ROGER DESCOMBES

Partitions en trois polynômes irréductibles sur un corps fini

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, nº 2 (1966-1967), exp. nº 12, p. 1-10

<http://www.numdam.org/item?id=SDPP_1966-1967__8_2_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
8e année, 1966/67, n° 12

13 février 1967

PARTITIONS EN TROIS POLYNÔMES IRRÉDUCTIBLES SUR UN CORPS FINI

par Roger DESCOMBES

1. Introduction.

Avant d'être établi par VINOGRADOV, le théorème sur les partitions des entiers impairs en trois nombres premiers a été l'objet de la part de HARDY et LITTLEWOOD de travaux d'approche plus simples, mais fondés sur une forme affaiblie de l'hypothèse de Riemann qui demeure conjecturale. L'établissement par A. WEIL de l'hypothèse de Riemann, pour les corps de fractions rationnelles sur les corps finis, autorise l'espoir d'un succès par la méthode de HARDY et LITTLEWOOD dans l'attaque des problèmes de partitions en éléments irréductibles dans l'anneau $F_q[X]$ des polynômes à une variable sur le corps fini F_q à q éléments. C'est ce succès que D. R. HAYES annonce pour un mémoire à paraître [4], où il promet de démontrer, pour des sommes de valeurs des caractères multiplicatifs sur $F_q[X]$, une majoration convenable, fondée sur la place des zéros des séries L associées à ces caractères. En admettant cette majoration, le présent exposé a pour but de présenter une adaptation, due à HAYES [3], de la méthode de HARDY et LITTLEWOOD au cas où $F_q[X]$ remplace $\mathbb{Z}$.

2. Position du problème.

Alors que, dans le cas de $\mathbb{Z}$, l'unité -1 est empêchée d'intervenir par la considération de sommes de nombres premiers, à l'exclusion des différences, le remplacement d'un élément irréductible de $F_q[X]$ par un de ses associés peut être interdit de diverses façons dans le dénombrement des partitions d'un élément N de $F_q[X]$ en trois éléments irréductibles. Suivant HAYES, nous imposerons à N d'être unitaire, et nous exigerons que les polynômes irréductibles αP , $\alpha' P'$, $\alpha'' P''$ de somme N aient tous le même degré r que N , avec des coefficients du degré r égaux à α , α' , α'' , fixés indépendamment de N dans F_q , non nuls, et tels que $\alpha + \alpha' + \alpha'' = 1$.

Le problème consiste alors à prouver que

$$\nu(N) = \sum_{\substack{P,P',P'' \\ \alpha P+\alpha' P'+\alpha'' P''=N}} 1 \qquad (P , P' , P'' \text{ irréductibles et unitaires})$$

n'est pas nul lorsque N est "assez grand". On y parvient par une évaluation asymptotique de $\nu(N)$, lorsque la "grandeur" de N augmente indéfiniment. Cette grandeur est mesurée par

$$\|N\| = q^r = q^{-v(N)} ,$$

c'est-à-dire par la valeur absolue sur $F_q(X)$ associée à la valuation à l'infini v , discrète et définie par

$$v(t) = \text{degré de } B - \text{degré de } A , \qquad \text{pour tout} \quad t = A/B \in F_q(X) ,$$

où A et B appartiennent à $F_q[X]$.

3. Enoncé des résultats.

THÉORÈME. - Avec les notations précédentes, on a

$$(1) \qquad \nu(N) = \frac{\|N\|^2}{\log_q^3\|N\|} \left[\prod_P \left(1 + \frac{1}{(\|P\| - 1)^3}\right) \prod_{P|N} \left(1 - \frac{1}{\|P\|^2 - 3\|P\| + 3}\right) + o(1)\right] ,$$

où le produit $\prod_P$ est étendu à tous les polynômes irréductibles unitaires de $F_q[X]$, et le produit $\prod_{P|N}$ à ceux d'entre eux qui divisent N .

Dans le second membre, le premier facteur, égal à q^{2r}/r^3 , tend vers $+\infty$ avec $\|N\|$, c'est-à-dire aussi bien avec q qu'avec r . C'est aussi dans ces circonstances que la notation $o(1)$ prend son sens ; de façon plus précise, le terme $\frac{q^{2r}}{r^3}\, o(1)$ est majoré en valeur absolue par $24q^{(7r+1)/4}$, pourvu que q soit différent de 2 . Le produit infini $\prod_P$ est convergent, parce que le nombre des polynômes irréductibles unitaires de degré r dans $F_q[X]$ est évidemment majoré par q^r , et que la série $\sum_r q^r(q^r - 1)^{-3}$ est convergente.

Le produit fini $\prod_{P|N}$ est non nul, si aucun de ses termes n'est nul, c'est-à-dire si aucun des polynômes P qui y interviennent n'est tel que $\|P\| = 2$. Or, cette dernière égalité n'est réalisée que pour les polynômes X et $X + 1$, avec $q = 2$; la suppression de tels facteurs pour N est analogue à l'élimination des entiers pairs dans le théorème classique de Vinogradov. D'ailleurs, dans $F_2[X]$, le seul choix possible pour α , α' et α'' est celui où $\alpha = \alpha' = \alpha'' = 1$; pour tout $r \geqslant 2$, les polynômes X^r et $(X + 1)^r$, qui admettent respectivement les racines 0 et 1 , ne peuvent être la somme de trois polynômes irréductibles P , P' et P'' de degré r , puisque cette somme prend la valeur $1 + 1 + 1 = 1$ quand on y substitue 0 ou 1 à la variable.

Pour simplifier quelques calculs, nous supposerons désormais $q \geqslant 3$. On vérifie alors aisément que, dans (1), le produit $\prod_{P|N}$, qui minore $\prod_{P} \times \prod_{P|N}$, est lui-même minoré par un nombre strictement positif indépendant de q et de r . Donc $\nu(N)$ dépasse 1 , et même tout entier, lorsque q ou r sont assez grands.

4. La série singulière.

Comme dans l'étude classique de HARDY et LITTLEWOOD (cf. [5], 5 ter Teil), on démontre le théorème en introduisant les produits du second membre de (1) par une famille sommable dite "série singulière", construite à l'aide des fonctions μ , φ et δ_H .

μ désigne la fonction de Möbius, égale, pour $H \in F_q[X]$, à $(-1)^k$ si H a k facteurs irréductibles tous distincts, à 0 si H a un facteur carré non constant, et à 1 si H est constant non nul.

φ est l'indicateur d'Euler,

$$\varphi(H) = \|H\| \prod_{P|H} \left(1 - \frac{1}{\|P\|}\right) , \qquad \text{avec } \varphi(1) = 1 .$$

δ_H est la somme de Ramanujan ;

$$\delta_H(N) = \sum_{D|(H,N)} \|D\| \, \mu(H/D) ,$$

où la sommation est étendue aux diviseurs unitaires D du p. g. c. d. (H , N) des polynômes H et N de $F_q[X]$.

PROPOSITION 1. - Lorsque H parcourt l'ensemble des polynômes unitaires de $F_q[X]$, la famille de terme général $\mu(H) \varphi^{-3}(H) \delta_H(N)$ est absolument sommable. Sa somme, notée $\sigma(N)$, vaut

$$\sigma(N) = \prod_P \left(1 + \frac{1}{(\|P\| - 1)^3}\right) \prod_{P|N} \left(1 - \frac{1}{\|P\|^2 - 3\|P\| + 3}\right) .$$

Preuve. - Si H_1 et H_2 sont sans facteur carré et sans facteur commun, on vérifie que $\delta_{H_1}(N) \, \delta_{H_2}(N) = \delta_{H_1 H_2}(N)$. Comme, pour $H = P$ irréductible, $\delta_P(N)$ vaut $\|P\| - 1$ ou -1 , selon que P divise N ou non, d'où $|\delta_P(N)| \leqslant \varphi(P)$, on a, pour tout H unitaire,

$$|\delta_H(N) \, \mu(H)| \leqslant \varphi(H) .$$

L'absolue sommabilité de la famille $(\mu(H) \, \varphi^{-3}(H) \, \delta_H(N))_H$ découle donc de celle de la famille $(\varphi^{-2}(H))_H$. Or, pour $q \geqslant 3$, le calcul de $\varphi(H)$ pour H irréductible, puis H quelconque, montre que $\varphi(H) \geqslant \sqrt{\|H\|}$. D'autre part, si h est le degré de H,

$$\varphi^{-1}(H) = q^{-h} \prod_{P|H} \left(1 - \frac{1}{\|P\|}\right)^{-1} \leqslant q^{-h} \prod_{P|H} 2 \quad ,$$

où le dernier produit, égal au nombre des diviseurs unitaires de H qui sont sans facteur carré, est majoré par le nombre total des diviseurs unitaires de H ; on sait (cf. [1]) que le nombre de tous ces diviseurs, pour tous les H de degré h, est égal à $(h+1)q^h$, d'où

$$\sum_{\substack{H \\ \deg H=h}} \varphi^{-1}(H) \leqslant h+1 \qquad \text{et} \qquad \sum_{\substack{H \\ \deg H=h}} \varphi^{-2}(H) \leqslant (h+1)q^{-h/2} \quad ,$$

ce qui établit la sommabilité de la famille $(\varphi^{-2}(H))_H$.

D'autre part, la fonction $H \longmapsto \mu(H)\, \varphi^{-3}(H)\, \delta_H(N)$ est multiplicative pour les couples de polynômes H_1, H_2 sans facteur carré et sans facteur commun, et nulle pour les H ayant un facteur carré. Par suite,

$$\sigma(N) = \prod_P \left(1 + \frac{\mu(P)\ \delta_P(N)}{\varphi^3(P)}\right) \quad ,$$

où le produit est étendu à tous les polynômes P irréductibles et unitaires. Le remplacement de $\mu(P)$, $\delta_P(N)$ et $\varphi(P)$ par leurs valeurs permet d'achever la preuve par un calcul facile.

5. Le caractère λ et la mesure de Haar.

Tout revient donc à évaluer $\nu(N)$ à l'aide de la famille sommable de la proposition 1. Dans ce but, on cherche d'abord à exprimer $\nu(N)$ par une intégrale pour la mesure de Haar ρ sur le groupe additif compact $\mathfrak{M}$, constitué par l'idéal de la valuation v, dans le complété $\widehat{F_q(X)}$ de $F_q(X)$ pour v. On introduit sur $\widehat{F_q(X)}$ (en tant que groupe additif) un caractère λ à valeurs complexes de module 1, défini comme suit à partir d'un caractère λ^* non principal du groupe additif F_q :

Pour tout $t \in \widehat{F_q(X)}$, $\lambda(t)$ est égal à la valeur $\lambda^*(\alpha_1)$ du caractère λ^*, pour le coefficient $\alpha_1 \in F_q$ du terme en X^{-1}, dans le développement "de Laurent" de t suivant les puissances croissantes de X^{-1}.

Ce développement commence au degré $v(t)$; bien entendu, si $v(t) > 1$, on choisit $\lambda(t) = \lambda^*(0) = 1$. En normalisant ρ par $\rho(\mathfrak{M}) = 1$, et en utilisant son invariance, on établit alors aisément le lemme suivant.

LEMME 1. - *Pour tout* $a \in \widehat{F_q(X)}$,

$$\int_{\mathfrak{M}} \lambda(at)\, d\rho(t) = \begin{cases} 1 & \text{si} \quad a \in \mathfrak{M} \quad (\text{c'est-à-dire, si} \quad v(a) > 0\ ) , \\ 0 & \text{sinon} . \end{cases}$$

Par suite, avec les notations du § 2 :

$$\int_{\mathfrak{M}} \lambda[(\alpha P + \alpha' P' + \alpha'' P'' - N)t]\, d\rho(t) = \begin{cases} 1 & \text{si} \quad N = \alpha P + \alpha' P' + \alpha'' P'' , \\ 0 & \text{sinon} , \end{cases}$$

d'où la proposition ci-dessous.

PROPOSITION 2. - *Soit* f *l'application de* $\widehat{F_q(X)}$ *dans le plan complexe définie par*

$$f(t) = \sum_P \lambda(Pt) \quad ,$$

où la sommation est étendue aux polynômes irréductibles unitaires de degré r *égal à celui de* N . *On a*

$$\nu(N) = \int_{\mathfrak{M}} f(\alpha t)\, f(\alpha' t)\, f(\alpha'' t)\, \lambda(-\,Nt)\, d\rho(t) \quad .$$

6. Partition de $\mathfrak{M}$ et relations $\mathcal{R}_H$.

Pour éviter la difficulté d'un recensement précis des polynômes irréductibles P qui interviennent dans la définition de f , HAYES remplace f par diverses approximations, chacune valable sur un ensemble d'une partition de $\mathfrak{M}$ définie de la façon suivante, et où les fractions " r-primordiales" remplacent celles d'une suite de Farey dans la méthode de HARDY et LITTLEWOOD.

Pour r entier > 0 fixé (égal au degré de N), une fraction $G/H \in F_q(X)$ est dite r-primordiale si, et seulement si, H est unitaire avec

$$0 \leqslant \deg H = h \leqslant \frac{r}{2} \quad \text{et} \quad \begin{cases} \deg G < \deg H \quad \text{et} \quad (G\ ,\ H) = 1 \quad \text{si} \quad \deg H > 0 , \\ G = 0 \quad \text{si} \quad H = 1 . \end{cases}$$

A toute fraction G/H r-primordiale, et à tout polynôme H unitaire de degré au plus égal à $[\frac{r}{2}]$ (partie entière de $\frac{r}{2}$), on associe respectivement les ensembles

$$\mathcal{V}_{G/H} = \{t \in \mathfrak{M} \mid \ v(t - G/H) > h + [\tfrac{r}{2}]\}$$

et

$$\mathcal{W}_H = \bigcup_G \mathcal{V}_{G/H} \quad ,$$

où $\bigcup_G$ est étendue aux G tels que G/H soit r-primordiale.

On établit facilement que deux boules ouvertes $\mathcal{V}_{G/H}$ d'indices différents ne vérifient pas de relation d'inclusion ; elles sont donc disjointes dans l'espace ultramétrique $\mathfrak{M}$. D'autre part, les boules $\mathcal{V}_{G/H}$ sont aussi fermées et de mesure $q^{-h-[r/2]}$; on en déduit que le complémentaire de leur réunion est ouvert et de mesure nulle, donc vide. Ainsi :

LEMME 2. - <u>Pour tout</u> r <u>fixé, les familles</u> $(\mathcal{V}_{G/H})$ <u>et</u> $(\mathcal{W}_H)$ <u>forment chacune une partition ouverte de</u> $\mathfrak{M}$.

Posons $s = r - [\frac{r}{2}] - h$, et notons $\mathcal{R}_H$ la relation $A \sim B$ entre polynômes unitaires de $F_q[X]$ définie par les deux conditions :

(i) H divise $A - B$;

(ii) Les $s + 1$ premiers coefficients de A coïncident avec les $s + 1$ premiers coefficients de B [dans les développements en série "de Laurent" en X^{-1} dans $\widehat{F_q(X)}$].

Avec ces notations, HAYES ([2], [3]) établit les lemmes suivants :

LEMME 3. - $\mathcal{R}_H$ <u>est une relation d'équivalence compatible avec la multiplication des polynômes ; les polynômes unitaires irréductibles de degré</u> r <u>sont tous inversibles modulo</u> $\mathcal{R}_H$.

LEMME 4. - <u>Si</u> A <u>et</u> B <u>sont unitaires de degré</u> r , <u>et congrus modulo</u> $\mathcal{R}_H$, <u>et si</u> $t \in \mathcal{W}_H$, <u>on a</u> $\lambda(At) = \lambda(Bt)$.

7. Estimation de f sur $\mathcal{W}_H$.

Dans tout ce paragraphe, r et H sont fixés, avec les conditions qui précèdent, ainsi, par suite, que $\mathcal{R}_H$ et aussi $\mathcal{W}_H$, auquel t est supposé appartenir. Les sommations notées $\sum_A$ (ou $\sum_B$) sont calculées lorsque A (ou B) décrit un système fixé de représentants unitaires de toutes les classes inversibles modulo $\mathcal{R}_H$; les sommations $\sum_P$ (resp. $\sum_{P \sim A}$) sont calculées lorsque P décrit l'ensemble des polynômes irréductibles unitaires de degré r (reps. ceux d'entre eux qui sont congrus à A modulo $\mathcal{R}_H$) ; les sommations $\sum_{\chi}$ (resp. $\sum_{\chi \neq \chi_0}$) sont calculées lorsque χ décrit l'ensemble de tous les caractères modulo $\mathcal{R}_H$ (resp. ceux d'entre eux qui sont non-principaux) définis sur le groupe multiplicatif des polynômes unitaires de $F_q[X]$ inversibles modulo $\mathcal{R}_H$.

Avec ces conventions, la définition de f et les lemmes 3 et 4 donnent

$$f(t) = \sum_{A} \Big(\sum_{P \sim A} \lambda(Pt) \Big) = \sum_{A} \Big[\lambda(At) \sum_{P \sim A} 1 \Big] .$$

Or il existe $q^s\,\varphi(H)$ classes modulo $\mathcal{R}_H$. Un résultat classique de dualité dans les groupes abéliens finis permet donc d'écrire

$$\sum_{\chi} \bar{\chi}(A)\, \chi(P) = \begin{cases} q^s\, \varphi(H) & \text{si } P \sim A , \\ 0 & \text{sinon ,} \end{cases}$$

d'où

$$f(t) = \sum_{A} \Big(\lambda(At) \sum_{P} \Big[\frac{1}{q^s\, \varphi(H)} \sum_{\chi} \bar{\chi}(A)\, \chi(P) \Big] \Big)$$

$$= \frac{1}{q^s\, \varphi(H)} \sum_{A} \lambda(At) \sum_{P} 1 + \frac{1}{q^s\, \varphi(H)} \sum_{\chi \neq \chi_0} \Big[\Big(\sum_{A} \bar{\chi}(A)\, \lambda(At) \Big) . \sum_{P} \chi(P) \Big] .$$

Dans le premier terme du dernier membre d'égalité, le facteur $\sum_{P} 1$ est de l'ordre de q^r/r ; plus précisément, on sait que

$$\Big| \sum_{P} 1 - \frac{q^r}{r} \Big| \leqslant q^{r/2} . \tag{2}$$

Dans le second terme, HAYES annonce [4] une majoration pour le facteur $\sum_{P} \chi(P)$ du type

$$\Big| \sum_{P} \chi(P) \Big| \leqslant q^{r/2} . \tag{3}$$

C'est cette différence d'ordre de grandeur qui justifie la séparation du caractère principal χ_0 des autres caractères χ.

D'autre part,

$$\sum_{\chi \neq \chi_0} \Big| \sum_{A} \bar{\chi}(A)\, \lambda(At) \Big| \leqslant \sum_{\chi} \Big| \sum_{A} \bar{\chi}(A)\, \lambda(At) \Big| \tag{4}$$

$$\leqslant \Big(\sum_{\chi} 1 \Big)^{1/2} \Big(\sum_{\chi} \Big| \sum_{A} \bar{\chi}(A)\, \lambda(At) \Big|^2 \Big)^{1/2}$$

$$= q^{s/2} \sqrt{\varphi(H)}\, \Big[\sum_{\chi} \Big(\sum_{A} \bar{\chi}(A)\, \lambda(At) \Big) \Big(\sum_{B} \chi(B)\, \lambda(-Bt) \Big) \Big]^{1/2}$$

$$= q^{s/2} \sqrt{\varphi(H)}\, \Big[\sum_{A} \sum_{B} \lambda(A - B)t . \sum_{\chi} \bar{\chi}(A)\, \chi(B) \Big]^{1/2} .$$

Comme $\sum_{\chi} \bar{\chi}(A)\, \chi(B)$ est nul pour A non congru à B modulo $\mathcal{R}_H$, c'est-à-dire, d'après le choix de A et B, pour $A \neq B$, le dernier membre de (4) est égal à

$$q^{s/2}\sqrt{\varphi(H)}\ [\sum_A 1.q^s\ \varphi(H)]^{1/2} = [q^s\ \varphi(H)]^{3/2}\ .$$

En tenant compte de (2) et (3), on peut donc énoncer la proposition suivante.

PROPOSITION 3. - Pour tout $t \in \mathscr{W}_H$, on a

$$|f(t) - \frac{q^r}{r}\frac{1}{q^s\ \varphi(H)}\sum_A \lambda(At)| \leqslant 2q^{(3r+1)/4}\ ,$$

où A décrit un système de représentants unitaires de toutes les classes inversibles modulo $\mathcal{R}_H$.

8. Indications sur l'achèvement des calculs.

La somme $\sum_A \lambda(At)$ de la proposition 3 est exploitée à l'aide des lemmes suivants.

LEMME 5. - Si C décrit un système de représentants de toutes les classes modulo H dans $F_q[X]$, on a

$$\sum_C \lambda(CN/H) = \begin{cases} \|H\| & \text{si } H|N\ , \\ 0 & \text{sinon}\ . \end{cases}$$

LEMME 6. - Si G décrit un système de représentants de toutes les classes modulo H inversibles dans $F_q[X]$, on a

$$\sum_G \lambda(GN/H) = \delta_H(N)\ .$$

LEMME 7. - Avec les notations du paragraphe 7, si α est non nul dans F_q, et si t appartient à $\mathscr{V}_{G/H}$, on a

$$\sum_A \lambda(\alpha At) = \begin{cases} \mu(H)q^s\ \lambda[\alpha X^r(t - G/H)] & \text{si } v(t - G/H) > r\ , \\ 0 & \text{sinon}\ . \end{cases}$$

Le lemme 5 s'établit en utilisant comme système de représentants C mod H, l'ensemble de tous les polynômes unitaires de même degré que H, ce qui donne à

$$\gamma_H(N) = \sum_C \lambda(CN/H)$$

la même valeur que tout autre système de représentants, et permet de calculer cette valeur. Le lemme 6 se déduit du lemme 5 en remarquant que la définition de $\delta_H(N)$ n'est autre que l'application de la formule d'inversion de Möbius à l'égalité

$$\gamma_H(N) = \sum_{D|H} \delta_D(N) \quad .$$

Enfin, la preuve du lemme 7 utilise le lemme 6 et un système de représentants A des classes inversibles modulo $\mathcal{R}_H$ de la forme $A = X^{[r/2]} HB + G$, où G décrit l'ensemble des polynômes de degré inférieur à celui h de H et premiers avec H (fractions G/H r-primordiales), et B l'ensemble des polynômes unitaires de degré $s = r - [\frac{r}{2}] - h$.

En posant, pour l'ensemble des polynômes A de la proposition 3

$$g(t) = \frac{q^r}{r} \frac{1}{q^s \varphi(H)} \sum_A \lambda(At) \quad ,$$

le lemme 7 prouve que, si $t \in \mathcal{V}_{G/H}$,

$$g(\alpha t)\ g(\alpha' t)\ g(\alpha'' t) = \begin{cases} \dfrac{q^{3r}}{r^3} \times \dfrac{\mu^3(H)}{\varphi^3(H)}\ \lambda[X^r(t - G/H)] & \text{si} \quad v(t - G/H) > r \ , \\ 0 \quad \text{sinon} \ . \end{cases}$$

En utilisant le lemme 2 et l'invariance de la mesure ρ , on trouve

$$\sum_H \sum_G \int_{\mathcal{V}_{G/H}} g(\alpha t)\ g(\alpha' t)\ g(\alpha'' t)\ \lambda(-Nt)\ d\rho(t) = \frac{q^{2r}}{r^3} \sum_H \Big[\frac{\mu(H)}{\varphi^3(H)} \sum_G \lambda(-GN/H)\Big] \quad ,$$

où les sommations sont étendues aux fractions G/H r-primordiales. D'après le lemme 6, le second membre est égal à

$$\frac{q^{2r}}{r^3} \sum_H \frac{\mu(H)}{\varphi^3(H)}\ \delta_H(-N) = \frac{q^{2r}}{r^3} \sum_H \frac{\mu(H)}{\varphi^3(H)}\ \delta_H(N) \quad .$$

Au facteur $\frac{q^{2r}}{r^3}$ près, il s'agit donc d'une somme partielle de la série singulière, contenant exactement les polynômes unitaires H de degré au plus égal à $[\frac{r}{2}]$. En majorant le reste correspondant de la série singulière, et en utilisant la proposition 3, on obtient finalement pour la valeur de $\nu(N)$ fournie par la proposition 2 une estimation à l'aide de $\sigma(N)$ qui, compte tenu de la proposition 1, constitue exactement l'objet du théorème énoncé au paragraphe 3.

9. Remarque.

Une méthode analogue mériterait d'être essayée dans le cas où on abandonne l'exigence d'égalité des degrés de N , P , P' et P'' et celle de la fixité de α , α' et α'' , et peut-être aussi dans le cas analogue à celui "de Goldbach" d'une partition en deux et non trois polynômes irréductibles.

BIBLIOGRAPHIE

[1] CARLITZ (Leonard). - The arithmetic of polynomials in a Galois field, Amer. J. of Math., t. 54, 1932, p. 39-50.

[2] HAYES (David R.). - The distribution of irreducibles in GF[q , x] , Trans. Amer. Math. Soc., t. 117, 1965, p. 101-127.

[3] HAYES (David R.). - The expression of a polynomial as a sum of three irreducibles, Acta Arith., Warszawa, t. 11, 1966, p. 461-488.

[4] HAYES (David R.). - A general character sum (à paraître).

[5] LANDAU (Edmund). - Vorlesungen über Zahlentheorie. Band 1, Teil 2. - New York, Chelsea Publishing Company, 1947.