References

[1] P. Erdős, *On the arithmetical density of the sum of two sequences one of which forms a basis for the integers*, Acta Arith. 1 (1936), pp. 197–200.
[2] H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press, Oxford 1966.
[3] H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. Math. (2) 43 (1942), pp. 523–527.
[4] L. G. Schnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. 107 (1933), pp. 649–690.
[5] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe*, J. Reine Angew Math. 194 (1955), pp. 111–140.

WASHINGTON STATE UNIVERSITY

Received on 15.4.1982
and in revised form on 4.3.1983 (1302)

ACTA ARITHMETICA
XLIV (1984)

Sommes de carrés de polynômes irréductibles dans $F_q[X]$

par

MIREILLE CAR (Marseille)

I. Introduction. Soit F_q le corps fini à q éléments, q étant un entier impair, et $F_q[X]$ l'anneau des polynômes à une variable sur le corps F_q. Certaines analogies entre les propriétés arithmétiques de l'anneau $F_q[X]$ et l'anneau Z des entiers relatifs ont été mises en évidence. En particulier, en ce qui concerne l'arithmétique additive les problèmes de Waring ([13]) et de Goldbach ([10]) ont été étudiés, et plus particulièrement, le problème de Waring pour les carrés ([3]–[9]). Il est démontré dans [7] que tout polynômes de $F_q[X]$ est somme de trois carrés sans que l'on ait une limitation des degrés des polynômes intervenant dans cette somme. Ceci conduit à introduire la définition suivante:

Si M est un polynôme de $F_q[X]$ de degré $2n$ ou $2n-1$, toute solution $(M_1, \ldots, M_k)$ de l'équation

$$M = M_1^2 + \ldots + M_k^2 \tag{E}$$

en polynômes $M_1, \ldots, M_k$ de degré au plus égal à n, est appelée *représentation restreinte de M en sommes de k carrés*. On a une estimation asymptotique du nombre $R_k(M)$ de ces représentations restreintes (cf. [1]), qui montre que, pour $k \geqslant 4$, tout polynôme de $F_q[X]$ de degré assez élevé admet une représentation restreinte en somme de k carrés, et que, pour $q \geqslant 53$, tout polynôme de $F_q[X]$ de degré assez élevé admet une représentation restreinte en somme de trois carrés. On peut aussi démontrer que pour $q \neq 3$, tout polynôme de $F_q[X]$ admet une représentation restreinte en somme de trois carrés, et que tout polynôme de $F_3[X]$ de degré différent de 3, admet une représentation restreinte en somme de trois carrés, [12].

On s'intéresse ici aux solutions $(P_1, \ldots, P_k)$ de l'équation (E) en polynômes irréductibles $P_1, \ldots, P_k$ satisfaisant aux mêmes conditions de degré, et au nombre $I_k(M)$ de représentations restreintes du polynôme M en somme de k carrés de polynômes irréductibles. On obtient, pour $k \geqslant 5$, une estimation asymptotique des nombres $I_k(M)$ qui montre que, pour $q \neq 3$, tout polynôme de $F_q[X]$ de degré assez élevé admet une représentation restreinte en somme de k carré de polynômes irréductibles, et que, pour

$q=3$, ce résultat reste vrai pour les polynômes non divisibles par les polynômes X, $X+1$, $X-1$.

II. Notations et conventions. Nous reprenons les notations introduites dans [2] et [10].

Soit H un polynôme de $F_q[X]$. On note $d^\circ H$ son degré, $\operatorname{sgn}(H)$ le coefficient du terme de plus haut degré de H, $\mathcal{C}_H$ l'ensemble de polynômes de degré strictement inférieur au degré de H identifié à l'ensemble des classes de congruence modulo H. Le groupe multiplicatif des classes inversibles modulo H sera noté $\mathcal{C}_H^*$, l'ordre de ce groupe sera noté $\Phi(H)$. La fonction ainsi définie a les mêmes propriétés que la fonction d'Euler classique. Le nombre de diviseurs irréductibles unitaires distincts de H sera noté $\omega(H)$.

On désigne par $\mathcal{U}$ l'ensemble des polynômes unitaires, par $\mathcal{I}$ l'ensemble des polynômes irréductibles.

Sur le corps $F_q(X)$ des fractions rationnelles on définit une valuation v par

$$v\left(\frac{A}{B}\right) = d^\circ A - d^\circ B,$$

si A et B sont des polynômes non nuls. Le complété de $F_q(X)$ pour cette valuation s'identifie au corps $\boldsymbol{K}$ des séries de Laurent en $1/X$, la valuation v se prolongeant à $\boldsymbol{K}$ par

$$v\Big(\sum_{s\in\boldsymbol{Z}} a_s X^s\Big) = -\sup\{r\in\boldsymbol{Z},\ a_r\neq 0\}.$$

A cette valuation v on associe la valeur absolue $|\ |_v$ définie par

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

Nous noterons simplement $|\ |$ cette valeur absolue, bien que ce symbole soit aussi utilisé pour désigner la valeur absolue classique sur le corps $\boldsymbol{R}$ des nombres réels, ou le corps $\boldsymbol{C}$ des nombres complexes.

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

$$\{t\in\boldsymbol{K}|\ v(t)>j\}.$$

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

Soit e un caractère non principal du groupe additif de F_q. On définit un caractère non principal du groupe additif $\boldsymbol{K}$ en posant

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

On note F_q^0 l'ensemble des éléments non nuls de F_q, et, pour tout élément $a\in F_q$, on désigne par $\varrho_j(a)$ le nombre de solutions $(a_1,\ldots,a_j)$ dans $F_q^0\times\ldots\times F_q^0$ de l'équation

$$a = a_1^2+\ldots+a_j^2.$$

Dans ce qui suit, le mot polynôme désignera toujours un polynôme de $F_q[X]$.

III. Propriétés du caractère E et de la mesure dt. Nous rappelons ici quatre résultats établis dans [10] que nous utiliserons fréquemment par la suite.

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

PROPOSITION III.2. (i) *Pour tout polynôme A, $E(A)=1$.*

(ii) *Si $u\in\mathcal{P}^2$, $E(u)=1$.*

(iii) *Pour tout polynôme H non nul, si A et B sont des polynômes congrus modulo H, $E(A/H)=E(B/H)$.*

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

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

PROPOSITION III.4. *Si G et H sont des polynômes premiers entre eux,*

$$\text{(III.2)} \qquad \sum_{R\in\mathcal{C}_H} E\left(\frac{G}{H}R\right) = 0.$$

IV. La méthode du cercle. Soit un entier $k\geqslant 5$. Dans ce paragraphe et dans les paragraphes suivants, s'il n'y a pas d'indication supplémentaire, les constantes impliquées par les symboles $\ll$ ne dépendront que de q et de k ou ne dépendront que de q.

Soit un nombre réel $h>0$ fixé. Il sera choisi ultérieurement en fonction de k. Soit un entier n tel que

$$\text{(IV.1)} \qquad n > 4h\frac{\log n}{\log q}+1, \qquad n > h^2\frac{\log^2 n}{\log^2 q}\left[\frac{q}{\log^2 q}+\frac{1}{8}\right].$$

Soit f l'application de $\mathcal{P}$ dans $\boldsymbol{C}$ définie par

$$\text{(IV.2)} \qquad f(t) = \sum_{\substack{P\in\mathcal{I}\\ d^\circ P\leqslant n}} E(tP^2).$$

Si M est un polynôme de degré $2n$ ou $2n-1$, la relation (III.1) montre que l'on a

$$\text{(IV.3)} \qquad I_k(M) = \int_{\mathcal{P}} f^k(t)\,E(-Mt)\,dt,$$

$I_k(M)$ désignant le nombre de représentations restreintes de M en somme de k carrés de polynômes irréductibles.

Posons

$$s = [h \log(n)/\log(q)], \tag{IV.4}$$

$$N = 2n-2s. \tag{IV.5}$$

On appelée *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) $G \in \mathcal{G}_H^*$.

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

$$\mathcal{U}_{G/H} = \left\{ t \in \mathcal{P},\ v\left(t - \frac{G}{H}\right) > N + d^\circ H \right\}$$

est appelée *arc de Farey à l'ordre N de centre G/H*.

Lorsque G/H décrit l'ensemble des fractions de Farey à l'ordre N, les arcs de Farey $\mathcal{U}_{G/H}$ forment une partition de $\mathcal{P}$. C'est le théorème 4.3 de [10].

Dans ce paragraphe, une fraction ou un arc de Farey désigneront toujours une fraction ou un arc de Farey à l'ordre N.

Sur les arcs de Farey $\mathcal{U}_{G/H}$ tels que $d^\circ H \leqslant 2s$ on a une bonne approximation de $f(t)$, ces arcs seront dits *majeurs*. Soit $\mathcal{M}$ leur réunion. Soit $\mathcal{M}'$ la réunion des arcs restant qui seront dits *mineurs*. Sur $\mathcal{M}'$ on a seulement une majoration de $|f(t)|$.

On pose pour tout entier $j \geqslant 1$,

$$\sigma_j = (q-1) \sum_{r=1}^{j} q^r/r. \tag{IV.6}$$

On note Ψ l'application de $\mathcal{P}_N$ dans $\boldsymbol{C}$ définie par

$$\Psi(u) = \begin{cases} \sigma_n & \text{si} \quad v(u) > 2n+1, \\ \sigma_{j-1} & \text{si} \quad v(u) = 2j \text{ avec } j \leqslant n, \\ \sigma_{j-1} + (q^j/j) \sum\limits_{b \in \boldsymbol{F}_q^0} e(ab^2) & \text{si} \quad v(u) = 2j+1 \text{ avec } j \leqslant n, \\ \qquad \text{et si } a \in \boldsymbol{F}_q^0 \text{ est tel que } v(u - aX^{-v(u)}) > v(u). \end{cases} \tag{IV.7}$$

On remarque que si $u = aX^{-v(u)} + v$, avec $a \in \boldsymbol{F}_q^0$ et $v(v) > v(u)$, $\Psi(u)$ ne dépend que de a et de $v(u)$. On pose alors

$$\Psi(u) = \varphi(a, v(u)). \tag{IV.8}$$

PROPOSITION IV.1. *Soit $t = G/H + u$ appartenant à l'arc majeur de centre G/H. Alors,*

$$\left| f^k(t) - \frac{W^k(G,H)}{\Phi^k(H)} \Psi^k(u) \right| \leqslant s q^{4s} q^{n/2} (\sigma_n)^{k-1}, \tag{IV.9}$$

où,

$$W(G,H) = \sum_{R \in \mathcal{G}_H^*} E\left(\frac{G}{H} R^2\right). \tag{IV.10}$$

Démonstration. La proposition X.3 de [2] nous donne

$$\left| f(t) - \frac{W(G,H)}{\Phi(H)} \Psi(u) \right| \leqslant s q^{4s} q^{n/2}.$$

On remarque que

$$\left| \frac{W(G,H)}{\Phi(H)} \Psi(u) \right| \leqslant |\Psi(u)| \leqslant \sigma_n,$$

et que, d'après le lemme 20 de [11],

$$|f(t)| \leqslant \sigma_n.$$

PROPOSITION IV.2. *Si t appartient à un arc mineur,*

$$|f(t)| \leqslant n s^{5/2} (\log n)\, q^n q^{-s/8}. \tag{IV.11}$$

Démonstration. C'est la proposition X.4 de [2].

PROPOSITION IV.3. *Soit G/H le centre d'un arc majeur. Soit*

$$I_{G/H,k}(M) = \int_{\mathcal{U}_{G/H}} f^k(t)\, E(-Mt)\, dt. \tag{IV.12}$$

Alors, on a

$$\left| I_{G/H,k}(M) - \frac{W^k(G,H)}{\Phi^k(H)} E\left(-M\frac{G}{H}\right) A_k(M) \right| \leqslant s q^{8s} q^{-3n/2} (\sigma_n)^{k-1} |H|^{-1}, \tag{IV.13}$$

avec

$$A_k(M) = \begin{cases} q^{-2n} \sum\limits_{j=1}^{k} \binom{k}{j} [\sigma_{n-1}]^{k-j} q^{nj} n^{-j} \varrho_j(0) & \text{si} \quad d^\circ M = 2n-1, \\ q^{-2n} \sum\limits_{j=1}^{k} \binom{k}{j} [\sigma_{n-1}]^{k-j} q^{nj} n^{-j} \varrho_j(\operatorname{sgn}(M)) & \text{si} \quad d^\circ M = 2n. \end{cases} \tag{IV.14}$$

Démonstration. Posons

$$J_k(M) = \int_{\mathscr{P}_{N+d^\circ H}} \Psi^k(u)\, E(-Mu)\, du.$$

Les relations (IV.9) et (III.1) nous donnent

$$\left| I_{G/H,k}(M) - \frac{W^k(G,H)}{\Phi^k(H)}\, E\left(-M\,\frac{G}{H}\right) J_k(M) \right| \ll s(\sigma_n)^{k-1}\, q^{4s+(n/2)-N-d^\circ H}.$$

Il suffit donc d'établir l'égalité

$$J_k(M) = A_k(M).$$

D'après (IV.7) et (IV.8),

$$J_k(M) = (\sigma_n)^k \int_{\mathscr{P}_{2n+1}} E(-Mu)\, du + \sum_{j=1+N+d^\circ H}^{2n+1} \sum_{a\in \mathbf{F}_q^0} \varphi^k(a,j)\, E(-MaX^{-j}) \int_{\mathscr{P}_j} E(-Mu)\, du,$$

d'où, avec (III.1),

$$J_k(M) = (\sigma_n)^k q^{-2n-1} + \sum_{j=d^\circ M+1}^{2n+1} q^{-j} \sum_{a\in \mathbf{F}_q^0} \varphi^k(a,j)\, E(-MaX^{-j}).$$

On applique alors la définition du caractère E. Si $d^\circ M = 2n-1$, les relations (IV.7) et (IV.8) nous donnent

$$J_k(M) = (\sigma_n)^k q^{-2n-1} + q^{-2n}(\sigma_{n-1})^k \times \sum_{a\in \mathbf{F}_q^0} e\big(-a\,\mathrm{sgn}(M)\big) + q^{-2n-1} \sum_{a\in \mathbf{F}_q^0} \left(\sigma_{n-1} + \frac{q^n}{n} \sum_{b\in \mathbf{F}_q^0} (ab^2)\right)^k,$$

$$J_k(M) = q^{-2n-1}\left\{(\sigma_n)^k - (\sigma_{n-1})^k + \sum_{j=1}^{k} \binom{k}{j} (\sigma_{n-1})^{k-j} q^{nj} n^{-j} \left[q\varrho_j(0) - (q-1)^j\right]\right\},$$

$$J_k(M) = q^{-2n-1} \sum_{j=1}^{k} \binom{k}{j} (\sigma_{n-1})^{k-j} q^{nj+1} n^{-j} \varrho_j(0),$$

ce qui est l'égalité cherchée. Le cas $d^\circ M = 2n$ se traite de la même façon.

Corollaire. *On a la relation*:

$$\left| \int_{\mathscr{A}} f^k(t)\, E(-Mt)\, dt - A_k(M) \sum_{\substack{H\in\mathscr{U} \\ d^\circ H \leqslant 2s}} \sum_{G\in\mathscr{G}_H^\circ} \frac{W^k(G,H)}{\Phi^k(H)}\, E\left(-M\,\frac{G}{H}\right) \right| \ll sq^{10s} q^{-3n/2} (\sigma_n)^{k-1}. \tag{IV.15}$$

V. Les séries singulières. L'estimation précédente fait apparaitre les premiers termes d'une série qui est absolument convergente pour $k \geqslant 5$, série que l'on va étudier dans ce paragraphe.

On pose, M et H étant des polynômes,

$$C_k(M,H) = \sum_{G\in\mathscr{G}_H^\circ} \frac{W^k(G,H)}{\Phi^k(H)}\, E\left(-M\,\frac{G}{H}\right). \tag{V.1}$$

Dans ce qui suit, le polynôme M est supposé fixé.

Proposition V.1. *La fonction $H \mapsto C_k(M,H)$ est multiplicative.*

Démonstration. Immédiate.

Proposition V.2. *Soient P un polynôme irréductible, G un polynôme premier à P et r un entier au moins égal à 2. Alors, on a*

$$W(G,P^r) = 0. \tag{V.2}$$

Démonstration. On a

$$W(G,P^r) = \sum_{R\in\mathscr{G}_{P^{r-1}}^\circ} \sum_{L\in\mathscr{G}_P} E\left(\frac{G}{P^r}\,[P^{r-1}L+R]^2\right) = \sum_{R\in\mathscr{G}_{P^{r-1}}^\circ} E\left(\frac{G}{P^r}\,R^2\right) \sum_{L\in\mathscr{G}_P} E\left(2\,\frac{G}{P}\,LR\right).$$

On conclut avec la relation (III.2).

Proposition V.3. *Soient P un polynôme irréductible et G un polynôme premier à P. Alors, on a*

$$|W(G,P)| \leqslant 1 + |P|^{1/2}. \tag{V.3}$$

Démonstration. (V.3) est une conséquence de la proposition VI.2 de [1]. Si P est un polynôme irréductible, on pose

$$\chi_k(M,P) = 1 + C_k(M,P), \tag{V.4}$$

et on désigne par $\mathscr{N}_k(M,P)$ le nombre de solutions $(M_1,\ldots,M_k)$ de la congruence

$$M \equiv M_1^2 + \ldots + M_k^2 \pmod{P}$$

telles que $M_1,\ldots,M_k$ soient non nuls modulo P.

Proposition V.4. *Soit P un polynôme irréductible. Alors, on a*

$$\Phi(P)^k \chi_k(M,P) = |P|\, \mathscr{N}_k(M,P). \tag{V.5}$$

Démonstration. On a

$$\Phi^k(P)\,C_k(M,P)=\sum_{G\in\mathscr{G}_P^*}\Big\{\sum_{R\in\mathscr{G}_P^*}E\Big(\frac{G}{P}R^2\Big)\Big\}^k E\Big(-M\frac{G}{P}\Big)$$

$$=\sum_{R_1\in\mathscr{G}_P^*}\ldots\sum_{R_k\in\mathscr{G}_P^*}\sum_{G\in\mathscr{G}_P^*}E\Big(\frac{G}{P}[R_1^2+\ldots+R_k^2-M]\Big).$$

La relation (III.2) nous donne alors,

$$\Phi^k(P)\,C_k(M,P)=\Phi(P).A_k(M,P)-\big(\Phi(P)^k-A_k(M,P)\big)$$

$$=|P|.A_k(M,P)-\Phi(P)^k.$$

Les nombres $A_k(M,P)$ nous seront donnés par l'étude des sommes de k carrés d'éléments non nuls dans le corps fini à $|P|$ éléments. Les résultats dont nous avons besoin sont donnés par la proposition suivante.

Proposition V.5. *Soit F_v le corps fini à v éléments. Soit λ le caractère quadratique du groupe multiplicatif F_v^0. Pour tout $a\in F_v$, soit $\theta_k(a)$ le nombre de solutions $(a_1,\ldots,a_k)\in F_v^0\times\ldots\times F_v^0$ de l'équation*

$$a=a_1^2+\ldots+a_k^2.$$

Alors,

(V.6) *pour tout $a\in F_v$, $\theta_k(a)\leqslant 2(v-1)^{k-1}$;*

(V.7) $$\theta_5(0)=v^4-5v^3+5v^2-5v\big(1+2\lambda(-1)\big)+4+10\lambda(-1);$$

(V.8) $$\theta_5(a)=v^4-5v^3+v^2\big(10+\lambda(a)\big)-5v\big(1-2\lambda(-a)\big)+5+10\lambda(-1)+5\lambda(a)\ \text{ si } a\in F_v^0;$$

(V.9) *pour tout $a\in F_v$, pour tout entier $k\geqslant 5$,*

$$\theta_k(a)\geqslant(v-1)^{k-4}\big(v^3-4v^2+v-4-10\lambda(-1)\big).$$

Démonstration. (1) Soit $a\in F_v$. $\theta_1(a)$ vaut 0 ou 2. La relation (V.6) s'établit par récurrence sur l'entier k en remarquant que

(ε) $$\theta_{k+1}(a)=\sum_{b\in F_v^0}\theta_k(a-b^2).$$

(2) Notons $r_k(a)$ le nombre de solutions $(a_1,\ldots,a_k)\in(F_v)^k$ de l'équation

$$a=a_1^2+\ldots+a_k^2.$$

Alors, on a

$$r_k(0)=\theta_k(0)+\binom{k}{1}\theta_{k-1}(0)+\ldots+\binom{k}{k-2}\theta_2(0)+r_1(0),$$

$$r_k(a)=\theta_k(a)+\binom{k}{1}\theta_{k-1}(a)+\ldots+\binom{k}{k-2}\theta_2(a)+\binom{k}{k-1}\theta_1(a),\quad\text{si } a\in F_v^0.$$

On en déduit les relations

$$\theta_k(0)=r_k(0)-\binom{k}{1}r_{k-1}(0)+\ldots+(-1)^{k-2}\binom{k}{k-2}r_2(0)+(-1)^{k-1}\binom{k-1}{k-2}r_1(0),$$

$$\theta_k(a)=r_k(a)-\binom{k}{1}r_{k-1}(a)+\ldots+(-1)^{k-1}\binom{k}{k-1}r_1(a),\quad\text{si } a\in F_v^0.$$

Au chapitre V de [1] on a établi les relations

$$r_{2j}(0)=v^{2j-1}-v^{j-1}\lambda(-1)^j+v^j\lambda(-1)^j,\quad r_{2j+1}(0)=v^{2j},$$

$$r_{2j}(a)=v^{2j-1}-v^{j-1}\lambda(-1)^j,\quad r_{2j+1}(a)=v^{2j}+v^j\lambda(-1)^j\lambda(a),\quad\text{si } a\in F_v^0,$$

valables pour tout entier $j\geqslant 1$.

Les relations (V.7) et (V.8) s'en déduisent.

Les relations (V.7) et (V.8) donnent la minoration

$$\theta_5(a)\geqslant(v-1)\big(v^3-4v^2+v-\big(4+10\lambda(-1)\big)\big)$$

valable pour tout $a\in F_v$. La minoration (V.9) se déduit de l'égalité (ε).

Corollaire. *Soit un entier $k\geqslant 5$ et P un polynôme irréductible. Alors,*

(i) *si $q>3$, ou si $q=3$ et si $d^\circ P>1$,*

(V.10) $$\chi_k(M,P)\geqslant\frac{|P|}{\Phi(P)^4}\,[|P|^3-4|P|^2+|P|-14];$$

(ii) *si $q=3$, si $d^\circ P=1$, et si P ne divise pas M,*

(V.11) $$\chi_k(M,P)\geqslant 3.$$

Démonstration. La relation (V.10) s'obtient à partir des relations (V.5) et (V.9). La relation (V.11) s'obtient à partir des relations (ε), (V.8) et (V.5).

Proposition V.6. *Soient un entier $k\geqslant 1$ et P un polynôme irréductible. Alors, on a*

(V.12) $$|C_k(M,P)|\leqslant\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^k|P|^{(2-k)/2}.$$

Démonstration. Avec les relations (V.1) et (V.3).

Proposition V.7. *Pour $k\geqslant 5$, la série*

(V.13) $$\mathfrak{S}_k(M)=\sum_{H\in\mathscr{H}}C_k(M,H)$$

est absolument convergente, et on a

$$\mathfrak{S}_k(M) = \prod_{P \in \mathscr{U} \cap \mathscr{P}} \chi_k(M, P); \tag{V.14}$$

de plus, pour tout $\varepsilon \in]0, \frac{1}{2}[$, *pour tout entier* $t \geqslant 0$,

$$\sum_{\substack{H \in \mathscr{U} \\ d^\circ H > t}} |C_k(M, H)| \ll q^{t[\varepsilon + 2 - (k/2)]}, \tag{V.15}$$

la constante impliquée par le symbole $\ll$ *ne dépendant que de* q, k *et* ε. *En outre, si* q *n'est pas égal à* 3, *il existe des constantes* $c_1 = c_1(q, k)$, $c_2 = c_2(q, k)$, *strictement positives, ne dépendant que de* q *et de* k, *telles que*

$$c_1 \leqslant \mathfrak{S}_k(M) \leqslant c_2. \tag{V.16}$$

Enfin, si $q = 3$, *la relation ci-dessus reste vraie si le polynôme* M *n'est pas divisible par les polynômes* X, $X+1$, $X-1$.

Démonstration. Si $q = 3$, on fait ici l'hypothèse supplémentaire que le polynôme M n'est divisible par aucun polynôme de degré 1. Soit H un polynôme sans facteur carré. D'après (V.12),

$$|C_k(M, H)| \leqslant \left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^{k\omega(H)} |H|^{1-k/2}.$$

On a alors, pour tout nombre réel $\varepsilon > 0$,

$$|C_k(M, H)| \ll |H|^{\varepsilon + 1 - k/2},$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q, k et ε, ainsi que les constantes impliquées par les symboles $\ll$ qui vont suivre. La proposition V.2 nous donne

$$\sum_{\substack{H \in \mathscr{U} \\ d^\circ H = j}} |C_k(M, H)| \leqslant q^{j(\varepsilon + 2 - k/2)}, \quad \text{pour tout } j \geqslant 0.$$

La relation (V.15) s'en déduit. Ceci prouve que la série $\mathfrak{S}_k(M)$ est absolument convergente. La fonction $H \mapsto C_k(M, H)$ étant multiplicative, la somme $\mathfrak{S}_k(M)$ s'écrit comme produit eulérien absolument convergent, d'où, (V.14). Les relations (V.4) et (V.12) nous donnent

$$1 - \left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^k |P|^{1-k/2} \leqslant \chi_k(M, P) \leqslant 1 + \left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^k |P|^{1-k/2}.$$

Le produit

$$\prod_{P \in \mathscr{P} \cap \mathscr{U}} \left(1 + \left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^k |P|^{1-k/2}\right)$$

est convergent. Soit $c_2(q, k)$ ce produit. On a ainsi la deuxième inégalité de (V.16).

Soit

$$d = \frac{2k \log(\sqrt{q}/(\sqrt{q}-1))}{(k-2)\log q}.$$

Si P est un polynôme irréductible tel que $d^\circ P > d$, $\chi_k(M, P) > 0$. Le produit

$$\gamma(q, k) = \prod_{\substack{P \in \mathscr{P} \cap \mathscr{U} \\ d^\circ P > d}} \left(1 - \left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^k |P|^{1-k/2}\right)$$

est convergent et strictement positif. On a

$$\mathfrak{S}_k(M) \geqslant \gamma(q, k) \Big\{ \prod_{\substack{P \in \mathscr{P} \cap \mathscr{U} \\ d^\circ P \leqslant d}} \chi_k(M, P) \Big\}.$$

Si $q \neq 3$, on pose

$$c_1(q, k) = \gamma(q, k) \prod_{\substack{P \in \mathscr{P} \cap \mathscr{U} \\ d^\circ P \leqslant d}} (\Phi(P)^{-4}(|P|^4 - 4|P|^3 + |P|^2 - 14|P|))$$

et la relation (V.10) donne la première inégalité de (V.16). Posons aussi

$$c_1(3, k) = 3^3 \gamma(3, k) \prod_{\substack{P \in \mathscr{P} \cap \mathscr{U} \\ 1 < d^\circ P \leqslant d}} (\Phi(P)^{-4}(|P|^4 - 4|P|^3 + |P|^2 - 14|P|)).$$

La relation (V.11) nous donne alors la première inégalité de (V.16) lorsque $q = 3$.

VI. Estimation de $I_k(M)$. Nous reprenons les hypothèses du paragraphe IV.

Proposition VI.1. *Soit un entier* $j \geqslant 2$. *Alors,*

$$\int_{\mathscr{A}'} |f(t)|^{2j} dt \ll \begin{cases} nq^{2n} & \text{si } j = 2, \\ q^{2n(j-1)} & \text{si } j > 2, \end{cases} \tag{VI.1}$$

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

Démonstration. Posons pour $t \in \mathscr{U}$,

$$g(t) = \sum_{\substack{A \in \mathbf{F}_q[X] \\ d^\circ A \leqslant n}} E(tA^2). \tag{i}$$

L'intégrale

$$\int_{\mathscr{P}} |g(t)|^{2j} dt \quad \text{(resp. } \int_{\mathscr{P}} |f(t)|^{2j} dt)$$

est égale au nombre de solutions $(A_1, \ldots, A_j, B_1, \ldots, B_j)$ en polynômes (resp. en polynômes irréductibles) $A_1, \ldots, A_j, B_1, \ldots, B_j$ de degré au plus n de l'équation

$$A_1^2 + \ldots + A_j^2 = B_1^2 + \ldots + B_j^2.$$

Par suite,

(ii) $$\int_{\mathscr{A}'} |f(t)|^{2j}\,dt \leqslant \int_{\mathscr{P}} |f(t)|^{2j}\,dt \leqslant \int_{\mathscr{P}} |g(t)|^{2j}\,dt.$$

Considérons ici une partition de $\mathscr{P}$ donnée par les arcs de Farey à l'ordre n

$$\mathscr{P} = \bigcup_{\substack{H\in\mathscr{U}\\ d^\circ H\leqslant n\\ G\in\mathscr{C}_H}} \mathscr{A}_{G/H}, \quad \text{avec} \quad \mathscr{A}_{G/H} = \left\{t\in\mathscr{P},\ v\left(t-\frac{G}{H}\right) > n+d^\circ H\right\}.$$

Lorsque t décrit l'arc $\mathscr{A}_{G/H}$, on a

(iii) $$g(t) = |H|^{-1} g\left(t-\frac{G}{H}\right) \sum_{R\in\mathscr{C}_H} E\left(\frac{G}{H}R^2\right).$$

C'est la proposition VIII.2 de [2]. On a aussi, et c'est la proposition V.2 de [1],

(iv) $$\left|\sum_{R\in\mathscr{C}_H} E\left(\frac{G}{H}R^2\right)\right| = |H|^{1/2}.$$

Avec (iii) et (iv) il vient

(v) $$\int_{\mathscr{P}} |g(t)|^{2j}\,dt \leqslant \sum_{\substack{H\in\mathscr{U}\\ d^\circ H\leqslant n}} \Phi(H)|H|^{-j} \int_{\mathscr{P}_{n+d^\circ H}} |g(t)|^{2j}\,dt.$$

On applique la proposition VIII.1 de [2].

$$g(t) = \begin{cases} q^{n+1} & \text{si} \quad v(t) > 2n+1,\\ q^i & \text{si} \quad v(t) = 2i \text{ avec } i\leqslant n,\\ q^i \sum_{b\in\mathbf{F}_q} e(ab^2) & \text{si} \quad v(t) = 2i+1 \text{ avec } i\leqslant n, \text{ et si } a\in\mathbf{F}_q^0\\ & \qquad \text{est tel que } v(t-aX^{-2i-1}) > 2i+1. \end{cases}$$

Si $H\in\mathscr{U}$ est tel que $d^\circ H\leqslant n$,

$$\int_{\mathscr{P}_{n+d^\circ H}} |g(t)|^{2j}\,dt = q^{2n(j-1)+2j-1} + \sum_{r=n+1+d^\circ H}^{2n+1} \int_{\mathscr{P}_{r-1}\setminus\mathscr{P}_r} |g(t)|^{2j}\,dt,$$

$$\int_{\mathscr{P}_{n+d^\circ H}} |g(t)|^{2j}\,dt \leqslant q^{2n(j-1)+2j-1} + \sum_{r=1}^{n} (q-1)(q^{2rj-2r} + q^{2(r+1)j-2r-1}),$$

où i est la partie entière de $(n+1+d^\circ H)/2$, d'où,

$$\int_{\mathscr{P}_{n+d^\circ H}} |g(t)|^{2j}\,dt \ll q^{2n(j-1)},$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de j. (Il en sera de même pour tous les autres symboles $\ll$ utilisés au cours de cette démonstration.) De (v) on déduit alors que

$$\int_{\mathscr{P}} |g(t)|^{2j}\,dt \ll q^{2n(j-1)} \sum_{\substack{H\in\mathscr{U}\\ d^\circ H\leqslant n}} \Phi(H)|H|^{-j} \ll q^{2n(j-1)} \sum_{r=0}^{n} q^{r(2-j)}.$$

On conclut alors avec (ii).

COROLLAIRE. *Soit un entier $j\geqslant 3$. Alors, on a*

(VI.2) $$\int_{\mathscr{A}'} |f(t)|^{2j+1}\,dt \ll ns^{5/2}\log(n)\,q^{n(2j-1)-s/8},$$

(VI.3) $$\int_{\mathscr{A}'} |f(t)|^{2j+2}\,dt \ll n^2 s^5 \log(n)^2 q^{2jn-s/4},$$

les constantes impliquées par les symboles $\ll$ ne dépendant que de q et de j. On a aussi,

(VI.4) $$\int_{\mathscr{A}'} |f(t)|^{5}\,dt \ll n^2 s^{5/2}\log(n)\,q^{3n-s/8},$$

(VI.5) $$\int_{\mathscr{A}'} |f(t)|^{6}\,dt \ll n^3 s^5 \log(n)^2 q^{4n-s/4}.$$

Démonstration. Avec la relation (IV.11).

LEMME. *On a les majorations*

(VI.6) $$n^{-k} q^{n(k-2)} \ll A_k(M) \ll n^{-k} q^{n(k-2)}.$$

Démonstration. Les relations (IV.14) et (V.6) nous donnent

$$A_k(M) \leqslant q^{-2n} \sum_{j=1}^{k} \binom{k}{j} (\sigma_{n-1})^{k-j} n^{-j} q^{nj} (2(q-1)^{j-1}) \leqslant 2(q-1)^{-1} q^{-2n} (\sigma_n)^k.$$

Avec la relation (IV.6) on voit aisément que

$$\sigma_n \ll n^{-1} q^n,$$

d'où la deuxième relation.

Les relations (V.9) et (IV.14) nous donnent, pour $q\neq 3$,

$$A_k(M) \geqslant q^{-2n} n^{-k} q^{nk} (q-1)^{k-4} (q^3 - 4q^2 + q - 14).$$

Si $q=3$, on a en particulier,

$$\varrho_3(0) = 2^3, \quad \varrho_4(1) = 2^4, \quad \varrho_5(-1) = 2^5.$$

La relation (IV.14) nous donne

$$A_k(M) \geqslant 2^{3-2n}\binom{k}{3}(2^{n-1}/n)^{k-3}\,n^{-3}\,2^{3n} \quad \text{si} \quad d^\circ M = 2n-1,$$

$$A_k(M) \geqslant 2^{4-2n}\binom{k}{4}(2^{n-1}/n)^{k-4}\,n^{-4}\,2^{4n} \quad \text{si} \quad d^\circ M = 2n \text{ et si } \operatorname{sgn} M = 1,$$

$$A_k(M) \geqslant 2^{5-2n}\binom{k}{5}(2^{n-1}/n)^{k-5}\,n^{-5}\,2^{5n} \quad \text{si} \quad d^\circ M = 2n \text{ et si } \operatorname{sgn} M = -1.$$

PROPOSITION VI.2. *On a les majorations*

$$|I_5(M) - A_5(M)\,\mathfrak{S}_5(M)| \ll A_5(M)\,n^7\,s^{5/2}\log(s)\,q^{-s/8}, \tag{VI.7}$$

$$|I_6(M) - A_6(M)\,\mathfrak{S}_6(M)| \ll A_6(M)\,n^9\,s^5\log(s)^2\,q^{-s/4}, \tag{VI.8}$$

$$|I_k(M) - A_k(M)\,\mathfrak{S}_k(M)| \ll A_k(M)\,n^{k+1}\,s^{5/2}\log(s)\,q^{-s/8}, \tag{VI.9}$$

pour $k \geqslant 7$, *impair*,

$$|I_k(M) - A_k(M)\,\mathfrak{S}_k(M)| \ll A_k(M)\,n^{k+2}\,s^5\log(s)^2\,q^{-s/4}, \tag{VI.10}$$

pour $k \geqslant 8$, *pair*.

Démonstration. Soit un entier $k \geqslant 5$. Soit $\varepsilon \in]0, \frac{1}{2}[$. Alors, d'après (IV.15), (V.15) et (VI.6),

$$|I_k(M) - A_k(M)\,\mathfrak{S}_k(M)| \ll A_k(M)\,q^{2s(\varepsilon+2-k/2)} + sq^{10s-(3n/2)}(\sigma_n)^{k-1} + \int_{\mathscr{A}'} |f(t)|^k\,dt.$$

Les relations (VI.2), (VI.3), (VI.4), (VI.5) et (VI.6) donnent alors le résultat annoncé.

Nous pouvons énoncer le théorème final.

THÉORÈME. *Soit un entier* $k \geqslant 5$. *Alors, pour tout nombre réel* $\alpha > 0$, *pour tout polynôme* M *non constant, on a*

$$I_k(M) = A_k(M)\,\mathfrak{S}_k(M) + O\big(A_k(M)(d^\circ M)^{-\alpha}\big),$$

les constantes impliquées par le symbole O *ne dépendant que de* q, k *et* α.

Démonstration. On choisit h en fonction de k et de α. Pour

$k = 5$	on prend	$h = 8\alpha + 57$,
$k = 6$	on prend	$h = 4\alpha + 37$,
k impair $\geqslant 7$	on prend	$h = 8\alpha + 8k + 9$,
k pair $\geqslant 8$	on prend	$h = 4\alpha + 4k + 9$.

Soit alors $n(q, k, \alpha)$ le plus petit entier n vérifiant (IV.1). Soit un entier $n \geqslant n(q, k, \alpha)$. On applique la proposition précédente à tout polynôme M de degré $2n$ ou $2n-1$.

On déduit du théorème que, pour tout polynôme M de degré "assez grand", le nombre $I_k(M)$ de représentations restreintes de M en somme de k carrés de polynômes irréductibles est strictement positif. Notons qu'énoncé ainsi, ce résultat pouvait être obtenu à partir de la seule estimation de $I_5(M)$. En effet, d'après les relations (V.16) et (VI.6), pour tout polynôme M de degré $2n$ ou $2n-1$,

$$I_5(M) \gg n^{-5}\,q^{3n}.$$

Soit un entier $k \geqslant 5$. Si M est de degré $2n$ ou $2n-1$,

$$I_k(M) \geqslant \sum_{\substack{P_1 \in \mathscr{P} \\ d^\circ P_1 < n}} \cdots \sum_{\substack{P_{k-5} \in \mathscr{P} \\ d^\circ P_{k-5} < n}} I_5(M - P_1^2 - \ldots - P_{k-5}^2),$$

et, d'après le lemme 20 de [11],

$$I_k(M) \gg n^{-k}\,q^{n(k-2)}.$$

References

[1] M. Car, *Sommes de carrés dans* $F_q[X]$, Dissertationes Mathematicae 215, Warszawa 1983.

[2] — *Sommes de carrés et d'irréductibles dans* $F_q[X]$, Ann. Fac. Sci. Toulouse Math. 3 (1981), p. 129–166.

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

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

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

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

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

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

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

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

[11] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Mathematicae 95, Warszawa 1972.

[12] J. P. Serre, Communication personnelle.

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

Reçu le 5. 10. 1982 (1322)