ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

MIREILLE CAR

Sommes d'un carré et d'un polynôme irréductible dans $IF_q[X]$

Annales de la faculté des sciences de Toulouse 5^e série, tome 6, n° 3-4 (1984), p. 185-213

<http://www.numdam.org/item?id=AFST_1984_5_6_3-4_185_0>

Annales Faculté des Sciences Toulouse
Vol VI, 1984, P 185 à 213

SOMMES D'UN CARRE ET D'UN POLYNOME IRREDUCTIBLE DANS $\mathbb{F}_q[X]$

Mireille Car *(1)*

(1) Laboratoire de Théorie des nombres, Faculté de St-Jérôme Rue Henri Poincaré 13397 Marseille Cédex 13 - France

Résumé : Soit $\mathbb{F}_q$ le corps fini à q éléments, q étant un entier impair $\geqslant 5$. On démontre ici que presque tout polynôme M de $\mathbb{F}_q[X]$ de degré au plus 2n admet une représentation comme somme

$$M = P + A^2,$$

où P est un polynôme irréductible de degré au plus 2n, où A est un polynôme de degré au plus n. On obtient aussi une estimation asymptotique du nombre de ces représentations.

Summary : Let $\mathbb{F}_q$ be the finite field with q element, q being odd $\geqslant 5$. We prove here that almost every polynomial M in $\mathbb{F}_q[X]$ of degree less than 2n has a representation as a sum

$$M = P + A^2,$$

where P is an irreducible polynomial of degree less than 2n, where A is a polynomial of degree less than n. We also get an asymptotic estimate for the number of these representations.

I. - INTRODUCTION

Soit $\mathbb{F}_q$ le corps fini à q éléments, q étant un entier impair et $\mathbb{F}_q[X]$ l'anneau des polynômes à une variable sur le corps $\mathbb{F}_q$. On a démontré dans [1] que tout polynôme de $\mathbb{F}_q[X]$ de degré «assez élevé» est représentable comme somme

$$P_1 + P_2 + A^2$$

où P_1 et P_2 sont des polynômes irréductibles, où A est un polynôme, ces polynômes étant soumis aux conditions de degré les plus restrictives possibles.

Il semble raisonnable de formuler pour les polynômes de $\mathbb{F}_q[X]$ une conjecture analogue à celle formulée par LITTLEWOOD [2] sur les entiers, à savoir :

«Si M *est un polynôme non carré dans* $\mathbb{F}_q[X]$ *de degré* 2n *ou* 2n−1, M *est représentable comme somme*

$$M = P + A^2$$

où P *est un polynôme irréductible de degré au plus* 2n, *où* A *est un polynôme de degré au plus* n».

En adaptant à $\mathbb{F}_q[X]$ la méthode utilisée dans [5] nous démontrons le théorème suivant :

THEOREME. *Soit* $\mathbb{F}_q$ *le corps fini à* q *éléments,* q *étant un entier impair,* $\geqslant 5$. *Alors, presque tous les polynômes de* $\mathbb{F}_q[X]$ *de degré au plus* 2n *peuvent s'écrire comme somme* $P + A^2$ *où* P *est un polynôme irréductible de degré au plus* 2n, *où* A *est un polynôme de degré au plus* n. *Le nombre d'exeptions est, quel que soit le nombre réel* $b > 0$, *au plus* $O(q^{2n}n^{-b})$, *les constantes impliquées par le symbole* O *ne dépendant que de* q *et de* b.

Notons que les conditions de degré exigées dans de telles représentations sont moins restrictives que celles formulées dans la conjecture.

La démonstration de ce théorème fournira en outre, pour presque tout polynôme M de degré au plus 2n, une estimation asymptotitque du nombre R(M) de solutions (P,A) de l'équation

$$M = P + A^2,$$

où P est un polynôme irréductible de degré au plus 2n, où A est un polynôme de degré au plus n.

II. - NOTATIONS ET CONVENTIONS

Nous reprenons les notations introduites en [1]. Le mot polynôme désignera toujours un polynôme de $\mathbf{IF}_q[X]$.

Soit H un polynôme. On note d^oH le degré de H, 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 C_H^*, l'ordre de ce groupe $\Phi(H)$. La fonction Φ ainsi définie est analogue à la fonction d'Euler classique. On désigne par $\omega(H)$ le nombre de facteurs irréductibles unitaires distincts de H.

On désigne par U l'ensemble des polynômes unitaires et par I l'ensemble des polynômes irréductibles unitaires. Sur U on définit la fonction de Môbius μ par

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

L'ensemble des polynômes H tels que $d^oH \leqslant m$ sera noté $\mathbf{F}_m$, l'ensemble des polynômes irréductibles P tels que $d^oP \leqslant m$ sera noté $\mathbf{I}_m$.

Si A,B et H sont des polynômes, la relation A divise B sera notée $A \mid B$, la relation A est congru à B modulo H sera notée $A \equiv B \pmod H$, le plus grand diviseur commun unitaire de A et de B sera noté (A,B).

Soient P un polynôme irréductible et M un polynôme non divisible par P. On définit le symbole de Legendre $(\frac{M}{P})$

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

Sur le corps $\mathbf{IF}_q(X)$ 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 $\mathbf{IF}_q(X)$ pour cette valuation s'identifie au corps $\mathbf{IK}$ des séries de Laurent formelles en 1/X à coefficients dans $\mathbf{IF}_q$, la valuation ν se prolonge à $\mathbf{IK}$ par

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

$\mathbb{Z}$ désignant l'anneau des entiers relatifs. A cette valuation ν est associée la valeur absolue $|\ |_\nu$ définie par

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

Nous noterons simplement $|\ |$ cette valeur absolue bien que ce dernier symbole désigne aussi la valeur absolue classique sur le corps $\mathbb{R}$ des nombres réels et le corps $\mathbb{C}$ des nombres complexes. On désigne par P l'idéal de valuation, et, pour tout entier relatif j, on désigne par P_j l'idéal

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

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

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

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

Soit un entier $N > 0$. On appelle *fraction de Farey à l'ordre* N toute fraction rationnelle G/H telle que

(i) H est un polynôme unitaire de $\mathbb{F}_N$,

(ii) $G \in C_H^*$.

L'ensemble des fractions de Farey à l'ordre N sera noté $\mathbb{R}_N$. Si G/H est une fraction de Farey à l'ordre N, on appelle *arc de Farey à l'ordre* N *de centre* G/H la boule

$$U_{G/H} = \frac{G}{H} + P_{N+d^oH}.$$

Lorsque G/H décrit $\mathbb{R}_N$ les arcs de Farey $U_{G/H}$ forment une participation de la boule unité P. C'est le théorème 4-3 de [4]. Une telle partition sera dite *dissection de Farey à l'ordre* N de P.

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

Dans ce qui suit, lorsqu'il n'y aura pas d'indication supplémentaire, les constantes impliquées par les symboles $\ll$, $\gg$ et O ne dépendront que de q ou seront absolues.

La référence à la formule (X–y), resp. à la formule (y) sera la référence à la formule (y) du chapitre X antérieur, resp. à la formule (y) du chapitre en cours.

III. - ESTIMATIONS DEDUITES DU THEOREME DES NOMBRES PREMIERS

Les polynômes de $\mathbb{F}_q[X]$ ont une répartition analogue à celle des nombres premiers, comme le montre le théorème suivant.

THEOREME Π. *Soit, pour tout entier* $n \geqslant 1$, $\pi(n)$ *le nombre de polynômes irréductibles unitaires de degré* n. *Alors, on a*

$$q^n - 2q^{n/2} \leqslant n\,\Pi(n) \leqslant q^n. \tag{1}$$

Démonstration. C'est le lemme 1 de [6].

PROPOSITION III-1. *Soit, pour tout entier* $n \geqslant 1$, $\Pi(n)$ *le nombre de polynômes irréductibles unitaires de degré au plus égal à* n. *Alors, on a*

$$(1-2/3^{3/2})\ q^n/n \leqslant \Pi(n) \leqslant q^{n+1}/(n+1). \tag{2}$$

Démonstration. C'est une conséquence immédiate du théorème Π.

PROPOSITION III-2. *1) Pour tout entier* $n \geqslant 1$, *on a*

$$\log(n) - 2/(\sqrt{q}-1) \leqslant \sum_{\substack{P \in I \\ d^oP \leqslant n}} \frac{1}{|P|} \leqslant 1 + \log(n). \tag{3}$$

2) Soit $u \in]0,1[$. *Alors, pour tout entier* $n \geqslant 1$, *on a*

$$\sum_{\substack{P \in I \\ d^oP \leqslant n}} |P|^{-u} \ll \frac{q^{n(1-u)}}{n}, \tag{4}$$

la constante impliquée par le symbole $\ll$ *ne dépendant que de* q *et de* u.

3) Pour tout polynôme M *de degré au moins égal à* 2, *on a*

$$|M| / \Phi(M) \ll \log(d^oM). \tag{5}$$

4) Soit $u \in]\frac{1}{2}, 1[$. *Alors, il existe une constante* $\alpha(u) > 0$, *ne dépendant que de* q *et de* u, *telle que, pour tout polynôme* M, *on ait*

$$\prod_{\substack{P \in I \\ P \mid M}} (1 - |P|^{-u})^{-1} \ll \exp(\alpha(u)\omega(M)^{1-u}), \tag{6}$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q *et de* u.

Démonstration. Les relations (3) et (4) sont des conséquences immédiates du théorème Π.

Soit $u \in]\frac{1}{2},1]$. Soit M un polynôme de degré au moins 2. Posons

(i) $$A(u,M) = \prod_{\substack{P \in I \\ P \mid M}} (1 - |P|^{-u})^{-1}.$$

Soit s l'entier déterminé par la relation

(ii) $$\Pi(s) \leqslant \omega(M) < \Pi(s+1),$$

avec la convention $\Pi(0) = 0$. On suppose $s \geqslant 1$. Soit alors

(iii) $$B(u,s) = \prod_{\substack{P \in I \\ d^0P \leqslant s+1}} (1 - |P|^{-u})^{-1}.$$

Notons J l'ensemble des polynômes irréductibles unitaires de degré au plus s+1, J'(M), resp. J"(M), l'ensemble des diviseurs irréductibles unitaires de M appartenant à J, resp., n'appartenant pas à J. La relation (ii) montre qu'il existe une application injective j de J"(M) dans l'ensemble J − J'(M). Si $P \in J''(M)$, $d^0P > s+1 \geqslant d^0(j(P))$, et,

$$(1 - |P|^{-u})^{-1} \leqslant (1 - |j(P)|^{-u})^{-1},$$

d'où,

$$A(u,M) = \prod_{P \in J'(M)} (1 - |P|^{-u})^{-1} \times \prod_{P \in J''(M)} (1 - |P|^{-u})^{-1} \leqslant$$

$$\prod_{P \in J'(M)} (1 - |P|^{-u})^{-1} \times \prod_{P \in J''(M)} (1 - |j(P)|^{-u})^{-1},$$

(iv) $$A(u,M) \leqslant B(u,s).$$

Soit $\sigma(u)$ la somme de la série

$$\frac{1}{2} \sum_{j=1}^{\infty} q^j/q^{ju}(q^{ju}-1)j.$$

On a

$$\log(B(u,s)) = \sum_{\substack{P\in I\\ d^oP\leqslant s+1}} |P|^{-u} + \sum_{\substack{P\in I\\ d^oP\leqslant s+1}} \sum_{k=2}^{\infty} \frac{1}{k\,|P|^{uk}} \leqslant \sum_{\substack{P\in I\\ d^oP\leqslant s+1}} |P|^{-u} + \sigma(u),$$

d'où,

$$B(u,s) \leqslant \exp(\sigma(u)) \exp\Big(\sum_{\substack{P\in I\\ d^oP\leqslant s+1}} |P|^{-u}\Big).$$

Avec (3) on obtient

(v) $$B(1,s) \leqslant \exp(1+\sigma(1))(s+1),$$

avec (4), il vient pour $u \neq 1$,

(vi) $$B(u,s) \leqslant \exp\left(\sigma(u) + \beta(u)\left(\frac{q^{(s+1)(1-u)}}{s+1}\right)\right)$$

$\beta(u)$ étant une constante qui ne dépend que de q et de u.

Si $\omega(M) \geqslant \Pi(2)$, la relation (ii) et le théorème Π nous donnent

$$d^oM \geqslant \sum_{\substack{P\in I\\ P\,|M}} d^oP \geqslant \sum_{\substack{P\in I\\ d^oP\leqslant s}} d^oP \geqslant q + \sum_{t=2}^{s} (q^t - 2q^{t/2}) \geqslant q^{s+1}\left(\frac{1}{q} - \frac{2}{q^2}\right),$$

d'où,

$$s+1 \leqslant \log\left(\frac{q^2 d^oM}{q-2}\right)(\log q)^{-1}.$$

Si $\omega(M) < \Pi(2)$,

$$s+1 \leqslant 2 \leqslant d^oM.$$

Dans les deux cas, de (iv) et (v) on déduit la majoration

$$A(1,M) \ll \log(d^oM).$$

La fonction Φ est multiplicative et, si P est un polynôme irréductible, on a

$$\Phi(P^j) = |P|^{j-1}(|P|-1)$$

pour tout entier $j > 0$. Par suite,

$$A(1,M) = |M| / \Phi(M),$$

d'où, la relation (5).

Avec (ii) et la relation (2) on obtient

$$q^{s+1}/(s+1) \leqslant \frac{q\omega(M)}{1-2/3\sqrt{3}},$$

d'où,

$$q^{(s+1)(1-u)}/(s+1) \leqslant (q^{s+1}/(s+1))^{1-u} \leqslant \left(\frac{q}{1-2/3\sqrt{3}}\right)^{1-u} \omega(M)^{1-u}.$$

La relation(6) se déduit alors de (iv) et (vi). Les relations (5) et (6) sont établies pour $s \geqslant 1$. Si $s = 0$, les relations (i) et (ii) nous donnent

$$A(u,M) \leqslant (1-q^{-u})^q,$$

et, les relations (5) et (6) sont triviales dans ce cas.

PROPOSITION III-3. *Soit un entier* $m \geqslant 0$. *Alors, on a*

$$(7) \qquad \sum_{\substack{H \in U \\ d^oH \geqslant m}} \frac{1}{|H|\Phi(H)} \ll q^{-m}.$$

Démonstration. Posons pour $H \in U$,

$$\sigma(H) = \sum_{\substack{D \in U \\ D \mid H}} |D|.$$

Comme pour le théorème 329 de [3] on démontre que

$$\frac{\sigma(H)\Phi(H)}{|H|^2} \geqslant \prod_{P \in I} (1 - |P|^{-2}),$$

ce dernier produit étant strictement positif. Par suite,

$$\sum_{\substack{H \in U \\ d^oH \geqslant m}} \frac{1}{|H|\Phi(H)} \ll \sum_{\substack{H \in U \\ d^oH \geqslant m}} \frac{\sigma(H)}{|H|^3} = \sum_{k=m}^{\infty} q^{-3k} s_k,$$

où

$$s_k = \sum_{\substack{H \in U \\ d^oH = k}} \sigma(H).$$

On a

$$s_k = \sum_{\substack{H \in U \\ d^oH=k}} \sum_{\substack{D \in U \\ D \mid H}} |D| = \sum_{\substack{D \in U \\ d^oD \leqslant k}} |D| \sum_{\substack{H \in U \\ d^oH=k \\ D \mid H}} 1 = \sum_{\substack{D \in U \\ d^oD \leqslant k}} q^k \leqslant q^{2k+1},$$

d'où,

$$\sum_{\substack{H \in U \\ d^oH \geqslant m}} \frac{1}{|H|\Phi(H)} \ll \sum_{k=m}^{\infty} q^{-k}.$$

IV. - LE CARACTERE E ET LA MESURE dt

Les quatre propositions suivantes ont été établies dans [4] ou se démontrent de façon similaire.

PROPOSITION IV-1. *Pour tout entier relatif* j, P_j *a pour mesure* q^{-j}.

PROPOSITION IV-2. *1) Pour tout polynôme* H, E(H) = 1.

2) Si H *est un polynôme non nul, si* A *et* B *sont des polynômes congrus modulo* H, E(A/H) = E(B/H).

3) Si $u \in P_1$, E(u) = 1.

PROPOSITION IV-3. *Soient un entier* $j \geqslant 0$, $u \in \mathbb{K}$ *et* $b \in P$. *Alors, on a*

$$(1) \qquad \int_{b+P_j} E(u)dt = \begin{cases} q^{-j} E(ub) & \text{si } \nu(u) > -j, \\ 0 & \text{si } \nu(u) \leqslant -j. \end{cases}$$

PROPOSITION IV-4. *Soient* $u \in P$ *et* j *un entier positif. Alors, on a*

$$(2) \qquad \sum_{B \in \mathbf{F}_j} E(uB) = \begin{cases} q^{j+1} & \text{si } \nu(u) > j+1, \\ 0 & \text{si } \nu(u) \leqslant j+1. \end{cases}$$

De cette proposition nous déduisons le corollaire suivant, qui d'ailleurs pourrait se démontrer directement très facilement.

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

$$\sum_{R \in C_H} E\left(\frac{G}{H} R\right) = 0. \tag{3}$$

PROPOSITION IV-5. *Soient* G *et* H *des polynômes premiers entre eux. Soit*

$$S(G,H) = \sum_{R \in C_H} E\left(\frac{G}{H} R^2\right). \tag{4}$$

Alors, on a

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

Démonstration. C'est la proposition V-2 de [1].

V. - LA METHODE DU CERCLE

Soit un nombre réel $h \geqslant 2$ qui sera choisi ultérieurement et qui pour l'instant est supposé fixé.

Soit un entier n assez grand pour que les conditions

$$q^n \geqslant n^{8h}, \quad n^{-3h}(q+1) \leqslant \frac{1}{4}, \tag{1}$$

soient réalisées.

Soit $t \in P$. On pose

$$f(t) = \sum_{A \in \mathbf{F}_n} E(tA^2), \tag{2}$$

$$g(t) = \sum_{P \in \mathbf{I}_{2n}} E(tP), \tag{3}$$

$$h(t) = \sum_{\substack{A \in \mathbf{F}_{2n} \\ d^oA \neq 0}} \frac{1}{d^oA} E(tA). \tag{4}$$

Si A/Q est une fraction rationnelle telle que (A,Q) = 1, on pose

$$f_{A/Q}(t) = |Q|^{-1} S(A,Q) f(t - \frac{A}{Q}), \tag{5}$$

$$g_{A/Q}(t) = \frac{\mu(Q)}{\Phi(Q)} h(t - \frac{A}{Q}), \tag{6}$$

en supposant, ce qui est toujours possible, que $Q \in U$.

Soit

$$s = \left[h \frac{\log n}{\log q} \right]. \tag{7}$$

On pose

$$y(t) = \sum_{\substack{Q \in U \\ d^0 Q \leqslant s}} \sum_{A \in C_Q^*} f_{A/Q}(t) g_{A/Q}(t). \tag{8}$$

Pour tout polynôme $M \in \mathbf{F}_{2n}$, soient

$$b(M) = \sum_{\substack{M = A^2 + B \\ 0 < d^0 B \\ A \in \mathbf{F}_n}} (d^0 B)^{-1}, \tag{9}$$

$$Y(M) = \sum_{\substack{Q \in U \\ d^0 Q \leqslant s}} \sum_{A \in C_Q^*} \frac{S(A,Q)\mu(Q)}{|Q| \Phi(Q)} E(-M \frac{A}{Q}). \tag{10}$$

PROPOSITION V-1. *Soit, pour tout polynôme* M *de degré au plus* 2n, R(M) *le nombre de solutions* $(A,P) \in \mathbf{F}_n \times \mathbf{I}_{2n}$ *de l'équation*

$$M = A^2 + P$$

Alors, on a

$$\sum_{M \in \mathbf{F}_{2n}} |R(M) - b(M)Y(M)|^2 = \int_P |f(t)g(t) - y(t)|^2 \, dt. \tag{11}$$

Démonstration. Soit $t \in P$. Alors avec (2) et (3), on a

$$f(t)g(t) = \sum_{M \in \mathbf{F}_{2n}} R(M)E(Mt),$$

avec (5), (6), (8) et (9) on a

$$y(t) = \sum_{\substack{Q \in U \\ d^0Q \leqslant s}} \sum_{A \in C_Q^*} \frac{\mu(Q)S(A,Q)}{|Q|\Phi(Q)} \sum_{M \in \mathbf{F}_{2n}} b(M)E\left((t-\frac{A}{Q})M\right),$$

puis, avec (10),

$$y(t) = \sum_{M \in \mathbf{F}_{2n}} E(tM)b(M)Y(M).$$

Par suite,

$$\int_P |f(t)g(t) - y(t)|^2 dt = \int_P \left| \sum_{M \in \mathbf{F}_{2n}} \Big\{R(M) - b(M)Y(M)\Big\} E(tM) \right|^2 dt =$$

$$\sum_{M \in \mathbf{F}_{2n}} \sum_{H \in \mathbf{F}_{2n}} \Big\{R(M) - b(M)Y(M)\Big\}\Big\{R(H) - b(H)Y(H)\Big\} \int_P E(t(M-H))dt,$$

et (11) se déduit de (IV-1).

Une majoration convenable de l'intégrale

$$I = \int_P |f(t)g(t) - y(t)|^2 dt \tag{12}$$

montrera que, pour «presque tout polynôme M», b(M)Y(M) est une bonne approximation de R(M). Pour celà, introduisons une dissection de Farey à l'ordre N de P où

$$N = 2n - 4s. \tag{13}$$

Les arcs de Farey seront notés $U_{G/H}$. Sur les arcs $U_{G/H}$ tels que $\frac{G}{H} \in \mathbf{R}_{4s}$ on a une bonne approximation de f(t) et de g(t). Notons F_1 l'ensemble $\mathbf{R}_{4s}$ et F_2 le complémentaire de F_1 dans $\mathbf{R}_N$.

PROPOSITION V-2. *On a*

$$I \leqslant 2I_1 + 2I_2 + 4I_3 + 4I_4, \tag{14}$$

où,

$$I_1 = \sum_{G/H \in F_1} \int_{U_{G/H}} |f(t)g(t) - f_{G/H}(t)g_{G/H}(t)|^2 dt, \tag{15}$$

$$I_2 = \sum_{G/H \in F_2} \int_{U_{G/H}} |f(t)g(t) - f_{G/H}(t)g_{G/H}(t)|^2 dt, \tag{16}$$

(17) $$I_3 = \sum_{G/H \in \mathbf{R}_N} \int_{U_{G/H}} \Big| \sum_{\substack{A/Q \in \mathbf{R}_s \\ A/Q \neq G/H}} f_{A/Q}(t) g_{A/Q}(t) \Big|^2 \, dt,$$

(18) $$I_4 = \sum_{\substack{G/H \in \mathbf{R}_N \\ d^oH > s}} \int_{U_{G/H}} |f_{G/H}(t) g_{G/H}(t)|^2 \, dt.$$

Démonstration. On a

$$I = \sum_{G/H \in \mathbf{R}_N} \int_{U_{G/H}} |f(t)g(t) - y(t)|^2 \, dt.$$

Si $G/H \in \mathbf{R}_N$, si $t \in U_{G/H}$,

$$|f(t)g(t) - y(t)|^2 \leqslant 2 \left\{ |f(t)g(t) - f_{G/H}(t) g_{G/H}(t)|^2 + |f_{G/H}(t) g_{G/H}(t) - y(t)|^2 \right\}$$

d'où,

(i) $$I \leqslant 2 I_1 + 2 I_2 + 2 I'$$

avec

(ii) $$I' = \sum_{G/H \in \mathbf{R}_N} \int_{U_{G/H}} |f_{G/H}(t) g_{G/H}(t) - y(t)|^2 \, dt.$$

Soit $t \in P$. Si $G/H \in \mathbf{R}_s$, d'après (8),

$$|f_{G/H}(t) g_{G/H}(t) - y(t)| = \Big| \sum_{\substack{A/Q \in \mathbf{F}_s \\ A/Q \neq G/H}} f_{A/Q}(t) g_{A/Q}(t) \Big|,$$

Si $G/H \in \mathbf{F}_N$ est tel que $d^oH > s$, toujours avec (8) on a

$$|f_{G/H}(t) g_{G/H}(t) - y(t)|^2 \leqslant 2 \Big(|f_{G/H}(t) g_{G/H}(t)|^2 + \Big| \sum_{A/Q \in \mathbf{F}_s} f_{A/Q}(t) g_{A/Q}(t) \Big|^2 \Big),$$

d'où,

(iii) $$I' \leqslant 2 I_3 + 2 I_4 .$$

On conclut avec (i), (ii) et (iii).

1. - Les fonctions f, g et h

PROPOSITION V-3. *Soit* $\frac{G}{H} \in F_1$. *Soit* $t = \frac{G}{H} + u$ *un élément de* $U_{G/H}$. *Alors, on a*

$$f(t) = |H|^{-1} S(G,H) f(u). \tag{19}$$

Démonstration. C'est la proposition VIII-2 de [1] .

PROPOSITION V-4. *Soit* $t \in P_n$. *Alors*

(i) *si* $\nu(t) > 2n+1$, $f(t) = q^{n+1}$,

(ii) *si* $\nu(t) = 2k$, *avec* $k \leqslant n$, $f(t) = q^k$,

(iii) *si* $\nu(t) = 2k+1$, *avec* $k \leqslant n$, $|f(t)| \leqslant q^{k+1}$.

Démonstration. C'est une conséquence immédiate de la proposition VIII-1 de [1] .

PROPOSITION V-5. *Soient* $\frac{G}{H} \in F_1$ *et* $t = \frac{G}{H} + u$ *un élément de* $U_{G/H}$. *Alors, on a*

$$|g(t) - \frac{\mu(H)}{\Phi(H)} h(u)| \ll s\, q^{n+8s}. \tag{20}$$

Démonstration. On utilise l'équivalence R_H déjà utilisée en [1] . Les polynômes A et B sont dits équivalents modulo R_H si

i) $A \equiv B \pmod H$,

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

Si A et B sont des polynômes équivalents modulo R_H , on a

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

C'est la proposition IX-2 de [1] . Pour tout entier $r \geqslant N$, soit M_r l'ensemble des polynômes

$$M = X^{N-d^oH} H B + R,$$

où B décrit l'ensemble des polynômes de degré r–N, où R décrit C_H . Alors, la réunion des ensembles M_r et des différentes classes modulo H constitue un système complet de représentants des

différentes classes modulo R_H . C'est la proposition IX-1 de [1] . Si A est un polynôme, notons P(r,H,A) le nombre de polynômes irréductibles de degré r équivalents à A modulo R_H . La relation (3) s'écrit alors,

$$g(t) = \sum_{r=1}^{N-1} \sum_{R \in C_H} E(tR)P(r,H,R) + \sum_{r=N}^{2n} \sum_{A \in M_r} E(tA)P(r,H,A).$$

Si les polynômes H et A ne sont pas premiers entre eux, et si P est un polynôme irréductible congru à A modulo H, P divise H, ceci ne peut se produire que si $d^oP \leqslant 4s$, d'où,

(i) $$|g(t) - \sum_{r=4s+1}^{N-1} \gamma_r - \sum_{r=N}^{2n} \Gamma_r| \leqslant (q-1)\Pi(4s).$$

avec

(ii) $$\gamma_r = \sum_{R \in C_H^*} E(tR)P(r,H,R) \ , \quad 4s < r < N,$$

(iii) $$\Gamma_r = \sum_{\substack{A \in M_r \\ (A,H)=1}} E(tA)P(r,H,A) \ , \quad N \leqslant r \leqslant 2n.$$

Une démonstration analogue à celles des propositions IX-3 et X-3 de [1] montre alors que

$$\left| \sum_{r=4s+1}^{N-1} \gamma_r + \sum_{r=N}^{2n} \Gamma_r - \frac{\mu(H)}{\Phi(H)} \sum_{r=4s+1}^{2n} \frac{1}{r} \sum_{\substack{B \in \mathbf{F}_r \\ B \notin \mathbf{F}_{r-1}}} E(uB) \right| \ll sq^{n+8s},$$

d'où, avec (4)

$$\left| \sum_{r=4s+1}^{N-1} \gamma_r + \sum_{r=N}^{2n} \Gamma_r - \frac{\mu(H)}{\Phi(H)} h(u) \right| \ll sq^{n+8s}.$$

On conclut avec (i) et (III-2).

Posons, pour tout entier $k \geqslant 1$,

(21) $$\sigma_k = (q-1) \sum_{j=1}^{k} q^j/j.$$

PROPOSITION V-6. *Soit* $t \in P$. *Alors,*

(i) *si* $\nu(t) > 2n+1$, *on a* $h(t) = \sigma_{2n}$,

(ii) *si* $\nu(t) \leqslant 2n+1$, *on a* $h(t) = \sigma_{\nu(t)-2} - q^{\nu(t)-1}/(\nu(t)-1)$.

Démonstration. On a

$$h(t) = \sum_{j=1}^{2n} \frac{1}{j} \left\{ \sum_{B \in F_j} E(tB) - \sum_{B \in F_{j-1}} E(tB) \right\}.$$

On conclut avec (IV-2).

PROPOSITION V-7. *Soient* $\frac{G}{H} \in F_2$ *et* $t \in U_{G/H}$. *Alors, on a*

$$|f(t)| \leqslant q^{n+1-2s}. \tag{22}$$

Démonstration. C'est la proposition VIII-3 de [1].

2. - Majoration de I_1, I_2 et I_4

PROPOSITION V-8. *On a*

$$I_1 \ll s^3 q^{2n+20s} \tag{23}$$

Démonstration. Soient $\frac{G}{H} \in F_1$ et $t = \frac{G}{H} + u$ un élément de $U_{G/H}$. Alors, avec (19), (5), (6) et (IV-5), il vient

$$|f(t)g(t) - f_{G/H}(t)g_{G/H}(t)| = |H|^{-1} |S(G,H)f(u)| \, |g(t) - \frac{\mu(H)}{\Phi(H)} h(u)| =$$

$$|H|^{-1/2} \, |f(u)| \, |g(t) - \frac{\mu(H)}{\Phi(H)} h(u)|.$$

La majoration (20) et la proposition V-4 nous donnent alors

$$|f(t)g(t) - f_{G/H}(t)g_{G/H}(t)| \ll s \, |H|^{-1/2} \, q^{2n+8s},$$

d'où, avec (IV-1),

$$I_1 \ll \sum_{G/H \in F_1} |H|^{-2} s^2 q^{2n+20s} \leqslant s^2 q^{2n+20s} \sum_{\substack{H \in U \\ d^0 H \leqslant 4s}} \Phi(H) \, |H|^{-2} \ll s^3 q^{2n+20s}.$$

PROPOSITION V-9. On a

$$\int_{P_N} |f(t)h(t)|^2 \, dt \ll q^{4n} n^{-2}. \tag{24}$$

Démonstration. On a

$$\int_{P_N} |f(t)h(t)|^2\,dt = \int_{P_{2n+1}} |f(t)h(t)|^2\,dt + \sum_{j=N}^{2n+1} \int_{\nu(t)=j} |f(t)h(t)|^2\,dt.$$

On applique les propositions V-4, V-6, III-1 et IV-1. Il vient

$$\int_{P_N} |f(t)h(t)|^2\,dt \ll q^{4n}/n^2 + \sum_{k=n-2s}^{n} q^{4k}/k^2.$$

La condition (1) et la relation (7) donnent la majoration annoncée.

PROPOSITION V-10. *On a*

$$I_2 \ll q^{4n-4s}n^{-1}. \tag{25}$$

Démonstration. Posons

$$K = \sum_{G/H \in F_2} \int_{U_{G/H}} |f(t)g(t)|^2\,dt \quad \text{et} \quad L = \sum_{G/H \in F_2} \int_{U_{G/H}} |f_{G/H}(t)g_{G/H}(t)|^2\,dt.$$

Alors,

$$I_2 \leqslant 2K + 2L. \tag{i}$$

La relation (22) nous donne

$$K \leqslant q^{2n+2-4s} \sum_{G/H \in F_2} \int_{U_{G/H}} |g(t)|^2\,dt \leqslant q^{2n+2-4s} \int_P |g(t)|^2\,dt,$$

d'où, avec (3) et (III-2),

$$K \leqslant q^{2n+2-4s}\,\Pi(2n) \leqslant q^{4n+3-4s}/2n+1.$$

$$K \ll q^{4n-4s}/n. \tag{ii}$$

Soit $G/H \in F_2$. Les relations (5), (6) et (IV-5) nous donnent

$$\int_{U_{G/H}} |f_{G/H}(t)g_{G/H}(t)|^2\,dt = \frac{\mu^2(H)\,|S(G,H)|^2}{|H|^2\,\Phi^2(H)} \int_{P_{N+d^oH}} |f(u)h(u)|^2\,du \leqslant$$

$$\frac{\mu^2(H)}{|H|\Phi^2(H)} \int_{P_N} |f(u)h(u)|^2\,du,$$

d'où, avec la proposition précédente,

$$L \ll q^{4n_n-2} \sum_{G/H \in F_2} \frac{\mu^2(H)}{|H|\Phi(H)^2} \leqslant q^{4n_n-2} \sum_{\substack{H \in U \\ 4s < d^oH \leqslant N}} 1/|H|\Phi(H).$$

On applique la proposition III-3 :

(iii) $$L \ll q^{4n-4s}/n^2.$$

On conclut avec (i), (ii) et (iii).

PROPOSITION V-11. *On a*

(26) $$I_4 \ll q^{4n-s}\, n^{-2}.$$

Démonstration. Comme pour la proposition précédente,

$$I_4 \ll q^{4n_n-2} \sum_{\substack{H \in U \\ s < d^oH \leqslant N}} \frac{1}{|H|\Phi(H)} \ll q^{4n-s_n-2}.$$

3. - Majoration de I_3

PROPOSITION V-12. *On a*

(27) $$I_3 \ll q^{4n-2s}(\log s)^2.$$

Démonstration. Posons, pour $t \in P$, $G/H \in \mathbf{R}_N$,

$$V(t) = \sum_{A/Q \in \mathbf{R}_s} |f_{A/Q}(t)|^2 \quad \text{et} \quad W(t, \frac{G}{H}) = \sum_{\substack{A/Q \in \mathbf{R}_s \\ \frac{A}{Q} \neq \frac{G}{H}}} |g_{A/Q}(t)|^2.$$

L'inégalité de Cauchy-Schwarz nous donne

(i) $$I_3 \leqslant \sum_{\frac{G}{H} \in \mathbf{R}_N} \int_{U_{G/H}} V(t)W(t, \frac{G}{H})dt.$$

Les propositions IV-5 et V-4 donnent alors

$$V(t) \ll q^{2n} \sum_{\substack{Q \in U \\ d^oQ \leqslant s}} \Phi(Q)\, |Q|^{-1},$$

(ii) $$V(t) \ll q^{2n+s}.$$

Soit $G/H \in \mathbf{R}_N$. Soit $A/Q \in \mathbf{R}_s$ avec $A/Q \neq G/H$. Soit $t \in U_{G/H}$. Alors,

$$\nu\left(\frac{G}{H} - \frac{A}{Q}\right) = d^oH + d^oQ - d^o(GQ - AH) \leqslant s + d^oH \leqslant 2n,$$

ceci grâce à la condition (1). Toujours, grâce à la condition (1), on a

$$\nu\left(t - \frac{G}{H}\right) > N + d^oH > s + d^oH,$$

d'où,

$$\nu\left(t - \frac{A}{Q}\right) = d^oH + d^oQ - d^o(GQ - AH).$$

La proposition V-6 nous donne alors

$$|h\left(t - \frac{A}{Q}\right)| \ll \frac{|H| \times |Q|}{|GQ - AH|};$$

d'où, avec (6),

$$|g_{A/Q}(t)|^2 \ll \frac{\mu^2(Q)}{\Phi^2(Q)} \frac{|H|^2\, |Q|^2}{|GQ - AH|^2},$$

et, avec (III-5)

(iii) $$W\left(t, \frac{G}{H}\right) \ll (\log s)^2\, |H|^2 \sum_{\substack{A/Q \in \mathbf{R}_s \\ \frac{A}{Q} \neq \frac{G}{H}}} |GQ - AH|^{-2}.$$

Les relations (i), (ii), (iii) nous donnent

$$I_3 \ll q^{5s} (\log s)^2 \sum_{\frac{G}{H} \in \mathbf{R}_N} |H| \sum_{\substack{\frac{A}{Q} \in \mathbf{R}_s \\ \frac{A}{Q} \neq \frac{G}{H}}} |GQ - AH|^{-2},$$

$$I_3 \ll q^{5s}(\log s)^2 \sum_{\substack{D\in U\\ d^oD\leqslant s}} \sum_{\substack{L\in U\\ d^o(DL)\leqslant s+N}} |LD|^{-2} \sum_{\substack{H\in U,\ Q\in U\\ d^oH\leqslant N\\ d^oQ\leqslant s\\ (H,Q)=D}} |H|\rho(H,Q,L,D),$$

où $\rho(H,Q,L,D)$ désigne le nombre de solutions $(G,A)\in C_H^* \times C_Q^*$ de l'équation

$$LD = GQ - AH.$$

Par suite,

$$I_3 \ll q^{5s}(\log s)^2 \sum_{\substack{D\in U\\ d^oD\leqslant s}} |D|^{-1} \sum_{\substack{L\in U\\ d^o(LD)\leqslant s+N}} |L|^{-2} \sum_{\substack{H\in U,\ Q\in U\\ d^oH\leqslant N\\ d^oQ\leqslant s\\ (H,Q)=D}} |H|,$$

$$I_3 \ll q^{6s}(\log s)^2 \sum_{\substack{D\in U\\ d^oD\leqslant s}} \sum_{\substack{S\in U\\ d^oS\leqslant N-d^oD}} |S|,$$

$$I_3 \ll q^{6s+2N}(\log s)^2 \ll q^{4n-2s}(\log s)^2.$$

4. - Le premier théorème

THEOREME A. *Soit un nombre réel* $h > 2$. *Alors, pour tout entier* n, *on a*

$$\sum_{M\in \mathbf{F}_{2n}} |R(M) - b(M)Y(M)|^2 \in \mathbf{O}(q^{4n}\, n^{-2-h}), \tag{28}$$

la constante impliquée par le symbole **O** *ne dépendant que de* q *et de* h.

Démonstration. Reprenons les notations de ce chapitre. Il existe un entier n_h tel que tout entier $n \geqslant n_h$ vérifie les conditions (1). Pour un tel entier n, les relations (11), (14), (23), (25), (26) et (27) donnent la majoration (28).

VI. - APPROXIMATION DE Y(M)

1. - Les séries de Dirichlet $L(\chi, .)$

Soit D un polynôme sans facteur carré de degré $m > 0$. Soit χ le caractère multiplicatif modulo D défini, pour tout polynôme irréductible P ne divisant pas D, par

$$\chi(P) = (\frac{D}{P}),$$

et prolongé aux polynômes H non premiers à D par $\chi(H) = 0$. Au caractère χ on associe la série de Dirichlet $L(\chi,z)$ définie a priori dans le disque $|z| < 1$ par

$$L(\chi,z) = \sum_{H \in U} \chi(H) (\frac{z}{q})^{d^oH}. \tag{1}$$

Le caractère χ n'est pas principal. C'est une conséquence immédiate des propriétés des symboles locaux dont on trouvera une étude au chapitre XIV de [7]. La série $L(\chi,z)$ est en fait un polynôme de degré pair $2d < m$. Les racines de ce polynôme sont deux à deux conjuguées et de module $\sqrt{q}$. Ceci est établi dans l'appendice V de [8]. Soient $\rho_1, \bar{\rho}_1, \ldots, \rho_d, \bar{\rho}_d$ les 2d racines de $L(\chi,z)$. On peut écrire

$$L(\chi,z) = \prod_{i=1}^{d} (\rho_i - z)(\bar{\rho}_i - z). \tag{2}$$

Enfin $L(\chi,z)$ se développe en produit eulérien absolument convergent dans le disque $|z| < 1$

$$L(\chi,z) = \prod_{P \in I} (1 - \chi(P)(\frac{z}{q})^{d^oP})^{-1}. \tag{3}$$

PROPOSITION VI-1. *On a*

$$|L(\chi,1)| \leqslant m. \tag{4}$$

Soit $u \in]0, \frac{1}{2}[$. *Alors, si* $|z| = q^u$, *on a*

$$|L(\chi,z)| \geqslant (q^{1/2} - q^u)^{2d}. \tag{5}$$

Démonstration. La minoration (5) se déduit immédiatement de (2). On remarque que

$$L(\chi,z) = \sum_{j=1}^{2d} (\sum_{\substack{H \in U \\ d^oH = j}} \chi(H)/|H|)z^j,$$

d'où,

$$|L(\chi,1)| \leqslant 2d \leqslant m.$$

2. - Approximation de Y(M)

Soit M un polynôme de $\mathbf{F}_{2n}$ tel que pour tout $a \in \mathbf{IF}_q$, non nul, aM ne soit pas carré dans $\mathbf{IF}_q$. Le polynôme M s'écrit de façon unique comme produit

$$M = U^2 D \tag{6}$$

où U est un polynôme unitaire, où D est un polynôme sans facteur carré de degré strictement positif. Si P est un polynôme irréductible ne divisant pas M, on a

$$(\frac{M}{P}) = (\frac{D}{P}) = \chi(P),$$

χ désignant le caractère modulo D défini comme au paragraphe précédent. Pour tout polynôme unitaire H, on pose

$$B(M,H) = \frac{\mu(H)}{|H|\Phi(H)} \sum_{G \in C_H^*} S(G,H) E(-M\frac{G}{H}). \tag{7}$$

PROPOSITION VI-2. *La fonction* $H \mapsto B(M,H)$ *est multiplicative.*

Démonstration. Immédiate.

PROPOSITION VI-3. *Soit* P *un polynôme irréductible. Alors, on a*

$$B(M,P) = \begin{cases} 0 & \text{si } P \mid M, \\ -\dfrac{\chi(P)}{\Phi(P)} & \text{si } P \nmid M. \end{cases} \tag{8}$$

Démonstration. On a

$$B(M,P) = -\frac{1}{|P|\Phi(P)} \sum_{G \in C_P^*} \sum_{A \in C_P} E(\frac{G}{P}A^2)\, E(-M\frac{G}{P}) =$$

$$-\frac{1}{|P|\Phi(P)} \sum_{A \in C_P} \sum_{G \in C_P^*} E((A^2-M)\frac{G}{P}).$$

$$B(M,P) = -\frac{1}{|P|\Phi(P)} \left(\rho\Phi(P) - (|P|-\rho)\right),$$

où ρ désigne le nombre de solutions de la congruence

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

Or, $\Phi(P) = |P| - 1$. On a donc

$$B(M,P) = (1-\rho)/\Phi(P).$$

Soit, pour tout entier $r \geqslant 0$,

$$b_r = \sum_{\substack{H \in U \\ d^oH = r}} B(M,H). \tag{9}$$

Si z est un nombre complexe de module strictement inférieur à 1, on pose

$$\Gamma(z) = \sum_{r=0}^{\infty} b_r z^r \tag{10}$$

PROPOSITION VI-4. *1) Le produit*

$$H(z) = \prod_{\substack{P \in I \\ P \nmid M}} \left(1 - \frac{\chi(P) z^{d^oP} + z^{2d^oP}}{\Phi(P)\,|P|}\right) \left(1 - \left(\frac{z}{q}\right)^{2d^oP}\right)^{-1} \tag{11}$$

est absolument convergent dans le disque $|z| < \sqrt{q}$.

2) Pour $|z| < 1$, *on a*

$$\Gamma(z) = \frac{H(z)}{L(\chi,z)} \times \prod_{\substack{P \in I \\ P \mid M}} \left(1 - \chi(P)\left(\frac{z}{q}\right)^{d^oP}\right)^{-1}. \tag{12}$$

Démonstration. Le premier point est immédiat.

Dans le disque $|z| < 1$ la série $\Gamma(z)$ est absolument convergente et peut s'écrire

$$\Gamma(z) = \sum_{H \in U} B(M,H) z^{d^oH}.$$

Les propositions VI-2 et VI-3 nous permettent de développer $\Gamma(z)$ en produit eulérien absolument convergent.

$$\Gamma(z) = \prod_{\substack{P \in I \\ P \nmid M}} \left(1 - \frac{\chi(P)}{\Phi(P)} z^{d^oP}\right),$$

d'où, avec (3),

$$\Gamma(z)L(\chi,z)=\left\{\prod_{\substack{P\in I\\ P\nmid M}}\left(1-\frac{\chi(P)}{\Phi(P)}z^{d^oP}\right)\left(1-\chi(P)(\frac{z}{q})^{d^oP}\right)^{-1}\right\}\left\{\prod_{\substack{P\in I\\ P\mid M}}(1-\chi(P)(\frac{z}{q})^{d^oP}\right\}^{-1}.$$

Si P ne divise pas M, $\chi^2(P)=1$, et,

$$\left(1-\frac{\chi(P)}{\Phi(P)}z^{d^oP}\right)\left(1-\chi(P)(\frac{z}{q})^{d^oP}\right)^{-1}=\left(1-\frac{\chi(P)}{\Phi(P)}z^{d^oP}\right)\left(1+\chi(P)(\frac{z}{q})^{d^oP}\right)\left(1-(\frac{z}{q})^{2d^oP}\right)^{-1},$$

d'où,

$$\Gamma(z)L(\chi,z)=H(z)\prod_{\substack{P\in I\\ P\mid M}}\left(1-\chi(P)(\frac{z}{q})^{d^oP}\right)^{-1}.$$

La relation (12) donne un prolongement holomorphe de Γ dans le disque $|z|<\sqrt{q}$. En particulier,

$$\Gamma(1)=\frac{H(1)}{L(\chi,1)}\prod_{\substack{P\in I\\ P\mid M}}(1-\chi(P)/|P|)^{-1}. \tag{13}$$

PROPOSITION VI-5. *On a*

$$\Gamma(1)\gg(d^oM\log(d^oM))^{-1}. \tag{14}$$

Démonstration. On a

$$H(1)\geqslant\prod_{P\in I}\left(1-\frac{2}{|P|\Phi(P)}\right)\left(1-\frac{1}{|P|^2}\right)^{-1},$$

et ce dernier produit est strictement positif. On a aussi

$$\prod_{\substack{P\in I\\ P\mid M}}(1-\chi(P)/|P|)^{-1}\geqslant\prod_{\substack{P\in I\\ P\mid M}}\left(1+\frac{1}{|P|}\right)^{-1}\geqslant\prod_{\substack{P\in I\\ P\mid M}}\left(1-\frac{1}{|P|}\right).$$

On conclut avec les relations (4) et (III-5).

On reprend maintenant les notations du chapitre précédent.

PROPOSITION VI-6. *Il existe des constantes* $u\in\,]0,\frac{1}{2}[$, $\beta>0$, *ne dépendant que de* q, *telles que*

$$|Y(M)-\Gamma(1)|\ll q^{-su}\exp(\beta\omega(M)^u). \tag{15}$$

Démonstration. Remarquons que

(i) $$\Gamma(1) = Y(M) + \sum_{r>s} b_r .$$

Soit $u \in]0,1/2[$ défini par la relation

$$q^{1/2} - q^u = 1.$$

Soit z un nombre complexe de module q^u. Alors, on a

$$|H(z)| \leqslant \prod_{P \in I} \left(1 + \frac{q^{ud^oP} + q^{2ud^oP}}{|P|\Phi(P)}\right)\left(1 - \frac{q^{2ud^oP}}{|P|^2}\right)^{-1} \ll 1.$$

Les relations (5) et (12) puis la relation (III-6) nous donnent

$$|\Gamma(z)| \ll \prod_{\substack{P \in I \\ P \mid M}} (1 - q^{(u-1)d^oP})^{-1} \ll \exp(\alpha(1-u)\omega(M)^u).$$

Par intégration sur le cercle $|z| = q^u$ on obtient la majoration

(ii) $$|b_r| \ll q^{-ru} \exp(\alpha(1-u)\omega(M)^u).$$

On a (15) avec (i) et (ii).

VII. - FIN DE LA DEMONSTRATION

LEMME 1. *Soit un nombre réel* $a \geqslant 0$. *Soit* $A(n)$ *l'ensemble des polynômes* $M \in \mathbf{F}_{2n}$ *tels que*

$$\omega(M) > (a+1)\frac{\log n}{\log 2}.$$

Alors, on a

(1) $$\mathrm{Card}(A(n)) \ll n^{-a} q^{2n}.$$

Démonstration. Pour tout polynôme H, on a

$$2^{\omega(H)} \leqslant d(H)$$

où d(H) désigne le nombre de diviseurs unitaires de H. Or,

$$\sum_{H \in \mathbf{F}_{2n}} d(H) = (2n+1)q^{2n+1},$$

par suite,

$$n^{a+1}\,\mathrm{Card}(A(n)) \leqslant \sum_{H \in \mathbf{F}_{2n}} 2^{\omega(H)} \leqslant \sum_{H \in \mathbf{F}_{2n}} d(H) = (2n+1)q^{2n+1}.$$

LEMME 2. *Si* $M \in \mathbf{F}_{2n}$ *on a*

$$q^n/n \ll b(M) \ll q^n/n. \tag{2}$$

Démonstration. Soit $M \in \mathbf{F}_{2n}$. Soit A un polynôme de degré n. Le polynôme $M-A^2$ est de degré 2n dans les cas suivants :

si $d^oM < 2n$,

si $d^oM = 2n$ et si $\mathrm{sgn}(M) \neq (\mathrm{sgn}(A))^2$,

sgn(M), resp. sgn(A), désignant le coefficient du terme de plus haut degré de M, resp. de A. Par suite,

$$b(M) \geqslant (q-2)q^n/2n.$$

D'autre part, si $r = [n/2]$,

$$b(M) \leqslant \sum_{\substack{A \in \mathbf{F}_n \\ 1 \leqslant d^o(M-A^2) \leqslant r}} 1/d^o(M-A^2) + \frac{2}{n} \sum_{\substack{A \in \mathbf{F}_n \\ d^o(M-A^2) \geqslant r}} 1 \leqslant \frac{2q^{n+1}}{n} + 2\sum_{B \in \mathbf{F}_r} 1,$$

$$b(M) \leqslant 2[q^{n+1}/n + q^{1+(n/2)}].$$

THEOREME B. *Pour tout entier* $n > 0$, *soit* V(n) *le nombre de polynômes* $M \in \mathbf{F}_{2n}$ *non représentables comme somme*

$$P + A^2$$

où $P \in \mathbf{F}_{2n}$, *où* $A \in \mathbf{F}_n$. *Alors, pour tout nombre réel* $b > 0$, *on a*

$$V(n) \ll q^{2n}\, n^{-b}, \tag{3}$$

la constante contenue dans le symbole $\ll$ *ne dépendant que de* q *et de* b.

Démonstration. Reprenons les notations du chapitre V. Soit un nombre réel $a > 0$ et un entier $n > 0$. Soit $V(n)$ l'ensemble des polynômes $M \in \mathbf{F}_{2n}$ tels que $R(M) = 0$. Soit $V'(n)$ l'ensemble des polynômes de $V(n)$ qui n'appartiennent pas à $A(n)$ et qui ne sont pas le produit d'un polynôme constant par un carré, l'ensemble $A(n)$ étant défini comme au lemme 1. Alors, on a

$$\text{(i)} \qquad V(n) \leqslant \mathrm{Card}(V'(n)) + \mathrm{Card}(A(n)) + q^{n+1}.$$

Soit $M \in V'(n)$. Alors,

$$|R(M) - b(M)Y(M)|^2 = b^2(M)Y^2(M).$$

On applique la proposition VI-6.

$$|Y(M) - \Gamma(1)| \ll q^{-su} \exp(\beta[(a+1)\log n / \log 2]^u),$$

d'où, avec (V-7),

$$|Y(M) - \Gamma(1)| \ll \mathrm{esp}(-hu \log(n) + \beta((a+1)\log n / \log 2)^u),$$

$$|Y(M) - \Gamma(1)| \ll n^{-hu/2}.$$

On suppose $h > \dfrac{2}{u}$. La relation (VI-14) nous donne

$$|Y(M)| \gg 1/n \log(n)$$

d'où, avec (2)

$$|R(M) - b(M)Y(M)|^2 \gg q^{2n}/n^4 \log n)^2$$

d'où,

$$\mathrm{Card}(V'(n))q^{2n} n^{-4}(\log n)^{-2} \ll \sum_{M \in \mathbf{F}_{2n}} |R(M) - b(M)Y(M)|^2.$$

Le théorème A nous donne alors

$$\text{(ii)} \qquad \mathrm{Card}(V'(n)) \ll q^{2n} n^{2-h}(\log n)^2.$$

On prend $h > \mathrm{Sup}(2/u, 2+b)$, $a = b$. Les relations (i), (ii) et (1) donnent le résultat annoncé.

THEOREME C. *Soit un nombre réel* $b > 2$. *Pour tout entier* $n > 0$, *soit* $W(n)$ *le nombre de polynômes* $M \in \mathbf{F}_{2n}$ *pour lesquels la relation*

$$|R(M) - b(M) \prod_{\substack{P \in I \\ P \nmid M}} (1 - (\frac{M}{P}) \Phi(P)^{-1})| \ll q^n n^{-b} \tag{4}$$

n'a pas lieu. Alors, pour tout nombre réel $a > 0$, *on a*

$$W(n) \ll q^{2n} n^{-a}, \tag{5}$$

la constante impliquée par le symbole $\ll$ *ne dépendant que de* q, a *et* b.

Démonstration. Le produit intervenant en (4) n'est rien d'autre que le produit $\Gamma(1)$ défini en (VI-13).

Soit $W(n)$ l'ensemble des polynômes $M \in \mathbf{F}_{2n}$ ne vérifiant pas la relation (4), soit $W'(n)$ l'ensemble des polynômes de $W(n)$ qui n'appartiennent pas à $A(n)$ et qui ne sont pas le produit d'un carré par une constante, l'ensemble $A(n)$ étant défini comme au lemme 1.

$$W(n) \leqslant \mathrm{Card}(W'(n)) + \mathrm{Card}(A(n)) + q^{n+1}. \tag{i}$$

Si $M \in W'(n)$, on a

$$|R(M) - b(M)\Gamma(1)| \geqslant q^n n^{-b}.$$

En procédant comme pour le théorème précédent, on obtient

$$|R(M) - b(M)Y(M)| \geqslant q^n n^{-b} + q^n n^{-1-hu/2},$$

ce qui conduit à la majoration

$$\mathrm{Card}(W'(n)) \ll q^{2n} n^{2b-2-h} + q^{2n} n^{hu-h}$$

les constantes impliquées par les symboles $\geqslant$ et $\ll$ ne dépendant que de q et de b. En prenant $h = \mathrm{Sup}\,(\frac{a}{1-u}, 2b+a-2)$ on obtient le résultat annoncé avec les relations (i) et (1).

REFERENCES

[1] M. CAR. *«Sommes de carrés et d'irréductibles dans* $\mathbb{F}_q[X]$*»*. Annales Faculté des Sciences de Toulouse, Vol. III, 1981, pp. 129-166.

[2] G.H. HARDY & J.E. LITTLEWOOD. *«Some problems of partitio numerorum : III : On the expression of a large number as sums of squares, higher powers and primes»*. Acta Math., 44, 1923, pp. 1-70.

[3] G.H. HARDY & E.M. WRIGHT. *«The theory of numbers»*. Oxford, at the Clarendon Press.

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

[5] R.J. MIECH. *«On the equation* $n = x^2+p$*»*. Trans, Amer. Math. Soc., 130, 1968, pp. 494-512.

[6] M. MIGNOTTE. *«Comptes rendus des journées de Théorie Analytique et Elémentaire des nombres»*. Limoges, 10-11 mars 1980.

[7] J.P. SERRE. *«Corps locaux»*. Hermann, Paris.

[8] A. WEIL. *«Basic number theory»*. Springer-Verlag, Berlin.

(Manuscrit reçu le 15 décembre 1982)