ACTA ARITHMETICA
XLIV (1984)

Ensembles de polynômes irréductibles et théorèmes de densité

par

MIREILLE CAR (Marseille)

I. Introduction. Soit $\boldsymbol{F}_q$ le corps fini à q éléments. Soit $\mathscr{U}$ l'ensemble des polynômes unitaires de l'anneau $\boldsymbol{F}_q[X]$ des polynômes à une variable sur le corps $\boldsymbol{F}_q$. Soit I un ensemble de polynômes irréductibles unitaires de $\boldsymbol{F}_q[X]$, $\mathscr{U}(I)$, resp. $\mathscr{Q}(I)$, l'ensemble des polynômes de $\mathscr{U}$, resp. l'ensemble des polynômes sans facteur carré de $\mathscr{U}$, dont tous les facteurs irréductibles sont dans I. On cherche une estimation asymptotique du nombre $a(n, I)$, resp. $b(n, I)$, de polynômes de degré n de $\mathscr{U}(I)$, resp. $\mathscr{Q}(I)$. Pour des commodités d'écriture, on admettra que le polynôme 1 appartient à l'ensemble $\mathscr{Q}(I)$ quel que soit l'ensemble I, de ce fait, on aura toujours

$$a(0, I) = b(0, I) = 1.$$

On ne peut espérer une estimation des nombres $a(n, I)$ et $b(n, I)$ qui soit valable dans tous les cas comme le montrent les deux exemples extrêmes suivants. Si P est l'ensemble de tous les polynômes irréductibles, on a

$$a(n, P) = q^n \quad \text{pour tout entier } n \geqslant 0,$$

$$b(n, P) = \begin{cases} q^n & \text{si } n \in \{0, 1\}, \\ (1-1/q)\,q^n & \text{pour tout entier } n \geqslant 2. \end{cases}$$

Si I est réduit à un seul polynôme irréductible P de degré d, on a

$$a(n, I) = \begin{cases} 0 & \text{si } d \text{ ne divise pas } n, \\ 1 & \text{si } d \text{ disive } n, \end{cases}$$

$$b(n, I) = \begin{cases} 0 & \text{si } n \neq d, \\ 1 & \text{si } n = d. \end{cases}$$

On verra que lorsque l'ensemble I vérifie certaines conditions de régularité on a une estimation asymptotique des nombres $a(n, I)$ et $b(n, I)$. Ces conditions sont de deux types. Le premier type de conditions correspond à une généralisation d'un théorème de Delange, [1], [5], aux polynômes de

$F_q[X]$, le deuxième type de conditions correspond à des conditions de régularité pour les degrés des polynômes de I. On aura aussi une généralisation de ces deux types de conditions.

Les estimations des nombres $a(n, I)$ et $b(n, I)$ sont basées sur des estimations auxilliaires de coefficients de séries entières, estimations qui seront données en annexe à la fin de ce travail.

II. Notations, conventions et rappels. Dans ce qui suit, le mot polynôme désignera toujours un polynôme unitaire de $F_q[X]$.

Si H est un tel polynôme, on note $d^\circ H$ le degré de H et $\Phi(H)$ le nombre de classes de congruence inversibles modulo H. Si A est un ensemble de polynômes, on note $A(n)$ le nombre de polynômes de degré n de A. Ainsi le nombre de polynômes irréductibles de degré n sera noté $P(n)$. Rappelons ici deux relations vérifiées par les nombres $P(n)$:

$$q^n = \sum_{d|n} dP(d), \tag{II.1}$$

d'où,

$$nP(n) = \sum_{d|n} \mu(d)\, q^{n/d}, \tag{II.2}$$

μ désignant la fonction de Möbius, ou encore,

$$nP(n) = q^n - e(n), \tag{II.3}$$

avec

$$0 \leqslant e(n) \leqslant 2q^{n/2}. \tag{II.4}$$

Soit un nombre réel $r > 0$. L'ensemble des nombres complexes z tels que $|z| < r$, resp. $|z| \leqslant r$, sera noté D_r, resp. $\bar{D}_r$.

Si F est un ensemble fini, on note $\langle F \rangle$ le nombre d'éléments de F.

III. Les séries génératrices. Soit I un ensemble de polynômes irréductibles. Les nombres $a(n, I)$ et $b(n, I)$ sont majorés par q^n. Les séries

$$f_I(z) = \sum_{n=0}^{\infty} a(n, I)(z/q)^n, \tag{III.1}$$

$$g_I(z) = \sum_{n=0}^{\infty} b(n, I)(z/q)^n \tag{III.2}$$

sont absolument convergentes dans le disque D_1. Si $z \in D_1$, on a

$$f_I(z) = \sum_{H \in \mathscr{U}(I)} (z/q)^{d^\circ H} \quad \text{et} \quad g_I(z) = \sum_{H \in \mathscr{D}(I)} (z/q)^{d^\circ H}.$$

Les fonctions caractéristiques des ensembles $\mathscr{U}(I)$ et $\mathscr{D}(I)$ sont multiplicatives. Pour $z \in D_1$, les sommes $f_I(z)$ et $g_I(z)$ se développent en produits eulériens absolument convergents

$$f_I(z) = \prod_{P \in I} (1-(z/q)^{d^\circ P})^{-1}, \quad g_I(z) = \prod_{P \in I} (1+(z/q)^{d^\circ P})$$

d'où,

$$g_I(z) = \frac{f_I(z)}{f_I(z^2/q)}, \tag{III.3}$$

et,

$$\log\{f_I(z)\} = \sum_{P \in I} \{(z/q)^{d^\circ P} + \sum_{k=2}^{\infty} (z/q)^{kd^\circ P}/k\}. \tag{III.4}$$

IV. Ensembles de densite. Nous introduisons ici plusieurs notions de densité pour les ensembles de polynômes irréductibles, ces notions n'étant pas indépendantes les unes des autres.

Soit I un ensemble de polynômes irréductibles.

DÉFINITION IV.1. L'ensemble I est dit *de densité* $d \in [0, 1]$, si l'on a, pour n tendant vers $+\infty$,

$$I(n) = dP(n) + o(P(n)). \tag{IV.1}$$

L'ensemble P de tous les polynômes irréductibles est ainsi de densité 1.

DÉFINITION IV.2. L'ensemble I est dit *régulier de densité d au sens de Delange*, s'il existe une fonction h holomorphe dans le disque fermé $\bar{D}_1$ telle que, pour tout $z \in D_1$ on ait,

$$\sum_{P \in I} (z/q)^{d^\circ P} = d \log\left(\frac{1}{1-z}\right) + h(z). \tag{IV.2}$$

Dans de nombreux cas on a une approximation de $I(n)$ plus précise que celle donnée par la relation (IV.1), ce qui conduit aux définitions suivantes:

DÉFINITION IV.3. Soient $d \in [0, 1]$ et $\delta \in]0, 1[$. L'ensemble I est dit *de densité d avec une approximation d'ordre* δ, si on a, pour n tendant vers $+\infty$,

$$I(n) = d\,\frac{q^n}{n} + O\left(\frac{q^{\delta n}}{n}\right), \tag{IV.3}$$

les constantes impliquées par le symbole O ne dépendant que de I.

DÉFINITION IV.4. Soient $d \in [0, 1]$ et $R \in]1, +\infty[$. L'ensemble I est dit *R-régulier de densité d*, s'il existe une fonction h holomorphe sur le disque D_R, telle que pour $z \in D_1$ on ait,

$$\sum_{P \in I} (z/q)^{d^\circ P} = d \log\left(\frac{1}{1-z}\right) + h(z). \tag{IV.4}$$

Si I est de densité d avec une approximation d'ordre $\delta \in]0, 1[$, I est de densité d avec une approximation d'ordre γ, pour tout $\gamma \in [\delta, 1[$ et, de même, si I est R-régulier de densité d, I est r-régulier de densité d pour tout $r \in]1, R]$.

PROPOSITION IV.1. *L'ensemble P de tous les polynômes irréductibles est de densité 1 avec une approximation d'ordre 1/2.*

Démonstration. Immédiate avec (II.3) et (II.4).

La proposition suivante donne les relations existant entre les différents type de densité introduits plus haut.

PROPOSITION IV.2. *Soit I une ensemble de polynômes irréductibles.*

(1) *Si pour $d \in [0, 1]$, $\delta \in]0, 1[$, I est de densité d avec une approximation d'ordre δ, I est de densité d.*

(2) *Si pour $d \in [0, 1]$, $R \in]1, +\infty[$, I est R-régulier de densité d, I est régulier de densité d.*

(3) *Si I est régulier de densité d, I est de densité d.*

(4) *Soit $d \in [0, 1]$. Alors, il existe $\delta \in]0, 1[$ tel que l'ensemble I soit de densité d avec une approximation d'ordre δ si et seulement si il existe $R \in]1, q]$ tel que I soit R-régulier de densité d.*

Démonstration. (a) Le deuxième point est immédiat. Avec (II.3) et (II.4) le premier point l'est tout autant.

(b) On suppose I régulier de densité d. La relation (IV.2) s'écrit

$$\sum_{n=1}^{\infty} I(n)(z/q)^n = d \sum_{n=1}^{\infty} z^n/n + \sum_{n=1}^{\infty} h_n z^n,$$

où $\sum_{n=1}^{\infty} h_n z^n$ est le développement en série de Taylor au voisinage de zéro de la fonction h. On en déduit

$$\text{(i)} \qquad I(n) = d\,\frac{q^n}{n} + n h_n \frac{q^n}{n},$$

d'où, avec (II.3) et (II.4)

$$I(n) = dP(n) + O\left(\frac{q^{n/2}}{n} + \frac{q^n}{n}(nh_n)\right).$$

La fonction h étant holomorphe dans le disque fermé $\bar{D}_1$,

$$nh_n \in o(1),$$

et la relation (IV.1) est vérifiée.

Si on suppose de plus que I est R-régulier de densité d, la fonction h est alors holomorphe dans le disque D_R et, pour tout $r \in]1, R[$,

$$nh_n \in o(r^{-n}),$$

et avec (i) on a

$$I(n) = d\,\frac{q^n}{n} + O\left(\frac{1}{n}\left(\frac{q}{r}\right)^n\right),$$

et la relation (IV.3) est vérifiée avec $\delta = 1 - \log r/\log q$.

(c) On suppose I de densité d avec une approximation d'ordre $\delta \in]0, 1[$. Alors, on a

$$I(n) = d\,q^n/n + \varrho(n) \qquad \text{avec} \qquad \varrho(n) \in O(q^{\delta n}/n),$$

d'où,

$$\sum_{P \in I} (z/q)^{d^\circ P} = \sum_{n=1}^{\infty} I(n)(z/q)^n = d \log\left(\frac{1}{1-z}\right) + \sum_{n=1}^{\infty} \varrho(n)(z/q)^n.$$

La série

$$\sum_{n=1}^{\infty} \varrho(n)(z/q)^n$$

est absolument convergente dans le disque $D_{q^{1-\delta}}$ et sa somme est holomorphe dans ce disque.

Donnons quelques exemples d'ensembles de polynômes irréductibles ayant une densité.

PROPOSITION IV.3. *Soit F un ensemble fini de polynômes irréductibles. Alors, pour tout $\delta \in]0, 1[$, F est de densité 0 avec une approximation d'ordre δ.*

Démonstration. Si $n > \sup_{P \in F} \{d^\circ P\}$, $F(n) = 0$, et (3) est vérifiée.

PROPOSITION IV.4. *Soient I et J des ensembles de polynômes irréductibles tels que $I \subset J$. Soit I' le complémentaire de I dans J.*

(1) *Si I et J sont de densités respectives d et u, alors I' est de densité $u-d$.*

(2) *Si I et J sont réguliers de densités respectives d et u, alors I' est régulier de densité $u-d$.*

(3) *Si I est de densité d avec une approximation d'ordre δ, si J est de densité u avec une approximation d'ordre γ, alors I' est de densité $u-d$ avec une approximation d'ordre $\sup(\delta, \gamma)$.*

(4) *Si I est R-régulier de densité d, si J est r-régulier de densité u, alors I' est R'-régulier de densité $u-d$ avec $R' = \inf(r, R)$.*

Démonstration. Immédiate.

COROLLAIRE. *Si F est un ensemble fini de polynômes irréductibles, le complémentaire de F dans l'ensemble P est de densité 1 avec l'approximation δ, quel que soit $\delta \in]0, 1[$.*

Remarque: Les ensembles finis de polynômes irréductibles ne sont pas les seuls ensembles de densité 0. Par exemple, on choisit pour tout entier $n \geqslant 4$, $I(n) = [q^{n/2} n^{-1}]$ polynômes irréductibles de degré n, ce qui est possible en raison de (II.2), et la réunion de ces polynômes irréductibles donne un ensemble de densité 0 avec une approximation d'ordre 1/2.

PROPOSITION IV.5. *Soient H un polynôme différent de 1 et L un polynôme premier à H. Alors, l'ensemble $I(H, L)$ des polynômes irréductibles congrus à L modulo H est de densité $1/\Phi(H)$ avec une approximation d'ordre 1/2.*

Démonstration. Le théorème 4 de [3] nous donne

$$\left| I(H, L)(n) - \frac{q^n}{n\Phi(H)} \right| \leqslant (1 + d^\circ H)\, q^{n/2}.$$

Le résultat principal de ce paragraphe est le théorème suivant analogue au théorème 21 de [1].

THÉORÈME 1. (1) *Soit I un ensemble de polynômes irréductibles régulier de densité $d \in]0, 1[$. Alors, il existe des constantes $A(I)$ et $B(I)$, ne dépendant que de I, telles que pour n tendant vers $+\infty$, on ait*

$$a(n, I) = A(I)\, q^n n^{d-1} + O(q^n n^{d-2}),$$

$$b(n, I) = B(I)\, q^n n^{d-1} + O(q^n n^{d-2}),$$

les constantes impliquées par les symboles O ne dépendant que de I.

(2) *Soit I un ensemble de polynômes irréductibles régulier de densité 1. Alors, il existe des constantes $A(I)$ et $B(I)$, ne dépendant que de I, telles que, pour tout entier $k > 0$, pour n tendant vers $+\infty$, on ait*

$$a(n, I) = A(I)\, q^n + o(q^n n^{-k}),$$

$$b(n, I) = B(I)\, q^n + o(q^n n^{-k}).$$

(3) *Soit I un ensemble de polynômes irréductibles régulier de densité 0. Alors, pour tout entier $k > 0$, pour n tendant vers $+\infty$, on a*

$$a(n, I) \in o(q^n n^{-k}),$$

$$b(n, I) \in o(q^n n^{-k}).$$

Démonstration. Posons

$$F(z) = f_I(z) \quad \text{et} \quad G(z) = g_I(z),$$

les fonctions f_I et g_I étant définies comme au paragraphe III.

La série

$$\sum_{P \in I} \sum_{k=2}^{\infty} \frac{1}{k} \left(\frac{z}{q}\right)^{k d^\circ P}$$

est absolument convergente dans le disque $D_{\sqrt{q}}$. La fonction

$$z \mapsto u(z) = \sum_{P \in I} \sum_{k=2}^{\infty} \frac{1}{k} \left(\frac{z}{q}\right)^{d^\circ P}$$

est holomorphe dans $D_{\sqrt{q}}$. On applique la relation (IV.2)

$$\log(F(z)) = d \log(1/(1-z)) + h(z) + u(z)$$

d'où,

(i) $$F(z) = H(z)(1-z)^{-d}, \quad \text{avec} \quad H(z) = \exp(h(z) + u(z)).$$

La fonction H est holomorphe dans le disque fermé $\bar{D}_1$ et ne s'annule pas sur ce disque. La relation (III.3) nous donne

(ii) $$G(z) = \{H(z)(1-z^2/q)^d / H(z^2/q)\}\,(1-z)^{-d}.$$

La fonction

$$z \mapsto K(z) = H(z)(1-z^2/q)^d\, H(z^2/q)^{-1}$$

est elle aussi holomorphe dans le disque fermé $\bar{D}_1$.

On applique alors la proposition A.1. Avec (III.1) et (III.2) il vient

$$a(n, I) q^{-n} = \begin{cases} H(1) n^{d-1}/\Gamma(d) + O(n^{d-2}) & \text{si} \quad d \in]0, 1[, \\ H(1) + o(n^{-k}) & \text{si} \quad d = 1, \end{cases}$$

$$b(n, I) q^{-n} = \begin{cases} K(1) n^{d-1}/\Gamma(d) + O(n^{d-2}) & \text{si} \quad d \in]0, 1[, \\ K(1) + o(n^{-k}) & \text{si} \quad d = 1, \end{cases}$$

k étant un entier strictement positif quelconque.

Si $d = 0$, les relations (i) et (ii) s'écrivent

$$F(z) = H(z) \quad \text{et} \quad G(z) = K(z).$$

On a, pour tout entier $k > 0$,

$$a(n, I) q^{-n} \in o(n^{-k}) \quad \text{et} \quad b(n, I) q^{-n} \in o(n^{-k}).$$

V. Polynômes ayant la repartition (h, L, d).

DÉFINITION V.1. Soit un entier $h \geqslant 2$. Pour $k \in \{0, \ldots, h-1\}$, soit I_k l'ensemble des polynômes irréductibles P tels que

$$d^\circ P \equiv k \pmod{h}.$$

Si L est une partie de $\{0, \ldots, h-1\}$, soit

$$J_L = \bigcup_{k \in L} I_k.$$

Un tel ensemble J_L *sera dit de type* (h, L).

Lorsque L est l'ensemble $\{0, \ldots, h-1\}$, $\mathscr{U}(J_L)$, resp. $\mathscr{Q}(J_L)$, est l'ensemble de tous les polynômes unitaires, resp. de tous les polynômes unitaires sans facteur carré, et les nombres $a(n, J_L)$ et $b(n, J_L)$ sont connus. Si $L = \emptyset$, $J_L = \emptyset$ et les nombres $a(n, J_L)$ et $b(n, J_L)$ sont connus. Nous allons établir une estimation des nombres $a(n, J_L)$ et $b(n, J_L)$ dans le cas général. Cette estimation se déduira de l'estimation des nombres $a(n, J)$ et $b(n, J)$ faite pour des ensembles J qui généralisent les ensembles de type (h, L).

DÉFINITION V.2. Soient un entier $h \geqslant 2$ et L une partie de l'ensemble $\{0, \ldots, h-1\}$. Soit $d \in [0, 1]$. On dit qu'un ensemble I de polynômes irréductibles admet la répartition (h, L, d) s'il existe $\delta \in]0, 1[$ tel que

(V.1) pour tout entier $n > 0$, congru modulo h à un élément de L, on ait

$$I(n) = d\,q^n/n + O\left(\frac{q^{\delta n}}{n}\right);$$

(V.2) pour tout entier $n > 0$, non congru modulo h à élément de L, on ait,

$$I(n) \in O\left(\frac{q^{\delta n}}{n}\right),$$

les constantes impliquées par les symboles O ne dépendant que de I.

Si L est la partie vide, et si I admet la répartition (h, L, d), I est de densité 0, avec une certaine approximation d'ordre δ. Si $L = \{0, \ldots, h-1\}$, et si I admet la répartition (h, L, d), I est de densité d avec une certaine approximation d'ordre δ. Un ensemble de type (h, L) admet la répartition $(h, L, 1)$.

Comme pour la proposition IV.5, on démontre la proposition suivante:

PROPOSITION V.1. *Soient H un polynôme différent de 1 et L un polynôme premier à H. Soient un entier $h \geqslant 2$ et K une partie non vide de $\{0, \ldots, h-1\}$. Alors, l'ensemble des polynômes irréductibles P tels que*

(i) *P est congru à L modulo H,*

(ii) *$d^\circ P$ est congru à un élément de K modulo h,*

admet la répartition $(h, K, 1/\Phi(H))$.

Le théorème suivant donne une estimation des nombres $a(n, I)$ et $b(n, I)$ lorsque I admet la répartition (h, L, d). L'hypothèse $L \neq \{0, \ldots, h-1\}$ faite dans ce théorème n'est pas indispensable, le théorème restant vrai pour $L = \{0, \ldots, h-1\}$, mais donnant des résultats moins bons, notemment en ce qui concerne le terme d'erreur, que les résultats obtenus directement à l'aide du théorème 1.

THÉORÈME 2. *Soient un entier $h \geqslant 2$, L une partie non vide de $\{0, \ldots, h-1\}$ distincte de $\{0, \ldots, h-1\}$. Soit $d \in [0, 1]$. Soit I un ensemble de polynômes irréductibles admettant la répartition (h, L, d). Soit*

$$\varrho = \cos(2\pi/h) + i \sin(2\pi/h).$$

Pour $k \in \{0, \ldots, h-1\}$, soit

$$\beta_k = \frac{d}{h} \sum_{l \in L} \varrho^{-kl}.$$

Alors, il existe des nombres complexes $A_k(I)$ et $B_k(I)$, $0 \leqslant k \leqslant h-1$, ne dépendant que de I tels que

(i) *$A_k(I)$ et $A_{h-k}(I)$ sont conjugués, $1 \leqslant k \leqslant h-1$,*

(ii) *$B_k(I)$ et $B_{h-k}(I)$ sont conjugués, $1 \leqslant k \leqslant h-1$,*

(iii) *$A_0(I)$ et $B_0(I)$ sont réels,*

(iv) *pour n tendant vers $+\infty$, on a*

$$a(n, I) = \sum_{k=0}^{h-1} A_k(I)\, n^{\overline{\beta_k}-1}\, \varrho^{-kn} q^n + O(q^n n^{d\langle L\rangle/h-2}),$$

$$b(n, I) = \sum_{k=0}^{h-1} B_k(I)\, n^{\overline{\beta_k}-1}\, \varrho^{-kn} q^n + O(q^n n^{d\langle L\rangle/h-2}),$$

d'où, en particulier, si L n'est pas réduit à $\{0\}$,

$$a(n, I) = A_0(I)\, q^n n^{d\langle L\rangle/h-1} + O(q^n n^{d\langle L\rangle\cos(2\pi/h)/h-1}),$$

$$b(n, I) = B_0(I)\, q^n n^{d\langle L\rangle/h-1} + O(q^n n^{d\langle L\rangle\cos(2\pi/h)/h-1}),$$

les constantes impliquées par ces symboles O ne dépendant que de I.

Démonstration. Reprenons les notations du paragraphe III et posons

$$a_n = a(n, I), \quad b_n = b(n, I), \quad f_I = f, \quad g_I = g.$$

Notons L' le complémentaire de L dans $\{0, \ldots, h-1\}$ et posons

$$\varepsilon(L) = \begin{cases} 0 & \text{si} \quad 0 \notin L, \\ 1 & \text{si} \quad 0 \in L. \end{cases}$$

Avec (III.4) on a

$$\log(f(z)) = \sum_{k=0}^{h-1} \sum_{\substack{m \equiv k \pmod h \\ m \neq 0}} I(m) \left[\left(\frac{z}{q}\right)^m + \sum_{s=2}^{\infty} \frac{1}{s} \left(\frac{z}{q}\right)^{ms} \right].$$

Si $j \notin L$ et si n est congru à j modulo h, on pose

$$I(n) = d\,q^n/n + r(n).$$

Alors, avec (V.1) et (V.2) on a

(i) $$\log(f(z)) = du(z) + v(z),$$

avec

(ii) $$u(z) = \sum_{l \in L} \sum_{\substack{m \equiv l \pmod h \\ m \neq 0}} z^m/m,$$

(iii) $$v(z)=\sum_{l\in L}\sum_{\substack{m\equiv l(\mathrm{mod}\,h)\\ m\neq 0}} r(m)(z/q)^m+$$

$$+\sum_{l\in L'}\sum_{\substack{m\equiv l(\mathrm{mod}\,h)\\ m\neq 0}} I(m)(z/q)^m+\sum_{k=0}^{h-1}\sum_{\substack{m\equiv k(\mathrm{mod}\,h)\\ m\neq 0}} I(m)\sum_{s=2}^{\infty}\frac{1}{s}\left(\frac{z}{q}\right)^{sm}.$$

La fonction v est holomorphe dans le disque $|z|<\inf(q^{1/2}, q^{1-\delta})$. La fonction

(iv) $$z\mapsto H(z)=\exp\big(v(z)\big)$$

est holomorphe dans ce disque et ne s'y annule pas.

Si $z\in D_1$,

$$u'(z)=\sum_{\substack{l\in L\\ l\neq 0}} z^{l-1}/(1-z^h)+\varepsilon(L)z^{h-1}/(1-z^h).$$

Alors,

$$u'(z)=\frac{1}{h}\sum_{l\in L}\sum_{j=0}^{h-1}\varrho^{-jl}(1-\varrho^j z)^{-1},$$

et

$$u(z)=\frac{1}{h}\sum_{l\in L}\sum_{j=0}^{h-1}\varrho^{-jl}\log\left(\frac{1}{1-\varrho^j z}\right),$$

$$\exp\big(u(z)\big)=\Big\{\prod_{l\in L}\prod_{j=0}^{h-1}(1-\varrho^j z)^{-\varrho^{-jl}}\Big\}^{1/h},$$

$$\exp\big(du(z)\big)=\prod_{j=0}^{h-1}(1-\varrho^j z)^{-\beta_j}.$$

Avec (i), (iv) et (III.3) on déduit

(v) $$f(z)=H(z)\prod_{j=0}^{h-1}(1-\varrho^j z)^{-\beta_j},$$

(vi) $$g(z)=K(z)\prod_{j=0}^{h-1}(1-\varrho^j z)^{-\beta_j},$$

avec

(vii) $$K(z)=H(z)H(z^2/q)^{-1}\prod_{j=0}^{h-1}(1-\varrho^j z^2/q)^{\beta_j}.$$

La fonction K est holomorphe dans le disque $|z|<\inf(q^{1/2}, q^{1-\delta})$. On applique la proposition A.2. Il vient

$$a_n q^{-n}=\frac{1}{\pi}\sum_{k=0}^{h-1}\varrho^{-kn}H(\varrho^k)\Big\{\prod_{j=1}^{h-1}(1-\varrho^j)^{-\beta_{j-k}}\Big\}\Gamma(1-\overline{\beta_k})\sin\big(\pi(1-\overline{\beta_k})\big)n^{\overline{\beta_k}-1}+$$

$$+O\big(n^{d\langle L\rangle/h-2}\big).$$

On a une formule analogue pour $b_n q^{-n}$ en remplaçant H par K. Les constantes impliquées par les symboles O intervenant dans ces formules ne dépendent que de H, resp. de K, et de h, c'est-à-dire, en fait, ne dépendent que de l'ensemble I.

La fonction H est à coefficients réels, $H(1)$ est réel et, pour $k=1, \ldots, h-1$, les nombres $H(\varrho^k)$ et $H(\varrho^{h-k})$ sont conjugués. On a le résultat annoncé en posant

$$A_k(I)=\frac{H(\varrho^k)}{\pi}\Big\{\prod_{j=1}^{h-1}(1-\varrho^j)^{-\beta_{j-k}}\Big\}\Gamma(1-\overline{\beta_k})\sin\big(\pi(1-\overline{\beta_k})\big).$$

Lorsque I est de type (h, L), il est possible de calculer exactement les constantes $A_k(I)$, ce qui conduit au théorème suivant:

THÉORÈME 3. *Soient un entier $h\geqslant 2$ et L une partie de $\{0, \ldots, h-1\}$ distincte de $\{0, \ldots, h-1\}$. Soit I l'ensemble des polynômes irréductibles de type (h, L). Pour $k\in\{0, \ldots, h-1\}$, soient*

$$\beta_k=\frac{1}{h}\sum_{l\in L}\varrho^{-kl},\qquad U_k=\prod_{j=1}^{h-1}(1-\varrho^j)^{-\beta_{j-k}},\qquad V_k=\prod_{j=0}^{h-1}(1-\varrho^{j+2k}q^{-1})^{\beta_j},$$

$$Y_k=\prod_{l\in L}\prod_{\substack{m\equiv l(\mathrm{mod}\,h)\\ m\neq 0}}\exp\left(\varrho^{km}\left[\frac{P(m)}{q^m}-\frac{1}{m}\right]+P(m)\sum_{s=2}^{\infty}\frac{1}{s}[\varrho^k/q]^{sm}\right),$$

$$Z_k=\prod_{l\in L}\prod_{\substack{m\equiv l(\mathrm{mod}\,h)\\ m\neq 0}}\exp\left(\frac{\varrho^{2km}}{q^m}\left[\frac{1}{m}-\frac{P(m)}{q^m}\right]-P(m)\sum_{s=2}^{\infty}\frac{1}{s}[\varrho^{2k}/q^2]^{sm}\right).$$

Alors, les nombres $A_k(I)$ et $B_k(I)$ sont donnés par les relations

$$A_k(I)=Y_k U_k\Gamma(1-\overline{\beta_k})\sin\big(\pi(1-\overline{\beta_k})\big)/\pi,$$

$$B_k(I)=Y_k U_k V_k Z_k\Gamma(1-\overline{\beta_k})\sin\big(\pi(1-\overline{\beta_k})\big)/\pi.$$

Démonstration. On reprend la démonstration du théorème 2. La relation (iii) s'écrit ici

$$v(z)=\sum_{l\in L}\sum_{\substack{m\equiv l(\mathrm{mod}\,h)\\ m\neq 0}}\left[P(m)\sum_{s=2}^{\infty}\frac{1}{s}\left(\frac{z}{q}\right)^{sm}+\left(\frac{P(m)}{q^m}-\frac{1}{m}\right)z^m\right],$$

d'où,

$$H(\varrho^k)=\exp\big(v(\varrho^k)\big)=Y_k,$$

$$K(\varrho^k)=H(\varrho^k)H(\varrho^{2k}/q)^{-1}\prod_{j=0}^{h-1}(1-\varrho^j\varrho^{2k}/q)=Y_k Z_k V_k.$$

Lorsque I est l'ensemble des polynômes irréductibles de degré divisible par h

les nombres β_k, U_k, V_k, Y_k et Z_k du théorème 2 prennent une forme particulièrement simple, ce qui conduit au corollaire suivant:

COROLLAIRE. *Soit un entier $h \geqslant 2$ et soit I l'ensemble des polynômes irréductibles de degré divisible par h. Alors, on a*

$$a(n, I) = b(n, I) = 0 \quad \text{si } h \text{ ne divise pas } n, \tag{1}$$

et, pour tout entier $n \geqslant 1$,

$$a(nh, I) = A\Gamma(1/h)^{-1} q^{nh} n^{1/h-1} + O(q^{nh} n^{1/h-2}), \tag{2}$$

$$b(nh, I) = B\Gamma(1/h)^{-1}(1-q^{-h})^{1/h} q^{nh} n^{1/h-1} + O(q^{nh} n^{1/h-2}), \tag{3}$$

avec

$$A = \prod_{P \in I'} (1-q^{-hd^{\circ}P/(h,d^{\circ}P)})^{(h,d^{\circ}P)\cdot 1/h}, \tag{4}$$

$$B = \prod_{P \in I'} (1+q^{-hd^{\circ}P/(h,d^{\circ}P)})^{-(h,d^{\circ}P)\cdot 1/h}, \tag{5}$$

I' désignant l'ensemble des polynômes irréductibles de degré non divisible par h, $(h, d^{\circ}P)$ désignant le p.g.c.d. *des nombres $d^{\circ}P$ et h, les constantes impliquées par les symboles O ne dépendant que de q et de h.*

Démonstration. Les polynômes de $\mathscr{U}(I)$ sont de degré divisible par h, d'où (1). On a

$$\beta_k = 1/h, \quad U_k = h^{-1}/h, \quad V_k = (1-q^{-h})^{-1}, \quad Y_k = \exp(y), \quad Z_k = \exp(z)$$

avec

$$y = \sum_{m=1}^{\infty} q^{-hm}\left[P(hm) - \frac{q^{hm}}{hm}\right] + P(hm) \sum_{s=2}^{\infty} \frac{1}{s} q^{-shm}.$$

Avec (II.2) il vient

$$y = \sum_{m=1}^{\infty} \frac{q^{-hm}}{hm} \sum_{\substack{d \mid hm \\ d \neq 1}} \mu(d)\, q^{hm/d} + P(hm) \sum_{s=2}^{\infty} \frac{1}{s} q^{-shm}$$

$$= \sum_{m=1}^{\infty} \frac{q^{-hm}}{hm} \Big[\sum_{\substack{d \mid hm \\ d \neq 1}} \mu(d)\, q^{hm/d} + \sum_{\substack{sk=m \\ s \neq 1}} P(hk)\, hk\Big]$$

Or, avec (II.1), on a

$$\sum_{\substack{sk=m \\ s \geqslant 2}} hkP(hk) = \sum_{d \mid hm} dP(d) - hmP(hm) - \sum_{\substack{d \mid hm \\ h \nmid d}} dP(d),$$

d'où, en utilisant encore la relation (II.2),

$$y = -\sum_{m=1}^{\infty} \frac{q^{-hm}}{hm} \sum_{\substack{d \mid hm \\ h \nmid d}} dP(d) = -\frac{1}{h} \sum_{\substack{d=1 \\ h \nmid d}}^{\infty} (d, h)\, P(d) \sum_{j=1}^{\infty} \frac{1}{j} q^{-jhd/(d,h)},$$

et

$$Y_k = \prod_{\substack{R \in P \\ h \nmid d^{\circ}R}} (1-q^{-hd^{\circ}R/(h,d^{\circ}R)})^{(h,d^{\circ}R)/h} = A.$$

De la même façon on démontre que

$$Y_k Z_k = B,$$

d'où, les relations (2) et (3).

Notons que ce corollaire peut se démontrer directement à l'aide de la proposition A.1 démontrée en annexe.

Annexe

PROPOSITION A.1. *Soit H une fonction holomorphe dans le disque fermé $\bar{D}_1$. Soit $d \in]0, 1]$. Soit, pour tout nombre complexe $z \neq 1$,*

$$f(z) = H(z)(1-z)^{-d}, \tag{1}$$

et

$$f(z) = \sum_{n=0}^{\infty} u_n z^n \tag{2}$$

le développement en série de Taylor au voisinage de 0 de la fonction f. Alors, si $d = 1$, on a, pour tout entier $k > 0$, pour n tendant vers $+\infty$,

$$u_n = H(1) + o(n^{-k}), \tag{3}$$

et, si $d < 1$, on a, pour n tendant vers $+\infty$,

$$u_n = \frac{H(1)}{\Gamma(d)} n^{d-1} + O(n^{d-2}), \tag{4}$$

les constantes impliquées par le symbole O ne dépendant que de d et de H.

Démonstration. On écrit le développement en série de Taylor à l'origine de la fonction H

$$H(z) = \sum_{j=0}^{\infty} h_j z^j. \tag{i}$$

La fonction H étant holomorphe dans le disque $\bar{D}_1$, on en déduit la convergence absolue des séries dérivées $H'(z), \ldots, H^{(k)}(z)$, au point 1, d'où, pour tout entier $k > 0$,

(ii) $$|h_j| \in o(j^{-k-1}).$$

Si $d = 1$, les relations (1) et (2) nous donnent

$$u_n = h_0 + \ldots + h_n = H(1) - \sum_{j=n+1}^{\infty} h_j,$$

et (3) se déduit de (ii).

On suppose $d < 1$. Alors,

$$(1-z)^{-d} = 1 + \sum_{n=1}^{\infty} v_n z^n,$$

où,

(iii) $$v_n = \frac{\Gamma(d+n)}{\Gamma(d)(n!)}.$$

Les relations (1) et (2) nous donnent

$$u_n = v_n H(1) + \sum_{i=1}^{n-1} h_i (v_{n-i} - v_n) + h_n(1-v_n) - v_n \sum_{p=n+1}^{\infty} h_p.$$

La formule de Stirling nous donne

(iv) $$\Gamma(d)\, v_n = n^{d-1}[1 + O(1/n)], \quad \text{si} \quad n > 0,$$

les constantes impliquées par le symbole O ne dépendant que de d, d'où, avec (ii), si k est un entier strictement positif quelconque,

(v) $$u_n = v_n H(1) + \sum_{i=1}^{n-1} h_i (v_{n-i} - v_n) + o(n^{-k}).$$

Des relations (ii) et (iv) on déduit aussi que

$$\sum_{i=1}^{n-1} h_i (v_{n-i} - v_n) = \sum_{i=1}^{n-1} h_i n^{d-1} \left(\left(1 - \frac{i}{n}\right)^{d-1} - 1 \right) + O\Big(\sum_{j=1}^{n-1} j^{-k-1} (n-j)^{d-2} \Big),$$

$$\sum_{i=1}^{n-1} h_i (v_{n-i} - v_n) \in O\Big(n^{d-2} \sum_{j=1}^{n-1} j^{-k-1} + \sum_{j=1}^{n-1} j^{-k-1} (n-j)^{d-2} \Big),$$

les constantes impliquées par les symboles O ne dépendant que de la fonction H. De plus,

$$\sum_{j=1}^{n-1} j^{-k-1} (n-j)^{d-2} \leqslant \left(\frac{n}{2}\right)^{d-2} \sum_{j=1}^{[n/2]} j^{-k-1} + \sum_{j=[n/2]+1}^{n-1} j^{-k-1} \ll n^{d-2} + n^{-k}$$

la constante impliquée par le symbole $\ll$ ne dépendant que de k et de d. On choisit $k > 2-d$. On conclut avec (iv) et (v).

PROPOSITION A.2. *Soit H une fonction holomorphe dans un disque D_R avec $R > 1$. Soient $d \in]0, 1]$, un entier $h \geqslant 2$ et L une partie non vide de $\{0, \ldots, h-1\}$ différente de $\{0, \ldots, h-1\}$. Soient*

$$\varrho = \cos(2\pi/h) + i \sin(2\pi/h)$$

et

(1) $$f(z) = H(z) \prod_{j=0}^{h-1} (1 - \varrho^j z)^{-\beta_j},$$

où

(2) $$\beta_j = \frac{d}{h} \sum_{k \in L} \varrho^{-kj}.$$

Soit

(3) $$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

le développement de Taylor au voisinage de 0 de la fonction f. Alors, pour n tendant vers $+\infty$, on a

(4) $$a_n = \sum_{k=0}^{h-1} \varrho^{-kn} \frac{H(\varrho^k)}{\pi} \Big\{ \prod_{j=1}^{h-1} (1-\varrho^j)^{-\beta_{j-k}} \Big\} \Gamma(1-\overline{\beta_k}) \sin\big(\pi(1-\overline{\beta_k})\big) n^{\overline{\beta_{k-1}}} + O(n^{d\langle L \rangle/h - 2}),$$

la constante impliquée par le symbole O ne dépendant que de H, R, h et d.

Démonstration. La démonstration utilise une métode due à Landau, [2], avec des séries entières à la place des séries de Dirichlet.

La fonction f est holomorphe en tout point du disque D_R autre que les points $1, \varrho, \ldots, \varrho^{h-1}$. Si Λ est un contour simple contenu dans le disque D_R, entourant un domaine ne contenant pas les points $1, \varrho, \ldots, \varrho^{h-1}$

(i) $$a_n = \frac{1}{2\pi i} \int_{\Lambda} \frac{f(z)}{z^{n+1}}\, dz.$$

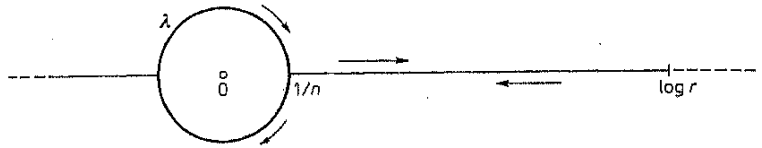
Nous allons définir un tel contour.

Soit $r = (1+R)/2$. Soit un entier n tel que

(ii) $$n > (\log r)^{-1}, \quad n > h/2\pi.$$

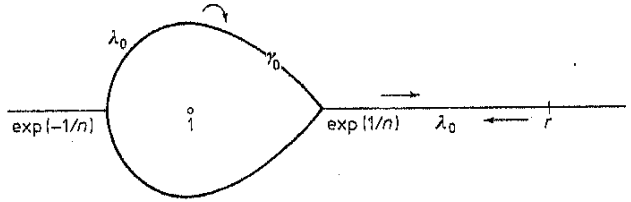
On désigne par λ le chemin formé par le segment d'axe réel joignant les

points $\log r$ et $1/n$, le cercle de centre 0 et de rayon $1/n$ décrit dans le sens négatif, le segment d'axe réel joignant les points $1/n$ et $\log r$



Pour $k \in \{0, \ldots, h-1\}$, soit λ_k l'image de λ par l'application

$$u \to \varrho^k \exp u$$

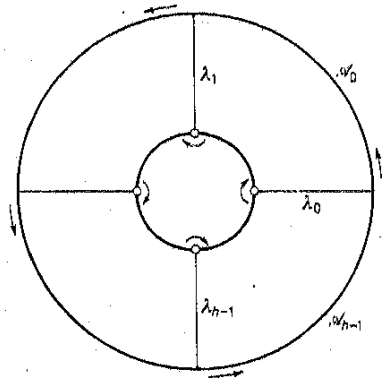


Alors, λ_0 est le chemin formé par le segment d'axe réel joignant les points r et $\exp(1/n)$ une courbe γ_0 entourant le point 1 et coupant l'axe réel aux points $\exp(1/n)$ et $\exp(-1/n)$, cette courbe étant décrite dans le sens négatif, le segment d'axe réel joignant les points $\exp(1/n)$ et r.

Les chemins λ_k se déduisent de λ_0 par des rotations de centre 0 et d'angles $2k\pi/h$. Le chemin λ_k entoure la racine h-ième de 1 ϱ^k. La deuxième des conditions (ii) assure que les chemins λ_k sont disjoints.

Pour $k \in \{0, \ldots, h-1\}$, soit $\mathscr{A}_k$ l'arc du cercle $\mathscr{C}_r$ de centre 0 et de rayon r joignant les points $r\varrho^k$ et $r\varrho^{k+1}$.

On désigne par Λ le contour formé par le chemin λ_0, l'arc $\mathscr{A}_0$, le chemin λ_1, l'arc $\mathscr{A}_1$, ..., le chemin λ_{h-1}, l'arc $\mathscr{A}_{h-1}$.



La proposition se déduit alors des trois lemmes suivants.

LEMME 1. *Il existe une constante $B(H, h, r)$ ne dépendant que de H, h et r telle que, pour $z \in \mathscr{C}_r$, on ait:*

$$|f(z)| \leqslant B(H, h, r). \tag{iii}$$

Démonstration. De façon triviale, pour $z \in \mathscr{C}_r$, pour $j = 0, \ldots, h-1$, on a

$$|(1-\varrho^j z)^{-\beta_j}| \leqslant e^{\pi}(r+1)^{\mathrm{Re}\,\beta_j} \leqslant e^{\pi}(r+1)^{d(h-1)/h} \leqslant e^{\pi}(r+1)^{h-1/h}.$$

La fonction H étant holomorphe dans le disque D_R, elle est bornée sur le disque fermé $\bar{D}_r \subset D_R$, d'où, avec (1),

$$|f(z)| \leqslant \sup_{z \in \bar{D}_r} |H(z)|\, e^{\pi}(r+1)^{h-1}.$$

LEMME 2. *Il existe une constante $C(H, h, r)$ ne dépendant que de H, h et r telle que pour $u \in \lambda$, pour $k \in \{0, \ldots, h-1\}$, on ait*

$$|f(\varrho^k \exp u) - (-u)^{-\alpha_k} A_k| \leqslant C(H, h, r)\,|u|^{1-\mathrm{Re}\,\alpha_k}, \tag{iv}$$

avec

$$A_k = H(\varrho^k) \prod_{j=1}^{h-1} (1-\varrho^j)^{-\beta_{j-k}}, \tag{v}$$

et

$$\alpha_k = \overline{\beta_k}. \tag{vi}$$

Démonstration. Soit $k \in \{0, \ldots, h-1\}$. Pour $z \in \lambda_0$, on a

$$f(\varrho^k z) = (1-z)^{-\alpha_k} V_k(z)\, H(\varrho^k z),$$

où

$$V_k(z) = \prod_{j=1}^{h-1} (1-\varrho^j z)^{-\beta_{j-k}}.$$

Posons

$$\varphi(u) = \begin{cases} (\exp(u)-1)/u & \text{si} \quad u \neq 0, \\ 1 & \text{si} \quad u = 0. \end{cases}$$

Soit $n(h, r)$ le plus petit entier n vérifiant la condition (ii). Soit $\mathscr{D}(h, r)$ le compact formé par la réunion du disque fermé $\overline{D_{1/n(h,r)}}$ et du segment $[0, \log r]$ de l'axe réel. La fonction

$$u \mapsto W_k(u) = V_k(e^u)\, H(\varrho^k e^u)\, [\varphi(u)]^{-\alpha_k}$$

est dérivable sur $\mathscr{D}(h, r)$ et sa dérivée y est bornée. Posons

$$C = C(H, h, r) = \sup_{0 \leqslant k \leqslant h-1} \left(\sup_{u \in \mathscr{D}(h,r)} |W_k'(u)| \right).$$

Alors, pour $u \in \lambda$, on a

$$|W_k(u) - W_k(0)| \leqslant C|u|,$$

d'où,

$$|f(\varrho^k \exp u) - (-u)^{-\alpha_k} W_k(0)| \leqslant C|u|\,|(-u)^{-\alpha_k}| \leqslant C|u|^{1-\mathrm{Re}\alpha_k}.$$

On vérifie facilement que $A_k = W_k(0)$.

LEMME 3. *Soit, pour* $k \in \{0, \ldots, h-1\}$,

$$J_k = \frac{1}{2\pi i} \int_{\lambda} (-u)^{-\alpha_k} \exp(-un)\, du. \tag{vii}$$

Alors,

$$\left| J_k - \frac{n^{\alpha_k - 1}\, \Gamma(1-\alpha_k) \sin(\pi(1-\alpha_k))}{\pi} \right| \leqslant \frac{6 n^{d\langle L\rangle/h - 2}}{\pi \log r}. \tag{viii}$$

Démonstration. On a

$$J_k = -\frac{1}{2\pi i} \int_{\mathscr{H}} n^{\alpha_k - 1} \exp(u)\, u^{-\alpha_k}\, du,$$

où $\mathscr{H}$ désigne l'image de λ par l'application

$$u \longmapsto -nu.$$

La formule de Hankel, dont on peut trouver une démonstration dans [6] nous donne alors,

$$J_k = n^{\alpha_k - 1}\, \frac{\Gamma(1-\alpha_k) \sin(\pi(1-\alpha_k))}{\pi} + \varepsilon_{n,k}\, n^{\alpha_k - 1},$$

où

$$|\varepsilon_{n,k}| \leqslant \frac{1}{\pi} \int_{n \log r}^{+\infty} e^{-x} |(-x)^{-\alpha_k}|\, dx = \frac{1}{\pi} \int_{n \log r}^{+\infty} e^{-x} x^{-\mathrm{Re}\alpha_k}\, dx \leqslant \frac{\Gamma(2 - \mathrm{Re}\,\alpha_k)}{\pi n \log r}.$$

On a

$$|\alpha_k| \leqslant d\langle L\rangle/h \leqslant d(h-1)/h < 1$$

d'où,

$$|\varepsilon_{n,k}| \leqslant \frac{6}{n \log r} \quad \text{et} \quad |n^{\alpha_k - 1}| \leqslant n^{d\langle L\rangle/h - 1}.$$

Nous pouvons achever la démonstration de la proposition. On a

$$\left| \sum_{k=0}^{h-1} \int_{\lambda_k} f(z)\, z^{-n-1}\, dz \right| \leqslant \int_{\mathscr{C}_r} |f(z)|\, |z|^{-n-1}\, dz,$$

d'où, avec (i) et (iii),

$$\left| a_n - \sum_{k=0}^{h-1} \frac{1}{2\pi i} \int_{\lambda_k} f(z)\, z^{-n-1}\, dz \right| \leqslant B(H, h, r) r^{-n}.$$

D'après la définition du chemin λ_k,

$$\int_{\lambda_k} f(z)\, z^{-n-1}\, dz = \varrho^{-kn} \int_{\lambda} f(\varrho^k \exp u) \exp(-nu)\, du,$$

d'où, avec (iv) et (vii),

$$|a_n - \sum_{k=0}^{h-1} \varrho^{-kn} A_k J_k| < B(H, h, r) r^{-n} + C(H, h, r) \sum_{k=0}^{h-1} L_k, \tag{ix}$$

où

$$L_k = \left| \int_{\lambda} |u|^{1-\mathrm{Re}\alpha_k} \exp(-nu)\, du \right| / 2\pi.$$

On a

$$L_k \leqslant \left[2 \int_{1/n}^{\log r} x^{1-\mathrm{Re}\alpha_k} \exp(-nx)\, dx + n^{\mathrm{Re}(\alpha_k) - 2} \int_0^{2\pi} \exp(-\cos t)\, dt \right] / 2\pi,$$

$$L_k \leqslant n^{\mathrm{Re}(\alpha_k) - 2} \left[e + \frac{1}{2\pi} \int_1^{n \log r} x^{1-\mathrm{Re}\alpha_k} e^{-x}\, dx \right] \leqslant n^{\mathrm{Re}(\alpha_k) - 2} \left[e + \frac{1}{\pi} \Gamma(2 - \mathrm{Re}\,\alpha_k) \right],$$

comme au lemme précédent,

$$|L_k| \leqslant n^{1/h - 2} \left(e + \frac{6}{\pi} \right). \tag{x}$$

Posons

$$K(H, h, r) = C(H, h, r) \left(e + \frac{6}{\pi} \right) + B(H, h, r) \sup_{n \geqslant n(h,r)} (n^2 r^{-n}),$$

$n(h, r)$ désignant encore ici le plus petit entier n vérifiant les conditions (ii). Les relations (viii), (ix) et (x) nous donnent alors

$$\left|a_n - \sum_{k=0}^{h-1} \varrho^{-kn} A_k(1-\alpha_k) \sin\left(\pi(1-\alpha_k)\right) n^{\alpha_k - 1}/\pi\right| \leqslant K(H, h, r)\, n^{d\langle L\rangle/h-2},$$

ce qui est la relation (4).

References

[1] H. Delange, *Sur la distribution des entiers ayant certaines propriétés*, Ann. Scient. Ec. Norm. Sup., série 3, 73 (1956), p. 15–74.

[2] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. (3) 13 (1908), p. 305–312.

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

[4] S. Saks and A. Zygmund, *Analytic functions*, Państwowe Wydawnictwo Naukowe, Warszawa 1959.

[5] J. P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. 22 (3–4) (1976), p. 227–260.

Reçu le 13. 1. 1983
et dans la forme modifiée le 4. 5. 1983 (1335)

ACTA ARITHMETICA
XLIV (1984)

Sur l'irréductibilité des trinômes $X^{p^r+1} - aX - b$ sur les corps finis F_{p^s}

par

S. Agou (Lyon)

Introduction. Soient a, b deux éléments non nuls du corps F_{p^s} et r, $r \geqslant 1$, un entier naturel. On donne dans cet article, lorsque r divise s ou lorsque r est un nombre premier impair une méthode pour déterminer explicitement des conditions d'irréductibilité des trinômes $X^{p^r+1} - aX - b$ sur les corps finis F_{p^s}, généralisant ainsi un travail de Ore [5], sur les polynômes $X^{p^s+1} - \alpha X^{p^s} - \beta X - \gamma$ de $F_{p^s}[X]$.

1. Formules explicites. Les résultats ci-dessous seront utilisés dans la 3ème partie.

1.1. Soient X_1, X_2 deux indéterminées et $F_p(\{X_1, X_2\})$ l'algèbre libre qu'elles engendrent avec F_p.

Pour tout entier naturel n, on désigne par S_n l'ensemble des éléments $\mu = (x_k, y_k, \ldots, x_1, y_1) \in N^{2k}$ où $k = E(n/3)+1$ et où μ est tel que:

1) si pour un indice $i \geqslant 1$ on a $x_i = 0$ alors $x_j = y_j = 0$ pour $j > i$,

2) si pour un indice $i > 1$ on a $y_i = 0$ alors $x_j = y_j = 0$ pour $j \geqslant i$,

3) $\sum_{i=1}^{k} (x_i + 2y_i) = n$.

On désigne par $\sum_n$ la quantité $\sum_{\mu \in S_n} X_1^{x_k} X_2^{y_k} \ldots X_1^{x_1} X_2^{y_1}$ de $F_p(\{X_1, X_2\})$, et on pose $\sum_0 = 1$.

Si $M = X_1^{x_k} X_2^{y_k} \ldots X_1^{x_1} X_2^{y_1}$ est un mot de $F_p(\{X_1, X_2\})$ on appelle poids du mot M, l'entier $\delta(M) = \sum_{i=1}^{k} (x_i + 2y_i)$.

Il est clair que les éléments de S_n correspondent bijectivement aux mots M de $F_p(\{X_1, X_2\})$ tels que $\delta(M) = n$.

Avec ces notations on a la:

1.1.1. Proposition. *Pour tout entier n, $n \geqslant 2$, on a dans $F_p(\{X_1, X_2\})[X]$ l'identité*

$$(1)\quad X^n = \Big(X^{n-2} + \sum_1 X^{n-3} + \ldots + \sum_{n-2}\Big) \cdot (X^2 - X_1 X - X_2) + \sum_{n-1} X + \sum_{n-2} X_2.$$