{q^{n+i+6s}}{d^oM} \sum_{\substack{H \in U \\ d^oH \leqslant 2s}} \Phi(H),$$

d'où, avec (XI-3) et (XI-11),

$$|R_i(M) - K_i(M)\mathcal{G}(M)| \leqslant K_i(M)\left(C_2q^{-s} + \frac{q-1}{q-2}\,d^oM\,q^{-s} + C_8 sq^{10s+n}\,d^oM/.\,M\,|(q-2)\right),$$

et (XI-14) et (XI-16) se déduisent du choix de s.

De la même façon, avec (XI-2) et (V-17),

$$|R^*_i(M) - K^*_i(M)\mathcal{G}(M)^*| \leqslant K^*_i(M)C_4q^{-s} + C_7(q-1)i\log(i)q^iq^{-s/8}\,|M|\,(d^oM)^{-1} +$$

$$C_9 sq^{2n+6s}q^{i/2}(d^oM)^{-2} \sum_{\substack{H \in U \\ d^oH \leqslant 2s}} \Phi(H),$$

et, avec (XI-12) et (XI-13),

$$|R^*_i(M) - K^*_i(M)\mathcal{G}(M)^*| \leqslant K^*_i(M)(C_4q^{-s} + C_7(q^2(q-1)/q-2)i^2\log(i)d^oMq^{-s/8}$$

$$+ C_9(q^3/q-2)q^{10s-n}q^{i/2}),$$

ici encore (XI-15) et (XI-17) se déduisent de (IV-7).

Cette dernière proposition achève la démonstration du théorème et montre que les nombres $R_i(M)$ et $R^*_i(M)$ sont asymptotiquement équivalents aux nombres strictement positifs $K_i(M)\mathcal{G}(M)$ et $K^*_i(M)\mathcal{G}(M)^*$.

NOTE DE LA REDACTION

«En raison d'une erreur matérielle du secrétariat de rédaction, la démonstration imprimée de la proposition VI-2 est incomplète. Un erratum sera publié dans le fascicule 3-4, 1981».

REFERENCES

[1] R. AYOUB. *«An introduction to the analytic theory of numbers»*. Mathematical Surveys n° 10, Amer. Math. Soc.

[2] M. CAR. *«Le problème de Waring pour l'anneau des polynômes sur un corps fini»*. C.R.A.S., Paris, Série A et B, 273, (1971).

[3] L. CARLITZ. *«On the representations of a polynomial on a Galois field as the sum of an even number of squares»*. Trans. Amer. Math. Soc., 35, (1933), pp. 397-410.

[4] L. CARLITZ. *«On the representations of a polynomial on a Galois field as the sum of an odd number of squares»*. Duke Math. Jour., 1, (1935), pp. 298-315.

[5] L. CARLITZ. *«Sums of squares of polynomials»*. Duke Math Jour., 3, (1937), pp. 1-7.

[6] L. CARLITZ. *«The singular series for sums of squares of polynomials»* Duke Math. Jour., 14, (1947), pp. 1105-1120.

[7] L. CARLITZ. *«A note on sums of three squares in* GF[q,x] ». Mathematics Magazine, 48, (1975), pp. 109-110.

[8] ECKFORD-COHEN. *«Sums of an even numbers of squares in* $GF[p^n,x]$, I». Duke Math. Jour., 14, (1947), pp. 251-267.

[9] ECKFORD-COHEN. *«Sums of an even number of squares in* $GF[p^n,x]$, II». Duke Math. Jour., 14, (1947), pp. 543-557.

[10] ELLISON & MENDES-FRANCE. *«Les nombres premiers»*. Hermann, Paris.

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

[12] K. PRACHAR. *«Primzahlverteilung»*. Springer-Verlag, Berlin.

[13] G. RHIN. *«Répartition modulo 1 dans un corps de séries formelles sur un corps fini»*. Thèse soutenue à l'Université de Paris VI, (1971).

[14] G. RHIN. *«Répartition modulo 1 dans un corps de séries formelles sur un corps fini»*. Dissertationes mathematicae, (1972).

[15] W. WEBB. *«Waring's problem in* GF[q,x] ». Acta. Arith., 22, (1972), pp. 207-220.

[16] W. WEBB. *«On the representation of polynomials over finite fields as sums of powers and irreducibles»*. Rocky Mountain J. Math., 3, (1973), pp. 23-29.

(Manuscrit reçu le 11 janvier 1980)