ANNALES

DE

L'INSTITUT FOURIER

Cécile DARTYGE & Gérald TENENBAUM

Sommes des chiffres de multiples d'entiers

Tome 55, n° 7 (2005), p. 2423-2474.

<http://aif.cedram.org/item?id=AIF_2005__55_7_2423_0>

Ann. Inst. Fourier, Grenoble
55, 7 (2005), 2423–2474

SOMMES DES CHIFFRES DE MULTIPLES D'ENTIERS

par Cécile DARTYGE & Gérald TENENBAUM

Sommaire.

1. Introduction.

Soit q un entier au moins égal à 2. Pour $n \in \mathbb{N}$, notons $s_q(n)$ la somme des chiffres de n en base q.

Mots-clés : sommes des chiffres, répartition dans les progressions arithmétiques, fonctions multiplicatives.
Classification math. : 11L07, 11B85, 11A63.

Dans les dernières décennies, de nombreuses recherches ont porté sur la répartition asymptotique de la fonction vectorielle

$$n \mapsto s_q(\mathbf{h}n) := \big(s_q(h_1n), \dots, s_q(h_rn)\big) \qquad (\mathbf{h} := (h_1, \dots, h_r) \in \mathbb{N}^{*r})$$

On pourra notamment consulter les travaux de Stolarsky [22], Schmidt [18], Schmid [17] pour le cas $q = 2$.

Dans [17] (théorème 1.1, ... 392), Schmid donne en particulier, pour $\mathbf{h} \in \mathbb{N}^{*r}$ et $\mathbf{a} \in \mathbb{Z}^r$ fixés, une estimation asymptotique du cardinal de l'ensemble

$$\{0 \leqslant n \leqslant x : s_q(\mathbf{h}n) = \mathbf{a}\}$$

lorsque $x \to \infty$.

D'autres informations sur la loi limite du vecteur $s_q(\mathbf{h}n)$ peuvent être déduites des résultats généraux de Indlekofer et Katai [11], [12], concernant les valeurs moyennes de fonctions de la forme $n \mapsto g_1(h_1n) \cdots g_k(h_kn)$ où les g_j $(1 \leqslant j \leqslant k)$ sont des fonctions q-multiplicatives[(1)] de module 1 : en effet, le choix $g_j(n) := \mathrm{e}^{it_j s_q(n)}$ avec $t_j \in \mathbb{R}$ fournit la transformée de Fourier multidimensionnelle de la loi de répartition de $s_q(\mathbf{h}n)$.

Tous ces résultats sont valables uniquement lorsque le vecteur à coordonnées entières $\mathbf{h}$ est fixé. La délicate question de la dépendance en $\mathbf{h}$ des termes d'erreurs et des constantes implicites n'y est pas abordée.

L'objet principal de ce travail consiste à préciser quantitativement, y compris du point de vue de l'uniformité en $\mathbf{h} \in \mathbb{N}^{*r}$, le degré d'indépendance asymptotique des suites $n \mapsto s_q(h_jn)$ et d'un caractère additif ou multiplicatif.[(2)] Un contrôle effectif du paramètre $\mathbf{h}$ s'avère en effet crucial pour de nombreuses applications arithmétiques.

Pour $\mathbf{h} := (h_1, \dots, h_r) \in \mathbb{N}^{*r}$, $\mathbf{k} \in \mathbb{N}^r$, $\boldsymbol{\alpha} \in \mathbb{R}^r$, $\vartheta \in \mathbb{R}$, nous introduisons les produits scalaires

$$\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n) = \sum_{1 \leqslant j \leqslant r} \alpha_j s_q(h_jn),$$

$$\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n + \mathbf{k}) = \sum_{1 \leqslant j \leqslant r} \alpha_j s_q(h_jn + k_j).$$

(1) Une fonction q-multiplicative g est une fonction arithmétique vérifiant $g(a + q^t b) = g(a)g(q^t b)$ pour tous nombres entiers $a \geqslant 0$, $b \geqslant 0$, $t \geqslant 0$ tels que $a < q^t$.

(2) Comme on le verra dans l'énoncé du Théorème 2.12 *infra*, nous englobons le cas d'un caractère multiplicatif dans celui, plus général, d'une fonction multiplicative à valeurs dans le disque unité.

Comme $s_q(qn) = s_q(n)$ pour tout entier n, nous pouvons sans perte de généralité restreindre l'étude de $n \mapsto \boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)$ au cas où $q \nmid h_j$ pour $1 \leqslant j \leqslant r$. Par commodité, nous appliquons cette même restriction au cas de $n \mapsto \boldsymbol{\alpha}\cdot s_q(\mathbf{h}n + \mathbf{k})$.

Posons $\mathrm{e}(t) := \exp(2i\pi t)$ $(t \in \mathbb{R})$. Une mesure de l'indépendance asymptotique évoquée plus haut est fournie, dans le cas d'un caractère additif, par la majoration des sommes « longues »

$$G_r(x;\vartheta) = G_r(x;\vartheta;\boldsymbol{\alpha},\mathbf{h}) := \sum_{n\leqslant x} \mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n) + \vartheta n\big), \tag{1·1}$$

et « courtes »

$$G_r(x,y;\vartheta) = G_r(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h}) := G_r(x+y;\vartheta;\boldsymbol{\alpha},\mathbf{h}) - G_r(x;\vartheta;\boldsymbol{\alpha},\mathbf{h}).$$

Pour des raisons précisées plus loin, nous nous intéressons également à la somme

$$G_r(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h},\mathbf{k}) := \sum_{x<n\leqslant x+y} \mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n+\mathbf{k}) + \vartheta n\big).$$

Lorsque $r = 1$, nous avons

$$\begin{aligned} G_1\left(q^K - 1;\vartheta;\alpha,1\right) &= \sum_{n<q^K} \mathrm{e}(\alpha s_q(n) + \vartheta n) \\ &= \prod_{0\leqslant k<K} \sum_{0\leqslant d<q} \mathrm{e}\big(d(\alpha + \vartheta q^k)\big). \end{aligned} \tag{1·2}$$

En exploitant cette identité, Gelfond [9] a établi, pour chaque entier $m \geqslant 1$, l'existence d'une constante $\lambda = \lambda_{m,q} \in]0,1[$ telle que l'on ait, uniformément pour $1 \leqslant j < m$, $(m, q-1) = 1$, $\vartheta \in \mathbb{R}$, $h \in \mathbb{N}^*$,

$$G_1(x;\vartheta;j/m;h) \ll (hx)^{\lambda}. \tag{1·3}$$

Il a en outre montré que, $\lambda_{2,2} = (\log 3)/\log 4$; cette valeur est en fait optimale, comme l'attestent les résultats de Newman [15] relatifs au cas $r = 1$, $h = 3$, $\vartheta = 0$. Gelfond déduit en particulier de (1·3) que, sous la condition $(m, q-1) = 1$, on a

$$\sum_{\substack{n\leqslant x\\ n\equiv b\,(\mathrm{mod}\,d)\\ s_q(n)\equiv a\,(\mathrm{mod}\,m)}} 1 = \frac{x}{md} + O(x^{\lambda}),$$

avec $\lambda = \lambda_{m,q}$, uniformément en a, b, d, m.

Lorsque $r \geqslant 2$, l'identité (1·2), qui reflète la q-additivité de la fonction s_q, n'a plus lieu, et il faut recourir à des techniques différentes. En 1982, Coquet (voir [4], théorèmes 1 et 3), a montré que, si les paramètres $\boldsymbol{\alpha} \in \mathbb{R}^r$, $\mathbf{h} \in \mathbb{N}^{*r}$ sont choisis de sorte que $n \mapsto (q-1)\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)$ ne soit pas constante modulo 1, on a pour chaque $\vartheta \in \mathbb{R}$,

$$G_r(x;\vartheta;\boldsymbol{\alpha},\mathbf{h}) = o(x). \tag{1·4}$$

Cette estimation est uniforme en ϑ, mais pas en $\mathbf{h}$. Une version effective a été donnée par Solinas [21] lorsque $\boldsymbol{\alpha} \in \mathbb{Q}^r$ et $\vartheta = 0$. Cela lui a permis de calculer, pour tous $\mathbf{a} \in \mathbb{Z}^r$, $m \in \mathbb{N}^*$, la densité de l'ensemble des entiers n satisfaisant à $s_q(\mathbf{h}n) \equiv \mathbf{a} \pmod m$. À la fin de son article, il cite[(3)] une majoration, établie dans sa thèse [20], de $\big|G_r(x;\boldsymbol{\alpha},\mathbf{h};0)\big|$ en fonction de $H := [h_1,\dots,h_r]$ et du ppcm m des dénominateurs des α_j, soit

$$\big|G_r(x;0;\boldsymbol{\alpha},\mathbf{h})\big| \leqslant \tfrac{12}{11} H^2 x^{1-\delta(H,m)} \qquad (x \geqslant 1), \tag{1·5}$$

avec $\delta(H,m) := 4\sin^2(\pi/2m)/\{q^4H^2\log(q^4H^2)\}$ s'il existe un j tel que $m \nmid a_j(q-1)$. La preuve de ce résultat repose sur un astucieux procédé inductif qui permet de réduire le problème à l'évaluation des puissances d'une matrice de taille $H \times H$. Cette technique semble délicate à transposer aux suites (1·1) lorsque $\vartheta \neq 0$ car la matrice prend alors une valeur différente à chaque pas de la récurrence.

La première partie de ce travail est dévolue à la majoration des quantités $\big|G_r(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h},\mathbf{k})\big|$. Les résultats obtenus sont énoncés au paragraphe 2.1, où nous mentionnons également des majorations moins fortes mais valables pour des r-uplets $\mathbf{h}$ pour lesquels

$$\|\mathbf{h}\|_\infty := \max_{1\leqslant j\leqslant r} |h_j|$$

est de l'ordre de x. Nous développons ensuite divers types d'applications, qui sont explicitées aux paragraphes 2.2 à 2.4.

(3) Nous rectifions une coquille dans cette assertion.

2. Énoncés des résultats.

2.1. Valeurs de $\alpha\cdot s_q(\mathbf{h}n)$ et majorations de $|G_r(x,y;\vartheta;\alpha,\mathbf{h},\mathbf{k})|$.

Notre résultat principal fournit une estimation uniforme en ϑ et cependant effective relativement aux vecteurs $\mathbf{h}$ et $\mathbf{k}$.

Nous notons traditionnellement $\omega(n)$, ou parfois, pour alléger les notations, ω_n, le nombre des facteurs premiers, comptés sans multiplicité, d'un entier $n \geqslant 1$.

Nous désignons par $\|u\|$ la distance d'un nombre réel u à l'ensemble des entiers et nous étendons la définition à $\mathbb{R}^r$ en posant

$$\|\mathbf{u}\| := \max_{1\leqslant j\leqslant r} \|u_j\| \qquad \big(\mathbf{u}\in\mathbb{R}^r\big).$$

Étant donnés un vecteur $\boldsymbol{\alpha}\in\mathbb{R}^r$ et un entier $X\geqslant 1$, il existe, en vertu de la version multidimensionnelle du théorème de Dirichlet (voir par exemple [24], lemme II.1.14.1), un entier $m\in[1,X^r]$ tel que $\|m\boldsymbol{\alpha}\|\leqslant 1/X$. Nous notons $m(\alpha;X^r)$ le plus petit des entiers m satisfaisant cette propriété. Il existe alors un vecteur $\mathbf{a}=\mathbf{a}(\boldsymbol{\alpha};X)\in\mathbb{Z}^r$ tel que $\|m\boldsymbol{\alpha}-\mathbf{a}\|_\infty\leqslant 1/X$.

Étant donnée une puissance de q, disons $\varrho=q^\nu$, nous notons

$$n=\sum_{j\geqslant 0} e_j(n)\varrho^j \tag{2·1}$$

le développement d'un entier générique n en base ϱ et posons, pour $E\geqslant 0$, $D\geqslant 0$,

$$\mathbb{N}(E,D;\varrho) := \{n\geqslant 0 : e_j(n)=0 \ (E<j\leqslant E+D)\}.$$

Ainsi $n\in\mathbb{N}(E,D;\varrho)$ si, et seulement si, $n=a+\varrho^{E+D}b$ avec $0\leqslant a<\varrho^E$, $b\geqslant 0$.

Théorème 2.1. — *Soient $r\in\mathbb{N}^*$, $\boldsymbol{\alpha}\in\mathbb{R}^r$, et $\mathbf{h}\in\mathbb{N}^{*r}$ un r-uplet dont les coordonnées sont deux à deux distinctes et non divisibles par q. On pose $h:=\|\mathbf{h}\|_\infty$. Il existe des constantes strictement positives δ et K, ne dépendant que de q et r, telles que les assertions suivantes soient vérifiées.*

Notons

$$X := \frac{84(q-1)rh\log(2Kqh)}{\log q}, \quad m := m\big(\boldsymbol{\alpha};X^r\big). \tag{2·2}$$

Sous la condition

$$(q-1)\mathbf{a}(\boldsymbol{\alpha};X)\notin\mathbb{Z}^r,$$

et lorsque

$$x\geqslant 0,\quad y\geqslant 1,\quad \vartheta\in\mathbb{R},\quad D\in\mathbb{N},\quad E\in\mathbb{N},\quad \mathbf{k}\in\mathbb{N}(E,D;\varrho)^r,$$

où ϱ désigne l'unique puissance de q vérifiant $2Kh<\varrho\leqslant 2Kqh$, on a

$$\big|G_r\big(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h},\mathbf{k}\big)\big|\leqslant y(8+3D/h)\mathrm{e}^{-\delta D/80m^2h}+4\varrho^{E+D}. \tag{2·3}$$

Des valeurs admissibles de δ et K sont

$$\delta:=\frac{1}{s(400\log 4s)^2q^3},\quad K:=K_0q^3s^5\log s \tag{2·4}$$

où K_0 est absolue et où l'on a posé $s:=r+\omega(q)$. En particulier, si $\|\mathbf{k}\|_\infty\leqslant\sqrt{y}$, on a

$$G_r(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h},\mathbf{k})\ll m^2\delta^{-1}y^{1-c_0/\{m^2h\log(Kh)\}}, \tag{2·5}$$

où la constante implicite est absolue. Une valeur admissible de c_0 est

$$c_0:=\frac{c_1}{q^3s(\log 4s)^2} \tag{2·6}$$

où c_1 est absolue.

Remarque. — Si l'on a $(q-1)\alpha_t\in\mathbb{Z}$ et $k_t=0$ pour un indice $t\in[1,r]$, alors $\mathrm{e}(\alpha_t s_q(h_tn))=\mathrm{e}(\alpha_th_tn)$ puisque $q^j\equiv 1\,(\mathrm{mod}\,q-1)$ pour tout entier $j\geqslant 0$; ce terme peut alors être regroupé avec $\mathrm{e}(\vartheta n)$ et l'on est ramené à un problème de dimension au plus $r-1$.

Le contrôle uniforme de tous les paramètres rend la formulation du Théorème 2.1 inévitablement technique. Nous énonçons à présent un corollaire simple qui permet d'en apprécier plus aisément le contenu.

Corollaire 2.2. — *Soient $q\geqslant 2$, $r\geqslant 1$ et $\boldsymbol{\alpha}\in\mathbb{R}^r\smallsetminus\big\{\mathbb{Z}/(q-1)\big\}^r$. On pose*

$$R=R(\boldsymbol{\alpha}):=\begin{cases}1 & \text{si } \boldsymbol{\alpha}\in\mathbb{Q}^r,\\ 2r+1 & \text{si } \boldsymbol{\alpha}\in\mathbb{R}^r\smallsetminus\mathbb{Q}^r.\end{cases}$$

Il existe deux constantes strictement positives A_1 et c_1, ne dépendant que de $\boldsymbol{\alpha}$, q et r, telles que l'on ait

$$|G_r(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h},\mathbf{k})| \leqslant A_1 y \mathrm{e}^{-c_1 L} \tag{2·7}$$

sous les conditions

$$\begin{cases} x \geqslant 0, \quad y \geqslant 3, \quad \vartheta \in \mathbb{R}, \quad L \geqslant 1, \quad \|\mathbf{k}\|_\infty \leqslant \sqrt{y}, \\ \|\mathbf{h}\|_\infty \log(2\|\mathbf{h}\|_\infty) \leqslant \left(\dfrac{\log y}{L}\right)^{1/R}, \\ h_i \neq h_j \ (1 \leqslant i < j \leqslant r), \quad q \nmid h_j \ (1 \leqslant j \leqslant r). \end{cases} \tag{2·8}$$

Contrairement à celle de Solinas dans [20], notre approche est directe et ne repose pas sur un raisonnement par récurrence. Comme l'atteste la comparaison de (1·5) et (2·5), cela permet une amélioration appréciable de la dépendance en $\mathbf{h}$.

Dans [6] nous utilisons le Théorème 2.1 pour montrer que, si $f \in \mathbb{Z}[X]$ est un polynôme de degré $d \geqslant 2$ dont les coefficients sont positifs ou nuls, et si g, $q \geqslant 2$, $m \geqslant 2$ sont des entiers tels que $(m, q-1) = 1$, alors

$$\sum_{\substack{n \leqslant N \\ s_q(f(n)) \equiv g \,(\mathrm{mod}\, m)}} 1 \gg N^{2/d!}.$$

Le contrôle des dépendances en $\mathbf{k}$ et y est déterminant pour cette application, qui a motivé l'insertion du paramètre $\mathbf{k}$ dans la définition de G_r.

Il est très vraisemblablement possible, par nos méthodes, de relâcher encore les contraintes relatives aux vecteurs $\mathbf{h}$ et $\mathbf{k}$. Cependant, de telles extensions sont certainement limitées par des phénomènes de mauvaises corrélations, comme celui mis en évidence par Mauduit et Sárközy [14] dans la formule

$$\sum_{0 \leqslant n < 2^M} (-1)^{s_2(n)+s_2(n+1)} = -\tfrac{1}{3}2^M - \tfrac{2}{3}(-1)^M \qquad (M \geqslant 0).$$

Dans les hypothèses du Théorème 2.1, nous avons

$$\|\boldsymbol{\alpha} - \mathbf{a}/m\|_\infty \leqslant 1/(mX) \tag{2·9}$$

avec $\mathbf{a} := \mathbf{a}(\boldsymbol{\alpha}; X) \in \mathbb{Z}^r$ et $m := m(\boldsymbol{\alpha}; X)$. Nous posons alors

$$M(n) = \mathbf{a}{\cdot}s_q(\mathbf{h}n) := \sum_{1\leqslant j\leqslant r} a_j s_q(h_j n).$$

Considérons un vecteur $\mathbf{a} \in \mathbb{Z}^r$ satisfaisant (2·9). Ainsi que nous l'avons précédemment remarqué, les sommes $G_r(x, y; \vartheta; \mathbf{a}/m, \mathbf{h}, \mathbf{k})$ sont de nature essentiellement triviale lorsque $m|a_j(q-1)$ pour tout indice j, $1 \leqslant j \leqslant r$. Dans le cas contraire, soit

$$\exists j \in [1, r] : \ m \nmid a_j(q-1), \tag{2·10}$$

nous posons

$$h^* = h^*(\mathbf{a}, m; q) := \max_{\substack{1\leqslant j\leqslant r\\ m\nmid a_j(q-1)}} h_j. \tag{2·11}$$

Sous l'hypothèse (2·10), Solinas [21] a établi l'existence d'au moins un entier $n \ll_q {h^*}^2$ tel que

$$M(n) \not\equiv 0 \,(\mathrm{mod}\, m). \tag{2·12}$$

D'intérêt intrinsèque, la première étape de notre preuve du Théorème 2.1 consiste à minorer de façon effective le nombre des solutions de (2·12) n'excédant pas une borne donnée. Nous construisons à cet effet des couples d'entiers (ℓ, n) tels que

$$M(\ell) - M(\ell-1) \not\equiv M(n) - M(n-1) \,(\mathrm{mod}\, m). \tag{2·13}$$

Pour tous entiers $N \geqslant 1$, $H \geqslant 3$, nous désignons par $Q(N, H)$ le nombre maximal de couples (ℓ, n) de $]N+1, N+H]^2$ vérifiant (2·13) et tels que les quadruplets $\{\ell-1, \ell, n-1, n\}$ soient deux à deux disjoints.[(4)]

Théorème 2.3. — *Soient $\mathbf{a} \in \mathbb{Z}^r$, $\mathbf{h} \in (\mathbb{N}^*)^r$ et $m \in \mathbb{N}^*$ satisfaisant (2·10). On suppose que les coordonnées h_j de $\mathbf{h}$ sont deux à deux distinctes et non divisibles par q.*

(i) On a $Q(0, H) > 0$ pour $H \geqslant 60h^*q^3(\omega_q + r)\log(2\omega_q + 2r)$, où h^* est défini par (2·11).

(4) Nos quadruplets $\{\ell-1, \ell, n-1, n\}$ sont des variantes simplifiées des quadruplets $\{\tau_1, \tau_2, \tau_3, \tau_4\}$ de Solinas dans [21], ... 144.

(ii) Il existe deux constantes positives K et δ, ne dépendant que de r et q, telles que l'on ait

$$Q(N,H) \geqslant \delta H$$

pour tous H, N vérifiant $H \geqslant Kh^*$, $N \geqslant 0$. Les valeurs de δ et K données en (2·4) sont admissibles.

Le Théorème 2.3 fournit aisément, pour les sommes $G_r(x,y;\vartheta;\boldsymbol{\alpha},\mathbf{h};\mathbf{k})$, une estimation non triviale valable même lorsque les coordonnées de $\mathbf{h}$ sont d'un ordre de grandeur comparable à celui de x. Nous donnons ci-dessous une formulation plus générale.

THÉORÈME 2.4. — *Soient $r \in \mathbb{N}^*$, $\boldsymbol{\alpha} \in \mathbb{R}^r$, et $\mathbf{h} \in \mathbb{N}^{*r}$. On pose $h := \|\mathbf{h}\|_\infty$. Il existe des constantes positives K et δ, ne dépendant que de r et q, telles que l'on ait pour $N \geqslant 0$, $H > Kh$, $q^V \geqslant h(N+H)$, $X := 4r(q-1)V$, $m := m\big(\boldsymbol{\alpha}; X^r\big)$, $(q-1)\mathbf{a}(\boldsymbol{\alpha};X) \notin \mathbb{Z}^r$, $\vartheta \in \mathbb{R}$,*

$$|G_r(N,H;\vartheta;\boldsymbol{\alpha},\mathbf{h})| \leqslant H\big(1-\delta/m^2\big). \tag{2·14}$$

Les valeurs de δ et K données en (2·4) sont admissibles.

Pour de petites valeurs de h et, par exemple, $\boldsymbol{\alpha} \in \mathbb{Q}^r$, la majoration (2·14) est significativement plus faible que (2·5). En revanche, nous obtenons ainsi un domaine de validité considérablement étendu : (2·14) a lieu dès que $H > Kh$ alors que (2·5) nécessite $\log H \gg h$.

Ainsi que nous l'avons mentionné plus haut, le Théorème 2.4 constitue l'étape liminaire de notre preuve du Théorème 2.1. La dernière phase du raisonnement consiste à mettre en œuvre un processus de découpage permettant une application itérée du Théorème 2.4. Le contrôle effectif de ce découpage est obtenu grâce à une estimation uniforme, énoncée au Théorème 6.1, des probabilités de grandes déviations pour la loi binomiale.

Nous concluons ce paragraphe par une application spécifique des Théorèmes 2.1 et 2.3.

Étant donnés des entiers positifs a, d, m satisfaisant à $(m, q-1) = 1$, définissons $n_d = n_d(a,m)$ comme le plus petit entier $n \geqslant 1$ tel que

$$s_q(nd) \not\equiv a \,(\mathrm{mod}\, m).$$

La question de l'ordre de grandeur de n_d est un problème ouvert intéressant. Une conséquence immédiate du Théorème 2.3 est la majoration universelle

$$n_d \leqslant 60dq^3(2+\omega_q)\log(4+2\omega_q) \qquad (d \geqslant 1). \tag{2·15}$$

L'exemple de $d = 1 + q^k$ où q est pair, $a = 0$, $m = 2$, montre que l'on peut avoir $n_d \geqslant d - 1$ pour une infinité d'entiers d. Il s'ensuit que l'ordre de grandeur en d de la majoration (2·15) est exact.

Le théorème suivant, qui résulte facilement du Théorème 2.1, implique que n_d est normalement de taille beaucoup plus modérée — et en fait bornée sur un ensemble de densité arbitrairement proche de l'unité.

Pour $\mathbf{a} \in \mathbb{Z}^r$, $\mathbf{h} \in \mathbb{N}^{*r}$, $x \geqslant 2$, nous désignons par $S(x; \mathbf{h}; \mathbf{a}, m)$ le nombre des entiers d de $[1, x]$ tels que

$$(\forall j \in [1, r]) \quad s_q(h_j d) \not\equiv a_j \,(\mathrm{mod}\, m).$$

Théorème 2.5. — *Soient $q \geqslant 2$, $r \geqslant 1$, $\mathbf{a} \in \mathbb{Z}^r$, $m \geqslant 2$ tels que $(m, q-1) = 1$. Soit $\mathbf{h} \in \mathbb{N}^{*r}$ un r-uplet dont les coordonnées sont deux à deux distinctes et non divisibles par q. On pose $h := \|\mathbf{h}\|_\infty$. Il existe une constante $c_2 = c_2(q) > 0$ telle que l'on ait, pour $x \geqslant 2$,*

$$S(x; \mathbf{h}; \mathbf{a}, m) = x\big(1 - 1/m\big)^r \Big\{1 + O\Big(2^r x^{-c_2(q)/\{m^2 rh(\log rh)^3\}}\Big)\Big\}, \tag{2·16}$$

où la constante implicite est absolue. Une valeur admissible de $c_2(q)$ est

$$c_2(q) = c_3/\{q^3 \omega_q \log^2(2\omega_q) \log q\}$$

où c_3 est absolue.

En particulier, pour chaque q fixé et toute fonction $\xi(d)$ tendant vers l'infini, on a

$$n_d \leqslant \xi(d)$$

pour presque tout entier d.

L'uniformité en r du Théorème 2.5 est susceptible d'applications relatives à l'existence, dans certaines suites d'entiers définies par des contraintes multiplicatives, d'une infinité d'entiers n tels que $s_q(n) \equiv a \,(\mathrm{mod}\, m)$. Nous développons ici quelques applications de cette nature. Les énoncés correspondants sont présentés au paragraphe suivant.

2.2. Quelques pas vers la conjecture de Gelfond et d'autres applications du Théorème 2.5.

À la fin de son article [9], Gelfond écrit (pour $(m, q-1) = 1$) : « *Il serait aussi intéressant de trouver le nombre de nombres premiers*

$p \leqslant x$ *tels que* $s_q(p) \equiv \ell \pmod m$. » Alors qu'il est naturel, au vu de ce que nous savons du comportement stochastique des nombres premiers, de conjecturer que les nombres $s_q(p)$ sont bien répartis dans les diverses classes de congruence modulo m, nous ne savons toujours pas si chacun des ensembles correspondants de nombres premiers est infini.

Fouvry et Mauduit [7], [8], ont récemment obtenu des avancées significatives vers la conjecture

$$\sum_{\substack{p\leqslant x\\ s_q(p)\equiv \ell \,(\mathrm{mod}\, m)}} 1 \sim \frac{x}{m\log x} \qquad \big((m, q-1)=1,\, x\to\infty\big). \tag{2·17}$$

Dans [7], ils déduisent du théorème de Chen, énoncé sous la forme qu'*il existe au moins* $\alpha_0 x/(\log x)^2$ *nombres premiers* $p \leqslant x$ *tels que* $2p+1$ *ait au plus deux facteurs premiers*, que l'on a, pour $a = 0$ ou 1,

$$\sum_{\substack{p_1p_2\leqslant x\\ s_2(p_1p_2)\equiv a \,(\mathrm{mod}\, 2)}} 1 \geqslant \frac{\alpha_0 x}{2(\log x)^2}.$$

L'argument utilisé ne s'étendant pas au cas $(m, q) \neq (2, 2)$, ils montrent notamment dans [8], à l'aide de méthodes de crible, que l'on a, sous la condition $(m, q-1) = 1$,

$$\sum_{\substack{n\leqslant x\\ s_q(n)\equiv a \,(\mathrm{mod}\, m)\\ n=p_1 \text{ ou } n=p_1p_2}} 1 \gg \frac{x}{\log x}. \tag{2·18}$$

L'indétermination $n = p_1$ ou $n = p_1p_2$ est liée à ce que l'on appelle traditionnellement le phénomène de parité du crible.[(5)] À défaut d'établir la conjecture de Gelfond (2·17), nous sommes à présent en mesure de lever cette indétermination. Dans l'énoncé suivant, la lettre p, avec ou sans indice, désigne un nombre premier. Nous notons $\mathcal{E}_k(x)$ l'ensemble des entiers $n \leqslant x$ ayant exactement k facteurs premiers, comptés avec multiplicité. Une estimation classique, due à Landau, stipule que l'on a, pour $k \geqslant 1$ fixé et x tendant vers l'infini,

$$|\mathcal{E}_k(x)| \sim \frac{x(\log_2 x)^{k-1}}{(k-1)!\log x}. \tag{2·19}$$

(5) Selberg [19] et Bombieri [3] ont remarqué que les méthodes de crible dans leurs formes d'origine ne sont pas suffisantes pour distinguer les entiers qui ont un nombre pair de facteurs premiers des entiers qui en ont un nombre impair.

THÉORÈME 2.6. — *Soient $a \in \mathbb{Z}$, et $k \geqslant 2$, $q \geqslant 2$, m, des entiers tels que $(m, q-1) = 1$. L'assertion suivante est vérifiée lorsque $x \to \infty$. Pour tous les entiers n de $\mathcal{E}_{k-1}(x)$ sauf au plus $o\big(|\mathcal{E}_{k-1}(x)|\big)$ d'entre eux, il existe un nombre premier $p \leqslant m(\log_2 x)\log_3 x$ tel que $s_q(np) \equiv a \pmod m$. De plus,*

$$\sum_{\substack{n\in\mathcal{E}_k(x)\\ s_q(n)\equiv a \,(\mathrm{mod}\, m)}} 1 \gg_{k,m,q} \frac{x(\log_2 x)^{k-2}}{(\log_3 x)\log x} \asymp \frac{|\mathcal{E}_k(x)|}{(\log_2 x)\log_3 x}. \tag{2·20}$$

La suite des entiers ayant un « grand » facteur premier constitue un autre exemple pour lequel nos techniques permettent d'établir la variante *ad hoc* de la conjecture de Gelfond.

THÉORÈME 2.7. — *Soient $a \in \mathbb{Z}$, et $m \geqslant 1$, $q \geqslant 2$, des entiers tels que $(m, q-1) = 1$. L'assertion suivante est vérifiée lorsque $x \to \infty$. Pour tous les nombres premiers $p \leqslant x$ sauf au plus $o(x/\log x)$ d'entre eux, il existe un entier $h \leqslant \{mq/(q-1)\}\log_2 x$ tel que $s_q(hp) \equiv a \pmod m$.*

L'énoncé suivant, qui étend un résultat de [7], concerne les entiers dont le ℓ-ième facteur premier appartient à un intervalle donné. Nous notons

$$P_1(n) > P_2(n) > \cdots > P_{\omega(n)}(n)$$

la suite décroissante des facteurs premiers distincts d'un entier générique n.

THÉORÈME 2.8. — *Soient $a \in \mathbb{Z}$, et $\ell \geqslant 1$, $m \geqslant 1$, $q \geqslant 2$, des entiers tels que $(m, q-1) = 1$. Soient α, β deux nombres réels vérifiant $0 \leqslant \alpha < \beta \leqslant 1/\ell$. Il existe une constante $\delta = \delta(\ell, m, q, \alpha, \beta) > 0$ telle que l'on ait, pour x assez grand,*

$$|\{n \leqslant x : s_q(n) \equiv a \pmod m,\ n^\alpha < P_\ell(n) < n^\beta\}| \geqslant \delta x. \tag{2·21}$$

Fouvry et Mauduit ont montré (2·21) pour $q = m = 2$ — cf. [7], corollaire 0. Leur astucieux argument est en fait valable pour $m = 2$ et q pair. Pour $m = 2$ et q impair, le problème est facile puisque $s_q(n) \equiv n \pmod 2$. La preuve donnée dans [7] repose sur la q-additivité de la fonction s_q et sur un résultat de Balog et Ruzsa [2] relatif aux ensembles stables de densité inférieure strictement positive. Cet argument est inopérant dans le cas $m \geqslant 3$.

Notre dernière application du Théorème 2.5 est de caractère général, dans le sens où elle se rapporte à un ensemble d'entiers arbitraire uniquement soumis à une contrainte de taille. Notre motivation consiste ici à montrer comment l'on peut tirer parti de la qualité du terme d'erreur de (2·16) pour établir que des suites rares satisfont à la conjecture de Gelfond.

THÉORÈME 2.9. — *Soient $a \in \mathbb{Z}$, et $m \geqslant 1$ et $q \geqslant 2$ des entiers tels que $(m, q-1) = 1$. Soit $c_1 \in]0,1[$. Il existe deux constantes strictement positives c_2 et c_3 ne dépendant que de c_1, m et q, telles que pour tout x assez grand et pour tout ensemble $\mathcal{A} \subset \mathbb{N} \cap [1,x]$ vérifiant*

$$|\mathcal{A}| \geqslant x \exp\big\{-c_2(\log x)^{1/3}/\log_2 x\big\}, \tag{2·22}$$

il existe au moins $c_1|\mathcal{A}|$ éléments n de $\mathcal{A}$ tels que $s_q(nd) \equiv a \pmod m$ pour au moins un entier $d \in \big[1, c_3 \log\big(x/|\mathcal{A}|\big)\big]$.

Remarque. — Il découle immédiatement de (2·22) que

$$\log\big(x/|\mathcal{A}|\big) \ll (\log x)^{1/3}/\log_2 x.$$

2.3. Applications aux progressions arithmétiques.

Le Théorème 2.1 peut à l'évidence être qualitativement interprété comme l'assertion que, sous certaines conditions techniques, des conditions du type $s_q(h_j n) \equiv a_j \pmod{m_j}$ $(1 \leqslant j \leqslant r)$ sont asymptotiquement indépendantes.

Nous nous proposons ici de donner, à l'aide de (2·5), une version quantitative de cette formulation.

Étant donnés $\mathbf{h} = (h_1, \dots, h_r)$, $\mathbf{m} = (m_1, \dots, m_r)$, $\mathbf{a} = (a_1, \dots, a_r)$ dans $\mathbb{N}^{*r}$, et $d \geqslant 1$, $b \in \mathbb{Z}$, nous posons

$$\begin{aligned}
\mathcal{A}(x; \mathbf{h}, \mathbf{a}, \mathbf{m}) &:= \big\{n \leqslant x : s_q(h_j n) \equiv a_j \pmod{m_j}\,(1 \leqslant j \leqslant r)\big\},\\
A(x; \mathbf{h}, \mathbf{a}, \mathbf{m}) &:= \big|\mathcal{A}(x; \mathbf{h}, \mathbf{a}, \mathbf{m})\big|,\\
A(x; \mathbf{h}, \mathbf{a}, \mathbf{m}; b, d) &:= |\mathcal{A}(x; \mathbf{h}, \mathbf{a}, \mathbf{m}) \cap (b + d\mathbb{Z})|\\
&= \sum_{\substack{n \leqslant x,\, n \equiv b \pmod d\\ s_q(h_j n) \equiv a_j \pmod{m_j}\,(1 \leqslant j \leqslant r)}} 1.
\end{aligned} \tag{2·23}$$

Comme $s_q(h_j n) \equiv h_j n \pmod{(q-1)}$ pour tous n, j, il est clair que tout entier n compté dans $A(x; \mathbf{h}, \mathbf{a}, \mathbf{m})$ vérifie également

$$h_j n \equiv a_j \pmod{m_j^*} \qquad (1 \leqslant j \leqslant r),$$

où l'on a posé $m_j^* := (m_j, q-1)$. Il s'ensuit qu'une condition nécessaire pour que $A(x; \mathbf{h}, \mathbf{a}, \mathbf{m}; b, d)$ soit non nul pour x assez grand est la solubilité du système

$$\begin{cases} h_j n \equiv a_j \pmod{m_j^*} & (1 \leqslant j \leqslant r)\\ n \equiv b \pmod d. \end{cases} \tag{2·24}$$

Lorsqu'il en est ainsi, les solutions de (2·24) sont périodiques modulo Δ, avec

$$\Delta := \left[d, \frac{m_1^*}{(h_1, m_1^*)}, \dots, \frac{m_r^*}{(h_r, m_r^*)}\right]. \tag{2·25}$$

Ainsi, une hypothèse d'équirépartition conduit à supputer que, pour chaque indice j de $[1,r]$, la condition $s_q(h_j n) \equiv a_j \pmod{m_j}$ est réalisée modulo Δ avec probabilité m_j^*/m_j. Si ces conditions sont statistiquement indépendantes, on s'attend donc à ce que $A(x;\mathbf{h},\mathbf{a},\mathbf{m};b,d)$ soit nul ou bien approché par $\prod_{1\leqslant j\leqslant r}(m_j^*/m_j)(x/\Delta)$. C'est effectivement ce qui résulte d'une application répétée du Théorème 2.1 avec $\vartheta = k/d$, $\alpha_j = k_j/m_j$, pour $0 \leqslant k < d$, $0 \leqslant k_j < m_j$ $(1 \leqslant j \leqslant r)$. Nous en déduisons immédiatement le résultat suivant, qui généralise et précise celui de Solinas [21].

Corollaire 2.10. — *Soient $r \in \mathbb{N}^*$, $\mathbf{m} \in \mathbb{N}^{*r}$, $\mathbf{h} \in \mathbb{N}^{*r}$. On suppose que $h_1 < h_2 < \cdots < h_r$, et $q \nmid h_j$ pour $1 \leqslant j \leqslant r$. Pour tous $\mathbf{a} \in \mathbb{Z}^r$, $b \in \mathbb{Z}$, $d \geqslant 1$ tels que le système de congruences (2·24) soit soluble, on a* :

$$A(x;\mathbf{h},\mathbf{a},\mathbf{m};b,d) = \frac{x}{\Delta}\prod_{j=1}^{r}\frac{m_j^*}{m_j} + O\Big(x^{1-c_0/\{m^2 h_r \log K h_r\}}\Big), \tag{2·26}$$

où Δ est défini par (2·25), c_0 et K sont définis en (2·6), et $m := [m_1,\dots,m_r]$. La constante implicite dépend au plus de r et q.

Une version de (2·26) valable pour les intervalles courts pourrait également être obtenue par la même méthode.

En combinant le Théorème 2.1 et l'inégalité du grand crible, nous obtenons un théorème statistique de type Bombieri-Vinogradov.

Théorème 2.11. — *Soient $A > 0$, $q, r \in \mathbb{N}^*$, $\mathbf{a} \in \mathbb{Z}^r$, $\mathbf{m} \in \mathbb{N}^{*r}$ tels que*

$$(m_1 \cdots m_r, q-1) = 1.$$

Il existe une constante $x_0 = x_0(A,\mathbf{a},\mathbf{m})$ telle que, sous les conditions

$$x > x_0(r), \qquad \mathbf{h} \in \mathbb{N}^{*r}, \qquad q \nmid h_j \ (1 \leqslant j \leqslant r),$$
$$h_i \neq h_j \ (1 \leqslant i < j \leqslant r), \qquad \max_{1\leqslant j\leqslant r} h_j \leqslant \frac{\log x}{(\log_2 x)^3},$$

on ait uniformément

$$\sum_{\substack{d\leqslant D\\(q,d)=1}} \max_{b(\mathrm{mod}\, d)} \left| A(x;\mathbf{h},\mathbf{a},\mathbf{m};b,d) - \frac{x}{m_1\cdots m_r d}\right| \ll_{A,\mathbf{m},q} \frac{x}{(\log x)^A}, \tag{2·27}$$

où l'on a posé $D := \sqrt{x}/(\log x)^{A+2}$.

Dans cet énoncé, dont nous aurions pu donner également une forme relative aux intervalles courts, nous n'avons choisi l'hypothèse $(m_1 \cdots m_r, q-1) = 1$ que pour les raisons de lisibilité. Il est toutefois possible de s'en affranchir et d'obtenir, par la même technique, une version en moyenne de (2·26).

Dans le cas $r = 1$, Fouvry et Mauduit [7], [8], ont montré que (2·27) est satisfaite pour $D = x^{\gamma_q}$ avec une valeur convenable de $\gamma_q > \frac{1}{2}$. Lorsque $q = 2$, on peut choisir $\gamma_2 = 0,55$: voir le corollaire 1 de [7]. Il est établi dans [8] (cf. le théorème principal et le paragraphe VI de cet article) que γ_q tend vers 1 quand q tend vers l'infini : on a $1 - \gamma_q \ll (\log_2 q)/\log q$. Les valeurs de γ_q trouvées sont par ailleurs suffisamment grandes pour fournir (2·18) par le biais de méthodes de crible.

2.4. Valeurs moyennes à coefficients multiplicatifs.

En utilisant l'estimation (1·3) de Gelfond et le principe d'inclusion-exclusion, Newman et Slater [16] ont montré que, pour toute suite d'entiers $\mathcal{A} = \{a_j\}_{j=1}^{\infty}$ telle que $\sum_{j=1}^{\infty} 1/a_j < \infty$, on a

$$\sum_{\substack{n \leqslant x \\ s_2(n) \equiv 0 \,(\mathrm{mod}\, 2)}} \chi(n) \sim \tfrac{1}{2} \sum_{n \leqslant x} \chi(n) \qquad (x \to \infty) \tag{2·28}$$

où l'on a posé

$$\chi(n) := \begin{cases} 1 & \text{si } n \not\equiv 0 \,(\mathrm{mod}\, a_j) \ (j \geqslant 1), \\ 0 & \text{dans le cas contraire.} \end{cases}$$

La théorie des ensembles de multiples (voir par exemple [10], théorème 0.1 et corollaire 0.13) nous apprend que le membre de droite de (2·28) est asymptotiquement équivalent à $c(\mathcal{A})x$ pour une constante convenable $c(\mathcal{A}) > 0$. Il s'ensuit que

$$\sum_{\substack{n \leqslant x \\ s_2(n) \equiv 0 \,(\mathrm{mod}\, 2)}} \chi(n) = c(\mathcal{A})x + o(x) \qquad (x \to \infty). \tag{2·29}$$

Lorsque les a_j sont deux à deux premiers entre eux, la fonction χ est multiplicative. Dans le cas particulier des entiers sans facteur carré, qui correspond au choix $\mathcal{A} = \{p^2 : p \text{ premier}\}$ $(j \geqslant 1)$, Newman et Slater montrent que l'on peut remplacer le terme d'erreur de (2·29) par $O\big(x^{9/10}\sqrt{\log x}\big)$ — on a alors, bien entendu, $c(\mathcal{A}) = 3/\pi^2$. Ce dernier

résultat peut donc être interprété comme une estimation de valeur moyenne pour une fonction du type

$$n \mapsto \mathrm{e}\big(\alpha s_q(n)\big) f(n)$$

avec $\alpha \in \mathbb{Q}$ et f multiplicative : ici $q = 2$, $\alpha = \frac{1}{2}$, $f = \chi$.

Dans le même esprit, et comme illustration du champ d'application de (1·4) avec $r = 2$ et $\vartheta = 0$, Coquet [4] a montré, que, si u ou v est irrationnel, la suite de terme général $us_q(n) + v\omega(n)$ est équirépartie modulo 1. Compte tenu du critère de Weyl, cela revient à montrer que, pour tout entier $\nu \neq 0$, on a

$$\sum_{n \leqslant x} \mathrm{e}\big(\nu u s_q(n) + \nu v \omega(n)\big) = o(x) \qquad (x \to \infty).$$

Il s'agit donc d'une estimation de même type que la précédente, avec $\alpha = \nu u$ et $f(n) = \mathrm{e}\big(\nu v \omega(n)\big)$.

En incorporant, dans la méthode de convolution de Daboussi [5], une estimation issue du Théorème 2.1 et essentielle dans la preuve du Théorème 2.11, nous obtenons un résultat général de cette nature. Nous désignons par $\mathbb{M}$ la classe des fonctions arithmétiques multiplicatives complexes à valeurs dans le disque unité.

Théorème 2.12. — *Soient $q \in \mathbb{N}^*$, $r \in \mathbb{N}^*$, $\boldsymbol{\alpha} \in \mathbb{R}^r \smallsetminus \big\{\mathbb{Z}/(q-1)\big\}^r$, et $c \in]0,1[$. On pose*

$$R^*(\boldsymbol{\alpha}) := \begin{cases} 1 & \text{si } \boldsymbol{\alpha} \in \mathbb{Q}^r, \\ 4r+1 & \text{si } \boldsymbol{\alpha} \notin \mathbb{Q}^r. \end{cases}$$

Sous les conditions

$$(2\cdot30)\quad x > r,\ \mathbf{h} \in \mathbb{N}^{*r},\ 0 < h_1 < \cdots < h_r < (\log x)^{c/R^*(\boldsymbol{\alpha})},\ q \nmid h_r,\ f \in \mathbb{M},$$

on a uniformément

$$(2\cdot31)\qquad \sum_{n \leqslant x} \mathrm{e}\big(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n)\big) f(n) \ll \frac{x}{\log_2 x}.$$

3. Un résultat d'espacement et d'autres estimations préliminaires.

Ainsi que nous l'avons signalé plus haut, notre preuve du Théorème 2.1 repose sur le Théorème 2.3. Pour établir cette dernière assertion, nous avons recours à cinq résultats auxiliaires. Le premier est un résultat de crible. Nous notons $P^-(n)$ le plus petit facteur premier d'un entier n avec la convention $P^-(1) = \infty$ et nous posons

$$\Phi(x,y) := |\{n \leqslant x : P^-(n) > y\}|. \tag{3·1}$$

Lemme 3.1. — *Il existe une constante absolue z_0 telle que l'on ait uniformément pour $x \geqslant 0$, $z > z_0$, $2 \leqslant y \leqslant z^{1/3}$,*

$$\Phi(x+z,y) - \Phi(x,y) \geqslant \frac{z}{4\log y}.$$

Démonstration. — Désignons par w la fonction de Buchstab et par ϱ celle de Dickman. La minoration d'Iwaniec [13] dans le crible de Rosser fournit immédiatement, pour $D := y^s$, $s \geqslant 1$,

$$\Phi(x+z,y) - \Phi(x,y) > (z-1)\prod_{p\leqslant y}(1-1/p)\big\{f(s) - B/(\log D)^{1/3}\big\} - D$$

où $f(s) := \mathrm{e}^\gamma\{w(s) - \varrho(s-1)/s\}$, γ désigne la constante d'Euler, et B est une constante absolue. On a en particulier

$$f(3) = \tfrac{2}{3}\mathrm{e}^\gamma \log 2,$$

d'où $\frac{1}{2}(\log 2)f(3) \approx 0,2852$. Il existe donc $c \in]\frac{2}{3}, 1[$ tel que $\frac{1}{2}(\log 2)f(3c) > \frac{1}{4}$. En utilisant la minoration

$$(\log y)\prod_{p\leqslant y}(1-1/p) \geqslant \tfrac{1}{2}\log 2 \qquad (y \geqslant 2) \tag{3·2}$$

(voir par exemple la démonstration du corollaire III.3.5.1 de [24]), et en choisissant $D = z^c \geqslant y^{3c}$ et $z > z_0 = z_0(B,c)$, on obtient bien le résultat indiqué. □

Lemme 3.2. — *Soient $h \geqslant 1$, $f \geqslant 0$, $\tau \geqslant 0$, $\xi \geqslant 0$ des nombres entiers. On a*

$$s_q\big(h(\xi + fq^\tau)\big) - s_q(h\xi) = s_q\left([h\xi/q^\tau] + hf\right) - s_q\left([h\xi/q^\tau]\right). \tag{3·3}$$

Démonstration. — L'énoncé coïncide avec le lemme 2 de [21]. Pour la commodité du lecteur, nous rappelons les détails, qui sont très simples.

Soit $b := [h\xi/q^\tau]$. Il existe donc un entier v tel que

$$h\xi = v + bq^\tau, \quad 0 \leqslant v < q^\tau.$$

Il s'ensuit que

$$\begin{aligned} s_q\big(h(\xi + fq^\tau)\big) - s_q(h\xi) &= s_q\big(v + (hf+b)q^\tau\big) - s_q(v + bq^\tau) \\ &= s_q(v) + s_q(b+hf) - s_q(v) - s_q(b) \\ &= s_q(b+hf) - s_q(b). \end{aligned}$$

□

Lemme 3.3. — *Soit $r \in \mathbb{N}^*$. Il existe une constante absolue z_0 et des constantes $\varepsilon_r > 0$, $\delta_r > 0$, ne dépendant que de r, telles que, pour tout r-uplet $(\vartheta_1, \dots, \vartheta_r) \in (\mathbb{Q} \smallsetminus \mathbb{Z})^r$, $\vartheta_j = a_j/d_j$, $(a_j, d_j) = 1$, et pour tous $x \geqslant 0$, $z \geqslant \max(z_0, r^4, d_1, \dots, d_r)$, on ait*

$$\Big|\Big\{x < n \leqslant x + z : \min_{1 \leqslant j \leqslant r} \|n\vartheta_j\| > \varepsilon_r\Big\}\Big| \geqslant \delta_r z. \tag{3·4}$$

Des valeurs admissibles de ε_r et δ_r sont $\varepsilon_r := 1/(100r\log 4r)$ et $\delta_r := 1/(400\log 4r)$.

Démonstration. — Posons $R := 100r\log(4r)$ et notons $s \in [1, r]$ le nombre des indices j tels que $d_j \geqslant R$. Quitte à réordonner les ϑ_j, nous pouvons supposer que ces indices sont les s premiers et que les dénominateurs $d_{s+1}, \dots, d_r$ sont strictement inférieurs à R.

Pour chaque j de $[1, s]$, la relation $\|n\vartheta_j\| \leqslant 1/R$ équivaut à l'existence d'un entier u de $[0, d_j/R]$ tel que $a_j n \equiv \pm u \pmod{d_j}$. On a donc

$$\Big|\Big\{x < n \leqslant x+z : \min_{1 \leqslant j \leqslant s} \|n\vartheta_j\| \leqslant 1/R\Big\}\Big| \leqslant \sum_{1 \leqslant j \leqslant s} \Big(\frac{z}{d_j} + 1\Big)\Big(\frac{2d_j}{R} + 1\Big) \leqslant \frac{6rz}{R}.$$

On vérifie par une étude standard que $r/R \leqslant 1/(25\log R)$. En notant que $\max(z_0, r^4) > R^3$ pour z_0 assez grand, le Lemme 3.1 nous permet donc de déduire de ce qui précède qu'il existe au moins

$$\frac{z}{4\log R} - \frac{6z}{25\log R} = \frac{z}{100\log R} \geqslant \frac{z}{400\log 4r}$$

entiers n de $]x, x+z]$ satisfaisant $\min_{1\leqslant j\leqslant s}\|n\vartheta_j\| > 1/R$ et $P^-(n) > R$. Or, pour un tel entier n, on a trivialement $\|n\vartheta_j\| \geqslant 1/d_j > 1/R$ lorsque $s < j \leqslant r$. Cela fournit bien la conclusion annoncée. □

Remarques. — (i) Nous n'avons pas cherché ici à optimiser les valeurs de ε_r et δ_r.

(ii) On peut montrer par la même technique l'existence d'une constante ε_r^* telle que

$$\sup_{n\in\mathbb{N}} \min_{1\leqslant j\leqslant r} \|n\vartheta_j\| > \varepsilon_r^* \tag{3·5}$$

uniformément pour $(\vartheta_1, \dots, \vartheta_r) \in (\mathbb{R}\smallsetminus\mathbb{Z})^r$, avec

$$\varepsilon_r^* \geqslant 1/(30r\log 2r). \tag{3·6}$$

Il serait intéressant de disposer d'un encadrement plus précis pour cette quantité. Pour $y \geqslant 2$, $N := \prod_{p\leqslant y} p$ et en choisissant pour ϑ_j tous les rationnels de la forme $1/p$ $(p \leqslant y)$ ou a/N $(1 \leqslant a \leqslant N,\ (a,N)=1)$, on a $r = \pi(y)+\varphi(N) \sim \mathrm{e}^{-\gamma}N/\log y$ $(y\to\infty)$, alors que $\min_{1\leqslant j\leqslant r}\|n\vartheta_j\| \leqslant 1/N$ pour tout entier n. On obtient donc

$$\varepsilon_r^* \leqslant \frac{\mathrm{e}^{-\tau}+o(1)}{r\log_2 r} \qquad (r\to\infty). \tag{3·7}$$

Comme nous utilisons (3·6) pour établir (2·15) et le Théorème 2.3(i), nous donnons brièvement les détails de la preuve de cette minoration. Lorsque $r=1$, on a $\sup_n \|n\vartheta_1\| = \frac{1}{2}$ si ϑ_1 est irrationnel et

$$\sup_n \|n\vartheta_1\| = [b/2]\,/b \geqslant \tfrac{1}{4}$$

si $\vartheta_1 = a/b$ avec $(a,b)=1$ et $b\geqslant 2$. Nous pouvons donc supposer dans la suite que $r\geqslant 2$.

Soit alors R le plus petit entier tel que

$$R\prod_{p\leqslant R}(1-1/p) > 3r \tag{3·8}$$

et soit $s\in[1,r]$ le nombre des indices j tels que $\vartheta_j \in \mathbb{R}\smallsetminus\cup_{1\leqslant k\leqslant R}(\mathbb{Z}/k)$. Quitte à réordonner les ϑ_j, nous pouvons supposer que ces indices sont les s premiers et que $\vartheta_{s+1}, \dots, \vartheta_r$ sont rationnels, de dénominateurs $\leqslant R$.

Pour chaque j de $[1,s]$, la suite $\{n \geqslant 1 : \|n\vartheta_j\| < 1/R\}$ possède une densité naturelle n'excédant pas $3/R$. On a donc

$$\mathrm{dens}\big\{n \geqslant 1 : \min_{1\leqslant j\leqslant s} \|n\vartheta_j\| < 1/R\big\} \leqslant 3r/R < \prod_{p\leqslant R}(1-1/p).$$

D'après un résultat élémentaire de crible, on en déduit qu'il existe au moins un entier n tel que $P^-(n) > R$ et $\min_{1\leqslant j\leqslant s} \|n\vartheta_j\| \geqslant 1/R$. Or, pour tout entier naturel n tel que $P^-(n) > R$, on a trivialement

$$\min_{s<j\leqslant r} \|n\vartheta_j\| \geqslant 1/R.$$

On peut montrer, en utilisant la minoration (3·2), que

$$R < 30r\log r. \tag{3·9}$$

En effet, comme le membre de gauche de (3·8) est une fonction croissante de R, il suffit de montrer qu'il excède $3r$ pour $R = R^* := 30r\log r$. Or, on déduit de (3·2) par une étude standard que

$$\frac{R^*\log 2}{2\log R^*} = \frac{15(\log 2)r\log r}{\log(30r\log r)} > 3r$$

si $r \geqslant 5$. Une vérification numérique relative aux cas $r = 2,3,4$ permet d'achever la preuve de (3·9). Comme $60\log 2 > 4$, on en déduit bien le résultat souhaité.

Lemme 3.4. — *Soient $1 \leqslant h_1 < \cdots < h_t =: h$, $d|(h,q)$, $s := \omega_q + t$ et z_0, ε_s, δ_s les quantités définies au Lemme 3.3.*

(i) On a pour $z \geqslant \max(z_0, s^4, h)$, $x \geqslant 0$,

$$\Big|\Big\{x < \nu \leqslant x+z : \min_{\substack{1\leqslant j\leqslant t\\ h_j\not\equiv 0\,(\mathrm{mod}\, h/d)}} \Big\|\frac{\nu h_j d}{h}\Big\| > \varepsilon_s,\ (\nu,q)=1\Big\}\Big| \geqslant \delta_s z. \tag{3·10}$$

(ii) Soient $\varepsilon > 0$, $\nu \in \mathbb{N}$, tels que $(\nu,q) = 1$ et $\|\nu h_j d/h\| > \varepsilon$ pour tout indice j tel que $h_j \not\equiv 0\,(\mathrm{mod}\, h/d)$, et soit τ un entier tel que $q^\tau > h/\varepsilon$. On définit v par $0 \leqslant v < h$, $v \equiv -\nu q^\tau d\,(\mathrm{mod}\, h)$, et l'on pose $\xi := (\nu q^\tau d + v)/h$. On a alors

$$(a) \qquad \Big[\frac{h\xi}{q^\tau}\Big] = \nu d = 1 + \Big[\frac{h(\xi-1)}{q^\tau}\Big],$$

$$(b) \qquad \Big[\frac{h_j\xi}{q^\tau}\Big] - \Big[\frac{h_j(\xi-1)}{q^\tau}\Big] = \begin{cases} 1 & \text{si } h_j \equiv 0\,(\mathrm{mod}\, h/d)\\ 0 & \text{si } h_j \not\equiv 0\,(\mathrm{mod}\, h/d)\end{cases} \quad (1 \leqslant j \leqslant t).$$

Démonstration. — Le point (i) est obtenu en appliquant le Lemme 3.3 à l'ensemble d'au plus s nombres rationnels constitué de ceux parmi les $h_j d/h$ $(1 \leqslant j \leqslant t)$ qui ne sont pas entiers et des $1/p$ lorsque p décrit les facteurs premiers de q.

Il reste à établir le point (ii). Pour le choix indiqué de ξ et τ, on a

$$\frac{h\xi}{q^\tau} = \nu d + \frac{v}{q^\tau}, \qquad \frac{h(\xi-1)}{q^\tau} = \nu d + \frac{v-h}{q^\tau}.$$

La condition (a) est donc bien réalisée.

Montrons (b). On a

$$\frac{h_j\xi}{q^\tau} = \frac{\nu h_j d}{h} + v_j, \quad \frac{h_j(\xi-1)}{q^\tau} = \frac{\nu h_j d}{h} + v_j - \frac{h_j}{q^\tau} \qquad (1 \leqslant j \leqslant t),$$

avec $0 \leqslant v_j := vh_j/hq^\tau < h_j/q^\tau < \varepsilon$. Cela implique immédiatement que, lorsque $h_j \equiv 0 \,(\mathrm{mod}\, h/d)$,

$$\left[\frac{h_j\xi}{q^\tau}\right] = \frac{\nu h_j d}{h} = 1 + \left[\frac{h_j(\xi-1)}{q^\tau}\right].$$

Réciproquement, si $h_j \not\equiv 0 \,(\mathrm{mod}\, h/d)$, il existe des entiers λ_j, ϱ_j tels que

$$\nu h_j = \lambda_j h/d + \varrho_j, \qquad \varepsilon < \varrho_j d/h < 1 - \varepsilon,$$

d'après le choix de ν. On en déduit que

$$\frac{h_j\xi}{q^\tau} = \frac{\nu d h_j}{h} + \frac{vh_j}{hq^\tau} = \lambda_j + \frac{\varrho_j d}{h} + v_j,$$

d'où

$$\left[\frac{h_j\xi}{q^\tau}\right] = \lambda_j = \left[\frac{h_j(\xi-1)}{q^\tau}\right].$$

Cela établit bien l'équivalence énoncée en (b). □

Le dernier énoncé de ce paragraphe est une généralisation du lemme 14 de [21].

LEMME 3.5. — *Soient $q \geqslant 2$, $h \geqslant 1$, $d := (h,q)$, $\nu \geqslant 1$, $(\nu,q) = 1$. Alors il existe un entier $f \in [0, q^2/d[$ tel que*

(i) $q \nmid \left(\nu + f\dfrac{h}{d}\right)c \qquad (1 \leqslant c < d)$,

(ii) $q \mid \nu d + fh$,

(iii) $q^2 \nmid \nu d + fh$.

Démonstration. — Lorsque $d = 1$, la condition (i) est vide. Comme $(h, q) = 1$, il existe au moins un entier f, $0 \leqslant f < q^2$, tel que $fh + \nu \equiv q \pmod{q^2}$. Cet entier vérifie bien (ii) et (iii).

Nous supposons dans la suite $d \geqslant 2$. La condition (i) implique alors $dq \nmid (\nu + fh/d)d$ donc $q^2 \nmid (\nu d + fh)$. Ainsi, (iii) est une conséquence de (i) et il nous suffit d'établir (i) et (ii). Soit $q_1 := \prod_{p^j \| q,\, p \nmid h/d} p^j$. Comme $(q/d, h/d) = (q_1, h/d) = 1$, il existe un entier g, $\nu d/q \leqslant g < \nu d/q + hq/d$, satisfaisant à

$$gq/d \equiv \nu \pmod{h/d}, \qquad g \equiv 1 \pmod{q_1}.$$

En particulier, on a, pour un entier f convenable,

$$gq/d = \nu + fh/d. \tag{3·11}$$

De plus, $(g, q) = 1$ puisque tout facteur premier de q/q_1 divise h/d. Pour l'entier f défini par (3·11), la condition (i) est donc bien réalisée et l'on a

$$0 \leqslant f = gq/h - \nu d/h < q^2/d.$$

□

4. Version effective d'un résultat de Solinas : preuve du Théorème 2.3.

Soit $t \geqslant 1$ le nombre des indices j tels que $m \nmid a_j(q-1)$. Quitte à réordonner les a_j nous pouvons supposer que ces indices sont les t premiers entiers et que

$$1 \leqslant h_1 < h_2 < \cdots < h_t = h^*.$$

Nous posons

$$M_1(n) := \sum_{1 \leqslant j \leqslant t} a_j s_q(h_j n), \qquad M_2(n) := \sum_{t < j \leqslant r} a_j s_q(h_j n),$$

de sorte que $M(n) = M_1(n) + M_2(n)$ pour tout $n \geqslant 1$. Notons encore $d := (h_t, q)$, $s := t + \omega_q$, et donnons-nous des paramètres $x \geqslant 0$, $z \geqslant \max(z_0, s^4, h_t)$, que nous préciserons ultérieurement. Nous notons

$$\mathcal{E}(x, z) := \left\{ x < \nu \leqslant x + z : \min_{\substack{1 \leqslant j \leqslant t \\ h_j \not\equiv 0 \,(\mathrm{mod}\, h_t/d)}} \left\| \frac{\nu h_j d}{h_t} \right\| > \varepsilon_s,\ (\nu, q) = 1 \right\}$$

l'ensemble apparaissant au membre de gauche de (3·10) et, pour chaque entier ν de $\mathcal{E}(x,z)$, nous définissons $\xi = \xi_\nu$ et τ (indépendant de ν) comme indiqué au point (ii) du Lemme 3.4. Nous choisissons τ aussi petit que possible ; nous avons donc certainement

$$q^\tau \leqslant qh_t/\varepsilon_s. \tag{4·1}$$

Nous notons immédiatement, à fins de référence ultérieure, que (3·10) implique

$$|\mathcal{E}(x,z)| \geqslant \delta_s z. \tag{4·2}$$

La première étape de la démonstration consiste à établir que, si $f = f_\nu$ est, par exemple, le plus petit des entiers f satisfaisant aux conditions du Lemme 3.5, alors le couple

$$(\ell_\nu, n_\nu) := (\xi, \xi + fq^\tau) \tag{4·3}$$

satisfait (2·13).

À cette fin, nous observons d'abord que, pour toutes valeurs de f, ξ, τ,

$$M_2(\xi + fq^\tau) - M_2(\xi - 1 + fq^\tau) - M_2(\xi) + M_2(\xi - 1) \equiv 0 \,(\mathrm{mod}\, m). \tag{4·4}$$

En effet, pour tout j de $]t, r]$, on a $m | a_j(q-1)$. De la relation

$$s_q(n) \equiv n \,(\mathrm{mod}\,(q-1)) \qquad (n \geqslant 0),$$

nous déduisons donc que

$$a_j s_q(h_j n) \equiv a_j h_j n \,(\mathrm{mod}\, a_j(q-1)) \equiv a_j h_j n \,(\mathrm{mod}\, m).$$

Cela implique bien que le membre de gauche de (4·4) est congru modulo m à

$$\sum_{t<j\leqslant r} a_j \big\{(\xi + fq^\tau) - (\xi - 1 + fq^\tau) - \xi + (\xi - 1)\big\} = 0.$$

Ainsi, la relation (2·13) équivaut à la relation analogue obtenue en y remplaçant M par M_1. Posons encore, pour $1 \leqslant j \leqslant t$,

$$\mu_j := a_j \big\{ s_q\left(h_j(\xi + fq^\tau)\right) - s_q\left(h_j(\xi - 1 + fq^\tau)\right) - s_q(h_j\xi) + s_q\left(h_j(\xi - 1)\right) \big\},$$

de sorte que

$$M_1(\xi + fq^\tau) - M_1(\xi - 1 + fq^\tau) - M_1(\xi) + M_1(\xi - 1) = \sum_{1 \leqslant j \leqslant t} \mu_j.$$

D'après le Lemme 3.2, on a, pour $1 \leqslant j \leqslant t$,

$$\mu_j = a_j \big\{ s_q\left(b_j + h_j f\right) - s_q\left(b_j\right) - s_q\left(b'_j + h_j f\right) + s_q\left(b'_j\right) \big\}, \tag{4·5}$$

avec $b_j := [h_j \xi / q^\tau]$, $b'_j := [h_j(\xi - 1)/q^\tau]$. Le Lemme 3.4 garantit que $b_j = b'_j$, et donc $\mu_j = 0$, lorsque $h_j \not\equiv 0 \,(\mathrm{mod}\, h_t/d)$. Lorsque $j = t$, le même énoncé fournit $b_t = \nu d = 1 + b'_t$. Il suit

$$\mu_t = a_t \big\{ s_q(\nu d + h_t f) - s_q(\nu d - 1 + h_t f) - s_q(\nu d) + s_q(\nu d - 1) \big\}.$$

D'après le Lemme 3.5, on a $\nu d + h_t f = uq + vq^2$ avec $1 \leqslant u < q$. De plus $\nu d \not\equiv 0 \,(\mathrm{mod}\, q)$, puisque $(\nu, q) = 1$ et $d < q$ d'après l'hypothèse que les h_j ne sont pas divisibles par q. Nous avons donc

$$\begin{aligned} s_q(\nu d + h_t f) &= u + s_q(v), \\ s_q(\nu d) - s_q(\nu d - 1) &= 1, \\ s_q(\nu d - 1 + h_t f) &= s_q(q - 1 + (u-1)q + vq^2) = q - 1 + u - 1 + s_q(v), \end{aligned}$$

d'où

$$\mu_t = -a_t(q - 1). \tag{4·6}$$

Il reste à examiner le cas des indices $j < t$ tels que $h_j = c_j h_t/d$ avec $1 \leqslant c_j < d$. D'après le Lemme 3.4, avec le choix indiqué plus haut de ξ, on a $b'_j = b_j - 1$ pour ces valeurs de j. Nous avons alors

$$\frac{h_j \xi}{q^\tau} = \frac{c_j h_t}{dq^\tau}\Big(\frac{\nu q^\tau}{h_t/d} + \frac{v}{h_t}\Big) = c_j \nu + \frac{c_j v}{dq^\tau}.$$

Cela implique immédiatement que $b_j = c_j \nu$, $b'_j = c_j \nu - 1$. Il s'ensuit que

$$b_j + h_j f = c_j \left(\nu + f h_t/d\right) \not\equiv 0 \,(\mathrm{mod}\, q),$$

d'après le point (i) du Lemme 3.5. D'où

$$s_q\left(b_j - 1 + h_j f\right) = s_q\left(b_j + h_j f\right) - 1.$$

De même, on a $s_q(c_j\nu - 1) = s_q(c_j\nu) - 1$ puisque $c_j\nu \not\equiv 0 \pmod q$. En reportant dans (4·5), nous obtenons que $\mu_j = 0$ pour les valeurs de j considérées dans ce dernier cas.

Nous avons finalement obtenu, avec les valeurs prescrites des paramètres,

$$M(fq^\tau + \xi) - M(fq^\tau + \xi - 1) - M(\xi) + M(\xi - 1) \equiv -a_t(q-1) \pmod m.$$

Cela montre bien que le couple (ℓ_ν, n_ν) défini par (4·3) satisfait (2·13).

Dans le cas $x = 0$, nous pouvons remplacer ε_s par ε_s^* dans la définition de $\mathcal{E}(x,z)$ et majorer aisément le plus petit entier ν admissible : on a

$$1 \leqslant \nu \leqslant h_t q/d$$

puisque les conditions imposées à ν sont $[h_t, q]$-périodiques. On en déduit que la relation (2·13) a lieu pour au moins un couple (ℓ_ν, n_ν) tel que

$$\ell_\nu < n_\nu \leqslant q^\tau(q+f) + 1 \leqslant \frac{qh_t}{\varepsilon_s^*}(q + q^2/d - 1) + 1 \leqslant 2q^3 h_t/\varepsilon_s^*$$

avec toujours $s = t + \omega_q$. Compte tenu de (3·5), cela implique bien le point (i) de l'énoncé du Théorème 2.3.

Pour établir le point (ii), il est nécessaire de fixer les paramètres x et z de façon que

$$N + 1 < \ell_\nu \leqslant n_\nu \leqslant N + H \qquad \big(\nu \in \mathcal{E}(x,z)\big). \tag{4·7}$$

Nous choisissons

$$x := (N+1)h_t/(q^\tau d), \qquad z := Hh_t/(3q^\tau d). \tag{4·8}$$

Nous en déduisons que, pour $\nu \in \mathcal{E}(x,z)$,

$$\ell_\nu = \xi_\nu \geqslant \nu q^\tau d/h_t > xq^\tau d/h_t = N + 1$$

et

$$\begin{aligned} n_\nu = \xi_\nu + f_\nu q^\tau &\leqslant \nu q^\tau d/h_t + 1 + q^{\tau+2} \\ &\leqslant (x+z)q^\tau d/h_t + 1 + q^3 h_t/\varepsilon_s \\ &\leqslant N + 2 + H/3 + q^3 h_t/\varepsilon_s \leqslant N + H, \end{aligned}$$

compte tenu de (4·1) et de l'hypothèse $H > Kh^* = Kh_t$.

Pour terminer la démonstration du Théorème 2.3, il nous reste à établir que l'on peut trouver un sous-ensemble $\mathcal{E}_1$ de $\mathcal{E}(x,z)$ vérifiant $|\mathcal{E}_1| \geqslant \delta H$ et tel que les quadruplets $\mathcal{Q}_\nu := \{\ell_\nu - 1, \ell_\nu, n_\nu - 1, n_\nu\}$ soient deux à deux disjoints lorsque ν parcourt $\mathcal{E}_1$.

Nous allons montrer que, pour chaque entier ν fixé dans $\mathcal{E}(x,z)$, le nombre des entiers ν' de $\mathcal{E}(x,z)$ tels que $\mathcal{Q}_\nu \cap \mathcal{Q}_{\nu'} \neq \varnothing$ ne dépasse pas q^2/d. Cela impliquera pleinement l'existence d'un sous-ensemble $\mathcal{E}_1$ tel que, sous la condition $z > \max(z_0, s^4, h_t)$, on ait

$$|\mathcal{E}_1| \geqslant |\mathcal{E}(x,z)|d/q^2 \geqslant \delta_s z d/q^2,$$

où la seconde inégalité découle de (4·2). Comme l'hypothèse $H > Kh_t$ garantit, avec le choix de z opéré en (4·8), que $z > \max(z_0, s^4, h_t)$ et comme on a, grâce à (4·1),

$$\frac{\delta_s z d}{q^2} = \frac{\delta_s h_t H}{3q^{\tau+2}} \geqslant \frac{\varepsilon_s \delta_s}{3q^3} H \geqslant \delta H,$$

cela complétera la démonstration du Théorème 2.3.

Fixons donc $\nu \in \mathcal{E}(x,z)$ et majorons le nombre de solutions ν' de

$$\{\xi' - 1, \xi', n' - 1, n'\} \cap \{\xi - 1, \xi, n - 1, n\} \neq \varnothing, \tag{4·9}$$

où l'on a posé $\xi := \xi_\nu$, $\xi' = \xi_{\nu'}$, etc.

Nous observons d'abord que l'application $\nu \mapsto \xi$ est injective. En effet, $\xi' = \xi$ équivaut à

$$\nu q^\tau d + v = \nu' q^\tau d + v'$$

où v, $v' \in [0, h_t[$. Comme $h_t < q^\tau$, on en déduit immédiatement que $v = v'$ et donc $\nu = \nu'$. De plus, aucune des relations

$$\xi' - 1 = \xi, \quad \xi' = n - 1, \quad \xi' = n + 1, \quad n' - 1 = n$$

ne peut se produire car on a $h_t\xi \equiv h_t n \equiv v \,(\mathrm{mod}\, q^\tau)$ pour tout ν et $h_t < \frac{1}{2}q^\tau$. Ainsi la relation (4·9) implique $\xi' = n$ ou $n' = n$. Dans le premier cas, on peut écrire

$$\nu' q^\tau d + v' = \nu q^\tau d + v + h_t q^\tau f,$$

d'où, par réduction modulo q^τ, $v = v'$. Il s'ensuit que

$$\nu' = \nu + f h_t/d,$$

ce qui contredit la relation (ii) du Lemme 3.5 puisque $(\nu', q) = 1$. La seule possibilité restante de réalisation de (4·9) est donc $n' = n$, soit

$$\nu' q^\tau d + v' + h_t q^\tau f' = \nu q^\tau d + v + h_t q^\tau f.$$

Comme précédemment, on obtient que $v' = v$, et donc

$$\nu' + f' h_t/d = \nu + f h_t/d.$$

Comme $f' \in [0, q^2/d[$, il y a donc au plus q^2/d solutions. □

5. Applications aux sommes d'exponentielles.

Dans ce paragraphe nous démontrons le Théorème 2.4. Posons

$$\begin{aligned} S :=& G_r(N+H; \vartheta; \boldsymbol{\alpha}, \mathbf{h}) - G_r(N; \vartheta; \boldsymbol{\alpha}, \mathbf{h}) \\ =& \sum_{N < n \leqslant N+H} \mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n) + \vartheta n\big) \end{aligned} \tag{5·1}$$

et $Q := Q(N, H) \geqslant \delta H$. D'après le Théorème 2.3, il existe une famille $\{\mathcal{Q}_j\}_{j=1}^{Q}$ de quadruplets disjoints du type $\mathcal{Q}_j := \{\ell_j - 1, \ell_j, n_j - 1, n_j\}$ satisfaisant (2·13) et

$$N + 1 < \ell_j < n_j \leqslant N + H.$$

Si S_j désigne la contribution de $\mathcal{Q}_j$ au membre de droite de (5·1), on peut écrire

$$|S| \leqslant H - 4Q + \sum_{1 \leqslant j \leqslant Q} |S_j|. \tag{5·2}$$

On a

$$|S_j| \leqslant |\mathrm{e}(\varphi_j + \vartheta) + 1| + |\mathrm{e}(\psi_j + \vartheta) + 1| \tag{5·3}$$

avec $\varphi_j := \boldsymbol{\alpha}\cdot\mathbf{x}_j$, $\psi_j := \boldsymbol{\alpha}\cdot\mathbf{y}_j$ où l'on a posé

$$\mathbf{x}_j := s_q(\mathbf{h}\ell_j) - s_q(\mathbf{h}(\ell_j - 1)), \quad \mathbf{y}_j := s_q(\mathbf{h}n_j) - s_q(\mathbf{h}(n_j - 1)).$$

Or, nous avons, pour tous u, $v \in \mathbb{R}$,

$$\begin{aligned}\{|\mathrm{e}(u)+1|+|\mathrm{e}(v)+1|\}^2 &\leqslant 2\big\{|\mathrm{e}(u)+1|^2+|\mathrm{e}(v)+1|^2\big\}\\ &= 4\big\{2+\cos(2\pi u)+\cos(2\pi v)\big\}\\ &= 8\big\{1+\cos(\pi(u+v))\cos(\pi(u-v))\big\}\\ &\leqslant 8\big\{1+|\cos(\pi(u-v))|\big\}.\end{aligned}$$

En utilisant l'inégalité classique $|\cos \pi w| \leqslant 1-4\|w\|^2$, nous obtenons

$$|\mathrm{e}(u)+1|+|\mathrm{e}(v)+1| \leqslant 4\big\{1-\|u-v\|^2\big\} \qquad (u,v\in\mathbb{R}). \tag{5·4}$$

Soit $X := 4r(q-1)V$ et $m = m(\boldsymbol{\alpha}; X^r)$. On a donc $\|m\boldsymbol{\alpha}\| \leqslant 1/X$ et, en vertu de la définition de V,

$$\max\{|\mathbf{x}_j|, |\mathbf{y}_j|\} \leqslant r(q-1)V = \tfrac{1}{4}X.$$

D'après (2·13), les entiers $c_j := \mathbf{a}(\boldsymbol{\alpha}; X)\cdot\mathbf{x}_j$ et $d_j := \mathbf{a}(\boldsymbol{\alpha}; X)\cdot\mathbf{y}_j$ sont distincts modulo m. De plus,

$$\Big\|\varphi_j - \frac{c_j}{m}\Big\| \leqslant \frac{1}{4m}, \quad \Big\|\psi_j - \frac{d_j}{m}\Big\| \leqslant \frac{1}{4m},$$

d'où

$$\|\varphi_j - \psi_j\| \geqslant \frac{1}{2m}.$$

Il s'ensuit, grâce à (5·3) et (5·4),

$$|S_j| \leqslant 4 - 1/m^2$$

La majoration annoncée en résulte immédiatement, en reportant dans (5·2). □

6. Grandes déviations pour la loi binomiale.

Le résultat suivant servira dans la preuve du Théorème 2.1 pour estimer les cardinaux de certains ensembles. Nous exploiterons notamment l'uniformité dans les divers paramètres. Pour $0 \leqslant p \leqslant 1$, $q := 1-p$, $n \in \mathbb{N}$, $0 \leqslant v \leqslant n$, nous posons

$$S_n^+(v,p) := \sum_{k\geqslant v}\binom{n}{k}p^k q^{n-k}, \quad S_n^-(v,p) := \sum_{k\leqslant v}\binom{n}{k}p^k q^{n-k}.$$

THÉORÈME 6.1. — *Pour chaque entier naturel n et chaque nombre réel $v \in [0,n]$, $S_n^+(v,p)$ est une fonction croissante de p sur $[0,v/n]$ et $S_n^-(v,p)$ est une fonction décroissante de p sur $[v/n,1]$. De plus, pour $p \in [0,1]$, $p+q=1$, $n \geqslant 0$, $0 \leqslant t \leqslant \sigma := \sqrt{pqn}$, on a*

$$S_n^{\pm}(pn \pm t\sigma, p) \leqslant \mathrm{e}^{-t^2/3}. \tag{6·1}$$

Démonstration. — Les assertions de monotonie résultent d'un banal calcul de dérivée dont nous omettons les détails. Soit $\varepsilon := tq/\sigma \leqslant q \leqslant 1$, de sorte que $\varepsilon pn = t\sigma$. Pour tout $x \geqslant 1$, nous avons

$$S_n^+(pn+t\sigma,p) \leqslant \sum_{k \geqslant (1+\varepsilon)pn} \binom{n}{k} p^k q^{n-k} x^{k-(1+\varepsilon)pn} \leqslant \frac{(px+q)^n}{x^{(1+\varepsilon)pn}}.$$

Choisissons optimalement $x := \mu/\lambda$ avec $\mu := 1+\varepsilon$, $\lambda := 1-\varepsilon p/q$. La majoration précédente vaut alors $(\lambda^{-q\lambda}\mu^{-p\mu})^n$.

Utilisons les inégalités

$$\begin{aligned}(1-u)\log\Big(\frac{1}{1-u}\Big) &\leqslant u - \tfrac{1}{2}u^2 \qquad (0 \leqslant u \leqslant 1),\\ (1+u)\log(1+u) &\geqslant u + \tfrac{1}{2}u^2 - \tfrac{1}{6}u^3 \qquad (0 \leqslant u \leqslant 1),\end{aligned}$$

d'où

$$\begin{aligned}-q\lambda\log\lambda &= q(1-\varepsilon p/q)\log\Big(\frac{1}{1-\varepsilon p/q}\Big) \leqslant \varepsilon p - \tfrac{1}{2}\varepsilon^2 p^2/q,\\ -p\mu\log\mu &= -p(1+\varepsilon)\log(1+\varepsilon) \leqslant -p\varepsilon - \tfrac{1}{2}p\varepsilon^2 + \tfrac{1}{6}p\varepsilon^3.\end{aligned}$$

Il suit

$$S_n^+(pn+t\sigma,p) \leqslant \exp\{-\tfrac{1}{2}\varepsilon^2 np/q + \tfrac{1}{6}np\varepsilon^3\} = \exp\{-\tfrac{1}{2}t^2 + \tfrac{1}{6}t^3q^2/\sigma\}.$$

Nous estimons $S_n^-(pn-t\sigma,p)$ en remarquant que, posant $\eta := \varepsilon p/q \leqslant p \leqslant 1$,

$$\begin{aligned}S_n^-(pn-t\sigma,p) &= \sum_{j>(1+\eta)qn} \binom{n}{j} q^j p^{n-j}\\ &\leqslant S_n^+(qn+t\sigma,q))\\ &\leqslant \exp\{-\tfrac{1}{2}\eta^2 nq/p + \tfrac{1}{6}nq\eta^3\} = \exp\{-\tfrac{1}{2}t^2 + \tfrac{1}{6}t^3p^2/\sigma\}.\end{aligned}$$

Les inégalités (6·1) s'obtiennent en majorant trivialement $\frac{1}{6}t^3\max(p,q)^2/\sigma$ par $\frac{1}{6}t^2$. □

Étant donnée une puissance de q explicite ou implicite $\varrho = q^\nu$, nous employons, dans la fin de ce paragraphe et dans tout le suivant, la notation (2·1) pour le développement de n en base ϱ. On a donc $0 \leqslant e_j(n) < \varrho$ pour tout indice j et $e_j(n) = 0$ pour j assez grand.

Nous utilisons le Théorème 6.1 dans la preuve du résultat suivant.

LEMME 6.2. — *Soient $q \geqslant 2$, $h \geqslant 1$, $\varrho := q^\nu > 30h$, $E \in \mathbb{N}$, $D \in \mathbb{N}^*$, $x \geqslant 0$ et $y > 2\varrho^{E+D}$. Si $\kappa_E^*(n)$ désigne le nombre des indices j de $]E, E+D]$ tels que*

$$e_{j-1}(n) \leqslant \varrho/6h < e_j(n),$$

alors on a

$$\kappa_E^*(n) > D/(16h) \tag{6·2}$$

pour tous les entiers n de $]x, x+y]$ sauf au plus $5(y+\varrho^{E+D})\mathrm{e}^{-D/(480h)}$ exceptions.

Démonstration. — Nous commençons par établir la majoration

$$|\{0 \leqslant m < \varrho^D : \kappa_0^*(m) \leqslant D/16h\}| \leqslant 5\varrho^D \mathrm{e}^{-D/(480h)}. \tag{6·3}$$

Sur l'espace $\Omega_D := \{m : 0 \leqslant m < \varrho^D\}$ muni de la probabilité uniforme, les fonctions e_j $(0 \leqslant j < D)$ sont des variables aléatoires indépendantes de même loi, uniforme sur $\{0, 1, \dots, \varrho - 1\}$. Posons

$$\kappa^+(m) := |\{j \in [1, D] \ : e_{j-1}(m) \leqslant \varrho/6h\}|,$$
$$\kappa^-(m) := |\{j \in [1, D[: \max\{e_{j-1}(m), e_j(m)\} \leqslant \varrho/6h\}|.$$

On a alors trivialement

$$\kappa_0^*(m) \geqslant \kappa^+(m) - \kappa^-(m).$$

Sur Ω_D, κ^+ est une variable aléatoire binomiale d'ordre D et de paramètre

$$(1 + [\varrho/6h])/\varrho > 1/6h.$$

D'après le Théorème 6.1, on a donc, pour tout $t \geqslant 0$,

$$\kappa^+(m) > D/8h \tag{6·4}$$

pour tous les entiers $m < \varrho^D$ sauf au plus

$$\varrho^D S_D^-\Big(\frac{D}{8h}, \frac{1}{6h}\Big) = \varrho^D S_D^-\Big(\frac{D}{6h} - t\sqrt{\frac{D}{6h}}, \frac{1}{6h}\Big) \leqslant \varrho^D \mathrm{e}^{-t^2/3}$$

d'entre eux, avec $t := \frac{1}{4}\sqrt{D/(6h)}$. Le nombre des exceptions à (6·4) n'excède donc pas

$$\varrho^D \mathrm{e}^{-D/(288h)}.$$

On ne peut pas appliquer directement le même raisonnement pour obtenir une majoration de $\kappa^-(m)$ car cette fonction ne suit pas une loi binomiale sur Ω_D. Cependant, notant $D_0 := [(D-1)/2]$, $D_1 := [D/2]$, on a $\kappa^-(m) = \kappa_0(m) + \kappa_1(m)$ pour tout m, avec

$$\kappa_0(m) := |\{j \in [1, D_0] \,:\, \max\{e_{2j-1}(n), e_{2j}(n)\} \leqslant \varrho/(6h)\}|,$$
$$\kappa_1(m) := |\{j \in [0, D_1[\,:\, \max\{e_{2j}(n), e_{2j+1}(n)\} \leqslant \varrho/(6h)\}|.$$

Les fonctions κ_i $(i = 0, 1)$ sont des variables binomiales sur Ω_D, de même paramètre

$$(1 + [\varrho/6h])^2/\varrho^2 \leqslant 1/(25h^2) < 1/(25h).$$

Il s'ensuit que les inégalités

$$\kappa_i(m) < \frac{D_i}{16h} \qquad (i = 0, 1)$$

ont lieu pour tous les entiers $m < \varrho^D$ sauf au plus

$$\varrho^D S_{D_i}^+\left(\frac{D_i}{25h} + \sqrt{\frac{D_i}{80h}}\sqrt{\frac{D_i}{25h}}, \frac{1}{25h}\right) \leqslant \varrho^D \mathrm{e}^{-D_i/(240h)}$$

exceptions. Nous obtenons donc, avec la majoration annoncée pour le nombre des cas exceptionnels,

$$\kappa_0^*(n) > \frac{D}{8h} - \frac{D_0 + D_1}{16h} \geqslant \frac{D}{16h}.$$

Cela établit bien (6·3).

Pour terminer la démonstration du Lemme 6.2, remarquons que, si $n = a + \varrho^E m + \varrho^{E+D} s$ avec $0 \leqslant m < \varrho^D$, $s \geqslant 0$, alors $\kappa_E^*(n) = \kappa_0^*(m)$. Nous en déduisons que

$$\sum_{\substack{x < n \leqslant x+y \\ \kappa_E^*(n) \leqslant D/(16h)}} 1 = \sum_{0 \leqslant a < \varrho^E} \sum_{\substack{0 \leqslant m < \varrho^D \\ \kappa_0^*(m) \leqslant D/(16h)}} \sum_{\substack{x < n \leqslant x+y \\ n \equiv a + m\varrho^E \,(\mathrm{mod}\, \varrho^{E+D})}} 1$$
$$\leqslant \Big(\frac{y}{\varrho^{E+D}} + 1\Big)\frac{5\varrho^{E+D}}{\mathrm{e}^{D/(480h)}} = \frac{5\big(y + \varrho^{E+D}\big)}{\mathrm{e}^{D/(480h)}}.$$

□

7. Preuve du Théorème 2.1.

Soit K la constante apparaissant dans (2·4). Quitte à altérer K_0, nous pouvons supposer $K > 15$. Notons ϱ la plus petite puissance de q excédant $2Kh$. On a donc

$$30h < 2Kh < \varrho \leqslant 2Kqh.$$

Soient $E \geqslant 0$, $D \geqslant 1$ des entiers tels que $y > 2\varrho^{E+D}$. Désignons par G_r^* la contribution à $G_r(x, y; \vartheta; \boldsymbol{\alpha}, \mathbf{h}, \mathbf{k})$ des entiers n satisfaisant (6·2). D'après le Lemme 6.2, nous avons

$$\begin{aligned} |G_r(x, y; \vartheta; \boldsymbol{\alpha}, \mathbf{h}, \mathbf{k}) - G_r^*| &\leqslant 5(y + \varrho^{E+D})\mathrm{e}^{-D/(480h)} \\ &\leqslant 8y\mathrm{e}^{-\delta D/(80hm^2)}, \end{aligned} \tag{7·1}$$

puisque $\delta/(80m^2) \leqslant \frac{1}{480}$ pour la valeur indiquée de δ. Nous pouvons nous limiter à estimer G_r^*.

Pour chaque entier n compté dans G_r^*, désignons par $j_1 < \cdots < j_{\kappa(n)}$ les indices j de $]E, E + D]$ satisfaisant à

$$e_{j-1}(n) \leqslant \varrho/(6h). \tag{7·2}$$

Convenons que $j_0 = 0$, $j_{\kappa(n)+1} = \infty$, et posons

$$n_i := \varrho^{-j_i} \sum_{j_i \leqslant t < j_{i+1}} e_t(n)\varrho^t \qquad \big(0 \leqslant i \leqslant \kappa(n)\big),$$

de sorte que l'on a identiquement, si $\kappa(n) = \kappa$,

$$n = \sum_{0 \leqslant i \leqslant \kappa} n_i \varrho^{j_i}. \tag{7·3}$$

Notant alors

$$d_i := j_{i+1} - j_i \quad (0 \leqslant i < \kappa),$$

nous déduisons de l'inégalité (6·2) que $d_i \geqslant 2$ pour au moins $\kappa_E^*(n) - 1 > D/(16h) - 1$ valeurs de $i \in [1, \kappa[$. De plus, comme

$$\sum_{1 \leqslant i < \kappa} d_i = j_\kappa - j_1 \leqslant D,$$

il y a au plus $D/(20h)$ valeurs de $i \in [1, \kappa[$ telles que $d_i > 20h$. Ainsi, pour chaque entier n compté dans G_r^*, il existe au moins

$$\kappa_D := \frac{D}{16h} - 1 - \frac{D}{20h} = \frac{D}{80h} - 1$$

valeurs de $i \in [1, \kappa(n)[$ telles que

$$2 \leqslant d_i \leqslant 20h. \tag{7·4}$$

Posons encore, pour chaque entier n fixé tel que $\kappa(n) = \kappa$,

$$\mathbf{j} := (j_1, \dots, j_\kappa),$$

et, notant ponctuellement $\mu(b; u, v) := \min_{u \leqslant t < v} e_t(b)$,

(7·5)

$$\mathcal{N}_i(\mathbf{j}) := \begin{cases} \left\{ b + e\varrho^{d_0-1} : 0 \leqslant b < \varrho^{d_0-1}, \mu(b; E, d_0 - 1) > \dfrac{\varrho}{6h} \geqslant e \right\} \\ \qquad\qquad (i = 0), \\ \left\{ b + e\varrho^{d_i-1} : 0 \leqslant b < \varrho^{d_i-1}, \mu(b; 0, d_i - 1) > \dfrac{\varrho}{6h} \geqslant e \right\} \\ \qquad\qquad (1 \leqslant i < \kappa), \\ \left\{ 0 \leqslant b \leqslant (x+y)/\varrho^{j_\kappa} : \mu(b; 0, D + E - j_\kappa) > \dfrac{\varrho}{6h} \right\} \\ \qquad\qquad (i = \kappa). \end{cases}$$

On a clairement, avec la notation (7·3),

$$n_i \in \mathcal{N}_i(\mathbf{j}) \qquad (0 \leqslant i \leqslant \kappa). \tag{7·6}$$

Réciproquement, chaque entier n de $]x, x+y]$ compté dans G_r^* possède une décomposition unique sous la forme (7·3) satisfaisant aux conditions (7·6).

Posons

$$p_h := \varrho - 1 - [\varrho/6h], \qquad q_h := 1 + [\varrho/6h].$$

Nous observons dès à présent que l'on a trivialement

$$|\mathcal{N}_i(\mathbf{j})| \leqslant \begin{cases} \varrho^E p_h^{d_0-1-E} q_h & (i = 0), \\ p_h^{d_i-1} q_h & (1 \leqslant i < \kappa), \\ (x+y) p_h^{E+D-j_\kappa} \varrho^{-E-D} & (i = \kappa). \end{cases} \tag{7·7}$$

En effet, lorsque $i<\kappa$, on a $\varrho/(6h)<e_t(n)\leqslant\varrho-1$ si $\max(j_i,E)\leqslant t<j_{i+1}-1$ et $0\leqslant e_t(n)\leqslant\varrho/(6h)$ si $t=j_{i+1}-1$ et, lorsque $i=\kappa$, on a $\varrho/(6h)<e_t(n)\leqslant\varrho-1$ pour tout indice t tel que $j_\kappa\leqslant t<E+D$.(6)

Notre démonstration repose essentiellement sur l'observation que l'on a, pour tous $i\in[0,\kappa[$, $s\in[1,r]$,

$$\begin{aligned}(7{\cdot}8)\qquad h_s\sum_{0\leqslant t\leqslant i}n_t\varrho^{j_t}&\leqslant h_s\sum_{0\leqslant j<j_{i+1}-1}(\varrho-1)\varrho^j+\frac{h_s\varrho}{6h}\varrho^{j_{i+1}-1}\\&\leqslant\Big(\frac{h_s}{\varrho}+\frac{h_s}{6h}\Big)\varrho^{j_{i+1}}<\tfrac13\varrho^{j_{i+1}}.\end{aligned}$$

Il s'ensuit que, pour tous $\mathbf{k}$, $\mathbf{k}'$, $\mathbf{k}''\in\mathbb{N}^r$, $s\in\mathbb{N}^*$, vérifiant $\mathbf{k}=\mathbf{k}'+\varrho^{E+D}\mathbf{k}''$, $\|\mathbf{k}'\|_\infty<\varrho^E$, $1\leqslant s\leqslant r$, nous avons

$$\begin{aligned}s_q(h_sn+k_s)&=s_q\bigg(h_s\sum_{0\leqslant i\leqslant\kappa}n_i\varrho^{j_i}+k_s\bigg)\\&=s_q\big(h_sn_0+k_s'\big)+\sum_{1\leqslant i<\kappa}s_q(h_sn_i)+s_q\big(h_\kappa n_\kappa+k_s''\varrho^{E+D-j_\kappa}\big)\end{aligned}$$

et donc

$$(7{\cdot}9)\qquad\boldsymbol{\alpha}{\cdot}s_q(\mathbf{h}n+\mathbf{k})=\boldsymbol{\alpha}{\cdot}s_q\big(\mathbf{h}n_0+\mathbf{k}'\big)+\sum_{1\leqslant i<\kappa}\boldsymbol{\alpha}{\cdot}s_q(\mathbf{h}n_i)+\boldsymbol{\alpha}{\cdot}s_q\big(\mathbf{h}n_\kappa+\mathbf{k}''\varrho^{E+D-j_\kappa}\big).$$

Soit $\mathcal{J}_\kappa$ l'ensemble des κ-uplets $\mathbf{j}=(j_1,\dots,j_\kappa)\in]E,E+D]^\kappa$ tels que les différences $d_i=j_{i+1}-j_i$ satisfassent (7·4) pour au moins κ_D valeurs de i. Nous déduisons de ce qui précède que

$$\begin{aligned}(7{\cdot}10)\qquad G_r^*=&\sum_{\kappa_D<\kappa\leqslant D}\sum_{\mathbf{j}\in\mathcal{J}_\kappa}\sum_{n_0\in\mathcal{N}_0(\mathbf{j})}\cdots\\&\cdots\sum_{n_{\kappa-1}\in\mathcal{N}_{\kappa-1}(\mathbf{j})}\prod_{0\leqslant i<\kappa}\varphi_i(n_i)\sum_{(x-m_\kappa)/\varrho^{j_\kappa}<n_\kappa\leqslant(x+y-m_\kappa)/\varrho^{j_\kappa}}\varphi_\kappa(n_\kappa),\end{aligned}$$

où l'on a posé

$$\begin{aligned}\varphi_0(\nu)&:=\mathrm{e}\big(\boldsymbol{\alpha}{\cdot}s_q(\mathbf{h}\nu+\mathbf{k}')+\vartheta\nu\big),\\\varphi_i(\nu)&:=\mathrm{e}\big(\boldsymbol{\alpha}{\cdot}s_q(\mathbf{h}\nu)+\vartheta\varrho^{j_i}\nu\big)\qquad(1\leqslant i<\kappa),\\\varphi_\kappa(\nu)&:=\mathrm{e}\big(\boldsymbol{\alpha}{\cdot}s_q\big(\mathbf{h}\nu+\mathbf{k}''\varrho^{E+D-j_\kappa}\big)+\vartheta\varrho^{j_\kappa}\nu\big),\end{aligned}$$

(6) L'estimation relative à $i=\kappa$ ne nous servira pas dans la suite.

et $m_\kappa := n_0 + n_1\varrho^{j_1} + \cdots + n_{\kappa-1}\varrho^{j_{\kappa-1}}$. Comme $m_\kappa/\varrho^{j_\kappa} < 1$ d'après (7·8), la somme intérieure vaut

$$\sum_{x/\varrho^{j_\kappa} < n_\kappa \leqslant (x+y)/\varrho^{j_\kappa}} \varphi_\kappa(n_\kappa) + O(1)$$

où la constante implicite n'excède pas 2. La contribution globale du dernier terme d'erreur peut alors être aisément estimée en faisant appel à (7·7) : elle est

$$\begin{aligned}
&\leqslant \sum_{\kappa_D < \kappa \leqslant D} \sum_{\mathbf{j}\in\mathcal{J}_\kappa} \prod_{0\leqslant i<\kappa} |\mathcal{N}_i(\mathbf{j})| \leqslant 2\varrho^E p_h^{-E} \sum_{\kappa_D<\kappa\leqslant D} \sum_{\mathbf{j}\in\mathcal{J}_\kappa} p_h^{j_\kappa-\kappa} q_h^\kappa \\
&\leqslant 2\varrho^E \sum_{E<j\leqslant E+D} \sum_{1\leqslant\kappa\leqslant j-E} \binom{j-E}{\kappa-1} p_h^{j-E-\kappa} q_h^\kappa \\
&\leqslant 2\varrho^E \sum_{E<j\leqslant E+D} \sum_{0\leqslant k\leqslant j-E} \binom{j-E}{k} p_h^{j-E-k-1} q_h^{k+1} \\
&\leqslant 2q_h p_h^{-1} \sum_{E<j\leqslant E+D} \varrho^j \leqslant 4\varrho^{E+D}.
\end{aligned} \tag{7·11}$$

Nous pouvons donc écrire

$$\left| G_r^* - \sum_{\kappa_D<\kappa\leqslant D} \sum_{\mathbf{j}\in\mathcal{J}_\kappa} \prod_{0\leqslant i\leqslant\kappa} S_i(\mathbf{j}) \right| \leqslant 4\varrho^{E+D} \tag{7·12}$$

avec

$$S_i(\mathbf{j}) := \begin{cases} \displaystyle\sum_{n_i\in\mathcal{N}_i(\mathbf{j})} \varphi_i(n_i) & (0\leqslant i<\kappa), \\ \displaystyle\sum_{\substack{x/\varrho^{j_\kappa} < n_\kappa \leqslant (x+y)/\varrho^{j_\kappa} \\ n_\kappa\in\mathcal{N}_\kappa(\mathbf{j})}} \varphi_\kappa(n_\kappa) & (i=\kappa)\ . \end{cases}$$

Il reste à estimer les $S_i(\mathbf{j})$. Nous déduisons de (7·5) que, pour $1\leqslant i<\kappa$, et si $d_i > 1$,

$$S_i(\mathbf{j}) = \sum_{0\leqslant f\leqslant \varrho/(6h)} \sum_{0\leqslant b<\varrho^{d_i-2}}{}^{*} \sum_{\varrho/6h<g<\varrho} \mathrm{e}\big(\lambda(f,b,g)\big) \tag{7·13}$$

où l'on a posé

$$\lambda(f,b,g) := \boldsymbol{\alpha}\cdot s_q\big(\mathbf{h}\big(g+\varrho b+f\varrho^{d_i-1}\big)\big) + \vartheta g\varrho^{j_i} + \vartheta b\varrho^{j_i+1} + \vartheta f\varrho^{j_{i+1}-1}$$

et où l'astérisque indique que la sommation est restreinte aux entiers b dont tous les chiffres sont $> \varrho/6h$, avec la convention que cette sommation est omise si $d_i = 2$. Pour tout triplet (f, b, g) du domaine de sommation, nous avons

$$g + \varrho b + f\varrho^{d_i-1} < \varrho + \varrho^{d_i-1} + \varrho^{d_i}/6h < \varrho^{d_i}.$$

Sous l'hypothèse (7·4) et avec la valeur de m donnée par (2·2), le Théorème 2.4 nous permet donc d'affirmer que la somme intérieure de (7·13) n'excède pas

$$(1 - \delta/m^2)p_h.$$

En estimant alors trivialement les sommes sur f et b, nous obtenons

$$|S_i(\mathbf{j})| \leqslant (1 - \delta/m^2)p_h^{d_i-1}q_h. \tag{7·14}$$

Reportons dans (7·12), en employant (7·14) lorsque $1 \leqslant i < \kappa$ et (7·4) a lieu et la majoration triviale issue de (7·7) dans le cas contraire et lorsque $i = 0$ ou κ. En tenant compte du fait que les éléments de $\mathcal{J}_\kappa$ sont tels que $2 \leqslant d_i \leqslant 20h$ pour au moins κ_D valeurs de $i \in [1, \kappa[$, nous obtenons

$$\begin{aligned}
\big|G_r^*\big| &\leqslant (1 - \delta/m^2)^{\kappa_D}\varrho^E p_h^{-E} \sum_{\kappa_D < \kappa \leqslant D} \sum_{\mathbf{j} \in \mathcal{J}_\kappa} p_h^{j_\kappa - \kappa} q_h^\kappa \left(2y\varrho^{-j_\kappa}\right) + \mathcal{R} \\
&\leqslant 2y(1 - \delta/m^2)^{\kappa_D} \sum_{1 \leqslant \kappa \leqslant D} \sum_{\kappa \leqslant j \leqslant D+E} \binom{j-E}{\kappa-1} p_h^{j-E-\kappa} q_h^\kappa \varrho^{E-j} + \mathcal{R} \\
&\leqslant 2y\mathrm{e}^{-\delta\kappa_D/m^2} \sum_{E < j \leqslant E+D} \varrho^{E-j} \sum_{0 \leqslant k \leqslant j-1} \binom{j-E}{k} p_h^{j-E-k-1} q_h^{k+1} + \mathcal{R} \\
&\leqslant 3yD\frac{q_h}{p_h}\mathrm{e}^{-\delta D/(80hm^2)} + \mathcal{R},
\end{aligned}$$

avec $|\mathcal{R}| \leqslant 4\varrho^{E+D}$. Grâce à (7·1), et en remarquant que $q_h/p_h \leqslant 1/h$, nous obtenons bien (2·3).

Pour établir (2·5), nous observons que sous l'hypothèse supplémentaire $\|\mathbf{k}\| \leqslant \sqrt{y}$, nous pouvons choisir $E = 1 + [(\log y)/2\log\varrho] + 1$, $\mathbf{k}'' = \mathbf{0}$, $D := [(\log y)/(4\log\varrho)]$, de sorte que $\varrho^{E+D} \ll y^{3/4}$.

8. Preuve du Théorème 2.5.

Étant donnés $m \geqslant 2$ et $\mathbf{h} \in \mathbb{N}^{*r}$ satisfaisant aux hypothèses de l'énoncé, nous posons

$$\chi_j(d) := \frac{1}{m-1} \sum_{1 \leqslant \nu < m} \mathrm{e}\Big(\frac{\nu\{s_q(h_j d) - a_j\}}{m}\Big) = \begin{cases} \dfrac{-1}{m-1} & \text{si } s_q(h_j d) \not\equiv a_j \pmod m, \\ 1 & \text{si } s_q(h_j d) \equiv a_j \pmod m, \end{cases}$$

de sorte que

$$S(x;\mathbf{h};\mathbf{a},m) = \Big(1 - \frac{1}{m}\Big)^r \sum_{d \leqslant x} \prod_{1 \leqslant j \leqslant r} \{1 - \chi_j(d)\}. \tag{8·1}$$

En développant ce produit et en intervertissant l'ordre des sommations, nous obtenons

$$\frac{S(x;\mathbf{h};\mathbf{a},m)}{\big(1-1/m\big)^r} = x + \sum_{1 \leqslant k \leqslant r} \frac{(-1)^k}{(m-1)^k} \sum_{1 \leqslant j_1 < \ldots < j_k \leqslant r} \sum_{\boldsymbol{\nu} \in [1,m[^k} G(x;\mathbf{j},\boldsymbol{\nu}), \tag{8·2}$$

où l'on a posé

$$G(x;\mathbf{j},\boldsymbol{\nu}) := \sum_{d \leqslant x} \mathrm{e}\Big(\sum_{1 \leqslant i \leqslant k} \frac{\nu_j}{m} (s_q(h_{j_i} d) - a_{j_i}) \Big).$$

La somme $G(x;\mathbf{j},\boldsymbol{\nu})$ peut être estimée grâce au Théorème 2.1 : elle est $\ll x^{1-\eta}$ avec

$$\eta = \frac{c_1}{q^3 s (\log 4s)^2 m^2 h \log\{K_0 H q^3 s^5 \log s\}},$$

où nous avons posé $s := r + \omega(q)$. On en déduit

$$S(x;\mathbf{h};\mathbf{a},m) = x\big(1-1/m\big)^r \Big\{ 1 + O\Big(x^{-\eta} \sum_{1 \leqslant k \leqslant r} \binom{r}{k} \Big) \Big\}.$$

Cela implique bien (2·16) avec la valeur annoncée pour $c_2(q)$.

Il reste à établir la seconde assertion de l'énoncé, relative à la taille de la fonction $d \mapsto n_d$.

Soient $\varepsilon > 0$ et $\xi(d)$ une fonction tendant vers l'infini avec d. Pour tout $H > 0$, on a

$$\sum_{\substack{d\leqslant x\\ n_d>\xi(d)}} 1 \leqslant \sum_{\substack{d\leqslant x\\ n_d>H}} 1 + O_H(1). \tag{8·3}$$

Pour majorer le cardinal figurant au membre de droite, nous appliquons (2·16) avec $\{h_1,\dots,h_r\} = \{1 \leqslant h \leqslant H : q \nmid h\}$ et donc $r = H(1-1/q)+O(1)$. Nous obtenons, pour une constante convenable $c_3(q) > 0$, l'estimation

$$\begin{aligned}\sum_{\substack{d\leqslant x\\ n_d>H}} 1 &\ll_{m,q} x\big(1-1/m\big)^{H(1-1/q)}\Big\{1+2^H x^{-c_3(q)/m^2H^2(\log H)^3}\Big\}\\ &\leqslant \varepsilon x,\end{aligned}$$

pour $H > H_0(\varepsilon, m)$ et $x > x_0(H)$. Cela implique bien la conclusion annoncée.

9. Applications du Théorème 2.5 : preuves des résultats du §2.2.

9.1. Preuve du Théorème 2.6.

Pour établir la première assertion du Théorème 2.6, nous choisissons

$$\{h_1,\dots,h_r\} = \big\{p \leqslant m(\log_2 x)\log_3 x : p \nmid q\big\}, \tag{9·1}$$

de sorte que $r = \{m + o(1)\}\log_2 x$. Le nombre des entiers n n'excédant pas x et tels que $s_q(np) \not\equiv a \pmod m$ pour tout nombre premier $p \leqslant m(\log_2 x)\log_3 x$ vaut donc exactement $S(x;\mathbf{h};\mathbf{a},m)$ lorsque $\mathbf{a} := (a,\dots,a)$. Or, en vertu de (2·16), nous avons

$$S(x;\mathbf{h};\mathbf{a},m) \ll x\big(1-1/m\big)^r = o\Big(\frac{x}{\log x}\Big). \tag{9·2}$$

D'après (2·19), cette majoration est $o\big(|\mathcal{E}_{k-1}(x)|\big)$, pour tout $k \geqslant 2$ fixé. Cela fournit bien la conclusion souhaitée.[7]

[7] Nous aurions en fait pu obtenir une majoration légèrement plus précise pour le plus petit nombre premier p réalisant la congruence $s_q(np) \equiv a \pmod m$, soit $p \leqslant A(\log_2 x)\log_3 x$ pour toute constante $A > 1/|\log(1-1/m)|$. Comme la borne trouvée n'a pas de signification particulière, nous avons privilégié sur ce point la simplicité de l'énoncé.

En remplaçant m par $2m$ dans (9·1) et en appliquant (9·2) avec

$$y = x/\{2m(\log_2 x)\log_3 x\}$$

au lieu de x, il vient

$$\sum_{\substack{n\in\mathcal{E}_k(x)\\ s_q(n)\equiv a\,(\mathrm{mod}\,m)}} 1 \gg |\mathcal{E}_{k-1}(y)| \gg \frac{x(\log_2 x)^{k-3}}{(\log x)\log_3 x}.$$

Ce résultat est légèrement inférieur à l'estimation annoncée (2·20). Nous obtenons une amélioration en appliquant cette technique à chaque élément d'une partition de l'ensemble dont le cardinal est à minorer.

À cette fin, nous introduisons les ensembles $\mathcal{E}_k(x,y) := \{n \in \mathcal{E}_k(x) : P^-(n) > y\}$, et nous notons que l'évaluation

$$(9\cdot3)\quad |\mathcal{E}_k(x,y)| \asymp \frac{x}{\log x}\frac{(\log u)^{k-1}}{(k-1)!} \quad \big(\tfrac{3}{2} \leqslant y \leqslant \mathrm{e}^{(\log x)^{2/5}},\ 1 \leqslant k \ll \log u\big),$$

où l'on a posé $u := (\log x)/\log y$, est une conséquence faible des estimations de Balazard dans [1]. Posons alors

$$T_j := 2mj(\log_2 x)\log_3 x \qquad \big(1 \leqslant j \leqslant J := \big[(\log x)^{1/4}\big]\big).$$

En appliquant (2·16) à x/T_{j+1} avec $\{h_1,\dots,h_r\} := \big\{p \in \big]T_j, T_{j+1}\big] : p \nmid q\big\}$ et en tenant compte de (9·3), nous obtenons, pour tout $k \geqslant 2$ fixé,

$$\sum_{\substack{n\in\mathcal{E}_k(x)\\ T_j<P^-(n)\leqslant T_{j+1}\\ s_q(n)\equiv a\,(\mathrm{mod}\,m)}} 1 \gg \left|\mathcal{E}_{k-1}\Big(\frac{x}{T_{j+1}}, T_{j+1}\Big)\right| \gg \frac{x(\log_2 x)^{k-2}}{T_{j+1}(\log x)} \qquad (1 \leqslant j \leqslant J).$$

L'évaluation souhaitée (2·20) en découle immédiatement par sommation sur j.

9.2. Preuve du Théorème 2.7.

Il suffit d'appliquer le Théorème 2.5 en choisissant

$$\{h_1,\dots,h_r\} = \{h \leqslant \{qm/(q-1)\}\log_2 x : q \nmid h\}.$$

Ici encore, nous aurions pu remplacer la constante m par toute constante A vérifiant $A > 1/|\log(1-1/m)|$.

9.3. Preuve du Théorème 2.8.

Posons $\mathcal{C} := \{n \geqslant 1 : n^\alpha < P_\ell(n) < n^\beta\}$. Cet ensemble est de densité positive : le cas $\ell = 1$ correspond aux entiers friables, et le cas $\ell \geqslant 2$ relève d'un théorème bien connu dû à Billingsley — voir, par exemple, [25] équation (1.6).

Soit $\eta > 0$ tel que l'on ait $|\mathcal{C} \cap [1, x]| \geqslant \eta x$ pour x assez grand et soit $t > 0$ tel que $\big(1 - 1/m\big)^t < \eta/3$. Une application du Théorème 2.5 avec $\{h_1, \dots, h_r\} = \{h \leqslant 2t : q \nmid h\}$ et $\mathbf{a} := (a, \dots, a)$ fournit

$$S(x; \mathbf{h}; \mathbf{a}, m) = \{1 + o(1)\}x\big(1 - 1/m\big)^r < \tfrac{1}{2}\eta x$$

pour x assez grand. On en déduit qu'il existe au moins $\eta x/2$ entiers n de $\mathcal{C} \cap [1, x]$ tels que la congruence $s(hn) \equiv a \,(\mathrm{mod}\, m)$ soit vérifiée pour au moins un entier $h \in [1, 2t]$. Il y a donc au moins $\eta x/4t$ entiers n de $\mathcal{C}$ et n'excédant pas $2tx$ tels que $s_q(n) \equiv a \,(\mathrm{mod}\, m)$. Cela termine la preuve du Théorème 2.8 : la valeur $\delta = \eta/8t^2$ est admissible.

9.4. Preuve du Théorème 2.9.

Posons $L := c_3 \log(x/|\mathcal{A}|)$ et appliquons le Théorème 2.5 avec $\mathbf{a} := (a, \dots, a)$ et

$$\{h_1, \dots, h_r\} = \{1 \leqslant \ell \leqslant L : \ell \not\equiv 0 \,(\mathrm{mod}\, q)\}.$$

Nous avons donc $r = (1 - 1/q)h + O(1)$ et $h := \max_{1 \leqslant j \leqslant r} h_j \leqslant L$. Il est aisé de vérifier que le terme d'erreur de (2·16) n'excède pas l'unité en valeur absolue dès que $r \leqslant \varepsilon(\log x)^{1/3}/\log_2 x$ et x est assez grand, où $\varepsilon = \varepsilon(m, q) > 0$ est une constante convenable. L'existence de $c_1|\mathcal{A}|$ éléments de $\mathcal{A}$ tels que $s(nd) \equiv a \,(\mathrm{mod}\, m)$ pour au moins un entier $d \leqslant c_3 \log(x/|\mathcal{A}|)$ résulte alors de la possibilité de choisir r assez grand pour que

$$S(x; \mathbf{h}; \mathbf{a}, m) \leqslant 2x(1 - 1/m)^r \leqslant \tfrac{1}{2}(1 - c_1)|\mathcal{A}|.$$

Les contraintes imposées à r sont certainement satisfaites si

$$m \log\big(4x/\{(1 - c_1)|\mathcal{A}|\}\big) \leqslant r \leqslant \varepsilon(\log x)^{1/3}/\log_2 x.$$

L'intervalle correspondant est de longueur plus grande que 1 ; il contient donc au moins un entier r, dès que $|\mathcal{A}| \geqslant x \exp\big(-c_2(\log x)^{1/3}/\log_2 x\big)$ où $c_2 > 0$ est une constante assez petite.

10. Sommes des chiffres et progressions arithmétiques.

Ce paragraphe est consacré à la preuve du Théorème 2.11. Nous nous donnons des r-uplets $\mathbf{a}$, $\mathbf{m}$, $\mathbf{h}$ satisfaisant aux conditions de l'énoncé.

Posons, pour $1 \leqslant j \leqslant r$,

$$\chi_j(n) := \sum_{1\leqslant k<m_j} \mathrm{e}\Big(\frac{k\{s_q(h_jn)-a_j\}}{m_j}\Big) = \begin{cases} m_j-1 & \text{si } s_q(h_jn)\equiv a_j \pmod{m_j},\\ -1 & \text{dans le cas contraire.}\end{cases}$$

Nous avons alors

$$A(x;\mathbf{h},\mathbf{a},\mathbf{m};b,d) = \frac{1}{m_1\cdots m_r} \sum_{\substack{n\leqslant x\\ n\equiv b \pmod d}} \prod_{1\leqslant j\leqslant r} \{1+\chi_j(n)\}.$$

Le terme principal de l'approximation apparaissant dans (2·27) pour le membre de gauche provient, après développement du produit en j, de la contribution du terme unité. La preuve de (2·27) peut donc être ramenée à celle de la proposition suivante, que nous énonçons, en vue d'applications ultérieures, sous une forme plus générale que nécessaire.

Proposition 10.1. — *Soient x, A, $\mathbf{h}$ des paramètres vérifiant les conditions du Théorème 2.11 et $\boldsymbol{\alpha} \in \mathbb{R}^r \smallsetminus \{\mathbb{Z}/(q-1)\}^r$. On suppose de plus que, si $\boldsymbol{\alpha} \notin \mathbb{Q}^r$, on a*

$$\|\mathbf{h}\|_\infty \leqslant \frac{(\log x)^{1/(2r+1)}}{(\log_2 x)^{(2r+3)/(2r+1)}}.$$

On a alors la majoration

$$\sum_{\substack{d\leqslant D\\ (d,q)=1}} \max_{b \pmod d} \Big| \sum_{\substack{n\leqslant x\\ n\equiv b \pmod d}} \mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)\big)\Big| \ll_{A,q,\boldsymbol{\alpha}} \frac{x}{(\log x)^A} \tag{10·1}$$

où l'on a posé $D := \sqrt{x}/(\log x)^{A+2}$.

Démonstration. — Le nombre réel x étant donné, nous notons $b_d = b_d(x)$ le résidu réalisant le maximum du terme général de la somme (10·1). Soit $h := \max_{1\leqslant j\leqslant r} h_j$. Nous désignons par ϱ l'unique puissance de q vérifiant $2h < \varrho \leqslant 2hq$ et nous posons

$$J := \left[\frac{\log x}{5\log \varrho}\right].$$

Conservant la notation (2·1) pour la décomposition d'un entier générique en base ϱ, nous désignons par $\mathbb{F}$ l'ensemble des entiers n n'excédant pas x tels que

$$e_j(n) \neq 0 \qquad (J \leqslant j < 2J)$$

et, pour $J \leqslant \nu < 2J$, par $\mathbb{F}_\nu$ l'ensemble des entiers $n \leqslant x$ tels que

$$e_j(n) \neq 0 \quad (J \leqslant j < \nu), \qquad e_\nu(n) = 0.$$

On a ainsi $\mathbb{N} \cap [1, x] = \mathbb{F} \cup \big(\cup_{J<\nu\leqslant 2J} \mathbb{F}_\nu\big)$, de sorte que le membre de gauche de (10·1) ne dépasse pas

$$\sum_{\substack{d\leqslant x\\(d,q)=1}} \Big\{ S_d + \sum_{J<\nu\leqslant 2J} |S_{\nu,d}| \Big\}$$

avec

$$\begin{aligned} S_d &:= \sum_{\substack{n\in\mathbb{F}\\ n\equiv b_d \,(\mathrm{mod}\, d)}} 1, \\ S_{\nu,d} &:= \sum_{\substack{n\in\mathbb{F}_\nu\\ n\equiv b_d \,(\mathrm{mod}\, d)}} \mathrm{e}\Big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)\Big) \\ &= \frac{1}{d} \sum_{0\leqslant k<d} \mathrm{e}\Big(-\frac{b_d k}{d}\Big) \sum_{n\in\mathbb{F}_\nu} \mathrm{e}\Big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n) + \frac{kn}{d}\Big). \end{aligned} \tag{10·2}$$

Commençons par estimer S_d. À cette fin, nous observons qu'un entier n de $\mathbb{F}$ est représenté de manière unique sous la forme

$$n = n_1 + \varrho^J n_2 + \varrho^{2J} n_3$$

avec $n_1 < \varrho^J$, $n_2 < \varrho^J$, $e_j(n_2) \neq 0$ $(0 \leqslant j < J)$, $n_3 \geqslant 0$. Il s'ensuit que, pour chaque $d \leqslant D$, on a

$$\begin{aligned} S_d &\leqslant \sum_{n_1} \sum_{n_2} \sum_{\substack{n_3\leqslant x/\varrho^{2J}\\ n_3\varrho^{2J}\equiv b_d - n_1 - n_2\varrho^J \,(\mathrm{mod}\, d)}} 1 \\ &\ll \varrho^J(\varrho-1)^J \frac{x}{d\varrho^{2J}} \ll \frac{x}{d}(1-1/\varrho)^J. \end{aligned}$$

Compte tenu du choix de ϱ et de la contrainte de taille sur h, nous obtenons donc

$$\sum_{\substack{d\leqslant D\\(d,q)=1}} S_d \ll x\Big(1-\frac{1}{2qh}\Big)^J \log x \ll x\mathrm{e}^{-(\log_2 x)^2/11}. \tag{10·3}$$

Considérons à présent la somme $S_{\nu,d}$. Chaque entier de $\mathbb{F}_\nu$ est décomposable de manière unique sous la forme

$$n = n_1 + n_2\varrho^J + n_3\varrho^{\nu+1}$$

avec

$$n_1 \leqslant \varrho^J, \quad n_2 < \varrho^{\nu-J}, \quad e_j(n_2)\neq 0 \ (0\leqslant j\leqslant \nu-J), \quad n_3\geqslant 0. \tag{10·4}$$

Posant $m := n_1 + n_2\varrho^J < \varrho^\nu$, nous avons donc

$$s_q(h_j n) = s_q(h_j m) + s_q(h_j n_3) \qquad (1\leqslant j\leqslant r),$$

d'où

$$\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n) = \boldsymbol{\alpha}\cdot s_q(\mathbf{h}m) + \boldsymbol{\alpha}\cdot s_q(\mathbf{h}n_3).$$

Reportons dans l'expression (10·2) de $S_{\nu,d}$ en notant $\mathcal{M}$ l'ensemble des entiers $<\varrho^\nu$ qui sont de la forme $n_1+n_2\varrho^J$ où n_1 et n_2 satisfont (10·4). Nous obtenons

$$S_{\nu,d} = \frac{1}{d}\sum_{0\leqslant k<d} \mathrm{e}\Big(-\frac{kb_d}{d}\Big)\sum_{m\in\mathcal{M}} \mathrm{e}\Big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}m)+m\frac{k}{d}\Big)G_r\Big(\frac{x-m}{\varrho^{\nu+1}};\frac{k}{d}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big).$$

L'erreur globale commise en remplaçant $x-m$ par x dans le premier argument de G_r est au plus ϱ^ν. En posant

$$\Gamma_\nu\Big(\frac{k}{d}\Big) := \sum_{m\in\mathcal{M}} \mathrm{e}\Big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}m)+m\frac{k}{d}\Big),$$

nous pouvons donc écrire

$$\begin{aligned}
|S_{\nu,d}| &\leqslant \frac{1}{d}\sum_{0\leqslant k<d}\Big|\Gamma_\nu\Big(\frac{k}{d}\Big)G_r\Big(\frac{x}{\varrho^{\nu+1}};\frac{k}{d}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big)\Big| + \varrho^\nu\\
&\leqslant \frac{\varrho^\nu}{d}\Big|G_r\Big(\frac{x}{\varrho^{\nu+1}};0;\boldsymbol{\alpha},\mathbf{h}\Big)\Big|\\
&\quad + \frac{1}{d}\sum_{t\mid d}\sum_{\substack{1\leqslant s<t\\(s,t)=1}}\Big|\Gamma_\nu\Big(\frac{s}{t}\Big)G_r\Big(\frac{x}{\varrho^{\nu+1}};\frac{s}{t}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big)\Big| + \varrho^\nu,
\end{aligned}$$

d'où

$$\sum_{\substack{d\leqslant D\\(d,q)=1}}|S_{\nu,d}|\ll \varrho^{\nu}\Big\{D+(\log x)\Big|G_r\Big(\frac{x}{\varrho^{\nu+1}};0;\boldsymbol{\alpha},\mathbf{h}\Big)\Big|\Big\}$$
$$+(\log x)\sum_{1\leqslant t\leqslant D}\frac{1}{t}\sum_{\substack{1\leqslant s<t\\(s,t)=1}}\Big|\Gamma_\nu\Big(\frac{s}{t}\Big)G_r\Big(\frac{x}{\varrho^{\nu+1}};\frac{s}{t}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big)\Big|.$$

D'après le Corollaire 2.2, nous avons, uniformément en $\vartheta\in\mathbb{R}$,

$$G_r\Big(\frac{x}{\varrho^{\nu+1}};\vartheta;\boldsymbol{\alpha},\mathbf{h}\Big)\ll\frac{x}{\varrho^{\nu}}\mathrm{e}^{-c(\log_2 x)^2}$$

où $c=c(\boldsymbol{\alpha},q,r)>0$. Nous appliquons cette estimation lorsque $\vartheta=0$ ou $s\varrho^{\nu+1}/t$ avec $t\leqslant T$ où $T=T_x>1$ est un paramètre qui sera précisé ultérieurement. Nous obtenons

$$\sum_{\substack{d\leqslant D\\(d,q)=1}}|S_{\nu,d}|\ll\frac{xT\log x}{\mathrm{e}^{c(\log_2 x)^2}}+(\log x)W \tag{10·5}$$

avec

$$W:=\sum_{T<t\leqslant D}\frac{1}{t}\sum_{\substack{1\leqslant s<t\\(s,t)=1}}\Big|\Gamma_\nu\Big(\frac{s}{t}\Big)G_r\Big(\frac{x}{\varrho^{\nu+1}};\frac{s}{t}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big)\Big|.$$

Nous majorons W grâce au grand crible sous forme analytique — voir, par exemple, [24], formule (30) . . . . 70. Pour $T<T_1\leqslant T_2\leqslant 2T_1$, nous avons

$$\sum_{T_1<t\leqslant T_2}\frac{1}{t}\sum_{\substack{1\leqslant s<t\\(s,t)=1}}\Big|\Gamma_\nu\Big(\frac{s}{t}\Big)G_r\Big(\frac{x}{\varrho^{\nu+1}};\frac{s}{t}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big)\Big|$$
$$\leqslant\frac{1}{T_1}\Bigg\{\sum_{\substack{T_1<t\leqslant T_2\\1\leqslant s<t\\(s,t)=1}}\Big|\Gamma_\nu\Big(\frac{s}{t}\Big)\Big|^2\sum_{\substack{T_1<t\leqslant T_2\\1\leqslant s<t\\(s,t)=1}}\Big|G_r\Big(\frac{x}{\varrho^{\nu+1}};\frac{s}{t}\varrho^{\nu+1};\boldsymbol{\alpha},\mathbf{h}\Big)\Big|^2\Bigg\}^{1/2}$$
$$\leqslant\frac{1}{T_1}\Big\{\big(\varrho^{\nu}+T_2^2\big)\varrho^{\nu}\frac{x}{\varrho^{\nu}}\Big(\frac{x}{\varrho^{\nu}}+T_2^2\Big)\Big\}^{1/2}\ll\frac{x}{T_1}+T_1\sqrt{x}+\frac{x}{\varrho^{\nu/2}}.$$

Choisissons $T_1=2^vT$, $T_2:=\min(2T_1,D)$ et sommons cette estimation sur tous les entiers v tels que $T_1\leqslant D$. Il s'ensuit que

$$W\ll\frac{x}{T}+D\sqrt{x}+\frac{x\log x}{\varrho^{J/2}}.$$

Reportons dans (10·5), choisissons $T:=(\log x)^{A+2}$ et sommons en ν. Nous obtenons bien le résultat requis. □

11. Sommes des chiffres et fonctions multiplicatives.

Nous nous proposons ici d'établir le Théorème 2.12. Ce résultat peut être considéré comme un analogue du théorème de Daboussi [5] selon lequel le spectre de Fourier–Bohr d'une fonction multiplicative complexe f de module au plus 1 est rationnel, autrement dit

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x} f(n)\mathrm{e}(-\vartheta n)=0 \qquad (\vartheta\in\mathbb{R}\smallsetminus\mathbb{Q}).$$

Notre approche s'inspire en fait de la preuve du théorème de Daboussi donnée dans [26] (exercice III.4.3, . 180). Elle contient également certains raffinements issus de travaux du second auteur, comme par exemple [23].

Pour simplifier l'écriture, nous posons dans toute la suite $R:=R^*(\boldsymbol{\alpha})$.

Nous commençons par établir que l'on peut, sans perte de généralité, supposer que $f(p^\nu)=0$ si $p|q$. Cette réduction purement technique permettra une simplification significative des calculs.

Supposons donc que l'estimation (2·31) est valable dans les conditions de l'énoncé mais sous l'hypothèse supplémentaire que le support de f est inclus dans l'ensemble des entiers premiers à q. En employant la notation $d\mid q^\infty$ pour signifier que chaque facteur premier de d divise q, nous pouvons alors écrire, lorsque f est une fonction multiplicative arbitraire de module au plus un,

$$\sum_{n\leqslant x} f(n)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)\big)=\sum_{d\mid q^\infty} f(d)\sum_{\substack{n\leqslant x/d\\(n,d)=1}} f(n)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}nd)\big). \tag{11·1}$$

Pour chaque entier d, nous avons

$$\boldsymbol{\alpha}\cdot s_q(\mathbf{h}nd)=\boldsymbol{\alpha}\cdot s_q(d\mathbf{h}n)=\boldsymbol{\alpha}\cdot s_q(\mathbf{h}_d n)$$

où $\mathbf{h}_d$ désigne le r-uplet dont la j-ième composante est le plus petit entier de la forme $h_j d/q^\nu$ avec $\nu\geqslant 0$. Cela implique que, quitte à y réordonner les indices de $\mathbf{h}_d$, la somme intérieure de (11·1) relève de la forme restreinte de notre énoncé tant que, disons, $d\leqslant(\log x)^{(1-c)/2R}$. Comme

$$\sum_{d\mid q^\infty}\frac{1}{d^\sigma}=\prod_{p\mid q}\frac{1}{1-p^{-\sigma}}\ll_{q,\sigma} 1$$

pour tout $\sigma>0$, cela implique pleinement le résultat souhaité.

Introduisons, pour chaque valeur du paramètre $y \geqslant 2$, les fonctions complètement multiplicatives u_y et v_y définies sur l'ensemble des nombres premiers par

$$u_y(p) := \begin{cases} 1 & \text{si } p > y, \\ 0 & \text{sinon,} \end{cases} \qquad v_y(p) := 1 - u_y(p).$$

Ainsi, v_y est la fonction indicatrice des entiers y-friables, alors que u_y détecte les entiers non éliminés par le crible d'Ératosthène de paramètre y.

La première étape de la démonstration consiste à établir que, pour tout $A > 0$ fixé et uniformément sous les conditions (2·30) et $1 \leqslant y \leqslant \sqrt{\log x}$, on a

$$\sum_{\substack{n \leqslant x \\ (n,q)=1}} u_y(n) \mathrm{e}\big(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n)\big) \ll_A \frac{x}{(\log x)^A}. \tag{11·2}$$

À cette fin, nous employons l'identité de convolution $u_y = \mathbf{1} * v_y\mu$, où μ désigne la fonction de Möbius. Nous pouvons donc écrire

$$\begin{aligned} \Big| \sum_{\substack{n \leqslant x \\ (n,q)=1}} u_y(n) \mathrm{e}(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n)) \Big| &= \Big| \sum_{\substack{md \leqslant x \\ (md,q)=1}} v_y(d)\mu(d) \mathrm{e}(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}md)) \Big| \\ &\leqslant \sum_{\substack{d \leqslant x^{1/3} \\ (d,q)=1}} \Big| \sum_{\substack{n \leqslant x \\ n \equiv 0 \,(\mathrm{mod}\, d) \\ (n,q)=1}} \mathrm{e}(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n)) \Big| + \sum_{d > x^{1/3}} \mu^2(d) v_y(d) \frac{x}{d}. \end{aligned} \tag{11·3}$$

Dans cette majoration, la somme intérieure en n peut être réécrite sous la forme

$$\sum_{\substack{n \leqslant x \\ n \equiv 0 \,(\mathrm{mod}\, d)}} \mathrm{e}(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}n)) \sum_{t \mid (q,n)} \mu(t) = \sum_{t \mid q} \mu(t) \sum_{\substack{n \leqslant x/t \\ n \equiv 0 \,(\mathrm{mod}\, d)}} \mathrm{e}(\boldsymbol{\alpha} \cdot s_q(\mathbf{h}nt)).$$

D'après la Proposition 10.1, le premier terme du membre de droite de (11·3) est donc $\ll x/(\log x)^A$, la constante implicite ne dépendant que de A, $\boldsymbol{\alpha}$, c et q. Or, lorsque x est assez grand, le second terme du membre de droite est nul puisque $\prod_{p \leqslant y} p < x^{1/3}$, en vertu du théorème des nombres premiers.

Dans un second temps, nous établissons (2·31) lorsque f est une fonction multiplicative de module inférieur à 1 telle que $f(p^\nu) = 0$ si $\nu \geqslant 2$ ou $p \mid q$.

Posons $K_x := (\log x)^{(1-c)/3R}$, $J_x := [\log K_x]$. Chaque entier sans facteur carré $n > K_x$ possède un facteur premier p_n maximal sous la contrainte

$$a_n := \prod_{\substack{p\|n\\ p<p_n}} p \leqslant K_x.$$

Décomposons alors canoniquement n sous la forme $n = a_n b_n$. Nous avons en particulier

$$a_n \leqslant K_x < a_n p_n.$$

Notons $P^+(n)$ le plus grand facteur premier d'un entier générique n avec la convention $P^+(1) = 1$. En scindant la somme

$$S(x) := \sum_{n\leqslant x} f(n)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)\big)$$

selon les valeurs de a_n, nous pouvons écrire

$$S(x) = \sum_{0\leqslant j\leqslant J_x} S_j + O(K_x) \tag{11·4}$$

avec

$$S_j := \sum_{ab\leqslant x}^{*} f(a)f(b)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}ab)\big)$$

où l'astérisque indique que les variables entières a et b sont soumises aux conditions de sommation

$$(*) \qquad P^+(a) < P^-(b), \quad K_x/\mathrm{e}^{j+1} < a \leqslant K_x/\mathrm{e}^j, \quad aP^-(b) > K_x.$$

Nous majorons S_j par l'inégalité de Cauchy-Schwarz. Nous avons, avec la notation (3·1)

$$|S_j|^2 \leqslant \Phi\Big(\frac{x\mathrm{e}^{j+1}}{K_x}, \mathrm{e}^j\Big) \sum_{\substack{b\leqslant x,\,(b,q)=1\\ P^-(b)>\mathrm{e}^j}} \big|Z_b\big|^2, \tag{11·5}$$

o ? l'on a pos ?

$$Z_b := \sum_{\substack{a\leqslant x/b,\,P^+(a)<P^-(b)\\ K_x/\min\left(\mathrm{e}^{j+1},P^-(b)\right)<a\leqslant K_x/\mathrm{e}^j}} f(a)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}ab)\big).$$

D'après une estimation standard de crible, nous avons

$$\Phi\Big(\frac{x\mathrm{e}^{j+1}}{K_x}, \mathrm{e}^j\Big) \ll x\frac{\mathrm{e}^{-J_x+j}}{j+1}\cdot$$

Développons le carré du module de la somme en a et désignons respectivement par U_j et V_j les contributions à la seconde somme en b de la diagonale et des termes rectangles. Nous avons

$$\begin{aligned}
U_j &\leqslant \sum_{\substack{b\leqslant x\\ P^-(b)>\mathrm{e}^j}} \sum_{\substack{a\leqslant x/b,\, P^+(a)<P^-(b)\\ K_x/\mathrm{e}^{j+1}<a\leqslant K_x/\mathrm{e}^j}} 1\\
&\ll \sum_{K_x/\mathrm{e}^{j+1}<a\leqslant K_x/\mathrm{e}^j} \sum_{\substack{b\leqslant x/a\\ P^-(b)>\max\big(P^+(a),\mathrm{e}^j\big)}} 1\\
&\ll \sum_{K_x/\mathrm{e}^{j+1}<a\leqslant K_x/\mathrm{e}^j} \frac{x}{a\{j+\log P^+(a)\}}\\
&\ll \sum_{p\leqslant K_x/\mathrm{e}^j} \frac{x}{p\{j+\log p\}} \sum_{\substack{K_x/p\mathrm{e}^{j+1}<a\leqslant K_x/p\mathrm{e}^j\\ P^+(a)\leqslant p}} \frac{1}{a}\cdot
\end{aligned}$$

La dernière somme intérieure peut être aisément évaluée grâce à la majoration

$$\Psi(x,y) := \sum_{n\leqslant x} v_y(n) \ll x\mathrm{e}^{-(\log x)/(2\log y)} \quad (x\geqslant 2, y\geqslant 2),$$

établie au chap. III.5 de [24]. Nous obtenons

$$U_j \ll \sum_{p\leqslant K_x/\mathrm{e}^j} \frac{x\mathrm{e}^{-(J_x-j)/(2\log p)}}{p\{j+\log p\}}\cdot$$

On a clairement

$$U_j \ll x/J_x \tag{11·6}$$

lorsque $j = J_x$. Lorsque $j < J_x \leqslant 2j$, nous avons

$$U_j \ll \sum_{p\leqslant \exp(J_x-j)} \frac{x\mathrm{e}^{-(J_x-j)/(2\log p)}}{pJ_x} \ll \frac{x}{J_x} \sum_{p\leqslant \exp(J_x-j)} \frac{\log p}{(J_x-j)p} \ll \frac{x}{J_x}\cdot$$

Si $J_x > 2j$, nous obtenons similairement $U_j \ll U_j^{(1)} + U_j^{(2)}$ avec

$$U_j^{(1)} \ll \frac{x}{j} \sum_{p \leqslant \mathrm{e}^j} \frac{\mathrm{e}^{-(J_x-j)/(2\log p)}}{p} \ll \frac{x}{j} \sum_{p \leqslant \mathrm{e}^j} \frac{\log p}{(J_x-j)p} \ll \frac{x}{J_x-j} \ll \frac{x}{J_x}$$

et

$$\begin{aligned} U_j^{(2)} &\ll \sum_{\mathrm{e}^j < p \leqslant \exp(J_x-j)} \frac{x\mathrm{e}^{-(J_x-j)/(2\log p)}}{p\log p} \\ &\ll \sum_{\mathrm{e}^j < p \leqslant \exp(J_x-j)} \frac{x(\log p)^2}{(J_x-j)^2 p\log p} \ll \frac{x}{J_x}. \end{aligned}$$

Nous avons donc établi que (11·6) est valable pour tout $j \leqslant J_x$.

Par ailleurs,

$$V_j \ll \sum_{K_x/\mathrm{e}^{j+1} < a,\, a' \leqslant K_x/\mathrm{e}^j} f(a)\overline{f(a')} \sum_{\substack{b \leqslant x/\max(a,a') \\ P^-(b) > y}} \mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}ab) - \boldsymbol{\alpha}\cdot s_q(\mathbf{h}a'b)\big)$$

avec $y := \max\{\mathrm{e}^j, P^+(aa'), K_x/\min(a,a')\}$. La somme intérieure de cette majoration relève donc d'une application de la majoration (11·2) à un vecteur $\mathbf{h}_1$ de dimension n'excédant pas $2r$ et dont la plus grande coordonnée ne dépasse pas

$$(\log x)^{c/R} K_x = (\log x)^{(1+2c)/3R}.$$

Il s'ensuit que

$$V_j \ll_A \frac{x}{(\log x)^A} \ll \frac{x}{J_x}.$$

En reportant dans (11·5), nous obtenons

$$S_j \ll \frac{x\mathrm{e}^{-(J_x-j)/2}}{\sqrt{(j+1)J_x}}.$$

Il résulte alors de (11·4) que

$$S(x) \ll \sum_{0 \leqslant j \leqslant J_x} \frac{x\mathrm{e}^{-(J_x-j)/2}}{\sqrt{(j+1)J_x}} + K_x \ll \frac{x}{J_x} \asymp \frac{x}{\log_2 x}. \tag{11·7}$$

Pour achever la démonstration, il nous reste à montrer que cette dernière estimation persiste lorsque l'on s'affranchit de l'hypothèse que le support de f est inclus dans l'ensemble des entiers sans facteur carré.

À cette fin, nous introduisons la fonction $g = \mu^2 f$, pour laquelle l'estimation (11·7) est valide. Ainsi qu'il a été établi dans [26],[(8)] la fonction multiplicative h définie par $f = g * h$ vérifie $h(p) = 0$, $|h(p^\nu)| \leqslant \nu + 1$ et donc

$$\sum_{m\geqslant 1} \frac{|h(m)|}{m} < \infty. \tag{11·8}$$

En observant que tout entier m tel que $h(m) \neq 0$ peut être décomposé de manière unique sous la forme $m = j^2k$ avec $k \mid j$, $\mu(k)^2 = 1$, nous pouvons même estimer la rapidité de convergence de cette série. Notant $n \mapsto \tau(n)$ la fonction nombre de diviseurs, nous avons, pour tout $M \geqslant 1$,

$$\sum_{m>M} \frac{|h(m)|}{m} \leqslant \sum_{\substack{j^2k>M\\ k\mid j}} \frac{\tau(j^2)\tau(k)}{j^2k} \leqslant \sum_{j^3>M} \frac{\tau(j^2)}{\varphi(j)^2} \ll \frac{(\log M)^2}{M^{1/3}}. \tag{11·9}$$

Nous pouvons alors écrire

$$\sum_{n\leqslant x} f(n)\mathrm{e}(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}n)) = \sum_{mn\leqslant x} h(m)g(n)\mathrm{e}(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}mn)) = T_1 + T_2 \tag{11·10}$$

avec

$$T_1 := \sum_{m\leqslant K_x} h(m) \sum_{n\leqslant x/m} g(n)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}mn)\big),$$
$$T_2 := \sum_{m>K_x} h(m) \sum_{n\leqslant x/m} g(n)\mathrm{e}\big(\boldsymbol{\alpha}\cdot s_q(\mathbf{h}mn)\big).$$

D'après (11·7) et (11·8), nous avons

$$T_1 \ll \sum_{m\leqslant K_x} \frac{|h(m)|x}{m\log_2 x} \ll \frac{x}{\log_2 x},$$

alors qu'il découle immédiatement de (11·9) que

$$T_2 \ll x \sum_{m>K_x} \frac{|h(m)|}{m} \ll \frac{x(\log_2 x)^2}{(\log x)^{(1-c)/9R}}.$$

Cela complète bien la démonstration.

(8) Voir l'exercice corrigé III.4.3, question (b).

BIBLIOGRAPHIE

[1] M. Balazard, Unimodalité de la distribution du nombre de diviseurs premiers d'un entier, Ann. Inst. Fourier, Grenoble, 40 n° 2 (1990), 255—270.

[2] A. Balog & I. Ruzsa, On an additive property of stable sets, in G. R. H. Greaves, G. Harman & M. N. Huxley : Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), 55—63, London Math. Soc. Lecture Note Ser., 237 (1997).

[3] E. Bombieri, The asymptotic sieve, Rend. Accad. Naz., XL (5) 1/2 (1975/76), 243—269 (1977).

[4] J. Coquet, Sur la représentation des multiples d'un entier dans une base, Publications mathématiques d'Orsay, 83.04.

[5] H. Daboussi, On a convolution method, in : E. Aparicio, C. Calderón, J. C. Peral (eds.), Congreso de Teoría de los Números (Universitad del País Vasco) (1989), 110–137.

[6] C. Dartyge & G. Tenenbaum, Congruences de sommes de chiffres de valeurs polynomiales, Bull. London Math. Soc. (à paraître).

[7] É. Fouvry & C. Mauduit, Sommes des chiffres et nombres presque premiers, Math. Ann., 305 (1996), 571–599.

[8] É. Fouvry & C. Mauduit, Méthodes de crible et fonctions sommes des chiffres, Acta Arith., 77 n° 4 (1996), 339–351.

[9] A.O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, Acta arith., 13 (1968), 259–265.

[10] R.R. Hall, Sets of multiples, Cambridge University Press, Cambridge, 1996.

[11] K.–H. Indlekofer & I. Katai, Investigations in the theory of q–additive and q–multiplicative functions, I, Acta Math. Hungar., 91 (1–2) (2001), 53–78.

[12] K.–H. Indlekofer & I. Katai, Investigations in the theory of q–additive and q–multiplicative functions, II, Acta Math. Hungar., 97 (1–2) (2002), 97–108.

[13] H. Iwaniec, Rosser's sieve, Acta arith., 36 (1980), 171—202.

[14] C. Mauduit & A. Sárközy, On finite pseudorandom binary sequences, II. The Champernowne, Rudin–Shapiro, and Thue–Morse sequences : a further construction, Journal number theory, 72 (1998), 1–21.

[15] D.J. Newman, On the number of binary digits in a multiple of three,, Proc. Amer. Math. Soc., 21 (1969), 719–721.

[16] D.J. Newman & M. Slater, Binary digit distribution over naturally defined sequences, Trans. Amer. Math. Soc., 213 (1975), 71–78.

[17] J. Schmid, The joint distribution of the binary digits of integer multiples, Acta arith., 63 (1984), 391–415.

[18] W.M. Schmidt, The joint distribution of the digits of certain integer s–tuples, in : Studies in Pure Mathematics in Memory of P. Turán, Birkhäuser (1983), 605–622.

[19] A. Selberg, On elementary methods in prime–number theory and their limitations, in : Proc. 11th Scand. Math Cong. Trondheim (1949), 13–22.

[20] J.A. Solinas, A theorem of metric diophantine approximation and estimates for sums involving binary digits, Thèse, University of Michigan, août 1985.

[21] J.A. Solinas, On the joint distribution of digital sums,, Journal number theory, 33 (1989), 132—151.

[22] K. Stolarsky, Integers whose multiples have anomalous digital frequencies, Acta arith., 38 (1980), 117–128.

[23] G. Tenenbaum, Sur une question d'Erdős et Schinzel, in : A. Baker, B. Bollobás, A. Hajnal (eds.) *A Tribute to Paul Erdős* (1990), 405—443.

[24] G. Tenenbaum, Introduction à la théorie analytique et probabiliste des nombres, 2ème édition, Cours spécialisés, n° 1, Société mathématique de France, 1995.

[25] G. Tenenbaum, A rate estimate in Billingsley's theorem for the size distribution of large prime factors, Quart. J. Math., 51 (2000), 385–403.

[26] G. Tenenbaum, en collaboration avec J. Wu, Exercices corrigés de théorie analytique et probabiliste des nombres, Cours spécialisés, n° 2, Société mathématique de France, 1996.

Manuscrit reçu le 17 juin 2004,
accepté le 2 mai 2005.

Cécile DARTYGE
Gérald TENENBAUM
Université Henri Poincaré Nancy 1
Institut Élie Cartan
BP 239
54506 Vandœuvre cedex (France).
dartyge@iecn.u–nancy.fr
gerald.tenenbaum@ciril.fr