SUR LES CHIFFRES DES NOMBRES PREMIERS

BRUNO MARTIN, CHRISTIAN MAUDUIT & JOËL RIVAT

RÉSUMÉ. L'objet de ce travail est d'étendre les théorèmes de Hadamard – de la Vallée Poussin et de Vinogradov au cas des nombres premiers vérifiant une contrainte digitale. Notre méthode repose sur l'estimation des sommes d'exponentielles de la forme $\sum_{n\leqslant x}\Lambda(n)\exp\big(2i\pi(f(n)+\beta n)\big)$, où Λ désigne la fonction de von Mangoldt, f une fonction digitale, et β un paramètre réel.

ABSTRACT. The aim of this work is to extend the theorems of Hadamard – de la Vallée Poussin and Vinogradov to the case of prime numbers verifying a digital constraint. Our method lies on the estimate of exponential sums of the form $\sum_{n\leqslant x}\Lambda(n)\exp\big(2i\pi(f(n)+\beta n)\big)$, where Λ denotes von Mangoldt's function, f a digital function, and $\beta\in\mathbb{R}$ a parameter.

1. Introduction

Dans tout cet article, q désigne un nombre entier supérieur ou égal à 2. Rappelons que tout entier strictement positif n admet un unique développement q-adique de la forme

$$n=\sum_{j=0}^{\nu} n_j q^j,\quad 0\leqslant n_j\leqslant q-1,\quad n_\nu\geqslant 1. \tag{1}$$

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

$$|n|_k=\#\{0\leqslant j\leqslant \nu\,|\,n_j=k\}.$$

En particulier la fonction somme des chiffres est définie pour tout nombre entier positif n par

$$s(n)=\sum_{j=0}^{\nu} n_j=\sum_{0\leqslant k<q} k\,|n|_k\,.$$

Dans la suite, nous notons $\mathcal{P}$ l'ensemble des nombres premiers et, pour tout nombre réel x, $\mathrm{e}(x)=\exp(2i\pi x)$, $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x, et pour tout $(a,m)\in\mathbb{Z}\times\mathbb{N}^*$, $\pi(x;a,m)$ le nombre de nombres premiers inférieurs ou égaux à x congrus à a modulo m. Enfin nous désignons par Λ la fonction de von Mangoldt définie pour tout nombre entier positif n par

$$\Lambda(n)=\begin{cases}\log p & \text{si } n=p^\ell \text{ avec } p \text{ premier et } \ell\geqslant 1,\\ 0 & \text{sinon,}\end{cases}$$

et par τ la fonction qui compte le nombre de diviseurs.

Date: 1er septembre 2011.

2000 *Mathematics Subject Classification.* Primary 11A63, 11L03, 11N05. Secondary 11L20, 11N60.

Ce travail a bénéficié d'une aide de l'Agence Nationale de la Recherche portant la référence « ANR-10-BLAN 0103 » MUNUM. Bruno Martin a également bénéficié d'un financement de l'Austrian Science Foundation FWF dans le cadre du projet S9605, faisant partie de l'Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

Afin de détecter les congruences nous utiliserons la relation d'orthogonalité classique

$$\frac{1}{m}\sum_{j=0}^{m-1} \mathrm{e}\Big(\frac{j(a-b)}{m}\Big) = \begin{cases} 1 & \text{si } a \equiv b \bmod m \\ 0 & \text{sinon.} \end{cases} \qquad (m \in \mathbb{N}^*, a, b \in \mathbb{Z}). \tag{2}$$

Même lorsque ce n'est pas mentionné, les constantes implicites dans les $\ll$ et O peuvent dépendre de la base de numération q.

1.1. **Fonctions q-additives et fonctions digitales.**

La notion de fonction q-additive a été introduite indépendamment par Bellman et Shapiro [3] et Gelfond [18]. Il s'agit des fonctions $f : \mathbb{N} \to \mathbb{R}$ qui vérifient pour tout $(a, b, j) \in \mathbb{N}^3$ tel que $0 \leqslant b < q^j$:

$$f(aq^j + b) = f(aq^j) + f(b).$$

Une fonction q-additive vérifie donc nécessairement $f(0) = 0$. Lorsque l'on a de plus $f(aq^j) = f(a)$ pour tout $(a, j) \in \mathbb{N}^2$ on dit que la fonction f est fortement q-additive. La fonction somme de chiffres appartient à la classe des fonctions fortement q-additives à valeurs entières.

Si f est fortement q-additive alors on a pour tout nombre entier positif n vérifiant (1) :

$$f\Big(\sum_{0\leqslant j\leqslant \nu} n_j q^j\Big) = \sum_{0\leqslant j\leqslant \nu} f(n_j) = \sum_{1\leqslant k<q} f(k)|n|_k, \tag{3}$$

de sorte que f est complètement déterminée par ses valeurs $f(k)$ pour $1 \leqslant k < q$. Réciproquement, toute fonction de la forme $f(n) = \sum_{1\leqslant k<q} \alpha_k |n|_k$ est fortement q-additive. Par contre on remarquera que la fonction $|\cdot|_0$ n'est pas fortement q-additive.

Notation 1. *On note $\mathcal{F}$ l'ensemble des fonctions $f : \mathbb{N} \to \mathbb{R}$ définies pour tout nombre entier positif n par*

$$f(n) = \sum_{0\leqslant k<q} \alpha_k |n|_k, \tag{4}$$

où $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ sont des nombres réels.

Drmota et Mauduit ont étudié dans [13] certaines propriétés statistiques de ces fonctions, appelées fonctions digitales et l'objet de ce travail est d'étudier les propriétés statistiques de la restriction de ces fonctions à l'ensemble des nombres premiers.

1.2. **Propriétés digitales des nombres premiers.**

On ne connaît pas d'algorithme simple permettant de savoir si un nombre entier est premier à partir de la donnée de son écriture en base q. Minsky et Papert ont d'ailleurs montré dans [30] que l'ensemble des nombres premiers n'est reconnaissable par aucun q-automate fini (pour cette notion, on pourra consulter [1] ou [15]). Cobham a présenté dans [5] plusieurs preuves alternatives de ce résultat qui a été généralisé par Hartmanis et Shank dans [22] et Schützenberger dans [33] en montrant qu'aucun ensemble infini de nombres premiers n'est reconnaissable par un q-automate fini (ni même par un automate à pile), par Mauduit dans [26] en montrant que l'ensemble des nombres premiers n'est engendré par aucun morphisme sur un alphabet fini et par Cassaigne et Le Gonidec dans [4] en montrant que l'ensemble des nombres premiers n'est reconnaissable par aucun q-automate infini (voir [27] pour cette dernière notion).

Il existe peu de résultats dans la littérature concernant les propriétés des chiffres des nombres premiers. Le théorème de Lejeune Dirichlet (voir [24, pp. 315–342] ou [11, p. 34]) concernant la répartition des nombres premiers dans les progressions arithmétiques peut être considéré comme le premier résultat dans ce domaine. Il permet de montrer, comme l'a remarqué Sierpiński, que pour toute suite finie de chiffres $a_1, \ldots, a_m$ et $b_1, \ldots, b_n$ telle que $\mathrm{pgcd}(b_n, q) = 1$, il existe une infinité de nombres premiers dont les m premiers chiffres sont successivement $a_1, \ldots, a_m$ et les n derniers chiffres successivement $b_1, \ldots, b_n$ ([34] contient une preuve de ce théorème dans le

cas $q = 10$ et attribue à une remarque de Knapowski le cas général). Harman a étendu dans [21] ce résultat à des nombres premiers qui possèdent certains chiffres librement préassignés, démontrant ainsi une conjecture due à Wolke [36] : pour tout nombre entier $t > 0$ fixé il existe un nombre entier $K(q,t)$ tel que si $k > K(q,t)$ alors pour tous $0 \leqslant j_1 < \cdots < j_t \leqslant k$ et pour tout $(b_1, \dots, b_t) \in \{0, \dots, q-1\}^t$ vérifiant $(b_1, q) = 1$ si $j_1 = 0$ et $b_t \neq 0$ si $j_t = k$, il existe une infinité de nombres premiers $p = \sum_{j=0}^{k} p_j q^j$ tels que $(p_{j_1}, \dots, p_{j_t}) = (b_1, \dots, b_t)$.

Signalons qu'à la fin de son article, Harman remarque que sa méthode devrait permettre d'obtenir une formule asymptotique analogue à celle obtenue par Wolke dans les cas particuliers où $t \in \{1, 2\}$ ainsi que, sous l'hypothèse de Riemann généralisée, dans le cas plus général, pour tout $0 < \varepsilon < 1$ et $k \geqslant k_0(\varepsilon)$, des nombres entiers t vérifiant $1 \leqslant t \leqslant (1-\varepsilon)\sqrt{k}$.

Copeland et Erdős [7] en 1946 ont montré, pour tout ensemble $\mathcal{E}$ de nombres entiers vérifiant, pour tout $\theta < 1$, $\mathrm{card}\{n \leqslant x,\ n \in \mathcal{E}\} \gg x^\theta$ pour x assez grand, la normalité du nombre réel dont l'écriture en base q est formée de 0, suivi de la concaténation dans l'ordre croissant des éléments de l'ensemble $\mathcal{E}$ écrits en base q. Il découle en particulier de leur théorème que si $f \in \mathcal{F}$ alors

$$\sum_{p \leqslant x} f(p) = \frac{x}{q \log q} \sum_{0 \leqslant k < q} \alpha_k + o(x).$$

Le théorème suivant démontré par Mauduit et Rivat dans [29] répond à une question posée en 1967 par Gelfond dans [18] concernant la somme des chiffres des nombres premiers (voir [17, 16, 10] pour une réponse partielle dans le cas des nombres presque premiers, c'est-à-dire ayant au plus r facteurs premiers, où $r \geqslant 2$ est un nombre entier fixé).

Théorème A. *Pour q et m entiers $\geqslant 2$, il existe $\sigma_{q,m} > 0$ tel que pour tout $a \in \mathbb{Z}$,*

$$\mathrm{card}\{p \leqslant x,\ s(p) \equiv a \bmod m\} = \frac{\mathrm{pgcd}(m, q-1)}{m} \pi(x; a, \mathrm{pgcd}(m, q-1)) + O_{q,m}(x^{1-\sigma_{q,m}}). \tag{5}$$

Le théorème A et ses généralisations présentées dans le paragraphe 9.1 concernent la recherche de nombres premiers dans une suite reconnaissable par un q-automate fini, puisqu'il est facile de vérifier que lorsque g est une fonction digitale à valeurs entières alors, pour tous nombres entiers $a \in \mathbb{Z}$ et $m \geqslant 2$, la suite formée des nombres entiers n tels que $g(n) \equiv a \bmod m$ est reconnaissable par un q-automate fini.

La recherche de nombres premiers dans une suite reconnaissable par un q-automate fini est un problème en général extrêmement difficile. Par exemple les suites $(2^n + 1)_{n \in \mathbb{N}}$ et $(2^n - 1)_{n \in \mathbb{N}}$ sont chacune reconnaissable par un 2-automate fini et les problèmes associés correspondent respectivement à la recherche de nombres premiers de Fermat et de Mersenne.

Lorsque $\mathbf{u}$ est une suite reconnaissable par un q-automate fini irréductible (c'est-à-dire dont le graphe de l'automate est fortement connexe) il résulte d'une remarque de Fouvry et Mauduit [17] que la suite $\mathbf{u}$ contient une infinité de nombres presque premiers. Mais le problème de la recherche de nombres presque premiers dans une suite automatique quelconque est lui aussi largement ouvert (voir [8], [9] et [6] pour le cas particulier des nombres ellipséphiques).

1.3. **Propriétés statistiques de suites arithmétiques.**

De nombreux travaux concernent l'étude des propriétés statistiques des suites de nombres entiers $\mathbf{u} = (u_n)_{n \in \mathbb{N}}$ définie par un algorithme « simple » (cf. [32]). En particulier l'étude précise des sommes d'exponentielles associées à ces suites permet d'étudier la répartition modulo 1 de la suite $(u_n \alpha)_{n \in \mathbb{N}}$ lorsque $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ainsi que la répartition dans les progressions arithmétiques de la suite $\mathbf{u}$ (voir par exemple [25] pour le cas des suites reconnaissables par un q-automate fini). Dans ce travail nous nous intéressons à l'étude beaucoup plus délicate des propriétés statistiques des suites extraites le long des nombres premiers d'une telle suite $\mathbf{u}$. Lorsque $u_n = n$ la répartition dans les progressions arithmétiques de la suite $(p)_{p \in \mathcal{P}}$ a été étudiée par Hadamard

et de la Vallée Poussin dans [19] et [12] et la répartition modulo 1 de la suite $(\alpha p)_{p\in\mathcal{P}}$ pour $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ par Vinogradov dans [35] (voir également [2, théorème 9.12] et [23, théorème 21.3]) :

Théorème B (Hadamard et de la Vallée Poussin)**.** *Si $(a,m)\in\mathbb{Z}\times\mathbb{N}^*$ vérifie $(a,m)=1$, alors*

$$\pi(x;a,m)\sim \frac{1}{\varphi(m)}\cdot\frac{x}{\log x},$$

où φ désigne la fonction indicatrice d'Euler.

Théorème C (Vinogradov)**.** *Si $\alpha\in\mathbb{R}\setminus\mathbb{Q}$ alors la suite $(\alpha p)_{p\in\mathcal{P}}$ est équirépartie modulo* 1.

L'objet du paragraphe 9.2 est de généraliser ces théorèmes au cas de la suite $\mathbf{u}$ constituée des nombres entiers n tels que $g(n)\equiv a \bmod m$, où g est une fonction digitale à valeurs entières donnée.

Enfin, de même que le théorème C constitue un ingrédient essentiel de la résolution du problème de Goldbach ternaire, les théorèmes 1 et 2 permettent de résoudre un problème de Goldbach ternaire pour des nombres premiers vérifiant des conditions digitales, ce qui constitue l'objet de la partie 9.3.

2. Résultats

Le Théorème A est une conséquence de l'estimation suivante obtenue par Mauduit et Rivat dans [29] : pour $\alpha\in\mathbb{R}$ tel que $(q-1)\alpha\in\mathbb{R}\setminus\mathbb{Z}$, il existe $\sigma_q(\alpha)>0$ tel que pour $x\geqslant 1$,

$$\sum_{n\leqslant x}\Lambda(n)\,\mathrm{e}\big(\alpha\, s(n)\big)\ll_{q,\alpha} x^{1-\sigma_q(\alpha)}. \tag{6}$$

Un raffinement dans la preuve de [29] permet de s'affranchir de la dépendance implicite en α et de fournir une forme explicite pour l'exposant $\sigma_q(\alpha)$: c'est l'objet du théorème 2.1 de [14], qui permet de choisir $\sigma_q(\alpha)=c\,\|(q-1)\alpha\|^2$ où c est une constante strictement positive qui ne dépend que de q.

Il est assez naturel de rechercher une estimation similaire à (6) pour une fonction fortement q-additive arbitraire. Le premier objectif de ce travail est d'établir un tel résultat en traitant plus généralement le cas des fonctions digitales, ce qui nous permet en particulier d'établir le théorème 4 qui généralise le théorème A. Le second objectif est de généraliser les théorèmes B et C au cas des nombres premiers vérifiant des conditions digitales ce qui nous conduit à établir respectivement les théorèmes 6 et 5.

En vue d'obtenir ces nouvelles applications, nous devons donc étudier la somme d'exponentielles plus générale

$$\sum_{n\leqslant x}\Lambda(n)\,\mathrm{e}\big(f(n)+\beta n\big)\quad (x\geqslant 1,\beta\in\mathbb{R}). \tag{7}$$

Pour estimer (7) nous allons distinguer deux cas selon que la suite $\alpha_0,\alpha_1,\dots,\alpha_{q-1}$ est une progression arithmétique modulo 1 ou non :

Cas 1 : la suite $\alpha_0,\alpha_1,\dots,\alpha_{q-1}$ est une progression arithmétique modulo 1, c'est-à-dire qu'il existe $\theta\in\mathbb{R}$ tel que pour tout $j\in\{0,\dots,q-1\}$ on a $\alpha_j=\alpha_0+j\theta \bmod 1$. Nous verrons que dans ce cas le comportement de la somme d'exponentielles (7) dépend de $(q-1)\theta$:

- si $(q-1)\theta\in\mathbb{R}\setminus\mathbb{Z}$ alors

$$\sum_{n\leqslant x}\Lambda(n)\,\mathrm{e}\big(f(n)+\beta n\big)=o(x),$$

- si $(q-1)\theta=\ell\in\mathbb{Z}$ alors, en écrivant

$$\alpha_j=\alpha_0+j\ell/(q-1) \bmod 1$$

pour $0 \leqslant j < q$, et en notant que $|n|_0 + \ldots + |n|_{q-1} = \lfloor \log_q n \rfloor + 1$, on parvient à l'identité

$$\begin{aligned}\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\big(f(n)+\beta n\big) &= \sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\Big(\alpha_0 \lfloor \log_q n\rfloor + \alpha_0 + \frac{\ell}{q-1}s(n) + \beta n\Big)\\ &= \mathrm{e}(\alpha_0)\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\Big(\alpha_0 \lfloor \log_q n\rfloor + \frac{\ell n}{q-1} + \beta n\Big),\end{aligned}$$

car $s(n) \equiv n \bmod (q-1)$ pour tout entier naturel n. En découpant la somme en n suivant des intervalles q-adiques, on se ramène ainsi à l'évaluation de sommes d'exponentielles de la forme

$$\sum_{y\leqslant n<x} \Lambda(n)\,\mathrm{e}(n\theta) \quad (\theta \in \mathbb{R}, 0 \leqslant y < x),$$

qui peuvent être estimées par des techniques classiques de théorie analytique des nombres.

Cas 2 : la suite $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ n'est pas une progression arithmétique modulo 1. Dans ce cas nous verrons que l'on a toujours

$$\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\big(f(n)+\beta n\big) = o(x).$$

Ceci nous conduit à introduire le sous-ensemble suivant de $\mathcal{F}$:

Notation 2. *On note $\mathcal{F}_0$ l'ensemble des éléments de $\mathcal{F}$ pour lesquels la suite des nombres réels $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ est une progression arithmétique modulo* 1.

Remarque 1.
- *Lorsque $q = 2$ on a $\mathcal{F} = \mathcal{F}_0$.*
- *Pour $q \geqslant 2$ et $f(n) = \alpha\, s(n)$ avec $\alpha \in \mathbb{R}$, on a $f \in \mathcal{F}_0$.*

Lemme 1. *La suite $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ est une progression arithmétique modulo 1 si et seulement si*

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

Démonstration. Si la suite $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ est une progression arithmétique modulo 1 alors il existe $t \in \mathbb{R}$ tel que pour tout $j \in \{0, \ldots, q-1\}$, $\alpha_j = \alpha_0 + jt \bmod 1$. Par conséquent pour tout $(i,j) \in \{0,\ldots,q-1\}^2$ on a $\|\alpha_i - \alpha_j - (i-j)t\| = 0$. Réciproquement, si

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

alors il existe un $t \in \mathbb{R}$ qui réalise ce minimum. Pour cette valeur de t tous les termes de la somme sont nuls, donc pour tout $j \in \{0,\ldots,q-1\}$ on a $\|\alpha_j - \alpha_0 - jt\|^2 = 0$ c'est-à-dire $\alpha_j = \alpha_0 + jt \bmod 1$. □

Pour tout $f \in \mathcal{F}$ on note

$$\sigma_q(f) = \min_{t\in\mathbb{R}} \sum_{0\leqslant j<i<q} \|\alpha_i - \alpha_j - (i-j)t\|^2 \tag{8}$$

et on remarque que

$$f \in \mathcal{F}_0 \Longleftrightarrow \sigma_q(f) = 0.$$

L'objectif des paragraphes 4, 5, 6, 7 et 8 est de démontrer les théorèmes suivants.

Théorème 1. *Pour tout $q \geqslant 2$, il existe $c_q > 0$ tel que pour tout $f \in \mathcal{F}_0$, $x \geqslant 2$, $\beta \in \mathbb{R}$, on a*

$$\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\big(f(n)+\beta n\big) \ll (\log x)^4 x^{1-c_q\|(q-1)\theta\|^2}, \tag{9}$$

où $\theta = \alpha_1 - \alpha_0$ et la constante implicite ne dépend que de q.

Théorème 2. *Pour tout $q \geqslant 2$, il existe $c_q > 0$ tel que pour tout $f \in \mathcal{F}$, $x \geqslant 2$, $\beta \in \mathbb{R}$, on a*

$$\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\big(f(n)+\beta n\big) \ll (\log x)^4 x^{1-c_q\sigma_q(f)}, \tag{10}$$

où la constante implicite ne dépend que de q.

Dans le paragraphe 9 nous montrons comment les théorèmes 1 et 2 permettent d'étudier, lorsque g est une fonction digitale à valeurs entières donnée, d'une part l'équirépartition modulo 1 de la suite $(\alpha g(p))_{p\in\mathcal{P}}$ pour $\alpha \in \mathbb{R}$, d'autre part les propriétés statistiques de la suite constituée des nombres premiers p tels que $g(p) \equiv a \bmod m$, et enfin de résoudre le problème de Goldbach ternaire pour des nombres premiers vérifiant des conditions digitales.

Afin d'alléger les énoncés nous donnons dans ce dernier paragraphe les théorèmes précis lorsque g est une fonction fortement q-additive à valeurs entières telle que les entiers $g(0), \dots, g(q-1)$ sont premiers entre eux, et nous expliquons comment ceux-ci permettent de traiter le cas général des fonctions digitales.

3. Description de la preuve des théorèmes 1 et 2

L'identité de Vaughan [1] appliquée à la somme (7) conduit à l'estimation de sommes classiquement qualifiées de type I et II, qui font l'objet des paragraphes 6 et 7 respectivement. La pertinence de ces estimations repose sur le comportement en moyenne et en norme infinie de la transformée de Fourier discrète d'une version tronquée de la fonction f, qui est définie et étudiée au paragraphe 5. La mise en œuvre de la méthode de Vaughan, et ainsi la preuve finale des théorèmes 1 et 2, sont effectuées au paragraphe 8.

La fonction somme des chiffres s correspond à un cas très particulier de fonction digitale car $(s(0), s(1), \dots, s(q-1)) = (0, 1, \dots, q-1)$ constitue une progression arithmétique. Dans la méthode mise en place dans [29] il est crucial de pouvoir estimer de manière très précise les transformées de Fourier discrètes :

$$|F_\lambda(h,\alpha)| = \frac{1}{q^\lambda}\prod_{j=1}^{\lambda}\left|\frac{\sin \pi q\left(\alpha-\frac{h}{q^j}\right)}{\sin \pi\left(\alpha-\frac{h}{q^j}\right)}\right|.$$

Lorsque f est une fonction digitale quelconque, l'étude des transformées de Fourier discrètes

$$|F_\lambda(h,\alpha)| = \frac{1}{q^\lambda}\prod_{j=1}^{\lambda}\varphi\left(\frac{h}{q^j}\right)$$

où $\varphi(t) = \left|\sum_{0\leqslant k<q} \mathrm{e}(\alpha_k - kt)\right|$, est extrêmement délicate. Si $\alpha_0, \dots, \alpha_{q-1}$ constitue une progression arithmétique modulo 1 (c'est-à-dire si $f \in \mathcal{F}_0$) la fonction φ est une somme géométrique et la méthode mise en place dans [29] se généralise et permet d'obtenir le théorème 1. Dans le cas général la stratégie développée dans [29] est inopérante et il est nécessaire d'étudier d'une manière beaucoup plus fine ces transformées de Fourier. C'est l'objet des lemmes 2, 3, 4, 5, 6, 7.

1. Voir par exemple [23] paragraphe 13.4

4. Lemmes techniques

Nous établissons dans cette section quelques lemmes utiles pour la section 5. Nous commençons par fournir deux lemmes généraux concernant certaines moyennes quadratiques et biquadratiques d'un polynôme trigonométrique.

Lemme 2. *Soit $K \in \mathbb{N}$ et $P(t) = \sum_{k=0}^{K} c_k \, \mathrm{e}(kt)$ ($c_k \in \mathbb{C}$). Alors pour tout nombre entier $N \geqslant K+1$ on a*

$$\frac{1}{N} \sum_{n=0}^{N-1} \left| P\left(t + \frac{n}{N}\right)\right|^2 = \sum_{k=0}^{K} |c_k|^2 .$$

Démonstration. En développant le carré du membre de gauche et en intervertissant les sommes on obtient

$$\sum_{k=0}^{K} \sum_{k'=0}^{K} c_k \overline{c_{k'}} \ \mathrm{e}((k-k')t) \ \frac{1}{N} \sum_{n=0}^{N-1} \mathrm{e}\left((k-k')\frac{n}{N}\right).$$

Pour tout $N \geqslant K+1$, il y a équivalence entre $k - k' \equiv 0 \bmod N$ et $k - k' = 0$, d'où l'égalité annoncée. □

Lemme 3. *Soit $K \in \mathbb{N}$ et $P(t) = \sum_{k=0}^{K} c_k \, \mathrm{e}(kt)$ ($c_k \in \mathbb{C}$). Alors $|P(t)|^2$ est un polynôme trigonométrique de degré K :*

$$|P(t)|^2 = \sum_{|k| \leqslant K} \left(\sum_j c_{j+k} \, \overline{c_j} \right) \mathrm{e}(kt),$$

où la somme sur j est restreinte par $\max(0, -k) \leqslant j \leqslant \min(K, K-k)$, et pour tout nombre entier $N \geqslant 2K+1$ on a

$$\frac{1}{N} \sum_{n=0}^{N-1} \left| P\left(t + \frac{n}{N}\right)\right|^4 = \sum_{k=-K}^{K} \left| \sum_j c_{j+k} \, \overline{c_j} \right|^2 .$$

Démonstration. On écrit

$$|P(t)|^2 = \sum_{i=0}^{K} \sum_{j=0}^{K} c_i \overline{c_j} \, \mathrm{e}((i-j)t)$$

et en posant $i = j+k$ on obtient la première égalité. Pour montrer la seconde égalité, on observe que $|P(t)|^2 = |Q(t)|$ avec

$$Q(t) = \sum_{|k| \leqslant K} \left(\sum_j c_{j+k} \, \overline{c_j} \right) \mathrm{e}((k+K)t) = \sum_{0 \leqslant k' \leqslant 2K} \left(\sum_j c_{j+k'-K} \, \overline{c_j} \right) \mathrm{e}(k't),$$

et on applique le lemme 2 à $Q(t)$. □

Pour $R \in \mathbb{N}^*$ et $u \in \mathbb{R}$, introduisons

$$\tilde{\varphi}_R(u) = \Big| \sum_{0 \leqslant r < R} \mathrm{e}(ru) \Big|. \tag{11}$$

Lemme 4. *Pour $L \geqslant 2$, $R \geqslant 2$, on a*

$$\frac{1}{RL} \sum_{|\ell| < L} \left(1 - \frac{|\ell|}{L}\right) \tilde{\varphi}_R\left(\frac{\ell}{RL}\right) \leqslant \frac{1}{4 - 2\sqrt{2}} < 1. \tag{12}$$

Démonstration. Pour $0 \leqslant a < 1$ fixé, la fonction $x \mapsto \sin(\pi a x)$ est concave sur $[0; 1/2]$, d'où $\sin(\pi a x) \geqslant 2x \sin(\pi a/2)$. En prenant $a = |\ell| / L$ et $x = 1/R$, on a donc

$$\frac{1}{R}\,\tilde{\varphi}_R\Big(\frac{\ell}{RL}\Big) = \frac{\sin\frac{\pi|\ell|}{L}}{R\sin\frac{\pi|\ell|}{LR}} \leqslant \frac{\sin\frac{\pi|\ell|}{L}}{2\sin\frac{\pi|\ell|}{2L}} = \cos\frac{\pi\ell}{2L}.$$

Le noyau de Fejér d'ordre $L-1$ vaut pour tout $t \in \mathbb{R}$:

$$K_L(t) = \sum_{|\ell|<L}\Big(1-\frac{|\ell|}{L}\Big)\cos(2\pi\ell t) = \sum_{|\ell|<L}\Big(1-\frac{|\ell|}{L}\Big)\,\mathrm{e}(\ell t) = \frac{1}{L}\Big(\frac{\sin\pi tL}{\sin\pi t}\Big)^2.$$

Nous avons ainsi

$$\frac{1}{RL}\sum_{|\ell|<L}\Big(1-\frac{|\ell|}{L}\Big)\,\tilde{\varphi}_R\Big(\frac{\ell}{RL}\Big) \leqslant \frac{1}{L}K_L\Big(\frac{1}{4L}\Big) = \frac{1}{L^2}\Big(\frac{\sin\frac{\pi}{4}}{\sin\frac{\pi}{4L}}\Big)^2 = \frac{1}{2L^2\sin^2\frac{\pi}{4L}}.$$

Par concavité de la fonction sinus, on a $\sin x \geqslant \frac{8x}{\pi}\sin\frac{\pi}{8}$ pour tout $x \in [0; \pi/8]$, ce qui, appliqué avec $x = \pi/4L \in [0; \pi/8]$, donne

$$\frac{1}{RL}\sum_{|\ell|<L}\Big(1-\frac{|\ell|}{L}\Big)\,\tilde{\varphi}_R\Big(\frac{\ell}{RL}\Big) \leqslant \frac{1}{8\sin^2\frac{\pi}{8}},$$

d'où la majoration (12) puisque $\sin^2\frac{\pi}{8} = (2-\sqrt{2})/4$. □

5. Étude de transformées de Fourier discrètes

Dans cette section nous considérons une fonction $f \in \mathcal{F}$ fixée ce qui revient à fixer un q-uplet $(\alpha_0, \dots, \alpha_{q-1})$ de nombres réels. Étant donné $\lambda \in \mathbb{N}$, nous introduisons les fonctions $|\cdot|_{\lambda,k}$ définie par

$$|n|_{\lambda,k} = \#\{0 \leqslant j < \lambda \,|\, n_j = k\} \quad (n = \sum_{j\geqslant 0} n_j q^j, 0 \leqslant n_j < q), \tag{13}$$

et la fonction f_λ définie par

$$f_\lambda(n) = \sum_{0\leqslant k<q} \alpha_k |n|_{\lambda,k}. \tag{14}$$

Remarquons que pour $j \in \{0, \dots, q-1\}$, $u, v \in \mathbb{N}$, $v < q$, $\lambda \in \mathbb{N}^*$,

$$|uq+v|_{\lambda,j} = |u|_{\lambda-1,j} + |v|_j, \tag{15}$$

d'où

$$f_\lambda(uq+v) = f_{\lambda-1}(u) + \sum_{0\leqslant j<q}\alpha_j|v|_j = f_{\lambda-1}(u) + \alpha_v.$$

La fonction $n \mapsto \mathrm{e}\big(f_\lambda(n)\big)$ étant q^λ périodique, nous pouvons considérer sa transformée de Fourier discrète

$$F_\lambda(h) := \frac{1}{q^\lambda}\sum_{0\leqslant u<q^\lambda}\mathrm{e}\Big(f_\lambda(u) - \frac{uh}{q^\lambda}\Big) \quad (h \in \mathbb{Z}). \tag{16}$$

On a $F_0 = 1$, et pour $\lambda \in \mathbb{N}^*$, en remplaçant u par $uq+v$ avec $0 \leqslant v < q$ et $0 \leqslant u < q^{\lambda-1}$, nous obtenons,

$$\begin{aligned} F_\lambda(h) &= \frac{1}{q^\lambda}\sum_{0\leqslant v<q}\mathrm{e}\Big(\alpha_v - \frac{vh}{q^\lambda}\Big)\sum_{0\leqslant u<q^{\lambda-1}}\mathrm{e}\Big(f_{\lambda-1}(u) - \frac{uh}{q^{\lambda-1}}\Big) \\ &= \frac{1}{q}\sum_{0\leqslant v<q}\mathrm{e}\Big(\alpha_v - \frac{vh}{q^\lambda}\Big)F_{\lambda-1}(h). \end{aligned}$$

Par récurrence, on obtient donc

$$|F_\lambda(h)| = \frac{1}{q^\lambda}\prod_{j=1}^{\lambda}\varphi\Big(\frac{h}{q^j}\Big) \quad (\lambda\in\mathbb{N}, h\in\mathbb{Z}), \tag{17}$$

où φ est la fonction 1-périodique définie par

$$\varphi(t) = \Big|\sum_{0\leqslant k<q}\mathrm{e}(\alpha_k - kt)\Big| \quad (t\in\mathbb{R}).$$

Les calculs ultérieurs nécessitent deux types de renseignements spécifiques concernant la fonction F_λ : une majoration en moyenne le long d'une progression arithmétique et une majoration en norme infinie.

5.1. **Estimations en moyenne.**

L'objectif de ce paragraphe est d'obtenir une estimation fine du comportement en moyenne de F_λ le long d'une progression arithmétique. Dans le cas de la fonction somme de chiffres et lorsque $q\geqslant 3$, cela repose essentiellement sur l'étude de la fonction de transfert

$$\Phi_1(t) = \frac{1}{q}\sum_{0\leqslant r<q}\varphi\Big(t+\frac{r}{q}\Big),$$

pour laquelle il faut fournir une borne uniforme meilleure que la racine carrée de la borne triviale : voir la preuve du lemme 16 [2] de [29]. Une telle majoration n'est pas disponible dans le cas plus général traité ici. Tout comme dans le cas $q=2$ pour la somme de chiffres (voir lemme 18 de [29]), il est nécessaire d'étudier la fonction de transfert d'ordre 2 soit

$$\begin{aligned}\Phi_2(t) &= \frac{1}{q}\sum_{0\leqslant r<q}\varphi\Big(\frac{t+r}{q}\Big)\Phi_1\Big(\frac{t+r}{q}\Big)\\ &= \frac{1}{q^2}\sum_{0\leqslant r<q}\varphi\Big(\frac{t+r}{q}\Big)\sum_{0\leqslant s<q}\varphi\Big(\frac{t+r}{q^2}+\frac{s}{q}\Big)\end{aligned}$$

Pour des raisons techniques qui apparaîtront clairement dans la preuve de la Proposition 1 *infra*, résultat principal de ce paragraphe, il nous faut en fait étudier une version plus générale de la fonction Φ_2 : nous introduisons

$$\Psi(t,R,S) = \frac{1}{q^2}\sum_{r<R}\varphi\Big(\frac{t+r}{R}\Big)\sum_{s<S}\varphi\Big(\frac{t+r}{qR}+\frac{s}{S}\Big) \quad (t\in\mathbb{R}, R,S\in\mathbb{N}^*). \tag{18}$$

Notons la majoration triviale $\Psi(t,R,S)\leqslant RS \quad (t\in\mathbb{R})$. Un majorant pour $\Psi(t,R,S)$ de la forme $(RS)^{\eta_q}$ avec $\eta_q<1/2$ est fourni au lemme 7 *infra*, dont la preuve repose sur les Lemmes 5 et 6 qui suivent.

Lemme 5. *Pour $R\mid q$ et $S\mid q$ on a*

$$\Psi(t,R,S)^2 \leqslant \frac{S^2}{q}\sum_{|\ell|<q/S}\left(1-\frac{S\,|\ell|}{q}\right)\tilde{\varphi}_R\left(\frac{\ell S}{qR}\right), \tag{19}$$

où $\tilde{\varphi}_R$ est définie en (11).

Démonstration. Commençons par remarquer que d'après le lemme 2 appliqué à la fonction φ, on a pour tout nombre entier $N\geqslant q$,

$$\frac{1}{N}\sum_{n=0}^{N-1}\varphi^2\left(t+\frac{n}{N}\right) = q. \tag{20}$$

2. La fonction de transfert y est notée Ψ_q.

En appliquant l'inégalité de Cauchy-Schwarz à la somme sur r dans l'expression (18) de $\Psi(t,R,S)$, et en observant à l'aide de (20) que

$$\frac{1}{q^2}\sum_{0\leqslant r<R}\varphi^2\left(\frac{t+r}{R}\right)=\frac{1}{q^2}\sum_{0\leqslant r<R}\varphi^2\left(\frac{t}{R}+\frac{rq/R}{q}\right)\leqslant\frac{1}{q^2}\sum_{0\leqslant r'<q}\varphi^2\left(\frac{t}{R}+\frac{r'}{q}\right)=1, \tag{21}$$

on voit qu'il suffit de majorer par le membre de droite de (19) l'expression

$$\frac{S}{q^2}\sum_{0\leqslant r<R}\sum_{0\leqslant s<S}\varphi^2\left(\frac{t+r}{qR}+\frac{s}{S}\right).$$

Maintenant on peut écrire

$$\sum_{0\leqslant s<S}\varphi^2\left(u+\frac{s}{S}\right)=\sum_{0\leqslant i<q}\sum_{0\leqslant j<q}\mathrm{e}(\alpha_i-\alpha_j-(i-j)u)\sum_{0\leqslant s<S}\mathrm{e}\left(-(i-j)\frac{s}{S}\right),$$

ce qui entraîne, d'après la relation 2,

$$\sum_{0\leqslant s<S}\varphi^2\left(u+\frac{s}{S}\right)=S\sum_{0\leqslant i<q}\sum_{\substack{0\leqslant j<q\\ j\equiv i \bmod S}}\mathrm{e}(\alpha_i-\alpha_j-(i-j)u).$$

Il suffit donc de majorer par le membre de droite de (19) l'expression

$$\frac{S^2}{q^2}\sum_{0\leqslant r<R}\sum_{0\leqslant i<q}\sum_{\substack{0\leqslant j<q\\ j\equiv i \bmod S}}\mathrm{e}\left(\alpha_i-\alpha_j-(i-j)\frac{t+r}{qR}\right).$$

En intervertissant les sommes et en majorant trivialement, il suffit finalement de montrer que le membre de droite de (19) est égal à l'expression

$$\frac{S^2}{q^2}\sum_{0\leqslant i<q}\sum_{\substack{0\leqslant j<q\\ j\equiv i \bmod S}}\left|\sum_{0\leqslant r<R}\mathrm{e}\left(-(i-j)\frac{r}{qR}\right)\right|.$$

En découpant par tranches de longueur S on obtient

$$\frac{S^2}{q^2}\sum_{0\leqslant i<S}\sum_{0\leqslant k<q/S}\sum_{\substack{0\leqslant j<q\\ j\equiv i \bmod S}}\tilde{\varphi}_R\left(\frac{-(i+kS-j)}{qR}\right),$$

c'est-à-dire en posant $j=i+k'S$,

$$\frac{S^2}{q^2}\sum_{0\leqslant i<S}\sum_{0\leqslant k<q/S}\sum_{0\leqslant k'<q/S}\tilde{\varphi}_R\left(\frac{-(kS-k'S)}{qR}\right),$$

ce qui, en comptant le nombre de représentations de $\ell=k'-k$, donne

$$\frac{S^3}{q^2}\sum_{|\ell|<q/S}\left(\frac{q}{S}-|\ell|\right)\tilde{\varphi}_R\left(\frac{\ell S}{qR}\right),$$

c'est-à-dire le membre de droite de (19). □

Lorsque $S<q$, le membre de droite de (19) est strictement inférieur à RS car dans ce cas il existe des valeurs de ℓ telles que $1\leqslant|\ell|<q/S$, et pour ces valeurs de ℓ on a $\tilde{\varphi}_R\left(\frac{\ell S}{qR}\right)<R$. En revanche, lorsque $S=q$, le majorant dans (19) vaut Rq et la majoration est donc triviale. Il est donc nécessaire d'obtenir une majoration plus précise dans ce cas. C'est l'objet du résultat suivant.

Lemme 6. *Pour tout nombre entier $R \geqslant 2$ tel que $R \mid q$ et tout $t \in \mathbb{R}$ on a*

$$\Psi^2(t,R,q) \leqslant Rq\ (1-\Theta(f)) \tag{22}$$

où

$$\Theta(f) = \left(1-\frac{1}{q}\right)\left\{1-\left(1-\frac{2}{q^2(q-1)}\sum_{k=1}^{q-1}\left|\sum_{j=0}^{q-1-k}\mathrm{e}(\alpha_j-\alpha_{j+k})\right|^2\right)^{1/2}\right\}$$

vérifie

$$\Theta_q := \min_{f\in\mathcal{F}}\Theta(f) \geqslant \left(1-\tfrac{1}{q}\right)\left\{1-\left(1-\tfrac{2}{q^2(q-1)}\right)^{1/2}\right\} > \frac{1}{q^3} > 0. \tag{23}$$

Démonstration. En appliquant l'inégalité de Cauchy-Schwarz à la somme en r dans l'expression (18) de $\Psi(t,R,S)$, on obtient

$$\begin{aligned}\Psi^2(t,R,q) &= \frac{1}{q^4}\left(\sum_{r<R}\varphi\Big(\frac{t+r}{R}\Big)\sum_{s<q}\varphi\Big(\frac{t+r}{qR}+\frac{s}{q}\Big)\right)^2\\ &\leqslant \frac{1}{q^4}\sum_{r<R}\varphi\Big(\frac{t+r}{R}\Big)^2\sum_{r<R}\Big(\sum_{s<q}\varphi\Big(\frac{t+r}{qR}+\frac{s}{q}\Big)\Big)^2\\ &\leqslant \frac{1}{q^2}\sum_{r<R}\Big(\sum_{s<q}\varphi\Big(\frac{t+r}{qR}+\frac{s}{q}\Big)\Big)^2,\end{aligned}$$

où la dernière égalité provient de (21). Cela donne, vu que φ est périodique de période 1,

$$\Psi^2(t,R,q) \leqslant \frac{1}{q^2}\sum_{r=0}^{R-1}\sum_{k=0}^{q-1}\sum_{\ell=0}^{q-1}\varphi\left(\frac{t+r}{qR}+\frac{k}{q}\right)\varphi\left(\frac{t+r}{qR}+\frac{k}{q}+\frac{\ell}{q}\right).$$

La contribution du terme $\ell = 0$ est d'après (20) :

$$\frac{1}{q^2}\sum_{r=0}^{R-1}\sum_{k=0}^{q-1}\varphi^2\left(\frac{t+r}{qR}+\frac{k}{q}\right) = R.$$

On isole ce terme $\ell = 0$ dans la majoration de $\Psi^2(t,R,q)$ ci-dessus et on applique l'inégalité de Cauchy-Schwarz à la triple somme en r, k et ℓ :

$$\Psi^2(t,R,q) \leqslant R + \frac{1}{q^2}\left(Rq(q-1)\sum_{r=0}^{R-1}\sum_{k=0}^{q-1}\sum_{\ell=1}^{q-1}\varphi^2\left(\frac{t+r}{qR}+\frac{k}{q}\right)\varphi^2\left(\frac{t+r}{qR}+\frac{k}{q}+\frac{\ell}{q}\right)\right)^{1/2}. \tag{24}$$

La triple somme dans la parenthèse vaut

$$\sum_{r=0}^{R-1}\sum_{k=0}^{q-1}\sum_{\ell=0}^{q-1}\varphi^2\left(\frac{t+r}{qR}+\frac{k}{q}\right)\varphi^2\left(\frac{t+r}{qR}+\frac{k}{q}+\frac{\ell}{q}\right) - \sum_{r=0}^{R-1}\sum_{k=0}^{q-1}\varphi^4\left(\frac{t+r}{qR}+\frac{k}{q}\right), \tag{25}$$

c'est-à-dire, d'après (20),

$$Rq^4 - \sum_{\ell=0}^{qR-1}\varphi^4\left(\frac{t+\ell}{qR}\right).$$

Or d'après le lemme 3 appliqué à la fonction φ, $\varphi^2(t)$ est un polynôme trigonométrique de degré $q-1$ qui vérifie pour tout nombre entier $N \geqslant 2q-1$,

$$\frac{1}{N}\sum_{n=0}^{N-1}\varphi^4\left(t+\frac{n}{N}\right) = \sum_{|k|\leqslant q-1}\left|\sum_j \mathrm{e}(\alpha_j-\alpha_{j+k})\right|^2. \tag{26}$$

Donc, comme $qR \geqslant 2q-1$ (car $R \geqslant 2$), la quantité (25) vaut

$$Rq^4 - Rq \sum_{|k|\leqslant q-1} \left| \sum_j \mathrm{e}(\alpha_j - \alpha_{j+k}) \right|^2,$$

ou encore, en isolant le terme $k=0$ et en exploitant la symétrie entre $-k$ et k :

$$Rq^4 - Rq^3 - 2\,Rq \sum_{k=1}^{q-1} \left| \sum_{j=0}^{q-1-k} \mathrm{e}(\alpha_j - \alpha_{j+k}) \right|^2,$$

ce qui, en mettant $Rq^3(q-1)$ en facteur et en reportant dans (24), donne

$$\Psi^2(t,R,q) \leqslant R + R(q-1)\left(1 - \frac{2}{q^2(q-1)} \sum_{k=1}^{q-1} \left| \sum_{j=0}^{q-1-k} \mathrm{e}(\alpha_j - \alpha_{j+k}) \right|^2 \right)^{1/2}$$

et fournit bien (22).

La minoration (23) s'obtient en ne conservant dans la définition de $\Theta(f)$ que le terme $k=q-1$ dans la sommation sur k. □

Introduisons la quantité

$$\eta_q = \max\left(\frac{1}{2} - \frac{\log(4-2\sqrt{2})}{4\log q - 2\log 2}, \frac{1}{2} + \frac{\log(1-\Theta_q)}{4\log q} \right). \tag{27}$$

En remarquant que $0 < \Theta_q < 1$, on a

$$\frac{1}{2} + \frac{\log(1-\Theta_q)}{4\log q} < \frac{1}{2}$$

et

$$0,38577665 < \frac{1}{2} - \frac{\log(4-2\sqrt{2})}{2\log 2} \leqslant \frac{1}{2} - \frac{\log(4-2\sqrt{2})}{4\log q - 2\log 2} < \frac{1}{2},$$

d'où

$$0,38577665 < \eta_q < \frac{1}{2}. \tag{28}$$

Nous sommes maintenant en mesure d'établir le résultat suivant.

Lemme 7. *On a pour $t \in \mathbb{R}$, $R \mid q$, $S \mid q$ et $R, S \geqslant 2$,*

$$\Psi(t,R,S) \leqslant (RS)^{\eta_q}. \tag{29}$$

Démonstration. Lorsque $S < q$, nous employons le lemme 5 :

$$\Psi^2(t,R,q) \leqslant \frac{S^2}{q} \sum_{|\ell|<q/S} \left(1 - \frac{S\,|\ell|}{q}\right) \tilde{\varphi}_R\left(\frac{\ell S}{qR}\right).$$

En appliquant le lemme 4 avec $L = q/S$, on obtient, pour $R \geqslant 2$, $S \mid q$, $S < q$ (et donc $S \leqslant q/2$ et $L \geqslant 2$),

$$\Psi(t,R,S)^2 \leqslant (RS)^{1-\frac{\log(4-2\sqrt{2})}{\log RS}},$$

et par suite, comme $RS \leqslant q^2/2$,

$$\Psi(t,R,S) \leqslant (RS)^{\frac{1}{2}-\frac{\log(4-2\sqrt{2})}{4\log q - 2\log 2}} \quad (S<q). \tag{30}$$

Lorsque $S = q$, on emploie (22) et (23), ce qui entraîne

$$\Psi^2(t,R,q) \leqslant Rq\,(1-\Theta_q) = (Rq)^{1+\frac{\log(1-\Theta_q)}{\log(Rq)}}$$

et par suite, comme $R \leqslant q$ et $\log(1-\Theta_q) < 0$,

$$\Psi(t,R,q) \leqslant (Rq)^{\frac{1}{2}+\frac{\log(1-\Theta_q)}{4\log q}} \tag{31}$$

Les deux inégalités (30) et (31) entraînent bien (29). □

La proposition suivante généralise les lemmes 17 et 18 de [29].

Proposition 1. *Pour $\lambda \in \mathbb{N}$, $a \in \mathbb{Z}$, $0 \leqslant \delta \leqslant \lambda$, $k \in \mathbb{N}^*$, $k | q^{\lambda-\delta}$, $q \nmid k$, on a*

$$\sum_{\substack{0\leqslant h<q^\lambda \\ h\equiv a \bmod kq^\delta}} |F_\lambda(h)| \leqslant k^{-\eta_q} q^{\eta_q(\lambda-\delta)+1} |F_\delta(a)|. \tag{32}$$

En particulier, pour $k=1$, $\delta=0$, on a

$$\sum_{0\leqslant h<q^\lambda} \big|F_\lambda(h)\big| \leqslant q^{\eta_q\lambda+1}. \tag{33}$$

Démonstration. Si $\lambda = \delta$, la condition $k \mid q^{\lambda-\delta}$ entraîne $k=1$ et le membre de gauche de (32) qui vaut $|F_\delta(a)|$ est bien inférieur au membre droite qui vaut lui $q|F_\delta(a)|$. Lorsque $\lambda > \delta$ nous reprenons les notations introduites dans la preuve du lemme 17 de [29] : on pose pour $\delta \leqslant \theta \leqslant \lambda$, $d_\theta = \operatorname{pgcd}(q^\theta, kq^\delta)$, $u_\theta = q^\theta/d_\theta$, et pour $\delta < \theta \leqslant \lambda$, $\rho_\theta = d_\theta/d_{\theta-1} \in \mathbb{N}$. Rappelons que l'on a alors

$$\rho_\theta \mid q \quad \text{et} \quad \rho_\theta < q, \tag{34}$$

et que par ailleurs

$$\operatorname{pgcd}(\rho_\theta, u_{\theta-1}) = 1 \quad (\delta < \theta \leqslant \lambda). \tag{35}$$

Enfin nous posons

$$G_\theta(a,d_\theta) = \sum_{\substack{0\leqslant h<q^\theta \\ h\equiv a \bmod d_\theta}} |F_\theta(h)| = \sum_{0\leqslant u<u_\theta} |F_\theta(a+ud_\theta)| \quad (\delta \leqslant \theta \leqslant \lambda). \tag{36}$$

En écrivant $u = su_{\theta-1} + v$ avec $0 \leqslant s < q/\rho_\theta$ et $0 \leqslant v < u_{\theta-1}$, on a, pour $\delta < \theta \leqslant \lambda$,

$$\begin{aligned} G_\theta(a,d_\theta) &= \sum_{0\leqslant v<u_{\theta-1}} \sum_{0\leqslant s<q/\rho_\theta} |F_\theta(a+vd_\theta+sq^{\theta-1}\rho_\theta)| \\ &= \sum_{0\leqslant v<u_{\theta-1}} \sum_{0\leqslant s<q/\rho_\theta} |F_\theta(a+v\rho_\theta d_{\theta-1}+sq^{\theta-1}\rho_\theta)| \end{aligned} \tag{37}$$

En employant l'écriture (17) de $|F_\theta|$ sous forme de produit, il vient

$$G_\theta(a,d_\theta) = \frac{1}{q} \sum_{0\leqslant v<u_{\theta-1}} |F_{\theta-1}(a+v\rho_\theta d_{\theta-1})| \sum_{0\leqslant s<q/\rho_\theta} \varphi\Big(\frac{a+v\rho_\theta d_{\theta-1}+sq^{\theta-1}\rho_\theta}{q^\theta}\Big).$$

La majoration triviale $\varphi(t) \leqslant q$ fournit donc la majoration

$$G_\theta(a,d_\theta) \leqslant \frac{q}{\rho_\theta} \sum_{0\leqslant v<u_{\theta-1}} |F_{\theta-1}(a+v\rho_\theta d_{\theta-1})|.$$

D'après (35), $v\rho_\theta$ parcourt bijectivement l'ensemble des classes modulo $u_{\theta-1}$ lorsque v varie entre 0 et $u_{\theta-1}$. Et comme la fonction $h \mapsto F_{\theta-1}(a+hd_{\theta-1})$ est $u_{\theta-1}$-périodique, il s'ensuit

$$G_\theta(a,d_\theta) \leqslant \frac{q}{\rho_\theta} G_{\theta-1}(a,d_{\theta-1}). \tag{38}$$

Nous effectuons à présent une seconde itération à partir de (37) : pour $\delta+1<\theta\leqslant\lambda$, en posant $v=ru_{\theta-2}+u$ avec $0\leqslant u<u_{\theta-2}$, $0\leqslant r<q/\rho_{\theta-1}$, on a

$$G_\theta(a,d_\theta)=\sum_{0\leqslant u<u_{\theta-2}}\sum_{s<q/\rho_\theta}\sum_{r<q/\rho_{\theta-1}}|F_\theta(a+u\rho_{\theta-1}d_{\theta-2}+rq^{\theta-2}\rho_{\theta-1}+sq^{\theta-1}\rho_\theta)|.$$

En employant l'écriture de $|F_\theta|$ sous forme de produit, on obtient en posant $R_\theta=q/\rho_\theta$ et $t_\theta=R_{\theta-1}(a+u\rho_{\theta-1}d_{\theta-2})/q^{\theta-1}$,

$$\begin{aligned}&G_\theta(a,d_\theta)\\&=\frac{1}{q^2}\sum_{0\leqslant u<u_{\theta-2}}|F_\theta(a+u\rho_{\theta-1}d_{\theta-2})|\sum_{r<R_{\theta-1}}\sum_{s<R_\theta}\varphi\Big(\frac{t_\theta+r}{R_{\theta-1}}\Big)\varphi\Big(\frac{t_\theta+r}{qR_{\theta-1}}+\frac{s}{R_\theta}\Big)\\&\leqslant\max_{t\in\mathbb{R}}|\Psi(t,R_{\theta-1},R_\theta)|\sum_{0\leqslant u<u_{\theta-2}}|F_{\theta-2}(a+u\rho_{\theta-1}d_{\theta-2})|,\end{aligned}$$

ce qui, comme $\mathrm{pgcd}(\rho_{\theta-1},u_{\theta-2})=1$, entraîne

$$G_\theta(a,d_\theta)\leqslant\max_{t\in\mathbb{R}}|\Psi(t,R_{\theta-1},R_\theta)|G_{\theta-2}(a,d_{\theta-2}).$$

Notons que d'après (34), on a $R_\theta\mid q$ et $R_\theta\geqslant 2$ pour $\delta<\theta\leqslant\lambda$. Par conséquent, d'après le lemme 7 appliqué avec $R=R_{\theta-1}$ et $S=R_\theta$,

$$G_\theta(a,d_\theta)\leqslant\Big(\frac{q^2}{\rho_\theta\rho_{\theta-1}}\Big)^{\eta_q}G_{\theta-2}(a,d_{\theta-2})\quad(\delta+1<\theta\leqslant\lambda).\tag{39}$$

En appliquant l'inégalité (39) $\lfloor(\lambda-\delta)/2\rfloor$ fois, puis éventuellement une fois l'inégalité (38), il vient

$$\sum_{\substack{0\leqslant h<q^\lambda\\ h\equiv a \bmod kq^\delta}}|F_\lambda(h)|=G_\lambda(a,d_\lambda)\leqslant(\rho_\lambda\dots\rho_{\delta+1})^{\eta_q}q^{2\lfloor(\lambda-\delta)/2\rfloor\eta_q+1}G_\delta(a,d_\delta).$$

Compte-tenu des identités

$$\rho_\lambda\dots\rho_{\delta+1}=\frac{d_\lambda}{d_\delta}=\frac{kq^\delta}{q^\delta}=k,$$

et

$$G_\delta(a,d_\delta)=G_\delta(a,q^\delta)=|F_\delta(a)|,$$

nous obtenons bien la majoration (32). □

5.2. **Estimation en norme infinie.**

Posons

$$q^{\gamma_q(f)}=\max_{t\in\mathbb{R}}\sqrt{\varphi(t)\varphi(qt)}.\tag{40}$$

Notons d'emblée qu'avec cette définition on a

$$\max_{h\in\mathbb{Z}}|F_\lambda(h)|\leqslant q^{\lambda(\gamma_q(f)-1)+1}.\tag{41}$$

En effet, cela résulte directement de l'expression (17) de F_λ sous forme de produit et de la suite d'inégalités

$$\prod_{j=1}^{\lambda}\varphi(tq^{-j})\leqslant q\prod_{0\leqslant j\leqslant\lfloor\lambda/2\rfloor}\varphi(tq^{-2j})\varphi(tq^{-2j-1})\leqslant q^{2\gamma_q(f)\lfloor\lambda/2\rfloor+1}\leqslant q^{\lambda\gamma_q(f)+1}\quad(t\in\mathbb{R}).$$

Mauduit et Rivat ont obtenu dans [29, Lemme 20] et [28, Lemme 7] des majorations de $\gamma_q(f)$ dans le cas particulier où $f(n)=\alpha s(n)$ avec $\alpha\in\mathbb{R}$. Nous commençons dans ce paragraphe par fournir une majoration générale de $\gamma_q(f)$ pour $f\in\mathcal{F}$ qui est, compte-tenu du lemme 1, non triviale dès que $f\notin\mathcal{F}_0$. Nous rappelons la définition de $\sigma_q(f)$ en (8).

Lemme 8. *Pour $f \in \mathcal{F}$, on a*

$$\varphi(t) \leqslant q \exp\Big(-\frac{8}{q} \|\alpha_i - \alpha_j - (i-j)t\|^2 \Big) \quad (0 \leqslant i, j < q, t \in \mathbb{R}). \tag{42}$$

De plus,

$$\gamma_q(f) \leqslant 1 - \frac{16}{q^2(q-1)\log q}\sigma_q(f). \tag{43}$$

Démonstration. Lorsque $i = j$, l'inégalité (42) est triviale. Lorsque $i \neq j$ nous avons

$$\begin{aligned}\varphi(t) &= \Big| \mathrm{e}(\alpha_i - it) + \mathrm{e}(\alpha_j - jt) + \sum_{\substack{0\leqslant k<q\\ k\notin\{i,j\}}} \mathrm{e}(\alpha_k - kt)\Big| \\ &\leqslant |\,\mathrm{e}(\alpha_i - it) + \mathrm{e}(\alpha_j - jt)| + q - 2 \\ &= \big|1 + \mathrm{e}\big(\alpha_i - \alpha_j - (i-j)t\big)\big| + q - 2.\end{aligned}$$

Or d'après le lemme 12 de [6], nous disposons de l'inégalité

$$|1 + \mathrm{e}(\beta)| \leqslant 2(1 - 4\|\beta\|^2) \quad (\beta \in \mathbb{R}).$$

Nous obtenons ainsi

$$\begin{aligned}\varphi(t) &\leqslant 2\big(1 - 4\|\alpha_i - \alpha_j - (i-j)t\|^2\big) + q - 2 \\ &= q\Big(1 - \frac{8}{q}\|\alpha_i - \alpha_j - (i-j)t\|^2\Big),\end{aligned}$$

et compte-tenu de l'inégalité de convexité $1 - x \leqslant \exp(-x)$ $(x \in \mathbb{R})$, nous obtenons bien (42). Par ailleurs, en employant l'inégalité (42) pour chaque couple (i, j) avec $0 \leqslant j < i < q$ nous avons

$$\begin{aligned}\varphi(t)^{q(q-1)/2} &\leqslant q^{q(q-1)/2} \exp\Big(-\frac{8}{q} \sum_{0\leqslant j<i<q} \|\alpha_i - \alpha_j - (i-j)t\|^2 \Big) \\ &\leqslant q^{q(q-1)/2} \exp\Big(-\frac{8}{q}\sigma_q(f)\Big).\end{aligned}$$

Cela fournit bien la majoration (43). □

La preuve du Théorème 1 nécessite une majoration spécifique de $\gamma_q(f)$ lorsque $f \in \mathcal{F}_0$. Pour ce faire, nous établissons en premier lieu un lemme technique. Nous introduisons la fonction $g_{q,\theta}$ définie pour $q \geqslant 2$, $\theta \in \mathbb{R}$, par

$$g_{q,\theta}(t) = \|\theta + t\|^2 + \|\theta + qt\|^2 \quad (t \in \mathbb{R}).$$

Lemme 9. *On a pour $q \geqslant 2$, $\theta \in \mathbb{R}$,*

$$\min_{t\in\mathbb{R}} g_{q,\theta}(t) \geqslant \frac{\|(q-1)\theta\|^2}{(q + \sqrt{2} - 1)^2}.$$

Démonstration. Dans ce qui suit on désigne par $\mathrm{d}(x, A)$ la distance, au sens de la valeur absolue, entre un nombre réel x et une partie A de $\mathbb{R}$. Posons $\delta_0 = \mathrm{d}\big((q-1)\theta, \mathbb{Z}\big)$ de sorte que

$$\mathrm{d}\Big(\theta, \frac{1}{q-1}\mathbb{Z}\Big) = \frac{\delta_0}{q-1},$$

et fixons $0 \leqslant \delta \leqslant \delta_0$, un paramètre à fixer ultérieurement.

Si $\|(q-1)t\| \geqslant \delta$, alors en employant l'inégalité $\|u\|^2 + \|u+v\|^2 \geqslant \frac{1}{2}\|v\|^2$ valable pour tous $u, v \in \mathbb{R}$, on obtient

$$g_{q,\theta}(t) \geqslant \frac{1}{2}\delta^2.$$

Si $\|(q-1)t\| < \delta$, cela signifie que $\mathrm{d}\big((q-1)t, \mathbb{Z}\big) < \delta$, soit

$$\mathrm{d}\Big(t, \frac{1}{q-1}\mathbb{Z}\Big) < \frac{\delta}{q-1}.$$

On a alors

$$\mathrm{d}\Big(t+\theta, \frac{1}{q-1}\mathbb{Z}\Big) \geqslant \mathrm{d}\Big(\theta, \frac{1}{q-1}\mathbb{Z}\Big) - \mathrm{d}\Big(t, \frac{1}{q-1}\mathbb{Z}\Big) \geqslant \frac{\delta_0 - \delta}{q-1}.$$

Il suit

$$\mathrm{d}(t+\theta, \mathbb{Z}) \geqslant \frac{\delta_0 - \delta}{q-1},$$

puis

$$g_{q,\theta}(t) \geqslant \frac{(\delta - \delta_0)^2}{(q-1)^2}.$$

Finalement

$$g_{q,\theta}(t) \geqslant \min\Big(\frac{1}{2}\delta^2, \frac{(\delta-\delta_0)^2}{(q-1)^2}\Big) \quad (t \in \mathbb{R}),$$

et en effectuant le choix $\delta = \frac{\delta_0\sqrt{2}}{q+\sqrt{2}-1}$, on parvient à la conclusion souhaitée. □

Nous sommes maintenant en mesure d'établir une majoration de $\gamma_q(f)$, non triviale dès qu'il existe $(i,j) \in \{0,\dots,q-1\}^2$ tel que $(q-1)(\alpha_i - \alpha_j) \notin \mathbb{Z}$.

Lemme 10. *Pour $f \in \mathcal{F}$, on a pour tout $(i,j) \in \{0,\dots,q-1\}^2$,*

$$\gamma_q(f) \leqslant 1 - \frac{4\,\|(q-1)(\alpha_i - \alpha_j)\|^2}{q(q+\sqrt{2}-1)^2 \log q}.$$

Démonstration. D'après la majoration (42) nous avons

$$\varphi(t)\varphi(qt) \leqslant q^2 \exp\Big(-\tfrac{8}{q}\; g_{q,\alpha_i-\alpha_j}\left((j-i)t\right)\Big).$$

L'emploi du lemme 9 fournit alors directement la conclusion souhaitée. □

On en déduit immédiatement lorsque $f \in \mathcal{F}_0$:

Lemme 11. *Pour $f \in \mathcal{F}_0$, on a*

$$\gamma_q(f) \leqslant 1 - \frac{4\,\|(q-1)\theta\|^2}{q(q+\sqrt{2}-1)^2 \log q}. \tag{44}$$

avec $\theta = \alpha_1 - \alpha_0$.

6. Sommes de type I

La majoration des sommes de type I constitue la partie facile de la preuve des théorèmes 1 et 2. La proposition 2 qui fournit une majoration des sommes de type I associées à la somme d'exponentielles (7) *via* la méthode de Vaughan, généralise ainsi la proposition 2 de [29] : la preuve en est d'ailleurs essentiellement identique, au moins une fois le lemme technique 12 établi. Nous la restituons sommairement dans le seul but de montrer comment le terme additionnel βn dans l'exponentielle peut être traité grâce à un argument de périodicité.

Pour $f \in \mathcal{F}$, $\lambda \in \mathbb{N}$, nous introduisons la fonction

$$\Phi_\lambda(t) = \sum_{0 \leqslant \ell < q^\lambda} \mathrm{e}\left(f_\lambda(\ell) + \ell t\right) \quad (t \in \mathbb{R}).$$

Lemme 12. *Pour $\in \mathbb{R}$, $t \in \mathbb{R}$, $N \geqslant 1$, on a*

$$\Big| \sum_{0<n<N} \mathrm{e}\big(f(n)+nt\big)\Big| \leqslant 2(q-1) \sum_{\lambda \leqslant \frac{\log N}{\log q}} \big|\Phi_\lambda(t)\big|.$$

Démonstration. Nous reprenons les notations de la partie 2 de [13] :

$$S_N(x_0, x_1, \dots, x_{q-1}, y) = \sum_{0<n<N} x_0^{|n|_0} x_1^{|n|_1} \dots x_{q-1}^{|n|_{q-1}} y^n,$$

et

$$T_{\nu,N}(x_0, x_1, \dots, x_{q-1}, y) = \sum_{0\leqslant n<N} x_0^{|n|_{\nu,0}} x_1^{|n|_{\nu,1}} \dots x_{q-1}^{|n|_{\nu,q-1}} y^n, \quad (N \geqslant 1, \nu \in \mathbb{N}),$$

où les fonctions $|\cdot|_{\nu,j}$ sont définies en (13), et nous posons

$$S_N = S_N\big(\mathrm{e}(\alpha_0), \mathrm{e}(\alpha_1), \dots, \mathrm{e}(\alpha_{q-1}), \mathrm{e}(t)\big)$$

et

$$T_{\nu,N} = T_{\nu,N}\big(\mathrm{e}(\alpha_0), \mathrm{e}(\alpha_1), \dots, \mathrm{e}(\alpha_{q-1}), \mathrm{e}(t)\big),$$

de sorte que

$$S_N = \sum_{0<n<N} \mathrm{e}\big(f(n)+nt\big)$$

et

$$T_{\nu,q^\nu} = \Phi_\nu(t). \tag{45}$$

Nous pouvons écrire $N = \ell q^\nu + N'$ avec $\nu = \lfloor \log N/\log q \rfloor$, $N' < q^\nu$, $1 \leqslant \ell < q$. Il résulte alors des formules fournies au lemme 2.1 de [13] que

$$\begin{aligned}
\Big| \sum_{0<n<N} \mathrm{e}\big(f(n)+nt\big)\Big| = \big|S_{\ell q^\nu + N'}\big| &\leqslant \big|S_{\ell q^\nu}\big| + \big|T_{\nu,N'}\big| \\
&\leqslant \big|S_{q^\nu}\big| + (\ell-1)\big|T_{\nu,q^\nu}\big| + \big|T_{\nu,N'}\big| \\
&\leqslant (q-1) \sum_{0\leqslant j<\nu} \big|T_{j,q^j}\big| + (\ell-1)\big|T_{\nu,q^\nu}\big| + \big|T_{\nu,N'}\big| \\
&\leqslant (q-1) \sum_{0\leqslant j\leqslant\nu} \big|T_{j,q^j}\big| + \big|T_{\nu,N'}\big|.
\end{aligned} \tag{46}$$

En posant $N' = mq^i + N''$ avec $i = \lfloor \log N'/\log q \rfloor$, $N'' < q^i$, $1 \leqslant m < q$, on a

$$\big|T_{\nu,N'}\big| \leqslant \big|T_{\nu,mq^i}\big| + \big|T_{i,N''}\big| \leqslant (q-1)\big|T_{i,q^i}\big| + \big|T_{i,N''}\big|.$$

En itérant le procédé, on aboutit à

$$\big|T_{\nu,N'}\big| \leqslant (q-1) \sum_{0\leqslant\lambda\leqslant i} \big|T_{\lambda,q^\lambda}\big|. \tag{47}$$

En insérant (47) dans (46) nous obtenons

$$\Big| \sum_{0<n<N} \mathrm{e}\big(f(n)+nt\big)\Big| \leqslant 2(q-1) \sum_{\lambda\leqslant\lfloor \log N/\log q\rfloor} \big|T_{\lambda,q^\lambda}\big|,$$

ce qui, compte tenu de (45), correspond bien à la conclusion attendue. □

Proposition 2. *On a pour $f \in \mathcal{F}$, $x \geqslant 2$, $\beta \in \mathbb{R}$, $1 \leqslant M \leqslant x^{1/3}$,*

$$\sum_{M<m\leqslant 2M} \max_{t\leqslant\frac{x}{m}} \left| \sum_{n\leqslant t} \mathrm{e}\left(f(mn)+\beta mn\right)\right| \ll x^{1-\kappa_q(f)} \log x,$$

la constante implicite ne dépendant que de q, avec

$$\kappa_q(f) := \min\Big(\frac{1}{6}, \frac{1-\gamma_q(f)}{3}\Big).$$

Démonstration. Nous posons

$$T := \sum_{M<m\leqslant 2M} \max_{t\leqslant \frac{x}{m}} \left|\sum_{0\leqslant n\leqslant t} \mathrm{e}\left(f(mn)+\beta mn\right)\right|.$$

Pour $M < m \leqslant 2M$, on a

$$\begin{aligned}\left|\sum_{0\leqslant n\leqslant t} \mathrm{e}\left(f(mn)+\beta mn\right)\right| &= \left|\frac{1}{m}\sum_{0\leqslant k<m}\sum_{0\leqslant \ell\leqslant mt} \mathrm{e}\left(f(\ell)+\ell\Big(\beta+\frac{k}{m}\Big)\right)\right| \\ &\leqslant 2+\frac{1}{M}\sum_{0\leqslant k<m}\left|\sum_{0<\ell<mt} \mathrm{e}\left(f(\ell)+\ell\Big(\beta+\frac{k}{m}\Big)\right)\right|.\end{aligned}$$

En employant le lemme 12 on obtient pour $mt \leqslant x$,

$$\left|\sum_{0<\ell<mt} \mathrm{e}\left(f(\ell)+\ell\Big(\beta+\frac{k}{m}\Big)\right)\right| \leqslant 2(q-1)\sum_{\lambda\leqslant \frac{\log x}{\log q}}\left|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\right|.$$

de sorte que l'on a

$$T \ll M + \frac{1}{M}\sum_{\lambda\leqslant \frac{\log x}{\log q}} S(M,q,\lambda)$$

avec

$$S(M,q,\lambda) := \sum_{M<m\leqslant 2M}\sum_{0\leqslant k<m}\left|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\right|. \tag{48}$$

En organisant la somme du membre de gauche de (48) selon la valeur de $d = \mathrm{pgcd}(k,m)$, on a

$$S(M,q,\lambda) = \sum_{1\leqslant d\leqslant 2M}\sum_{M<m\leqslant 2M}\sum_{\substack{0\leqslant k<m\\ \mathrm{pgcd}(k,m)=d}}\left|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\right|.$$

Tout comme la fonction F_λ, la fonction Φ_λ admet une écriture sous forme de produit [3] : $|\Phi_\lambda(t)| = \prod_{0\leqslant j<\lambda}\varphi(-q^j t)$. En introduisant pour chaque d fixé un paramètre $\lambda_1 \leqslant \lambda$, on a donc, d'après la définition de $\gamma_q(f)$ en (40),

$$\big|\Phi_\lambda(t)\big| \leqslant \big|\Phi_{\lambda_1}(t)\big| q^{\gamma_q(f)(\lambda-\lambda_1)+1}.$$

Comme de plus les nombres réels k/m sont d^2/M^2 bien espacés, on peut appliquer l'inégalité de Sobolev-Gallagher à la fonction $t\mapsto \Phi_{\lambda_1}(\beta+t)$ et aux nombres k/m, et on obtient

$$\begin{aligned}&\sum_{M<m\leqslant 2M}\sum_{\substack{0\leqslant k<m\\ \mathrm{pgcd}(k,m)=d}}\left|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\right| \\ &\quad\ll q^{\gamma_q(f)(\lambda-\lambda_1)}\sum_{M/2<m\leqslant M}\sum_{\substack{0\leqslant k<m\\ \mathrm{pgcd}(k,m)=d}}\left|\Phi_{\lambda_1}\Big(\beta+\frac{k}{m}\Big)\right| \\ &\quad\ll q^{\gamma_q(f)(\lambda-\lambda_1)}\left(\frac{M^2}{d^2}\int_0^1\big|\Phi_{\lambda_1}(\beta+t)\big|dt+\frac{1}{2}\int_0^1\big|\Phi'_{\lambda_1}(\beta+t)\big|dt\right).\end{aligned}$$

3. On aura remarqué que $\Phi_\lambda(t) = q^\lambda F_\lambda(-q^\lambda t)$.

Comme la fonction Φ_{λ_1} est 1-périodique, on a

$$\begin{aligned}\sum_{M<m\leqslant 2M}\sum_{\substack{0\leqslant k<m\\ \mathrm{pgcd}(k,m)=d}}\Big|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\Big| &\\ \ll\ q^{\gamma_q(f)(\lambda-\lambda_1)}\left(\frac{M^2}{d^2}\int_0^1\big|\Phi_{\lambda_1}(t)\big|dt+\frac{1}{2}\int_0^1\big|\Phi'_{\lambda_1}(t)\big|dt\right).&\end{aligned}$$

En appliquant l'inégalité de Cauchy-Schwarz puis l'égalité de Parseval, on obtient pour $\lambda\in\mathbb{N}$,

$$\int_0^1\big|\Phi_\lambda(t)\big|dt\leqslant\Big(\int_0^1\big|\Phi_\lambda(t)\big|^2dt\Big)^{1/2}=q^{\lambda/2}.$$

Par ailleurs,

$$\big|\Phi'_\lambda(t)\big|\ll\sum_{0\leqslant j<\lambda}q^j\prod_{\substack{0\leqslant i<\lambda\\ i\neq j}}\varphi(-q^it)\ll\sum_{0\leqslant j<\lambda}q^jq^{\lambda-j}\prod_{0\leqslant i<j}\varphi(-q^it)=q^\lambda\sum_{0\leqslant j<\lambda}\Phi_j(t).$$

On a donc

$$\begin{aligned}\sum_{M<m\leqslant 2M}\sum_{\substack{0\leqslant k<m\\ \mathrm{pgcd}(k,m)=d}}\Big|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\Big|&\ll q^{\gamma_q(f)(\lambda-\lambda_1)}\left(\frac{M^2}{d^2}q^{\lambda_1/2}+q^{\lambda_1}\sum_{0\leqslant j<\lambda_1}q^{j/2}\right)\\ &\ll q^{\gamma_q(f)(\lambda-\lambda_1)}\left(\frac{M^2}{d^2}q^{\lambda_1/2}+q^{3\lambda_1/2}\right).\end{aligned}$$

On choisit alors

$$\lambda_1=\min\left(\lambda,\left\lfloor\frac{2\log(M/d)}{\log q}\right\rfloor\right).$$

Compte tenu des inégalités $q^{\lambda_1}\leqslant\min(q^\lambda,M^2/d^2)$, $q^{-\lambda_1}\leqslant\max(q^{-\lambda},qd^2/M^2)$, on obtient

$$\begin{aligned}\sum_{M<m\leqslant 2M}\sum_{\substack{0\leqslant k<m\\ \mathrm{pgcd}(k,m)=d}}\Big|\Phi_\lambda\Big(\beta+\frac{k}{m}\Big)\Big|&\ll\frac{M^2}{d^2}q^{\gamma_q(f)(\lambda-\lambda_1)+\lambda_1/2}\\ &\ll\frac{M^2}{d^2}q^{\lambda/2}+\frac{M^{3-2\gamma_q(f)}}{d^{3-2\gamma_q(f)}}q^{\gamma_q(f)\lambda}\\ &\ll\frac{M^2}{d^2}q^{\lambda/2}+\frac{M^{3-2\gamma_q(f)}}{d}q^{\gamma_q(f)\lambda},\end{aligned}$$

la dernière inégalité résultant du fait que $\gamma_q(f)\leqslant 1$. Il suit

$$S(M,q,\lambda)\ll M^2q^{\lambda/2}+M^{3-2\gamma_q(f)}\log(2M)q^{\gamma_q(f)\lambda},$$

puis

$$T\ll x^{1/2}M+x^{\gamma_q(f)}M^{2-2\gamma_q(f)}\log(2M).$$

Comme $1\leqslant M\leqslant x^{1/3}$, on obtient bien la conclusion souhaitée. □

7. Sommes de type II

Proposition 3. *On a pour tout $f\in\mathcal{F}$, toutes suites de nombres complexes a_m et b_n avec $|a_m|\leqslant 1$, $|b_n|\leqslant 1$, $x\geqslant 2$, $x^{27/82}\leqslant M,N\leqslant x$, $MN\leqslant x$,*

$$\sum_{M<m\leqslant 2M}\sum_{\substack{N<n\leqslant 2N\\ mn\leqslant x}}a_mb_n\,\mathrm{e}\left(f(mn)+\beta mn\right)\ll x^{1-\xi_q(f)}\log x, \tag{49}$$

la constante implicite ne dépendant que de q, avec

$$\xi_q(f) = \frac{1}{20}\min\left(\Big(\frac{1}{2}-\eta_q\Big)\frac{\log 2}{\log q}, 2\big(1-\gamma_q(f)\big)\right). \tag{50}$$

Démonstration. Quitte à intervertir les rôles de m et n, on peut supposer que $M \leqslant N$. Comme les constantes implicites sont autorisées à dépendre de q, la majoration (49) est vraie lorsque $N \leqslant (16q)^2$. Nous supposons donc dans la suite que $N > (16q)^2$. Nous posons

$$S := \sum_{M<m\leqslant 2M}\sum_{\substack{N<n\leqslant 2N\\ mn\leqslant x}} a_m b_n\, \mathrm{e}\left(f(mn)+\beta mn\right) \quad (|a_m|, |b_n| \leqslant 1, M \leqslant N).$$

Notons tout d'abord que d'après l'inégalité de Cauchy-Schwarz,

$$S^2 \ll M \sum_{M<m\leqslant 2M}\Big|\sum_{\substack{N<n\leqslant 2N\\ mn\leqslant x}} b_n\, \mathrm{e}\left(f(mn)+\beta mn\right)\Big|^2.$$

Rappelons l'inégalité de van der Corput (cf. par exemple lemme 4 de [29]) : pour tous nombres complexes $z_1, \dots, z_N$ et $R' \in \mathbb{N}^*$, on a

$$\Big|\sum_{1\leqslant j\leqslant N} z_j\Big|^2 \leqslant \frac{N+R'-1}{R'}\left\{\sum_{1\leqslant j\leqslant N}|z_j|^2 + 2\sum_{1\leqslant r<R'}\Big(1-\frac{r}{R'}\Big)\sum_{1\leqslant j\leqslant N-r}\Re\left(z_{j+r}\overline{z_j}\right)\right\} \tag{51}$$

où $\Re(z)$ désigne la partie réelle de z.

Considérons R un nombre réel tel que

$$4 \leqslant R \leqslant 4N^{1/4}, \tag{52}$$

et que nous fixerons ultérieurement. L'inégalité (51) appliquée aux nombres complexes

$$z_j = b_{N+j}\, \mathrm{e}\left(f(m(N+j))+\beta m(N+j)\right) \mathbb{1}_{m(N+j)\leqslant x},$$

de modules inférieur à 1, et à $R' = \lceil R\rceil$ (le plus petit entier $\geqslant R$) fournit la majoration

$$\begin{aligned}\Big|\sum_{\substack{N<n\leqslant 2N\\ mn\leqslant x}} b_n\, \mathrm{e}\left(f(mn)+\beta mn\right)\Big|^2 &\leqslant \frac{N+R'-1}{R'}\sum_{\substack{N<n\leqslant 2N\\ mn\leqslant x}} 1\\ &\quad +2\,\frac{N+R'-1}{R'}\sum_{1\leqslant r<R'}\big(1-\tfrac{r}{R'}\big)\\ &\qquad \sum_{\substack{N<n\leqslant 2N-r\\ m(n+r)\leqslant x}} \Re\left(b_{n+r}\overline{b_n}\,\mathrm{e}\left(f(m(n+r))-f(mn)+\beta mr\right)\right).\end{aligned} \tag{53}$$

En sommant sur m l'inégalité (53), puis en intervertissant les sommations, et enfin en observant que $\frac{N+R'-1}{R'} \leqslant \frac{N+R}{R}$, $R \leqslant N$ et que la condition $r < R' = \lceil R\rceil$ équivaut à la condition $r < R$ pour r entier, nous obtenons la majoration

$$S^2 \ll \frac{N^2M^2}{R} + MN\max_{1\leqslant r<R}\sum_{N<n\leqslant 2N}\left|\sum_{\substack{M<m\leqslant 2M\\ m(n+r)\leqslant x}}\mathrm{e}\Big(f\big(m(n+r)\big)-f(mn)+mr\beta\Big)\right|. \tag{54}$$

Le paramètre R ayant vocation à être choisi relativement petit par rapport à M et N, la quantité mr est petite devant mn et l'addition de mr ne va donc pas changer les chiffres de mn de poids supérieurs à un certain paramètre λ, sauf dans certains cas relativement rares. De sorte que

l'on peut espérer remplacer dans (54) la fonction f par la fonction tronquée f_λ définie en (14) au prix d'une erreur dont la contribution à S^2 est $o((MN)^2)$. Cet argument a été développé et explicitement mis en forme dans le lemme 5 de [29]. Nous le formalisons ici sous une forme légèrement différente, en y incorporant le raffinement obtenu au lemme 3.4 de [14].

Désormais nous désignons par λ l'unique nombre entier tel que $q^{\lambda-1} \leqslant MR^2 < q^\lambda$. Notons que cela entraîne que $q^\lambda \leqslant qMR^2 \leqslant 16qMN^{1/2} \leqslant MN$. Lorsque $k, b \in \mathbb{N}^*$ et $kq^\lambda \leqslant b < (k+1)q^\lambda$, on a

$$|b|_j = |k|_j + |b|_{\lambda,j} \quad (0 \leqslant j < q).$$

Par conséquent, sous la condition $kq^\lambda \leqslant mn < m(n+r) < (k+1)q^\lambda$, ce qui revient à dire que les chiffres de mn et $m(n+r)$ de poids supérieur à λ sont les mêmes, nous avons

$$f\big(m(n+r)\big) - f(mn) = f_\lambda\big(m(n+r)\big) - f_\lambda(mn).$$

Nous devons donc montrer que la contribution à la somme figurant dans (54) des couples (m,n) avec $M < m \leqslant 2M$, $N < n \leqslant 2N$ pour lesquels il existe $k \in \mathbb{N}^*$ tel que

$$mn < kq^\lambda \leqslant m(n+r) \tag{55}$$

est relativement petite. Comme $mr \leqslant 2MR < q^\lambda/2$, et par suite, $0 < mr/q^\lambda < 1$, la condition (55) est équivalente à $\{mn/q^\lambda\} \geqslant 1 - mr/q^\lambda$. On a donc

$$\begin{aligned}
&\sum_{N<n\leqslant 2N} \Bigg| \sum_{\substack{M<m\leqslant 2M\\ m(n+r)\leqslant x}} \mathrm{e}\Big(f\big(m(n+r)\big) - f(mn) + mr\beta\Big)\Bigg| \\
&\quad = \sum_{N<n\leqslant 2N} \Bigg| \sum_{\substack{M<m\leqslant 2M\\ m(n+r)\leqslant x}} \mathrm{e}\Big(f_\lambda\big(m(n+r)\big) - f_\lambda(mn) + mr\beta\Big)\Bigg| \\
&\qquad + O\Big(\sum_{n\leqslant 2N} \sum_{\substack{m\leqslant 2M\\ \{mn/q^\lambda\}\geqslant 1-mr/q^\lambda}} 1\Big).
\end{aligned}$$

Or,

$$\begin{aligned}
\sum_{n\leqslant 2N} \sum_{\substack{m\leqslant 2M\\ \{mn/q^\lambda\}\geqslant 1-mr/q^\lambda}} 1 &\leqslant \sum_{n\leqslant 2N} \sum_{\substack{m\leqslant 2M\\ \{mn/q^\lambda\}\geqslant 1-2MR/q^\lambda}} 1 \\
&\leqslant \sum_{k\leqslant 4MN} \tau(k) \mathbb{1}_{\{k/q^\lambda\}\geqslant 1-2MR/q^\lambda} \\
&\leqslant \sum_{0\leqslant j\leqslant 4MN/q^\lambda} \sum_{jq^\lambda\leqslant k<(j+1)q^\lambda} \tau(k) \mathbb{1}_{\{k/q^\lambda\}\geqslant 1-2MR/q^\lambda} \\
&= \sum_{0\leqslant j\leqslant 4MN/q^\lambda} \sum_{(j+1)q^\lambda - 2MR\leqslant k<(j+1)q^\lambda} \tau(k).
\end{aligned}$$

D'après le lemme 3.5 de [14] on a uniformément pour $x^{27/82} \leqslant y \leqslant x$:

$$\sum_{x-y\leqslant n\leqslant x} \tau(n) \ll y \log x.$$

Ici on a

$$\big((j+1)q^\lambda\big)^{27/82} \leqslant \big(4MN + q^\lambda\big)^{27/82} \leqslant (5x)^{27/82} \leqslant 2MR \leqslant MR^2 \leqslant q^\lambda \leqslant (j+1)q^\lambda$$

et nous obtenons,

$$\sum_{n\leqslant 2N}\sum_{\substack{m\leqslant 2M\\ \{mn/q^\lambda\}\geqslant 1-mr/q^\lambda}} 1 \ll MR\sum_{0\leqslant j\leqslant 4MN/q^\lambda}\log\big((j+1)q^\lambda\big)$$
$$\ll (\log x)MR\Big(\frac{MN}{q^\lambda}+1\Big)\ll (\log x)\frac{MN}{R}.$$

Ainsi,

$$S^2\ll (\log x)\frac{N^2M^2}{R}+MN\max_{1\leqslant r\leqslant R}S_2(r,M,N,\lambda), \tag{56}$$

avec

$$S_2(r,M,N,\lambda):=\sum_{N<n\leqslant 2N}\Bigg|\sum_{\substack{M<m\leqslant 2M\\ m(n+r)\leqslant x}}\mathrm{e}\Big(f_\lambda\big(m(n+r)\big)-f_\lambda(mn)+mr\beta\Big)\Bigg|.$$

Rappelant la définition de F_λ en (16), nous avons d'après la formule d'inversion de la transformée de Fourier discrète,

$$\mathrm{e}(f_\lambda(n))=\sum_{0\leqslant h<q^\lambda}F_\lambda(h)\,\mathrm{e}\big(nh/q^\lambda\big).$$

Nous en déduisons l'identité

$$\sum_{\substack{M<m\leqslant 2M\\ m(n+r)\leqslant x}}\mathrm{e}\Big(f_\lambda\big(m(n+r)\big)-f_\lambda(mn)+mr\beta\Big)$$
$$=\sum_{0\leqslant h,k<q^\lambda}F_\lambda(h)\overline{F_\lambda(-k)}\sum_{\substack{M<m\leqslant 2M\\ m(n+r)\leqslant x}}\mathrm{e}\Big(\frac{m\big((h+k)n+hr\big)}{q^\lambda}+mr\beta\Big). \tag{57}$$

En insérant (57) dans (7) puis en effectuant la somme géométrique sur m nous obtenons

$$S_2\leqslant\sum_{0\leqslant h,k<q^\lambda}|F_\lambda(h)||F_\lambda(-k)|\sum_{N<n\leqslant 2N}\min\left(M,\frac{1}{\Big|\sin\pi\frac{(h+k)n+hr+r\beta q^\lambda}{q^\lambda}\Big|}\right).$$

Nous employons alors le lemme suivant qui découle directement du lemme 6 de [29].

Lemme 13. *Soient $a,m\in\mathbb{Z}$ avec $m\geqslant 1$ et $d=\mathrm{pgcd}(a,m)$. Soit $b\in\mathbb{R}$. Pour tout réel $M>0$, on a*

$$\sum_{0\leqslant n\leqslant m-1}\min\left(M,\frac{1}{\Big|\sin\pi\frac{an+b}{m}\Big|}\right)\ll d\min\left(M,\frac{1}{\sin\pi\frac{d}{m}\,\big\|\frac{b}{d}\big\|}\right)+m\log m.$$

Nous découpons ainsi l'intervalle $]N;2N]$ en un nombre $\ll 1+N/q^\lambda$ d'intervalles de longueur q^λ, et nous organisons les sommes en h et k suivant les valeurs de $\mathrm{pgcd}(h+k,q^\lambda)$ de sorte que

$$S_2\ll\Big(1+\frac{N}{q^\lambda}\Big)\Big(S_3^{(1)}+S_3^{(2)}\Big)$$

avec

$$S_3^{(1)}:=\sum_{d|q^\lambda}d\sum_{\substack{0\leqslant h,k<q^\lambda\\ \mathrm{pgcd}(h+k,q^\lambda)=d}}|F_\lambda(h)||F_\lambda(-k)|\min\left(M,\frac{1}{\sin\pi\frac{d}{q^\lambda}\,\Big\|\frac{hr+q^\lambda\beta r}{d}\Big\|}\right)$$

et

$$S_3^{(2)}:=q^\lambda\log q^\lambda\sum_{0\leqslant h,k<q^\lambda}|F_\lambda(h)||F_\lambda(-k)|.$$

Pour estimer $S_3^{(2)}$, nous employons l'inégalité (33) :

$$S_3^{(2)} \ll (\log N) q^\lambda \Big(\sum_{0 \leqslant h < q^\lambda} |F_\lambda(h)| \Big)^2 \ll (\log x) q^{(1+2\eta_q)\lambda}. \tag{58}$$

Pour estimer $S_3^{(1)}$, nous commençons par remplaçer la condition $\operatorname{pgcd}(h+k, q^\lambda) = d$ par la condition plus faible ($h \equiv a \bmod d$ et $k \equiv -a \bmod d$) avec a parcourant l'ensemble des classes résiduelles modulo d. Nous obtenons ainsi

$$S_3^{(1)} \leqslant \sum_{d \mid q^\lambda} d \sum_{0 \leqslant a < d} \min\left(M, \frac{1}{\sin \pi \frac{d}{q^\lambda} \left\| \frac{ar + q^\lambda \beta r}{d} \right\|} \right) \Bigg(\sum_{\substack{0 \leqslant h < q^\lambda \\ h \equiv a \bmod d}} |F_\lambda(h)| \Bigg)^2.$$

Pour $d \mid q^\lambda$, on note $v_q(d)$ le plus grand entier m tel que $q^m | d$. En employant la Proposition 1 sous la forme

$$\sum_{\substack{0 \leqslant h < q^\lambda \\ h \equiv a \bmod d}} |F_\lambda(h)| \ll \Big(\frac{q^\lambda}{d} \Big)^{\eta_q} \big| F_{v_q(d)}(a) \big| \quad (d \mid q^\lambda),$$

il suit

$$S_3^{(1)} \ll q^{2\eta_q \lambda} \sum_{d \mid q^\lambda} d^{1-2\eta_q} \sum_{0 \leqslant a < d} \big| F_{v_q(d)}(a) \big|^2 \min\left(M, \frac{1}{\sin \pi \frac{d}{q^\lambda} \left\| \frac{ar + q^\lambda \beta r}{d} \right\|} \right).$$

D'après l'inégalité (41), on a

$$S_3^{(1)} \ll q^{2\eta_q \lambda} \sum_{d \mid q^\lambda} d^{1-2\eta_q} q^{(-2+2\gamma_q(f)) v_q(d)} \sum_{0 \leqslant a < d} \min\left(M, \frac{1}{\sin \pi \frac{d}{q^\lambda} \left\| \frac{ar + q^\lambda \beta r}{d} \right\|} \right).$$

La fonction sinus étant concave sur $[0, \pi]$, on a

$$\sin\Big(\pi \frac{d}{q^\lambda} \left\| \frac{ar + q^\lambda \beta r}{d} \right\| \Big) \geqslant \frac{d}{q^\lambda} \sin\Big(\pi \left\| \frac{ar + q^\lambda \beta r}{d} \right\| \Big) = \frac{d}{q^\lambda} \Big| \sin \pi \frac{ar + q^\lambda \beta r}{d} \Big|.$$

Ainsi

$$S_3^{(1)} \ll q^{(1+2\eta_q)\lambda} \sum_{d \mid q^\lambda} d^{-2\eta_q} q^{(-2+2\gamma_q(f)) v_q(d)} \sum_{0 \leqslant a < d} \min\left(\frac{dM}{q^\lambda}, \frac{1}{\Big| \sin \pi \frac{ar + q^\lambda \beta r}{d} \Big|} \right).$$

Nous pouvons alors employer une nouvelle fois le lemme 13 :

$$\begin{aligned} &\sum_{0 \leqslant a < d} \min\left(\frac{dM}{q^\lambda}, \frac{1}{\Big| \sin \pi \frac{ar + q^\lambda \beta r}{d} \Big|} \right) \\ &\quad \ll \quad (r,d) \min\left(\frac{dM}{q^\lambda}, \frac{1}{\sin \pi \frac{\operatorname{pgcd}(r,d)}{d} \left\| \frac{q^\lambda r \beta}{\operatorname{pgcd}(r,d)} \right\|} \right) + d \log d. \end{aligned}$$

Il suffit maintenant de majorer trivialement le minimum par $\frac{dM}{q^\lambda}$ pour obtenir une majoration indépendante de β :

$$\sum_{0 \leqslant a < d} \min\left(\frac{dM}{q^\lambda}, \frac{1}{\Big| \sin \pi \frac{ar + q^\lambda \beta r}{d} \Big|} \right) \ll \frac{rdM}{q^\lambda} + d \log d \ll d \log d,$$

la dernière inégalité résultant du fait que $r \leqslant R$ et $q^\lambda \asymp MR^2$. Ainsi nous avons

$$S_3^{(1)} \ll (\log N) q^{(1+2\eta_q)\lambda} \sum_{d \mid q^\lambda} d^{1-2\eta_q} q^{(-2+2\gamma_q(f)) v_q(d)}.$$

Nous décomposons à présent d sous la forme $d = kq^\delta$ avec $0 \leqslant \delta \leqslant \lambda$, $q \nmid k$, et donc $v_q(d) = \delta$, ce qui entraîne

$$S_3^{(1)} \ll (\log x) q^{(1+2\eta_q)\lambda} \sum_{0\leqslant\delta\leqslant\lambda} q^{\delta(-1+2\gamma_q(f)-2\eta_q)} \sum_{\substack{k\mid q^{\lambda-\delta}\\ q\nmid k}} k^{1-2\eta_q}.$$

Posons

$$0 < w_q = \Big(\frac{1}{2} - \eta_q\Big)\frac{\log 2}{\log q} \leqslant \frac{1}{2} - \eta_q \leqslant \frac{1}{4} \tag{59}$$

(d'après (28)). Comme $\mathrm{pgcd}(k,q)$ est un diviseur strict de q, il en résulte que $(k,q) \leqslant q/2$ et nous en déduisons $k = \mathrm{pgcd}(k, q^{\lambda-\delta}) \leqslant (k,q)^{\lambda-\delta} \leqslant (q/2)^{\lambda-\delta}$. Nous avons donc, en employant la majoration $\tau(n) \ll n^{\omega_q}$,

$$\begin{aligned}\sum_{\substack{k\mid q^{\lambda-\delta}\\ q\nmid k}} k^{1-2\eta_q} &\leqslant \tau(q^{\lambda-\delta})\big(q/2\big)^{(1-2\eta_q)(\lambda-\delta)}\\ &\ll q^{\omega_q(\lambda-\delta)+(1-2\eta_q)(\lambda-\delta)-(1-2\eta_q)\frac{\log 2}{\log q}(\lambda-\delta)}\\ &= q^{-\omega_q(\lambda-\delta)+(1-2\eta_q)(\lambda-\delta)},\end{aligned}$$

d'où

$$S_3^{(1)} \ll (\log x) q^{(2-\omega_q)\lambda} \sum_{0\leqslant\delta\leqslant\lambda} q^{\delta(2\gamma_q(f)-2+\omega_q)} \ll (\log x) q^{(2-\omega_q)\lambda}\big(1 + q^{\lambda(2\gamma_q(f)-2+\omega_q)}\big).$$

Finalement,

$$S_3^{(1)} \ll (\log x)\big(q^{(2-\omega_q)\lambda} + q^{2\gamma_q(f)\lambda}\big). \tag{60}$$

Ainsi, en regroupant les estimations (58) et (60) nous obtenons

$$S_2 \ll (\log x)\Big(1 + \frac{N}{q^\lambda}\Big)\big(q^{(2-\omega_q)\lambda} + q^{2\gamma_q(f)\lambda} + q^{(1+2\eta_q)\lambda}\big).$$

Posons

$$\mu_q(f) = \min\Big(\omega_q, 1-2\eta_q, 2\big(1-\gamma_q(f)\big)\Big) = \min\Big(\omega_q, 2\big(1-\gamma_q(f)\big)\Big).$$

Remarquons que l'on a, d'après (59),

$$0 < \mu_q(f) < \frac{1}{4}. \tag{61}$$

On a ainsi

$$S_2 \ll (\log x)\Big(1 + \frac{N}{q^\lambda}\Big) q^{(2-\mu_q(f))\lambda},$$

d'où, d'après (56),

$$S^2 \ll (\log x)\Big(N^2M^2R^{-1} + NMq^{(2-\mu_q(f))\lambda} + N^2Mq^{(1-\mu_q(f))\lambda}\Big).$$

Comme $q^\lambda \asymp MR^2$, il suit

$$S^2 \ll (\log x)NM\Big(NMR^{-1} + M^{2-\mu_q(f)}R^{4-2\mu_q(f)} + NM^{1-\mu_q(f)}R^{2-2\mu_q(f)}\Big). \tag{62}$$

Il nous faut à présent déterminer R de manière optimale suivant les tailles respectives de M et N. Lorsque

$$M \leqslant N^{1-\frac{2\mu_q(f)}{3}}, \tag{63}$$

nous posons $R = 4M^{\frac{\mu_q(f)}{3-2\mu_q(f)}}$: cette égalité entraîne que les premier et troisième termes de la somme figurant au membre de gauche de (62) sont de même ordre de grandeur. On peut vérifier que pour ce choix, la condition (52) est bien satisfaite. En effet, on a

$$4 \leqslant 4M^{\frac{\mu_q(f)}{3-2\mu_q(f)}} \leqslant 4N^{1/10} \leqslant 4N^{1/4}.$$

Nous obtenons alors

$$S^2 \ll (\log x)NM\Big(NM^{1-\frac{\mu_q(f)}{3-2\mu_q(f)}} + M^{2-\mu_q(f)+\frac{(4-2\mu_q(f))\mu_q(f)}{3-2\mu_q(f)}}\Big). \tag{64}$$

La condition (63) est précisément équivalente au fait que le deuxième terme de la somme figurant dans (64) n'excède pas le premier. Par conséquent,

$$S^2 \ll (\log x)N^2M^{2-2c_1} \quad (M \leqslant N^{1-\frac{2\mu_q(f)}{3}}), \tag{65}$$

avec

$$c_1 = c_1(q,f) = \frac{\mu_q(f)}{6-4\mu_q(f)}.$$

Lorsque

$$N^{1-\frac{2\mu_q(f)}{3}} \leqslant M \leqslant N, \tag{66}$$

nous posons $R = 4N^{\frac{1}{5-2\mu_q(f)}}M^{-\frac{1-\mu_q(f)}{5-2\mu_q(f)}}$: là encore il est facile de constater que la condition (52) est remplie. Ce choix de R entraîne cette fois que les premier et deuxième termes de la somme figurant dans (62) sont de même ordre de grandeur. Sous la condition (66), les premier et troisième termes de la somme figurant dans (62) n'excèdent pas le deuxième. Ainsi

$$S^2 \ll (\log x)N^{2-2c_2}M^{2+2c_2-2c_3} \quad (N^{1-\frac{2\mu_q(f)}{3}} \leqslant M \leqslant N),$$

avec

$$c_2 = c_2(q,f) = \frac{1}{10-4\mu_q(f)} \quad \text{et} \quad c_3 = c_3(q,f) = \frac{\mu_q(f)}{10-4\mu_q(f)}.$$

Notons bien que pour $j = 1,2,3$, nous avons $0 < c_j < 1$ et que par ailleurs, $c_3 < c_2$. Nous obtenons donc la majoration uniforme

$$S \ll \Big(NM^{1-c_1} + N^{1-c_2}M^{1+c_2-c_3}\Big)\log x. \tag{67}$$

Sous les conditions $M \leqslant N \leqslant x$, $MN \leqslant x$ et $M \geqslant x^{27/82}$, qui entraînent d'ailleurs $M \leqslant \sqrt{x}$, on a donc,

$$\begin{aligned} S &\ll \Big(xM^{-c_1} + (MN)^{1-c_2}M^{2c_2-c_3}\Big)\log x \\ &\ll \Big(xM^{-c_1} + x^{1-c_2}(\sqrt{x})^{2c_2-c_3}\Big)\log x \\ &\ll \Big(x^{1-27c_1/82} + x^{1-c_3/2}\Big)\log x \\ &\ll \Big(x^{1-c_4}\log x\Big), \end{aligned}$$

avec $c_4 = \min(27c_1/82, c_3/2)$. Or $c_1 \geqslant \frac{\mu_q(f)}{6}$ et $c_3 \geqslant \frac{\mu_q(f)}{10}$, ce qui implique la majoration

$$S \ll x^{1-\mu_q(f)/20}\log x.$$

Compte-tenu de la définition de $\mu_q(f)$, nous obtenons bien la conclusion souhaitée. □

8. Preuve des théorèmes 1 et 2

Rappelons l'identité de Vaughan pour la fonction de von Mangoldt (cf proposition 3.4 de [23] par exemple) : pour $u \geqslant 1$ et $n \geqslant 1$, on a

$$\Lambda(n) = \Lambda(n)\mathbb{1}_{n\leqslant u}(n) + \sum_{\substack{mk=n\\ k\leqslant u}} \log(m)\mu(k) - \sum_{\substack{mk\ell=n\\ k,\ell\leqslant u}} \mu(k)\Lambda(\ell) + \sum_{\substack{mk\ell=n\\ k,\ell>u}} \mu(k)\Lambda(\ell). \tag{68}$$

Posons à présent $u = x^{27/82}$ de sorte que $u \leqslant x^{1/3}$. Nous déduisons de (68) la décomposition

$$\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\left(f(n)+\beta n\right) = S_0 + S_1 - S_2 + S_3,$$

avec

$$S_0 = \sum_{n\leqslant u} \Lambda(n)\,\mathrm{e}\left(f(n)+\beta n\right),$$

$$S_1 = \sum_{\substack{m\leqslant u\\ mn\leqslant x}} \mu(m)\log(n)\,\mathrm{e}\left(f(mn)+\beta mn\right),$$

$$S_2 = \sum_{\substack{m_1\leqslant u\\ m_2\leqslant u\\ m_1m_2n\leqslant x}} \mu(m_1)\Lambda(m_2)\,\mathrm{e}\left(f(m_1m_2n)+\beta m_1m_2n\right),$$

et

$$S_3 = \sum_{\substack{u<m<x\\ u<n_1<x\\ mn_1n_2\leqslant x}} \mu(m)\Lambda(n_1)\,\mathrm{e}\left(f(mn_1n_2)+\beta mn_1n_2\right).$$

Nous avons classiquement

$$S_0 \ll u.$$

La somme S_1 peut être traitée comme une somme de type I.

$$\begin{aligned} S_1 &= \sum_{m\leqslant u}\mu(m) \sum_{n\leqslant x/m} \mathrm{e}\left(f(mn)+\beta mn\right)\int_1^n \frac{dt}{t}\\ &= \sum_{m\leqslant u}\mu(m)\int_1^x \sum_{t<n\leqslant x/m} \mathrm{e}\left(f(mn)+\beta mn\right)\frac{dt}{t}.\\ &\ll (\log x)\sum_{m\leqslant u}\max_{t\leqslant x/m}\Big|\sum_{t<n\leqslant x/m}\mathrm{e}\left(f(mn)+\beta mn\right)\Big|\\ &\ll (\log x)\sum_{m\leqslant u}\max_{t\leqslant x/m}\Big|\sum_{n<t}\mathrm{e}\left(f(mn)+\beta mn\right)\Big|. \end{aligned}$$

En découpant la sommation en m suivant des intervalles dyadiques, et en employant la Proposition 2, nous obtenons la majoration

$$S_1 \ll x^{1-\kappa_q(f)}(\log x)^3.$$

Pour traiter S_2, nous posons $m = m_1m_2$ de sorte que

$$S_2 = \sum_{m\leqslant u^2}\Big(\sum_{\substack{m_1m_2=m\\ m_1\leqslant u\\ m_2\leqslant u}}\mu(m_1)\Lambda(m_2)\Big)\sum_{mn\leqslant x}\mathrm{e}\left(f(mn)+\beta mn\right).$$

De la majoration

$$\sum_{\substack{m_1m_2=m\\ m_1\leqslant u\\ m_2\leqslant u}}\mu(m_1)\Lambda(m_2) \leqslant \sum_{m_2|m}\Lambda(m_2) = \log m,$$

nous déduisons que

$$\begin{aligned} S_2 &\ll (\log u) \sum_{m\leqslant u^2} \Big| \sum_{n\leqslant x/m} \mathrm{e}\left(f(mn)+\beta mn\right) \Big| \\ &\ll (S_I + S_{II} + u^3)\log x, \end{aligned}$$

avec

$$\begin{aligned} S_I &= \sum_{m\leqslant u} \Big| \sum_{n\leqslant x/m} \mathrm{e}\left(f(mn)+\beta mn\right) \Big| \\ S_{II} &= \sum_{u<m\leqslant u^2} \Big| \sum_{u<n\leqslant x/m} \mathrm{e}\left(f(mn)+\beta mn\right) \Big|. \end{aligned}$$

Nous traitons S_I comme une somme de type I en découpant la sommation sur m suivant des intervalles dyadiques et en appliquant la Proposition 2 :

$$S_I \ll x^{1-\kappa_q(f)}(\log x)^2.$$

Nous traitons S_{II} comme une somme de type II : en découpant les sommations sur m et n suivant des intervalles dyadiques il vient

$$S_{II} \ll (\log x)^2 \sup \left| \sum_{M<m\leqslant 2M} a_m \sum_{\substack{N<n\leqslant 2N \\ mn\leqslant x}} b_n \,\mathrm{e}\left(f(mn)+\beta mn\right) \right|$$

où le supremum est pris sous les contraintes $|a_m|\leqslant 1$, $|b_n|\leqslant 1$ pour tous entiers m et n, $M>u$, $N>u$, $MN\leqslant x$. En appliquant la Proposition 3, nous avons donc

$$S_{II} \ll (\log x)^3 x^{1-\xi_q(f)}.$$

Ainsi

$$S_2 \ll (\log x)^3 \Big(x^{1-\kappa_q(f)} + x^{1-\xi_q(f)} + x^{81/82} \Big).$$

Traitons enfin la somme S_3.

$$S_3 = (\log x) \sum_{u<m\leqslant x/u} \mu(m) \sum_{u<n\leqslant x/m} \Big(\frac{1}{\log x} \sum_{\substack{u<n_1\leqslant x \\ n_1n_2=n}} \Lambda(n_1) \Big) \mathrm{e}\left(f(mn)+\beta mn\right)$$

Nous remarquons que

$$\sum_{\substack{u<n_1\leqslant x \\ n_1n_2=n}} \Lambda(n_1) \leqslant \log n,$$

de sorte que l'on peut réécrire S_3 sous la forme

$$S_3 = (\log x) \sum_{u<m\leqslant x/u} a_m \sum_{u<n\leqslant x/m} b_n \,\mathrm{e}\left(f(mn)+\beta mn\right)$$

avec $|a_m|\leqslant 1$, $|b_n|\leqslant 1$ pour tous entiers m et n. En procédant comme pour S_{II}, nous obtenons donc

$$S_3 \ll (\log x)^4 x^{1-\xi_q(f)}.$$

Finalement, nous avons

$$\sum_{n\leqslant x} \Lambda(n)\,\mathrm{e}\left(f(n)+\beta n\right) \ll (\log x)^4 \Big(x^{1-\kappa_q(f)} + x^{1-\xi_q(f)} + x^{1-1/82} \Big) \ll (\log x)^4 x^{1-\tau_q(f)},$$

avec

$$\begin{aligned}\tau_q(f) &= \min\Big(\kappa_q(f), \xi_q(f), \frac{1}{82}\Big)\\ &= \min\Big(\frac{1}{20}\Big(\frac{1}{2}-\eta_q\Big)\frac{\log 2}{\log q}, \frac{1-\gamma_q(f)}{10}, \frac{1-\gamma_q(f)}{3}, \frac{1}{82}, \frac{1}{6}\Big)\\ &= \min\Big(\frac{1}{20}\Big(\frac{1}{2}-\eta_q\Big)\frac{\log 2}{\log q}, \frac{1-\gamma_q(f)}{10}, \frac{1}{82}\Big).\end{aligned}$$

D'après la majoration (43), on a pour tout $f \in \mathcal{F}$

$$\tau_q(f) \geqslant \min\Big(\frac{1}{20}\Big(\frac{1}{2}-\eta_q\Big)\frac{\log 2}{\log q}, \frac{8\sigma_q(f)}{5q^2(q-1)\log q}, \frac{1}{82}\Big).$$

Comme $\sigma_q(f) \leqslant q(q-1)/8$, nous aboutissons à

$$\tau_q(f) \geqslant c_q\sigma_q(f),$$

avec

$$c_q = \frac{1}{q(q-1)}\min\Big(\frac{2(\frac{1}{2}-\eta_q)\log 2}{5\log q}, \frac{8}{5q\log q}, \frac{4}{41}\Big) > 0$$

ce qui fournit l'énoncé du théorème 2.

De la même manière, lorsque $f \in \mathcal{F}_0$, nous obtenons grâce à la majoration (44) et en tenant du compte du fait que $\|(q-1)\theta\|^2 \leqslant 1/4$,

$$\tau_q(f) \geqslant c_q \|(q-1)\theta\|^2$$

avec

$$c_q = \min\Big(\frac{(\frac{1}{2}-\eta_q)\log 2}{5\log q}, \frac{2}{5q(q+\sqrt{2}-1)^2\log q}, \frac{2}{41}\Big) > 0,$$

ce qui fournit l'énoncé du théorème 1.

9. Applications

Nous présentons dans cette section quelques applications des théorèmes 1 et 2.

Notation 3. *Lorsque d est un nombre entier supérieur ou égal à 2 et a un nombre entier inversible modulo d, on note $i_d(a)$ l'unique entier $b \in \{1, \dots, d-1\}$ tel que $ab \equiv 1 \bmod d$. On prolonge cette notation à $d = 1$, en posant pour tout $a \in \mathbb{Z}$, $i_1(a) = 0$.*

Notation 4. *Pour $q \geqslant 2$, on note $\mathcal{D}$ le sous-ensemble de $\mathbb{R}^q$ des q-uplets $(\alpha_0, \dots, \alpha_{q-1})$ tels que la suite $\alpha_0, \dots, \alpha_{q-1}$ n'est pas une progression arithmétique modulo 1 dont la raison est un multiple entier de $1/(q-1)$.*

Pour établir nos résultats, nous emploierons systématiquement la proposition suivante qui est un corollaire presque immédiat des théorèmes 1 et 2.

Proposition 4. *Soit $q \geqslant 2$, $(\alpha_0, \dots, \alpha_{q-1}) \in \mathbb{R}^q$ et $f = \sum_{0\leqslant k<q}\alpha_k|\cdot|_k \in \mathcal{F}$. Si l'on a $(\alpha_0, \dots, \alpha_{q-1}) \in \mathcal{D}$, alors il existe $\tau_{q,f} > 0$ tel que pour tout $x \geqslant 2$, $\beta \in \mathbb{R}$,*

$$\sum_{p\leqslant x} \mathrm{e}\Big(f(p)+\beta p\Big) \ll (\log x)^3 x^{1-\tau_{q,f}}. \tag{69}$$

Démonstration. En effectuant une intégration par parties standard (voir par exemple le lemme 11 de [29]), on obtient

$$\sum_{p\leqslant x} \mathrm{e}\Big(f(p)+\beta p\Big) \ll \frac{1}{\log x}\max_{t\leqslant x}\Big|\sum_{n\leqslant t}\Lambda(n)\,\mathrm{e}\Big(f(n)+\beta n\Big)\Big| + \sqrt{x} \quad (x\geqslant 2). \tag{70}$$

Si $f\in\mathcal{F}_0$, alors d'après le théorème 1 on a

$$\sum_{n\leqslant t}\Lambda(n)\,\mathrm{e}\Big(f(n)+\beta n\Big) \ll (\log t)^4 x^{1-c_q\|(q-1)\theta\|^2},$$

avec $c_q>0$ et $\theta=\alpha_1-\alpha_0$. Comme $(\alpha_0,\dots,\alpha_{q-1})\in\mathcal{D}$, la raison de la progression arithmétique $(\alpha_0,...,\alpha_{q-1})$ n'est pas un multiple de $1/(q-1)$ et donc $\|(q-1)\theta\|>0$. On peut alors choisir $\tau_{q,f}=\min\Big(\frac{1}{2},c_q\,\|(q-1)\theta\|^2\Big)>0$.

Si $f\notin\mathcal{F}_0$, alors d'après le théorème 2 on a

$$\sum_{n\leqslant t}\Lambda(n)\,\mathrm{e}\Big(f(n)+\beta n\Big) \ll (\log t)^4 t^{1-\sigma_q(f)},$$

avec $\sigma_q(f)>0$ d'après le lemme 1. On peut alors poser $\tau_{q,f}=\min\Big(\frac{1}{2},\sigma_q(f)\Big)>0$. □

Maintenant et dans la suite de cette section nous considérons une fonction g de $\mathcal{F}$ à valeurs dans $\mathbb{Z}$, soit de la forme

$$g=\sum_{0\leqslant k<q} a_k|\cdot|_k \tag{71}$$

avec $a_k\in\mathbb{Z}$ pour $0\leqslant k<q$.

9.1. **Propriétés statistiques de la suite** $(g(p))_{p\in\mathcal{P}}$.

9.1.1. *Équirépartition modulo 1 de la suite* $(\alpha g(p))_{p\in\mathcal{P}}$. Rappelons qu'une suite (u_n) de nombres réels est équirépartie modulo 1 si pour tout intervalle I inclus dans $[0;1]$,

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}\mathbb{1}_{\{u_n\}\in I}=|I|, \tag{72}$$

où $|I|$ désigne la longueur de l'intervalle I. Selon le critère de Weyl, ceci est équivalent à dire que pour tout entier relatif non nul h,

$$\sum_{n\leqslant x}\mathrm{e}(hu_n)=o(x)\quad(x\to\infty).$$

Le résultat suivant généralise le théorème 2 de [29] concernant l'équirépartition modulo 1 de la suite $(\alpha s_q(p))_{p\in\mathcal{P}}$.

Théorème 3. *Soit $q\geqslant 2$, $g=\sum_{0\leqslant k<q}a_k|\cdot|_k$ avec $a_k\in\mathbb{Z}$ pour tout $0\leqslant k<q$ et $\alpha\in\mathbb{R}$. Si la suite $a_0,\dots,a_{q-1}$ est constante alors la suite $(\alpha g(p))_{p\in\mathcal{P}}$ n'est pas équirépartie modulo 1. Dans le cas contraire la suite $(\alpha g(p))_{p\in\mathcal{P}}$ est équirépartie modulo 1 si, et seulement si, $\alpha\in\mathbb{R}\setminus\mathbb{Q}$.*

Démonstration. Supposons tout d'abord que $a_0=a_1=\ldots=a_{q-1}$. Étant donné $\alpha\in\mathbb{R}$, supposons par l'absurde que la suite $(\alpha g(p))_{p\in\mathcal{P}}$ est équirépartie modulo 1 : d'après le critère de Weyl, on a

$$\frac{1}{\pi(x)}\sum_{p<x}\mathrm{e}(\alpha g(p))=o(1)\quad(x\to\infty),$$

et donc, pour $j\in\mathbb{N}^*$,

$$\sum_{q^{j-1}\leqslant p<q^j}\mathrm{e}\big(\alpha g(p)\big)=o\big(\pi(q^j)\big)\quad(j\to\infty).$$

Par ailleurs,

$$\sum_{q^{j-1}\leqslant p<q^j} \mathrm{e}\big(\alpha g(p)\big) = \sum_{q^{j-1}\leqslant p<q^j} \mathrm{e}\left(\alpha a_0 \left\lfloor \frac{\log p}{\log q}\right\rfloor\right)$$
$$= e(\alpha a_0 j)\big(\pi(q^j)-\pi(q^{j-1})\big) + O(1).$$

Comme $e(\alpha a_0 j)\neq 0$, on obtient ainsi

$$\frac{\pi(q^j)-\pi(q^{j-1})}{\pi(q^j)} = o(1) \quad (j\to\infty),$$

une contradiction puisque le théorème des nombres premiers (théorème B) fournit

$$\lim_{j\to\infty} \frac{\pi(q^j)-\pi(q^{j-1})}{\pi(q^j)} = 1-\frac{1}{q}.$$

Traitons à présent le cas où la suite $a_0,\dots,a_{q-1}$ n'est pas constante. Si α est rationnel, alors la suite $(\alpha g(p))_{p\in\mathcal{P}}$ ne comporte qu'un nombre fini de termes modulo 1 et n'est donc pas équirépartie modulo 1. Étant donné $\alpha\in\mathbb{R}\setminus\mathbb{Q}$ et $h\in\mathbb{Z}^*$, supposons par l'absurde que $h\alpha a_0,\dots,h\alpha a_{q-1}$ est une progression arithmétique modulo 1 de raison $\ell/(q-1)$ avec $\ell\in\mathbb{Z}$. Si j est tel que $a_j\neq a_0$, comme

$$h\alpha(a_j-a_0) = \frac{j\ell}{q-1} \mod 1,$$

on aboutit à $h\alpha\in\mathbb{Q}$ ce qui est absurde. Donc $(h\alpha a_0,\dots,h\alpha a_{q-1})\in\mathcal{D}$ et d'après la proposition 4 et le théorème B,

$$\sum_{p\leqslant x} \mathrm{e}\big(\alpha h g(p)\big) = o\big(\pi(x)\big) \quad (h\in\mathbb{Z}^*, x\to\infty).$$

La conclusion résulte alors du critère de Weyl. □

9.1.2. *Répartition dans les progressions arithmétiques de la suite* $(g(p))_{p\in\mathcal{P}}$. Nous étudions ici le comportement asymptotique de la quantité

$$\{p\leqslant x,\ g(p)\equiv b \bmod m\}$$

lorsque x tend vers l'infini, et g est une fonction de la forme (71). Nous établissons d'abord quelques lemmes techniques, puis nous traitons le cas d'une classe particulière de fonctions g avant d'aborder le cas général.

Lemme 14. *Soient $a_0,\dots,a_{q-1}$ des nombres entiers premiers dans leur ensemble, et des nombres entiers m et n avec $m\neq 0$. On a l'implication*

$$m \mid na_k \text{ pour tout } 0\leqslant k\leqslant q-1 \Rightarrow m\mid n.$$

Démonstration. Nous posons $M=\mathrm{pgcd}(m,n)$, $m'=m/M$, $n'=n/M$. La relation $m\mid na_k$ entraîne $m'\mid n'a_k$ et, comme $\mathrm{pgcd}(m',n')=1$, d'après le lemme de Gauss, $m'\mid a_k$. Comme k est arbitraire dans cette dernière relation, et que les $a_0,\dots,a_{q-1}$ sont premiers entre eux, cela entraîne que $m'=1$ et par suite $M=m$ et enfin $m\mid n$. □

Lemme 15. *Soient $a_1,\dots,a_{q-1}$ des nombres entiers premiers dans leur ensemble et $j\in\mathbb{N}$ tel que $\frac{j}{m}(0,a_1,\dots,a_{q-1})\notin\mathcal{D}$. Alors on a*

$$\frac{m}{\mathrm{pgcd}(m,q-1)} \mid j.$$

Démonstration. On a pour tout entier $1 \leqslant k \leqslant q-1$,

$$\frac{j}{m}a_k = \frac{k\ell}{q-1} \bmod 1,$$

avec $\ell \in \mathbb{Z}$ fixé. Cela entraîne que $m \mid (q-1)ja_k$ pour $1 \leqslant k \leqslant q-1$ et d'après le lemme de Gauss,

$$\frac{m}{\operatorname{pgcd}(m, q-1)} \mid ja_k \quad (1 \leqslant k \leqslant q-1).$$

En appliquant le lemme 14, nous obtenons bien la conclusion souhaitée. □

Lemme 16. *Soient $a_1, \ldots, a_{q-1}$ des nombres entiers premiers dans leur ensemble et $r \in \mathbb{N}$ tel que $1 \leqslant r < \operatorname{pgcd}(m, q-1)$ et $\frac{r}{\operatorname{pgcd}(m,q-1)}(0, a_1, \ldots, a_{q-1}) \notin \mathcal{D}$. Il existe $d \mid \operatorname{pgcd}(m, q-1)$ tel que $\operatorname{pgcd}(a_1, d) = 1$ et pour tout $1 \leqslant k < q$,*

$$a_k \equiv a_1 k \bmod d. \tag{73}$$

De plus, on a

$$d \geqslant \frac{\operatorname{pgcd}(m, q-1)}{r}.$$

Démonstration. Comme $\frac{r}{\operatorname{pgcd}(m,q-1)}(a_1, \ldots, a_{q-1}) \notin \mathcal{D}$, il existe $\ell \in \mathbb{Z}$ tel que

$$\frac{r}{\operatorname{pgcd}(m, q-1)}a_k = \frac{k\ell}{q-1} \bmod 1 \quad (1 \leqslant k < q), \tag{74}$$

d'où

$$ra_k = \frac{k\ell}{(q-1)/\operatorname{pgcd}(m, q-1)} \bmod 1 \quad (1 \leqslant k < q).$$

Comme $ra_1 \in \mathbb{Z}$, cela entraîne que $(q-1)/\operatorname{pgcd}(m, q-1)$ divise ℓ et donc qu'il existe $t \in \mathbb{Z}$ tel que

$$\ell = \frac{t(q-1)}{\operatorname{pgcd}(m, q-1)}. \tag{75}$$

Le cas $t = 0$ est à exclure. En effet, cela entraînerait d'après (74) que $\operatorname{pgcd}(m, q-1) \mid ra_k$ pour tout k, et par suite $\operatorname{pgcd}(m, q-1) \mid r$ d'après le lemme 14, ce qui n'est pas possible puisque $1 \leqslant r < \operatorname{pgcd}(m, q-1)$. En insérant (75) dans (74), on obtient

$$\frac{r}{\operatorname{pgcd}(m, q-1)}a_k = \frac{kt}{\operatorname{pgcd}(m, q-1)} \bmod 1 \quad (1 \leqslant k < q),$$

et par suite

$$ra_k \equiv kt \bmod \operatorname{pgcd}(m, q-1) \quad (1 \leqslant k < q). \tag{76}$$

Introduisons à présent $\delta = \operatorname{pgcd}(r, m, q-1)$. En considérant la relation (76) pour $k = 1$, on constate que $\delta \mid t$. On pose alors $r' = r/\delta$, $t' = t/\delta$, $d = \operatorname{pgcd}(m, q-1)/\delta$. Comme r est non nul, les entiers r' et d sont premiers entre eux. En posant $s = i_d(r')$, il vient

$$r'a_k \equiv kt' \bmod d \quad (1 \leqslant k < q),$$

puis

$$a_k \equiv kc \bmod d \quad (1 \leqslant k < q), \tag{77}$$

avec $c = st'$. En considérant (77) pour $k = 1$, il vient $c \equiv a_1 \bmod d$ et nous obtenons bien (73). De plus la relation (73) entraîne directement que $\operatorname{pgcd}(d, a_1)$ divise tous les entiers a_k pour $k \in \{1, \ldots, q-1\}$, et par conséquent $\operatorname{pgcd}(d, a_1) = 1$. Par ailleurs, $d \mid \operatorname{pgcd}(m, q-1)$ et comme $\delta \leqslant r$, on a bien $d \geqslant \operatorname{pgcd}(m, q-1)/r$. □

À présent, nous introduisons la classe $\mathcal{F}^+$ des fonctions g de la forme

$$g = \sum_{1\leqslant k<q} a_k|\cdot|_k \text{ avec } a_1,\dots,a_{q-1}\in\mathbb{Z} \text{ et } \operatorname{pgcd}(a_1,\dots,a_{q-1})=1. \tag{78}$$

La classe $\mathcal{F}^+$ est incluse dans l'ensemble des fonctions fortement q-additives.

Nous rappelons qu'étant donné $m\in\mathbb{Z}$, on dit qu'une suite $(g(p))_{p\in\mathcal{P}}$ est équirépartie modulo m si pour tout $b\in\mathbb{Z}$,

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\operatorname{card}\{p\leqslant x,\, g(p)\equiv b \bmod m\}=\frac{1}{m}.$$

On voit par exemple d'après le théorème A que la suite $(s(p))_{p\in\mathcal{P}}$ est équirépartie modulo m dès que $\operatorname{pgcd}(m,q-1)=1$. En revanche, dès que $\operatorname{pgcd}(m,q-1)>1$, des cas dégénérés apparaissent. Cela est dû au fait pour tout diviseur d de $q-1$, on a (cf lemme 12 de [29] par exemple) pour tout $n\in\mathbb{N}$,

$$s(n)\equiv n \bmod d. \tag{79}$$

La relation (79) peut entraîner un défaut d'équirépartition pour des fonctions distinctes de la somme de chiffres. Considérons à cet égard les exemples suivants. Lorsque $q=5$, $m=2$, $g=|\cdot|_1+|\cdot|_3$, on a pour $b\in\mathbb{Z}$,

$$\begin{aligned} g(p)\equiv b \bmod 2 &\iff |p|_1+2|p|_2+3|p|_3+4|p|_4\equiv b \bmod 2\\ &\iff s(p)\equiv b \bmod 2\\ &\iff p\equiv b \bmod 2, \end{aligned}$$

de sorte que

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\operatorname{card}\{p\leqslant x,\, g(p)\equiv b \bmod 2\}=\begin{cases}1 & \text{si } b \text{ est impair,}\\ 0 & \text{sinon.}\end{cases}$$

Maintenant, lorsque $q=7$, $m=6$, $g=2|\cdot|_1+|\cdot|_2+2|\cdot|_4+|\cdot|_5$, on a d'une part pour $b\in\mathbb{Z}$,

$$g(p)\equiv b \bmod 6 \Longrightarrow 2|p|_1+|p|_2+2|p|_4+|p|_5\equiv b \bmod 3$$

et d'autre part

$$\begin{aligned} 2|p|_1+|p|_2+2|p|_4+|p|_5\equiv b \bmod 3 &\iff 2(|p|_1+2|p|_2+|p|_4+2|p|_5)\equiv b \bmod 3\\ &\iff 2s(p)\equiv b \bmod 3\\ &\iff s(p)\equiv 2b \bmod 3\\ &\iff p\equiv 2b \bmod 3, \end{aligned}$$

et on obtient un cas dégénéré dès que $b\equiv 0 \bmod 3$.

Ces considérations et ces exemples nous conduisent à introduire la définition suivante.

Définition 1. *Étant donnés des entiers $q,m\geqslant 2$ et $g\in\mathcal{F}^+$, on appelle entier caractéristique de g, m et q et on note $d=d_{g,m,q}$, le plus grand diviseur positif de* $\operatorname{pgcd}(m,q-1)$ *tel que pour tout $n\in\mathbb{N}$,*

$$g(n)\equiv g(1)s_q(n)\equiv g(1)n \bmod d. \tag{80}$$

On pose alors

$$\begin{aligned} J_1&=\{0\leqslant j\leqslant m-1,\ \frac{m}{d}\mid j\},\\ J_2&=\{0,1,\dots,m-1\}\setminus J_1. \end{aligned} \tag{81}$$

Notons que l'entier d est bien défini puisque la relation (80) est toujours satisfaite pour $d = 1$. De plus les entiers $g(1)$ et d sont premiers entre eux : d'après la relation (80) appliquée pour $n = 1, 2, \dots, q-1$, le plus grand diviseur commun de $g(1)$ et d divise tous les entiers a_j qui sont supposés premiers entre eux.

Par ailleurs observons que $d = 1$ dès que $\operatorname{pgcd}(m, q-1) = 1$. Enfin, remarquons que (80) est équivalente à

$$a_k \equiv a_1 k \bmod d \quad (1 \leqslant k < q). \tag{82}$$

Proposition 5. *Soit $q, m \geqslant 2$, $g \in \mathcal{F}^+$ et $d = d_{g,m,q}$ l'entier caractéristique défini en (4). Il existe $\sigma_{g,m,q} > 0$ tel que pour $j \in J_2$, $x \geqslant 2$, $\beta \in \mathbb{R}$, on a*

$$\sum_{p \leqslant x} \mathrm{e}\Big(\frac{j}{m} g(p) + \beta p\Big) \ll (\log x)^3 x^{1-\sigma_{g,m,q}}.$$

La constante implicite ne dépend que de q.

Démonstration. Soit $j \in J_2$. Si $\frac{m}{\operatorname{pgcd}(m,q-1)} \nmid j$, alors $\frac{j}{m}(0, a_1, \dots, a_{q-1}) \in \mathcal{D}$ d'après le lemme 15, et donc, d'après la proposition 4, il existe $\tau_{q,\frac{j}{m}g} > 0$ tel que

$$\sum_{p \leqslant x} \mathrm{e}\Big(\frac{j}{m} g(p) + \beta p\Big) \ll (\log x)^3 x^{1-\tau_{q,\frac{j}{m}g}} \quad \Big(\frac{m}{\operatorname{pgcd}(m, q-1)} \nmid j\Big).$$

Si $d = \operatorname{pgcd}(m, q-1)$, la preuve est achevée. Supposons à présent que $d < (m, q-1)$ et que $\frac{m}{\operatorname{pgcd}(m,q-1)} \mid j$: comme de surcroît $\frac{m}{d} \nmid j$, l'entier j peut alors s'écrire sous la forme

$$j = \frac{m}{\operatorname{pgcd}(m, q-1)}\Big(u\frac{\operatorname{pgcd}(m, q-1)}{d} + r\Big),$$

avec $0 \leqslant u < d$ et $1 \leqslant r < \operatorname{pgcd}(m, q-1)/d$. On a donc

$$\begin{aligned}\sum_{p \leqslant x} \mathrm{e}\Big(\frac{j}{m} g(p) + \beta p\Big) &= \sum_{p \leqslant x} \mathrm{e}\left(g(p)\Big(\frac{u}{d} + \frac{r}{\operatorname{pgcd}(m, q-1)}\Big) + \beta p\right) \\ &= \sum_{p \leqslant x} \mathrm{e}\Big(\frac{g(1)pu}{d} + \frac{r g(p)}{\operatorname{pgcd}(m, q-1)} + \beta p\Big),\end{aligned}$$

où la deuxième égalité résulte de (80). Ainsi,

$$\Big|\sum_{p \leqslant x} \mathrm{e}\Big(\frac{j}{m} g(p) + \beta p\Big)\Big| \leqslant \Big|\sum_{p \leqslant x} \mathrm{e}\Big(\frac{r}{\operatorname{pgcd}(m, q-1)} g(p) + \Big(\frac{g(1)u}{d} + \beta\Big)p\Big)\Big|.$$

Supposons par l'absurde que $\frac{r}{\operatorname{pgcd}(m,q-1)}(0, a_1, \dots, a_{q-1}) \notin D$. D'après le lemme 16, il existe $d' | \operatorname{pgcd}(m, q-1)$ tel que $\operatorname{pgcd}(a_1, d') = 1$ et

$$a_k \equiv a_1 k \bmod d', \quad (1 \leqslant k < q),$$

et de plus

$$d' \geqslant \frac{\operatorname{pgcd}(m, q-1)}{r} > d,$$

ce qui contredit la maximalité de d. Par conséquent,

$$\tfrac{r}{\operatorname{pgcd}(m,q-1)}(0, a_1, \dots, a_{q-1}) \in \mathcal{D},$$

et donc, d'après la proposition 4,

$$\sum_{p\leqslant x} \mathrm{e}\Big(\frac{j}{m}g(p)+\Big(\frac{g(1)u}{d}+\beta\Big)p\Big) \ll (\log x)^3 x^{1-\tau_{q,\frac{r}{\mathrm{pgcd}(m,q-1)}g}}, \tag{83}$$

avec $\tau_{q,\frac{r}{\mathrm{pgcd}(m,q-1)}g}>0$. Nous obtenons bien la conclusion souhaitée avec

$$\sigma_{g,m,q}=\min\left(\min_{\frac{m}{\mathrm{pgcd}(m,q-1)}\nmid j}\tau_{q,\frac{j}{m}g},\min_{1\leqslant r<\frac{\mathrm{pgcd}(m,q-1)}{d}}\tau_{q,\frac{r}{\mathrm{pgcd}(m,q-1)}g}\right)>0. \tag{84}$$

□

Nous sommes maintenant en mesure d'établir le résultat principal de ce paragraphe. Conformément à l'usage, $\pi(x;\ell,k)$ désigne le nombre de nombres premiers congrus à ℓ modulo k n'excédant pas x. Le résultat suivant généralise le théorème 3 de [29].

Théorème 4. *Soient $q,m\geqslant 2$, $g\in\mathcal{F}^+$ et $d=d_{g,q,m}$ l'entier caractéristique défini en* (80)*. On pose $c=i_d(g(1))$. On a pour tout $x\geqslant 2$, $b\in\mathbb{Z}$,*

$$\mathrm{card}\{p\leqslant x,\, g(p)\equiv b \bmod m\}=\begin{cases}0 \text{ ou } 1 & \text{si } \mathrm{pgcd}(b,d)>1,\\ \frac{d}{m}\pi(x;bc,d)+O\big((\log x)^3x^{1-\sigma_{g,m,q}}\big) & \text{sinon,}\end{cases} \tag{85}$$

où $\sigma_{g,m,q}>0$ est défini en (84)*, et la constante implicite ne dépend que de q. En particulier la suite $(g(p))_{p\in\mathcal{P}}$ est équirépartie modulo m si, et seulement si, $d=1$.*

Démonstration. On a les inclusions d'ensembles

$$\begin{aligned}\{p\leqslant x,\, g(p)\equiv b \bmod m\}&\subseteq\{p\leqslant x,\, g(p)\equiv b \bmod d\}\subseteq\{p\leqslant x,\, g(1)p\equiv b \bmod d\}\\ &\subseteq\mathrm{card}\{p\leqslant x,\, p\equiv bc \bmod d\}\subseteq\{p\leqslant x,\, \mathrm{pgcd}(b,d)\mid p\},\end{aligned} \tag{86}$$

ce qui implique que l'ensemble $\{p\leqslant x,\, g(p)\equiv b \bmod m\}$ contient au plus un élément dès que $\mathrm{pgcd}(b,d)>1$. Supposons à présent que $\mathrm{pgcd}(b,d)=1$. Nous pouvons écrire la décomposition

$$\mathrm{card}\{p\leqslant x,\, g(p)\equiv b \bmod m\}=S_1+S_2$$

avec

$$S_1=\frac{1}{m}\sum_{j\in J_1}\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big)$$

$$S_2=\frac{1}{m}\sum_{j\in J_2}\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big).$$

D'après la proposition 5 nous avons

$$S_2\ll(\log x)^3x^{1-\sigma_{g,m,q}}.$$

Tout entier $j\in J_1$ est de la forme $j=um/d$ avec $0\leqslant u<d$, d'où

$$S_1=\sum_{p\leqslant x}\sum_{0\leqslant u<d}\mathrm{e}\Big(\frac{u}{d}(g(p)-b)\Big).$$

D'après (80), on obtient

$$S_1=\sum_{p\leqslant x}\sum_{0\leqslant u<d}\mathrm{e}\Big(\frac{u}{d}(g(1)p-b)\Big)=d\sum_{\substack{p\leqslant x\\ g(1)p\equiv b \bmod d}}1=d\pi(x;bc,d),$$

et la preuve est achevée. □

Nous sommes maintenant en mesure d'étudier en toute généralité la quantité

$$\mathrm{card}\{p \leqslant x,\, g(p) \equiv b \bmod m\}.$$

Comme nous allons le voir, il est toujours possible de se ramener au cas où $g \in \mathcal{F}^+$ et d'employer ainsi le théorème 4.

En effet si g est non nulle et fortement q-additive donc de la forme

$$g = \sum_{1 \leqslant k < q} a_k |\cdot|_k,$$

on peut introduire δ le plus grand diviseur commun des entiers $a_1, \ldots, a_{q-1}$ puis la fonction $\widetilde{g}$ définie par $g = \delta\widetilde{g}$. Les coefficients $\widetilde{g}(1) = \widetilde{a_1}, \ldots, \widetilde{g}(q-1) = \widetilde{a_{q-1}}$ sont premiers dans leur ensemble, et donc $\widetilde{g} \in \mathcal{F}^+$. Par ailleurs, la relation de congruence $g(p) \equiv b \bmod m$ est équivalente à une relation du type $\widetilde{g}(p) \equiv \widetilde{b} \bmod \widetilde{m}$ avec $\widetilde{m}, \widetilde{b} \in \mathbb{Z}$.

Plus généralement, si g est une fonction de la forme

$$g = \sum_{0 \leqslant k < q} a_k |\cdot|_k,$$

on peut introduire la fonction g_0 fortement q-additive définie par

$$g_0 = \sum_{1 \leqslant k < q} (a_k - a_0) |\cdot|_k,$$

et on a alors

$$\begin{aligned} g(n) &= a_0(|n|_0 + \ldots + |n|_{q-1}) + g_0(n) \\ &= a_0\big(\lfloor \log_q n \rfloor + 1\big) + g_0(n). \end{aligned}$$

Et en se ramenant au cas précédent, on peut évaluer le nombre de nombres premiers p d'un intervalle de la forme $[q^{j-1}, q^j[$ satisfaisant à $g(p) \equiv b \bmod m$. En effet, avec ces notations,

$$\mathrm{card}\{q^{j-1} \leqslant p < q^j,\, g(p) \equiv b \bmod m\} = \mathrm{card}\{q^{j-1} \leqslant p < q^j,\, g_0(p) \equiv b - a_0 j \bmod m\}. \tag{87}$$

Suivant les valeurs de j, la quantité (87) peut valoir 0, 1 ou alors approximativement $c\big(\pi(q^j) - \pi(q^{j-1})\big)$ où c est une constante qui ne dépend ni de j, ni de b. De sorte qu'il existe des cas pour lesquels la limite

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \mathrm{card}\{p \leqslant x,\, g(p) \equiv b \bmod m\}$$

existe, d'autres pour lesquels elle n'existe pas. À titre d'illustration, nous présentons deux exemples.

Lorsque $q = 3$, $m = 4$, $g = 2|\cdot|_0 + |\cdot|_1$, on a pour $j \in \mathbb{N}^*$, $q^{j-1} \leqslant x < q^j$,

$$\{q^{j-1} \leqslant p < x,\, g(p) \equiv 1 \bmod 4\} = \{q^{j-1} \leqslant p < x,\, |p|_1 \equiv 1 - 2j \bmod 4\}.$$

L'entier caractéristique de $q = 3$, $m = 4$ et $n \mapsto |n|_1$ vaut 2. Donc en appliquant le théorème 4, nous obtenons,

$$\mathrm{card}\{q^{j-1} \leqslant p < x,\, g(p) \equiv 1 \bmod 4\} = \frac{\pi(x) - \pi(q^{j-1})}{2} + O\big((\log x)^3 x^{1-\sigma_{g,m,q}}\big) \tag{88}$$

et ainsi,

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \mathrm{card}\{p \leqslant x,\, 2|p|_0 + |p|_1 \equiv 1 \bmod 4\} = \frac{1}{2}.$$

Toujours avec $q = 3$, $m = 4$, on a maintenant pour $g = |\cdot|_0 + |\cdot|_1$, $j \in \mathbb{N}^*$, $q^{j-1} \leqslant x < q^j$,

$$\{q^{j-1} \leqslant p < x,\, g(p) \equiv 1 \bmod 4\} = \{q^{j-1} \leqslant p < x,\, |p|_1 \equiv 1 - j \bmod 4\},$$

et nous obtenons,

$$\text{(89)}\qquad \operatorname{card}\{q^{j-1}\leqslant p<x,\ g(p)\equiv 1 \bmod 4\}=\begin{cases}0 \text{ ou } 1 \text{ si } j \text{ est impair,}\\ \frac{\pi(x)-\pi(q^{j-1})}{2}+O\big((\log x)^3x^{1-\sigma_{g,m,q}}\big) \text{ sinon,}\end{cases}$$

de sorte que la quantité

$$\frac{1}{\pi(x)}\operatorname{card}\{p\leqslant x,\ |p|_0+|p|_1\equiv 1 \bmod 4\}$$

n'a pas de limite lorsque $x\to\infty$.

Dans la suite, nous poursuivons notre étude des nombres premiers satisfaisant à une condition du type $g(p)\equiv b \bmod m$. Nous nous restreindrons cependant désormais au cas où $g\in\mathcal{F}^+$: comme nous venons de l'expliquer, on peut toujours se ramener à ce cas, bien que des énoncés tout à la fois maniables et valables en toute généralité semblent difficile à obtenir.

9.2. **Propriétés statistiques de la suite constituée des nombres premiers p tels que $g(p)\equiv b \bmod m$.**

9.2.1. *Équirépartition modulo* 1. Soit $g\in\mathcal{F}^+$. Au vu du théorème 4, la suite des nombres premiers satisfaisant à une relation du type $g(p)\equiv b \bmod m$ ne comporte un nombre infini de termes que si $\operatorname{pgcd}(b,d)>1$, d étant l'entier caractéristique de g, m et q.

Théorème 5. *Soit $q,m\geqslant 2$, $g\in\mathcal{F}^+$, $d=d_{g,m,q}$ l'entier caractéristique défini en* (80)*, $b\in\mathbb{Z}$ tel que $\operatorname{pgcd}(b,d)=1$ et $\alpha\in\mathbb{R}$. La suite $u=(p\alpha)$, où p parcourt l'ensemble des nombres premiers p vérifiant la condition $g(p)\equiv b \bmod m$, est équirépartie modulo 1 si, et seulement si α est un nombre irrationnel.*

Démonstration. Si α est un nombre rationnel, la suite u ne prend qu'un nombre fini de valeurs modulo 1 et n'est donc pas équirépartie modulo 1. Supposons réciproquement que α est irrationnel. D'après le critère de Weyl, il suffit de prouver que pour tout $h\in\mathbb{Z}^*$,

$$\text{(90)}\qquad \frac{1}{\operatorname{card}\{p\leqslant x,\ g(p)\equiv b \bmod m\}}\sum_{\substack{p\leqslant x\\ g(p)\equiv b \bmod m}}\mathrm{e}(h\alpha p)=o\big(1\big)\quad(x\to\infty).$$

La condition $\operatorname{pgcd}(b,d)=1$ entraîne, en vertu du théorème 4 et du théorème B,

$$\text{(91)}\qquad \operatorname{card}\{p\leqslant x,\ g(p)\equiv b \bmod m\}\asymp_{m,q,d}\pi(x).$$

Par ailleurs,

$$\begin{aligned}\Big|\sum_{\substack{p\leqslant x\\ g(p)\equiv b \bmod m}}\mathrm{e}(h\alpha p)\Big|&=\Big|\frac{1}{m}\sum_{j=0}^{m-1}\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}(g(p)-b)+h\alpha p\Big)\Big|\\ &\leqslant\ \frac{1}{m}\sum_{j\in J_1}\Big|\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}g(p)+h\alpha p\Big)\Big|+\frac{1}{m}\sum_{j\in J_2}\Big|\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}g(p)+h\alpha p\Big)\Big|.\end{aligned}$$

D'après la proposition 5, on a

$$\frac{1}{m}\sum_{j\in J_2}\Big|\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}g(p)+h\alpha p\Big)\Big|\ll(\log x)^3x^{1-\sigma_{g,m,q}}.$$

Par ailleurs, si $j \in J_1$ alors $j = um/d$ avec $0 \leqslant u < d$ et d'après (80)

$$\begin{aligned}\sum_{p\leqslant x} \mathrm{e}\Big(\frac{j}{m}g(p) + h\alpha p\Big) &= \sum_{p\leqslant x} \mathrm{e}\Big(\frac{u}{d}g(p) + h\alpha p\Big)\\ &= \sum_{p\leqslant x} \mathrm{e}\Big(\frac{u}{d}g(1)p + h\alpha p\Big)\\ &= \sum_{p\leqslant x} \mathrm{e}\Big(p\Big(\frac{ug(1)}{d} + h\alpha\Big)\Big).\end{aligned}$$

Comme α est un nombre irrationnel, le nombre $\frac{ug(1)}{d}+h\alpha$ l'est également. Or d'après le théorème C et le critère de Weyl, on a

$$\sum_{p\leqslant x} \mathrm{e}\Big(p\big(\tfrac{ug(1)}{d} + h\alpha\big)\Big) = o\big(\pi(x)\big) \quad (x \to \infty), \tag{92}$$

et par suite,

$$\frac{1}{m}\sum_{j\in J_1}\Big|\sum_{p\leqslant x} \mathrm{e}\Big(\frac{j}{m}g(p) + h\alpha p\Big)\Big| = o\big(\pi(x)\big) \quad (x \to \infty). \tag{93}$$

Finalement nous avons

$$\frac{1}{m}\sum_{0\leqslant j<m}\Big|\sum_{p\leqslant x} \mathrm{e}\Big(\frac{j}{m}g(p) + h\alpha p\Big)\Big| = o\big(\pi(x)\big) \quad (x \to \infty), \tag{94}$$

et compte-tenu de (91), nous obtenons bien la relation (90). □

9.2.2. *Répartition dans les progressions arithmétiques.* Nous aurons l'usage d'une version généralisée du théorème des restes chinois (voir [31]).

Lemme 17. *Soit $a_1, a_2 \in \mathbb{Z}$, $n_1, n_2 \in \mathbb{Z}^*$. Le système d'équations*

$$\begin{cases} x \equiv a_1 \bmod n_1\\ x \equiv a_2 \bmod n_2\end{cases}$$

admet une solution si, seulement si, $a_1 \equiv a_2 \bmod \mathrm{pgcd}(n_1, n_2)$. Dans ce cas, la solution est unique modulo $\mathrm{ppcm}(n_1, n_2)$.

Théorème 6. *Soit $q, m \geqslant 2$, $g \in \mathcal{F}^+$, $d = d_{m,q,g}$ l'entier caractéristique défini en* (80). *On pose $c = i_d(g(1))$. On a pour tous $k \geqslant 2$ et $\ell, b \in \mathbb{Z}$,*

$$\begin{aligned}&\mathrm{card}\{p \leqslant x,\, p \equiv \ell \bmod k,\, g(p) \equiv b \bmod m\}\\ &= \begin{cases} 0 & \text{si } \ell \not\equiv bc \bmod \mathrm{pgcd}(k, d)\\ \frac{d}{m}\pi(x; v, \mathrm{ppcm}(k, d)) + O((\log x)^3 x^{1-\sigma_{g,m,q}}) & \text{sinon,}\end{cases}\end{aligned} \tag{95}$$

où $\sigma_{q,m,f} > 0$ est défini en (84), *et v est une solution du système*

$$\begin{cases} v \equiv \ell \bmod k\\ v \equiv bc \bmod d.\end{cases}$$

En particulier, lorsque $d = 1$, on a

$$\mathrm{card}\{p \leqslant x,\, p \equiv \ell \bmod k,\, g(p) \equiv b \bmod m\} = \frac{\pi(x; \ell, k)}{m} + O((\log x)^3 x^{1-\sigma_{g,m,q}}).$$

Démonstration. Notons tout d'abord que d'après (80),

$$\begin{aligned}\{p\leqslant x,\, p\equiv \ell \bmod k,\, g(p)\equiv b \bmod m\} &\subseteq \{p\leqslant x,\, p\equiv \ell \bmod k,\, g(p)\equiv b \bmod d\}\\ &\subseteq \{p\leqslant x,\, p\equiv \ell \bmod k,\, g(1)p\equiv b \bmod d\}\\ &\subseteq \{p\leqslant x,\, p\equiv \ell \bmod k,\, p\equiv bc \bmod d\},\end{aligned}$$

ce qui, d'après le lemme 17, règle le cas $\ell \not\equiv bc \bmod \mathrm{pgcd}(k,d)$. Supposons à présent que l'on a $\ell \equiv bc \bmod \mathrm{pgcd}(k,d)$. Nous avons

$$\begin{aligned}\mathrm{card}\{p\leqslant x,\, p\equiv \ell \bmod k,\, g(p)\equiv b \bmod m\} &= \frac{1}{m}\sum_{0\leqslant j<m}\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big)\\ &= S_1 + O(S_2)\end{aligned}$$

avec

$$S_1 = \frac{1}{m}\sum_{j\in J_1}\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big)$$

$$S_2 = \frac{1}{m}\sum_{j\in J_2}\Big|\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}g(p)\Big)\Big|.$$

Lorsque $j\in J_2$, on a d'après la proposition 5

$$\Big|\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}g(p)\Big)\Big| \leqslant \frac{1}{k}\sum_{0\leqslant n<k}\Big|\sum_{p\leqslant x}\mathrm{e}\Big(\frac{j}{m}g(p)+\frac{n}{k}p\Big)\Big| \ll (\log x)^3 x^{1-\sigma_{g,m,q}},$$

et par suite,

$$S_2 \ll (\log x)^3 x^{1-\sigma_{g,m,q}}.$$

Par ailleurs,

$$S_1 = \frac{1}{m}\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k}}\sum_{0\leqslant u<d}\mathrm{e}\Big(\frac{u}{d}(g(1)p-b)\Big) = \frac{d}{m}\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k\\ g(1)p\equiv b \bmod d}} 1 = \frac{d}{m}\sum_{\substack{p\leqslant x\\ p\equiv \ell \bmod k\\ p\equiv bc \bmod d}} 1,$$

ce qui, compte-tenu du lemme 17 et de la définition de v, fournit bien le résultat escompté. □

9.3. **Problème de Goldbach ternaire avec conditions digitales.**

Notre dernière application concerne une généralisation d'un résultat classique de Vinogradov concernant le problème de Goldbach ternaire (cf. par exemple [11] chapitre 26) : rappelons que pour tout $A>0$ fixé,

$$r(N) := \sum_{\substack{n_1,n_2,n_3\\ n_1+n_2+n_3=N}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) = \frac{1}{2}\mathfrak{S}(N)N^2 + O_A\Big(\frac{N^2}{(\log N)^A}\Big) \quad (N\in\mathbb{N}^*).$$

avec

$$\mathfrak{S}(N) = \prod_{p\mid N}\Big(1-\frac{1}{(p-1)^2}\Big)\prod_{p\nmid N}\Big(1-\frac{1}{(p-1)^3}\Big),$$

et que lorsque N est un entier impair on a $\mathfrak{S}(N)\gg 1$, de sorte que $r(N)\gg N^2$ pour tout entier N impair suffisamment grand.

Dans ce qui suit, nous considérons pour $i\in\{1,2,3\}$ une base de numération entière $q_i\geqslant 2$ ainsi qu'une fonction g_i fortement q-additive non nulle, donc de la forme

$$g_i(n) = \sum_{1\leqslant k<q_i} a_{ik}|n|_k^i \quad (a_{ik}\in\mathbb{Z} \text{ pour } i\in\{1,2,3\}, 1\leqslant k<q_i), \tag{96}$$

où $|n|_k^i$ désigne le nombre d'occurrences du chiffre k dans le développement en base q_i de n. On suppose également que pour chaque $i \in \{1,2,3\}$, $\mathrm{pgcd}(a_{i1}, \dots, a_{i(q_i-1)}) = 1$. Pour chaque $i \in \{1,2,3\}$, nous considérons un entier $m_i \geqslant 2$.

Afin d'énoncer un résultat clair, nous faisons également l'hypothèse dans ce qui suit que les entiers caractéristiques $d_i = d_{g_i,m_i,q_i}$ $(i = 1,2,3)$ sont tous égaux à 1. C'est notamment le cas dès que $\mathrm{pgcd}(m_i, q_i - 1) = 1$ pour tout $i \in \{1,2,3\}$.

Usant de la notation $\mathbf{x}$ pour désigner un triplet (x_1, x_2, x_3), nous introduisons

$$r(N, \mathbf{q}, \mathbf{m}, \mathbf{b}) = \sum_{\substack{n_1,n_2,n_3 \\ n_1+n_2+n_3=N \\ g_i(n_i)\equiv b_i \bmod m_i,\, i\in\{1,2,3\}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3), \tag{97}$$

où $\mathbf{b} = (b_1, b_2, b_3)$ est un triplet de nombres entiers.

Théorème 7. *Sous ces hypothèses, il existe $\mu_{\mathbf{q},\mathbf{m},\mathbf{g}} > 0$ tel que pour $N \geqslant 2$,*

$$r(N, \mathbf{q}, \mathbf{m}, \mathbf{b}) = \frac{r(N)}{m_1 m_2 m_3} + O((\log N)^5 N^{2-\mu_{\mathbf{q},\mathbf{m},\mathbf{g}}}),$$

où la constante implicite ne dépend que de $\mathbf{q}$. En particulier, il existe un entier N_0 dépendant de $\mathbf{q}$, $\mathbf{m}$ et $\mathbf{g}$ tel que tout entier impair $N > N_0$ s'écrit sous la forme

$$N = p_1 + p_2 + p_3 \quad \text{avec } g_i(p_i) \equiv b_i \bmod m_i \text{ pour } i \in \{1,2,3\}, \tag{98}$$

où p_1, p_2 et p_3 sont des nombres premiers.

Remarque 2. *Il est possible de s'affranchir de l'hypothèse faite sur les entiers caractéristiques d_1, d_2, d_3 et, sous les conditions $\mathrm{pgcd}(b_i, d_i) = 1$ pour $i \in \{1,2,3\}$, d'obtenir une formule asymptotique générale pour $r(N, \mathbf{q}, \mathbf{m}, \mathbf{b})$ dont le terme principal serait à un coefficient multiplicatif près la quantité*

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_j\equiv c_j \bmod d_j \\ j\in\{1,2,3\}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3), \tag{99}$$

où l'on a posé pour $i \in \{1,2,3\}$, $c_j = b_j i_{d_j}(g_j(1))$. Une formule asymptotique pour la quantité (99) est contenue dans le résultat principal de [20] : pour $A > 0$, $N \geqslant 2$, $\mathrm{pgcd}(c^2{}_j, d_j) = 1$ pour $j \in \{1,2,3\}$, on a

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_j\equiv c_j \bmod d_j \\ j\in\{1,2,3\}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) = \frac{\sigma_3(N) N^2}{2\varphi(d_1)\varphi(d_2)\varphi(d_3)} + O\Big(\frac{N}{(\log N)^A}\Big),$$

où φ désigne la fonction indicatrice d'Euler, et où la constante implicite est autorisée à dépendre de A, d_1, d_2 et d_3. La quantité $\sigma_3(N)$ est une série singulière issue de la méthode du cercle : la définition de $\sigma_3(N)$ étant fastidieuse, nous renvoyons à [20] pour les détails et nous bornons à signaler que $\sigma_3(N) = 0$ si, et seulement si :

- *soit $N \not\equiv c_1 + c_2 + c_3 \bmod (\mathrm{pgcd}(d_1, d_2, d_3))$;*
- *soit il existe un nombre premier p et un triplet d'entiers deux à deux distincts $(j,k,\ell) \in \{1,2,3\}$ tels que $p \mid \mathrm{pgcd}(d_j, d_k)$, $p \nmid d_\ell$ et $p \mid n - (c_j + c_k)$.*

Démonstration. Nous employons ici la notation

$$T_i(x; \alpha, \beta) = \sum_{n\leqslant x} \Lambda(n)\, \mathrm{e}\big(\alpha g_i(n) + \beta n\big) \quad (\alpha, \beta \in \mathbb{R}).$$

Rappelons que l'on peut écrire $r(N)$ sous la forme

$$r(N) = \int_0^1 \Big(\sum_{n\leqslant N} \Lambda(n)\,\mathrm{e}(nt)\Big)^3 \mathrm{e}(-Nt)dt. \tag{100}$$

De même, en employant la relation d'orthogonalité (2), on a

$$\begin{aligned} &r(N,\mathbf{q},\mathbf{m},\mathbf{b})\\ &= \int_0^1 \mathrm{e}(-Nt) \prod_{i=1}^3 \Bigg(\sum_{\substack{n\leqslant N\\ g_i(n)\equiv b_i \bmod m_i}} \Lambda(n)\,\mathrm{e}(nt)\Bigg) dt\\ &= \frac{1}{m_1m_2m_3} \sum_{\substack{0\leqslant k_1<m_1\\ 0\leqslant k_2<m_2\\ 0\leqslant k_3<m_3}} \mathrm{e}\Big(-\frac{k_1b_1}{m_1}-\frac{k_2b_2}{m_2}-\frac{k_3b_3}{m_3}\Big) \int_0^1 \mathrm{e}(-Nt) \prod_{i=1}^3 T_i\Big(N;\frac{k_i}{m_i},t\Big)dt. \end{aligned}$$

En isolant le terme correspondant à $k_1=k_2=k_3=0$, nous obtenons

$$r(N,\mathbf{q},\mathbf{m},\mathbf{b}) = \frac{r(N)}{m_1m_2m_3} + O\Big(\frac{S}{m_1m_2m_3}\Big), \tag{101}$$

avec

$$S = \sum_{\substack{0\leqslant k_1<m_1\\ 0\leqslant k_2<m_2\\ 0\leqslant k_3<m_3\\ (k_1,k_2,k_3)\neq(0,0,0)}} \int_0^1 \prod_{i=1}^3 \Big|T_i\Big(N;\frac{k_i}{m_i},t\Big)\Big|dt. \tag{102}$$

Considérons un triplet (k_1,k_2,k_3) tel que $(k_1,k_2,k_3)\neq(0,0,0)$. Sans restreindre la généralité, on peut supposer que $k_1\neq 0$. En utilisant l'inégalité $|ab|\leqslant \max(|a|^2,|b|^2)$, on obtient alors,

$$\int_0^1 \prod_{i=1}^3 \Big|T_i\Big(N;\frac{k_i}{m_i},t\Big)\Big|dt \leqslant \max_{t\in[0;1]} \Big|T_1\Big(N;\frac{k_1}{m_1},t\Big)\Big| \max_{i=2,3} \int_0^1 \Big|T_i\Big(N;\frac{k_i}{m_i},t\Big)\Big|^2 dt. \tag{103}$$

Comme d_1 vaut 1, l'ensemble J_1 (voir définition en (81)) relatif à d_1 est réduit à $\{0\}$. Par conséquent, k_1/m_1 appartient à l'ensemble J_2 relatif à d_1, et d'après la proposition 5, on obtient *via* une intégration par parties standard,

$$T_1\Big(N;\frac{k_1}{m_1},t\Big) \ll (\log N)^4 N^{1-\sigma_{g_1,m_1,q_1}}.$$

En employant l'égalité de Parseval on obtient ainsi

$$\begin{aligned} \int_0^1 \prod_{i=1}^3 \Big|T_i\Big(N;\frac{k_i}{m_i},t\Big)\Big|dt &\ll_{q_1} (\log N)^4 N^{1-\sigma_{g_1,m_1,q_1}} \sum_{n\leqslant N} \Lambda(n)^2\\ &\ll_{q_1} N^{2-\sigma_{g_1,m_1,q_1}} (\log N)^5, \end{aligned}$$

où la dernière majoration résulte de la majoration $\Lambda(n)\leqslant \log n$ et de l'inégalité classique de Tchebychev, $\sum_{n\leqslant N}\Lambda(n)\ll N$. En posant,

$$\mu_{\mathbf{q},\mathbf{m},\mathbf{g}} = \min_{i\in\{1,2,3\}} \sigma_{g_i,m_i,q_i} > 0, \tag{104}$$

nous obtenons

$$S \ll_{\mathbf{q}} m_1m_2m_3\, N^{2-\mu_{\mathbf{q},\mathbf{m},\mathbf{g}}} (\log N)^5. \tag{105}$$

En insérant (105) dans (101), nous obtenons bien la conclusion souhaitée. □

Références

[1] J.-P. Allouche et J. Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[2] P. T. Bateman et H. G. Diamond, *Analytic number theory*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004. An introductory course.

[3] R. Bellman et H. N. Shapiro, On a problem in additive number theory, *Ann. of Math. (2)* **49** (1948), 333–340.

[4] J. Cassaigne et M. Le Gonidec, Propriétés et limites de la reconnaissance d'ensembles d'entiers par automates dénombrables, *Journal de Théorie des Nombres de Bordeaux* **22**,2 (2010), 307–338.

[5] A. Cobham, Uniform tag sequences, *Math. Systems Theory* **6** (1972), 164–192.

[6] S. Col, Diviseurs des nombres ellipséphiques, *Period. Math. Hungar.* **58**,1 (2009), 1–23.

[7] A. H. Copeland et P. Erdős, Note on normal numbers, *Bull. Amer. Math. Soc.* **52** (1946), 857–860.

[8] C. Dartyge et C. Mauduit, Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres, *J. Number Theory* **81**,2 (2000), 270–291.

[9] C. Dartyge et C. Mauduit, Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers, *Journal of Number Theory* **91** (2001), 230–255.

[10] C. Dartyge et G. Tenenbaum, Sommes des chiffres de multiples d'entiers, *Ann. Inst. Fourier* **55**,7 (2005), 2423–2474.

[11] H. Davenport, *Multiplicative number theory*, *Graduate Texts in Mathematics* vol. 74, Springer-Verlag, New York, éd. third, 2000. Revised and with a preface by Hugh L. Montgomery.

[12] C. J. de la Vallée Poussin, Recherches analytiques sur la théorie des nombres premiers, *Brux. S. sc.* **21** (1896), 183–256, 281–362, 363–397.

[13] M. Drmota et C. Mauduit, Weyl sums over integers with affine digit restrictions, *J. Number Theory* **130**,11 (2010), 2404–2427.

[14] M. Drmota, C. Mauduit et J. Rivat, Primes with an Average Sum of Digits, *Compositio* **145**,2 (2009), 271–292.

[15] S. Eilenberg, *Automata, languages, and machines. Vol. A*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York, 1974. Pure and Applied Mathematics, Vol. 58.

[16] E. Fouvry et C. Mauduit, Méthodes de crible et fonctions sommes des chiffres, *Acta Arithmetica* **77**,4 (1996), 339–351.

[17] E. Fouvry et C. Mauduit, Sommes des chiffres et nombres presques premiers, *Mathematische Annalen* **305** (1996), 571–599.

[18] A. O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.* **13** (1967/1968), 259–265.

[19] J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, *Bull. Soc. Math. France* **24** (1896), 199–220.

[20] K. Halupczok, On the ternary Goldbach problem with primes in independent arithmetic progressions, *Acta Math. Hungar.* **120**,4 (2008), 315–349.

[21] G. Harman, Primes with preassigned digits, *Acta Arith.* **125**,2 (2006), 179–185.

[22] J. Hartmanis et H. Shank, On the recognition of primes by automata, *J. Assoc. Comput. Mach.* **15** (1968), 382–389.

[23] H. Iwaniec et E. Kowalski, *Analytic number theory*, *American Mathematical Society Colloquium Publications* vol. 53, American Mathematical Society, Providence, RI, 2004.

[24] G. Lejeune Dirichlet, *Mathematische Werke. Bände I, II, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von L. Kronecker*, Chelsea Publishing Co., Bronx, N.Y., 1969.

[25] C. Mauduit, Automates finis et ensembles normaux, *Ann. Inst. Fourier* **36**,2 (1986), 1–25.

[26] C. Mauduit, Propriétés arithmétiques des substitutions, in *Séminaire de Théorie des Nombres, Paris, 1989–90*, pp. 177–190, *Progr. Math.* vol. 102, Birkhäuser Boston, Boston, MA, 1992.

[27] C. Mauduit, Propriétés arithmétiques des substitutions et automates infinis, *Ann. Inst. Fourier* **56**,7 (2006), 2525–2549.

[28] C. Mauduit et J. Rivat, La somme des chiffres des carrés, *Acta Mathematica* **203** (2009), 107–148.

[29] C. Mauduit et J. Rivat, Sur un problème de Gelfond : la somme des chiffres des nombres premiers, *Annals of Mathematics* **171**,3 (2010), 1591–1646.

[30] M. Minsky et S. Papert, Unrecognizable sets of numbers, *J. Assoc. Comput. Mach.* **13** (1966), 281–286.

[31] O. Ore, The general Chinese remainder theorem, *Amer. Math. Monthly* **59** (1952), 365–370.

[32] G. Rauzy, *Propriétés statistiques de suites arithmétiques*, Presses Universitaires de France, Paris, 1976. Le Mathématicien, No. 15, Collection SUP.

[33] M.-P. Schützenberger, A remark on acceptable sets of numbers, *J. Assoc. Comput. Mach.* **15** (1968), 300–303.

[34] W. Sierpiński, Sur les nombres premiers ayant des chiffres initiaux et finals donnés, *Acta Arith.* **5** (1959), 265–266.

[35] I. M. Vinogradov, *The method of Trigonometrical Sums in the Theory of Numbers, translated from the Russian, revised and annotated by K.F. Roth and A. Davenport*, Interscience, London, 1954.

[36] D. Wolke, Primes with preassigned digits, *Acta Arith.* **119**,2 (2005), 201–209.

Adresse électronique:
martin@lmpa.univ-littoral.fr, mauduit@iml.univ-mrs.fr, rivat@iml.univ-mrs.fr

LMPA, Centre Universitaire de la Mi-Voix, Maison de la Recherche Blaise Pascal, 50 rue F.Buisson B.P. 699, 62228 Calais Cedex.

Institut de Mathématiques de Luminy CNRS-UMR 6206, 163 avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France.