ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

MIREILLE CAR

Sommes de deux carrés dans $IF_q[X]$ et problèmes de diviseurs

Annales de la faculté des sciences de Toulouse 5^e série, tome 5, n° 2 (1983), p. 89-108

<http://www.numdam.org/item?id=AFST_1983_5_5_2_89_0>

Annales Faculté des Sciences Toulouse
Vol V, 1983, P. 89 à 108

SOMMES DE DEUX CARRES DANS $\mathbb{F}_q[X]$ ET PROBLEMES DE DIVISEURS

Mireille Car (1)

(1) *Laboratoire de Théorie des Nombres, 13397 Marseille - France.*

Résumé : Soit $\mathbb{F}_q$ le corps fini à q éléments. On donne une estimation asymptotique du nombre de polynômes unitaires de degré m de $\mathbb{F}_q[X]$ qui ont un diviseur de degré [m/2] . On a ainsi, lorsque q est impair, et que -1 est carré dans $\mathbb{F}_q$, une estimation du nombre de polynômes unitaires de degré m s'écrivant comme sommes de deux carrés, sommes soumises à certaines conditions de degré.

Summary : Let $\mathbb{F}_q$ be a finite field with q elements. We give an asymptotic estimate for the number of monic polynomials of degree m in $\mathbb{F}_q[X]$ which have a divisor of degree [m/2] . When q is odd and -1 is a square in $\mathbb{F}_q$, this give us an estimate for the number of monic polynomials of degree m in $\mathbb{F}_q[X]$ which are sums of two squares, these sum satisfying some degree conditions.

I - INTRODUCTION

Soit $\mathbb{F}_q$ le corps fini à q éléments et $\mathbb{F}_q[X]$ l'anneau des polynômes à une indéterminée sur le corps $\mathbb{F}_q$.

Si le corps $\mathbb{F}_q$ est de caractéristique 2, seuls les carrés de $\mathbb{F}_q[X]$ sont sommes de deux carrés, et il y a q^n polynômes unitaires de degré 2n qui sont sommes de deux carrés. On supposera q impair.

Si -1 *n'est pas carré dans le corps* $\mathbf{IF}_q$, une condition nécessaire et suffisante pour que le polynôme M de $\mathbf{IF}_q[X]$ soit somme de deux carrés est que M soit norme dans $\mathbf{IF}_q[X]$ d'un polynôme de l'extension $\mathbf{IF}_{q^2}[X]$. En particulier, ceci ne peut avoir lieu que si le degré de M est pair. De plus, si le polynôme M de degré 2n s'écrit comme somme de deux carrés

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

les polynômes A et B sont de degré au plus n. On a un développement asymptotique du nombre $\mathbf{A}(2n)$ de polynômes unitaires de degré 2n qui sont sommes de deux carrés :

$$\mathbf{A}(2n) = \frac{q^{2n}}{\sqrt{\pi n}} \, (a_0 + a_1/n + \ldots + a_L/n^L + \mathbf{O}(n^{-L-1})),$$

où $a_0, a_1, \ldots, a_L, \ldots$ sont des constantes qui ne dépendent que de q, où la constante contenue dans le $\mathbf{O}$ ne dépend que de q et de L. Ceci est établi dans [1] où seuls les coefficients a_0 et a_1 sont calculés explicitement, le calcul des autres coefficients devenant rapidement inextricable.

Si -1 *est carré dans* $\mathbf{IF}_q$, le problème des sommes de deux carrés $\mathbf{IF}_q[X]$ est, soit trivial, si on n'impose aucune condition de degré, car, dans ce cas, pour tout polynôme M de $\mathbf{IF}_q[X]$ on a

$$M = \left(\frac{M+1}{2}\right)^2 - \left(\frac{M-1}{2}\right)^2,$$

soit, beaucoup plus difficile, si on impose les conditions de degré les plus restrictives possibles, ce que nous faisons ici. On dira qu'un polynôme M de $\mathbf{IF}_q[X]$ de degré 2n ou $2n-1$ admet une représentation restreinte en somme de deux carrés, s'il existe des polynômes A et B de degré au plus n, tels que

$$M = A^2 + B^2.$$

Une telle représentation est équivalente à la représentation de M comme produit

$$M = UV$$

où U et V sont des polynômes de degré n si M est de degré 2n, où U et V sont des polynômes de degré n et $n-1$ si M est de degré $2n-1$. On a la caractérisation :

Un polynôme M de $\mathbf{IF}_q[X]$ admet une représentation restreinte en somme de deux carrés si et seulement si M admet un diviseur de degré égal à la partie entière du degré de M.

Le problème ainsi exprimé se pose que -1 soit, ou ne soit pas carré dans $\mathbf{IF}_q$, que q

soit pair ou impair. C'est sous cette forme que nous l'étudions ici. Dans [3] ERDOS a étudié un problème similaire pour les entiers. Sa démonstration reprise et améliorée dans [6] nous aidera beaucoup. Nous obtiendrons une majoration et une minoration du nombre $\mathbf{A}(m)$ de polynômes de degré m admettant un diviseur de degré [m/2] et nous en déduirons le théorème suivant :

THEOREME. *Pour tout entier* $m \geqslant 1$, *soit* $\mathbf{A}(m)$ *le nombre de polynômes unitaires de degré* m *de* $\mathbf{IF}_q[X]$ *admettant un diviseur de degré* [m/2]. *Alors, pour tout nombre réel* $\epsilon > 0$, *il existe un entier* $m(q,\epsilon)$ *ne dépendant que de* q *et de* ϵ, *tel que pour* $m \geqslant m(q,\epsilon)$ *on ait*

$$q^m\, m^{-\alpha-\epsilon} \leqslant \mathbf{A}(m) \ll q^m\, m^{-\alpha}\, (\log m)^{-1/2},$$

où

$$\alpha = 1 - \frac{1 + \log(\log 2)}{\log 2}$$

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

La démonstration de ce théorème nécessite l'estimation du nombre de polynômes de degré n admettant k kacteurs irréductibles. Cette estimation est donnée au paragraphe III.

II - NOTATIONS ET CONVENTIONS

On désigne par *U* l'ensemble des polynômes unitaires de $\mathbf{IF}_q[X]$. Le mot polynôme désignera toujours un polynôme de *U*. Soit A un tel polynôme. On note

d^oA le degré de A,

$|A|$ le nombre q^{d^oA},

$d(A)$ le nombre de diviseurs unitaires de A.

Si A s'écrit comme produit

$$A = P_1^{u_1} \ldots P_r^{u_r},$$

où $P_1,\ldots,P_r$ sont des polynômes irréductibles deux à deux distincts, où $u_1,\ldots,u_r$ sont des entiers strictement positifs, on pose

$$\omega(A) = r \quad \text{et} \quad \Omega(A) = u_1 + \ldots + u_r .$$

Si $\omega(A) = \Omega(A)$ le polynôme A est dit sans facteur carré.

Soient A et B deux polynômes. On note

(A,B) le plus grand diviseur commun de A et de B,

A | B la relation A divise B.

On désigne par I l'ensemble des polynômes irréductibles. Pour tout entier $m \geqslant 1$, on désigne par $A(m)$ l'ensemble des polynômes de degré m ayant un facteur irréductible de degré $[m / 2]$.

Si B est un ensemble fini de polynômes, on note

$\| B \|$ le nombre d'éléments de B,

et, pour tout nombre réel y, on note

$$\sigma_y(B) \text{ la somme } \sum_{B \in B} |B|^y.$$

III - RAPPELS

Dans $\mathbf{IF}_q[X]$ les polynômes irréductibles ont une répartition analogue à celle des nombres premiers. Cette distribution est donnée par le théorème suivant auquel nous nous référerons souvent par la suite.

THEOREME II. *Soit* $\pi(n)$ *le nombre de polynômes irréductibles unitaires de degré* n *de* $\mathbf{IF}_q[X]$. *Alors, pour tout entier* $n \geqslant 1$,

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

C'est le lemme 1 de [5].

Soient k et n des entiers strictements positifs. On désigne par

$\mathbf{P}_k(n)$ le nombre de polynômes $H \in U$ tels que $\Omega(H) = k$,

$q_k(n)$ le nombre de polynômes $H \in U$ tels que $\Omega(H) = \omega(H)$ et $\Omega(H) = k$.

On a des estimations de ces nombres $\mathbf{P}_k(n)$ et $q_k(n)$. Elles sont données par le

THEOREME **F**. *Soit un nombre réel* $B > 0$. *Alors, on a*

$$q_k(n) << \frac{q^n (\log n)^{k-1}}{n\,(k-1)!} \quad \textit{si } 1 \leqslant k \leqslant B\log(n),$$

Soit un nombre réel $B \in]0,q[$. *Alors, on a*

$$\mathbf{P}_k(n) << \frac{q^n (\log n)^{k-1}}{n\,(k-1)!} \quad \textit{si } 1 \leqslant k \leqslant B\log(n).$$

(les constantes impliquées par les symboles $<<$ *ne dépendant que de* q *et de* B*).*

Ce théorème a été établi en [2] .

IV - MAJORATION DE A(m)

Dans ce paragraphe les constantes impliquées par les symboles $<<$ ne dépendent que de q ou sont absolues.

LEMME. *Soient* a *et* b *des nombres réels tels que* $0 < b < 1 < a$. *Alors, pour tout nombre réel* $x > 0$, *on a*

$$(1) \qquad \sum_{h \geqslant ax} \frac{x^h}{h!} << \left(\frac{e}{a}\right)^{ax} x^{-1/2},$$

$$(2) \qquad \sum_{h \leqslant bx} \frac{x^h}{h!} << \left(\frac{e}{b}\right)^{bx} x^{-1/2}.$$

Démonstration. C'est le lemme 1.3.2, chapitre I, de [6] .

PROPOSITION IV-1. *Soit*

$$\alpha = 1 - \frac{1 + \log(\log 2)}{\log(2)} .$$

Alors, pour tout entier $m \geqslant 2$, *on a*

$$(3) \qquad \mathbf{A}(m) << q^m m^{-\alpha} (\log m)^{-1/2}.$$

Démonstration. Soit un entier n tel que

$$(*) \qquad \log(2n+1) < 2\log(2)\log(n).$$

Cette condition est réalisée dès que n est supérieur à une constante absolue n_o . Soit $m \in \{2n, 2n+1\}$.

Posons

$$a = \frac{\log m}{\log 2}, \quad b = \frac{13 \log m}{10 \log 2}, \quad c = \frac{11 \log m}{10 \log 2} .$$

On partage l'ensemble $A(m)$ en quatre sous-ensembles $A_i(m)$ $(1 \leqslant i \leqslant m)$ déterminés par les conditions suivantes

$$H \in A_1(m) \iff \Omega(H) < a,$$

$$H \in A_2(m) \iff a \leqslant \Omega(H) < b,$$

$$H \in A_3(m) \iff b \leqslant \Omega(H) \text{ et } \omega(H) < c,$$

$$H \in A_4(m) \iff b \leqslant \Omega(H) \text{ et } \omega(H) \geqslant c.$$

On pose

$$A_i(m) = \| A_i(m) \| . \quad (1 \leqslant i \leqslant 4)$$

On a

$$A_1(2n) \leqslant \sum_{k+\ell \leqslant a} \mathbf{P}_k(n)\mathbf{P}_\ell(n) \quad \text{et} \quad A_1(2n+1) \leqslant \sum_{k+\ell < a} \mathbf{P}_k(n)\mathbf{P}_\ell(n+1).$$

La condition (*) permet d'appliquer le théorème **F** aux nombres $\mathbf{P}_k(n)$, $\mathbf{P}_\ell(n)$, $\mathbf{P}_\ell(n+1)$.

$$A_1(2n) << \sum_{k+\ell<a} \frac{q^{2n}(\log(n))^{k+\ell-2}}{n^2\,(k-1)!\,(\ell-1)!} << \frac{q^m}{m^2} \sum_{k+\ell<a} \frac{(\log(m))^{k+\ell-2}}{(k-1)!\,(\ell-1)!}.$$

On a une majoration analogue pour $A_1(2n+1)$, d'où,

$$A_1(m) << \frac{q^m}{m^2} \sum_{j<Y} \frac{(\log m)^j}{j!} \sum_{i=0}^{j} \frac{j!}{i!\,(j-i)!} = \frac{q^m}{m^2} \sum_{j<Y} \frac{(2\log(m))^j}{j!},$$

avec

$$Y = a - 2 = \frac{\log m}{\log 2} - 2.$$

Avec (2) il vient

$$A_1(m) << q^m\, m^{-2}\, (\log m)^{-1/2}\, (2e\log(2))^{\frac{\log m}{\log 2}},$$

(i) $$A_1(m) << q^m\, m^{-\alpha}\, (\log m)^{-1/2}.$$

On a

$$A_2(m) \leqslant \sum_{a \leqslant k < b} \mathbf{P}_k(m).$$

Le théorème **F** s'applique aux nombres $\mathbf{P}_k(m)$ tels que $k < b = \dfrac{13 \log m}{10 \log 2}$, d'où

$$A_2(m) \ll q^m m^{-1} \sum_{a \leqslant k < b} \frac{(\log m)^{k-1}}{(k-1)!} .$$

La majoration (1) du lemme nous donne

$$\text{(ii)} \qquad A_2(m) \ll q^m m^{-\alpha} (\log m)^{-1/2} .$$

Si $H \in A_3(m)$, H est divisible par le carré d'un polynôme L tel que $\Omega(L) > a/10$, d'où :

$$A_3(m) \leqslant \sum_{\substack{L \in U \\ d^oL \leqslant m \\ \Omega(L) > a/10}} \sum_{\substack{H \in U \\ d^oH = m \\ L^2 \mid H}} 1 \leqslant q^m \sum_{\substack{L \in U \\ a/10 < d^oL \leqslant m}} |L|^{-2} \ll q^m q^{-a/10} \leqslant$$

$$q^m 2^{-a/10} ;$$

$$\text{(iii)} \qquad A_3(m) \ll q^m m^{-1/10} .$$

Si $H \in A_4(m)$,

$$d(H) \geqslant 2^{\omega(H)} \geqslant 2^{11a/10} = m^{11/10},$$

d'où

$$A_4(m) \ll m^{-11/10} \sum_{\substack{H \in U \\ d^oH = m}} d(H) .$$

Il est facile d'établir, et c'est le lemme 2 de [5], que

$$\sum_{\substack{H \in U \\ d^oH = m}} d(H) = (m+1)q^m ,$$

d'où

$$\text{(iv)} \qquad A_4(m) \ll q^m m^{-1/10} .$$

Les majorations (i), (ii), (iii) et (iv) nous donnent la majoration

$$\mathbf{A}(m) \ll q^m m^{-\alpha} (\log m)^{-1/2}$$

valable dans le cas où $m \in \{2n,2n+1\}$, l'entier n vérifiant la condition (*). Un changement de constante permet de lever cette restriction.

V - MINORATION DE $\mathbf{A}(m)$

On construit un ensemble G_m contenu dans $A(m)$ dont on minorera le nombre d'éléments.

Soit un entier $K \geqslant 3$. Cet entier sera choisi ultérieurement au paragraphe 5. Jusque là, K est supposé fixé, et les constantes impliquées par les symboles $\mathbf{0}$ et $\ll$ que nous utiliserons ne dépendront que de q et de K ou seront absolues.

1. - Construction de l'ensemble G_m

Soit m un entier tel que

$$m > 2^{4K}\ ,\ m > \left(\frac{2\log(m)}{K\log(2)}\ (1+2m^{-1/K})\right)^K . \tag{1}$$

Soit

$$t = \left[\frac{\log(m)}{2K\log(2)}\right]. \tag{2}$$

Pour $k \in \{1,\ldots,K-2\}$, soit P_k l'ensemble des polynômes irréductibles P tels que

$$m^{k/K} \leqslant d^oP < m^{(k+1)/K} . \tag{3}$$

Soit B l'ensemble des polynômes sans facteur carré ayant exactement t facteurs irréductibles unitaires dans chaque ensemble P_k, $1 \leqslant k \leqslant K-2$, et n'ayant pas d'autres facteurs irréductibles. Les conditions (1) assurent que l'ensemble B n'est pas vide. En outre on a la

PROPOSITION V-1. *Soient*

$$\beta(m) = \left(\frac{\log(m)}{2K\log(2)} - 1\right) m^{1-\frac{2}{K}}, \tag{4}$$

$$b(m) = \left(\frac{\log(m)}{2K\log(2)}\right) m^{1-\frac{2}{K}} (1 + 2m^{-1/K}) . \tag{5}$$

Alors, si $B \in B$,

$$\beta(m) \leqslant d^oB \leqslant b(m), \tag{6}$$

et, en conséquence

$$\| B \| \leqslant \frac{q^{b(m)+1}}{q-1}. \tag{7}$$

Démonstration. Immédiate, à partir des relations (1), (2) et (3).

On pose m = 2n ou m = 2n+1 suivant la parité de m. Pour $j \in \{n,n+1\}$, soit H_j l'ensemble des polynômes de degré j s'écrivant comme produit PB où $B \in B$, où P est un polynôme irréductible. De la proposition précédente on déduit que la décomposition

$$H = PB\ ,\ P \in I\ ,\quad B \in B,$$

des polynômes de H_j est unique. On pose alors

$$P = p(H)\ ,\ B = B(H).$$

Soit G_m l'ensemble des polynômes s'écrivant comme produit UV où $U \in H_n$, où $V \in H_{m-n}$. On a

$$\| G_m \| \leqslant A(m)\ . \tag{8}$$

D'autre part, on a la

PROPOSITION V-2. *Soit* $\mathbf{S}_m$ *le nombre de solutions de l'équation*

$$UV' = U'V \tag{E}$$

telles que $U \in H_n$, $U' \in H_n$, $V \in H_{m-n}$, $V' \in H_{m-n}$. *Alors, on a*

$$\| H_n \times H_{m-n} \|^2 \leqslant \mathbf{S}_m \| G_m \|\ . \tag{9}$$

Démonstration. Pour tout entier $h \geqslant 1$, soit r_h le nombre de polynômes $G \in G_m$ tels que l'équation G = UV ait exactement h solutions (U,V) dans $H_n \times H_{m-n}$. Alors,

$$\| G_m \| = \sum_{h=1}^{\infty} r_h\ ,\ \mathbf{S}_m = \sum_{h=1}^{\infty} h^2 r_h\ ,\ \| H_n \times H_{m-n} \| = \sum_{h=1}^{\infty} h r_h\ ,$$

ces sommes étant en fait finies. L'inégalité de Cauchy-Schwarz donne (9).

2. - Estimations auxiliaires

Ces estimations sont basées sur le théorème II énoncé au paragraphe III.

PROPOSITION V-3. *Si* $h \in \{1,...,K-2\}$, *soit* I_h *la réunion des ensembles* $P_1, P_2, ..., P_h$, si $h \in \{1,...,K-3\}$, *soit* I'_h *la réunion des ensembles* $P_{h+1}, ..., P_{k-2}$. *Alors, on a*

$$(10) \qquad \left| \sigma_{-1}(P_h) - \frac{\log m}{K} \right| \leqslant \frac{19}{10} m^{-h/K} \qquad \text{si } 1 \leqslant h \leqslant K-2,$$

$$(11) \qquad \left| \sigma_{-1}(I_h) - h\frac{\log m}{K} \right| << m^{-1/K} \qquad \text{si } 1 \leqslant h \leqslant K-2,$$

$$(12) \qquad \left| \sigma_{-1}(I'_h) - (K-2-h)\frac{\log m}{K} \right| << m^{-h/K} \qquad \text{si } 1 \leqslant h < K-2,$$

$$(13) \qquad \sigma_{-2}(P_h) \leqslant \frac{q}{q-1} q^{-m^{h/K}} m^{-h/K} \qquad \text{si } 1 \leqslant h \leqslant K-2,$$

$$(14) \qquad \frac{\{\sigma_{-1}(I'_h)\}^{2(K-2-h)t}}{\{[(K-2-h)t]!\}^2} << t^{-1}(2e\log(2))^{2(K-2-h)t} \qquad \text{si } 1 \leqslant h < K-2,$$

$$(15) \qquad \frac{\{\sigma_{-1}(I_h)\}^{2ht}}{\{[ht/2]!\}^4} << t^{-2}(4e\log(2))^{2ht} \qquad \text{si } 1 \leqslant h \leqslant K-2 \text{ et si } ht \text{ est pair,}$$

$$(16) \qquad \frac{\{\sigma_{-1}(I_h)\}^{2ht}}{\{r!(r+1)!\}^2} << t^{-2}(4e\log(2))^{2ht} \qquad \text{si } 1 \leqslant h \leqslant K-2, \text{ si } ht \text{ est impair et si } ht = 2r+1.$$

Démonstration. Les relations (10), (11), (12) et (13) sont des conséquences immédiates de (1), (3) et du théorème II, la constante 19/10 est très grossièrement calculée mais cela suffit pour les calculs ultérieurs. Les relations (14), (15) et (16) se déduisent des relations (2), (11) et (12) et de la formule de Stirling.

PROPOSITION V-4. *On a*

$$(17) \qquad \sigma_{-1}(B) >> (\log m)^{-\frac{K-2}{2}} m^{(1-\frac{\alpha}{2})(1-\frac{2}{K})},$$

où,

$$\alpha = 1 - \frac{1 + \log(\log 2)}{\log(2)}.$$

Démonstration. Désignons par B_i , $1 \leqslant i \leqslant K-2$, l'ensemble des polynômes sans facteur carré, produits de t facteurs irréductibles de P_i et n'ayant pas d'autres facteurs irréductibles. Tout polynôme $B \in B$ s'écrit de façon unique comme produit $B_1 \ldots B_{K-2}$ où $B_i \in B_i$, d'où,

$$\sigma_{-1}(B) = \sum_{(B_1,\ldots,B_{K-2}) \in B_1 \times \ldots \times B_{K-2}} |B_1,\ldots,B_{K-2}|^{-1} ,$$

$$(*) \qquad \sigma_{-1}(B) = \prod_{i=1}^{K-2} \sigma_{-1}(B_i) .$$

Le lemme 13, p. 147, de [4] nous donne

$$\sigma_{-1}(B_i) \geqslant \frac{1}{t!}\{\sigma_{-1}(P_i)\}^t \left\{1 - \binom{t}{2} [\sigma_{-1}(P_i)]^{-2} \sigma_{-2}(P_i)\right\}.$$

Les relations (1), (10) et (13) nous donnent

$$\binom{t}{2}\{\sigma_{-1}(P_i)\}^{-2} \sigma_{-2}(P_i) \leqslant \frac{q}{2(q-1)} t^2 K^2 (\log m)^{-2} \left(1 + \frac{19}{5} m^{-i/K} (\log m)^{-1}\right)^2 q^{-m^{i/K}} m^{-i/K} \leqslant$$

$$\frac{q^{-15}}{32(q-1)} \left(1 + \frac{19}{80} (4K\log(2))^{-1}\right) t^2 K^2 (\log m)^{-2} .$$

Avec la relation (2) il vient

$$\binom{t}{2} \{\sigma_{-1}(P_i)\}^{-2} \sigma_{-2}(P_i) \leqslant \frac{q^{-15}}{32(q-1)} (4K^2\log(2))^{-1} \left(1 + \frac{19}{80} (4K\log(2))^{-1}\right),$$

et,

$$\sigma_{-1}(B_i) >> \frac{1}{t!}\{\sigma_{-1}(P_i)\}^t .$$

D'après les relations (10) et (12),

$$\sigma_{-1}(B_i) >> \frac{1}{t!} \left(\frac{\log m}{K}\right)^t .$$

Avec (2) et la formule de Stirling, il vient

$$\sigma_{-1}(B_i) >> t^{-1/2} \left(\frac{e\log(m)}{tK}\right)^t >> (\log m)^{-1/2} (2e\log(2))^{\frac{\log m}{2K \log 2}} ,$$

et, avec (*),

$$\sigma_{-1}(B) >> (\log m)^{-\frac{K-2}{2}} (2e\log(2))^{\frac{(K-2)\log(m)}{2K\log(2)}} ,$$

$$\sigma_{-1}(B) >> (\log m)^{-\frac{K-2}{2}} m^{(1-\frac{\alpha}{2})\frac{K-2}{K}}.$$

PROPOSITION V-5. *On a*

$$\sigma_{-1/2}(B) \leqslant q^{(b(m)+1)/2}. \tag{18}$$

Démonstration. Avec (6) il vient

$$\sigma_{-1/2}(B) \leqslant \sum_{\substack{B \in U \\ \beta(m) \leqslant d^{o}B \leqslant b(m)}} |B|^{-1/2} = \sum_{\beta(m) \leqslant r \leqslant b(m)} q^{r/2}.$$

3. - Minoration de $\| H_j \|$

PROPOSITION V-6. *Soit* $j \in \{n, n+1\}$. *Alors, on a*

$$\| H_j \| >> q^j (\log m)^{-\frac{K-2}{2}} m^{\frac{\alpha}{K} - \frac{\alpha}{2} - \frac{2}{K}}. \tag{19}$$

Démonstration. Un polynôme de H_j est de degré j et s'écrit de façon unique comme produit PB où $P \in I$ et $B \in B$, d'où,

$$\| H_j \| = \sum_{B \in B} \pi(j - d^{o}B).$$

On applique le théorème II.

$$\| H_j \| \geqslant \sum_{B \in B} \frac{q^{j-d^{o}B}}{j-d^{o}B} (1 - 2q^{-(j-d^{o}B)/2}) \geqslant \frac{q^j}{j} \sum_{B \in B} \frac{1}{|B|} - 2q^{\frac{j}{2}} \sum_{B \in B} \frac{|B|^{-1/2}}{j-d^{o}B}.$$

Avec (1), (5) et (6) il vient

$$\| H_j \| \geqslant \frac{q^j}{j} \sigma_{-1}(B) - \frac{4}{j} \sigma_{-1/2}(B).$$

Les propositions précédentes nous donnent

$$\| H_j \| >> \frac{q^j}{j} (\log m)^{-\frac{K-2}{2}} m^{(1-\frac{\alpha}{2})(1-\frac{2}{K})}.$$

4. - Majoration de $\mathbf{S}_m$

PROPOSITION V-7. *Il existe une constante* $\tau = \tau(q,K)$ *ne dépendant que de* q *et de* K, *telle que*

$$\mathbf{S}_m \ll (\log m)^{K+\tau-4}\, m^{\frac{1}{2K\log 2}}\, \| H_n \times H_{m-n} \| . \tag{20}$$

Démonstration. Soit $(U,U',V',V') \in H_n \times H_n \times H_{m-n} \times H_{m-n}$ une solution de l'équation

$$UV' = U'V. \tag{E}$$

Il existe des polynômes irréductibles P,P',Q,Q', des polynômes B,B',C,C' de B tels que

$$P\,B\,Q'C' = P'B'Q\,C,$$

et, d'après la proposition V- 1,

$$P\,Q' = P'Q. \tag{E'}$$

Si $P = Q'$, alors, $P = P' = Q = Q'$. Si $P \neq Q'$, l'équation (E') n'est satisfaite que dans les cas suivants

(i) $P = P'$ et $Q = Q'$,

(ii) $P = Q$ et $P' = Q'$.

Si (i) a lieu et si les polynômes U et V sont premiers entre eux, V divise V' resp. U divise U', mais V et V' sont de même degré et unitaires. On a donc dans ce cas $U = U'$ et $V = V'$.
Si (ii) a lieu et si les polynômes U et U' sont premiers entre eux, U divise V, resp. U' divise V'. Ceci ne peut avoit lieu que si m est pair. En effet, si $m = 2n+1$, il existe un polynôme H de degré 1 tel que $V = UH$. Ce polynôme H est quotient de deux polynômes de B, ses facteurs irréductibles sont dans $P_1 \cup \ldots \cup P_{K-2}$, et de degré au moins égal à $m^{1/K}$ ce qui est impossible compte tenu de la condition (1). Si $m = 2n$, comme pour (i) on a $U = V$ et $U' = V'$.
On partage les $\mathbf{S}_m$ solutions (U,U',V,V') de (E) en cinq classes :

(1) les solutions telles que $p(U) = p(U') = p(V) = p(V')$;
(2) les solutions telles que $p(U) \neq p(V)$ et $(U,V) = 1$;
(3) les solutions telles que $p(U) \neq p(U')$ et $(U,U') = 1$;
(4) les solutions telles que $p(U) \neq p(V)$ et $(U,V) \neq 1$;
(5) les solutions telles que $p(U) \neq p(U')$ et $(U,U') \neq 1$;

la troisième classe pouvant être vide. On note $S_1,\ldots,S_5$ le nombre d'éléments de ces classes.

Le polynôme irréductible p(U) est de degré au plus $n+1-\beta(m) \leqslant n$. Il y a moins de $q^n \| B \|^4$ solutions dans la première classe, d'où,

(a) $$S_1 \leqslant q^{n+4b(m)}.$$

On a

(b) $$S_2 = \| H_n \times H_{m-n} \|,$$

(c) $$S_3 = \begin{cases} \| H_n \|^2 & \text{si} \quad m = 2n, \\ 0 & \text{si} \quad m = 2n+1. \end{cases}$$

Si (U,U,V,V') est une solution de la quatrième classe, resp. de la cinquième classe, $(U,V) \neq 1$ et $(U,V) = (B(U),B(V))$ resp. $(U,U') = 1$ et $(U,U') = (B(U),B(U'))$. Les facteurs irréductibles de (U,V), resp. (U,U'), appartiennent aux ensembles $P_1, \ldots, P_{K-2}$.

Si D est un polynôme sans facteur carré, dont les facteurs irréductibles sont dans la réunion des ensembles $P_1, \ldots, P_{K-2}$, soit h(D) le plus petit entier h tel que tous les facteurs irréductibles de D soient dans $I_h = P_1 \cup \ldots \cup P_h$. On a alors

$$\omega(D) \leqslant th(D).$$

Notons $D_{h,k}$, $1 \leqslant h \leqslant K-2$, $1 \leqslant k \leqslant ht$, l'ensemble des polynômes D sans facteur carré, dont les facteurs irréductibles sont dans $P_1 \cup \ldots \cup P_{K-2}$ et tels que $h(D) = h$ et $\omega(D) = k$. Notons S(h,k) resp. T(h,k), le nombre de solutions (U,U',V,V') de (E) appartenant à la quatrième classe, resp. à la cinquième classe, telles que $h((U,V)) = h$, $\omega((U,V)) = k$, resp. telles que $h((U,U')) = h$, $\omega((U,U')) = k$. On a

(d) $$S_4 = \sum_{h=1}^{K-2} \sum_{k=1}^{ht} S(h,k),$$

(e) $$S_5 = \sum_{h=1}^{K-2} \sum_{k=1}^{ht} T(h,k).$$

Considérons maintenant un polynôme $D \in D_{h,k}$. Pour $j \in \{n,n+1\}$ soit $H_{D,j}$ le nombre de solutions $Y \in H_j$ de la congruence

$$Y \equiv 0 \pmod{D}.$$

Il y a au plus $H_{D,n} \cdot H_{D,j}$ couples $(Y,Z) \in H_n \times H_j$ tels que $(Y,Z) = D$.

LEMME 1. *Soient* $U \in H_n$, $V \in H_j$ *tels que* $(U,V) = D$. *Alors, il y a au plus* $q_k(d^oD)$ *solutions* $(U,U',V,V') \in H_n \times H_n \times H_j \times H_j$ *de l'équation* (E).

Démonstration. Si (U,U',V,V') est une solution de (E),

$$(*) \qquad V' \equiv 0 \pmod{\frac{V}{D}}.$$

Réciproquement, si $V' \in H_j$ vérifie (*), l'équation UV' = U'V a une seule solution U'. Si $V' \in H_j$ vérifie (*), il existe un polynôme W tel que $V' = W\frac{V}{D}$, le polynôme W est sans facteur carré et vérifie les relations :

$$d^oW = d^oD \ , \ \omega(W) = \omega(D) = k.$$

LEMME 1'. *Soient* U *et* U' *des polynômes de* H_n *tels que* D = (U,U'). *Alors, il y a au plus* $q_k(j-n+d^oD)$ *solutions* $(U,U',V,V') \in H_n \times H_n \times H_j \times H_j$ *de l'équation* (E).

Démonstration. Semblable à celle du lemme 1.

LEMME 2. *Posons* $\ell = ht - k$, $r = (K-2-h)t$. *Alors, pour* $j \in \{n,n+1\}$,

$$H_{D,j} \leqslant \frac{q^j}{j\,|D|}\left(1 + \frac{2b(m)}{j}\right)\frac{\{\sigma_{-1}(I_h)\}^{\ell}}{\ell!}\ \frac{\{\sigma_{-1}(I'_h)\}^{r}}{r!},$$

le dernier terme étant pris égal à 1 *lorsque* $h = K-2$.

Démonstration. Soit $U \in H_j$ congru à 0 modulo D. Alors,

$$d^oU = j \ \text{ et } \ U = PDB', \text{ avec } P \in I, \ \ DB' \in B.$$

Posons B' = LR où tous les facteurs irréductibles de L sont dans I_h, où tous les facteurs irréductibles de R sont dans I'_h . On peut avoir L = 1 si k = ht, R = 1 si h = K–2. On a

$$\omega(L) + \omega(D) = ht \ \text{ et } \ \omega(R) = (K-2-h)t.$$

Notons L, resp. R, l'ensemble des polynômes sans facteur carré ayant ℓ facteurs irréductibles dans I_h , resp. ayant r facteurs irréductibles dans I'_h . On a alors

$$H_{D,j} \leqslant \sum_{L \in L} \ \sum_{R \in R} \pi(j - d^o(DLR)).$$

Le théorème Π nous donne

$$H_{D,j} \leqslant |D|^{-1} q^j \sum_{L \in L} \sum_{R \in R} \frac{1}{|LR|^{(j-d^o(DLR))}},$$

d'où, avec (6), (4) et (1),

$$H_{D,j} \leqslant \frac{q^j}{j|D|} \left(1 + \frac{2b(m)}{j}\right) (\sigma_{-1}(L))(\sigma_{-1}(R)).$$

Les polynômes de L étant produits de ℓ facteurs irréductibles de I_h deux à deux distincts, on a

$$\sigma_{-1}(L) \leqslant \frac{\{\sigma_{-1}(I_h)\}^\ell}{\ell!},$$

et, dans le cas où $h \neq K-2$, on a de même,

$$\sigma_{-1}(R) \leqslant \frac{\{\sigma_{-1}(I'_h)\}^r}{r!}.$$

Les lemmes 1, 1' et 2 nous donnent donc

$$S(h,k) << \frac{q^m}{m^2} \sum_{D \in D_{h,k}} |D|^{-2} q_k(d^oD) \frac{\{\sigma_{-1}(I_h)\}^{2\ell} \{\sigma_{-1}(I'_h)\}^{2r}}{\{\ell!\}^2 \{r!\}^2},$$

$$T(h,k) << \frac{q^m}{m^2} \sum_{D \in D_{h,k}} |D|^{-2} q_k(d^oD+m-2n) \frac{\{\sigma_{-1}(I_h)\}^{2\ell} \{\sigma_{-1}(I'_h)\}^{2r}}{\{\ell!\}^2 \{r!\}^2}.$$

Doit $D \in D_{h,k}$. Alors,

$$k = \omega(D) \leqslant th \leqslant h\log(m)/2K\log(2),$$

$$d^oD + m-2n \geqslant d^oD \geqslant m^{h/K},$$

$$\log(d^oD + m-2n) \geqslant \log(d^oD) \geqslant \frac{h}{k}\log(m) \geqslant \omega(D).$$

On applique le théorème **F**.

$$q_k(d^oD) << \frac{|D|}{d^oD} \frac{(\log d^oD)^{k-1}}{(k-1)!},$$

$$q_k(d^oD + m-2n) << \frac{|D|}{d^oD} \frac{(\log d^oD)^{k-1}}{(k-1)!}. \quad (\text{car } m \in \{2n, 2n+1\})$$

Les sommes S(h,k) et T(h,k) se majoreront de façon identique. On a

$$q_k(d^oD) << |D|\, m^{-h/K}\, \frac{(\log d^oD)^k}{k!}\ ,$$

on a aussi

$$d^oD \leqslant ht\, m^{(h+1)/K},$$

d'où, avec (11)

$$\log d^oD \leqslant \sigma_{-1}(I_h)\,(\frac{h+1}{h})\,(1+u(m)),$$

où

$$(+) \qquad u(m) << \frac{\log(\log m)}{\log(m)}\ .$$

On a donc la majoration

$$S(h,k) << \frac{q^m}{m^2}\,\sigma_{-1}(D_{h,k})\,m^{-h/K}\,(\frac{h+1}{k})^k\,(1+u(m))^k\,\frac{\{\sigma_{-1}(I_h)\}^{2\ell+k}\{\sigma_{-1}(I'_h)\}^{2r}}{\{k!\}\{\ell!\}^2\{r!\}^2}\ .$$

Pour $k \leqslant ht$,

$$(\frac{h+1}{h})^k \leqslant e^t\ ,$$

et, d'après (+) , il existe une constante $\tau = \tau\ (q,K)$ ne dépendant que de q et de K, telle que

$$(1+u(m))^k << (\log m)^\tau\ .$$

Les polynômes de $D_{h,k}$ étant produits de k facteurs irréductibles distincts de I_h ,

$$\sigma_{-1}(D_{h,k}) \leqslant \frac{\{\sigma_{-1}(I_h)\}^k}{k!}\ .$$

On avait posé au lemme 2

$$\ell = ht - k \quad \text{et} \quad r = (K-2-h)t\ .$$

On a donc

$$S(h,k) << (\log m)^\tau\ e^t\, q^m\, m^{-2-h/K}\ \frac{\{\sigma_{-1}(I_h)\}^{2ht}\{\sigma_{-1}(I'_h)\}^{2(K-2-h)t}}{\{k!\,(ht-k)!\}^2\{[(K-2-h)t]!\}^2}\ .$$

On a une majoration analogue pour T(h,k).
Les relations (d) et (e) nous donnent

$$S_4 + S_5 << (\log m)^{\tau}\, e^t \frac{q^m}{m^2} \sum_{h=1}^{K-2} m^{-h/K} \sum_{k=1}^{ht} \frac{\{\sigma_{-1}(I_h)\}^{2ht}\{\sigma_{-1}(I'_h)\}^{2(K-2-h)t}}{\{k!\,(ht-k)!\}^2\{[(K-2-h)t]!\}^2}.$$

La fonction $k \mapsto k!\,(ht-k)!$ atteint son minimum pour $k = ht/2$, ou pour $k = (ht-1)/2$ suivant que ht est pair ou impair. Les majorations (14) et (15) nous donnent alors,

$$S_4 + S_5 << (\log m)^{\tau}\, e^t \frac{q^m}{m^2} \sum_{h=1}^{K-2} m^{-h/K}\, 2^{2ht_t - 2}\, (2e\log(2))^{2(K-2)t},$$

d'où, avec (2),

$$S_4 + S_5 << (\log m)^{\tau-2}\, m^{1/2K\log 2}\, q^m\, m^{-2}\, m^{(1+\frac{1+\log(\log 2)}{\log 2})(\frac{K-2}{K})}.$$

On conclut avec les relations (a), (b), (c) et (19).

5. - Minoration de $\mathbf{A}(m)$

C'est ici que l'on va choisir K.

PROPOSITION V-8. *Pour tout nombre réel* $\epsilon > 0$, *il existe un entier* $m(q,\epsilon)$ *ne dépendant que de* q *et de* ϵ, *tel que, pour tout entier* $m \geqslant m(q,\epsilon)$, *on ait*

$$\mathbf{A}(m) \geqslant q^m\, m^{-\alpha-\epsilon}.$$

Démonstration. On prend pour K le plus petit entier $K = K(\epsilon)$ tel que

$$\frac{4 - 2\alpha + (1/2\log 2)}{K} < \frac{\epsilon}{2}.$$

Il existe un entier $m(\epsilon)$ tel que tout entier $m \geqslant m(\epsilon)$ vérifie les conditions (1). Soit $m \geqslant m(\epsilon)$ et soit $n = [\frac{m}{2}]$. On a démontré que

(8) $$\mathbf{A}(m) \geqslant \| G_m \|,$$

(9) $$\| G_m \| \geqslant \| H_n \times H_{m-n} \|^2 (\mathbf{S}_m)^{-1},$$

$$\|H_j\| \gg q^j (\log m)^{-\frac{K-2}{2}} m^{\frac{\alpha}{K}-\frac{\alpha}{2}-\frac{2}{K}}, \text{ si } j = n, n+1, \tag{19}$$

$$\mathbf{S}_m \ll \|H_n \times H_{m-n}\| (\log m)^{K+\tau-4} m^{\frac{1}{2K\log 2}}, \tag{20}$$

où la constante τ ne dépend que de q et de K, et donc ici de q et de ϵ. Il existe une constante $\Theta > 0$, ne dépendant que de q et de ϵ, telle que, pour $m \geqslant m(\epsilon)$,

$$\mathbf{A}(m) \geqslant \Theta (\log m)^{6-\tau-2K} q^m m^{-\alpha-\epsilon/2}.$$

Il suffit de prendre pour $m(q,\epsilon)$ le plus petit entier $m \geqslant m(\epsilon)$ tel que

$$\Theta (\log m)^{6-\tau-2K} \geqslant m^{-\epsilon/2}.$$

REFERENCES

[1] M. CAR. *«Normes dans* $\mathbf{IF}_q[X]$ *de polynômes de* $\mathbf{IF}_{q^h}[X]$*»*. C.R.A.S., Paris, t. 288, (9 avril 1979).

[2] M. CAR. *«Factorisation dans* $\mathbf{IF}_q[X]$*»*. C.R.A.S., Paris, t. 294, (25 janvier 1982).

[3] P. ERDOS. *«Sur une inégalité asymptotique en théorie des nombres»*. Vestrik Leningrad Univ., 13, (1960), p.p. 41-49.

[4] H. HALBERSTAM. L. ROTH. *«Sequences»*. Oxford, at the Clarendon Press.

[5] M. MIGNOTTE. *«Statistiques sur* $\mathbf{IF}_q[X]$*»*. Comptes rendus des Journées de théorie analytique et élémentaire des nombres. Limoges (10-11 mars 1980).

[6] G. TENENBAUM. *«Estimations asymptotiques de fonctions arithmétiques liées aux diviseurs»*. Thèse, Bordeaux, 30 avril 1976.

(Manuscrit reçu le 15 décembre 1981)