



HAL
open science

Nombres premiers avec contraintes digitales multiples

Bruno Martin, Christian Mauduit, Joel Rivat

► **To cite this version:**

Bruno Martin, Christian Mauduit, Joel Rivat. Nombres premiers avec contraintes digitales multiples. Bulletin de la société mathématique de France, 2019, 147 (2), pp.259-287. 10.24033/bsmf2781 . hal-03526404

HAL Id: hal-03526404

<https://hal.science/hal-03526404>

Submitted on 13 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

NOMBRES PREMIERS AVEC CONTRAINTES DIGITALES MULTIPLES

BRUNO MARTIN, CHRISTIAN MAUDUIT & JOËL RIVAT

RÉSUMÉ. Soit $q \geq 2$ un nombre entier. Pour tout nombre entier $n \geq 1$ et $k \in \{0, \dots, q-1\}$ nous notons $|n|_k$ le nombre d'apparitions du chiffre k dans le développement de n en base q . Nous étudions la distribution jointe des fonctions $(n \mapsto |n|_k)_{1 \leq k < q}$ le long de la suite des nombres premiers. Nous obtenons notamment une formule asymptotique pour le cardinal de l'ensemble des nombres premiers p n'excédant pas x et équilibrés en base q (*i.e* dont les chiffres en base q satisfont à la condition $||p|_i - |p|_j| \leq 1$ pour tout $(i, j) \in \{0, \dots, q-1\}^2$).

ABSTRACT. Let $q \geq 2$ be an integer. For every positive integer n and $k \in \{0, \dots, q-1\}$ we denote by $|n|_k$ the number of occurrences of the digit k in the representation of n in base q . We study the joint distribution of the functions $(n \mapsto |n|_k)_{1 \leq k < q}$ along the sequence of prime numbers. We obtain an asymptotic formula for the number of primes less than x which are balanced in base q (*i.e* such that the digits in base q satisfy the condition $||p|_i - |p|_j| \leq 1$ for all $(i, j) \in \{0, \dots, q-1\}^2$).

1. NOTATIONS ET RAPPELS

Dans tout ce qui suit, q est un nombre entier supérieur ou égal à 2 et p désigne systématiquement un nombre premier. On note \log_q la fonction logarithme en base q . Pour $x \in \mathbb{R}$, $\pi(x)$ désigne le nombre de nombres premiers n'excédant pas x , tandis que pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, $\pi(x; a, b)$ désigne le nombre de nombres premiers p n'excédant pas x et tels que $p \equiv a \pmod{b}$. Pour $t \in \mathbb{R}$, on note $\|t\|$ la distance de t au nombre entier le plus proche et l'on pose $e(t) = e^{2i\pi t}$. Si $\mathbf{u} = (u_1, \dots, u_n)$ et $\mathbf{v} = (v_1, \dots, v_n)$ sont des éléments de \mathbb{R}^n , on note $\mathbf{u} \cdot \mathbf{v} = \sum_{j=1}^n u_j v_j$ leur produit scalaire usuel et $\|\mathbf{u}\|_\infty = \max_{1 \leq j \leq n} |u_j|$. La fonction indicatrice d'Euler est désignée par la lettre φ .

Rappelons que tout nombre entier strictement positif n admet un unique développement q -adique de la forme

$$(1) \quad n = \sum_{j=0}^{\nu} n_j q^j, \quad 0 \leq n_j \leq q-1, \quad n_\nu \geq 1.$$

Pour $n = 0$, on convient de poser $\nu = 0$ et $n_0 = 0$. Conformément à l'usage, on désigne pour tout $0 \leq k \leq q-1$ par $|\cdot|_k$ la fonction comptant le nombre d'apparitions du chiffre k dans le développement en base q , soit

$$|n|_k = \#\{0 \leq j \leq \nu : n_j = k\}$$

Date: 3 novembre 2018.

2010 Mathematics Subject Classification. 11A63, 11J71, 11L20, 11N05.

Key words and phrases. prime numbers, exponential sums, digital functions, uniform distribution modulo 1.

Ce travail a bénéficié de l'aide de l'Agence Nationale de la Recherche portant les références «ANR-14-CE34-0009» MUDERA.

et on appelle fonction digitale (à valeurs entières) toute fonction $g : \mathbb{N} \rightarrow \mathbb{Z}$ de la forme

$$g(n) = \sum_{k=0}^{q-1} a_k |n|_k,$$

avec $(a_0, \dots, a_{q-1}) \in \mathbb{Z}^q$. Un exemple classique de fonction digitale est donné par la fonction somme des chiffres en base q définie, pour tout nombre entier n , par

$$s_q(n) = \sum_{j=0}^{\nu} n_j = \sum_{k=1}^{q-1} k |n|_k.$$

2. PRÉSENTATION DES RÉSULTATS

L'objet de cet article est d'étudier la distribution jointe du $(q-1)$ -uplet de fonctions $(n \mapsto |n|_k)_{1 \leq k \leq q-1}$ le long de la suite des nombres premiers.

2.1. Distribution dans les progressions arithmétiques. C'est avec l'article [5] de Gelfond que s'ouvre le problème de déterminer la répartition dans les progressions arithmétiques des valeurs prises par une fonction digitale à valeurs entières le long d'une suite donnée. En particulier Gelfond pose la question de déterminer la répartition de $s_q(p)$ dans les progressions arithmétiques lorsque p parcourt l'ensemble des nombres premiers. Ce problème a été résolu par Mauduit et Rivat qui obtiennent, étant donné un nombre entier $m \geq 2$, l'existence de $\sigma_{q,m} > 0$ tel que pour tous $a \in \mathbb{Z}$, $x \geq 2$, on a

$$\text{card}\{p \leq x : s_q(p) \equiv a \pmod{m}\} = \frac{\text{pgcd}(m, q-1)}{m} \pi(x; a, \text{pgcd}(m, q-1)) + O(x^{1-\sigma_{q,m}}).$$

Plusieurs auteurs ont étendu ce résultat à d'autres classes de fonctions digitales ou automatiques (cf. [10], [1], [12], [6], [14]). Nous obtenons dans cet article un premier exemple de résultat de ce type dans le cas multi-dimensionnel.

Théorème 1. *Il existe $c = c(q) > 0$ tel que l'on a uniformément pour tous $x \geq 2$, $\mathbf{m} = (m_1, \dots, m_{q-1}) \in (\mathbb{Z} \setminus \{0\})^{q-1}$ et $\boldsymbol{\ell} = (\ell_1, \dots, \ell_{q-1}) \in \mathbb{Z}^{q-1}$,*

$$\text{card}\{p \leq x : \forall k \in \{1, \dots, q-1\}, |p|_k \equiv \ell_k \pmod{m_k}\} = \frac{d_{\mathbf{m}} \pi(x; \mathbf{v}_{\boldsymbol{\ell}}, d_{\mathbf{m}})}{m_1 \dots m_{q-1}} + O((\log x)^3 x^{1-c/\|\mathbf{m}\|_{\infty}^4}),$$

où l'on a posé

$$(2) \quad d_{\mathbf{m}} = \text{pgcd}(m_1, 2m_2, \dots, km_k, \dots, (q-1)m_{q-1}, q-1) \quad \text{et} \quad \mathbf{v}_{\boldsymbol{\ell}} = \sum_{k=1}^{q-1} k \ell_k.$$

La constante implicite ne dépend que de q .

Le théorème 1 n'a d'intérêt que si $(\mathbf{v}_{\boldsymbol{\ell}}, d_{\mathbf{m}}) = 1$, puisque l'on a l'inclusion

$$\{p \leq x : \forall k \in \{1, \dots, q-1\}, |p|_k \equiv \ell_k \pmod{m_k}\} \subseteq \{p \leq x : p \equiv \mathbf{v}_{\boldsymbol{\ell}} \pmod{d_{\mathbf{m}}}\}.$$

2.2. Loi locale. Étant donnée une fonction arithmétique $g : \mathbb{N}^* \rightarrow \mathbb{Z}$, un problème classique consiste à déterminer sa loi locale, c'est-à-dire obtenir une estimation asymptotique pour tout $k \in \mathbb{Z}$ de la quantité

$$\text{card}\{n \leq x : g(n) = k\}$$

lorsque $x \rightarrow +\infty$. Les exemples classiques sont les fonctions Ω et ω (voir par exemple [15] chapitre II.6.1) qui dénombrent le nombre de facteurs premiers d'un nombre entier, comptés avec ou sans leur ordre de multiplicité. Plusieurs travaux récents traitent du cas où g est une fonction digitale. Le premier résultat de cet ordre a été obtenu par Mauduit et Sárközy dans [13] qui établissent une formule asymptotique pour $\text{card}\{n < q^\nu : s_q(n) = k\}$, uniforme pour $\nu \rightarrow +\infty$ et $0 \leq k \leq \frac{q-1}{2}\nu$. En s'appuyant sur ces résultats lorsque k est proche de la valeur moyenne $\frac{q-1}{2}\nu$, Fouvry et Mauduit étudient dans [4] l'ensemble

$$\mathcal{E} = \left\{ n \in \mathbb{N}^* : s_q(n) = \frac{q-1}{2} \lfloor \log_q n \rfloor + B(\lfloor \log_q n \rfloor) \right\},$$

où $B : \mathbb{N} \rightarrow \mathbb{R}$ est une fonction telle que pour tout $j \in \mathbb{N}$, $\frac{q-1}{2}j + B(j) \in \mathbb{N}$ et telle que

$$(3) \quad \text{il existe } K > 0 \text{ tel que pour tout } n \in \mathbb{N}^*, |B(n)| \leq Kn^{1/4}.$$

Par exemple, pour $g = s_2$ et $B(j) = \lfloor j/2 \rfloor - j/2$, on a¹

$$\mathcal{E} = \left\{ n \in \mathbb{N}^* : s_2(n) = \left\lfloor \frac{1}{2} \log_2 n \right\rfloor \right\}.$$

Le théorème 1.1 de [4] montre que pour tout $x \geq 2$, on a

$$(4) \quad \text{card}\{n \leq x : n \in \mathcal{E}\} = \sqrt{\frac{6}{\pi(q^2-1)}} \frac{x}{\sqrt{\log_q x}} + O\left(\frac{x}{\log_q x}\right),$$

où la constante implicite ne dépend que de K et q . Fouvry et Mauduit étudient alors la régularité statistique de l'ensemble \mathcal{E} en établissant que pour tout $\beta \in \mathbb{R} \setminus \mathbb{Q}$, la suite $(n\beta)_{n \in \mathcal{E}}$ est équirépartie modulo 1 (théorème 1.2 de [4]).

Remarque 1. La formule (4) n'est plus valable en toute généralité sous la condition² :

$$(5) \quad \text{il existe } K > 0 \text{ tel que pour tout } n \in \mathbb{N}^*, |B(n)| \leq Kn^{1/2},$$

mais le théorème 1.2 de [4] reste valide sous la condition (5). En effet, sous la condition (5), on peut assez rapidement vérifier qu'il existe des constantes $C_1, C_2 > 0$ dépendant de K et q telles que pour tout $x \geq x_0(K, q)$ on a

$$C_1 \frac{x}{\sqrt{\log x}} \leq \text{card}\{n \leq x : n \in \mathcal{E}\} \leq C_2 \frac{x}{\sqrt{\log x}}$$

1. Rappelons que pour tout $y \in \mathbb{R}$, on a $\lfloor y/2 \rfloor = \lfloor \lfloor y \rfloor / 2 \rfloor$.

2. Par exemple pour $q = 2$, et

$$B(j) = \begin{cases} \lfloor \sqrt{j} \rfloor & \text{si } j \text{ est pair,} \\ -\lfloor j/2 \rfloor & \text{si } j \text{ est impair,} \end{cases}$$

on peut montrer, à l'aide de la formule de Stirling, que la suite $\left(\left(\frac{2^\nu}{\sqrt{\nu}} \right)^{-1} \text{card}\{n \leq 2^\nu : n \in \mathcal{E}\} \right)_{\nu \in \mathbb{N}^*} =$

$\left(\left(\frac{2^\nu}{\sqrt{\nu}} \right)^{-1} \binom{\nu}{\frac{\nu}{2} + B(\nu)} \right)_{\nu \in \mathbb{N}^*}$ ne converge pas.

et ceci permet de constater, en examinant la démonstration du théorème 1.2 de [4], que la condition (5) reste suffisante pour garantir que pour tout $\beta \in \mathbb{R} \setminus \mathbb{Q}$ la suite $(\beta n)_{n \in \mathcal{E}}$ est équirépartie modulo 1.

Dans [11], Mauduit étudie les ensembles de nombres entiers reconnaissables par un q -automate infini déterministe associé à une marche aléatoire de moyenne nulle sur un réseau de dimension d , l'exemple le plus simple étant l'ensemble des nombres entiers $n \in \mathbb{N}^*$ satisfaisant à $|n|_0 = |n|_1 = \dots = |n|_{q-1}$ (on a ici $d = q - 1$). Plus généralement Drmota et Mauduit [2] considèrent

$$\mathcal{N} = \left\{ n \in \mathbb{N}^* : L_k(|n|_0, |n|_1, \dots, |n|_{q-1}) = \lfloor \eta_k \log_q n \rfloor + v_k, k = 1, \dots, m \right\},$$

où $\mathcal{L} = (L_1, \dots, L_m)$ est une famille de formes linéaires définies sur \mathbb{R}^q , $\boldsymbol{\eta} = (\eta_1, \dots, \eta_m) \in \mathbb{R}^m$ et $\mathbf{v} = (v_1, \dots, v_m) \in \mathbb{Z}^m$. Sous des hypothèses assez générales sur le triplet $(\mathcal{L}, \boldsymbol{\eta}, \mathbf{v})$ que nous ne détaillons pas ici, Drmota et Mauduit déterminent l'ordre de grandeur du cardinal de $\mathcal{N} \cap [1, x]$, et montrent que pour tout $\beta \in \mathbb{R} \setminus \mathbb{Q}$, la suite $(\beta n)_{n \in \mathcal{N}}$ est équirépartie modulo 1.

Dans [3], Drmota, Mauduit et Rivat étudient la loi locale de s_q au voisinage de sa valeur moyenne le long de la suite des nombres premiers : ils obtiennent que pour tout $\varepsilon \in]0, 1/2[$, $k \in \mathbb{N}^*$ tel que $(k, q) = 1$, on a

$$(6) \quad \text{card}\{p \leq x : s_q(p) = k\} = \frac{q-1}{\varphi(q-1)} \frac{\pi(x)}{\sqrt{2\pi\sigma_q^2 \log_q x}} \left(e^{-\frac{(k-\mu_q \log_q x)^2}{2\sigma_q^2 \log_q x}} + O((\log x)^{-\frac{1}{2}+\varepsilon}) \right),$$

où $\mu_q = \frac{q-1}{2}$ et $\sigma_q^2 = \frac{q^2-1}{12}$. Ce résultat est étendu dans [8] à toute fonction $g = \sum_{1 \leq k < q} a_k | \cdot |_k$ avec $(a_k)_{1 \leq k < q} \in \mathbb{Z}^{q-1}$. Nous obtenons dans cet article un résultat de ce type dans le cas multidimensionnel.

Théorème 2. Soit $\varepsilon \in]0, 1/2[$, $r \in \{1, \dots, q-1\}$ et $\mathbf{k} = (k_1, \dots, k_r) \in \mathbb{N}^r$ tel que $1 \leq k_1 < \dots < k_r \leq q-1$. On a uniformément pour tous $x \geq 2$ et $\mathbf{b} = (b_1, \dots, b_r) \in \mathbb{N}^r$,

$$(7) \quad \text{card}\{p \leq x : |p|_{k_1} = b_1, \dots, |p|_{k_r} = b_r\} = \delta_{\mathbf{k}} C_{r,q} \frac{\pi(x; \mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}})}{(\log_q x)^{r/2}} e^{-\frac{1}{2}R(u_{x,\mathbf{b}})} + O\left(\frac{\pi(x)}{(\log x)^{\frac{r+1}{2}-\varepsilon}}\right),$$

avec³

$$(8) \quad \delta_{\mathbf{k}} = \text{pgcd}(k'_1, \dots, k'_s, q-1) \text{ où } \{k'_1, \dots, k'_s\} = \{1, \dots, q-1\} \setminus \{k_1, \dots, k_r\},$$

$$C_{r,q} = \sqrt{\frac{q^{r+1}}{(q-r)(2\pi)^r}},$$

$$R(\boldsymbol{\alpha}) = q \sum_{i=1}^r \alpha_i^2 + \frac{q}{q-r} \left(\sum_{i=1}^r \alpha_i \right)^2 \quad \text{et} \quad u_{x,\mathbf{b}} = \left(\frac{\frac{1}{q} \log_q x - b_1}{\sqrt{\log_q x}}, \dots, \frac{\frac{1}{q} \log_q x - b_r}{\sqrt{\log_q x}} \right).$$

La constante implicite dans (7) ne dépend que de ε , q et k_1, \dots, k_r .

Comme l'on a

$$\{p \leq x : |p|_{k_1} = b_1, \dots, |p|_{k_r} = b_r\} \subseteq \{p \leq x : p \equiv \mathbf{b} \cdot \mathbf{k} \pmod{\delta_{\mathbf{k}}}\},$$

3. On convient que si $r = q-1$, alors $s = 0$ et $\delta_{\mathbf{k}} = q-1$.

le théorème 2 n'est intéressant que si $(\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}) = 1$ et si les nombres entiers b_1, \dots, b_r sont proches de la valeur $\frac{1}{q} \log_q x$, soit

$$(9) \quad \forall i \in \{1, \dots, r\}, b_i = \frac{1}{q} \log_q x + O(\sqrt{\log x}).$$

2.3. Nombres premiers équilibrés en base q .

Définition 1. On dit qu'un nombre entier $n \geq 1$ est équilibré en base q s'il satisfait

$$(10) \quad \forall (i, j) \in \{0, \dots, q-1\}^2, \quad ||n|_i - |n|_j| \leq 1.$$

On note \mathcal{E}_q l'ensemble des nombres équilibrés en base q .

Cet ensemble est reconnaissable par un q -automate infini déterministe au sens de [11] associé à une marche aléatoire sur un réseau de dimension $q-1$. On peut montrer facilement que $\text{card}\{n \leq x : n \in \mathcal{E}_q\}$ est de même ordre de grandeur que $\frac{x}{(\log_q x)^{(q-1)/2}}$ (par exemple de manière analogue à la proposition 4.1 de [11]).

Remarque 2. Si $q \geq 4$, alors il n'existe pas de nombre premier p tel que $|p|_0 = \dots = |p|_{q-1}$. En effet, si $|p|_0 = \dots = |p|_{q-1} = k$ avec $k \in \mathbb{N}^*$, alors

$$p \equiv s(p) \equiv \frac{q(q-1)}{2} k \pmod{q-1}.$$

Or si $q \geq 5$ est impair, $\text{pgcd}(\frac{q(q-1)}{2}, q-1) \geq \frac{q-1}{2} > 1$, et si $q \geq 4$ est pair, $\text{pgcd}(\frac{q(q-1)}{2}, q-1) \geq q-1 > 1$.

Théorème 3. Il existe une fonction $Q : \mathbb{R} \rightarrow \mathbb{R}$, strictement positive, 1-périodique si q est pair, 2-périodique si q est impair, non constante, tel que pour tout $\varepsilon > 0$, $x \geq 2$,

$$(11) \quad N_q(x) := \text{card}\{p \leq x : p \in \mathcal{E}_q\} = Q\left(\frac{\log_q x}{q}\right) \frac{x}{(\log_q x)^{(q+1)/2}} \left(1 + O\left((\log x)^{-1/2+\varepsilon}\right)\right).$$

La constante implicite dans (11) ne dépend que de ε et q .

Remarque 3. Le théorème 1 de [8] fournit une estimation uniforme en $\beta \in \mathbb{R}$ de la somme d'exponentielles

$$\sum_{\substack{p \leq x \\ g(p)=k}} e(\beta p)$$

lorsque $g = \sum_{1 \leq k < q} a_k | \cdot |_k$ avec $(a_k)_{1 \leq k < q} \in \mathbb{Z}^{q-1}$ et $(a_0, \dots, a_{q-1}) = 1$. En suivant la méthode développée pour établir le théorème 1 de [8], il est possible de démontrer le résultat suivant : avec les mêmes notations et hypothèses que celles du théorème 2 on a uniformément pour tout $\beta \in \mathbb{R}$,

$$(12) \quad \sum_{\substack{p \leq x \\ |p|_{k_1}=b_1, \dots, |p|_{k_r}=b_r}} e(\beta p) = \frac{\delta_{\mathbf{k}} C_{r,q}}{(\log_q x)^{r/2}} \left(\sum_{\substack{p \leq x \\ p \equiv \mathbf{b} \cdot \mathbf{k} \pmod{\delta_{\mathbf{k}}}} e(\beta p) \right) e^{-\frac{1}{2}R(u_x, \mathbf{b})} + O\left(\frac{\pi(x)}{(\log x)^{\frac{r+1}{2}-\varepsilon}}\right).$$

On peut ainsi déduire de (12) et du critère de Weyl (cf. [7] théorème 2.1 par exemple) que la suite $(\beta p)_{p \in \mathcal{E}_q}$ est équirépartie modulo 1 pour tout $\beta \in \mathbb{R} \setminus \mathbb{Q}$. Nous omettons la démonstration de ce résultat, elle relève d'arguments similaires à ceux employés dans les preuves du corollaire 1 de [8] et du théorème 3 du présent article.

2.4. **Cas général.** Les techniques développées dans cet article permettent d'étudier la distribution jointe de r fonctions données de la forme $g_j(p) = \sum_{1 \leq k < q} a_k^{(j)} |p|_k$ pour $1 \leq j \leq r$ avec $a_k^{(j)} \in \mathbb{Z}$. Néanmoins diverses complications arithmétiques peuvent survenir d'un cas à un autre, même en supposant que pour tout $j \in \{1, \dots, r\}$, $\text{pgcd}(a_k^{(j)})_{1 \leq k < q} = 1$ et que la famille $(g_j)_{1 \leq j \leq r}$ est libre sur \mathbb{Z} :

- il peut exister des nombres entiers $m \geq 2$ tels que la famille $(g_j)_{1 \leq j \leq r}$ soit liée sur \mathbb{Z}_m .
- il peut exister des nombres entiers $m \geq 2$ tels que la famille (s_q, g_1, \dots, g_r) soit liée sur \mathbb{Z}_m ce qui induit des restrictions dans la mesure où pour tout $n \in \mathbb{N}$, $s_q(n) \equiv n \pmod{q-1}$.

Par exemple pour garantir que l'ensemble des nombres premiers satisfaisant en base $q = 5$ à

$$(13) \quad \begin{cases} |p|_1 + |p|_2 + |p|_3 = k_1 \\ |p|_2 + 2|p|_4 = k_2 \\ |p|_1 + |p|_2 + 3|p|_3 + 2|p|_4 = k_3 \end{cases}$$

n'est pas vide il faut imposer les conditions $\text{pgcd}(k_1 + k_2, 2) = 1$, $\text{pgcd}(k_2 + k_3, 4) = 1$ et $k_1 - k_3 \equiv 0 \pmod{2}$, les deux premières conditions provenant de la relation $s_5(n) \equiv n \pmod{4}$ pour tout $n \in \mathbb{N}$. Il semble ainsi difficile d'énoncer et de démontrer des résultats tout à la fois généraux et maniables.

Le problème est encore plus complexe si l'on souhaite prendre en compte le nombre de zéros. Rappelons que la situation est déjà délicate pour $r = 1$ comme en témoignent les exemples fournis dans [10] pp. 191-193.

3. ESTIMATION D'UNE SOMME D'EXPONENTIELLES

Les démonstrations des résultats annoncés reposent sur l'estimation obtenue pour une somme d'exponentielles dans [9]. Nous reformulons ici les théorèmes 1 et 2 de [9]. Rappelons que Λ désigne la fonction de von Mangoldt.

Théorème A. *Il existe $c_0 = c_0(q) > 0$ tel que l'on a uniformément pour tous $x \geq 2$, $\beta \in \mathbb{R}$ et $g = \sum_{0 \leq k < q} \alpha_k | \cdot |_k$ (avec $(\alpha_0, \dots, \alpha_{q-1}) \in \mathbb{R}^q$),*

$$(14) \quad \sum_{n \leq x} \Lambda(n) e(g(n) + \beta n) \ll (\log x)^4 x^{1-c_0 \|(q-1)(\alpha_1 - \alpha_0)\|^2},$$

et

$$(15) \quad \sum_{n \leq x} \Lambda(n) e(g(n) + \beta n) \ll (\log x)^4 x^{1-c_0 \sigma_q(g)},$$

où

$$\sigma_q(g) = \min_{t \in \mathbb{R}} \sum_{0 \leq j < i < q} \|\alpha_i - \alpha_j - (i-j)t\|^2.$$

Signalons que la constante c_0 , qui dépend de q , peut être explicitée en reprenant les démonstrations des théorèmes 1 et 2 de [9].

Nous pouvons en déduire la majoration suivante.

Proposition 1. *Il existe $c_1 = c_1(q) > 0$ tel que l'on a uniformément pour tous $x \geq 2$, $\beta \in \mathbb{R}$ et $(\alpha_1, \dots, \alpha_{q-1}) \in \mathbb{R}^{q-1}$,*

$$\sum_{p \leq x} e \left(\sum_{1 \leq k < q} \alpha_k |p|_k + \beta p \right) \ll (\log x)^3 x^{1-c_1 \tau_q(\alpha_1, \dots, \alpha_{q-1})}$$

avec

$$\tau_q(\alpha_1, \dots, \alpha_{q-1}) = \|(q-1)\alpha_1\|^2 + \sum_{2 \leq k < q} \|\alpha_k - k\alpha_1\|^2.$$

Démonstration. Posons $g = \sum_{1 \leq k < q} \alpha_k |\cdot|_k$. D'après le théorème A nous avons

$$\begin{aligned} \sum_{n \leq x} \Lambda(n) e \left(\sum_{1 \leq k < q} \alpha_k |n|_k + \beta \right) &\ll (\log x)^4 x^{1-\frac{c_0}{2}(\sigma_q(g) + \|(q-1)\alpha_1\|^2)}. \\ &\ll (\log x)^4 x^{1-c_2(\sigma_q(g) + \|(q-1)\alpha_1\|^2)}, \end{aligned}$$

avec

$$c_2 = \min \left(\frac{c_0}{2}, \frac{1}{2} \left(\frac{1}{4} + \frac{q(q-1)}{8} \right)^{-1} \right).$$

Une intégration par parties standard donne

$$\begin{aligned} \sum_{p \leq x} e \left(\sum_{1 \leq k < q} \alpha_k |p|_k + \beta p \right) &\ll \frac{1}{\log x} \max_{t \leq x} \left| \sum_{n \leq t} \Lambda(n) e \left(\sum_{1 \leq k < q} \alpha_k |n|_k + \beta \right) \right| + \sqrt{x} \\ &\ll (\log x)^3 x^{1-c_2(\sigma_q(g) + \|(q-1)\alpha_1\|^2)} + \sqrt{x} \\ &\ll (\log x)^3 x^{1-c_2(\sigma_q(g) + \|(q-1)\alpha_1\|^2)}, \end{aligned}$$

où la dernière inégalité résulte de la définition de c_2 . Il nous reste à remarquer que d'après le lemme 4 de [10], nous avons

$$\sigma_q(g) \geq \frac{1}{(q-1)((q-1)^2 + 1)} \sum_{2 \leq k < q} \|\alpha_k - k\alpha_1\|^2.$$

Cela fournit la conclusion attendue avec $c_1 = c_2((q-1)((q-1)^2 + 1))^{-1}$. □

4. PREUVE DU THÉORÈME 1

Nous introduisons l'ensemble

$$\mathcal{H} = \{(t_1, \dots, t_{q-1}) \in \mathbb{Z}^{q-1} : \forall k \in \{1, \dots, q-1\}, 0 \leq t_k < m_k\}$$

ainsi que les deux sous-ensembles

$$\mathcal{H}_1 = \left\{ (t_1, \dots, t_{q-1}) \in \mathcal{H} : \frac{m_1}{d_m} \mid t_1 \text{ et } \forall k \in \{2, \dots, q-1\}, t_k = \frac{km_k t_1}{m_1} \pmod{m_k} \right\},$$

et $\mathcal{H}_2 = \mathcal{H} \setminus \mathcal{H}_1$. Notons que la condition $\frac{m_1}{d_{\mathbf{m}}} \mid t_1$ entraîne que le nombre $\frac{km_k t_1}{m_1}$ est entier pour tout $k \in \{2, \dots, q-1\}$. Nous avons

$$\begin{aligned} & \text{card} \left\{ p \leq x : \forall k \in \{1, \dots, q-1\}, |p|_k \equiv \ell_k \pmod{m_k} \right\} \\ &= \frac{1}{m_1 \dots m_{q-1}} \sum_{p \leq x} \sum_{(t_1, \dots, t_{q-1}) \in \mathcal{H}} e \left(\sum_{1 \leq k < q} \frac{|p|_k - \ell_k}{m_k} t_k \right) \\ &= \frac{S_1}{m_1 \dots m_{q-1}} + O(S_2), \end{aligned}$$

avec

$$S_1 = \sum_{p \leq x} \sum_{(t_1, \dots, t_{q-1}) \in \mathcal{H}_1} e \left(\sum_{1 \leq k < q} \frac{|p|_k - \ell_k}{m_k} t_k \right)$$

et

$$S_2 = \max_{(t_1, \dots, t_{q-1}) \in \mathcal{H}_2} \left| \sum_{p \leq x} e \left(\sum_{1 \leq k < q} |p|_k \frac{t_k}{m_k} \right) \right|.$$

Commençons par traiter S_1 . Pour chaque valeur de $k \in \{2, \dots, q-1\}$, la sommation sur t_k le long de \mathcal{H}_1 est réduite à un seul terme correspondant à l'unique nombre entier t tel que $0 \leq t < m_k$ et $t \equiv km_k t_1 / m_1 \pmod{m_k}$. En effectuant le changement de variables $t_1 = rm_1 / d_{\mathbf{m}}$, nous obtenons ainsi

$$\begin{aligned} S_1 &= \sum_{p \leq x} \sum_{0 \leq r < d_{\mathbf{m}}} e \left(\sum_{1 \leq k < q} (|p|_k - \ell_k) \frac{kr}{d_{\mathbf{m}}} \right) = \sum_{p \leq x} \sum_{0 \leq r < d_{\mathbf{m}}} e \left(\frac{r}{d_{\mathbf{m}}} (s_q(p) - v_{\ell}) \right) \\ &= \sum_{p \leq x} \sum_{0 \leq r < d_{\mathbf{m}}} e \left(\frac{r}{d_{\mathbf{m}}} (p - v_{\ell}) \right) = d_{\mathbf{m}} \pi(x, v_{\ell}, d_{\mathbf{m}}). \end{aligned}$$

Pour majorer S_2 et conclure la démonstration, nous allons établir pour tout $(t_1, \dots, t_{q-1}) \in \mathcal{H}_2$ la majoration

$$(16) \quad \sum_{p \leq x} e \left(\sum_{1 \leq k < q} |p|_k \frac{t_k}{m_k} \right) \ll (\log x)^3 x^{1-c_1/\|\mathbf{m}\|_{\infty}^4}.$$

Compte-tenu de la proposition 1, il suffit pour cela de montrer la minoration

$$(17) \quad \tau_q \left(\frac{t_1}{m_1}, \dots, \frac{t_{q-1}}{m_{q-1}} \right) \geq \frac{1}{\|\mathbf{m}\|_{\infty}^4}.$$

Soit $(t_1, \dots, t_{q-1}) \in \mathcal{H}_2$. S'il existe $k \in \{2, \dots, q-1\}$ tel que $t_k \neq \frac{km_k t_1}{m_1} \pmod{m_k}$, alors $m_1 m_k$ ne divise pas $t_k m_1 - km_k t_1$ et donc

$$\tau_q \left(\frac{t_1}{m_1}, \dots, \frac{t_{q-1}}{m_{q-1}} \right) \geq \left\| \frac{t_k}{m_k} - k \frac{t_1}{m_1} \right\|^2 = \left\| \frac{t_k m_1 - km_k t_1}{m_1 m_k} \right\|^2 \geq \frac{1}{(m_1 m_k)^2} \geq \frac{1}{\|\mathbf{m}\|_{\infty}^4}.$$

Supposons à présent que pour tout $2 \leq k < q$, $t_k = km_k t_1 / m_1 \pmod{m_k}$ et que $\frac{m_1}{d_{\mathbf{m}}} \nmid t_1$. En particulier pour toute valeur de k , le nombre $km_k t_1 / m_1$ est entier. Supposons par l'absurde que $\frac{m_1}{\text{pgcd}(q-1, m_1)} \mid t_1$. Il existe donc $0 \leq s < \text{pgcd}(q-1, m_1)$ tel que

$$(18) \quad t_1 = \frac{sm_1}{\text{pgcd}(q-1, m_1)}$$

et donc pour tout $2 \leq k < q$, $\text{pgcd}(q-1, m_1) \mid skm_k$. Posons $d'_m = \text{pgcd}(m_1, 2m_2, \dots, (q-1)m_{q-1})$. D'après le théorème de Bézout, il existe $(u_2, \dots, u_{q-1}) \in \mathbb{Z}^{q-2}$ tels que

$$\sum_{k=2}^{q-1} u_k m_k = d'_m.$$

En multipliant cette égalité par s , nous obtenons que $\text{pgcd}(q-1, m_1)$ divise sd'_m , et une application du lemme de Gauss permet d'en déduire que $\frac{\text{pgcd}(q-1, m_1)}{d_m}$ divise s . Compte tenu de (18), cela entraîne que m_1/d_m divise t_1 , une contradiction. Nous avons donc $\frac{m_1}{\text{pgcd}(q-1, m_1)} \nmid t_1$. Nous en déduisons la minoration

$$\begin{aligned} \tau_q\left(\frac{t_1}{m_1}, \dots, \frac{t_{q-1}}{m_{q-1}}\right) &\geq \left\| (q-1) \frac{t_1}{m_1} \right\|^2 = \left\| \frac{q-1}{\text{pgcd}(q-1, m_1)} \cdot \frac{t_1}{\frac{m_1}{\text{pgcd}(q-1, m_1)}} \right\|^2 \\ &\geq \left(\frac{\text{pgcd}(q-1, m_1)}{m_1} \right)^2 \geq \frac{1}{m_1^2} \geq \frac{1}{\|\mathbf{m}\|_\infty^2}, \end{aligned}$$

où la deuxième inégalité vient du fait que pour tout $(a, b, c) \in (\mathbb{Z} \setminus \{0\})^3$ tels que $(a, c) = 1$ et $c \nmid b$, on a $\|ab/c\| \geq 1/c$. Nous avons bien établi la minoration (17) pour tout $(t_1, \dots, t_{q-1}) \in \mathbb{Z}^{q-1}$.

5. DÉMONSTRATION DU THÉORÈME 2

Soit $r \in \{1, \dots, q-1\}$ et $\mathbf{k} = (k_1, \dots, k_r) \in \{1, \dots, q-1\}^r$. Nous posons pour tout $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r) \in \mathbb{R}^r$,

$$S(\boldsymbol{\alpha}, \mathbf{k}, x) = \sum_{p \leq x} e\left(\sum_{i=1}^r \alpha_i |p|_{k_i}\right)$$

et pour tous $b \in \mathbb{Z}$ et $d \in \mathbb{N}^*$,

$$S_{b,d}(x; \boldsymbol{\alpha}, \mathbf{k}) = \sum_{\substack{p \leq x \\ p \equiv b \pmod{d}}} e\left(\sum_{i=1}^r \alpha_i |p|_{k_i}\right).$$

Nous commençons par le résultat suivant.

Lemme 1. *Soit $r \in \mathbb{N}^*$ tel que $1 \leq r \leq q-1$, $\mathbf{k} = (k_1, \dots, k_r) \in \{1, \dots, q-1\}^r$ tel que $k_1 < \dots < k_r$. Il existe $c = c(q, k_1, \dots, k_r) > 0$ tel que l'on a pour tous $x \geq 2$, $0 < \xi < 1/2$ et $\mathbf{b} = (b_1, \dots, b_r) \in \mathbb{N}^r$,*

$$(19) \quad \begin{aligned} &\text{card}\{p \leq x : |p|_{k_1} = b_1, \dots, |p|_{k_r} = b_r\} \\ &= \delta_{\mathbf{k}} \int_{\left[-\frac{\xi}{2(q-1)}, \frac{\xi}{2(q-1)}\right] \times [-\xi, \xi]^{r-1}} S_{\mathbf{k} \cdot \mathbf{b}, \delta_{\mathbf{k}}}(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} + O\left((\log x)^3 x^{1-c\xi^2/4(q-1)^2}\right), \end{aligned}$$

où $\delta_{\mathbf{k}}$ est défini en (8). La constante implicite ne dépend que de q .

Démonstration. Notons $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ et commençons par remarquer que

$$\text{card}\{p \leq x : |p|_{k_1} = b_1, \dots, |p|_{k_r} = b_r\} = \int_{\mathbb{T}^r} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha}.$$

Nous distinguons deux cas.

Premier cas : $k_1 > 1$

On a alors $\delta_{\mathbf{k}} = \text{pgcd}(k'_1, \dots, k'_s, q-1) = 1$. De plus d'après la proposition 1, on a

$$S(x; \boldsymbol{\alpha}, \mathbf{k}) \ll (\log x)^3 x^{1-c_1\mu(\alpha_1, \dots, \alpha_r)}$$

avec

$$\mu(\alpha_1, \dots, \alpha_r) = \sum_{1 \leq j \leq r} \|\alpha_j\|^2.$$

On a

$$\int_{\mathbb{T}^r} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} = \int_{H_1} + \int_{H_2}$$

avec

$$H_1 = \left[-\frac{\xi}{2(q-1)}, \frac{\xi}{2(q-1)}\right] \times [-\xi, \xi]^{r-1} \quad \text{et} \quad H_2 = \mathbb{T}^r \setminus H_1.$$

Si $\boldsymbol{\alpha} \in H_2$, alors il existe $j \in \{1, \dots, r\}$ tel que $\|\alpha_j\| \geq \frac{\xi}{2(q-1)}$, et donc

$$\int_{H_2} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \ll (\log x)^3 x^{1-c_1\xi^2/4(q-1)^2},$$

ce qui donne bien (19) puisque $\delta_{\mathbf{k}} = 1$ et donc $S(x; \boldsymbol{\alpha}, \mathbf{k}) = S_{\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}}(x; \boldsymbol{\alpha}, \mathbf{k})$.

Deuxième cas : $k_1 = 1$

Nous effectuons la décomposition

$$\int_{\mathbb{T}^r} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} = \int_{H_1} + \int_{H_2}$$

avec

$$H_1 = \bigcup_{\ell=0}^{\delta_{\mathbf{k}}-1} \left(\left[\frac{\ell}{\delta_{\mathbf{k}}} - \frac{\xi}{2(q-1)}, \frac{\ell}{\delta_{\mathbf{k}}} + \frac{\xi}{2(q-1)} \right] \times \prod_{j=2}^r \left[\frac{k_j \ell}{\delta_{\mathbf{k}}} - \xi, \frac{k_j \ell}{\delta_{\mathbf{k}}} + \xi \right] \right),$$

et $H_2 = \mathbb{T}^r \setminus H_1$. Notons que dans la définition de H_1 , la réunion $\bigcup_{\ell=0}^{\delta_{\mathbf{k}}-1}$ est disjointe puisque $\frac{\xi}{2(q-1)} < \frac{1}{2\delta_{\mathbf{k}}}$. Nous avons par conséquent

$$\begin{aligned} & \int_{H_1} \sum_{p \leq x} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\ &= \sum_{\ell=0}^{\delta_{\mathbf{k}}-1} \int_{\left[\frac{\ell}{\delta_{\mathbf{k}}} - \frac{\xi}{2(q-1)}, \frac{\ell}{\delta_{\mathbf{k}}} + \frac{\xi}{2(q-1)} \right] \times \prod_{j=2}^r \left[\frac{k_j \ell}{\delta_{\mathbf{k}}} - \xi, \frac{k_j \ell}{\delta_{\mathbf{k}}} + \xi \right]} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha}. \end{aligned}$$

Pour tout $\ell \in \{0, \dots, \delta_{\mathbf{k}} - 1\}$, on effectue dans l'intégrale

$$\int_{\left[\frac{\ell}{\delta_{\mathbf{k}}} - \frac{\xi}{2(q-1)}, \frac{\ell}{\delta_{\mathbf{k}}} + \frac{\xi}{2(q-1)} \right] \times \prod_{j=2}^r \left[\frac{k_j \ell}{\delta_{\mathbf{k}}} - \xi, \frac{k_j \ell}{\delta_{\mathbf{k}}} + \xi \right]}$$

le changement de variables $\alpha_1 = \alpha'_1 + \frac{\ell}{\delta_{\mathbf{k}}}$ et $\alpha_j = \alpha'_j + \frac{k_j \ell}{\delta_{\mathbf{k}}}$ pour tout $j \in \{2, \dots, r\}$. Cela fournit

$$\begin{aligned} & \int_{H_1} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\ &= \int_{\left[-\frac{\xi}{2(q-1)}, \frac{\xi}{2(q-1)} \right] \times [-\xi, \xi]^{r-1}} \sum_{p \leq x} e\left(\sum_{j=1}^r \alpha_j |p|_{k_j} \right) \sum_{\ell=0}^{\delta_{\mathbf{k}}-1} e\left(\frac{\ell \sum_{j=1}^r k_j (|p|_{k_j} - b_j)}{\delta_{\mathbf{k}}} \right) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \end{aligned}$$

Or, compte-tenu du fait que $\delta_{\mathbf{k}} = \text{pgcd}(k'_1, \dots, k'_s, q-1)$ et de la relation $s_q(n) \equiv n \pmod{q-1}$, nous avons pour tout $n \in \mathbb{N}$,

$$\sum_{j=1}^r k_j |n|_{k_j} \equiv \sum_{j=1}^r k_j |n|_{k_j} + \sum_{i=1}^s k'_i |n|_{k'_i} \equiv s_q(n) \equiv n \pmod{\delta_{\mathbf{k}}}.$$

Nous en déduisons

$$\begin{aligned} & \int_{H_1} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\ &= \int_{\left[-\frac{\xi}{2(q-1)}, \frac{\xi}{2(q-1)}\right] \times [-\xi, \xi]^{r-1}} \sum_{p \leq x} e\left(\sum_{j=1}^r \alpha_j |p|_{k_j}\right) \sum_{\ell=0}^{\delta_{\mathbf{k}}-1} e\left(\frac{\ell(p - \mathbf{b} \cdot \mathbf{k})}{\delta_{\mathbf{k}}}\right) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\ &= \delta_{\mathbf{k}} \int_{\left[-\frac{\xi}{2(q-1)}, \frac{\xi}{2(q-1)}\right] \times [-\xi, \xi]^{r-1}} S_{\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}}(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha}. \end{aligned}$$

Il reste à majorer $\int_{H_2} S(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha}$. On a d'après la proposition 1

$$S(x; \boldsymbol{\alpha}, \mathbf{k}) \ll (\log x)^3 x^{1-c_1 \mu(\boldsymbol{\alpha})},$$

avec

$$\mu(\boldsymbol{\alpha}) = \|(q-1)\alpha_1\|^2 + \sum_{2 \leq j \leq r} \|\alpha_j - k_j \alpha_1\|^2 + \sum_{1 \leq j \leq s} \|k'_j \alpha_1\|^2.$$

Pour conclure, il suffit donc de montrer qu'il existe $c > 0$ tel que pour tout $\boldsymbol{\alpha} \in H_2$,

$$(20) \quad \mu(\boldsymbol{\alpha}) \geq c \frac{\xi^2}{4(q-1)^2}.$$

Soit donc $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r) \in H_2$. Le lemme 3 de [10] stipule que l'on a pour tous $n \geq 2$, $(v_1, \dots, v_n) \in \mathbb{Z}^n \setminus \{0, \dots, 0\}$ et $\alpha \in \mathbb{R}$,

$$\sum_{k=1}^n \|v_k \alpha\|^2 \geq \left(\sum_{j=1}^n v_j^2\right)^{-1} \text{pgcd}(v_1, \dots, v_n)^2 \|\text{pgcd}(v_1, \dots, v_n) \alpha\|^2.$$

Nous en déduisons que l'on a, si $s \geq 1$,

$$\mu(\boldsymbol{\alpha}) \geq \|(q-1)\alpha_1\|^2 + \sum_{1 \leq j \leq s} \|k'_j \alpha_1\|^2 \geq c \|\text{pgcd}(q-1, k'_1, \dots, k'_s) \alpha_1\|^2 = c \|\delta_{\mathbf{k}} \alpha_1\|^2,$$

avec $c \in]0, 1]$ qui dépend de k'_1, \dots, k'_s et $q-1$. Si $s = 0$, alors $\delta_{\mathbf{k}} = q-1$ et on a donc encore $\mu(\boldsymbol{\alpha}) \geq c \|\delta_{\mathbf{k}} \alpha_1\|^2$. À présent distinguons deux sous-cas. Si pour tout $\ell \in \{0, \dots, \delta_{\mathbf{k}} - 1\}$, on a

$$\alpha_1 \notin \left[\frac{\ell}{\delta_{\mathbf{k}}} - \frac{\xi}{2(q-1)}, \frac{\ell}{\delta_{\mathbf{k}}} + \frac{\xi}{2(q-1)} \right],$$

alors on a $\|\delta_{\mathbf{k}} \alpha_1\| \geq \frac{\delta_{\mathbf{k}} \xi}{2(q-1)} \geq \frac{\xi}{2(q-1)}$, et par conséquent $\mu(\boldsymbol{\alpha}) \geq \frac{c \xi^2}{4(q-1)^2}$. Si en revanche, il existe $\ell \in \{0, \dots, d-1\}$ tel que

$$\alpha_1 \in \left[\frac{\ell}{\delta_{\mathbf{k}}} - \frac{\xi}{2(q-1)}, \frac{\ell}{\delta_{\mathbf{k}}} + \frac{\xi}{2(q-1)} \right],$$

alors il existe $j \in \{2, \dots, r-1\}$ tel que

$$(21) \quad \alpha_j \notin \left[\frac{k_j \ell}{\delta_{\mathbf{k}}} - \xi, \frac{k_j \ell}{\delta_{\mathbf{k}}} + \xi \right]$$

puisque $\alpha \in H_2$. On a de plus

$$(22) \quad k_j \alpha_1 \in \left[\frac{k_j \ell}{\delta_{\mathbf{k}}} - \frac{k_j \xi}{2(q-1)}, \frac{k_j \ell}{\delta_{\mathbf{k}}} + \frac{k_j \xi}{2(q-1)} \right] \subseteq \left[\frac{k_j \ell}{\delta_{\mathbf{k}}} - \frac{\xi}{2}, \frac{k_j \ell}{\delta_{\mathbf{k}}} + \frac{\xi}{2} \right],$$

car $q-1 \geq k_j$. Nous déduisons de (21) et (22) que $\|\alpha_j - k_j \alpha_1\| \geq \xi/2$, et donc $\mu(\alpha) \geq \xi^2/4$. Nous avons bien établi (19) dans tous les cas. \square

Remarquons à ce stade que pour démontrer le théorème 2, on peut supposer que x est suffisamment grand, quitte à augmenter la valeur des constantes implicites dans (7). On peut également supposer que $(\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}) = 1$ puisque la formule (7) est triviale dans le cas contraire. Appliquons maintenant (19) avec $\xi = (\log x)^{\eta-1/2}$, où $\eta > 0$ est un nombre réel qui sera fixé ultérieurement. En posant

$$I = [-\xi, \xi] \quad \text{et} \quad I' = \left[-\frac{\xi}{2(q-1)}, \frac{\xi}{2(q-1)} \right],$$

nous avons donc

$$\begin{aligned} & \text{card}\{p \leq x : |p|_{k_1} = b_1, \dots, |p|_{k_r} = b_r\} \\ &= \delta_{\mathbf{k}} \int_{I' \times I^{r-1}} S_{\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}}(x; \alpha, \mathbf{k}) e(-\alpha \cdot \mathbf{b}) d\alpha + O\left(\frac{\pi(x)}{(\log x)^{\frac{r+1}{2}}}\right). \end{aligned}$$

Pour obtenir (7), il nous suffit donc d'établir pour x suffisamment grand la formule

$$(23) \quad \int_{I' \times I^{r-1}} S_{\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}}(x; \alpha, \mathbf{k}) e(-\alpha \cdot \mathbf{b}) d\alpha = C_{r,q} \frac{\pi(x; \mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}})}{(\log_q x)^{r/2}} e^{-\frac{1}{2}R(u_x, \mathbf{b})} + O\left(\frac{\pi(x)}{(\log x)^{\frac{r+1}{2}-\varepsilon}}\right).$$

Pour cela nous employons une généralisation de la proposition 2.2 de [3]. Elle se démontre de la même manière mais nous donnons les détails de la preuve par souci de complétude au paragraphe 6.

Proposition 2. *Soit η, ν deux nombres réels tels que $0 < 2\eta < \nu < 1/3$. On a uniformément pour tous $x \geq x_0(\nu, \eta)$, $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{q-1}) \in \mathbb{R}^q$ avec $\alpha_0 = 0$ et tel que $\|\alpha\|_{\infty} \leq (\log_q x)^{\eta-1/2}$, $d \in \mathbb{N}^*$ et $b \in \mathbb{Z}$ tels que $\text{pgcd}(b, d) = 1$,*

$$(24) \quad \sum_{\substack{p \leq x \\ p \equiv b \pmod{d}}} e\left(\sum_{k=0}^{q-1} \alpha_k |p|_k\right) = \pi(x; b, d) e(m(\alpha) \log_q x) e^{-2\pi^2 \mathcal{Q}(\alpha) \log_q x} \left(1 + O(\|\alpha\|_{\infty}^3 \log x)\right) \\ + O(\pi(x) \|\alpha\|_{\infty} (\log_q x)^{\nu}),$$

avec

$$m(\alpha) = \frac{1}{q} \sum_{k=0}^{q-1} \alpha_k \quad \text{et} \quad \mathcal{Q}(\alpha) = \frac{1}{q} \sum_{k=0}^{q-1} \alpha_k^2 - m(\alpha)^2 = \frac{1}{2q} \sum_{0 \leq k, k' < q} (\alpha_k - \alpha_{k'})^2.$$

La constante implicite dans (24) ne dépend que de η, ν et q .

Appliquons la Proposition 2 au vecteur $\tilde{\alpha} = (0, \tilde{\alpha}_1, \dots, \tilde{\alpha}_{q-1}) \in \mathbb{R}^q$ avec $\tilde{\alpha}_{k_j} = \alpha_j$, $\tilde{\alpha}_{k'_j} = 0$ et avec les nombres entiers $d = \delta_{\mathbf{k}}$ et $b = \mathbf{b} \cdot \mathbf{k}$. Cela donne l'estimation

$$(25) \quad \int_{I' \times I^{r-1}} S_{\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}}(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\ = \pi(x; \mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}) \int_{I' \times I^{r-1}} e\left(\sum_{j=1}^r \alpha_j \left(\frac{1}{q} \log_q x - b_j\right)\right) e^{-2\pi^2 Q(\boldsymbol{\alpha}) \log_q x} \left(1 + O(\|\boldsymbol{\alpha}\|_{\infty}^3 \log x)\right) \\ + O(\|\boldsymbol{\alpha}\|_{\infty} (\log_q x)^{\nu}) d\boldsymbol{\alpha},$$

avec

$$Q(\boldsymbol{\alpha}) = \frac{1}{q} \sum_{j=1}^r \alpha_j^2 - \left(\frac{1}{q} \sum_{j=1}^r \alpha_j\right)^2.$$

Notons que puisque $\left(\sum_{j=1}^r \alpha_j\right)^2 \leq r \sum_{j=1}^r \alpha_j^2$, on a

$$Q(\boldsymbol{\alpha}) \geq \frac{1}{q} \left(1 - \frac{r}{q}\right) \sum_{1 \leq j \leq r} \alpha_j^2 \geq \frac{1}{q^2} \sum_{1 \leq j \leq r} \alpha_j^2.$$

En conséquence,

$$\int_{\mathbb{R}^r \setminus (I' \times I^{r-1})} e^{-2\pi^2 Q(\boldsymbol{\alpha}) \log_q x} d\boldsymbol{\alpha} \\ \leq \sum_{j=1}^r \int_{\{\boldsymbol{\alpha} \in \mathbb{R}^r : |\alpha_j| \geq (\log x)^{\eta-1/2}/(2(q-1))\}} e^{-\frac{2\pi^2}{q^2} \log_q x \sum_{j=1}^r \alpha_j^2} d\boldsymbol{\alpha} \\ = r \int_{|t| \geq (\log x)^{\eta-1/2}/(2(q-1))} e^{-\frac{2\pi^2}{q^2} t^2 \log_q x} dt \cdot \left(\int_{\mathbb{R}} e^{-\frac{2\pi^2}{q^2} t^2 \log_q x} dt\right)^{r-1} \\ = r \left(\frac{q}{\sqrt{2\pi \log_q x}}\right)^{r-1} \int_{|t| \geq (\log x)^{\eta-1/2}/(2(q-1))} e^{-\frac{2\pi^2}{q^2} t^2 \log_q x} dt.$$

Or on a pour tout $v \geq 0$,

$$\int_v^{+\infty} e^{-t^2} dt \leq \frac{e^{-v^2}}{v+1}$$

et donc

$$\int_{\mathbb{R}^r \setminus (I' \times I^{r-1})} e^{-2\pi^2 Q(\boldsymbol{\alpha}) \log_q x} d\boldsymbol{\alpha} \leq r \left(\frac{q}{\sqrt{2\pi \log_q x}}\right)^r \cdot \frac{e^{-d_1 (\log x)^{2\eta}}}{1 + d_2 (\log x)^{\eta}},$$

avec $d_1, d_2 > 0$ qui dépendent de q . Remarquons par ailleurs que pour tout $\gamma > 0$,

$$\int_{I' \times I^{r-1}} \|\boldsymbol{\alpha}\|_{\infty}^{\gamma} d\boldsymbol{\alpha} \leq (\log x)^{(\eta-1/2)(r+\gamma)}.$$

Il en résulte que sous l'hypothèse $\eta < \nu/2$, on a

$$\begin{aligned}
(26) \quad & \int_{I' \times I^{r-1}} S_{\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}}(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\
& = \pi(x; \mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}) \int_{\mathbb{R}^r} e\left(\sum_{j=1}^r \alpha_j \left(\frac{\log_q x}{q} - b_j\right)\right) e^{-2\pi^2 Q(\boldsymbol{\alpha}) \log_q x} d\boldsymbol{\alpha} \\
& \quad + O\left(\frac{\pi(x)}{(\log_q x)^{\frac{r+1}{2} - (\nu + (r+1)\eta)}}\right).
\end{aligned}$$

Nous effectuons le changement de variables $\boldsymbol{\alpha}' = 2\pi\boldsymbol{\alpha}\sqrt{\log_q x}$ dans l'intégrale figurant en (26), et cela donne

$$\begin{aligned}
& \int_{I' \times I^{r-1}} S_{\mathbf{b} \cdot \mathbf{k}, d}(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} \\
& = \frac{\pi(x; \mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}})}{(\log_q x)^{r/2} (2\pi)^r} \int_{\mathbb{R}^r} \exp\left(i \sum_{j=1}^r \alpha_j \frac{\frac{1}{q} \log_q x - b_j}{\sqrt{\log_q x}} - \frac{1}{2} Q(\boldsymbol{\alpha})\right) d\boldsymbol{\alpha} + O\left(\frac{\pi(x)}{(\log_q x)^{\frac{r+1}{2} - (\nu + (r+1)\eta)}}\right).
\end{aligned}$$

Nous employons alors le résultat suivant qui est standard et dont on pourra trouver une démonstration dans, par exemple, [16] p. 15.

Lemme 2. Soit $n \in \mathbb{N}^*$, Q une forme quadratique définie positive sur \mathbb{R}^n et A sa matrice dans la base canonique, $\mathbf{u} \in \mathbb{R}^n$. On a

$$\int_{\mathbb{R}^n} \exp\left(-\frac{1}{2} Q(\mathbf{x}) + i\mathbf{u} \cdot \mathbf{x}\right) d\mathbf{x} = \sqrt{\frac{(2\pi)^n}{\det A}} \exp\left(-\frac{1}{2} R(\mathbf{u})\right),$$

où R est la forme quadratique dont la matrice dans la base canonique est A^{-1} .

Dans notre cas, la matrice associée à la forme quadratique Q dans la base canonique de \mathbb{R}^r est

$$A = \frac{1}{q^2} \begin{pmatrix} q-1 & -1 & \dots & -1 \\ -1 & \ddots & \ddots & -1 \\ \vdots & \ddots & \ddots & -1 \\ -1 & \dots & -1 & q-1 \end{pmatrix}.$$

On a

$$\det(A) = \frac{q-r}{q^{r+1}} \quad \text{et} \quad A^{-1} = \begin{pmatrix} \frac{q(q+1-r)}{q-r} & \frac{q}{q-r} & \dots & \frac{q}{q-r} \\ \frac{q}{q-r} & \ddots & \ddots & \frac{q}{q-r} \\ \vdots & \ddots & \ddots & \frac{q}{q-r} \\ \frac{q}{q-r} & \dots & \frac{q}{q-r} & \frac{q(q+1-r)}{q-r} \end{pmatrix}.$$

La forme quadratique R associée à A^{-1} dans la base canonique est donnée par

$$\begin{aligned}
R(\boldsymbol{\alpha}) & = \frac{q(q+1-r)}{q-r} \sum_{i=1}^r \alpha_i^2 + \frac{2q}{q-r} \sum_{1 \leq i < j \leq r} \alpha_i \alpha_j \\
& = q \sum_{i=1}^r \alpha_i^2 + \frac{q}{q-r} \left(\sum_{i=1}^r \alpha_i\right)^2.
\end{aligned}$$

Nous obtenons donc

$$\int_{I^r \times I^{r-1}} S_{\mathbf{b}, \mathbf{k}, \delta_{\mathbf{k}}}(x; \boldsymbol{\alpha}, \mathbf{k}) e(-\boldsymbol{\alpha} \cdot \mathbf{b}) d\boldsymbol{\alpha} = C_{r,q} \frac{\pi(x; \mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}})}{(\log_q x)^{r/2}} e^{-\frac{1}{2}R(u_x, \mathbf{b})} + O\left(\frac{\pi(x)}{(\log_q x)^{\frac{r+1}{2} - (\nu + (r+1)\eta)}\right).$$

Pour en déduire (23) et ainsi conclure, il suffit de poser pour $0 < \varepsilon < 1/2$, $\nu = \frac{4\varepsilon}{5+r}$ et $\eta = \frac{\varepsilon}{5+r}$ qui satisfont bien à $0 < 2\eta < \nu < 1/3$. Pour achever la preuve du théorème 2, il reste à démontrer la proposition 2.

6. DÉMONSTRATION DE LA PROPOSITION 2

Ce qui suit est une adaptation de la démonstration de la proposition 2.2 de [3], nous adoptons ainsi des notations similaires et omettons certains détails par moments. Nous posons

$$L = L(x) = \log_q x.$$

Pour $\boldsymbol{\alpha} \in \mathbb{R}^q$, nous posons

$$T_{\boldsymbol{\alpha}}(n) = \sum_{k=0}^{q-1} \alpha_k |n|_k$$

et remarquons que pour tous $x \geq 2$ et $1 \leq n \leq x$,

$$T_{\boldsymbol{\alpha}}(n) = \sum_{0 \leq j \leq L} \alpha_{\varepsilon_j(n)}.$$

Nous munissons l'ensemble $\Omega_x = \{p \leq x : p \equiv b \pmod{d}\}$ de la probabilité uniforme et considérons la variable aléatoire $X_{\boldsymbol{\alpha}} : \Omega_x \rightarrow \mathbb{C}$ définie par

$$X_{\boldsymbol{\alpha}} = \frac{T_{\boldsymbol{\alpha}} - Lm(\boldsymbol{\alpha})}{\sqrt{L}}.$$

Étant donné un nombre réel $0 < \nu < 1$, nous posons pour tous $x \geq 2$ et $1 \leq n \leq x$,

$$T_{\boldsymbol{\alpha}, \nu}(n) = \sum_{L^{\nu} \leq j \leq L - L^{\nu}} \alpha_{\varepsilon_j(n)}$$

Nous employons également la notation

$$L' = \text{card}\{j \in \mathbb{N} : L^{\nu} \leq j \leq L - L^{\nu}\}$$

et introduisons la variable aléatoire $X_{\boldsymbol{\alpha}, \nu} : \Omega_x \rightarrow \mathbb{C}$

$$X_{\boldsymbol{\alpha}, \nu} = \frac{T_{\boldsymbol{\alpha}, \nu} - L'm(\boldsymbol{\alpha})}{\sqrt{L'}}.$$

Nous posons également

$$\begin{aligned} \varphi_1(\boldsymbol{\alpha}) &= \mathbb{E}(e^{iX_{\boldsymbol{\alpha}}}) = \frac{1}{\pi(x; b, d)} \sum_{\substack{p \leq x \\ p \equiv b \pmod{d}}} e^{i \frac{T_{\boldsymbol{\alpha}}(p) - Lm(\boldsymbol{\alpha})}{\sqrt{L}}}, \\ \varphi_2(\boldsymbol{\alpha}) &= \mathbb{E}(e^{iX_{\boldsymbol{\alpha}, \nu}}) = \frac{1}{\pi(x; b, d)} \sum_{\substack{p \leq x \\ p \equiv b \pmod{d}}} e^{i \frac{T_{\boldsymbol{\alpha}, \nu}(p) - L'm(\boldsymbol{\alpha})}{\sqrt{L'}}}. \end{aligned}$$

Lemme 3. Pour tout $\alpha \in \mathbb{R}^q$, on a

$$\varphi_1(\alpha) = \varphi_2(\alpha) + O(\|\alpha\|_\infty L^{\nu-1/2}).$$

Démonstration. C'est une conséquence rapide de l'inégalité $|e^{it} - e^{is}| \leq |s - t|$ valable pour tout $(s, t) \in \mathbb{R}^2$, et des estimations $L - L' \ll L^\nu$ et $L^{-1/2} - L'^{-1/2} \ll L^{\nu-3/2}$. \square

Nous introduisons à présent une suite $(Z_j)_{L^\nu \leq j \leq L-L^\nu}$ de variables aléatoires indépendantes définies sur le même espace de probabilité $(\Omega, \mathcal{A}, \mathbb{P})$, toutes de loi uniforme sur $\{0, \dots, q-1\}$ et nous posons successivement

$$\bar{T}_{\alpha, \nu} = \sum_{L^\nu \leq j \leq L-L^\nu} \alpha_{Z_j}, \quad \bar{X}_{\alpha, \nu} = \frac{\bar{T}_{\alpha, \nu} - L' m(\alpha)}{\sqrt{L'}} \quad \text{et} \quad \varphi_3(\alpha) = \mathbb{E}(e^{i\bar{X}_{\alpha, \nu}}).$$

Lemme 4. Il existe une constante $c_3 = c_3(q) > 0$ telle que l'on a uniformément pour tous $\alpha \in \mathbb{R}^q$ et $1 \leq d \leq L'$,

$$(27) \quad \mathbb{E}(X_{\alpha, \nu}^d) = \mathbb{E}(\bar{X}_{\alpha, \nu}^d) + O((8qL^{\nu+1/2} \|\alpha\|_\infty)^d e^{-c_3 L^\nu}).$$

Démonstration. En développant les puissances d -ièmes, on obtient

$$(28) \quad \mathbb{E}(X_{\alpha, \nu}^d) - \mathbb{E}(\bar{X}_{\alpha, \nu}^d) = \sum_{L^\nu \leq j_1, \dots, j_d \leq L-L^\nu} \sum_{\ell_1, \dots, \ell_d \in \{0, \dots, q-1\}} \frac{\alpha_{\ell_1} - m(\alpha)}{\sqrt{L'}} \dots \frac{\alpha_{\ell_d} - m(\alpha)}{\sqrt{L'}} \Delta_{j_1, \dots, j_d}^{\ell_1, \dots, \ell_d}$$

avec

$$\begin{aligned} \Delta_{j_1, \dots, j_d}^{\ell_1, \dots, \ell_d} &= \mathbb{P}(\varepsilon_{j_1} = \ell_1, \dots, \varepsilon_{j_d} = \ell_d) - \mathbb{P}(Z_{j_1} = \ell_1, \dots, Z_{j_d} = \ell_d) \\ &= \frac{1}{\pi(x; b, d)} \text{card}\{p \leq x : p \equiv b \pmod{d}, \varepsilon_{j_1}(p) = \ell_1, \dots, \varepsilon_{j_d}(p) = \ell_d\} - \frac{1}{q^d}. \end{aligned}$$

D'après le lemme 4.5 de [3], il existe $c_3 > 0$ tel que l'on a uniformément pour $1 \leq d \leq L'$, $L^\nu \leq j_1 < \dots < j_d \leq L - L^\nu$ et $\ell_1, \dots, \ell_d \in \{0, \dots, q-1\}$,

$$\Delta_{j_1, \dots, j_d}^{\ell_1, \dots, \ell_d} \ll (4L^\nu)^d e^{-c_3 L^\nu}.$$

En insérant cette majoration dans (28), et en utilisant l'inégalité $|\alpha_\ell - m(\alpha)| \leq 2 \|\alpha\|_\infty$ pour tout $\ell \in \{0, \dots, q-1\}$, nous obtenons la majoration annoncée. \square

Lemme 5. Soit $0 < \nu < 1$ un nombre réel. On a pour tous $x \geq x_0(\nu)$, $w \in \mathbb{C}$ et $\alpha \in \mathbb{R}^q$ tels que $|w| \|\alpha\|_\infty \leq L^{1/6}$,

$$\mathbb{E}(e^{w\bar{X}_{\alpha, \nu}}) = e^{\frac{w^2}{2} \mathcal{Q}(\alpha)} \left(1 + O(L^{-1/2} |w|^3 \|\alpha\|_\infty^3) \right).$$

Démonstration. On a pour tout $z \in \mathbb{C}$,

$$\begin{aligned} \mathbb{E}(e^{z\bar{T}_{\alpha, \nu}}) &= \left(\frac{1}{q} \sum_{j=0}^{q-1} e^{z\alpha_j} \right)^{L'} \\ &= \exp \left(L' \left(zm(\alpha) + \frac{z^2}{2} \mathcal{Q}(\alpha) + O(|z|^3 \|\alpha\|_\infty^3) \right) \right) \\ &= e^{L'(zm(\alpha) + \frac{z^2}{2} \mathcal{Q}(\alpha))} \left(1 + O(L|z|^3 \|\alpha\|_\infty^3) \right). \end{aligned}$$

On pose alors $z = w/\sqrt{L'}$, ce qui donne bien le résultat annoncé. \square

Lemme 6. Soit $0 < \nu < 1$, $0 < 2\eta < \kappa < 1/3$ et D le plus grand nombre entier pair n'excédant pas L^κ . On a pour tous $x \geq x_0(\nu, \eta, \kappa)$, $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{q-1}) \in \mathbb{R}^q$ avec $\alpha_0 = 0$ et $\|\boldsymbol{\alpha}\|_\infty \leq L^\eta$,

$$\frac{\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^D)}{D!} \ll \|\boldsymbol{\alpha}\|_\infty e^{-c_4 L^\kappa},$$

avec $c_4 = \frac{2\kappa - \eta}{4} > 0$.

Démonstration. On peut supposer $\boldsymbol{\alpha} \neq (0, \dots, 0)$. D'après la formule intégrale de Cauchy on a pour tout $w_0 > 0$,

$$\frac{\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^D)}{D!} = \frac{1}{2i\pi} \int_{|w|=w_0} \mathbb{E}(e^{w\overline{X}_{\boldsymbol{\alpha}, \nu}}) \frac{dw}{w^{D+1}}.$$

Comme $\alpha_0 = 0$, on a $\mathcal{Q}(\boldsymbol{\alpha}) \geq \frac{1}{2q} \|\boldsymbol{\alpha}\|_\infty^2$, et on peut ainsi employer le lemme 5 avec $w = w_0 = \sqrt{D/\mathcal{Q}(\boldsymbol{\alpha})}$. Cela donne

$$\frac{\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^D)}{D!} = \frac{\mathcal{Q}(\boldsymbol{\alpha})^{D/2}}{D^{D/2} 2\pi} \int_{-\pi}^{\pi} e^{-\frac{D}{2} e^{i\theta} - iD\theta} \left(1 + O\left(\frac{D^{3/2}}{L^{1/2}}\right)\right) d\theta,$$

ce qui entraîne

$$\frac{\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^D)}{D!} \ll \frac{\mathcal{Q}(\boldsymbol{\alpha})^{D/2}}{D^{D/2}} \int_{-\pi}^{\pi} e^{\frac{D}{2} \cos(\theta)} d\theta \ll \frac{\|\boldsymbol{\alpha}\|_\infty^D e^{D/2}}{D^{D/2}},$$

où la dernière majoration résulte du fait que $\mathcal{Q}(\boldsymbol{\alpha}) \leq \|\boldsymbol{\alpha}\|_\infty^2$. Il suit

$$\begin{aligned} \frac{\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^D)}{D!} &\ll \|\boldsymbol{\alpha}\|_\infty \exp\left((D-1) \log(L^\eta) + \frac{D}{2} - \frac{D}{2} \log D\right) \\ &\ll \|\boldsymbol{\alpha}\|_\infty \exp\left(\left(\eta - \frac{\kappa}{2}\right) L^\kappa \log L + \frac{L^\kappa}{2}\right), \end{aligned}$$

d'où nous déduisons la majoration requise. \square

Lemme 7. Soit $0 < 2\eta < \nu < 1/3$ des nombres réels. Il existe $c > 0$ tel que l'on a uniformément pour tous $x \geq x_0(\nu, \eta)$ et $\boldsymbol{\alpha} = (0, \alpha_1, \dots, \alpha_{q-1}) \in \mathbb{R}^q$ tel que $\|\boldsymbol{\alpha}\|_\infty \leq L^\eta$,

$$\varphi_2(\boldsymbol{\alpha}) = \varphi_3(\boldsymbol{\alpha}) + O(\|\boldsymbol{\alpha}\|_\infty e^{-cL^\nu}).$$

Démonstration. Soit κ un nombre réel tel que $0 < 2\eta < \kappa < \nu$ et D le plus grand nombre entier pair n'excédant pas L^κ . En utilisant le développement de Taylor

$$e^{iu} = \sum_{0 \leq d < D} \frac{(iu)^d}{d!} + O\left(\frac{u^D}{D!}\right)$$

(valable uniformément pour tout $u \in \mathbb{R}$) et les lemmes 4 et 6 nous obtenons :

$$\begin{aligned} |\varphi_2(\boldsymbol{\alpha}) - \varphi_3(\boldsymbol{\alpha})| &\ll \max_{1 \leq d < D} |\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^d) - \mathbb{E}(X_{\boldsymbol{\alpha}, \nu}^d)| + \frac{\mathbb{E}(\overline{X}_{\boldsymbol{\alpha}, \nu}^D)}{D!} \\ &\ll \|\boldsymbol{\alpha}\|_\infty \left((8qL^{\nu+1/2+\eta})^{L^\kappa} e^{-c_3 L^\nu} + e^{-c_4 L^\nu} \right) \ll \|\boldsymbol{\alpha}\|_\infty e^{-c_5 L^\nu}, \end{aligned}$$

avec $c_5 = \min(c_3/2, c_4) > 0$. \square

Nous sommes maintenant en mesure d'achever la démonstration de la proposition 2. D'après les lemmes 3 et 7 on a

$$\varphi_1(\boldsymbol{\alpha}) = \varphi_3(\boldsymbol{\alpha}) + O(\|\boldsymbol{\alpha}\|_\infty L^{\nu-1/2}).$$

Le lemme 5 appliqué avec $w = i$ donne alors l'estimation asymptotique

$$\varphi_1(\boldsymbol{\alpha}) = e^{-\frac{1}{2}\mathcal{Q}(\boldsymbol{\alpha})} \left(1 + O(L^{-1/2} \|\boldsymbol{\alpha}\|_\infty^3) \right) + O(\|\boldsymbol{\alpha}\|_\infty L^{\nu-1/2}),$$

valable uniformément pour tout $\|\boldsymbol{\alpha}\|_\infty \leq L^\eta$. En effectuant le changement de variables $\boldsymbol{\alpha} = 2\pi\sqrt{L'}\boldsymbol{\alpha}'$, nous obtenons l'estimation (24).

7. DÉMONSTRATION DU THÉORÈME 3

Commençons par caractériser les nombres équilibrés d'un intervalle de la forme $[q^{m-1}, q^m[$ avec $m \in \mathbb{N}^*$. On pose

$$m = qt + r \quad (t \in \mathbb{N}, 1 \leq r \leq q).$$

Soit $n \in [q^{m-1}, q^m[$. On a l'équivalence (29)

$$n \in \mathcal{E}_q \iff \forall k \in \{0, \dots, q-1\}, |n|_k = t + v_k \text{ avec } v_0, \dots, v_{q-1} \in \{0, 1\} \text{ et } \sum_{0 \leq k < q} v_k = r.$$

Si l'on pose pour tout $k \in \{0, \dots, q-1\}$, $b_k = t + v_k$, avec les notations du théorème 2 la condition $(\mathbf{b} \cdot \mathbf{k}, \delta_{\mathbf{k}}) = 1$ s'écrit

$$\text{pgcd}\left(\frac{q(q-1)t}{2} + \sum_{1 \leq k < q} kv_k, q-1\right) = 1.$$

On remarque alors que

$$\text{pgcd}\left(\frac{q(q-1)t}{2} + \sum_{1 \leq k < q} kv_k, q-1\right) = \begin{cases} \text{pgcd}\left(\sum_{1 \leq k < q} kv_k, q-1\right) & \text{si } q \text{ ou } t \text{ est pair,} \\ \text{pgcd}\left(\frac{q-1}{2} + \sum_{1 \leq k < q} kv_k, q-1\right) & \text{sinon.} \end{cases}$$

Nous introduisons en conséquence les ensembles

$$F_{q,r,0} = \left\{ (v_0, \dots, v_{q-1}) \in \{0, 1\}^q : \sum_{0 \leq k < q} v_k = r, \text{pgcd}\left(\sum_{1 \leq k < q} kv_k, q-1\right) = 1 \right\},$$

$$F_{q,r,1} = \left\{ (v_0, \dots, v_{q-1}) \in \{0, 1\}^q : \sum_{0 \leq k < q} v_k = r, \text{pgcd}\left(\frac{q-1}{2} + \sum_{1 \leq k < q} kv_k, q-1\right) = 1 \right\}.$$

Posons à présent pour $t \geq 0$, $1 \leq r \leq q$ et $q^{qt+r-1} \leq x \leq q^{qt+r}$,

$$V_{t,r}(x) = \text{card}\{q^{qt+r-1} \leq p < x : p \in \mathcal{E}_q\},$$

et notons ℓ l'unique élément de $\{0, 1\}$ tel que $qt \equiv \ell \pmod{2}$. L'ensemble $V_{t,r}(x)$ contient au plus un nombre premier équilibré tel que

$$\text{pgcd}\left(\frac{q(q-1)t}{2} + \sum_{1 \leq k < q} kv_k, q-1\right) > 1.$$

D'après l'équivalence (29), on a pour tout $t \geq 1$ et $q^{qt+r-1} \leq x \leq q^{qt+r}$,

$$\begin{aligned} V_{t,r}(x) &= \sum_{(v_0, \dots, v_{q-1}) \in F_{q,r,\ell}} \sum_{\substack{q^{qt+r-1} \leq p < x \\ \forall k \geq 0, |p|_k = t + v_k}} 1 + O(1) = \sum_{(v_0, \dots, v_{q-1}) \in F_{q,r,\ell}} \sum_{\substack{q^{qt+r-1} \leq p < x \\ \forall k \geq 1, |p|_k = t + v_k}} 1 + O(1) \\ &= \sum_{(v_0, \dots, v_{q-1}) \in F_{q,r,\ell}} \sum_{\substack{p < x \\ \forall k \geq 1, |p|_k = t + v_k}} 1 - \sum_{(v_0, \dots, v_{q-1}) \in F_{q,r,\ell}} \sum_{\substack{p < q^{qt+r-1} \\ \forall k \geq 1, |p|_k = t + v_k}} 1 + O(1). \end{aligned}$$

On applique alors le théorème 2 et le théorème des nombres premiers en progression arithmétique sous la forme $\pi(x; a, m) = \frac{x}{\varphi(m) \log x} + O\left(\frac{x}{(\log x)^2}\right)$. On obtient

$$(30) \quad V_{t,r}(x) = C_q \operatorname{card}(F_{q,r,\ell}) \cdot \frac{x - q^{qt+r-1}}{(qt)^{(q+1)/2}} \left(1 + O((qt)^{-\frac{1}{2} + \varepsilon})\right),$$

avec

$$C_q = \frac{q-1}{\varphi(q-1) \log q} \cdot \frac{q^{q/2}}{(2\pi)^{(q-1)/2}}.$$

Nous sommes maintenant en mesure de démontrer le théorème 3. Pour $x \geq 1$, nous introduisons les uniques nombres entiers T et R tels que $T \geq 0$, $1 \leq R \leq q$ et

$$q^{qT+R-1} \leq x < q^{qT+R}.$$

On a

$$N_q(x) := N_q^{(1)}(x) + N_q^{(2)}(x) + N_q^{(3)}(x)$$

avec

$$N_q^{(1)}(x) = \sum_{\substack{p < q^{qT} \\ p \in \mathcal{E}_q}} 1, \quad N_q^{(2)}(x) = \sum_{\substack{q^{qT} \leq p < q^{qT+R-1} \\ p \in \mathcal{E}_q}} 1 \quad \text{et} \quad N_q^{(3)}(x) = \sum_{\substack{q^{qT+R-1} \leq p \leq x \\ p \in \mathcal{E}_q}} 1.$$

Premier cas : q est pair. Posons $y = \frac{1}{q} \log_q x$. On a

$$(31) \quad T = \lfloor y \rfloor \quad \text{et} \quad R = \lfloor q\{y\} \rfloor + 1.$$

On peut supposer $x \geq q^{2q}$ et donc $T \geq 2$. D'après (30), on a

$$\begin{aligned} N_q^{(1)}(x) &= \sum_{0 \leq t < T} \sum_{1 \leq r \leq q} V_{t,r}(q^{qt+r}) \\ &= (q-1)C_q \sum_{1 \leq r \leq q} \frac{q^{r-1}}{q^{(q+1)/2}} \operatorname{card}(F_{q,r,0}) \sum_{1 \leq t < T} \frac{q^{qt}}{t^{(q+1)/2}} \left(1 + O((qt)^{-\frac{1}{2} + \varepsilon})\right) + O(\log(x)). \end{aligned}$$

À ce stade nous utilisons l'estimation standard suivante (cf. [4] lemme 2.3 par exemple) : pour tout nombre entier $g \geq 2$ et tout nombre réel $\alpha \geq 0$, on a uniformément pour tout nombre entier $\nu \geq 1$,

$$\sum_{t=1}^{\nu} \frac{g^t}{t^\alpha} = \frac{g^{\nu+1}}{(g-1)\nu^\alpha} + O\left(\frac{g^\nu}{\nu^{\alpha+1}}\right).$$

On obtient alors, compte tenu du fait que $F_{q,1,0}$ est non vide,

$$\begin{aligned} N_q^{(1)}(x) &= \frac{(q-1)C_q}{q^q-1} \cdot \frac{q^{qT}}{(qT)^{(q+1)/2}} \sum_{1 \leq r \leq q} q^{r-1} \text{card}(F_{q,r,0}) \left(1 + O((qT)^{-\frac{1}{2}+\varepsilon})\right) \\ &= \frac{(q-1)C_q}{q^q-1} \cdot \frac{xq^{-q\{y\}}}{(\log_q x)^{(q+1)/2}} \sum_{1 \leq r \leq q} q^{r-1} \text{card}(F_{q,r,0}) \left(1 + O((\log x)^{-\frac{1}{2}+\varepsilon})\right). \end{aligned}$$

Ensuite, on a

$$\begin{aligned} N_q^{(2)}(x) &= \sum_{1 \leq r < R} V_{T,r}(q^{qT+r}) \\ &= (q-1)C_q \cdot \frac{q^{qT}}{(qT)^{(q+1)/2}} \sum_{1 \leq r < R} q^{r-1} \text{card}(F_{q,r,0}) \left(1 + O((qT)^{-\frac{1}{2}+\varepsilon})\right) \\ &= (q-1)C_q \cdot \frac{xq^{-q\{y\}}}{(\log_q x)^{(q+1)/2}} \sum_{1 \leq r \leq \lfloor q\{y\} \rfloor} q^{r-1} \text{card}(F_{q,r,0}) \left(1 + O((\log x)^{-\frac{1}{2}+\varepsilon})\right). \end{aligned}$$

Enfin,

$$\begin{aligned} N_q^{(3)}(x) &= V_{T,R}(x) = C_q \cdot \frac{x - q^{qT+R-1}}{(\log_q x)^{(q+1)/2}} \text{card}(F_{q,R,0}) \left(1 + O((\log x)^{-1/2+\varepsilon})\right) + O(1) \\ &= C_q \cdot \frac{x}{(\log_q x)^{(q+1)/2}} \left(1 - q^{-q\{y\}}\right) \text{card}(F_{q,\lfloor q\{y\} \rfloor+1,0}) \left(1 + O((\log x)^{-1/2+\varepsilon})\right) + O(1). \end{aligned}$$

Nous obtenons bien (11) avec pour $y \in \mathbb{R}$,

$$\begin{aligned} Q(y) &= (q-1)C_q \left(\frac{1}{q^q-1} q^{-q\{y\}} \sum_{1 \leq r \leq q} q^{r-1} \text{card}(F_{q,r,0}) + q^{-q\{y\}} \sum_{1 \leq r \leq \lfloor q\{y\} \rfloor} q^{r-1} \text{card}(F_{q,r,0}) \right. \\ &\quad \left. + (q-1)^{-1} (1 - q^{-q\{y\}}) \text{card}(F_{q,\lfloor q\{y\} \rfloor+1,0}) \right). \end{aligned}$$

Le fait que $F_{q,1,0}$ est non vide entraîne que la fonction Q est strictement positive. Elle est également non constante. En effet, pour $q \geq 4$, on remarque que $F_{q,q,0}$ est vide et donc que pour $\frac{q-1}{q} < y < 1$, on a

$$Q(y) = q^{-qy} (q-1)C_q \left(\frac{1}{q^q-1} \sum_{1 \leq r < q} q^{r-1} \text{card}(F_{q,r,0}) + \sum_{1 \leq r < q} q^r \text{card}(F_{q,r,0}) \right).$$

Pour $q = 2$, compte-tenu du fait que $\text{card}(F_{2,1,0}) = 2$ et $\text{card}(F_{2,2,0}) = 1$, on constate que pour $1/2 < y < 1$,

$$Q(y) = C_2 \left(1 + \frac{4}{3} \cdot 2^{-2y}\right).$$

Deuxième cas : q est impair. Dans ce cas le calcul fait intervenir la parité de T , aussi introduisons-nous les uniques nombres entiers $T' \geq 0$ et $L \in \{0, 1\}$ tels que $T = 2T' + L$. On a alors, en posant $z = \frac{1}{2q} \log_q x$,

$$T' = \lfloor z \rfloor, \quad L = \lfloor 2\{z\} \rfloor \quad \text{et} \quad R = \lfloor q\{2z\} \rfloor + 1.$$

En distinguant les cas $L = 0$ et $L = 1$, on obtient pour $x \geq q^{2q}$,

$$\begin{aligned} N_q^{(1)}(x) &= \sum_{1 \leq t < 2T'+L} \sum_{1 \leq r \leq q} V_{t,r}(q^{qt+r}) + O(1) \\ &= \frac{(q-1)C_q}{q^{2q}-1} \cdot \frac{xq^{-q\{2z\}}}{(\log_q x)^{(q+1)/2}} \left(\sum_{1 \leq r \leq q} q^{r-1} \text{card}(F_{q,r,L}) + q^q \sum_{1 \leq r \leq q} q^{r-1} \text{card}(F_{q,r,1-L}) \right) \\ &\quad \cdot \left(1 + O((\log x)^{-1/2+\varepsilon}) \right). \end{aligned}$$

On a ensuite

$$\begin{aligned} N_q^{(2)}(x) &= \sum_{1 \leq r < R} V_{2T'+L,r}(q^{(2T'+L)+r}) \\ &= (q-1)C_q \cdot \frac{xq^{-q\{2z\}}}{(\log_q x)^{(q+1)/2}} \sum_{1 \leq r < R} q^{r-1} \text{card}(F_{q,r,L}) \left(1 + O((\log x)^{-1/2+\varepsilon}) \right). \end{aligned}$$

Enfin on a

$$\begin{aligned} N_q^{(3)}(x) &= C_q \cdot \frac{x - q^{(2T'+L)q+R}}{(\log_q x)^{(q+1)/2}} \text{card}(F_{q,R,L}) \left(1 + O((\log x)^{-1/2+\varepsilon}) \right) + O(1) \\ &= C_q \cdot \frac{x(1 - q^{-\{q\{2z\}\})}}{(\log_q x)^{(q+1)/2}} \text{card}(F_{q,R,L}) \left(1 + O((\log x)^{-1/2+\varepsilon}) \right) + O(1). \end{aligned}$$

Nous obtenons bien (11) avec cette fois pour $y \in \mathbb{R}$,

$$\begin{aligned} Q(y) &= (q-1)C_q \left(\frac{q^{-q\{y\}}}{q^{2q}-1} \left(\sum_{1 \leq r \leq q} q^r \text{card}(F_{q,r,\lfloor 2\{y/2\} \rfloor}) + q^q \sum_{1 \leq r \leq q} q^r \text{card}(F_{q,r,1-\lfloor 2\{y/2\} \rfloor}) \right) \right. \\ &\quad \left. + q^{-q\{y\}} \sum_{1 \leq r \leq \lfloor q\{y\} \rfloor} q^r \text{card}(F_{q,r,\lfloor 2\{y/2\} \rfloor}) \right. \\ &\quad \left. + (q-1)^{-1}(1 - q^{-\{q\{y\}\}}) \text{card}(F_{q,\lfloor q\{y\} \rfloor+1,\lfloor 2\{y/2\} \rfloor}) \right). \end{aligned}$$

Là encore, la fonction Q est strictement positive car $F_{q,1,0}$ est non vide. Par ailleurs, comme $F_{q,q,1}$ est vide pour $q \geq 3$, on a pour $(q-1)/q < y < 1$,

$$Q(y) = K_q q^{-qy},$$

avec

$$K_q = C_q \left(\frac{1}{q^{2q}-1} \left(\sum_{1 \leq r \leq q} q^r \text{card}(F_{q,r,0}) + q^q \sum_{1 \leq r < q} q^r \text{card}(F_{q,r,1}) \right) + \sum_{1 \leq r < q} q^r \text{card}(F_{q,r,0}) \right) > 0.$$

En conséquence, Q n'est pas constante.

RÉFÉRENCES

- [1] M. DRMOTA, Subsequences of automatic sequences and uniform distribution, in *Uniform distribution and quasi-Monte Carlo methods*, pp. 87–104, *Radon Ser. Comput. Appl. Math.* vol. 15, De Gruyter, Berlin, 2014.
- [2] M. DRMOTA ET C. MAUDUIT, Weyl sums over integers with affine digit restrictions, *J. Number Theory* **130**,11 (2010), 2404–2427.

- [3] M. DRMOTA, C. MAUDUIT ET J. RIVAT, Primes with an Average Sum of Digits, *Compositio* **145**,2 (2009), 271–292.
- [4] E. FOUVRY ET C. MAUDUIT, Sur les entiers dont la somme des chiffres est moyenne, *J. Number Theory* **114**,1 (2005), 135–152.
- [5] A. O. GELFOND, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.* **13** (1967/1968), 259–265.
- [6] G. HANNA, Sur les occurrences des mots dans les nombres premiers, *Acta Arith.* **178**,1 (2017), 15–42.
- [7] L. KUIPERS ET H. NIEDERREITER, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.
- [8] B. MARTIN, C. MAUDUIT ET J. RIVAT, Propriétés locales des chiffres des nombres premiers, à paraître dans *J. Instit. Math. Jussieu*.
- [9] B. MARTIN, C. MAUDUIT ET J. RIVAT, Théorème des nombres premiers pour les fonctions digitales, *Acta Arith.* **165**,1 (2014), 11–45.
- [10] B. MARTIN, C. MAUDUIT ET J. RIVAT, Fonctions digitales le long des nombres premiers, *Acta. Arith.* **170**,2 (2015), 175–197.
- [11] C. MAUDUIT, Propriétés arithmétiques des substitutions et automates infinis, *Ann. Inst. Fourier* **56**,7 (2006), 2525–2549.
- [12] C. MAUDUIT ET J. RIVAT, Prime numbers along Rudin-Shapiro sequences, *J. Eur. Math. Soc. (JEMS)* **17**,10 (2015), 2595–2642.
- [13] C. MAUDUIT ET A. SÁRKÖZY, On the arithmetic structure of the integers whose sum of digits is fixed, *Acta Arithmetica* **81** (1997), 145–173.
- [14] C. MÜLLNER, Automatic sequences fulfill the Sarnak conjecture, *Duke. Math. J.* **166**,17 (2017), 3219–3290.
- [15] G. TENENBAUM, *Introduction à la théorie analytique et probabiliste des nombres*, Belin, Paris, éd. 3^e, 2008.
- [16] A. ZEE, *Quantum field theory in a nutshell*, Princeton University Press, Princeton, NJ, éd. second, 2010.

Adresse électronique: Bruno.Martin@univ-littoral.fr

Adresse électronique: mauduit@iml.univ-mrs.fr

Adresse électronique: rivat@iml.univ-mrs.fr

BRUNO MARTIN, UNIV. LITTORAL CÔTE D’OPALE, EA 2797 – LMPA – LABORATOIRE DE MATHÉMATIQUES PURES ET APPLIQUÉES JOSEPH LIOUVILLE, F-62228 CALAIS, FRANCE.

CHRISTIAN MAUDUIT, UNIVERSITÉ D’AIX-MARSEILLE ET INSTITUT UNIVERSITAIRE DE FRANCE, INSTITUT DE MATHÉMATIQUES DE MARSEILLE CNRS UMR 7373, 163 AVENUE DE LUMINY, CASE 907, 13288 MARSEILLE CEDEX 9, FRANCE.

JOËL RIVAT, UNIVERSITÉ D’AIX-MARSEILLE, INSTITUT DE MATHÉMATIQUES DE MARSEILLE CNRS UMR 7373, 163 AVENUE DE LUMINY, CASE 907, 13288 MARSEILLE CEDEX 9, FRANCE.