

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

FRANÇOIS DRESS

Fonctions arithmétiques sur l'anneau des polynômes à coefficients dans un corps fini

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 4 (1962-1963), exp. n° 13, p. 1-9

http://www.numdam.org/item?id=SDPP_1962-1963__4__A11_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1962-1963, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

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

FONCTIONS ARITHMÉTIQUES
SUR L'ANNEAU DES POLYNÔMES À COEFFICIENTS DANS UN CORPS FINI

par François DRESS

1. Introduction.

On se donne un corps fini $\mathbb{C}\mathbb{G}(p^n)$, $p^n = q$, et on considère l'anneau des polynômes à une indéterminée X . Soit

$$F(X) = a_0 x^v + a_1 x^{v-1} + \dots + a_{v-1} x + a_v.$$

Deux polynômes F et G sont dits associés si $F = aG$, $a \in \mathbb{C}\mathbb{G}(p^n)$. Si $a_0 = 1$, F est dit unitaire. Dans toute la suite de cet exposé, il ne sera considéré que des polynômes unitaires.

Si $\partial^0 F = v$, on pose $|F| = q^v$. On peut alors définir une fonction zêta :

$$\zeta(s) = \sum_F \frac{1}{|F|^s} = \sum_{v=0}^{\infty} q^v \frac{1}{q^{vs}} = \frac{1}{1 - q^{1-s}} \quad (s = \sigma + i\tau, \sigma > 1).$$

L'unicité de la décomposition en polynômes irréductibles et l'absolue convergence pour $\sigma > 1$ des séries et produits considérés permet d'obtenir l'égalité fonctionnelle :

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{|p|^s}}$$

le produit infini étant étendu à tous les polynômes irréductibles (unitaires).

2. Fonctions arithmétiques. Valeurs moyennes.

On peut définir dans cet anneau, les fonctions arithmétiques usuelles de la même manière que dans $\mathbb{Z}$. En raison de la constance de la norme pour les polynômes de même degré, et de la forme très simple de la fonction zêta, la sommation à degré constant des fonctions arithmétiques multiplicatives sera aisée.

Fonctions de diviseurs. - $d(F) = \sum_{f|F} 1$ et $\sigma(F) = \sum_{f|F} |f|$. On a

$$\sum_F \frac{d(F)}{|F|^s} = \prod_p \left(1 + \frac{2}{|p|^s} + \frac{3}{|p|^{2s}} + \dots\right) = \prod_p \left(\frac{1}{1 - \frac{1}{|p|^s}}\right)^2 = \zeta^2(s) = \left(\frac{1}{1 - q^{1-s}}\right)^2$$

d'où

$$\sum_{\nu=0}^{\infty} \frac{\sum_{\substack{F \\ d(F)=\nu}} d(F)}{q^{\nu s}} = \sum_{\nu=0}^{\infty} \frac{(\nu+1) q^{\nu}}{q^{\nu s}}$$

et

$$\begin{aligned} \sum_F \frac{\sigma(F)}{|F|^s} &= \prod_p \left(1 + \frac{1+|p|}{|p|^s} + \frac{1+|p|+|p|^2}{|p|^{2s}} + \dots \right) \\ &= \prod_p \left(1 + \frac{1}{|p|^s} + \frac{1}{|p|^{2s}} + \dots \right) \left(1 + \frac{|p|}{|p|^s} + \frac{|p|^2}{|p|^{2s}} + \dots \right) \\ &= \zeta(s) \zeta(s-1) = \frac{1}{(1-q^{1-s})(1-q^{2-s})} = 1 + \frac{q+q^2}{q^s} + \frac{q^2+q^3+q^4}{q^{2s}} + \dots \end{aligned}$$

d'où :

$$\sum_{\nu=0}^{\infty} \frac{\sum_{\substack{F \\ d(F)=\nu}} \sigma(F)}{q^{\nu s}} = \sum_{\nu=0}^{\infty} \frac{q^{\nu}(q^{\nu+1}-1)/q-1}{q^{\nu s}}$$

ce qui donne

$$\sum_{\substack{F \\ d(F)=\nu}} \sigma(F) = \nu+1 \quad \text{et} \quad \sum_{\substack{F \\ d(F)=\nu}} \sigma(F) = \frac{q^{\nu+1}-1}{q-1}.$$

Indicateur d'Euler.

$$\varphi(F) = \sum_{(f,F)=1} 1 = \prod_{\substack{p^k | F \\ p^{k+1} \nmid F}} |p|^k - |p|^{k-1}.$$

On a .

$$\begin{aligned} \sum_F \frac{\varphi(F)}{|F|^s} &= \prod_p \left\{ 1 + (|p|-1) \left(\frac{1}{|p|^s} + \frac{|p|}{|p|^{2s}} + \dots \right) \right\} = \prod_p \left(\frac{1 - \frac{1}{|p|^s}}{1 - \frac{|p|}{|p|^s}} \right) \\ &= \frac{\zeta(s-1)}{\zeta(s)} = \frac{1 - q^{1-s}}{1 - q^{2-s}} \end{aligned}$$

d'où

$$\sum_{\nu=0}^{\infty} \frac{\sum_{\substack{F \\ d(F)=\nu}} \varphi(F)}{q^{\nu s}} = 1 + \sum_{\nu=1}^{\infty} \frac{q^{2\nu} - q^{2\nu-1}}{q^{\nu s}}$$

ce qui donne

$$\sum_{\substack{F \\ d(F) \geq 1}} \varphi(F) = q^{\nu} \left(1 - \frac{1}{q} \right).$$

Fonction de Möbius.

$$\mu(F) = \begin{cases} 1 & \text{si } F = 1 \\ (-1)^{\sum_i 1} & \text{si } F = \prod_i p_i \\ 0 & \text{si } f^2 | F \end{cases}$$

on a

$$\sum_F \frac{\mu(F)}{|F|^s} = \prod_p \left(1 - \frac{1}{|p|^s}\right) = \frac{1}{\zeta(s)} = 1 - q^{1-s}$$

ce qui donne

$$\sum_{\delta^0_{F=v}} \mu(F) = \begin{cases} 1 & \text{si } v = 0 \\ -1 & \text{si } v = 1 \\ 0 & \text{si } v \geq 2 \end{cases}$$

On peut enfin calculer la proportion de polynômes "square-free" par degré :

$$\sum_F \frac{|\mu(F)|}{|F|^s} = \prod_p \left(1 + \frac{1}{|p|^s}\right) = \prod_p \frac{1 - \frac{1}{|p|^{2s}}}{1 - \frac{1}{|p|^s}} = \frac{\zeta(s)}{\zeta(2s)} = \frac{1 - q^{1-2s}}{1 - q^{1-s}}$$

d'où

$$\sum_{v=0}^{\infty} \frac{\sum_{\delta^0_{F=v}} |\mu(F)|}{q^{vs}} = 1 + \frac{q}{q^s} + \sum_{v=2}^{\infty} \frac{q^v - q^{v-1}}{q^{vs}}$$

ce qui donne

$$\sum_{\delta^0_{F=v}} |\mu(F)| = \begin{cases} 1 & \text{si } v = 0 \text{ ou } 1 \\ 1 - \frac{1}{q} & \text{si } v \geq 2 \end{cases}$$

3. Polynômes irréductibles. Nombre par degré.

On désigne par $\pi(v) = \pi_q(v)$ le nombre de polynômes irréductibles (unitaires) de degré v . La fonction zêta donne

$$\frac{1}{1 - q^{1-s}} = \zeta(s) = \prod_p \frac{1}{1 - \frac{1}{|p|^s}} = \prod_{v=1}^{\infty} \left(\frac{1}{1 - \frac{1}{q^{vs}}} \right)^{\pi(v)} \quad (s = \sigma + i\tau, \sigma > 1) ;$$

on prend alors les logarithmes des deux membres, ce qui donne

$$\sum_{\lambda=1}^{\infty} \frac{1}{\lambda q^{\lambda(s-1)}} = \sum_{\lambda=1}^{\infty} \pi(\lambda) \sum_{\mu=1}^{\infty} \frac{1}{\mu q^{\lambda \mu s}}$$

soit, en égalant les coefficients de $\frac{1}{q^{vs}}$,

$$\frac{q^v}{v} = \sum_{\lambda|v} \frac{\lambda \pi(\lambda)}{v}$$

d'où, en utilisant la formule d'inversion de Möbius,

$$v\pi(v) = \sum_{\lambda|v} \mu(v) q^{v/\lambda}$$

résultat qui peut encore s'écrire :

$$\pi(v) = \frac{1}{v} (q^v - \sum_{p_i | v} q^{v/p_i} + \sum_{p_i p_j | v} q^{v/p_i p_j} - \dots) = \frac{1}{v} \{q^v + O(q^{v/2})\} \quad (v \rightarrow \infty) .$$

4. Répartition fine. Premiers résultats de CARLITZ et UCHIYAMA.

On désigne par $\pi(v ; r, t) = \pi_q(v ; r, t)$ le nombre de polynômes irréductibles tels que les r premiers coefficients $(a_1, \dots, a_r)$ et les t derniers $(a_{v-t+1}, \dots, a_v)$ soient fixés.

Le paragraphe précédent montre que

$$\pi(v ; 0, 0) = \frac{1}{v} \{q^v + O(q^{v/2})\} \quad (v \rightarrow \infty) .$$

Un résultat déjà ancien donne des formules exactes [6] pour $\pi(v ; 1, 0)$. Elles sont du même type que celles permettant de calculer $\pi(v)$, mais beaucoup plus compliquées. Elles ne seront pas indiquées ici. Elles peuvent d'ailleurs se résumer en

$$\pi(v ; 1, 0) = \frac{1}{v} \{q^{v-1} + O(q^{v/2})\} \quad (v \rightarrow \infty) .$$

CARLITZ en 1952 ([6]) et UCHIYAMA en 1954 ([7]) ont démontré les formules suivantes :

$$\pi(v ; 1, 1) = \frac{1}{v} \left\{ \frac{q^{v-1}}{q-1} + O(q^{v/2}) \right\} \quad (v \rightarrow \infty)$$

$$\pi(v ; 0, 2) = \frac{1}{v} \left\{ \frac{q^{v-1}}{q-1} + O(q^{v/2}) \right\} \quad (v \rightarrow \infty)$$

valables pour $q = p^n$, p premier impair (la présence du facteur $\frac{q^{v-1}}{q-1}$ et non de q^{v-2} est due au fait que la valeur 0 du dernier coefficient a_v est exclue).

Etude de $\pi(v ; 1, 1)$. Préliminaires. - On définit tout d'abord deux fonctions $\lambda(F)$ et $\chi(F)$, $F = x^v + a_1 x^{v-1} + \dots + a_v$, fonctions qui sont respectivement des caractères additif et multiplicatif sur le corps fini $CG(p^n)$:

Si $t(\alpha)$ désigne la trace absolue de $\alpha \in CG(p^n)$, $t(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{n-1}}$, on définit $E(\alpha) = e^{(2\pi i t(\alpha))/p}$. Ensuite, b étant un élément quelconque de $CG(p^n)$, on pose

$$\begin{cases} \lambda(F) = \lambda_b(F) = E(ba_1) & \text{si } \partial^0 F \geq 1 \\ \lambda(1) = 1 . \end{cases}$$

Si γ désigne une racine primitive de $CG(p^n)$, on peut écrire $\alpha = \gamma^r$, et on définit $X(\alpha) = e^{2\pi i r/q-1}$ ($\alpha \neq 0$), $X(0) = 0$. Ensuite, étant donné c entier, $0 \leq c < q-1$, on pose :

$$\chi(F) = \chi_0(F) = X^c(a_v) .$$

Ces fonctions λ et χ possèdent un certain nombre de propriétés qui serviront pour la suite de la démonstration et qui vont être exposées maintenant.

Comme conséquences directes de la définition, on a :

$$\begin{aligned} (1) \quad & \lambda(AB) = \lambda(A) \lambda(B) \quad \chi(AB) = \chi(A) \chi(B) . \\ (2) \quad & \sum_{\lambda} \lambda(F) = \begin{cases} q & \text{si } a_1 = 0 \\ 0 & \text{si } a_1 \neq 0 \end{cases} \quad \sum_{\chi} \chi(F) = \begin{cases} q-1 & \text{si } a_v = 1 \\ 0 & \text{si } a_v \neq 1 . \end{cases} \\ (3) \quad & \sum_{\substack{F \\ \partial^0 F = v \geq 1 \\ \lambda \neq \lambda_0}} \lambda(F) = 0 \quad \sum_{\substack{F \\ \partial^0 F = v \geq 1 \\ \chi \neq \chi_0}} \chi(F) = 0 . \end{aligned}$$

On étudie enfin la somme

$$\sum_{a \in CG(p^n)} E(ba) X^c(a) \quad (b \neq 0, c \neq 0) .$$

Soit donc

$$\tau = \sum E(ba) X^c(a) = \sum_{a \neq 0} E(ba) X^c(a)$$

puisque $X(0) = 0$

$$\begin{aligned} |\tau|^2 &= \tau \cdot \bar{\tau} = \sum_{a \neq 0} E(ba) X^c(a) \sum_{a' \neq 0} E(-ba') X^c(a'^{-1}) \\ &= \sum_{a \neq 0} \sum_{a' \neq 0} E[b(a - a')] X^c(aa'^{-1}) = \sum_{a'' \neq 0} X^c(a'') \sum_{a' \neq 0} E[ba'(a'' - 1)] \\ &= \sum_{a''=1} + \sum_{a'' \neq 1} = X^c(1) \cdot q + \sum_{a'' \neq 1} X^c(a'') \cdot 0 = q \end{aligned}$$

donc :

$$(4) \quad |\tau| = \sqrt{q} .$$

Démonstration de $\pi(v; 1, 1)$. — On considère la série

$$L(s, \lambda, \chi) = \sum_F \frac{\lambda(F) \chi(F)}{|F|^s} \quad (s = \sigma + i\tau, \sigma > 1)$$

si on pose :

$$\tau_v = \tau_v(\lambda, \chi) = \sum_{\partial^0 F = v} \lambda(F) \chi(F)$$

il vient :

$$L(s, \lambda, \chi) = \sum_{v=0}^{\infty} \frac{\tau_v(\lambda, \chi)}{q^{vs}} .$$

Quatre cas sont alors à considérer :

$$1^\circ \quad \lambda = \lambda_0, \quad \chi = \chi_0$$

$$L(s, \lambda_0, \chi_0) = \sum_{x \in F} \frac{1}{|F|^s} = \frac{1 - q^{-s}}{1 - q^{-1-s}}$$

$$2^\circ \quad \lambda = \lambda_0, \quad \chi \neq \chi_0$$

$$L(s, \lambda_0, \chi) = \sum_F \frac{\chi(F)}{|F|^s} = 1 \quad \text{d'après (3)}$$

$$3^\circ \quad \lambda \neq \lambda_0, \quad \chi = \chi_0$$

$$L(s, \lambda, \chi_0) = \sum_{x \in F} \frac{\lambda(F)}{|F|^s} = 1 - q^{-s} \quad \text{d'après (3)}$$

$$4^\circ \quad \lambda \neq \lambda_0, \quad \chi \neq \chi_0$$

$$L(s, \lambda, \chi) = 1 + \sum_{v=1}^{\infty} \frac{\tau_v(\lambda, \chi)}{|q|^{vs}} \quad \text{si } \tau_v = \sum_{a_1, \dots, a_v} E(ba_1) X^c(a_v)$$

$$\tau_v(\lambda, \chi) = 0 \quad \text{si } v \geq 1$$

$$|\tau_1(\lambda, \chi)| = \sqrt{q} \quad \text{d'après (4)}$$

$$L(s, \lambda, \chi) = 1 + \frac{\tau_1(\lambda, \chi)}{q^s} .$$

Mais on a

$$L(s, \lambda, \chi) = \sum_F \frac{\lambda(F) \chi(F)}{|F|^s} = \prod_p \frac{1}{1 - \frac{\lambda(p) \chi(p)}{|p|^s}}$$

ce qui donne, en prenant le logarithme,

$$\text{Log } L(s, \lambda, \chi) = \sum_p \left\{ \sum_{r=1}^{\infty} \frac{1}{r} \frac{\lambda(p^{rs}) \chi(p^r)}{|p|^{rs}} \right\} .$$

Soient maintenant $\alpha, \beta \in \text{CG}(p^n)$, $\beta \neq 0$. Si on considère la somme

$$\sum_{\lambda, \chi} E(-\alpha) X^{-c}(\beta) \text{Log } L(s, \lambda, \chi)$$

d'après la propriété (2), seuls les termes dont les premier et dernier coefficients sont α et β vont se trouver affectés d'un coefficient non nul lors de la sommation. Soit

$$\sum_{\lambda, \chi} E(-\alpha) X^{-c}(\beta) \text{Log } L(s, \lambda, \chi) = q(q-1) \sum_{(p,r)} \frac{1}{r} \frac{1}{|p|^{rs}}$$

où le signe $\sum_{(p,r)}$ indique que la somme est étendue aux couples (p, r) tels que p^r ait pour premier et dernier coefficients α et β .

Le premier membre va avoir des termes dérivant de :

$$\begin{aligned}
 1^\circ \quad \text{Log } L(s, \lambda_0, \chi_0) &= \sum_{v=1}^{\infty} \frac{1}{v} \left(\frac{1}{q^{v(s-1)}} - \frac{1}{q^{rs}} \right) = \sum_{v=1}^{\infty} \frac{1}{v} \times \frac{q^v - 1}{q^{vs}} \\
 2^\circ \quad \text{Log } L(s, \lambda_0, \chi) &= 0 \\
 3^\circ \quad \text{Log } L(s, \lambda, \chi_0) &= - \sum_{v=1}^{\infty} \frac{1}{v} \frac{1}{q^{vs}} \\
 4^\circ \quad \text{Log } L(s, \lambda, \chi) &= \sum_{v=1}^{\infty} \frac{(-1)^{v-1}}{v} \times \frac{r_1^v(\lambda, \chi)}{q^{vs}} .
 \end{aligned}$$

Quant au second membre, on aura, en désignant par $N(v, r)$ le nombre de p de $\delta^0 v/r$ et tels que p^r ait pour premier et dernier coefficients α et β :

$$\sum_{(p,r)} \frac{1}{r} \frac{1}{|p|^{rs}} = \sum_{v=1}^{\infty} \frac{1}{v} \frac{w_v}{q^{vs}}$$

avec

$$\frac{1}{v} w_v = \sum_{r|v} \frac{1}{r} N(v, r)$$

soit

$$\begin{aligned}
 \frac{1}{v} w_v &= N(v, 1) + \sum_{\substack{r|v \\ r \geq 2}} \frac{1}{r} N(v, r) \\
 &= \pi(v; 1, 1) + O\left(\frac{q^{v/2}}{v}\right) .
 \end{aligned}$$

D'où enfin, en prenant le coefficient de $\frac{1}{q^{vs}}$ dans chaque membre :

$$\begin{aligned}
 \frac{1}{v} \{q^v - 1 - \sum_b E(-b\alpha) + (-1)^{v-1} \sum_{\substack{\lambda \neq \lambda_0 \\ \chi \neq \chi_0}} E(-b\alpha) X^{-c}(\beta) \tau_1^v(\lambda, \chi)\} \\
 = q(q-1) \{\pi(v; 1, 1) + O\left(\frac{q^{v/2}}{v}\right)\} .
 \end{aligned}$$

ce qui, en tenant compte de $|\tau_1| = \sqrt{q}$, soit $|\tau_1^v| = q^{v/2}$, démontre la formule de Carlitz.

On peut remarquer dès maintenant que l'hypothèse de Riemann pour les séries $L(s, \lambda, \chi)$ est vraie d'après $|\tau_1(\lambda, \chi)| = \sqrt{q}$, ce qui entraîne en outre $O(q^{v/2})$ pour la formule.

Démonstration de $\pi(v; 0, 2)$. - Cette démonstration est très semblable à la précédente. Au lieu de définir $\lambda(F)$ et $\chi(F)$, on définit $\tilde{\lambda}(F)$ et $\chi(F)$:

$$\begin{cases} \tilde{\lambda}(F) = \tilde{\lambda}_b(F) = E(b \frac{q^{v-1}}{a_v}) & \text{si } \delta^0 F \geq 1, \quad a_v \neq 0 \\ \tilde{\lambda}(1) = 1 \text{ et } \tilde{\lambda}(F) = 0 & \text{si } a_v = 0 \end{cases} ;$$

et on termine la démonstration en utilisant :

$$L(s, \tilde{\lambda}, \chi) = \sum_F \frac{\tilde{\lambda}(F) \chi(F)}{|F|^s} = \prod_p \frac{1}{1 - \frac{\tilde{\lambda}(p) \chi(p)}{|p|^s}}.$$

On peut faire la même remarque sur l'hypothèse de Riemann pour les séries $L(s, \tilde{\lambda}, \chi)$ et pour $O(q^{v/2})$.

5. Derniers résultats d'UCHIYAMA.

Les résultats précédents peuvent se généraliser, mais on perd $O(q^{v/2})$. En 1955, UCHIYAMA [8], a démontré la formule suivante :

$$\pi(v; r, t) = \frac{1}{v} q^{v-r-t} \left(\frac{q}{q-1} \right)^\varepsilon + O(q^{\theta v}) \quad (v \rightarrow \infty)$$

sous la condition $p > \max(r, t-1)$, θ étant une constante indépendante de q et de v , $\frac{1}{2} \leq \theta < 1$ (ε étant égal à 0 ou 1 suivant que $t=0$ ou $t \geq 1$, cf. début du paragraphe 4).

Pour sa démonstration, UCHIYAMA généralise les caractères sur $CG(p^n)$ employés par CARLITZ et considère des séries du même type $L(s, \lambda^{(r)}, \tilde{\chi}^{(t-1)}, \chi)$ qu'on n'explicitera pas ici.

Hypothèse de Riemann pour les séries $L(s, \lambda, \tilde{\lambda}, \chi)$. — Si cette hypothèse était vérifiée, on aurait $\theta = \frac{1}{2}$. On peut considérer cette hypothèse comme très probable. En effet UCHIYAMA [8] remarque que cette hypothèse permettrait de démontrer la conjecture de MORDELL (1946) légèrement généralisée, à savoir :

$$\left| \sum_{x \in CG(p^n)} e^{2i\pi t \{f(x)\}/p} \right| \leq (v-1) q^{1/2} \quad (v = \partial^0 f).$$

Or cette dernière inégalité a été démontrée par CARLITZ et UCHIYAMA en 1957 [10] à partir de l'hypothèse de Riemann par André WEIL pour les variétés algébriques, sous réserve que f ne soit pas de la forme $g^p = g + u$, $u \in CG(p^n)$ (ce qui est le cas en particulier si $\partial^0 f \leq p-1$).

BIBLIOGRAPHIE

- [1] CARLITZ (Leonard). — The arithmetic of polynomials in a Galois field, Amer. J. of Math., t. 54, 1932, p. 39-70.
(Fonctions arithmétiques. Loi de réciprocité quadratique.)
- [2] CARLITZ (Leonard). — On the representation of a polynomial in a Galois field as the sum of an even number of squares, Trans. Amer. math. Soc., t. 35, 1933, p. 397-410.

- [3] CARLITZ (Leonard). - Some topics in the arithmetic of polynomials, Bull. Amer. math. Soc., t. 48, 1942, p. 679-691.
(Fonctions arithmétiques. Sommes de carrés.)
 - [4] COHEN (Eckford). - Sums of an even number of squares in $GF[p^n, x]$, Duke math. J., t. 14, 1947, p. 251-267.
 - [5] COHEN (Eckford). - Arithmetic functions of polynomials, Proc. Amer. math. Soc., t. 3, 1952, p. 352-358.
(Problème type Goldbach.)
 - [6] CARLITZ (Leonard). - A theorem of Dickson on irreducible polynomials, Proc. Amer. math. Soc., t. 3, 1952, p. 693-700.
 - [7] UCHIYAMA (Saburô). - Sur les polynômes irréductibles dans un corps fini, I., Proc. Japan Acad., Tokyo, t. 30, 1954, p. 523-527.
 - [8] UCHIYAMA (Saburô). - Sur les polynômes irréductibles dans un corps fini, II., Proc. Japan Acad., Tokyo, t. 31, 1955, p. 267-269.
 - [9] UCHIYAMA (Saburô). - Note on the mean value of $V(f)$, I, II et III, Proc. Japan Acad., Tokyo, t. 31, 1955, p. 199-201 et p. 321-323 ; t. 32, 1956, p. 97-98.
($V(f)$ est le nombre de valeurs distinctes prises par un polynôme f .)
 - [10] CARLITZ (L.) et UCHIYAMA (S.). - Bounds for exponential sums, Duke math. J., t. 24, 1957, p. 37-41.
-