ACTA ARITHMETICA
LXIX.3 (1995)

Répartition modulo 1 dans un corps de séries formelles sur un corps fini

par

Mireille Car (Marseille)

Introduction. Soit q une puissance d'un nombre premier p et soit $\mathbb{F}_q$ le corps fini à q éléments. Une certaine analogie entre l'arithmétique de l'anneau $\mathbb{Z}$ des entiers rationnels et celle de l'anneau $\mathbb{F}_q[T]$ a conduit à étendre à $\mathbb{F}_q[T]$ de nombreuses questions de l'arithmétique classique. L'équirépartition modulo 1 est une de ces questions. Le corps des nombres réels est alors remplacé par le corps $\mathbb{F}_q((T^{-1}))$ des séries de Laurent formelles, complété du corps $\mathbb{F}_q(T)$ des fractions rationnelles pour la valuation à l'infini et l'intervalle $[0,1[$ est remplacé par l'idéal de valuation. L. Carlitz [1] a donné une définition de l'équirépartition modulo 1 dans le corps $\mathbb{F}_q((T^{-1}))$ qui s'est révélée fructueuse puisqu'elle permet l'utilisation d'un critère de Weyl [1], [7], la généralisation des premiers résultats de Weyl [2], [3], du théorème de Koksma [7], ou du théorème de Vinogradov [8]. Il est bien connu que la suite $(\sqrt{n}\,)$ est équirépartie modulo 1. Il est donc naturel de poser la question de l'équirépartition modulo 1 de la suite $(H^{1/2})$, H décrivant la suite des polynômes de $\mathbb{F}_q[T]$ admettant une racine carrée $H^{1/2}$ dans le corps $\mathbb{F}_q((T^{-1}))$, et, plus généralement, celle de la suite $(H^{1/l})$, H décrivant la suite des polynômes de $\mathbb{F}_q[T]$ admettant une racine l-ième $H^{1/l}$ dans le corps $\mathbb{F}_q((T^{-1}))$. C'est ce qui est fait dans ce qui suit, où l'on précise ce que l'on entend par racine l-ième. On démontre que pour $l \geq 2$, la suite $(H^{1/l})$ est équirépartie modulo 1, et que pour $l \geq 3$, la suite $(P^{1/l})$ est équirépartie modulo 1, P décrivant la suite des polynômes irréductibles de $\mathbb{F}_q[T]$ admettant une racine l-ième dans le corps $\mathbb{F}_q((T^{-1}))$.

I. Préliminaires

I.1. *Notations et rappels.* On pose $\mathbf{R} = \mathbb{F}_q[T]$, $\mathbf{K} = \mathbb{F}_q(T)$. La valuation à l'infini sur le corps $\mathbf{K}$ est l'application ν de $\mathbf{K}$ dans $\mathbb{Z} \cup \{\infty\}$ définie par $\nu(0) = \infty$ et $\nu(A/B) = \deg B - \deg A$, si A et B sont des polynômes non nuls.

Le complété de $\mathbf{K}$ pour la valuation ν est le corps $\mathbf{K}_\infty = \mathbb{F}_q((T^{-1}))$ des séries de Laurent formelles

$$y = \sum_{n=-\infty}^{\infty} y_n T^n, \tag{I.1.1}$$

où $y_n \in \mathbb{F}_q$, les coefficients y_n étant tous nuls pour n assez grand. On prolonge la valuation ν à $\mathbf{K}_\infty$ en posant pour $y \neq 0$,

$$\nu(y) = -\sup\{n \in \mathbb{Z} \mid y_n \neq 0\}. \tag{I.1.2}$$

Soit $\mathfrak{P}$ l'idéal de valuation de $\mathbf{K}_\infty$. Le corps $\mathbf{K}_\infty$ est localement compact, un système fondamental de voisinages compacts de l'origine étant fourni par les puissances de l'idéal $\mathfrak{P}$. A constante multiplicative près, il existe une seule mesure de Haar sur $\mathbf{K}_\infty$. On choisit la mesure de Haar $\mu = dt$ normalisée à 1 sur l'idéal de valuation, c'est-à-dire telle que

$$\int_{\mathfrak{P}} dt = 1. \tag{I.1.3}$$

Tout $y \in \mathbf{K}_\infty$ s'écrit de façon unique comme somme

$$y = [y] + \{y\}, \qquad [y] \in \mathbf{R},\ y \in \mathfrak{P}. \tag{I.1.4}$$

Si $y \in \mathbf{K}_\infty$ s'écrit $y = \sum_{n=-\infty}^{\infty} y_n T^n$, on pose

$$\mathrm{Res}(y) = y_{-1}, \tag{I.1.5}$$

si de plus $y \neq 0$, on pose

$$\mathrm{sgn}(y) = y_{-\nu(y)}. \tag{I.1.6}$$

Soit $\psi : \mathbb{F}_q \mapsto \mathbb{C}$ un caractère additif non trivial. Pour tout $y \in \mathbf{K}_\infty$, on pose

$$E(y) = \psi(\mathrm{Res}(y)). \tag{I.1.7}$$

Alors E est un caractère additif non trivial de $\mathbf{K}_\infty$.

Pour tout $a \in \mathbf{K}_\infty$ et tout $r \in \mathbb{Z}$, soit

$$\mathcal{B}(a, r) = \{y \in \mathbf{K}_\infty \mid \nu(y - a) > r\}. \tag{I.1.8}$$

Alors, on a (cf. [4])

$$\mu(\mathcal{B}(a, r)) = q^{-r}. \tag{I.1.9}$$

On notera $\mathbb{F}_q^*$, $\mathbf{R}^*$, $\mathbf{K}^*$, $\mathbf{K}_\infty^*$ l'ensemble des éléments non nuls de $\mathbb{F}_q$, $\mathbf{R}$, $\mathbf{K}$, $\mathbf{K}_\infty$ respectivement.

I.2. *Équirépartition modulo* 1. Soit $\Theta = (\theta_n)$, une suite à valeurs dans $\mathbf{K}_\infty$. Pour tout entier $N > 0$, tout $b \in \mathfrak{P}$ et tout $r \in \mathbb{Z}$, soit $A(\Theta, N, b, r)$ le nombre d'entiers $n \in \{1, \ldots, N\}$ tels que $\{\theta_n\} \in \mathcal{B}(b, r)$. Soit alors,

$$\Delta(\Theta, N, b, r) = \frac{A(\Theta, N, b, r)}{N} - \mu(\mathcal{B}(a, r)) = \frac{A(\Theta, N, b, r)}{N} - q^{-r}, \tag{I.2.1}$$

et

$$D(\Theta, N) = \sup_{b \in \mathfrak{P}, r \in \mathbb{Z}} |\Delta(\Theta, N, b, r)|. \tag{I.2.2}$$

DÉFINITION I.2.1 (Carlitz). Une suite Θ à valeurs dans $\mathbf{K}_\infty$ est dite *équirépartie modulo* 1 si la suite $(D(\Theta, N))$ tend vers 0 lorsque N tend vers ∞.

On a alors le critère de Weyl (cf. [1], [7]) :

THÉORÈME I.2.2. *Une suite Θ à valeurs dans $\mathbf{K}_\infty$ est équirépartie modulo* 1 *si et seulement si pour tout $H \in \mathbf{R}^*$ non nul, la suite $((1/N)\sum_{n=1}^{N} E(H\theta_n))$ tend vers* 0 *lorsque N tend vers ∞.*

I.3. *Les racines l-ièmes dans $\mathbf{K}_\infty^*$.* Soit un entier $l \geq 2$ non divisible par la caractéristique p du corps $\mathbb{F}_q$. Dans $\mathbb{F}_q^*$ il y a exactement

$$r = \frac{q-1}{\text{p.g.c.d.}(l, q-1)} \tag{I.3.1}$$

puissances l-ièmes. Soit $\mathcal{L}$ l'ensemble de ces r puissances l-ièmes.

LEMME I.3.1. *Soient*

$$a = \sum_{j=-\infty}^{N} a_j T^j, \qquad b = \sum_{j=-\infty}^{n} b_j T^j$$

des éléments de $\mathbf{K}_\infty^*$. Alors $a = b^l$ si et seulement si les trois conditions suivantes sont réalisées :

(i) $N = ln$,
(ii) $a_N = b_n^l$,
(iii) *pour tout entier $k \geq 1$, on a*

$$a_{N-k} = l b_n^{l-1} b_{n-k} + \sum_{\substack{i_1+\ldots+i_l=N-k \\ n-k<i_1\leq n \\ \cdots\cdots\cdots \\ n-k<i_l\leq n}} b_{i_1} \ldots b_{i_l}. \tag{I.3.2}$$

Démonstration. Immédiate.

PROPOSITION I.3.2. *Soit $a \in \mathbf{K}_\infty^*$. Alors, il existe $b \in \mathbf{K}_\infty^*$ tel que $a = b^l$ si et seulement si $\nu(a) \equiv 0 \bmod l$ et $\operatorname{sgn}(a) \in \mathcal{L}$. Dans ce cas il y a exactement r éléments $b \in \mathbf{K}_\infty^*$ tels que $a = b^l$.*

Démonstration. Les conditions (i) et (ii) du lemme ci-dessus montrent la nécessité des conditions. Soit $a = \sum_{j=-\infty}^{ln} a_j T^j$ un élément de $\mathbf{K}_\infty^*$ tel que $\nu(a) = -ln$ et tel que $\operatorname{sgn}(a) = a_{ln}$ soit une puissance l-ième dans $\mathbb{F}_q$. Soit $\beta \in \mathbb{F}_q^*$ tel que $\operatorname{sgn}(a) = \beta^l$. On pose $b_n = \beta$. Ensuite, on détermine $b_{n-1}, b_{n-2}, \ldots, b_{n-k}, \ldots$ à l'aide des relations (I.3.2). On pose $b = \sum_{j=-\infty}^{n} b_j T^j$. Alors, $a = b^l$. De plus, toute solution β de l'équation $\operatorname{sgn}(a) = \beta^l$ détermine une et une seule solution b de l'équation $a = b^l$.

Nous pouvons maintenant définir la fonction racine l-ième.

Soit $\mathcal{L} = \{\alpha_1, \dots, \alpha_r\}$. Pour chaque indice $i \in \{1, \dots, r\}$, on choisit $\beta_i \in \mathbb{F}_q^*$ tel que $\alpha_i = \beta_i^l$. Si $a \in \mathbf{K}_\infty^*$ est tel que $\nu(a) \equiv 0 \bmod l$ et $\operatorname{sgn}(a) \in \mathcal{L}$, on désigne par $a^{1/l}$ l'unique élément de $\mathbf{K}_\infty^*$ tel que

$$(a^{1/l})^l = a, \quad \operatorname{sgn}(a^{1/l}) = \beta_i \quad \text{si } \operatorname{sgn}(a) = \alpha_i. \tag{I.3.3}$$

I.4. *L'ordre sur* $\mathbf{R}$. On considère une bijection $i \mapsto \mathcal{X}_i$ de $\{0, \dots, q-1\}$ sur $\mathbb{F}_q$ telle que $\mathcal{X}_0 = 0$. On peut aussi supposer, mais ce n'est pas indispensable, que $\mathcal{X}_1 = 1$. On ordonne $\mathbb{F}_q$ en posant $\mathcal{X}_i < \mathcal{X}_{i+1}$ pour tout $i \in \{0, \dots, q-1\}$. Soit un entier positif n. On écrit n en base q :

$$n = n_0 + n_1 q + \dots + n_s q^s, \quad n_i \in \{0, \dots, q-1\}, \tag{I.4.1}$$

et on pose

$$H_n = \mathcal{X}_{n_0} + \mathcal{X}_{n_1} T + \dots + \mathcal{X}_{n_s} T^s. \tag{I.4.2}$$

L'application $n \mapsto H_n$ est une bijection de $\mathbb{N}$ sur $\mathbf{R}$ telle que

$$m \le n \Rightarrow \deg H_m \le \deg H_n. \tag{I.4.3}$$

On ordonne $\mathbf{R}$ en posant, pour tout entier naturel n,

$$H_n < H_{n+1}. \tag{I.4.4}$$

II. Le théorème. Soit un entier $l \ge 2$ non divisible par la caractéristique p du corps $\mathbb{F}_q$. L'ensemble $\mathcal{L} = \{\alpha_1, \dots, \alpha_r\}$ des puissances l-ièmes de $\mathbb{F}_q^*$ introduit au paragraphe précédent est maintenant indexé suivant l'ordre croissant de $\mathbb{F}_q$.

Un polynôme $K \in \mathbf{R}^*$ admet une racine l-ième dans $\mathbf{K}_\infty^*$ si et seulement si $\deg K \equiv 0 \bmod l$ et $\operatorname{sgn}(K) \in \mathcal{L}$. Soit $\mathbf{L}$ l'ensemble de ces polynômes. Soit (L_n) la suite de ces polynômes, indexée suivant l'ordre croissant de $\mathbf{R}$. Soit $\mathbf{I}$ l'ensemble des polynômes irréductibles de $\mathbb{F}_q[T]$ et soit (P_n) la suite formée par les polynômes de $\mathbf{L} \cap \mathbf{I}$, indexée suivant l'ordre croissant de $\mathbf{R}$.

Dans ce qui suit, à l'aide du critère de Weyl, on démontre le théorème suivant.

THÉORÈME. *La suite* $(L_n^{1/l})$ *est équirépartie modulo* 1. *De plus, pour* $l \ge 3$, *la suite* $(P_n^{1/l})$ *est équirépartie modulo* 1.

II.1. *Le lemme fondamental*

LEMME II.1.1 (Lemme préliminaire). *Soit* k *un entier naturel et soit* $H \in \mathbf{R}^*$. *Soit* $L \in \mathbf{L}$ *de degré* lk. *Alors, pour tout* $Z \in \mathbf{R}$ *tel que* $\deg Z < (l-1)k - \deg H - 1$, *on a*

(i) $(L + Z) \in \mathbf{L}$,
(ii) $\operatorname{Res}(HL^{1/l}) = \operatorname{Res}(H(L+Z)^{1/l})$.

Démonstration. On a $\operatorname{sgn}(L) \in \mathcal{L}$. Soit $Z \in \mathbf{R}$ tel que $\deg Z < (l-1)k - 1 - \deg H$. Alors, $\deg(L+Z) = \deg L = lk$ et $\operatorname{sgn}(L+Z) =$

$\mathrm{sgn}(L)$, d'où le (i). De plus, d'après la définition de la fonction racine l-ième, $\mathrm{sgn}(L^{1/l}) = \mathrm{sgn}((L+Z)^{1/l})$. D'autre part, on a

$$Z = L + Z - L = ((L+Z)^{1/l})^l - (L^{1/l})^l,$$

d'où

$$Z = ((L+Z)^{1/l} - L^{1/l})\Big(\sum_{j=0}^{l-1}((L+Z)^{1/l})^j (L^{1/l})^{l-1-j}\Big). \tag{1}$$

Pour tout $j \in \{0, \dots, l-1\}$, on a

$$\nu(((L+Z)^{1/l})^j (L^{1/l})^{l-1-j}) = -(l-1)k,$$
$$\mathrm{sgn}(((L+Z)^{1/l})^j (L^{1/l})^{l-1-j}) = (\mathrm{sgn}(L^{1/l}))^{l-1},$$

d'où

$$\nu\Big(\sum_{j=0}^{l-1}((L+Z)^{1/l})^j (L^{1/l})^{l-1-j}\Big) = -(l-1)k,$$

et, avec (1), il vient

$$\nu((L+Z)^{1/l} - L^{1/l}) = -\deg Z + (l-1)k \geq 2 + \deg H,$$

d'où

$$\nu(H((L+Z)^{1/l} - L^{1/l})) \geq 2.$$

On conclut avec (I.1.5).

Lemme II.1.2 (Lemme fondamental). *Soit H un polynôme non nul, et soit h son degré. Soit k un entier tel que $(l-1)k \geq h$. Alors, pour tout $\alpha \in \mathcal{L}$, tout $\zeta \in \mathbb{F}_q$, tout $Y \in \mathbf{R}$ de degré $< k+h$, il existe un et un seul élément $\eta = \eta(\alpha, Y)$ dans $\mathbb{F}_q$ tel que pour tout $Z \in \mathbf{R}$ de degré $< (l-1)k - h - 1$, on ait*

$$\zeta = \mathrm{Res}(H(\alpha T^{lk} + YT^{(l-1)k-h} + \eta T^{(l-1)k-h-1} + Z)^{1/l}).$$

Démonstration. Posons $H = a_0 + \ldots + a_h T^h$. Soient $\alpha \in \mathcal{L}$, $\beta = \alpha^{1/l}$, $\zeta \in \mathbb{F}_q$ et $(y_{lk-1}, \dots, y_{(l-1)k-h}) \in \mathbb{F}_q^{k+h}$. Si $u = \sum_{j=-\infty}^{k} u_j T^j$ est un élément de $\mathbf{K}_\infty$, on a

$$\mathrm{Res}(Hu) = a_h u_{-h-1} + a_{h-1} u_{-h} + \ldots + a_0 u_{-1}. \tag{1}$$

Pour $s = 1, \dots, k+h$, on considère la relation (e_s) suivante :

$$y_{lk-s} = l\beta^{l-1} u_{k-s} + \sum_{\substack{i_1+\ldots+i_l = lk-s \\ k-s < i_1 \leq n \\ \cdots\cdots\cdots\cdots \\ n-k < i_l \leq n}} u_{i_1} \ldots u_{i_l}. \tag{e_s}$$

On détermine $u_{k-1}, \dots, u_{-h}$ à l'aide des relations $(e_1), \dots, (e_{k+h})$. Le coefficient a_h étant non nul, il existe un unique élément $u_{-h-1} \in \mathbb{F}_q$ tel que

$$\zeta = a_h u_{-h-1} + a_{h-1} u_{-h} + \ldots + a_0 u_{-1}. \tag{2}$$

Il existe alors un unique élément $\eta = y_{(l-1)k-h-1} \in \mathbb{F}_q$ solution de l'équation (e_{k+h+1}) suivante :

$$y_{(l-1)k-h-1} = l\beta^{l-1}u_{-h-1} + \sum_{\substack{i_1+\ldots+i_l=(l-1)k-h-1 \\ k-s<i_1\le n \\ \cdots\cdots\cdots \\ n-k<i_l\le n}} u_{i_1}\ldots u_{i_l}.$$

Soit

$$K = \alpha T^{lk} + y_{lk-1}T^{lk-1} + \ldots + y_{(l-1)k-h}T^{(l-1)k-h} + \eta T^{(l-1)k-h-1}. \tag{3}$$

Avec (1), (2) et (I.3.2), il vient $\zeta = \mathrm{Res}(HK^{1/l})$, et, d'après le lemme précédent, pour tout $Z \in \mathbf{R}$ de degré $< (l-1)k-h-1$, on a $\zeta = \mathrm{Res}(H(K+Z)^{1/l})$.

Corollaire II.1.3. *Soit H un polynôme non nul. Soit k un entier tel que $(l-1)k \ge \deg H$. Pour tout sous-ensemble $\mathbf{A} \subset \mathbf{R}$ et pour tout $i \in \{1,\ldots,r\}$, soit*

$$\sigma(\mathbf{A};k,i) = \sum_{\substack{A\in\mathbf{A} \\ \deg A = lk \\ \mathrm{sgn}(A)=\alpha_i}} \psi(\mathrm{Res}(HA^{1/l})).$$

Alors,

(a) *si* $\mathbf{A} = \mathbf{L}$, $\sigma(\mathbf{A};k,i) = 0$,
(b) *si* $\mathbf{A} = \mathbf{L}\cap\mathbf{I}$, $|\sigma(\mathbf{A};k,i)| \le (k+\deg H+2)q^{1+\deg H+k(1+l/2)}$.

Démonstration. Posons $h = \deg H$. Pour $\zeta \in \mathbb{F}_q$, soit $\omega(\zeta)$ le nombre de $A \in \mathbf{A}$ tels que

(i) $\deg A = lk$,
(ii) $\mathrm{sgn}(A) = \alpha_i$,
(iii) $\mathrm{Res}(HA^{1/l}) = \zeta$.

Alors,

$$\sigma(\mathbf{A};k,i) = \sum_{\zeta\in\mathbb{F}_q} \psi(\zeta)\omega(\zeta). \tag{1}$$

Pour $Y \in \mathbf{R}$ de degré $< k+h$, soit

$$K(\alpha_i,Y,\zeta) = \alpha_i T^{lk} + YT^{(l-1)k-h} + \eta T^{(l-1)k-h-1}, \tag{2}$$

où $\eta = \eta(\alpha_i,Y)$ est l'élément défini au lemme fondamental tel que

$$\mathrm{Res}(HK(\alpha_i,Y,\zeta)^{1/l}) = \zeta.$$

Soit aussi $a(lk;Y,\zeta)$ le nombre de $A \in \mathbf{A}$ tels que

$$\deg(A - K(\alpha_i,Y,\zeta)) < (l-1)k-h-1. \tag{3}$$

Alors

$$\omega(\zeta) = \sum_{\substack{Y\in\mathbf{R}\\ \deg Y<k+h}} a(lk;Y,\zeta).$$

Si $\mathbf{A}=\mathbf{L}$, $a(lk;Y,\zeta)=q^{(l-1)k-h-1}$, et

$$\sigma(\mathbf{A};k,i) = q^{lk-1}\sum_{\zeta\in\mathbb{F}_q}\psi(\zeta).$$

Le caractère ψ étant non principal, $\sigma(\mathbf{A};k,i)=0$.

On suppose $\mathbf{A}=\mathbf{L}\cap\mathbf{I}$. Alors $a(lk;Y,\zeta)$ est le nombre de polynômes irréductibles P tels que

$$\deg(P-K(\alpha_i,Y,\zeta)) < (l-1)k-h-1.$$

D'après [8], théorème 4,

$$a(lk;Y,\zeta) = \frac{q^{(l-1)k-h-1}}{lk} + e(lk;Y,\zeta),$$

avec

$$|e(lk;Y,\zeta)| \le (k+h+2)q^{lk/2},$$

d'où

$$\sigma(\mathbf{A};k,i) = \frac{q^{lk-1}}{lk}\sum_{\zeta\in\mathbb{F}_q}\psi(\zeta) + \sum_{\zeta\in\mathbb{F}_q}\psi(\zeta)\sum_{\substack{Y\in Z\\ \deg Y<k+h}} e(lk;Y,\zeta),$$

$$|\sigma(\mathbf{A};k,i)| \le q^{k+h+1}(k+h+2)q^{lk/2}.$$

II.2. *Démonstration du théorème*. On désigne par $\mathbf{A}$ l'un de deux ensembles $\mathbf{L}$ ou $\mathbf{L}\cap\mathbf{I}$, (A_n) désigne la suite (L_n) si $\mathbf{A}=\mathbf{L}$, la suite (P_n) si $\mathbf{A}=\mathbf{L}\cap\mathbf{I}$. Dans $\mathbf{R}$, il y a q^m polynômes unitaires de degré m. Soit π_m le nombre de polynômes irréductibles unitaires de $\mathbf{R}$. On a (cf. [6], p. 82)

$$q^m - 2q^{m/2} \le m\pi_m \le q^m. \tag{II.2.1}$$

Dans $\mathbf{A}$, il y a donc a_m polynômes de degré lm, avec

$$a_m = \begin{cases} rq^{lm} & \text{si } \mathbf{A}=\mathbf{L},\\ r\pi_{lm} & \text{si } \mathbf{A}=\mathbf{L}\cap\mathbf{I}, \end{cases} \tag{II.2.2}$$

et il y a b_s polynômes de degré $\le s$, avec

$$b_s = a_1 + \ldots + a_s. \tag{II.2.3}$$

La suite (b_s) est strictement croissante. De plus,

$$b_s = \frac{r(q^{l(s+1)}-q^l)}{q^l-1} \quad \text{si } \mathbf{A}=\mathbf{L}, \tag{II.2.4}$$

et il existe deux constantes strictement positives $\kappa_1 = \kappa_1(q,l)$ et $\kappa_2 = \kappa_2(q,l)$ telles que

$$\kappa_1 \frac{q^{ls}}{s} \le b_s \le \kappa_2 \frac{q^{ls}}{s} \quad \text{si } \mathbf{A} = \mathbf{L} \cap \mathbf{I}. \tag{II.2.5}$$

Soit $H \in \mathbf{R}^*$. Soit

$$h = \deg H. \tag{II.2.6}$$

Soit N un entier assez grand pour que les conditions suivantes soient satisfaites :

$$N > b_{\lceil 1+(h+1)/(l-1)\rceil}, \quad N > N_{h,l}, \tag{II.2.7}$$

$\lceil x \rceil$ désignant le plus petit entier $\ge x$, $N_{h,l}$ étant égal à 0, si $\mathbf{A} = \mathbf{L}$, et tel que l'implication suivante soit vraie :

$$\kappa_2 \frac{q^{lt}}{lt} \ge N_{h,l} \Rightarrow \frac{q^{(l/2-1)t}}{t^2} \ge 4lq^h \quad \text{et} \quad t \ge h+2 \tag{II.2.8}$$

si $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$. Notons que cette implication ne peut avoir lieu que si $l \ge 3$. Dans le cas où $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$, on supposera donc $l \ge 3$.

Soit

$$W(N) = \sum_{n=1}^{N} E(H(A_n)^{1/l}). \tag{II.2.9}$$

Dans ce qui suit, une somme portant sur l'ensemble vide sera supposée nulle.

Il existe un et un seul entier t tel que

$$b_{t-1} \le N < b_t. \tag{II.2.10}$$

On pose

$$S_1 = \sum_{n=1}^{b_{t-1}} E(H(A_n)^{1/l}). \tag{II.2.11}$$

Si $N > b_{t-1}$, il existe un unique entier $s \in \{0, \dots, r-1\}$ tel que

$$1 + b_{t-1} + sa_t \le N \le b_{t-1} + (s+1)a_t. \tag{II.2.12}$$

On pose

$$S_2 = \sum_{j=0}^{s-1} \sum_{n=1+b_{t-1}+ja_t}^{b_{t-1}+(j+1)a_t} E(H(A_n)^{1/l}) \quad \text{si } N < b_{t-1} + (s+1)a_t, \tag{II.2.13}$$

$$S_2 = \sum_{j=0}^{s} \sum_{n=1+b_{t-1}+ja_t}^{b_{t-1}+(j+1)a_t} E(H(A_n)^{1/l}) \quad \text{si } N = b_{t-1} + (s+1)a_t. \tag{II.2.14}$$

Enfin, si $N < b_{t-1} + (s+1)a_t$, on pose

$$S_3 = \sum_{n=1+b_{t-1}+sa_t}^{N} E(H(A_n)^{1/l}). \tag{II.2.15}$$

Trivialement, on a

$$W(N) = S_1 + S_2 + S_3. \tag{II.2.16}$$

PROPOSITION II.2.1. (a) *Si* $\mathbf{A} = \mathbf{L}$, *on a*

$$S_2 = 0, \quad |S_1| \le q^{1+h/(l-1)}.$$

(b) *Si* $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$, *on a*

$$|S_1| \le r(t+h+1)q^{h+t(1+l/2)} + q^{1+h/(l-1)}, \quad |S_2| \le r(t+h+2)q^{1+h+t(1+l/2)}.$$

D é m o n s t r a t i o n. La somme S_1 porte sur les polynômes $A \in \mathbf{A}$ de degré $\le l(t-1)$, la somme S_2, lorsqu'elle n'est pas vide, porte soit sur les polynômes $A \in \mathbf{A}$ de degré lt tels que $\operatorname{sgn}(A) \in \{\alpha_1, \dots, \alpha_{s-1}\}$ si $N < b_{t-1} + (s+1)a_t$, soit sur les polynômes $A \in \mathbf{A}$ de degré lt tels que $\operatorname{sgn}(A) \in \{\alpha_1, \dots, \alpha_s\}$ si $N = b_{t-1} + (s+1)a_t$. Donc

$$S_1 = \sum_{\substack{A \in \mathbf{A} \\ (l-1)\deg A \le h}} E(HA^{1/l}) + \sum_{\substack{k \le t-1 \\ (l-1)k > h}} \sum_{i=1}^{r} \sum_{\substack{A \in \mathbf{A} \\ \deg A = lk \\ \operatorname{sgn}(A) = \alpha_i}} E(HA^{1/l}).$$

La première somme est majorée par $q^{1+h/(l-1)}$. D'après le corollaire au lemme fondamental, si $\mathbf{A} = \mathbf{L}$, la deuxième somme vaut 0 et, si $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$, la deuxième somme est majorée par

$$\sum_{\substack{k \le t-1 \\ (l-1)k > h}} \sum_{i=1}^{r} (k+h+2)q^{1+h+k+kl/2} \le r(t+h+1)q^{h+t(1+l/2)}.$$

La somme S_2 se traite de même.

PROPOSITION II.2.2. (a) *Si* $\mathbf{A} = \mathbf{L}$, *on a*

$$|S_3| \le q^{(l-1)t-h}.$$

(b) *Si* $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$, *on a*

$$|S_3| \le 2q^{(l-1)t-h} + (t+h+2)q^{t+tl/2+h}.$$

D é m o n s t r a t i o n. Nous supposerons $N < b_{t-1} + (s+1)a_t$, car, sinon, il n'y a rien à démontrer. Posons

$$j = 1 + sa_t + b_{t-1}. \tag{1}$$

Alors, avec (II.2.15),

$$S_3 = \sum_{n=j}^{N} E(H(A_n)^{1/l}),$$

d'où

$$|S_3| \le N - j + 1. \tag{2}$$

Les polynômes A_i intervenant dans S_3 s'écrivent

$$A_i = \alpha_i T^{lt} + H_{n_i}, \quad j \le i \le N,$$

la suite (H_{n_i}) étant strictement croissante dans $\mathbf{R}$. On écrit n_N en base q :

$$n_N = c_0 + c_1 q^t + \ldots + c_m q^m. \tag{3}$$

On distingue deux cas.

Premier cas : $m \le (l-1)t - h - 1$. La suite (H_n) étant indexée suivant l'ordre croissant, la suite (n_i) est aussi strictement croissante, d'où

$$N - j \le n_N - n_j \le n_N \le q^{m+1} - 1,$$

et, avec (2),

$$|S_3| \le q^{(l-1)t-h}. \tag{4}$$

Deuxième cas : $m > (l-1)t - h - 1$. On a

$$H_{n_N} = \mathcal{X}_{c_0} + \mathcal{X}_{c_1} T + \ldots + \mathcal{X}_{c_m} T^m.$$

Les polynômes H_{n_i} intervenant dans la somme S_3 sont de la forme

$$H_{n_i} = y_0 + y_1 T + \ldots + y_m T^m \le \mathcal{X}_{c_0} + \mathcal{X}_{c_1} T + \ldots + \mathcal{X}_{c_m} T^m.$$

Soit $\mathcal{Y}$ l'ensemble des polynômes

$$Y = y_{(l-1)t-h} + y_{(l-1)t-h+1} T + \ldots + y_m T^{m-(l-1)t+h}$$

tels que pour tout polynôme $W \in \mathbf{R}$ de degré $< (l-1)t - h$, on ait

$$Y T^{(l-1)t-h} + W \le H_{n_N}.$$

Soit μ le plus grand des indices $i \in \{j, \ldots, N\}$ pour lesquels A_i s'écrive

$$A_i = \alpha_s T^{lt} + Y T^{(l-1)t-h} + W,$$

avec $Y \in \mathcal{Y}$ et $W \in \mathbf{R}$ vérifiant $\deg W < (l-1)t - h$. On pose alors

$$S_4 = \sum_{i=j}^{\mu} E(H(A_i)^{1/l}), \tag{5}$$

$$S_5 = \sum_{i=\mu+1}^{N} E(H(A_i)^{1/l}). \tag{6}$$

On a

$$S_3 = S_4 + S_5. \tag{7}$$

On procède comme pour le corollaire au lemme fondamental. On a

$$S_4 = \sum_{\zeta \in \mathbb{F}_q} \psi(\zeta)\omega(\zeta),$$

où, pour $\zeta \in \mathbb{F}_q$, $\omega(\zeta)$ désigne le nombre de couples (Y, W) tels que

(i) $Y \in \mathcal{Y}$,
(ii) $W \in \mathbf{R}$, $\deg W < (l-1)t - h$,
(iii) $(\alpha_s T^{lt} + YT^{(l-1)t-h} + W) \in \mathbf{A}$,
(iv) $\mathrm{Res}(H(\alpha T^{lt} + YT^{(l-1)t-h} + W)^{1/l}) = \zeta$.

Ici encore

$$\omega(\zeta) = \sum_{Y \in \mathcal{Y}} a(lt; Y, \zeta),$$

où $a(lt; Y, \zeta)$ désigne toujours le nombre de $A \in \mathbf{A}$ tels que

$$\deg(A - K(\alpha_i, Y, \zeta)) < (l-1)t - h - 1,$$

avec

$$K(\alpha_i, Y, \zeta) = \alpha_i T^{lt} + YT^{(l-1)t-h} + \eta(\alpha_i, Y)T^{(l-1)t-h-1},$$

$\eta(\alpha_i, Y)$ étant l'élément défini au lemme fondamental. On obtient

$$S_4 = 0 \quad \text{si } \mathbf{A} = \mathbf{L}. \tag{8}$$

On suppose $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$. Alors,

$$|S_4| \leq \#(\mathcal{Y})(t + h + 2)q^{tl/2},$$

d'où

$$|S_4| \leq (t + h + 2)q^{t(l/2+1)+h} \quad \text{si } \mathbf{A} = \mathbf{L} \cap \mathbf{I}. \tag{9}$$

Trivialement, si S_5 n'est pas la somme vide,

$$|S_5| \leq N - \mu. \tag{10}$$

Dans l'écriture de n_N en base q, soit τ le plus petit indice $> (l-1)t - h$ tel que $c_\tau \neq 0$. En fait,

$$n_N = c_m q^m + c_{m-1}q^{m-1} + \ldots + c_\tau q^\tau + c_{(l-1)t-h-1}q^{(l-1)t-h-1} + \ldots + c_0.$$

Tout polynôme

$$A = \alpha_s T^{lt} + y_m T^m + y_{m-1}T^{m-1} + \ldots + y_\tau q^\tau + y_{\tau-1}q^{\tau-1} + \ldots + y_0,$$

dont les coefficients (y_i) vérifient les conditions $(\mathcal{C})$ suivantes :

$$(\mathcal{C}) \qquad y_m \leq \mathcal{X}_{c_m}, \quad y_{m-1} \leq \mathcal{X}_{c_{m-1}}, \ \ldots, \ y_{\tau+1} \leq \mathcal{X}_{c_{\tau+1}}, \quad y_\tau < \mathcal{X}_{c_\tau},$$

appartient à l'ensemble $\mathbf{L}$ et est inférieur à A_{n_N}. Dans le cas où $\mathbf{A} = \mathbf{L}$, on a donc

$$n_\mu \geq c_m q^m + c_{m-1}q^{m-1} + \ldots + (c_\tau - 1)q^\tau + (q-1)q^{\tau-1} + \ldots + (q-1),$$
$$n_\mu \geq n_N - q^{(l-1)t-h}.$$

Supposons $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$. D'après [8], théorème 4, pour tout polynôme

$$Y = \alpha_s T^{lt} + y_m T^m + y_{m-1}T^{m-1} + \ldots + y_\tau q^\tau + \ldots + y_{(l-1)t-h}T^{(l-1)t-h}$$

dont les coefficients (y_i) vérifient les conditions $(\mathcal{C})$, il existe

$$\mathit{\Pi}(lt; Y, (l-1)t-h) = \frac{q^{(l-1)t-h}}{lt} + \varrho(lt; Y, (l-1)t-h)$$

polynômes irréductibles $P \in \mathbf{R}$ tels que $\deg(P - Y) < (l-1)t - h$ avec

$$|\varrho(lk; Y, (l-1)t-h)| \leq (t+h+2)q^{lt/2}.$$

De tels polynômes P appartiennent à $\mathbf{L} \cap \mathbf{I} = \mathbf{A}$. On a supposé $N > N_{l,h}$. On a donc

$$\frac{q^{(l-1)t-h}}{lt} \geq 4tq^{lt/2} \geq 2(t+h+2)q^{lt/2},$$
$$\mathit{\Pi}(lt; Y, (l-1)t-h) \geq q^{(l-1)t-h}/(2lt) \geq 1.$$

Ici,

$$n_\mu \geq c_m q^m + c_{m-1}q^{m-1} + \ldots + (c_\tau - 1)q^\tau + (q-1)q^{\tau-1} + \ldots + (q-1)q^{(l-1)t-h},$$
$$n_\mu \geq n_N - 2q^{(l-1)t-h} + 1.$$

D'où

$$N - \mu \leq \begin{cases} q^{(l-1)t-h} & \text{si } \mathbf{A} = \mathbf{L}, \\ 2q^{(l-1)t-h} - 1 & \text{si } \mathbf{A} = \mathbf{L} \cap \mathbf{I}. \end{cases}$$

On conclut avec (4), (7)–(10).

Proposition II.2.3. *On a*

$$\text{(II.2.17)} \qquad \left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll N^{-1/l} \quad \textit{si } \mathbf{A} = \mathbf{L},$$

$$\text{(II.2.18)} \qquad \left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll (\log N)^{3/2+1/l} N^{1/l-1/2}$$
$$\textit{si } \mathbf{A} = \mathbf{L} \cap \mathbf{I} \textit{ et si } 3 \leq l \leq 4,$$

$$\text{(II.2.19)} \qquad \left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll (\log N)^{1-1/l} N^{-1/l}$$
$$\textit{si } \mathbf{A} = \mathbf{L} \cap \mathbf{I} \textit{ et si } l > 5,$$

les constantes impliquées par le symbole $\ll$ ne dépendant que de q et de l.

Démonstration. On se place d'abord dans le cas $\mathbf{A} = \mathbf{L}$. Avec (II.2.9), (II.2.16), les propositions II.2.1 et II.2.2, il vient

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \le \frac{1}{N}(q^{(l-1)t-h} + q^{1+h/(l-1)}),$$

puis, avec (II.2.10) et (II.2.4), on a

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \le \frac{(q^{(l-1)t-h} + q^{1+h/(l-1)})(q^l-1)}{r(q^{lt}-q^l)},$$

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll q^{-t} \ll N^{-1/l},$$

d'où (II.2.17).

On se place maintenant dans le cas $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$. Il vient alors

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right|$$
$$\le \frac{1}{N}(q^{1+h/(l-1)} + (2r+1)(t+h+2)q^{1+h+t(1+l/2)} + 2q^{(l-1)t-h}).$$

Les relations (II.2.10) et (II.2.5) donnent alors

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll \frac{t^2 q^{t(1+l/2)} + tq^{(l-1)t}}{q^{lt}}.$$

Pour $l \le 4$,

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll t^2 q^{t(1-l/2)},$$

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll (\log N)^{3/2+1/l} N^{1/l-1/2},$$

d'où (II.2.18). Pour $l > 4$,

$$\left|\frac{1}{N}\sum_{n=1}^{N} E(H(A_n)^{1/l})\right| \ll tq^{-t} \ll (\log N)^{1-1/l} N^{-1/l},$$

d'où (II.2.19).

Le critère de Weyl, théorème I.2.2, nous donne alors le résultat annoncé.

Dans le cas $\mathbf{A} = \mathbf{L} \cap \mathbf{I}$, la restriction $l \ge 3$ provient du fait suivant. Dans la démonstration intervient en fait le nombre $I(lk; y_{lk}, y_{(l-1)k-1}, \dots, y_{(l-1)k-h-1})$ de polynômes irréductibles P de degré lk,

$$P = y_{lk}T^{lk} + y_{lk-1}T^{lk-1} + \ldots + y_{(l-1)k-1}T^{(l-1)k-1} + \ldots$$
$$\ldots + y_{(l-1)k-h-1}T^{(l-1)k-h} + \ldots + y_0,$$

dont les coefficients $y_{lk}, y_{(l-1)k-1}, \ldots, y_{(l-1)k-h-1}$ sont fixés. Aucune approximation de ce nombre n'étant connue, on utilise un théorème de répartition des polynômes irréductibles qui donne le nombre $\Pi(lk, Y, lk-h-1)$ de polynômes irréductibles P de degré lk, de la forme

$$P = Y + y_{(l-1)k-h-2}T^{(l-1)k-h-2} + \ldots + y_0,$$

dont les coefficients $y_{lk}, y_{lk-1}, \ldots, y_{(l-1)k-1}, \ldots, y_{(l-1)k-h-1}$ sont fixés. Ceci introduit un terme d'erreur d'ordre $kq^{k+lk/2}$ plus grand que l'ordre du terme principal lorsque $l = 2$.

On pourrait penser établir pour le nombre $I(lk; y_{lk}, y_{(l-1)k-1}, \ldots$ $\ldots, y_{(l-1)k-h-1})$ un théorème analogue aux théorèmes établis dans [8] ou [5] pour les nombres $\Pi(lk; Y, lk-h-1)$. Mais cela semble être un problème très difficile.

Bibliographie

[1] L. Carlitz, *Diophantine approximations in fields of characteristic p*, Proc. Amer. Math. Soc. 3 (1952), 187–208.

[2] A. Dijksma, *Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$*, part I, Nederl. Akad. Wetensch. Proc. Ser. A 72 (1969), 376–383.

[3] —, *Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$*, part II, ibid. 73 (1970), 187–195.

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

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

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

[7] D. de Mathan, *Approximations diophantiennes dans un corps local*, Bull. Soc. Math. France Mém. 21 (1970).

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

LABORATOIRE DE MATHÉMATIQUES
CASE 322
FACULTÉ DES SCIENCES DE SAINT-JÉRÔME
AVENUE ESCADRILLE NORMANDIE-NIEMEN
13397 MARSEILLE CEDEX 20, FRANCE

Reçu le 19.7.1993 (2463)