

Congruences de sommes de chiffres de valeurs polynomiales

Cécile Dartyge et Gérald Tenenbaum

Abstract. Let $m, g, q \in \mathbb{N}$ with $q \geq 2$ and $(m, q-1) = 1$. For $n \in \mathbb{N}$, denote by $s_q(n)$ the sum of digits of n in the q -ary digital expansion. Given a polynomial f with integer coefficients, degree $d \geq 1$, and such that $f(\mathbb{N}) \subset \mathbb{N}$, it is shown that there exists $C = C(f, m, q) > 0$ such that for any $g \in \mathbb{Z}$, and all large N ,

$$|\{0 \leq n \leq N : s_q(f(n)) \equiv g \pmod{m}\}| \geq CN^{\min(1, 2/d)}.$$

In the special case $m = q = 2$ and $f(n) = n^2$, the value $C = 1/20$ is admissible.

Classification AMS : principale 11B85, secondaires 11N37, 11N69.

1. Introduction

Soit q un entier supérieur ou égal à 2. Pour $n \in \mathbb{N}$, on note $s_q(n)$ la somme des chiffres de n en base q . En 1968, Gelfond [3] a montré que si $f(X) = aX + b$ est un polynôme de degré 1 à coefficients positifs ou nuls, la suite $\{s_q(f(n))\}_{n=0}^{\infty}$ est bien répartie dans les progressions arithmétiques de raison fixée m dès que $(m, q-1) = 1$.⁽¹⁾

À la fin de son article, Gelfond pose le problème de l'extension de son résultat aux polynômes de degré quelconque et, à défaut, d'estimer asymptotiquement, pour tous entiers m et q satisfaisant $(m, q-1) = 1$, la quantité

$$(1.1) \quad A(N; f; g, m) := |\{0 \leq n \leq N : s_q(f(n)) \equiv g \pmod{m}\}|$$

lorsque $f \in \mathbb{Z}[X]$ est un polynôme de degré au moins égal à 2.

Cette question s'insère naturellement dans une problématique générale de la théorie des nombres. Il s'agit de décrire les interactions, ou l'indépendance, des diverses structures dont une suite d'entiers peut être munie. En l'occurrence, le problème de Gelfond consiste à vérifier l'heuristique selon laquelle une suite définie par composition d'une fonction de nature algébrique (un polynôme) et d'une fonction de nature algorithmique (la somme des chiffres) se comporte de manière stochastique — le critère retenu ici étant la bonne répartition dans les progressions arithmétiques.

À notre connaissance, la seule avancée sur ce problème obtenue dans la littérature concerne un analogue de type Piatetski-Shapiro, où la fonction polynomiale f est

1. On peut ramener le cas général à celui étudié par Gelfond : si $d := (m, q-1)$, $m_1 := m/d$, on a identiquement $s_q(f(n)) \equiv f(n) \pmod{d}$. Pour tout résidu g modulo m représenté par f modulo d , il s'ensuit donc que

$$\{n \in \mathbb{N} : s_q(f(n)) \equiv g \pmod{m}\} = \bigcup_{\substack{0 \leq w < d \\ f(w) \equiv g \pmod{d}}} \{w + td : t \geq 0, s_q(f(w + td)) \equiv g \pmod{m_1}\}.$$

remplacée, dans (1.1), par $n \mapsto [n^c]$ avec $1 < c < 2$. À l'instar du problème de la répartition des nombres premiers dans les suites arithmétiques, on peut en effet considérer que ce cadre permet une interpolation graduée de la difficulté entre le cas des polynômes de degré 1 et celui des polynômes quadratiques. En 1995, Mauduit et Rivat [4] ont ainsi établi que la suite $\{s_q([n^c])\}_{n=0}^{\infty}$ est équirépartie dans les progressions arithmétiques si $c \in [1, 4/3[$.

L'objet du présent travail consiste à fournir des minoration de $A(N; f; g, m)$ lorsque f est un polynôme de degré supérieur à 2. Nous commençons par le cas emblématique $q = m = 2$, $f(X) = X^2$.

Théorème 1.1. *La densité inférieure de la suite des entiers n tels que $s_2(n^2)$ est pair (resp. impair) est au moins égale à $\frac{5}{8} - \frac{13}{32}\sqrt{2} \approx 0,05047 > \frac{1}{20}$.*

Courte et élémentaire, la preuve de ce résultat repose principalement sur la 2-additivité de la fonction s_2 et sur la formule bien connue

$$(1.2) \quad \sum_{0 \leq n \leq N} (-1)^{s_2(n)} = \frac{1}{2}(-1)^{s_2(N)} \{1 + (-1)^N\} \quad (N \in \mathbb{N}).$$

Comme les idées essentielles de notre méthode y apparaissent sous une forme affranchie des difficultés techniques inhérentes au cas général, nous avons choisi de présenter à part, au paragraphe 2, la démonstration du Théorème 1.1.

Notre résultat principal s'énonce comme suit.

Théorème 1.2. *Soient g , m et q des entiers tels que $q \geq 2$ et $(m, q-1) = 1$. Soit f un polynôme à coefficients entiers, de degré $d \geq 1$ et tel que $f(\mathbb{N}) \subset \mathbb{N}$. Il existe deux constantes $C = C(f, q, m) > 0$ et $N_0 = N_0(f, q, m) \geq 1$ telles que*

$$(1.3) \quad A(N; f; g, m) \geq CN^{\min(1, 2/d!)} \quad (N \geq N_0).$$

Remarques. (i) Le cas $d = 1$ n'a été inclus dans cet énoncé que par souci de complétude : le théorème de Gelfond dans [3] fournit alors une estimation plus précise.

(ii) Lorsque $d = 2$, il découle de (1.3) que

$$\liminf_{N \rightarrow \infty} A(N; f; g, m)/N > 0.$$

L'extension d'une telle propriété au cas $d \geq 3$ semble hors de portée de notre méthode.

Pour exhiber des entiers n tels que $s_q(f(n)) \equiv g \pmod{m}$, nous construisons des m -uplets (n_1, \dots, n_m) tels que

$$s_q(f(n_j)) \equiv s_q(f(n_1)) + j - 1 \pmod{m} \quad (2 \leq j \leq m).$$

Nous employons à cette fin un argument récursif de descente reposant sur une représentation des différences $s_q(f(n_j)) - s_q(f(n_1))$ en fonction de valeurs $s_q(f^*(n_1))$

où f^* décrit un ensemble de polynômes de degré au plus $d - 1$. Il est donc indispensable, pour la mise en place du raisonnement, de considérer, et de contrôler, simultanément toutes les congruences relatives à un module donné. Nous sommes ainsi conduits à établir, au Théorème 3.1 *infra*, une propriété plus générale et passablement technique, énoncée sous forme matricielle, dont le Théorème 1.2 est un cas particulier.

L'étape la plus délicate de la preuve du Théorème 3.1 concerne le degré 2, qui repose lui-même sur une version effective du cas des polynômes linéaires. Il s'agit alors d'estimer, uniformément dans les divers paramètres, des sommes du type :

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

où $\mathbf{h} := (h_1, \dots, h_r) \in \mathbb{N}^{*r}$, $\mathbf{k} \in \mathbb{N}^r$, $\boldsymbol{\alpha} \in \mathbb{Q}^r$, $\vartheta \in \mathbb{R}$, et

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

Étendant des travaux de Gelfond relatifs à la dimension $r = 1$, nous avons obtenu dans [2] des estimations en dimension quelconque. Nous extrayons de ce travail l'énoncé nécessaire à la mise en œuvre de notre méthode, qui est un cas particulier du théorème 2.1 de [2].

Théorème A ([2]). Soient $r \in \mathbb{N}^*$, $\boldsymbol{\alpha} \in \mathbb{Q}^r \setminus \{\mathbb{Z}/(q-1)\}^r$, m le plus petit dénominateur commun aux α_j ($1 \leq j \leq r$) 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 $h := \|\mathbf{h}\|_\infty = \max_{1 \leq j \leq r} |h_j|$. Il existe des constantes δ et K , ne dépendant que de q et r , telles que, notant ϱ l'unique puissance de q vérifiant $2Kh < \varrho \leq 2Kqh$, on ait, pour $x \geq 0$, $\vartheta \in \mathbb{R}$, et tout vecteur \mathbf{k} de \mathbb{N}^r de la forme $\mathbf{k} = \mathbf{k}' + \varrho^{E+D}\mathbf{k}''$ avec $D, E \in \mathbb{N}$, $\mathbf{k}', \mathbf{k}'' \in \mathbb{N}^r$, $\|\mathbf{k}'\|_\infty < \varrho^E$, $y > 2\varrho^{D+E}$,

$$(1.4) \quad |G_r(x, y; \vartheta; \boldsymbol{\alpha}, \mathbf{h}, \mathbf{k})| \leq y(8 + 3D/h)e^{-\delta D/4m^2 h} + 4\varrho^{E+D}.$$

En particulier, si $\|\mathbf{k}\|_\infty \leq \sqrt{y}$, on a

$$(1.5) \quad G_r(x, y; \vartheta; \boldsymbol{\alpha}, \mathbf{h}, \mathbf{k}) \ll m^2 \delta^{-1} y^{1-c_0/\{m^2 h \log(Kh)\}},$$

où la constante implicite est absolue.

Des majorations de ce type ont déjà été obtenues par Coquet [1] et Solinas [5]. Le lecteur trouvera dans [2] d'autres références et commentaires sur ce problème. L'application développée dans le présent travail nécessite de manière cruciale l'uniformité en x de la majoration (1.4), autrement dit l'aspect « petits intervalles » du théorème A.

2. Parité de la somme des chiffres des carrés

Le nombre des entiers $n \in [0, N]$ tels que $s_2(n^2)$ est pair vaut

$$\frac{1}{2} \sum_{0 \leq n \leq N} \{1 + (-1)^{s_2(n^2)}\}.$$

Le Théorème 1.1 est donc une conséquence du résultat suivant.

Théorème 2.1. *On a*

$$\left| \sum_{0 \leq n \leq N} (-1)^{s_2(n^2)} \right| \leq \left(\frac{13}{16} \sqrt{2} - \frac{1}{4} \right) N + \frac{9}{2} \quad (N \geq 0).$$

Démonstration. On peut supposer $N \geq 3$ puisque l'inégalité est trivialement vérifiée pour $0 \leq N \leq 2$. Soit R l'unique entier tel que $2^{R+1/2} < N \leq 2^{R+3/2}$. On a $R \geq 1$.

Posons $c = \sqrt{2} - 1$. Pour tout entier n de $I := [0, c2^R]$, on peut écrire

$$(2.1) \quad n^2 = \ell 2^{R+1} + b$$

avec

$$(2.2) \quad 0 \leq \ell \leq c^2 2^{R-1} = \left(\frac{3}{2} - \sqrt{2} \right) 2^R, \quad 0 \leq b < 2^{R+1}.$$

Il résulte immédiatement de (2.1) que

$$(2.3) \quad s_2(n^2) = s_2(b) + s_2(\ell).$$

De plus,

$$(n + 2^R)^2 = n^2 + 2^{R+1}n + 2^{2R} = b + (n + \ell)2^{R+1} + 2^{2R}.$$

Comme on déduit de (2.2) que $n + \ell < (c + \frac{1}{2}c^2)2^R = 2^{R-1}$, il s'ensuit que

$$s_2\left((n + 2^R)^2\right) = s_2(b) + s_2(n + \ell) + 1$$

d'où, en vertu de (2.3),

$$(2.4) \quad s_2\left((n + 2^R)^2\right) - s_2(n^2) = s_2(n + \ell) - s_2(\ell) + 1.$$

En désignant par I_ℓ l'ensemble des entiers de I satisfaisant à $\ell 2^{R+1} \leq n^2 < (\ell + 1)2^{R+1}$, nous pouvons donc écrire

$$\begin{aligned} \left| \sum_{n \in I} (-1)^{s_2(n^2)} + \sum_{n \in 2^{R+1}I} (-1)^{s_2(n^2)} \right| &= \left| \sum_{n \in I} \left\{ (-1)^{s_2(n^2)} + (-1)^{s_2((n+2^R)^2)} \right\} \right| \\ &\leq \sum_{n \in I} \left\{ 1 + (-1)^{s_2((n+2^R)^2) - s_2(n^2)} \right\} \\ &= \sum_{\ell \leq c^2 2^{R-1}} \sum_{n \in I_\ell} \left\{ 1 + (-1)^{s_2(n+\ell) - s_2(\ell) + 1} \right\} \\ &\leq |I| - \sum_{\ell \leq c^2 2^{R-1}} (-1)^{s_2(\ell)} \sum_{n \in \ell + I_\ell} (-1)^{s_2(n)}. \end{aligned}$$

Désignons par S_ℓ la somme intérieure. D'après (1.2), on a $|S_\ell| \leq 2$ pour tout ℓ . De plus, $|S_\ell| \leq 1$ sauf éventuellement si la borne inférieure de $\ell + I_\ell$ est impaire, la borne supérieure paire. Or, comme les intervalles I_ℓ sont consécutifs, on a

$$\max(\ell + I_\ell) + 2 = \min(\ell + 1 + I_{\ell+1})$$

pour tout ℓ . Cela implique $\min(|S_\ell|, |S_{\ell+1}|) \leq 1$ pour tout ℓ et donc

$$\left| \sum_{n \in I} (-1)^{s_2(n^2)} + \sum_{n \in 2^R + I} (-1)^{s_2(n^2)} \right| \leq |I| + \frac{3}{2}(1 + c^2 2^{R-1}) + 2,$$

d'où, puisque $I \cup (2^R + I) \subset [0, N]$,

$$\begin{aligned} \left| \sum_{n \leq N} (-1)^{s_2(n^2)} \right| &\leq N + 1 - |I| + \frac{3}{4}c^2 2^R + \frac{7}{2} \leq N - 2^R \left(\frac{3}{4}c^2 - c \right) + \frac{9}{2} \\ &= N \left(1 - \frac{2^R(10\sqrt{2} - 13)}{4N} \right) + \frac{9}{2} \leq \left(\frac{13}{16}\sqrt{2} - \frac{1}{4} \right) N + \frac{9}{2}. \end{aligned}$$

□

3. Démonstration du Théorème 1.2

Nous établissons ici un résultat général dont le Théorème 1.2 est une conséquence immédiate. Désignons par $\mathcal{P}_d(I, J)$ l'ensemble des matrices $I \times J$ du type

$$M = (f_{ij})_{\substack{0 \leq i < I \\ 0 \leq j < J}}$$

où les f_{ij} sont des polynômes à coefficients entiers positifs ou nuls tels que :

- (i) $\deg f_{i0} = d$ ($0 \leq i < I$),
- (ii) si λ_i désigne le coefficient dominant de f_{i0} pour $0 \leq i < I$, alors

$$\lambda_i / \lambda_h \notin \{q^\nu : \nu \in \mathbb{Z}\} \quad (0 \leq i < h < I),$$

- (iii) $\deg f_{ij} < d$ ($0 \leq i < I, 1 \leq j < J$).

Pour chaque matrice M de $\mathcal{P}_d(I, J)$, on note $n \mapsto \sigma(n; M)$ la fonction arithmétique à valeurs dans \mathbb{N}^I définie par

$$\sigma(n; M) := \left(\sum_{0 \leq j < J} s_q(f_{ij}(n)) \right)_{0 \leq i < I}.$$

Théorème 3.1. Soient d, m, I, J des entiers strictement positifs, et soit M une matrice de $\mathcal{P}_d(I, J)$. Il existe des constantes positives $C = C(m, M)$ et $N_0 = N_0(m, M)$ telles que

$$(3.1) \quad \min_{\mathbf{g} \in (\mathbb{Z}/m\mathbb{Z})^I} \sum_{\substack{n \leq N \\ \sigma(n; M) \equiv \mathbf{g} \pmod{m}}} 1 \geq CN^{\min(1, 2/d!)} \quad (N > N_0).$$

Démonstration. Commençons par examiner le cas $d = 1$. Ainsi qu'il est établi dans la remarque qui suit cette démonstration, la relation (3.1) est alors satisfaite sous la forme plus précise d'une formule asymptotique.

Cependant, la preuve du cas $d = 2$ nécessite un renforcement de nature différente, que nous décrivons maintenant. Par hypothèse, il existe des nombres entiers λ_i, μ_i ($0 \leq i < I$) et μ_{ij} ($0 \leq i < I, 1 \leq j < J$) tels que

$$f_{i0}(n) = \lambda_i n + \mu_i \quad (0 \leq i < I), \quad f_{ij}(n) = \mu_{ij} \quad (0 \leq i < I, 1 \leq j < J).$$

On a donc, pour tout $\mathbf{g} \in (\mathbb{Z}/m\mathbb{Z})^I$,

$$(3.2) \quad \sum_{\substack{x < n \leq x+N \\ \sigma(2n; M) \equiv \mathbf{g} \pmod{m}}} 1 = \frac{1}{m^I} \sum_{2x < n \leq 2x+2N} \frac{1 + (-1)^n}{2} \prod_{0 \leq i < I} \{1 + \chi_i(n)\}$$

où l'on a posé

$$\chi_i(n) := \sum_{1 \leq \nu < m} e\left(\frac{\nu}{m} \{s_q(\lambda_i n + \mu_i) + \vartheta_i - g_i\}\right)$$

avec $\vartheta_i := \sum_{1 \leq j < J} s_q(\mu_{ij})$ ($0 \leq i < I$). Nous allons établir que le membre de gauche de (3.2) est $\gg_M N$ sous l'hypothèse que le vecteur $\boldsymbol{\mu} := (\mu_i)_{0 \leq i < I}$ vérifie

$$(3.3) \quad \boldsymbol{\mu} = \boldsymbol{\mu}' + q^\Delta \boldsymbol{\mu}''$$

où $\|\boldsymbol{\mu}'\|_\infty \ll_M 1$ et $\Delta = \Delta(M)$ est une constante assez grande.

Cela résulte simplement du théorème A. En effet, en développant le produit en i dans (3.2) et appliquant (1.4) avec $\mathbf{h} = \boldsymbol{\lambda}$, $\mathbf{k}' = \boldsymbol{\mu}'$, $\mathbf{k}'' = \boldsymbol{\mu}''$, et $q^\Delta = \varrho^D$, nous obtenons que, pour $N > N_1(\Delta, m, M)$, chaque somme d'exponentielles non triviale est majorée en module par $e^{-c\Delta} N$ où $c = c(M) > 0$. Un choix convenable de Δ fournit donc, par exemple, sous l'hypothèse (3.3),

$$(3.4) \quad \sum_{\substack{x < n \leq x+N \\ \sigma(2n; M) \equiv \mathbf{g} \pmod{m}}} 1 \geq N/(3m^I) \quad (N > N_0(m, M)).$$

Considérons ensuite le cas $d = 2$. Il existe des nombres entiers positifs ou nuls λ_i, μ_i, ν_i ($0 \leq i < I$) et λ_{ij}, μ_{ij} ($0 \leq i < I, 1 \leq j < J$) tels que

$$f_{i0}(n) = \lambda_i n^2 + \mu_i n + \nu_i \quad (0 \leq i < I), \\ f_{ij}(n) = \lambda_{ij} n + \mu_{ij} \quad (0 \leq i < I, 1 \leq j < J).$$

De plus, les λ_i sont strictement positifs et satisfont la condition (ii) ci-dessus. Donnons-nous alors trois paramètres $\varepsilon \in]0, 1[$, $\eta \in]0, 1[$, $\ell \in \mathbb{N} \cap]\frac{1}{4}\varepsilon^2 q^R, \frac{1}{2}\varepsilon^2 q^R]$, posons

$$\ell_i := \ell \lambda_i \quad (0 \leq i < I),$$

définissons $R \in \mathbb{N}$ par $q^{R-1} < \varepsilon N \leq q^R$, et considérons l'ensemble $\mathcal{A}_\ell := \mathcal{A}_\ell(\varepsilon, \eta)$ de tous les entiers n satisfaisant à

$$(3.5) \quad \ell q^R \leq n^2 < q^R(\ell + \eta).$$

Définissons X_ℓ , et N_ℓ par $\mathcal{A}_\ell = [X_\ell, X_\ell + N_\ell[\cap \mathbb{N}$. Nous notons immédiatement, à fins de référence ultérieure, que (3.5) implique

$$\frac{\eta}{3\varepsilon} \leq \frac{\eta q^{R/2}}{3\sqrt{\ell}} \leq N_\ell \leq \frac{\eta q^{R/2}}{2\sqrt{\ell}} \leq \frac{\eta}{\varepsilon}.$$

Si $\eta = \eta(M)$ est assez petit, on a pour tout n de \mathcal{A}_ℓ ,

$$\ell_i q^R \leq f_{i0}(n) < (\ell_i + 1)q^R \quad (0 \leq i < I).$$

Posant

$$f_{i0}(n) = \ell_i q^R + v_{in}$$

de sorte que $0 \leq v_{in} < q^R$, nous pouvons donc écrire, pour tous $i \in [0, I[$, $T \geq 0$, $0 \leq t \leq T$, et si $\varepsilon = \varepsilon(m, M, T)$ est assez petit,

$$f_{i0}(n + tq^R) = \ell_i q^R + v_{in} + tq^R f'_{i0}(n) + \lambda_i t^2 q^{2R},$$

d'où

$$\begin{aligned} s_q(f_{i0}(n + tq^R)) &= s_q(v_{in}) + s_q(\ell_i + t f'_{i0}(n)) + s_q(\lambda_i t^2) \\ &= s_q(f_{i0}(n)) + s_q(\ell_i + t f'_{i0}(n)) + s_q(\lambda_i t^2) - s_q(\ell_i) \\ &= s_q(f_{i0}(n)) + s_q(2t\lambda_i n + \ell_i + t\mu_i) + s_q(\lambda_i t^2) - s_q(\ell_i). \end{aligned}$$

Par ailleurs, nous avons, sous les mêmes hypothèses,

$$f_{ij}(n + tq^R) = f_{ij}(n) + \lambda_{ij} tq^R \quad (0 \leq i < I, 1 \leq j < J),$$

d'où

$$s_q(f_{ij}(n + tq^R)) = s_q(f_{ij}(n)) + s_q(t\lambda_{ij}) \quad (1 \leq i < I, 0 \leq j < J).$$

Nous obtenons donc, pour $n \in \mathcal{A}_\ell(\varepsilon, \eta)$, $0 \leq t \leq T$,

$$(3.6) \quad \sigma(n + tq^R; M) - \sigma(n; M) = s_q(\mathbf{h}_t 2n + \mathbf{k}_t) + \boldsymbol{\varrho}_t$$

où l'on a posé

$$\begin{aligned} \mathbf{h}_t &:= (\lambda_i t)_{0 \leq i < I}, & \mathbf{k}_t &:= (\mu_i t + \ell_i)_{0 \leq i < I}, \\ \mathbf{e}_t &:= \left(s_q(\lambda_i t^2) - s_q(\ell_i) + \sum_{1 \leq j < J} s_q(t \lambda_{ij}) \right)_{0 \leq i < I}. \end{aligned}$$

Soient $W := m^I$ et $\{t_w\}_{w=1}^W$ une suite finie d'entiers strictement positifs deux à deux distincts tels que

$$(3.7) \quad (t_w, q \prod_{0 \leq i < I} \lambda_i) = 1 \quad (1 \leq w \leq W).$$

Soit alors $\{\mathbf{g}_w\}_{w=1}^W$ une suite exhaustive de vecteurs de $(\mathbb{Z}/m\mathbb{Z})^I$. En appliquant (3.4) avec IW au lieu de I et pour une matrice dont la première colonne est $\mathbf{h}n + \mathbf{k}$ avec

$$h_r := \lambda_i t_w, \quad k_r := \mu_i t_w + \ell_i \quad \text{si } r = i + (w-1)I \quad (0 \leq i < I, 1 \leq w \leq W),$$

nous obtenons que, si $\ell \equiv 0 \pmod{q^\Delta}$ pour une constante convenable $\Delta = \Delta(M, T)$, et si ε assez petit en fonction de m, M, T et η , il existe au moins

$$C|\mathcal{A}_\ell| \geq \frac{C\eta q^{R/2}}{3\sqrt{\ell}}$$

entiers n de \mathcal{A}_ℓ tels que

$$\sigma(n + t_w q^R; M) - \sigma(n; M) \equiv \mathbf{g} + \mathbf{g}_w \pmod{m} \quad (1 \leq w \leq W).$$

Pour chacun de ces entiers, il existe un w tel que $\mathbf{g}_w + \sigma(n; M) \equiv 0 \pmod{m}$. Le nombre total des entiers $n \leq N$ satisfaisant $\sigma(n; M) \equiv \mathbf{g} \pmod{m}$ est donc au moins égal à

$$\sum_{\substack{\frac{1}{4}\varepsilon^2 q^R < \ell \leq \frac{1}{2}\varepsilon^2 q^R \\ \ell \equiv 0 \pmod{q^\Delta}}} \frac{C\eta q^{R/2}}{3\sqrt{\ell}} \gg N.$$

Comme $\mathcal{A}_\ell + tq^R \subset [1, N]$ pour $t \leq T$, $\frac{1}{4}\varepsilon^2 q^R < \ell \leq \frac{1}{2}\varepsilon^2 q^R$ et ε assez petit, cela établit bien le cas $d = 2$ de notre théorème.

Nous procédons ensuite par récurrence sur d . Supposons donc la propriété établie jusqu'au rang $d-1$ avec $d \geq 3$. Soit $N \geq 1$ et $R \in \mathbb{N}$ tel que $q^{R-1} < N \leq q^R$. Pour tous entiers $n \geq 0$, $t \geq 0$, et tout polynôme f de degré au plus d et à coefficients entiers positifs ou nuls, on peut écrire la formule de Taylor

$$(3.8) \quad f(n + tq^R) = \sum_{0 \leq v \leq d} \frac{t^v q^{Rv}}{v!} f^{(v)}(n).$$

Il s'ensuit que si, $n \leq C_1 N^{1/d} \leq C_1 q^{R/d}$ où C_1 est une constante strictement positive ne dépendant que de f , on a

$$(3.9) \quad s_q\left(f(n + tq^R)\right) = \sum_{0 \leq v \leq d} s_q\left(\frac{t^v}{v!} f^{(v)}(n)\right).$$

En appliquant cette formule à tous les polynômes f_{ij} et en notant $M_v := M^{(v)}/v!$ où $M^{(v)}$ désigne la dérivée d'ordre v de la matrice M , nous obtenons

$$(3.10) \quad \sigma(n + tq^R; M) - \sigma(n; M) = \sum_{1 \leq v \leq d} \sigma(n; t^v M_v).$$

Soit $\{t_w\}_{w=1}^W$ une suite finie d'entiers positifs deux à deux distincts satisfaisant (3.7). Appliquons (3.10) avec $t = t_w$ pour $1 \leq w \leq W$. Nous obtenons

$$\sigma(n; A) = \sigma(n; B)$$

où

$$A := (a_{rs})_{\substack{0 \leq r < IW \\ 0 \leq j < J}} = \begin{pmatrix} M(\cdot + t_1 q^R) - M \\ \vdots \\ M(\cdot + t_W q^R) - M \end{pmatrix}$$

et

$$B := (b_{ru})_{\substack{0 \leq r < IW \\ 0 \leq u < dJ}} = \begin{pmatrix} t_1 M_1 & t_1^2 M_2 & \cdots & t_1^d M_d \\ t_2 M_1 & t_2^2 M_2 & \cdots & t_2^d M_d \\ \vdots & \vdots & \cdots & \vdots \\ t_W M_1 & t_W^2 M_2 & \cdots & t_W^d M_d \end{pmatrix}$$

sont respectivement définies par

$$a_{rs}(n) := f_{ij}(n + t_w q^R) - f_{ij}(n) \quad \text{si } \begin{cases} r = i + (w-1)I & \text{où } 0 \leq i < I, 1 \leq w \leq W, \\ s = j & \text{où } 0 \leq j < J, \end{cases}$$

et

$$b_{ru}(n) := \frac{t_w^v}{v!} f_{ij}^{(v)}(n) \quad \text{si } \begin{cases} r = i + (w-1)I & \text{où } 0 \leq i < I, 1 \leq w \leq W, \\ u = j + (v-1)J & \text{où } 0 \leq j < J, 1 \leq v \leq d. \end{cases}$$

On a $B \in \mathcal{P}_{d-1}(IW, dJ)$. En effet, on a d'une part

$$\begin{cases} \deg b_{r0} = d-1 & (0 \leq r < IW) \\ \deg b_{ru} < d-1 & (0 \leq r < IW, 1 \leq u < dJ) \end{cases}$$

et, d'autre part, si μ_r désigne le coefficient dominant de b_{r0} , alors, pour $1 \leq r < r_1 < IW$, il existe des indices i, i_1, w et w_1 tels que $\mu_r = t_w \lambda_i$, $\mu_{r_1} = t_{w_1} \lambda_{i_1}$ et donc

$$\frac{\mu_r}{\mu_{r_1}} = \frac{t_w \lambda_i}{t_{w_1} \lambda_{i_1}} \notin \{q^\nu : \nu \in \mathbb{Z}\}.$$

Choisissons $W = I^m$ et désignons par $\{\mathbf{g}_w\}_{w=1}^W$ une suite exhaustive de vecteurs de $(\mathbb{Z}/m\mathbb{Z})^I$, il découle de l'hypothèse de récurrence que l'on a

$$\sigma(n + t_w q^R; M) - \sigma(n; M) \equiv \mathbf{g} + \mathbf{g}_w \pmod{m} \quad (1 \leq w \leq W)$$

pour au moins $C_0 N^{2/d!}$ entiers $n \leq C_1 N^{1/d}$. Or, pour chacun de ces entiers, il existe un w tel que $\mathbf{g}_w + \sigma(n; M) \equiv 0 \pmod{m}$. \square

Remarque. Par la méthode décrite plus haut, la majoration (1.5) fournit immédiatement que, dans le cas $d = 1$, la relation (3.1) a lieu sous la forme forte suivante :

$$(3.11) \quad (\forall \mathbf{g} \in (\mathbb{Z}/m\mathbb{Z})^I) \quad \sum_{\substack{x < n \leq x+N \\ \sigma(n; M) \equiv \mathbf{g} \pmod{m}}} 1 = \frac{N + O(N^{1-\kappa})}{m^I}$$

où $\kappa = \kappa(m, M) > 0$, uniformément en $x \geq 0$.

Bibliographie

- [1] J. Coquet, Sur la représentation des multiples d'un entier dans une base, *Publications mathématiques d'Orsay* 83.04, Colloque Hubert Delange (7-8 juin 1982), 20-37.
- [2] C. Dartyge et G. Tenenbaum, Sommes de chiffres de multiples d'entiers, *Ann. Inst. Fourier (Grenoble)*, à paraître.
- [3] A. O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.* **13** (1968), 259-265.
- [4] C. Mauduit et J. Rivat, Répartition des fonctions q -multiplicatives dans la suite $([n^c])_{n \in \mathbb{N}}$, $c > 1$, *Acta Arith.* **71**, n° 2 (1995), 171-179.
- [5] J. A. Solinas, On the joint distribution of digital sums, *J. Number Theory* **33** (1989), 132-151.

Cécile Dartyge & Gérald Tenenbaum
 Institut Élie Cartan
 Université Henri Poincaré–Nancy 1
 BP 239
 54506 Vandœuvre Cedex
 France
 dartyge@iecn.u-nancy.fr, gerald.tenenbaum@ciril.fr