ACTA ARITHMETICA
LXXXVIII.2 (1999)

Distribution des polynômes irréductibles dans $\mathbb{F}_q[T]$

par

Mireille Car (Marseille)

I. Introduction. Soit q une puissance d'un nombre premier p et $\mathbb{F}_q$ le corps fini à q éléments. En 1924, Artin [1, pp. 242–246] prouvait pour l'anneau $\mathbb{F}_p[T]$ le théorème suivant, analogue au théorème des nombres premiers dans les progressions arithmétiques.

Théorème I.1. *Soit $Q \in \mathbb{F}_p[T]$ et soit R un polynôme premier à Q. Soit $\pi(n; Q, R)$ le nombre de polynômes irréductibles unitaires de degré n congrus à R modulo Q. Alors*,

$$\pi(n; Q, R) = \frac{p^n}{n\phi(Q)} + O\left(\frac{p^{\theta n}}{n}\right),$$

θ étant une constante < 1.

En 1965, D. R. Hayes [2] introduisait la notion de congruence arithmétique et généralisait le théorème d'Artin de la façon suivante :

Théorème I.2. *Soient un entier $k \geq 1$ et $\mathbf{a} = (a_1, \ldots, a_k)$ une suite de k éléments de $\mathbb{F}_q$. Soit $Q \in \mathbb{F}_q[T]$ et soit R un polynôme premier à Q. Soit, pour $n \geq k$, $\pi(n; \mathbf{a}, Q, R)$ le nombre de polynômes irréductibles unitaires $P \in \mathbb{F}_q[T]$ de degré n congrus à R modulo Q et tels que*

$$\deg(P - T^n - a_1 T^{n-1} - \ldots - a_k T^{n-k}) < n - k.$$

Alors,

$$\pi(n; \mathbf{a}, Q, R) = \frac{q^{n-k}}{n\phi(Q)} + O\left(\frac{q^{\theta n}}{n}\right),$$

θ étant une constante < 1.

En 1972, en faisant appel au théorème de Weil sur la fonction zéta des courbes, G. Rhin [6] améliorait les résultats de D. Hayes de la façon suivante :

Théorème I.3. *Soient un entier k, Q et R des polynômes unitaires de $\mathbb{F}_q[T]$ premiers entre eux. Soit $\pi(n; k, Q, R)$ le nombre de polynômes*

1991 *Mathematics Subject Classification*: Primary 11T55.

irréductibles unitaires P de degré n congrus à R modulo Q et tels que

$$\deg(PT^{\deg(R)} - RT^n) < n + \deg(R) - k.$$

Alors, si $k + \deg(Q) \geq 1$,

$$\left|\pi(n;k,Q,R) - \frac{q^{n-k}}{n\phi(Q)}\right| \leq (k+1+\deg(Q))q^{n/2}.$$

Très récemment, en reprenant des idées se trouvant à la fois dans [2] et dans [6], Hsu [3] améliorait encore ce résultat et établissait le

THÉORÈME I.4. *Les hypothèses et notations étant celles du théorème précédent*,

$$\pi(n;k,Q,R) \leq \frac{q^{n-k}}{n\phi(Q)} + \left(1 - \frac{1}{q^k\phi(Q)}\right)(k-1+\deg(Q))\frac{q^{n/2}}{n},$$

$$\pi(n;k,Q,R) \geq \frac{q^{n-k}}{n\phi(Q)} - \left(\left(1 - \frac{1}{q^k\phi(Q)}\right)(k+3+\deg(Q))\right)\frac{q^{n/2}}{n} - \frac{\deg(Q)}{nq^k\phi(Q)}.$$

Nous nous intéressons ici à une généralisation des résultats contenus dans les théorèmes précédents. Plus précisément, nous nous intéressons aux polynômes irréductibles unitaires P congrus à R modulo Q, ayant mêmes k premiers coefficients que le polynôme R et tels que $\theta(P) = \alpha$, θ étant un caractère modulo un polynôme D fixé, α étant l'une quelconque des valeurs prises par θ. Le nombre de ces polynômes sera noté $\pi(n;k,Q,R,D,\theta,\alpha)$. Nous déduirons de notre étude une estimation des nombres $\pi^+(n;k,Q,R)$, resp. $\pi^-(n;k,Q,R)$, où $\pi^+(n;k,Q,R)$, resp. $\pi^-(n;k,Q,R)$, désigne le nombre de polynômes irréductibles unitaires P de degré n congrus à R modulo Q, ayant mêmes premiers coefficients que le polynôme R, et tels que D soit inversible et carré modulo P, resp. ne soit pas carré modulo P. Nous obtiendrons aussi une estimation des nombres $\pi^+(n;D)$, resp. $\pi^-(n;D)$, de polynômes irréductibles unitaires P de degré n tels que D soit carré, resp. ne soit pas carré modulo D. Une définition plus précise de ces nombres sera donnée dans la suite de ce travail quand nous aurons précisé quelques définitions. En plus de la généralisation proposée, notre travail apporte une petite amélioration du terme d'erreur. Il fait aussi référence aux résultats établis en [2] et [6].

II. Préliminaires. On pose $\mathbb{A} = \mathbb{F}_q[T]$. On désigne par $\mathbb{M}$ l'ensemble des polynômes unitaires de $\mathbb{F}_q[T]$ et par $\mathbb{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[T]$.

Soient $Q \in \mathbb{M}$ et k un entier naturel. Soit $\mathcal{R}_{Q,k}$ la relation d'équivalence sur $\mathbb{M}$ définie par

$$A \equiv B \bmod \mathcal{R}_{Q,k}$$
$$\Leftrightarrow A \equiv B \bmod Q \text{ et } \deg(AT^{\deg(B)} - BT^{\deg(A)}) < \deg(AB) - k.$$

L'équivalence $\mathcal{R}_{Q,0}$ est simplement la congruence modulo Q. On note $\mathcal{R}_Q$ l'équivalence $\mathcal{R}_{Q,0}$ et $\mathcal{R}_k$ l'équivalence $\mathcal{R}_{1,k}$. Notons que $A \equiv B \bmod \mathcal{R}_{Q,k}$ $\Leftrightarrow$ $A \equiv B \bmod \mathcal{R}_Q$ et $A \equiv B \bmod \mathcal{R}_k$. On remarque aussi que tout polynôme unitaire est inversible modulo $\mathcal{R}_k$. Le groupe formé par les classes de $\mathbb{M}$ inversibles modulo $\mathcal{R}_{Q,k}$, resp. modulo $\mathcal{R}_Q$, est noté $\mathcal{C}_{Q,k}$, resp. $\mathcal{C}_Q$. On note $\mathcal{G}_{Q,k}$, resp. $\mathcal{G}_Q$, le dual de ces groupes et $g(\mathcal{C}_{Q,k}) = \phi(Q)q^k$, resp. $g(\mathcal{C}_Q) = \phi(Q)$, leur ordre qui est aussi l'ordre de leur dual. Rappelons qu'à tout caractère $\chi \in \mathcal{G}_{Q,k}$, on associe un caractère modulaire sur $\mathbb{M}$ que l'on note par le même symbole en posant $\chi(H) = 0$ si H n'est pas inversible modulo $\mathcal{R}_{Q,k}$ et $\chi(H) = \chi(\overline{H})$ si H est inversible modulo $\mathcal{R}_{Q,k}$, $\overline{H}$ désignant la classe de H modulo $\mathcal{R}_{Q,k}$.

Pour tout entier $n \geq 1$, pour tout $R \in \mathbb{M}$ premier à Q, soit $\pi(n; k, Q, R)$ le nombre de polynômes irréductibles unitaires P de degré n, congrus à R modulo $\mathcal{R}_{Q,k}$.

Soient D un polynôme unitaire premier à Q, k un entier naturel et θ un caractère modulo D d'ordre d. Soit $\alpha \in \mathrm{Im}(\theta)$. Pour $R \in \mathbb{M}$ premier à Q, soit $\mathit{\Pi}(n; k, Q, R, D, \theta, \alpha)$ le nombre de $P \in \mathbb{I}$ de degré n, congrus à R modulo $\mathcal{R}_{Q,k}$ et tels que $\theta(P) = \alpha$.

Pour tout polynôme D premier à Q, non nécessairement unitaire, mais sans facteur carré, pour $R \in \mathbb{M}$ premier à Q, soit $\pi^+(n; k, Q, R, D)$, resp. $\pi^-(n; k, Q, R, D)$, le nombre de $P \in \mathbb{I}$ de degré n, congrus à R modulo $\mathcal{R}_{Q,k}$ et tels que D soit inversible et carré mod P, resp. tels que D ne soit pas carré modulo P. Notons aussi $\pi^+(n; D)$, resp. $\pi^-(n; D)$, le nombre de $P \in \mathbb{I}$ de degré n tels que D soit inversible et carré mod P, resp. tels que D ne soit pas carré modulo P.

Faisons d'abord quelques remarques très élémentaires. Quand $D = 1$, θ ne peut être que le caractère unité. Dans ce cas, $\alpha = 1$ et $\pi(n; k, Q, R, D, \theta, \alpha)$ $= \pi(n; k, Q, R, 1, 1, 1) = \pi(n; k, Q, R)$. Si en plus, $Q = 1$, $\pi(n; k, Q, R)$ est le nombre de polynômes irréductibles unitaires de degré n dont les k premiers coefficients sont égaux à ceux de R. Le nombre $\pi(n; k, 1, R)$ sera noté $\pi(n; k, R)$. Si $D \neq 1$ et si θ est le caractère unité, $\alpha = 1$ et $\pi(n; k, Q, R, D, \theta, \alpha) = \pi(n; k, Q, R, D, 1, 1)$ est le nombre de $P \in \mathbb{I}$ de degré n, congrus à R modulo $\mathcal{R}_{Q,k}$ et ne divisant pas D. En dehors d'un nombre fini d'entiers n, $\pi(n; k, Q, R, D, 1, 1) = \pi(n; k, Q, R)$. Plus précisément, si n n'est pas le degré d'un facteur irréductible de D, $\pi(n; k, Q, R, D, 1, 1) = \pi(n; k, Q, R)$, sinon, $|\pi(n; k, Q, R, D, 1, 1) - \pi(n; k, Q, R)| \leq \nu(n, D)$ où $\nu(n, D)$ est le nombre de diviseurs irréductibles unitaires de D et l'estimation des nombres $\pi(n; k, Q, R, D, 1, 1)$ se ramène à celle des nombres $\pi(n; k, Q, R)$ qui seule retiendra notre intérêt dans ce travail.

Dans ce qui suit, on convient que le caractère θ est d'ordre $d > 1$ dès que $D \neq 1$. Si $k = 0$, $Q = 1$, $\pi(n; k, Q, R, D, \theta, \alpha) = \pi(n; D, \theta, \alpha)$ est le nombre de $P \in \mathbb{I}$ de degré n tels que $\theta(P) = \alpha$. En particulier si $d = 2$, θ est le caractère quadratique, $\pi(n; D, \theta, 1)$ est le nombre de polynômes irréductibles unitaires P de degré n ne divisant pas D pour lesquels D est carré modulo P, et $\pi(n; D, \theta, -1)$ est le nombre de polynômes irréductibles unitaires P de degré n pour lesquels D n'est pas carré modulo P.

III. Les principaux théorèmes. Ce travail a pour but essentiel la démonstration du théorème suivant.

THÉORÈME III.1. *Soient $Q \in \mathbb{M}$, $D \in \mathbb{M}$ premiers entre eux, k un entier naturel tels que $k + \deg(QD) \geq 1$ et θ un caractère modulo D d'ordre d. Alors, pour tout $R \in \mathbb{M}$ premier à Q, tout $\alpha \in \mathrm{Im}(\theta)$ et tout entier $n \geq 1$, on a*

$$\frac{q^{n-k}}{d\phi(Q)} - \left(1 - \frac{1}{d\phi(Q)q^k}\right)(k - 1 + \deg(QD))q^{n/2} - 2q^{n/2} - \deg(QD)$$
$$\leq n\pi(n; k, Q, R, D, \theta, \alpha) \leq \frac{q^{n-k}}{d\phi(Q)} + \left(1 - \frac{1}{d\phi(Q)q^k}\right)(k - 1 + \deg(QD))q^{n/2}.$$

Une version moins précise mais plus simple de ce théorème pourra être retenue sous la forme suivante.

THÉORÈME III.1′. *Soient $Q \in \mathbb{M}$, $D \in \mathbb{M}$ premiers entre eux, k un entier naturel tels que $k + \deg(QD) \geq 1$ et θ un caractère modulo D d'ordre d. Alors, pour tout $R \in \mathbb{M}$ premier à Q, tout $\alpha \in \mathrm{Im}(\theta)$ et tout entier $n \geq 1$, on a*

$$\frac{q^{n-k}}{d\phi(Q)} - (k + 1 + \deg(QD))q^{n/2} \leq n\pi(n; k, Q, R, D, \theta, \alpha)$$
$$\leq \frac{q^{n-k}}{d\phi(Q)} + (k - 1 + \deg(QD))q^{n/2}.$$

Si l'on applique le théorème III.1 ou le théorème III.1′ dans le cas où $D = 1$, on obtient le

COROLLAIRE III.2. *Soient $Q \in \mathbb{M}$ et k un entier naturel tels que $k + \deg(Q) \geq 1$. Alors, pour tout $R \in \mathbb{M}$ premier à Q et tout entier $n \geq 1$, on a*

$$\frac{q^{n-k}}{\phi(Q)} - \left(1 - \frac{1}{d\phi(Q)q^k}\right)(k - 1 + \deg(Q))q^{n/2} - 2q^{n/2} - \deg(Q) \leq n\pi(n; k, Q, R)$$
$$\leq \frac{q^{n-k}}{n\phi(Q)} + \left(1 - \frac{1}{q^k\phi(Q)}\right)(k - 1 + \deg(Q))q^{n/2},$$

ou le

COROLLAIRE III.2′. *Soient $Q \in \mathbb{M}$ et k un entier naturel tels que $k + \deg(Q) \geq 1$. Alors, pour tout $R \in \mathbb{M}$ premier à Q et tout entier $n \geq 1$, on a*

$$\frac{q^{n-k}}{\phi(Q)} - (k+1+\deg(Q))q^{n/2} \leq n\pi(n;k,Q,R) \leq \frac{q^{n-k}}{n\phi(Q)} + (k-1+\deg(Q))q^{n/2}.$$

On retrouve le résultat donné dans [3] avec une meilleure minoration. Si l'on applique ce corollaire dans le cas où $Q = T^s$, on retrouve, sous l'hypothèse $k + s \geq 1$, une estimation donnée par le théorème 1.3 de [2]. C'est le

COROLLAIRE III.3. *Soient k et s des entiers naturels tels que $k + s \geq 1$, $\mathbf{a} = (a_1, \ldots, a_k)$ un élément de $\mathbb{F}_q^k$ et $\mathbf{b} = (b_1, \ldots, b_s)$ un élément de $\mathbb{F}_q^s$. Soit $\pi(n;\mathbf{a},\mathbf{b})$ le nombre de polynômes irréductibles unitaires de degré n dont les $k+1$ premiers coefficients, resp. les s derniers coefficients, sont* 1, $a_1, \ldots, a_k$, *resp.* $b_1, \ldots, b_s$. *Alors,*

$$\frac{q^{n-k-s+1}}{q-1} - (k+s+2)q^{n/2} \leq n\pi(n;\mathbf{a},\mathbf{b}) \leq \frac{q^{n-k-s+1}}{q-1} + \left(1 - \frac{1}{q^{k+s}(q-1)}\right)(k+s)q^{n/2}.$$

Soit θ un caractère modulo D d'ordre d. Soit $\alpha \in \mathrm{Im}(\theta)$. Il existe exactement $r = \phi(D)/d$ classes modulo D dont l'image par θ est égale à α. Soient $A_1, \ldots, A_r$ des représentants de ces classes. Soit H un polynôme irréductible unitaire. Alors $\theta(H) = \alpha$ si et seulement si il existe $i = 1, \ldots, r$ tel que H soit congru à A_i modulo D. Soit $R \in \mathbb{M}$ inversible modulo l'équivalence $\mathcal{R}_{Q,k}$ et soit, pour $i = 1, \ldots, r$, $R_i \in \mathbb{M}$ congru à R modulo $\mathcal{R}_{Q,k}$ et à A_i modulo D. Alors,

$$\pi(n;k,Q,R,D,\theta,\alpha) = \sum_{i=1}^{r} \pi(n;k,QD,R_i). \tag{0}$$

On peut obtenir une estimation des nombres $\pi(n;k,Q,R,D,\theta,\alpha)$ à l'aide des théorèmes I.3 ou I.4. En procédant ainsi, on obtient

$$n\pi(n;k,Q,R,D,\theta,\alpha) \leq \frac{q^{n-k}}{d\phi(Q)} + \frac{\phi(D)}{d}\left(1 - \frac{1}{q^k\phi(QD)}\right)(k-1+\deg(QD))q^{n/2},$$

et

$$n\pi(n;k,Q,R,D,\theta,\alpha)$$
$$\geq \frac{q^{n-k}}{d\phi(Q)} - \frac{\phi(D)}{d}\left(\left(1-\frac{1}{q^k\phi(QD)}\right)(k-1+\deg(QD)+3)\right)q^{n/2} - \frac{\deg(Q)}{dq^k\phi(Q)},$$

ce qui est moins bon que le résultat donné par le théorème III.1 ci-dessus.

Dans le cas où $k=0$, $D=1$ et $\deg(Q)=1$, resp. où $k=0$, $Q=1$ et $\deg(D)=1$, le théorème III.1′ donne

$$\frac{q^n}{q-1} - 1 - 2q^{n/2} \leq n\pi(n;Q,R) \leq \frac{q^n}{q-1},$$

resp.

$$\frac{q^n}{d} - 1 - 2q^{n/2} \leq n\pi(n;D,\theta,\alpha) \leq \frac{q^n}{d}.$$

Une étude de ces cas particuliers nous permettra d'obtenir de meilleurs résultats, à savoir les théorèmes III.4 et III.5 ci-dessous.

THÉORÈME III.4. *Soit $Q \in \mathbb{M}$ de degré 1. Alors, pour tout $R \in \mathbb{M}$ premier à Q et tout entier $n \geq 1$,*

$$\frac{q^n-1}{q-1} - 2q^{n/2} \leq n\pi(n;Q,R) \leq \frac{q^n-1}{q-1}.$$

THÉORÈME III.5. *Soient $D \in \mathbb{M}$ de degré 1, θ un caractère modulo D d'ordre d et $\alpha \in \mathrm{Im}(\theta)$. Alors, pour tout entier $n \geq 1$, on a*

$$\frac{q^n-1}{d} - 2q^{n/2} \leq n\pi(n;D,\theta,\alpha) \leq \frac{q^n-1}{d}.$$

Citons enfin quelques conséquences du théorèmes III.1′.

THÉORÈME III.6. *Soit D un polynôme non constant sans facteur carré. Alors, pour tout entier $n \geq 1$, on a*

$$\frac{q^n}{2} - (\deg(D)+1)q^{n/2} \leq n\pi^+(n;D) \leq \frac{q^n}{2} + (\deg(D)-1)\frac{q^{n/2}}{2},$$
$$\frac{q^n}{2} - (\deg(D)+1)q^{n/2} \leq n\pi^-(n;D) \leq \frac{q^n}{2} + (\deg(D)-1)\frac{q^{n/2}}{2}.$$

THÉORÈME III.7. *Soient D un polynôme non constant sans facteur carré, $Q \in \mathbb{M}$ premier à D et k un entier naturel. Alors, pour tout $R \in \mathbb{M}$ premier à Q et tout entier $n \geq 1$, on a*

$$\frac{q^{n-k}}{2\phi(Q)} - (k+1+\deg(QD))q^{n/2}$$
$$\leq n\pi^+(n;k,Q,R) \leq \frac{q^{n-k}}{2\phi(Q)} + (k-1+\deg(QD))q^{n/2},$$

$$\frac{q^{n-k}}{2\phi(Q)} - (k+1+\deg(QD))q^{n/2}$$
$$\leq n\pi^{-}(n;k,Q,R) \leq \frac{q^{n-k}}{2\phi(Q)} + (k-1+\deg(QD))q^{n/2}.$$

IV. Démonstration des théorèmes III.1 et III.1′. Rappelons tout d'abord deux résultats concernant les nombres $\pi(n)$.

THÉORÈME IV.1. *Soit un entier $n \geq 1$. Alors, on a*

$$q^n = \sum_{m \mid n} m\pi(m), \tag{IV.1}$$

$$q^n - 2q^{n/2} \leq n\pi_n \leq q^n. \tag{IV.2}$$

P r e u v e. Le premier résultat est bien connu. On peut en trouver une preuve au paragraphe 2, chapitre 3 de [4]. La majoration (IV.2) de $n\pi_n$ est une conséquence immédiate de (IV.1). La minoration (IV.2) de $n\pi_n$ est une conséquence non immédiate de (IV.1). Une preuve de ce résultat se trouve dans [5].

Soient $Q \in \mathbb{M}$ et k un entier naturel. Soient D un polynôme unitaire premier à Q, k un entier naturel et θ un caractère modulo D d'ordre d. Soit $\alpha \in \mathrm{Im}(\theta)$.

Si n et m sont des entiers strictement positifs tels que m divise n, on désigne par $\nu(n,m,A,\alpha)$ le nombre de polynômes $P \in \mathbb{I}$ tels que

(i) $\deg(P) = m$,
(ii) $P^{n/m} \equiv A \bmod \mathcal{R}_{Q,k}$,
(iii) $\theta(P^{n/m}) = \alpha$.

On remarque que $\pi(n;k,Q,A,D,\theta,\alpha) = \nu(n,n,A,\alpha)$.

On définit sur $\mathbb{M}$ la fonction Λ de von Mangoldt par $\Lambda(H) = \deg(P)$ si H est puissance d'un polynôme irréductible unitaire P, et $\Lambda(H) = 0$ dans tous les autres cas.

PROPOSITION IV.2. *On a*

$$dg(\mathcal{C}_{Q,k}) \sum_{m \mid n} m\nu(n,m,A,\alpha) \tag{IV.3}$$
$$= \sum_{j=0}^{d-1} \alpha^{-j} \sum_{\chi \in \mathcal{G}_{Q,k}} \overline{\chi(A)} \sum_{\substack{H \in \mathbb{M} \\ \deg(H)=n}} \Lambda(H)\chi(H)(\theta(H))^j.$$

P r e u v e. Notons S la somme de droite. On inverse l'ordre des sommations dans S. On utilise les relations d'orthogonalité suivantes, valables pour

tout $H \in \mathbb{M}$:

$$\sum_{j=0}^{d-1} \alpha^{-j}\theta(H)^j = \begin{cases} d & \text{si } \theta(H) = \alpha, \\ 0 & \text{si } \theta(H) \neq \alpha. \end{cases}$$

$$\sum_{\chi \in \mathcal{G}_{Q,k}} \overline{\chi(A)}\chi(H) = \begin{cases} g(\mathcal{C}_{Q,k}) & \text{si } H \equiv A \bmod \mathcal{R}_{Q,k}, \\ 0 & \text{si } H \not\equiv A \bmod \mathcal{R}_{Q,k}. \end{cases}$$

Il vient

$$S = dg(\mathcal{C}_{Q,k}) \sum_{H \in \mathbb{H}} \Lambda(H),$$

où $\mathbb{H}$ désigne l'ensemble des polynômes $H \in \mathbb{M}$ tels que $\deg(H) = n$, $\theta(H) = \alpha$ et $H \equiv A \bmod \mathcal{R}_{Q,k}$. Dans cette dernière somme $\Lambda(H)$ est non nul si et seulement si H est une puissance d'un polynôme irréductible P. Dans ce cas, $\Lambda(H) = \deg(P)$ et $\deg(P)$ divise n.

On pose

$$g = g(\mathcal{C}_{Q,k}). \tag{IV.4}$$

Pour $\chi \in \mathcal{G}_{Q,k}$, $j \in \{0, \dots, d-1\}$, on pose

$$S(\chi, j) = \sum_{\substack{H \in \mathbb{M} \\ \deg(H) = n}} \Lambda(H)\chi(H)(\theta(H))^j, \tag{IV.5}$$

$$\pi(n; A, \alpha) = \pi(n; k, Q, A, D, \theta, \alpha). \tag{IV.6}$$

Proposition IV.3. *Soit χ_0 le caractère unité dans $\mathcal{G}_{Q,k}$. Alors, on a*

$$q^n - \deg(QD) \leq S(\chi_0, 0) \leq q^n. \tag{IV.7}$$

P r e u v e. Si les polynômes H et Q, resp. les polynômes H et D, ne sont pas premiers entre eux, on a $\chi_0(H) = 0$, resp. $\theta(H) = 0$, d'où

$$S(\chi_0, 0) = \sum_{\substack{H \in \mathbb{H} \\ \deg(H) = n \\ (H, QD) = 1}} \Lambda(H) = \sum_{\substack{P \in \mathbb{I} \\ k \deg(P) = n \\ (P, QD) = 1}} \deg(P).$$

L'égalité (IV.1) donne alors,

$$S(\chi_0, 0) = q^n - \sum_{m|n} m\#\{P \in \mathbb{I} \mid \deg(P) = m,\ P \mid QD\} \geq q^n - \sum_{\substack{P \in \mathbb{I} \\ P|QD}} \deg(P),$$

d'où (IV.7).

Proposition IV.4. *Soient $j \in \{1, \dots, d-1\}$ et $\chi \in \mathcal{G}_{Q,k}$ tels que $(\chi, j) \neq (\chi_0, 0)$, χ_0 désignant toujours le caractère unité dans $\mathcal{G}_{Q,k}$. Alors,*

$$|S(\chi, j)| \leq (k - 1 + \deg(QD))q^{n/2}. \tag{IV.8}$$

P r e u v e. Les polynômes Q et D étant premiers entre eux, les groupes $\mathcal{C}_{QD,k}$ et $\mathcal{C}_{Q,k} \times \mathcal{C}_D$ sont isomorphes. Les groupes duaux $\mathcal{G}_{QD,k}$ et $\mathcal{G}_{Q,k} \times \mathcal{G}_D$ sont aussi isomorphes. L'application $(\chi, \varrho) \mapsto \chi\varrho$ est un isomorphisme de $\mathcal{G}_{Q,k} \times \mathcal{G}_D$ sur $\mathcal{G}_{QD,k}$. En particulier, $\chi\varrho$ est le caractère unité de $\mathcal{G}_{QD,k}$ si et seulement si χ est le caractère unité de $\mathcal{G}_{Q,k}$ et ϱ le caractère unité de $\mathcal{G}_D$.

Soient $j \in \{1, \dots, d-1\}$ et $\chi \in \mathcal{G}_{Q,k}$ tels que $(\chi, j) \neq (\chi_0, 0)$. Soit $\lambda = \chi\theta^j$. L'un au moins des caractères χ et θ^j n'est pas le caractère unité et λ n'est pas le caractère unité. On associe au caractère λ la fonction $L(\lambda, \cdot)$ définie pour tout nombre complexe z de module $1/q$ par

$$L(\lambda, z) = \sum_{H \in \mathbb{M}} \lambda(H) z^{\deg(H)}. \tag{1}$$

D'après le lemme 8.2 de [3], pour tout entier $n \geq k + \deg(QD)$, toute classe $\alpha \in \mathcal{C}_{Q,k}$ contient exactement $q^{n-k-\deg(QD)}$ polynômes unitaires de degré n. Par suite, $L(\lambda, z)$ est un polynôme de degré

$$d(\lambda) < k + \deg(QD). \tag{2}$$

Aux paragraphes 3, 4 et 5 de [6] on montre comment associer au caractère λ un quasi-caractère ω non principal du groupe $\mathbb{J}(\mathbb{K})$ des idèles du corps $\mathbb{K} = \mathbb{F}_q(T)$. La fonction L associée au quasi-caractère ω, notée L_ω, est alors un polynôme dont les racines sont des entiers algébriques de module $q^{-1/2}$ (cf. [7, Appendice 5]). Soit $\mathbb{S}$ l'ensemble formé par la réunion de la place à l'infini et des places associées aux diviseurs irréductibles du produit QD. D'après [6, théorème 3], pour tout $v \in \mathbb{S}$, il existe un nombre complexe $\varepsilon(v)$ de module 0 ou 1 tel que

$$L(\lambda, z) = L_\omega(z) \prod_{v \in \mathbb{S}} (1 - \varepsilon(v) z^{\deg(v)}).$$

Par suite, il existe $d(\lambda)$ nombres complexes $\omega_1, \dots, \omega_{d(\lambda)}$ de module 1 ou $q^{-1/2}$ tels que

$$L(\lambda, z) = \prod_{i=1}^{d(\lambda)} \left(1 - \frac{z}{\omega_i}\right). \tag{3}$$

Dans le disque $|z| < 1/q$, la série $L(\lambda, z)$ s'écrit comme produit eulérien absolument convergent

$$L(\lambda, z) = \prod_{P \in \mathbb{I}} (1 - \lambda(P) z^{\deg(P)})^{-1}. \tag{4}$$

On calcule $zL'(\lambda, z)/L(\lambda, z)$ au moyen des relations (3) et (4). Par identification des coefficients de z^n dans les deux relations obtenues, il vient

$$\sum_{\substack{H\in\mathbb{H}\\ \deg(H)=n\\ (H,QD)=1}} \Lambda(H)\lambda(H) = -\sum_{i=1}^{d(\lambda)}\left(\frac{1}{\omega_i}\right)^n,$$

d'où,

$$\sum_{\substack{H\in\mathbb{H}\\ \deg(H)=n}} \Lambda(H)\chi(H)(\theta(H))^j = -\sum_{i=1}^{d(\lambda)}\left(\frac{1}{\omega_i}\right)^n,$$

$$|S(\chi,j)| \le d(\lambda)q^{n/2}. \tag{5}$$

On conclut avec (2) et (5).

Proposition IV.5. *Soient $A\in\mathbb{M}$ premier à Q et $\alpha\in\mathrm{Im}(\theta)$. Alors, pour tout entier $n\ge 1$, on a*

$$\begin{aligned}\frac{q^n}{gd} - \frac{\deg(QD)}{gd} - \left(1-\frac{1}{dg}\right)(k-1+\deg(QD))q^{n/2} - 2q^{n/2}\\ \le n\pi(n;A,\alpha) \le \frac{q^n}{gd} + \left(1-\frac{1}{dg}\right)(k-1+\deg(QD))q^{n/2}.\end{aligned} \tag{IV.9}$$

P r e u v e. La proposition IV.2 s'écrit

$$dg\Big(n\pi(n;A,\alpha) + \sum_{\substack{m|n\\ m\ne n}} m\nu(n,m,A,\alpha)\Big) = \sum_{j=0}^{d-1}\alpha^{-j}\sum_{\chi\in\mathcal{G}_{Q,k}}\overline{\chi(A)}S(\chi,j).$$

On en déduit la majoration

$$dgn\pi(n;A,\alpha) \le \sum_{j=0}^{d-1}\alpha^{-j}\sum_{\chi\in\mathcal{G}_{Q,k}}\overline{\chi(A)}S(\chi,j) \tag{1}$$

ainsi que la minoration

$$dgn\pi(n;A,\alpha) \ge \sum_{j=0}^{d-1}\alpha^{-j}\sum_{\chi\in\mathcal{G}_{Q,k}}\overline{\chi(A)}S(\chi,j) - dg\sum_{\substack{m|n\\ m\ne n}} m\pi_m. \tag{2}$$

Avec la majoration (1) et les majorations (IV.7) et (IV.8), on a

$$dgn\pi(n;A,\alpha) \le q^n + (dg-1)(k-1+\deg(QD))q^{n/2},$$

d'où la majoration (IV.9). La minoration (IV.2) nous donne

$$dgn\pi(n;A,\alpha) \ge \sum_{j=0}^{d-1}\alpha^{-j}\sum_{\chi\in\mathcal{G}_{Q,k}}\overline{\chi(A)}S(\chi,j) - 2dgq^{n/2}.$$

Avec (IV.7) et (IV.8) on obtient alors

$$dgn\pi(n;A,\alpha) \geq q^n - \deg(QD) - (dg-1)(k-1+\deg(QD))q^{n/2} - 2dgq^{n/2},$$

d'où la minoration (IV.9).

La proposition IV.5 est en fait le théorème III.1 annoncé.

V. Démonstration des autres théorèmes. On désignera par $\boldsymbol{N}_n$ la norme de l'extension $\mathbb{F}_{q^n}(T)$ de $\mathbb{F}_q(T)$.

V.1. *Démonstration du théorème III.4.* Supposons $k=0$, $\deg(D)=0$ et $\deg(Q)=1$. Ici encore $\mathcal{C}_D$ est trivial, θ est le caractère unité et α ne peut prendre que la valeur 1. L'équivalence $\mathcal{R}_{Q,k}$ est la congruence modulo Q, et le groupe $\mathcal{C}_Q$ s'identifie au groupe multiplicatif $\mathbb{F}_q^*$ du corps $\mathbb{F}_q$. Dans ce cas, pour tout $a \in \mathbb{F}_q^*$,

$$\pi(n;k,Q,a,D,\theta,\alpha) = \pi(n;0,Q,a,1,1,1) = \pi(n;Q,a).$$

Posons $Q = T-b$. L'application $H \mapsto H_b$ où $H_b(T) = H(T+b)$ réalise une bijection de l'ensemble des polynômes irréductibles unitaires P tels que $P(b)=a$ sur l'ensemble des polynômes irréductibles unitaires P tels que $P(0)=a$. Cette bijection préserve les degrés. Par suite, pour tout entier n, $\pi(n;Q,a) = \pi(n;T,a)$. Notons Γ_q le dual de $\mathbb{F}_q^*$. La proposition IV.2 nous donne ici

$$(q-1)\sum_{m|n} m\nu(n,m,a) = d\#(\mathcal{G}_{Q,k})\sum_{m|n} m\nu(n,m,A,\alpha) = \sum_{\gamma\in\Gamma_q} \overline{\gamma(a)}S(\gamma)$$

avec

$$S(\gamma) = \sum_{\substack{H\in\mathbb{H}\\ \deg(H)=n}} \Lambda(H)\gamma(H).$$

On a

$$S(\gamma) = \sum_{\substack{H\in\mathbb{H}\\ \deg(H)=n}} \Lambda(H)\gamma(H(0)) = \sum_{b\in\mathbb{F}_q^*}\gamma(b) \sum_{\substack{H\in\mathbb{H}\\ \deg(H)=n\\ H(0)=b}} \Lambda(H),$$

$$S(\gamma) = \sum_{b\in\mathbb{F}_q^*}\gamma(b) \sum_{\substack{P\in\mathbb{I}\\ k\deg(P)=n\\ P(0)^k=b}} \deg(P) = \sum_{b\in\mathbb{F}_q^*}\gamma(b) \sum_{\substack{\omega\in\mathbb{F}_{q^n}^*\\ \boldsymbol{N}_n(\omega)=b}} 1.$$

Pour tout $b\in\mathbb{F}_q^*$ il y a exactement $(q^n-1)/(q-1)$ éléments $\omega\in\mathbb{F}_{q^n}^*$ tels que $\boldsymbol{N}_n(\omega)=b$, d'où,

$$S(\gamma) = \frac{q^n-1}{q-1}\sum_{b\in\mathbb{F}_q^*}\gamma(b) = \begin{cases} 0 & \text{si } \gamma\neq\gamma_0,\\ q^n-1 & \text{si } \gamma=\gamma_0,\end{cases}$$

γ_0 désignant le caractère unité de $\mathbb{F}_q^*$.

On en déduit

$$n\pi(n;T,a)+\sum_{\substack{m|n\\ m<n}} m\nu(n,m,a)=\frac{q^n-1}{q-1},$$

$$n\pi(n;T,a)\le\frac{q^n-1}{q-1},\qquad n\pi(n;T,a)\ge\frac{q^n-1}{q-1}-\sum_{\substack{m|n\\ m<n}} m\Pi_m,$$

et, avec (IV.2),

$$n\pi(n;T,a)\ge\frac{q^n}{q-1}-\frac{1}{q-1}-2q^{n/2}.$$

V.2. *Démonstration du théorème III.5.* Supposons $k=0$, $\deg(D)=1$, $\deg(Q)=0$. Ici, le groupe $\mathcal{C}_{Q,k}$ est trivial, le groupe $\mathcal{C}_D$ s'identifie au groupe multiplicatif $\mathbb{F}_q^*$, son dual s'identifie au groupe Γ_q introduit ci-dessus. On a $\phi(D)=q-1$ et d divise $q-1$. La proposition IV.2 nous donne ici

$$d\sum_{m|n} m\nu(n,m,A,\alpha)=\sum_{j=0}^{d-1}\alpha^{-j}\sum_{\substack{H\in\mathbb{M}\\ \deg(H)=n}}\Lambda(H)\theta(H)^j.$$

Posons $D=T+b$. Pour tout polynôme unitaire H, $\theta(H)=\theta(H(-b))$. Comme précédemment,

$$d\sum_{m|n} m\nu(n,m,A,\alpha)=\sum_{j=0}^{d-1}\alpha^{-j}\sigma_j,$$

avec

$$\sigma_j=\sum_{\substack{b\in\mathbb{F}_{q^n}\\ \beta\ne -b}}\theta(\boldsymbol{N}_n(\beta-b))^j.$$

On a $\sigma_0=q^n-1$, et, pour $j=1,2,\dots,d-1$,

$$\sigma_j=\sum_{\substack{\gamma\in\mathbb{F}_{q^n}\\ \gamma\ne 0}}\theta(\boldsymbol{N}^{(n)}(\gamma))^j=\frac{q^n-1}{q-1}\sum_{c\in\mathbb{F}_q^*}\theta(c)^j=0.$$

On en déduit

$$d\sum_{m|n} m\nu(n,m,A,\alpha)=q^n-1,$$

et on achève la démonstration comme pour le théorème III.5.

V.3. *Démonstration des théorèmes III.6 et III.7.* Soient un entier $k\ge 0$, Q un polynôme unitaire et R un polynôme premier à Q. Soit D polynôme non nul de $\mathbb{F}_q[T]$ sans facteur carré. On pose $D=\operatorname{sgn}(D)\Delta$, $\operatorname{sgn}(D)$ étant un élément non nul de $\mathbb{F}_q$, Δ étant un polynôme unitaire de $\mathbb{F}_q[T]$. Soit θ

le caractère quadratique modulo Δ. Si $P \in \mathbb{I}$ ne divise pas Δ, $\theta(P) = \left(\frac{\Delta}{P}\right)$, où $\left(\frac{\cdot}{P}\right)$ désigne le symbole de Legendre modulo P. Si $\mathrm{sgn}(D)$ est carré dans $\mathbb{F}_q$, pour tout $P \in \mathbb{I}$, $\left(\frac{\Delta}{P}\right) = \theta(P)$. Le théorème III.1′ donne les théorèmes III.6 et III.7. On suppose $\mathrm{sgn}(D)$ non carré dans $\mathbb{F}_q$. Alors, si $P \in \mathbb{I}$, $\mathrm{sgn}(D)$ est carré modulo P si et seulement si $\deg(P)$ est pair. On a donc, pour tout entier n pair,

$$\pi^+(n;k,Q,R) = \pi(n;k,Q,R,\Delta,\theta,1),$$
$$\pi^-(n;k,Q,R) = \pi(n;k,Q,R,\Delta,\theta,-1),$$
$$\pi^+(n) = \pi(n;\Delta,\theta,1), \quad \pi^-(n) = \pi(n;\Delta,\theta,-1),$$

et, pour tout entier n impair,

$$\pi^+(n;k,Q,R) = \pi(n;k,Q,R,\Delta,\theta,-1),$$
$$\pi^-(n;k,Q,R) = \pi(n;k,Q,R,\Delta,\theta,1),$$
$$\pi^+(n) = \Pi(n;\Delta,\theta,-1), \quad \pi^-(n) = \Pi(n;\Delta,\theta,1).$$

Les théorèmes III.6 et III.7 se déduisent encore du théorème III.1′.

Références

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. II*, Math. Z. 19 (1924), 207–246.

[2] D. R. Hayes, *The distribution of irreducibles in $GF[q,x]$*, Trans. Amer. Math. Soc. 117 (1965), 101–127.

[3] C. H. Hsu, *The distribution of irreducible polynomials in $\mathbb{F}_q[T]$*, J. Number Theory 61 (1996), 85–96.

[4] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, 1986.

[5] M. Mignotte, *Statistiques sur $\mathbb{F}_q[X]$*, Comptes Rendus des Journées de Théorie Analytique et Elémentaire des Nombres, Limoges, 1980.

[6] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Math. 95 (1972).

[7] A. Weil, *Basic Number Theory*, 3ième ed., Springer, Berlin, 1974.

Laboratoire de Mathématiques
Cour A
Faculté des Sciences de Saint-Jérôme
Avenue Escadrille Normandie Niemen
13397 Marseille Cedex 20, France
E-mail: mireille.car@math.u-3mrs.fr

Reçu le 21.10.1997
et révisé le 15.9.1998 (3284)