Blocs des chiffres des nombres premiers

Gautier Hanna

UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Thèse de doctorat

Discipline : Mathématiques

présentée par

Gautier Hanna

Blocs des chiffres des nombres premiers

---

dirigée par Thomas Stoll et Anne de Roton

Soutenue le 27 Septembre 2016 devant le jury composé de :

M. Jean-Paul Allouche	Institut Mathématique Jussieu	président
M. Christian Mauduit	Aix-Marseille Université	rapporteur
M. Olivier Robert	Université Lyon ICJ	examinateur
M^{lle} Anne de Roton	IECL, Université de Lorraine	codirectrice
M. Thomas Stoll	IECL, Université de Lorraine	directeur
M. Gérald Tenenbaum	IECL, Université de Lorraine	examinateur

au vu des rapports de

M. Étienne Fouvry,	Université Paris-Sud
M. Christian Mauduit,	Aix-Marseille Université

Institut Élie Cartan de Lorraine,
UMR 7502, Vandœuvre-lès-Nancy,
F-54506, France

1. Université de Lorraine, Institut Élie Cartan de Lorraine, UMR 7502, Vandœuvre-lès-Nancy, F-54506, France ;

2. CNRS, Institut Élie Cartan de Lorraine, UMR 7502, Vandœuvre-lès-Nancy, F-54506, France

École doctorale IAEM-ED77
Informatique,Automatique,Électronique-Électrotechnique, Mathématiques
Faculté des Sciences et Technologies
Bâtiment du 2ème cycle - Atrium
Boulevard des Aiguillettes
BP 70239
54506 Vandœuvre-lès-Nancy Cedex

Remerciements

Lorsque je n'étais pas très âgé, j'ai, comme tout enfant un tant soit peu aimé, subi de nombreuses fois les multiples attentions des adultes. Parmi les manies qu'ils affectaient, l'une des plus récurrentes consistait à me demander mon futur métier. À cette question je répondais souvent « chercheur ». Je me représentais en blouse blanche, un peu débraillé, au milieu d'innombrables instruments de formes originales, manipulant quelque pipette dans un but mal défini. Cette image que je me faisais de mon futur ressemblait plus à la casquette de Charles Bovary qu'à un cahier des charges de CPE, mais je me persuadais avec toute la vigueur de mon enfance que là était mon destin. On aurait pu rétorquer à cet enfant trop rêveur qu'il n'avait aucune conscience de ce dans quoi il se lançait, seulement, mes parents étaient des gens intelligents, qui savaient qu'il y avait autre chose que les éléments concrets du quotidien des adultes. Ils se sont contentés dans ma vie, et c'était déjà beaucoup, de m'encourager dans ma voie, ne projetant pas leurs désirs sur moi, mais me rappelant que le plus important était de prendre plaisir dans la tâche. À l'appui de ce conseil, ils m'ont soutenu, et depuis le font toujours.

Les années passant, ce rêve a été mis en retrait par les différents enseignements. L'image que je projetais a disparu peu à peu. Je me suis limité à suivre les cours, à passer mes classes sans me soucier du futur. Les mathématiques, du fait des figures successives de mes professeurs, avaient pris une place importante dans mes affinités. C'est tout naturellement vers elles que je m'étais dirigé dans le supérieur. Mon projet initial de faire de la recherche ne réapparut qu'après la Licence. Je fis le choix, contre l'avis de l'administration, de partir en Master Recherche et Agrégation, et je fus déterminé, devant l'étude des nouvelles matières et les systèmes d'apprentissage différents de ce que j'avais connu alors, notamment la rédaction des mémoires, à persévérer dans mon choix. Mes directeurs de mémoire, Bernhard Haak pour celui de Master 1 et Sylvain Golénia pour celui de Master 2, me laissèrent une grande autonomie que je pus beaucoup apprécier. Le véritable déclic concernant mon envie de faire une thèse fut le cours de théorie analytique des nombres que me donna Pascal Autissier, en particulier lorsqu'il nous eut fourni une preuve du théorème de Dirichlet. Je compris que ce théorème répondait à un problème concernant les chiffres des nombres premiers - qu'il y a une infinité de premiers finissant par 1, 3, 7 ou 9 - que je m'étais posé en classe de Terminale, alors que nous étudiions la notion de primalité, et que j'eus tenté naïvement de résoudre, y ayant renoncé dès que je me fus aperçu que je n'avais pas les capacités mathématiques. Suite à ce cours, je pris conscience que la théorie analytique des nombres, et particulièrement ce type de problème, était le sentier dans lequel je pouvais le plus facilement me repérer : l'idéal pour me lancer dans la recherche. Il me fallait partir de Bordeaux,

on me conseilla Nancy, où, grâce à l'Institut Elie Cartan Lorraine et la Faculté des Sciences et Techniques, à travers son Ecole Doctorale, je pus accomplir cette thèse.

Je ne mesure pas totalement l'impact de ma rencontre avec Anne de Roton. Dès les premiers contacts, elle me prit sous son aile, me fournit des compléments de cours sur des problèmes ouverts afin que je découvrisse d'autres mathématiques. Elle et le Professeur Thomas Stoll prirent beaucoup de temps avec moi afin de déterminer un sujet de thèse adapté à mes aspirations. Tous les deux crurent en moi avec une grande conviction et se battirent pour que j'obtinsse une bourse de thèse, et convainquirent le Laboratoire de Mathématiques de Nancy de m'accorder leur confiance. Ils trouvèrent toujours du temps à me consacrer, me firent rencontrer beaucoup de monde, me soutinrent toujours et m'accompagnèrent dans les moments difficiles, qu'ils fussent mathématiques ou extra-mathématiques. Ils me firent également, petit à petit, estimer le travail de relecture et la satisfaction de voir, peu à peu, des grandes lignes et de la structure chaotique émerger un texte autonome, cohérent et sans fioritures. Avec eux, toute l'équipe de théorie analytique des nombres de Nancy fut fort accueillante, notamment par la disponibilité de ses membres. Je pense tout particulièrement à Cécile Dartyge, qui, bien qu'elle ne fût pas ma directrice, s'inquiéta beaucoup de l'avancement de ma thèse, et accepta toujours de discuter avec moi lors de différentes conférences.

Je devais faire de la recherche, mais pas seulement. Le Professeur Wolfgang Bertram, Khalid Koufany, Vladimir Latocha et aussi Anne de Roton (de nouveau) m'aidèrent beaucoup dans ma charge d'enseignement : emploi du temps adéquat, gentillesse et facilité de contact, don d'anciens cours. Le Professeur Séraphin Méfire chercha toujours à alléger mon travail à coup de services. De quoi aborder sereinement ma charge d'enseignant. Je pense aussi à l'équipe administrative de l'IECL, Laurence Quirot, Elodie Cunat, Paola Schneider, dont le soutien et l'efficacité me permirent de me consacrer pleinement aux mathématiques. Vous avez tous contribué à ce que cette thèse soit un réel plaisir.

Julien Cassaigne fut d'une grande aide quant à sa rédaction de la non-automaticité des suites étudiées dans le Chapitre 2, Régine Marchand me fournit une piste précieuse (voire la solution) pour le Chapitre 3. Ils m'offrirent le luxe, pendant ce doctorat, de pouvoir compter sur l'aide de chercheurs expérimentés tels qu'eux. Ma gratitude va aussi à Pierrick Gaudry, qui accepta de faire partie de mon comité de suivi de thèse. En grand merci aussi à Bruno Martin, qui s'est régulièrement intéressé à mes travaux, et qui aurait fait partie de mon jury s'il n'était pas partie au Canada.

J'ajouterai que mon plaisir est grand de compter dans mon jury le Professeur Jean-Paul Allouche et Olivier Robert. Ils eurent tous les deux la gentillesse de s'intéresser à mes travaux lors de différentes rencontres, Olivier Robert m'ayant aidé à plusieurs reprises, en m'aiguillant sur quelques problèmes que j'étais amené à résoudre, à relever les obstacles que je rencontrais, allant même jusqu'à me fournir un schéma de preuve. Il me donna encore divers conseils concernant l'interaction avec le monde mathématique. La présence du Professeur Tenenbaum dans mon jury fait quant à elle l'objet d'une forme de fierté, émotion ressentie durant mes trois années passées à Nancy, pour avoir été dans la même équipe que lui, pour avoir pu entendre ses exposés et pour avoir suivi ses cours. Son *Introduction à la théorie*

analytique et probabiliste des nombres a été, comme pour beaucoup d'étudiants dans mon domaine, une aide incontournable de mon apprentissage. Ma reconnaissance va également aux Professeurs Fouvry et Mauduit qui acceptèrent d'être les rapporteurs de ma thèse, alors que le Professeur Fouvry dut faire l'effort, pour faire son rapport, de se replonger dans la théorie de Mauduit et Rivat, dont la technique s'est encore étoffée depuis ses débuts, et que le Professeur Mauduit ne m'avait pas rencontré. Ils ont tous deux consacré beaucoup de temps à la relecture de ma thèse, et leurs différentes remarques concernant la rédaction et la précision de mes résultats m'ont été très utiles. J'espère que je serai digne de l'attention qu'ils m'ont portée.

Un conseil que me donna ma directrice de thèse fut de développer des activités en parallèle de mon doctorat, dans le but de ne pas être trop décontenancé dans les moments creux. C'est un conseil que je ne peux m'empêcher de transmettre aux autres doctorants, tant il me semble utile. Une activité parmi d'autres : créer, en même temps que ce travail, une revue de poésie avec une bande d'amis, de poètes. Tout démarra un lundi, enfin plusieurs lundi, de 18 heures à 20 heures. On se réunissait, on buvait de la bière, on lisait des auteurs phares, on les présentait, on débattait puis on écrivait. Il y avait Poéma, aussi. Un festival de Poésie et d'écriture contemporaine en Lorraine. Franck, un ami, mais qui ne venait pas les lundis, s'occupait - et s'occupe encore - de l'organisation. Le projet de revue mit du temps avant de se monter : deux tentatives avortées. Qu'importe. Théo, Théophile, Mathieu, Alysson, Didier et Franck sont les noms que j'associe à cette idée.

Et Chloé bien sûr. Chloé qui n'a cessé de me soutenir en trois ans. Chloé qui a subi mes sautes d'humeur lorsque mes travaux n'avançaient pas bien, mais qui continuait à croire en moi. Chloé, qui, alors que j'ai tenté de lui donner par le biais de métaphores ma vision de ce qu'était mon travail, a cru que j'étais Indiana Jones. Elle qui a accepté de me suivre à Marseille, qui m'a donné une seconde famille. Pour tout ceci, merci.

Je ne suis pas certain que la personne que je suis a une vision beaucoup plus précise de ce qu'est le métier de chercheur que l'enfant qu'il fut. Par contre, je me sens fier et ému à l'idée de devenir officiellement cette personne. Non pas parce que j'accomplis là une volonté implacable de vingt-sept ans, mais parce que ceci implique un parcours sinueux, beaucoup de rencontres, des joies et des tristesses. Une belle aventure humaine, concentrée en près de cent-soixante pages, même si elles ne racontent a priori pas cette aventure.

Merci à vous tous, vraiment.

Table des matières

Notations

$\mathbb{P}(X)$	Probabilité de l'événement X.
$\mathbb{Z}$	Ensemble des entiers relatifs.
$\mathbb{R}$	Ensemble des nombres réels.
$\mathbb{C}$	Ensemble des nombres complexes.
$\lfloor x \rfloor$	Partie entière inférieure de x.
$\lceil x \rceil$	Partie entière supérieure de x.
$\|x\|_{\mathbb{Z}}$	Distance de x à l'entier le plus proche.
$a \bmod n$	Reste de la division euclidienne de a par n.
$\mathcal{P}(a, m)$	Ensemble des nombres premiers congrus à a modulo m.
$\Re(z)$	Partie réelle de z.
$\chi_\alpha(x)$	Indicatrice de $[0, \alpha) + \mathbb{Z}$, elle vaut $\lfloor x \rfloor - \lfloor x - \alpha \rfloor$ en x.
$r_{\mu_0,\mu_2}(n)$	u tel que $n = kq^{\mu_2} + uq^{\mu_0} + (n \bmod q^{\mu_0})$ et $0 \leq u < q^{\mu_2 - \mu_0}$ si μ_0 et μ_2 sont des entiers tels que $\mu_0 < \mu_2$. Il s'agit de l'entier représentant les chiffres de n allant de μ_0 à μ_2 en base q.
$T_q(n)$	$\lfloor \log n / \log q \rfloor$.
$\omega(n)$	Nombre de facteurs premiers distincts de n.
$\tau(n)$	Nombre de diviseurs de n.
$e(x)$	$\exp(2i\pi x)$.
$f(x) = O(g(x))$ ou $f(x) \ll g(x)$	Il existe une constante réelle positive C telle que $\|f(x)\| \leq Cg(x)$.
$f(x) \ll_A g(x)$	Il existe une constante réelle positive C_A dépendant de A telle que $\|f(x)\| \leq C_A g(x)$.
$f(x) = o(g(x))$	Il existe une fonction $\epsilon(x) \to 0$ telle que $f(x) = g(x)\epsilon(x)$, $x \to \infty$.
$f(x) \sim g(x)$	$f(x) = g(x)(1 + o(1))$.

Introduction

0.1 Nombres premiers dans les progressions arithmétiques

De l'étude de la théorie analytique des nombres, une notion intuitive et importante se dégage : si deux suites infinies d'entiers sont créées de manière indépendante, alors on s'attend à ce que leur intersection soit non vide et qu'elle satisfasse à un certain nombre de propriétés en lien avec les deux suites de départ. Si l'étude structurelle de la nouvelle suite considérée peut sembler ambitieuse, on peut au moins espérer obtenir une estimation asymptotique de son nombre d'éléments et que cette estimation se présente comme fonction des deux suites de départ.

Pour illustrer cette notion, on peut considérer l'ensemble des nombres premiers dans une même classe de congruence : si q est un entier supérieur ou égal à 2 et a un autre entier compris entre 0 et $q-1$, que peut-on dire des nombres premiers dont le reste de la division euclidienne par q vaut a ? Si a n'est pas premier avec q, alors on conclut immédiatement qu'il ne peut y avoir qu'au plus un nombre premier dans la classe de congruence de a. Dans le cas où a est premier avec q, ce que l'on note $(a,q)=1$, une première réponse est apportée par le théorème de la progression arithmétique de Dirichlet, dont nous pouvons trouver une version quantitative dans [Ten08, Théorème 8.13] (dans toute cette thèse, p désignera un nombre premier et $\varphi(n)$ vaudra le nombre d'entiers inférieurs à n et premiers avec n).

Théorème 0.1.1. *Si q est un entier supérieur ou égal à 2, alors pour tout entier a premier avec q nous avons :*

$$\sum_{\substack{p\leq x\\ p\equiv a \pmod q}} \frac{1}{p} \sim \frac{\log\log x}{\varphi(q)} \qquad (x\to\infty).$$

Ce théorème implique en particulier que chaque progression arithmétique admissible (avec a et q premiers entre eux) contient une infinité de nombres premiers, et même dans un certain sens que les nombres premiers sont régulièrement répartis parmi les classes possibles. Ce théorème ne fournit cependant pas de formule précise pour le nombre de nombres premiers $\pi(x;a,q)$ inférieurs à x et congrus à a modulo q. Si les notions de primalité et de congruence sont (en prenant compte des obstructions naturelles évoquées ci-avant) effectivement indépendantes, il est naturel de conjecturer que

$$\pi(x;a,q) \sim \frac{\pi(x)}{\varphi(q)} = \frac{\#\{p\leq x\}}{\#\{0\leq a<q : (a,q)=1\}}. \tag{1}$$

Une première difficulté majeure de ce problème est de déterminer la valeur asymptotique du nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à x. Il a été conjecturé par Gauss que $\pi(x) \sim x/\log x$, et ce résultat a été démontré indépendamment en 1896 par Hadamard et La Vallée-Poussin et est désormais connu sous le nom du théorème des nombres premiers. Notons $f(x) = O(g(x))$ s'il existe une constante C positive telle que $|f(x)| \leq Cg(x)$. Le théorème des nombres premiers s'énonce ainsi et peut être trouvé dans [Brü95, Page 82], ou [Ten08, Théorème 4.1] :

Théorème 0.1.2 (Théorème des nombres premiers)**.** *Il existe une constante strictement positive c telle que l'on a pour x tendant vers l'infini :*

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log(t)} + O\left(x \exp\left(-c\sqrt{\log x}\right)\right).$$

Dès lors, l'estimation (1) se démontre par le théorème suivant ([Brü95, Page 116]), qui est une conséquence du théorème de Siegel-Walfisz :

Théorème 0.1.3. *Soient q un entier plus grand que 1 fixé et a un entier premier avec q. Alors il existe une constante strictement positive c telle que l'on a pour x tendant vers l'infini :*

$$\pi(x; a, q) = \varphi(q)^{-1} \int_2^x \frac{\mathrm{d}t}{\log(t)} + O\left(x \exp\left(-c\sqrt{\log x}\right)\right). \tag{2}$$

L'énoncé usuel du théorème de Siegel-Walfisz utilise la notation 'm' en lieu et place de 'q'. Le choix est fait ici pour mettre en évidence le lien avec les problèmes digitaux*. De plus, le théorème de Siegel-Walfisz donne un résultat uniforme pour $q \leq (\log x)^N$ et la constante c du théorème dépend alors de N (voir par exemple [Ten08, Théorème 8.17]), aussi le résultat que nous avons énoncé est-il plus faible que le théorème de Siegel-Walfisz.

0.2 Questions digitales

Le Théorème 0.1.3 possède une interprétation digitale c'est-à-dire qui concerne les chiffres. Durant cette thèse, sauf mention contraire, q désigne un entier supérieur ou égal à 2. Pour tout entier n positif, nous pouvons écrire :

$$n = \sum_{i \geq 0} \epsilon_i(n) q^i = \sum_{i=0}^{T_q(n)} \epsilon_i(n) q^i \tag{3}$$

où $T_q(n) = \lfloor \log n / \log q \rfloor$ et pour tout i, $0 \leq \epsilon_i(n) < q$. Nous appelons (3) l'écriture de n en base q. L'égalité dans (3) résulte du fait que $\epsilon_k(n) = 0$ dès que $k > T_q(n)$. Nous pouvons synthétiser ces propos en disant que $T_q(n)$ est l'indice du dernier chiffre non nul de n en base q. On parlera de problème digital lorsque l'on s'intéressera à un problème lié à l'écriture en base q.

∗. Le terme "fonction digitale" étant déjà apparu dans la littérature [MMR15], il nous a paru approprié de nommer ainsi les problèmes liés aux chiffres.

L'étude de ce type de problèmes a connu des avancées majeures ces dernières années, avancées dues notamment au fait que l'informatique théorique porte un grand intérêt à l'écriture des entiers en base q, notamment en base 2 (écriture binaire) des nombres. La connexion de l'écriture des entiers en base q d'un nombre avec les suites automatiques est une des raisons de cet intérêt [AS03, Theorem 5.2.7]. Le travail que nous avons effectué dans cette thèse trouve par ailleurs sa source dans une question d'informatique théorique [Kal11, Kal12].

L'étude des chiffres possède également un intérêt mathématique intrinsèque. Au-delà de l'indépendance entre primalité et digitalité (dont nous parlerons plus tard en détail) il existe une série de problèmes ardus, dont le célèbre problème de la normalité qui consiste à déterminer si un nombre réel donné est normal. Écrivons un nombre réel x compris entre 0 et 1 sous la forme

$$x = \sum_{i \geq 0} \epsilon_i(x) q^{-i},$$

avec toujours $0 \leq \epsilon_i(x) < q$, mais où il peut y avoir cette fois-ci un nombre infini de chiffres $\epsilon_i(x)$ non nuls. Si à présent k est un entier strictement positif, s un k-uplet de chiffres compris entre 0 et $q-1$ et n un entier strictement positif, nous notons $N(s, n, x)$ le nombre d'occurrences du k-uplet s dans les n premiers chiffres de x. Par exemple $N(12, 4, 0.121212\ldots) = 2$. Nous dirons que x est q-normal si

$$\forall k \geq 1 \quad \forall s \in \{0, \ldots, q-1\}^k : \quad \lim_{n \to \infty} \frac{N(s, n, x)}{n} = \frac{1}{q^k}$$

et que x est normal si x est q-normal pour tout entier q supérieur ou égal à 2. Borel a démontré dans [Bor09] que presque tout réel, au sens de la mesure de Lebesgue, est normal. Champernowne a démontré que le réel $0,1234567891011\ldots$, dont les décimales sont la concaténation des entiers consécutifs, est un nombre 10-normal [Cha33], Copeland et Erdős que la concaténation des nombres premiers est un nombre 10-normal [CE46]. Il existe également de nombreux résultats permettant de dire qu'un nombre créé par concaténations successives est normal, dont par exemple [DMR16, Mad14]. Sierpiński a aussi donné une construction ineffective d'un nombre normal [Sie17], mais nous ne sommes pas encore aujourd'hui en mesure de déterminer si un nombre irrationnel donné non construit pour répondre à ce problème (tel que π ou $\sqrt{2}$) est normal.

Un autre problème consiste à donner une suite infinie d'entiers et à déterminer asymptotiquement le nombre de ces entiers dont les chiffres possédent une certaine propriété. Le Théorème 0.1.1 implique que pour chaque base q et chaque valeur admissible a de chiffre des unités (rappelons qu'il faut que celui-ci soit premier avec la base), il existe une infinité de nombres premiers dont le chiffre des unités est a. Il permet aussi 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 b_n soit premier avec q, il existe une infinité de nombres premiers dont les m premiers chiffres sont successivement $a_1, \ldots, a_m$ et les n derniers $b_1, \ldots, b_n$ ([Sie59] contient une preuve de ce théorème dans le cas $q = 10$ et attribue à une remarque de Knapowski le cas général).

Le Théorème 0.1.3 affirme que les nombres premiers sont équirépartis selon les valeurs admissibles de leur chiffre des unités. C'est un fait que l'on peut facilement

observer sur les petits nombres premiers. Commençons par exclure 2 et 5 qui sont exceptionnels, car ce sont les seuls nombres premiers se terminant par 2 ou 5. Nous pouvons alors observer que les nombres premiers restant semblent bien répartis selon qu'en base 10 ils finissent par 1, 3, 7 ou 9 : si on les trie jusqu'à 50, nous pouvons remarquer que $3, 13, 23, 43$ finissent par 3 ; $11, 31, 41$ finissent par 1 ; $7, 17, 37$ finissent par 7 et $19, 29$ finissent par 9, ce qui donne une répartition de $(3, 4, 3, 2)$.

Il existe des résultats généraux sur des ensembles de nombres premiers aux chiffres préassignés. Dans ce domaine, nous devons le meilleur résultat actuel à Bourgain [Bou15] qui peut assigner une proportion positive de chiffres. Bourgain montre qu'en base 2, il existe une constante strictement positive c telle que si $A = (i_1, i_2, \ldots, i_k)$ est un k-uplet de $\{1, \ldots, n\}$ de cardinal $k = cn$ et si $(a_1, a_2, \ldots, a_k)$ est un k-uplet de chiffres en base 2, alors le nombre de nombres premiers inférieurs ou égaux à 2^n pour lesquels les chiffres $\varepsilon_{i_1}, \varepsilon_{i_2}, \ldots, \varepsilon_{i_k}$ d'indices dans A sont respectivement $a_1, a_2, \cdots, a_k$ vaut asymptotiquement $\pi(2^n)/2^{cn}$. Bourgain explique aussi que sa méthode fonctionne pour n'importe quelle base q, mais la démonstration est faite dans le cas $q = 2$ pour éviter d'alourdir les calculs.

Citons aussi le cas des nombres premiers ellipséphiques : ce sont les nombres premiers qui ont un certain nombre de chiffres proscrits. Soit a un entier compris entre 0 et 9, dans [May16], Maynard estime le nombre de nombres premiers qui ne possèdent pas de a dans leur écriture décimale (voir également la liste des références de [May16]).

0.3 Méthode de Mauduit et Rivat

Un résultat fondateur de Mauduit et Rivat ([MR10]) a permis une avancée majeure dans la lignée de la recherche des chiffres des nombres premiers.

0.3.1 Questions de Gelfond

Avant de l'énoncer, replaçons le résultat de [MR10] dans son contexte. Soient n un entier, et $\epsilon_0(n), \epsilon_1(n)$ etc. ses chiffres en base q. La somme des chiffres de n en base q est définie par

$$s_q(n) = \sum_{i \geq 0} \epsilon_i(n) = \sum_{i=0}^{T_q(n)} \epsilon_i(n).$$

En 1968, Gelfond a démontré le résultat suivant :

Théorème 0.3.1. *Soient q, m et d des nombres entiers positifs tels que q soit supérieur ou égal à 2 et que m soit premier avec $q - 1$. Alors pour tout $(a, r) \in \{0, \ldots, m-1\} \times \{0, \ldots, d-1\}$:*

$$\#\{n < N : s_q(n) \equiv a \bmod m,\ n \equiv r \bmod d\} = \frac{N}{md} + O(N^\lambda)$$

avec $\lambda = \frac{1}{2 \log q} \log\left(\frac{q \sin \pi/2m}{\sin \pi/2mq}\right) < 1$.

Ainsi, il y a "indépendance" entre la "somme des chiffres" et "les progressions arithmétiques". La preuve de Gelfond consiste à regarder les sommes d'exponentielles et à montrer, en utilisant les propriétés de la somme des chiffres, que la quantité

$$\left|\sum_{n<N} e(\alpha s_q(n))\right|$$

est petite pour α un réel non entier et $e(x)$ signifiant $\exp(2i\pi x)$. L'article se conclut sur trois problèmes que nous énonçons à la lumière des résultats actuels :

(a) Si q_1, q_2 sont des entiers supérieurs ou égaux à 2 et premiers entre eux, et si $(m_1, q_1 - 1) = (m_2, q_2 - 1) = 1$, existe-t-il un réel $\lambda < 1$ tel que pour tous entiers l_1 et l_2

$$\#\{n < N : \ s_{q_1}(n) \equiv l_1 \mod m_1, \quad s_{q_2}(n) \equiv l_2 \mod m_2\} = \frac{N}{m_1 m_2} + O(N^\lambda)\,?$$

(b) Soit $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. Soit m un entier supérieur ou égal à 2 tel que $(m, q-1) = 1$, existe-t-il un réel $\lambda < 1$ tel que pour tout entier a compris entre 0 et $m-1$, on ait

$$\#\{p < N : \ p \text{ premier}, \ s_q(p) \equiv a \mod m\} = \frac{\pi(x)}{m} + O(N^\lambda)\,?$$

(c) Pour tout polynôme P à valeurs entières sur $\mathbb{N}$ existe-t-il un réel $\lambda < 1$ tel que pour tout entier a compris entre 0 et $m-1$, on ait

$$\#\{n < N : \ s_q(P(n)) \equiv a \mod m\} = Q(a, D)\frac{N}{m} + O(N^\lambda),$$

où $D = (m, q-1)$ est le pgcd de m et $q-1$ et

$$Q(a, D) := \#\{0 \leq n < D : \ P(n) \equiv a \bmod D\}\,?$$

Le premier problème a été résolu dans un premier temps par Bésineau [Bés72] sans terme explicite d'erreur, puis par Kim [Kim99]. Le meilleur terme d'erreur connu actuellement est celui donné par Berend et Kolesnik [BK16]. Dans le troisième problème, $Q(a, D)$ est une constante de renormalisation qui exprime des contraintes liées à la fonction somme de chiffres (telle la "règle de 9"). Ce sont les mêmes contraintes qui imposent la restriction aux entiers m premiers avec $q-1$ dans le deuxième problème. Le résultat de Mauduit et Rivat [MR10] permet de répondre au second problème :

Théorème 0.3.2. *Pour q et m entiers supérieurs ou égaux à 2, il existe une constante $\sigma_{q,m}$ strictement positive telle que pour tout a entier :*

$$\#\{p \leq x : s_q(p) \equiv a \bmod m\} = \frac{(m, q-1)}{m}\,\pi(x; a, (m, q-1)) + O_{q,m}(x^{1-\sigma_{q,m}}).$$

Dans le cas où $(m, q-1) = 1$, on retrouve bien la formule annoncée dans la seconde question. Avant ce résultat, Fouvry et Mauduit avaient démontré dans [FM96] le

Théorème 0.3.3. *Soit $\mathcal{P}_2$ l'ensemble des entiers positifs possédant au plus deux facteurs premiers, soient également q et m des entiers supérieurs ou égaux à 2 tels que m soit premier avec $q-1$. Alors pour tout entier a et pour x tendant vers l'infini, on a la minoration :*

$$\#\{n \leq x : \ s_q(n) \equiv a \bmod m, \ n \in \mathcal{P}_2\} \gg_{q,m} \frac{x}{\log x}.$$

Dartyge et Tenenbaum [CG05] avaient obtenu une minoration valable pour les entiers possédant exactement r facteurs premiers :

Théorème 0.3.4. *Soient q, m, et r des entiers supérieurs ou égaux à 2 tels que m soit premier avec $q-1$. Alors pour tout entier a et x tendant vers l'infini, on a la minoration :*

$$\#\{n \leq x : \ s_q(n) \equiv a \bmod m, \ n = p_1 \dots p_r\} \gg_{q,m,r} \frac{x(\log\log x)^{r-2}}{\log x \cdot \log\log\log x}.$$

La méthode que Mauduit et Rivat ont utilisée dans [MR10] a permis d'apporter, à travers le Théorème 0.3.2, une réponse complète au deuxième problème de Gelfond, près de quarante ans après que celui-ci a été posé. De plus, elle est fondamentale dans notre travail, c'est pourquoi nous expliquons brièvement son principe.

Plutôt que de compter le nombre de nombres premiers, il est usuel de faire appel à la fonction de von Mangoldt :

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^r, \\ 0 & \text{sinon.} \end{cases} \tag{4}$$

En utilisant le Lemme A.1.1, et par (A.11) Mauduit et Rivat réduisent le problème à l'estimation de la somme

$$\sum_{n \leq x} \Lambda(n) e(\alpha s_q(n)) \tag{5}$$

avec α un nombre réel. Le théorème des nombres premiers (Théorème 0.1.2) est équivalent au fait que

$$\sum_{n \leq x} \Lambda(n) \sim x.$$

Par analogie, on dit souvent qu'une fonction f, ou une suite $(f(n))_{n \geq 0}$, vérifie un théorème des nombres premiers si on arrive à donner une estimation asymptotique pour

$$\sum_{n \leq x} \Lambda(n) f(n).$$

Le résultat central de Mauduit et Rivat est le théorème suivant :

Théorème 0.3.5. *Pour q un entier supérieur ou égal à 2 et α un réel tel que $(q-1)\alpha$ ne soit pas un entier, il existe une constante réelle $\sigma_q(\alpha)$ strictement positive telle que*

$$\sum_{n \leq x} \Lambda(n) e(\alpha s_q(n)) = O_{q,\alpha}(x^{1-\sigma_q(\alpha)}). \tag{6}$$

Ainsi la suite $(e\alpha s_q(n))_{n\geq 0}$ satisfait à un théorème des nombres premiers. Dans [DMR09], Drmota, Mauduit et Rivat ont démontré qu'il existe une constante c_1 strictement positive telle que

$$\sum_{n\leq x} \Lambda(n)e(\alpha s_q(n)) \ll (\log x)^4 x^{1-c_1\|(q-1)\alpha\|_{\mathbb{Z}}^2}$$

et si cet article a paru avant [MR10], il n'en reste pas moins une amélioration.

Pour obtenir (6), Mauduit et Rivat utilisent une identité combinatoire due à Vaughan qui fait apparaître des sommes multiples de la forme

$$\sum_m \sum_n a_m b_n g(mn).$$

Ces sommes sont qualifiées de sommes de type I lorsqu'au moins l'un des coefficients a_m ou b_n est lisse, par exemple $b_n = 1$ ou $b_n = \log n$, et de type II lorsque les coefficients ont chacun une structure arithmétique qu'on estime trop complexe pour pouvoir être exploitée. Majorer des sommes de type I et de type II permet de contrôler (5). Au Lemme A.1.2, un schéma de démonstration de ce fait est donné, la démonstration complète est faite dans [MR10, Lemme 1].

Le traitement des sommes de type II est la partie la plus technique de [MR10]. Il repose sur une observation simple : si r est significativement plus petit que n, les chiffres de $m(n+r)$ et ceux de mn coïncident assez rapidement au-delà de la taille de mr, une différence n'étant possible que par la propagation d'une retenue. Ainsi, il devient possible, quitte à faire apparaître un terme d'erreur que l'on peut contrôler, de remplacer dans $s_q(m(n+r)) - s_q(mn)$ la fonction s_q par une fonction tronquée en λ (un paramètre qui dépend de m) : $s_q^{(\lambda)}$. Cette nouvelle fonction $s_q^{(\lambda)}$ ne prend en compte que les chiffres avant λ, et devient ainsi q^λ périodique.

Puisque la fonction $e(\alpha s_q^{(\lambda)}(\cdot))$ est q^λ périodique, il est possible de rattacher la "nouvelle" somme de type II à la transformée de Fourier discrète de $e(\alpha s_q(\cdot))$. Par la suite il est possible d'utiliser des outils d'analyse harmonique pour effectuer un contrôle sur cette transformée de Fourier. La corrélation $s_q(m(n+r)) - s_q(mn)$ peut être obtenue à partir des sommes de type II grâce à l'utilisation de l'inégalité de van der Corput (Théorème A.2.3), par un procédé analogue à celui utilisé par Vinogradov dans son résultat concernant la conjecture de Goldbach [Dav80, Chapter 26].

La méthode que nous venons de décrire a été développée par ses auteurs dans [MR09], pour démontrer que la somme des chiffres des carrés était bien répartie selon les classes de congruences, répondant ainsi au cas le plus simple du troisième problème de Gelfond. Dans ce cas la solution trouvée a été de remplacer la fonction somme des chiffres par une fonction doublement tronquée : seuls les chiffres du milieu ont une réelle influence sur les estimations regardées. La méthode a été utilisée par Drmota, Mauduit et Rivat pour donner une réponse partielle, mais plus générale, à la troisième question de Gelfond [DMR11] et permet de résoudre de nombreux problèmes liés à la recherche des sous-suites de suites définies par des contraintes digitales [Bou13, DMR09, DMR16, MMR15]. Notons que la dernière avancée dans ce champ est due à Müllner qui parvient, dans un travail parallèle à celui de cette thèse, et avec une autre méthode, à montrer qu'il existe une large classe de suites

automatiques qui vérifient toutes un théorème des nombres premiers [Mül16, arxiv, Février 2016].

Comme nous l'avons évoqué, le contrôle des sommes de type I et de type II permet d'obtenir un théorème des nombres premiers à travers l'équation (6), mais il s'avère que ce contrôle permet d'obtenir la même majoration pour une somme définie avec la fonction de Möbius

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n = p_1 \dots p_r \text{ est sans facteur carré,} \\ 1 & \text{si } n = 1, \\ 0 & \text{sinon} \end{cases} \tag{7}$$

en lieu et place de $\Lambda(n)$ (une démonstration de cette majoration est faite dans le Lemme A.1.3). La connexion avec la fonction de Möbius n'est pas surprenante : le théorème des nombres premiers est équivalent au fait que

$$\sum_{n \leq x} \mu(n) = o(x) \tag{8}$$

et la formule $\Lambda = \log * \mu$ où le signe $*$ désigne la convolution de Dirichlet permet de relier la fonction de Möbius à la fonction de von Mangoldt.

Il est naturel, au vu de l'équivalence entre le théorème des nombres premiers et (8) de chercher une classe de fonctions f, ou une suite $(f(n))_{n\geq 0}$ satisfaisant à

$$\sum_{n \leq x} \mu(n) f(n) = o(x). \tag{9}$$

Le cas échéant nous dirons que f vérifie un principe d'aléa de Möbius. Sarnak a énoncé un critère espéré suffisant pour qu'une fonction f donnée satisfasse à un principe d'aléa de Möbius. Plusieurs résultats dans cette direction sont connus, mais une démonstration globale n'a à ce jour pas encore été donnée. Dans [Tao12], Tao expose un survol de ce problème. Par la technique qu'utilisent Mauduit et Rivat, il est possible, en utilisant le Lemme A.1.3, de décliner le Théorème 0.3.5 en un principe d'aléa de Möbius pour la suite $(e(\alpha s_q(n)))_{n\geq 0}$ pour tout α tel que $(q-1)\alpha$ ne soit pas entier.

0.3.2 Questions de Kalai

Parallèlement au développement de la méthode de Mauduit et Rivat, Kalai a posé dans [Kal11] la question suivante : si N est un entier strictement positif, étant donné S un sous-ensemble de $\{1, \dots, N\}$, μ la fonction de Möbius, et si on note $x = (x_1, \dots, x_N)$ les éléments de $\{0,1\}^N = \mathbb{F}_2^N$, a-t-on pour tout $A > 0$,

$$\hat{\mu}(S) = \frac{1}{2^N} \sum_{x \in \mathbb{F}_2^N} \mu(x_1 + 2x_2 + \dots + 2^{N-1}x_N)(-1)^{\sum_{i\in S} x_i} = O(N^{-A}) \ ? \tag{10}$$

Dans le cas extrême $S = \{1, \dots, N\}$, comme

$$\sum_{i \in S} x_i = \sum_{1 \leq i \leq N} x_i = s_2(x_1 + 2x_2 + \dots + 2^{N-1}x_N),$$

la formule (10) résulte de [MR10].

Green [Gre12] a répondu à la question de Kalai dans le cas d'ensemble S de petite taille en montrant le

Théorème 0.3.6. *Supposons que $S \subseteq \{1, \dots, N\}$ est de taille k. Alors $\hat{\mu}(S) = O(ke^{-cN^{1/2}/k})$ où c est une constante absolue strictement positive.*

Green répond ainsi à la question dans le cas où $|S| = O(N^{1/2}/\log N)$. Bourgain [Bou13] parvient à démontrer le résultat pour tout S, en adaptant la méthode de Mauduit et Rivat et en s'appuyant sur les résultats de Green dans le cas où $|S|$ est petit. De plus, Bourgain démontre que la borne de (10) peut être remplacée par $O(2^{-N^{1/10}})$.

On peut reformuler le résultat de Bourgain de la manière suivante : soit P_N un polynôme de $\mathbb{F}_2[X_1, \dots, X_N]$ de degré au plus 1 (le degré d'un polynôme est ici le nombre maximal de variables intervenant dans un monôme), alors :

$$\frac{1}{2^N} \sum_{x \in \mathbb{F}_2^N} \mu(x_1 + 2x_2 + \cdots + 2^{N-1}x_N)(-1)^{P_N(x_1,\dots,x_N)} = o(1). \tag{11}$$

Suite au résultat de Bourgain, Kalai [Kal12] a étendu le problème en posant la question suivante centrale pour cette thèse :

> The Rudin-Shapiro sequence (also known as the Golay-Rudin-Shapiro sequence) is defined as follows.
>
> Let $a_n = \sum_i \epsilon_i \epsilon_{i+1}$ where $\epsilon_1, \epsilon_2, \dots$ are the digits in the binary expansion of n.
>
> $WS(n)$, the n th term of the Rudin Shapiro sequence is defined by $WS(n) = (-1)^{a_n}$.
>
> Question : Prove that $\sum_{i=0}^{n} WS(i)\mu(i) = o(n)$.
>
> Here, $\mu(n)$ is the Möbius function.
>
> **Motivation**
>
> This question continues a one-year old question walsh-fourier-transform-of-the-mobius-function. The two parts of the old question on "Möbius randomness" was settled by Green and by Bourgain, respectively. This question represent the simplest case, which is quite important in its own right, where some new idea/method may be needed.
>
> **Motivation (2)**
>
> Under the translation $0 \to 1, 1 \to -1$, the "Walsh-Fourier" functions can be considered as (all) linear functions over $\mathbb{Z}/2\mathbb{Z}$. It turned out that proving Möbius randomness for a few of them suffices to deduce Möbius randomness for AC0 functions. This was the second part of our old question that was proved by Green. Bourgain showed Mobius randomness for all Walsh functions (namely all linear functions over $\mathbb{Z}/2\mathbb{Z}$.) What about low degree polynomials instead of linear polynomials ? The Rudin-Shapiro sequence represent a very simple example of quadratic polynomial.
>
> If we can extend the results to polynomials over $\mathbb{Z}/2\mathbb{Z}$ of degree at most polylog (n) this will imply by a result of Razborov Mobius randomness for AC0(2) circuits. (This is interesting also under GRH).

Tao [Kal12] a donné une stratégie pour démontrer un principe d'aléa de Möbius dans le cas particulier de la suite de Rudin-Shapiro, et Mauduit et Rivat [MR15] ont

prouvé une formule asymptotique avec un terme d'erreur explicite et ont également obtenu un théorème des nombres premiers dans ce cas. De plus, Mauduit et Rivat traitent deux suites similaires définies par

$$\beta_\delta(n) = \sum_{i\geq 0} \epsilon_i(n)\epsilon_{i+\delta+1}(n) \tag{12}$$

et

$$b_d(n) = \sum_{i\geq 0} \epsilon_i(n)\epsilon_{i+1}(n)\cdots\epsilon_{i+d-1}(n), \tag{13}$$

où δ et d sont des entiers supérieurs ou égaux à 1. Dans le cas $\delta = 0$ et $d = 2$, β_δ et b_d comptent toutes les deux le nombre de blocs '11' en base 2, et ainsi $((-1)^{b_2(n)})_{n\geq 0}$ et $((-1)^{\beta_0(n)})_{n\geq 0}$ correspondent à la suite de Rudin-Shapiro.

La suite $(\beta_\delta(n))_{n\geq 0}$ a été introduite par Allouche et Liardet [AL91]. Le principal objectif de [AL91] est de trouver une suite $(b(n))_{n\geq 0}$ qui possède les mêmes propriétés que la suite qui compte le nombre de blocs '11' en base 2, notamment le fait que,

$$\sup_{\theta\in\mathbb{R}} \left| \sum_{n<N} e(n\theta)e(\alpha b(n)) \right| \leq C' N^{\sigma(\alpha)}$$

avec C' ne dépendant pas de α et $\sigma(\alpha) < 1$ dès que α n'est pas un entier. Cette propriété a été vérifiée pour la suite qui compte le nombre de '11' en base 2 par Allouche et Mendès France [AMF85] et est cruciale dans la méthode de Mauduit et Rivat. Dans [MR15], Mauduit et Rivat redémontrent le résultat d'Allouche et Liardet, soit cette propriété pour la suite $(\beta_\delta(n))_{n\geq 0}$, mais en utilisant une technique différente. Ils démontrent un résultat similaire pour la suite $(b_d(n))_{n\geq 0}$ et obtiennent de plus le résultat suivant [MR15, Theorem 4] :

Théorème 0.3.7. *Pour d un entier supérieur ou égal à 2, α et ϑ deux nombres réels et x un nombre supérieur ou égal à 2, nous avons :*

$$\left| \sum_{n\leq x} \Lambda(n)e(b_d(n)\alpha + n\vartheta) \right| \ll x(\log x)^{\frac{11}{4}} 2^{-\gamma(2\lfloor \log x/80\log 2\rfloor)/20}$$

et

$$\left| \sum_{n\leq x} \mu(n)e(b_d(n)\alpha + n\vartheta) \right| \ll x(\log x)^{\frac{11}{4}} 2^{-\gamma(2\lfloor \log x/80\log 2\rfloor)/20}$$

où

$$\gamma(\lambda) = \frac{-\lambda}{d\log 2} \log\left(1 - 2^{3-d}\left(\sin\frac{\pi\|\alpha\|_{\mathbb{Z}}}{4}\right)^2\right) - \frac{1}{2}.$$

Mauduit et Rivat obtiennent un résultat similaire pour la suite $\beta_\delta(n)$ [MR15, Theorem 3]. La seule différence consiste en la définition de la fonction γ. Ces résultats découlent de deux théorèmes beaucoup plus larges [MR15, Theorem 1-2] qui donnent deux conditions suffisantes pour qu'une fonction $f : \mathbb{N} \to \mathbb{U}$, où $\mathbb{U}$ désigne l'ensemble

des nombres complexes de module 1, satisfasse à un théorème des nombres premiers et un principe d'aléa de Möbius.

Les résultats de [MR15, Theorem 1-2] reposent sur la méthode développée dans [MR10]. Notre thèse s'appuyant sur les résultats de [MR15] nous allons exposer ici les idées principales menant aux théorèmes principaux de [MR15] en précisant les différences avec [MR10].

L'analyse de Fourier utilisée dans [MR10] repose sur un contrôle des normes L^∞ et L^1 de la transformée de Fourier discrète de la fonction $e(\alpha s_q(\cdot))$. Malheureusement, un tel contrôle pour la norme L^1 de la fonction $e(\alpha b_d(\cdot))$, si $d = 2$, n'est plus possible. Une nouveauté importante de [MR15] consiste à regarder une petite fenêtre de chiffres correspondant aux indices du milieu en introduisant, comme Mauduit et Rivat l'ont fait dans [MR09], une fonction doublement tronquée. La différence entre [MR09] et [MR15] réside dans la taille de la fenêtre considérée. Le fait de regarder une fenêtre étroite de chiffres permet d'avoir des estimations plus fines des objets et ainsi de se passer d'une estimation de la norme L^1.

L'article de Mauduit et Rivat ne se contente pas de regarder les suites $(b_d(n))_{n\geq 0}$ et $(\beta_\delta(n))_{n\geq 0}$, mais donne deux conditions sur les suites suffisantes pour obtenir un théorème des nombres premiers et un principe d'aléa de Möbius. Le nom donné à la première propriété est *Carry property*, soit propriété de propagation. Elle signifie en substance qu'il est possible, pour une suite $(a(n))_{n\geq 0}$ à valeurs entières, de remplacer a dans la corrélation $a(n+k)-a(n)$ par une troncation de a : le terme d'erreur commis est alors petit. Cette propriété permet de pratiquer des troncations successives tout en contrôlant l'erreur commise au cours de l'argumentation. Pour une définition plus précise de la propriété de propagation, voir la Définition 1.2.1. La deuxième propriété (Définition 1.2.2) ne possède pas de nom dans [MR15], mais elle explicite un contrôle de la transformée de Fourier de la fonction associée à la suite $(e(\alpha a(n)))_{n\geq 0}$: il est naturel de la nommer propriété de Fourier. Mauduit et Rivat montrent que si f est une fonction complexe à valeurs dans le disque unité qui vérifie les propriétés de propagation - la corrélation est alors énoncée de sorte qu'elle corresponde au fait que f est à valeurs dans $\mathbb{U}$ - et de Fourier, alors elle vérifie un théorème des nombres premiers de type (6) et un principe d'aléa de Möbius (9). Pour conclure, Mauduit et Rivat montrent que les suites $(e(\alpha b_d(n)))_{n\geq 0}$ et $(e(\alpha\beta_\delta(n))_{n\geq 0}$ vérifient l'une et l'autre les propriétés de propagation et de Fourier.

0.4 Résultats

Les trois chapitres de cette thèse constituent une réflexion progressive sur la recherche d'un théorème des nombres premiers et d'un principe d'aléa de Möbius pour des suites liées aux blocs de chiffres. Cette recherche est principalement axée sur la taille des blocs de chiffres considérés.

Ainsi, le premier chapitre, qui est l'objet d'un article accepté dans une revue [Han16b], fournit un théorème des nombres premiers pour la fonction $e(\alpha a(\cdot))$, où $a : \mathbb{N} \to \mathbb{N}$ est une suite qui compte le nombre d'occurrences d'un mot donné dans l'écriture *finie* d'un entier en base q, ou une autre suite liée à cette suite. Si $T_2(n)$ désigne l'indice du dernier chiffre non nul dans l'écriture en base 2 de n,

le deuxième chapitre fournit un théorème des nombres premiers pour la fonction $e(\alpha a_P(\cdot))$, où $a_P(n)$ compte le nombre d'occurrences du mot constitué de $P(T_2(n))$ '1' consécutifs dans l'écriture de n en base 2, où $P : \mathbb{N} \to \mathbb{N}$ est une fonction croissante. Si $\alpha = 1/2$ et $P(x) = x$, la fonction $e(\alpha a_P(\cdot))$ vaut -1 si n s'écrit de la forme $2^k - 1$ et 1 sinon, si la méthode devait s'appliquer, on obtiendrait que la moitié des nombres premiers seraient de la forme $2^k - 1$, aussi avons-nous essayé de déterminer la croissance maximale pour que la méthode s'applique. Dans le Chapitre 3, nous nous sommes intéressés à ce qui pouvait se produire lorsque la taille limite obtenue dans le Chapitre 2 et suggérée par le Chapitre 1 se trouvait dépassée. Nous montrons ainsi que la méthode ne peut plus s'appliquer.

L'étude des suites qui comptent les blocs de chiffres en base q est une extension naturelle des travaux de Mauduit et Rivat : la suite $(b_d(n))_{n\geq 0}$ compte le nombre de blocs constitués de d '1' en base 2, tandis que la suite $(\beta_\delta(n))_{n\geq 0}$ compte les blocs de $\delta + 2$ chiffres qui commencent et finissent par '1'.

Il est usuel, lorsque l'on étudie ce genre de suite, de regarder pour un entier n considéré non pas son écriture finie

$$n = \sum_{i=0}^{T_q(n)} \epsilon_i(n) q^i$$

mais son écriture infinie

$$n = \sum_{i\geq 0} \epsilon_i(n) q^i,$$

où on a posé $\epsilon_i(n) = 0$ pour tout i plus grand que $T_q(n)$. Le fait qu'il n'y a pas besoin d'arrêter le comptage à une valeur dépendant de n pousse à choisir l'écriture infinie plutôt que l'écriture finie, nous avons néanmoins choisi de travailler à partir de l'écriture finie d'un entier au cours de cette thèse.

La raison de ce choix est qu'il est plus naturel de considérer l'écriture finie : si on désire compter le nombre de blocs '01' dans '101' on répondra naturellement que ce nombre est 1 ; alors qu'avec l'écriture $\ldots 00101$ ce nombre est 2. Un autre problème majeur dans le comptage de blocs en écriture infinie est qu'il n'est pas possible de compter des blocs constitués exclusivement de zéros. Notons que les suites permettant de compter des blocs en écriture *infinie* sont un cas particulier des suites digitales qui sont, sous condition de l'écriture infinie d'un entier en base q, de la forme

$$a(n) = \sum_{i\geq 0} g(\epsilon_i(n), \ldots, \epsilon_{i+l-1}(n)),$$

où $g : \{0, \ldots, q-1\}^l \to \mathbb{N}$ est telle que $g(0, \ldots, 0) = 0$. On trouve un aperçu de ces suites dans le livre d'Allouche et Shallit [AS03, Section 3.3], lesquelles ont été intensivement étudiées dans la thèse de Cateland [Cat92]. Elles sont parfois appelées blocs-additives.

Durant cette thèse, nous avons essayé d'isoler les propriétés des suites $(b_d(n))_{n\geq 0}$ et $(\beta_\delta(n))_{n\geq 0}$ qui permettent de conclure aux propriétés de propagation et de Fourier des fonctions $e(\alpha b_d(\cdot))$ et $e(\alpha\beta_\delta(\cdot))$, afin de généraliser le résultat de Mauduit et Rivat à une classe de suites, et de donner une réponse partielle à la question de Kalai en montrant un principe d'aléa de Möbius pour une classe de polynômes plus étendue.

Ces polynômes sont associés aux suites qui comptent les blocs de chiffres, telle la suite $(\#012_q(n))_{n\geq 0}$ qui compte le nombre de blocs 012 dans l'écriture en base q *finie* de n, si q est un entier supérieur ou égal à 3, ou à la suite qui compte le nombres de blocs $0 * *1 * 2$ dans cette même écriture, où $*$ signifie qu'il y a un espace entre deux chiffres consécutifs.

Nous avons été amené à définir dans le Chapitre 1 une classe de suites (qu'on nomme β-récursives) régies par un certain nombre de propriétés que nous aurons l'occasion de préciser (Définition 1.3.1). Dans cette partie de l'introduction, dans un premier temps nous exposerons nos résultats du Chapitre 1 en les interprétant selon les suites qui comptent les blocs, dans un second temps nous relierons nos résultats à la question de Kalai, enfin dans un troisième temps nous expliquerons sommairement les principes et la méthode.

Les suites β-récursives possèdent une écriture simple qui dépend de $T_q(n)$ et de la "taille" des blocs regardés : si β est un entier supérieur ou égal à 2 fixé, et si pour tout entier $\tilde{n}$ strictement plus petit que $q^{\beta-1}$ on préassigne une valeur $a(\tilde{n})$, alors une suite β-récursive $(a(n))_{n\geq 0}$ satisfera à :

$$a(n) = a\left(\left\lfloor n/q^{T_q(n)-\beta+2}\right\rfloor\right) + \sum_{i=0}^{T_q(n)-\beta+1} g(\epsilon_i(n), \ldots, \epsilon_{i+\beta-1}(n)) \tag{14}$$

où $g : \{0, \ldots, q-1\}^\beta \to \mathbb{Z}$ est ici une fonction quelconque qui sera appelée fonction de propagation. On peut notamment demander $g(0, \ldots, 0) \neq 0$ contrairement au cas des suites bloc-additives. On remarque que si n est plus grand que $q^{\beta-1}$, alors comme $q^{T_q(n)} \leq n < q^{T_q(n)+1}$, on a $q^{\beta-2} \leq \left\lfloor n/q^{T_q(n)-\beta+2}\right\rfloor < q^{\beta-1}$, de sorte que (14) est bien définie.

Les suites β-récursives généralisent :

1. Les suites digitales (ou blocs-additives). On impose $g(0, \ldots, 0) = 0$ et on préassigne les valeurs $a(\tilde{n})$ de manière judicieuse. L'explicitation de ce fait est entreprise dans la Remarque 1.3.3.
2. Les suites qui comptent les blocs de chiffres en *écriture finie*, quelle que soit la base, et ce même si ce bloc est constitué uniquement de 0.
3. D'autres suites liées au comptage de blocs, comme les suites qui comptent le nombre de blocs de taille β constitués du même chiffre (pour $\beta = q = 3$ la suite comptera le nombre de blocs '000', 111' et '222') ou encore des fonctions comptant des blocs, mais avec des espaces préassignés arbitraires entre les valeurs des chiffres, telle la suite $(\beta_\delta(n))_{n\geq 0}$.

Nous montrons un théorème des nombres premiers et un principe d'aléa de Möbius pour toute suite β-récursive, sous une condition technique assez peu restrictive. Toutes les suites comptant les blocs, ainsi que la suite $(\beta_\delta(n))_{n\geq 0}$ satisfont à cette condition. Cette condition est discutée dans la Partie 1.8.1 de notre thèse : il y est notamment donné un vaste panel de suites définies sur les chiffres satisfaisant à cette condition. Si α est un nombre rationnel et $(a(n))_{n\geq 0}$ une suite β-récursive, alors la suite $e(\alpha a(n))_{n\geq 0}$ est une suite automatique [Sha16]. Ainsi nos résultats concernant le principe de Möbius sont obtenus par [Mül16] mais ont été obtenus avant cette parution.

Nous formulons à présent une partie des résultats du premier chapitre dans le contexte de la question de Kalai.

Si notre fonction g intervenant dans (14), dans le cas où $q = 2$, est un polynôme à β variables (qu'on nomme à présent $\tilde{P}$), satisfaisant à certaines conditions techniques (de sorte que notre méthode s'applique), en imposant $a(\tilde{n}) = 0$ pour tout $\tilde{n}$ plus petit que $2^{\beta-1}$, nous obtenons

$$\sum_{n<2^N} \mu(n)(-1)^{\sum_{i\leq T_2(n)-\beta+1} \tilde{P}(\epsilon_i(n),\ldots,\epsilon_{i+\beta-1}(n))} = o(2^N) \qquad (N \to \infty). \tag{15}$$

Il y a plusieurs interprétations possibles de la question de Kalai. La première consiste à étendre le résultat de Bourgain [Bou13] à des suites dont les valeurs $(a(n))_{n\geq 0}$ correspondent à la valuation en les chiffres de n d'un polynôme P appartenant à $\mathbb{Z}[X_1, \ldots, X_{T_2(n)+1}]$, de degré au plus polylog(n), ou polylog$(T_2(n))$. Le terme polylog n'est pas précisé dans [Kal12] : ou bien il s'agit de la fonction polylogarithme, ou bien il s'agit d'une puissance de logarithme. En effet, dans la théorie de la complexité, on dit dit que la complexité est polylog(n) s'il existe une constante c telle que la complexité est $(\log n)^c$ [Bla]. Pour replacer nos résultats par rapport à (15), la suite de Rudin-Shapiro s'écrit sous la forme $a(n) = (-1)^{\sum_{i\leq T_2(n)-1} \epsilon_i(n)\epsilon_{i+1}(n)}$.

Dans cette interprétation, le Chapitre 1 de notre thèse, à travers l'équation (15), fournit un résultat partiel, mais explicite une large classe de polynômes auxquels un principe de Möbius est satisfait. Le degré des polynômes étant constant.

Une autre interprétation est toutefois possible, et nos résultats fournissent pour cette dernière une réponse différente. En suivant les notations que Bourgain utilise dans [Bou15], il s'agit alors, pour répondre à la question de Kalai, de démontrer que pour tout entier N supérieur ou égal à 2, et tout polynôme P_N de $\mathbb{F}_2[X_1, \ldots, X_N]$ de degré inférieur à polylog(N) :

$$\sum_{n<2^N} \mu(n)(-1)^{P_N(n)} = o(2^N), \tag{16}$$

où $P_N(n) = P_N(\epsilon_0(n), \ldots, \epsilon_{N-1}(n))$. Cette dernière écriture est possible parce que tout entier inférieur à 2^N possède au plus N chiffres binaires. S'il en possède moins, on complète son écriture en assignant la valeur 0 aux chiffres manquants. Ainsi, 2 qui est inférieur à 2^4 peut s'écrire sous forme binaire 0010.

Comme nous allons le voir à présent, le fait de fixer N nous oblige à restreindre notre classe de polynômes. Soit N un entier positif supérieur ou égal à β. Il est possible, toujours en considérant une suite β-récursive dont la fonction de propagation g est un polynôme $\tilde{P}$ de β variables, de définir un polynôme P_N en N variables $X_1, \ldots, X_N$ à partir de notre polynôme $\tilde{P}$ à travers la formule suivante :

$$P_N(X_1, \ldots, X_N) = \sum_{i=1}^{N-\beta+1} \tilde{P}(X_i, \ldots X_{i+\beta-1}). \tag{17}$$

Nous avons alors défini une suite de polynômes $(P_N)_{N\geq\beta}$ que l'on peut compléter en une suite $(P_N)_{N\geq 0}$ en définissant les polynômes manquants par $P_0 = P_1 = \ldots = P_\beta$. Ces derniers sont notamment des polynômes à β variables.

Cependant, l'équation (15) ne répond pas forcément à la question de Kalai sous la forme (16). En effet, si N est un entier supérieur ou égal à 2 et si n est un entier strictement inférieur à 2^N, la valeur

$$P(n) := \sum_{i=0}^{T_2(n)-\beta+1} \tilde{P}(\epsilon_i(n), \dots, \epsilon_{i+\beta-1}(n)) \tag{18}$$

peut être différente de la valeur

$$P_N(n) := \sum_{i=0}^{N-\beta} \tilde{P}(\epsilon_i(n), \dots, \epsilon_{i+\beta-1}(n)), \tag{19}$$

tout comme elle peut être égale.

Soit, en effet, n tel que $T_2(n) = N-1$: alors les formules (18) et (19) coïncident. Ainsi, si on désire répondre à la question de Kalai dans le cadre de cette interprétation, il est nécessaire, dans l'écriture (14), d'avoir $a(\lfloor n/2^{T_2(n)-\beta+2} \rfloor) = 0$ pour tous les entiers n tels que $T_2(n) = N-1$.

Soit à présent n tel que $T_2(n)$ soit très petit devant $N-1$. En posant $n' = 2^{N-T_2(n)-1}n$, nous avons $T_2(n') = N-1$ et $a(\lfloor n/2^{T_2(n)-\beta+2} \rfloor) = a(\lfloor n'/2^{T_2(n')-\beta+2} \rfloor) = 0$, car justement $T_2(n') = N-1$.

Notre valuation $a(n)$ est alors exactement de la forme de (18) et il devient nécessaire de compléter (18) en (19). Ceci n'est possible que si la différence entre (19) et (18) est nulle. Puisqu'elle est constituée des $\tilde{P}(\epsilon_i, \dots, \epsilon_{i+\beta-1})$, où l'indice i est supérieur ou égal à $T_2(n) - \beta + 2$, ceci impose que $\tilde{P}(\epsilon_i, \dots, \epsilon_{i+\beta-2}, 0) = 0$, et donc que $\tilde{P}$ doit être de la forme $Z_{i_1} \dots Z_{i_{d-1}} X_{i_d}$, avec $1 \leq i_1 < \dots < i_{d-1} < i_d \leq \beta$ et $Z_i = X_i$ ou $1 - X_i$.

Les conditions techniques sur la fonction $\tilde{P}$ nous imposent $i_1 = 1$ et $i_d = \beta$. Sous ces conditions, nous avons le résultat quantitatif suivant :

Théorème 0.4.1. *Soient N un entier supérieur ou égal à 3, β un entier compris entre 2 et $N-1$. Soient $i_1, \dots, i_d$ tels que $1 = i_1 < i_2 < \dots < i_d = \beta$. Nous définissons alors un polynôme $\tilde{P}_1$ de $\mathbb{Z}[Y_1, \dots, Y_\beta]$ par*

$$\tilde{P}_1(Y_1, \dots, Y_\beta) = Z_{i_1} \dots Z_{i_{d-1}} Y_{i_d},$$

où la variable Z_i signifie Y_i ou $1 - Y_i$. Soit le polynôme à N variables

$$P_N(X_1, \dots, X_N) := \sum_{i=1}^{N-\beta+1} \tilde{P}_1(X_i, \dots, X_{i+\beta-1}),$$

alors il existe des constantes absolues strictement positives C_1 et C_2 telles que

$$\sum_{n<2^N} \mu(n)(-1)^{P_N(n)} \ll N^{C_1} 2^{N - C_2 N \frac{1}{\beta 2^\beta} + o\left(\frac{N}{\beta 2^\beta}\right)} \qquad (N \to \infty), \tag{20}$$

où $P_N(n) = P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$.

Pour les entiers n qui possèdent exactement N chiffres binaires, nous obtenons une version affaiblie du Théorème 0.4.1, dans le sens où l'intervalle de sommation est restreint, mais dans lequel la contrainte $\tilde{P}(\epsilon_i, \dots, \epsilon_{i+\beta-2}, 0) = 0$ est caduque :

Théorème 0.4.2. *Soient N un entier supérieur ou égal à 3, β un entier compris entre 2 et $N-1$. Soient $i_1, \dots, i_d$, telles que $1 = i_1 < i_2 < \dots < i_d = \beta$. Nous définissons alors un polynôme $\tilde{P}_1$ de $\mathbb{Z}[Y_1, \dots, Y_\beta]$ par*

$$\tilde{P}_1(Y_1, \dots, Y_\beta) = Z_{i_1} \dots Z_{i_d},$$

où la variable Z_i signifie Y_i ou $1 - Y_i$. Soit le polynôme à N variables

$$P_N(X_1, \dots, X_N) := \sum_{i=1}^{N-\beta+1} \left[\tilde{P}_1(X_i, \dots, X_{i+\beta-1}) + \tilde{P}_2(X_i, \dots, X_{i+\beta-2}) + \tilde{P}_3(X_{i+1}, \dots, X_{i+\beta-1}) \right],$$

avec $\tilde{P}_2$ et $\tilde{P}_3$ des polynômes de $\mathbb{Z}[X_1, \dots, X_{\beta-1}]$ quelconques. Alors, il existe des constantes absolues C_1 et C_2 (les mêmes que celles du Théorème 0.4.1) strictement positives telles que

$$\sum_{2^{N-1} \le n < 2^N} \mu(n)(-1)^{P_N(n)} \ll N^{C_1} 2^{N - C_2 N \frac{1}{\beta 2^\beta} + o\left(\frac{N}{\beta 2^\beta}\right)} \qquad (N \to \infty), \tag{21}$$

où $P_N(n) = P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$.

La forme des polynômes obtenus dans les Théorèmes 0.4.1 et 0.4.2 vient de la technique employée. Cette technique nécessite que les polynômes soient de la forme

$$P(X_1, \dots, X_N) = \sum_{i=1}^{N-\beta+1} Q(X_i, \dots, X_{i+\beta-1}),$$

avec Q un polynôme satisfaisant une condition de non-trivialité correspondant à (1.68) une fois pris en compte les changements de notations. Cette condition est nécessaire : il existe des polynômes Q ne satisfaisant pas cette condition pour lesquels la technique du Chapitre 1 ne marche pas (si Q est un polynôme constant par exemple). La forme des polynômes donnée dans les Théorèmes 0.4.1 et 0.4.2 est moins générale que la condition (1.68) mais permet d'être plus explicite sur les polynômes autorisés. Nous donnons à présent un panel de ces polynômes.

Le Théorème 0.4.2 suggère qu'il serait possible, en modifiant légèrement les arguments de notre thèse, d'obtenir un principe d'aléa de Möbius pour les polynômes définis dans le Théorème 0.4.2. Parmi ces polynômes, nous pouvons citer

— $P_N(X_1, \dots, X_N) = \sum_{i=1}^{N-\beta+1} (1 - X_i) \cdots (1 - X_{i+\beta-1})$.
Il faut prendre $\{i_1, \dots, i_d\} = \{0, \dots, \beta\}$ et $Z_i = (1 - Y_i)$ pour tout i, de sorte que $\tilde{P}_1(Y_1, \dots, Y_\beta) = (1 - Y_1) \cdots (1 - Y_\beta)$.

— $P_N(X_1, \dots, X_N) = \sum_{i=1}^{N-3} [(1 - X_i) X_{i+1} (1 - X_{i+3}) + X_{i+2}]$.
Il faut prendre $\beta = 4$, $\{i_1, i_2, i_3\} = \{0, 1, 3\}$, $Z_1 = 1 - Y_1$, $Z_2 = Y_2$, $Z_4 = 1 - Y_4$ de sorte que $\tilde{P}_1(X_1, \dots, X_4) = (1 - X_1) X_2 (1 - X_4)$ et $\tilde{P}_2(X_1, X_2, X_3) = X_3$.

Notons que l'équation (15) est satisfaite pour les polynômes $\tilde{P}$ de la forme $\tilde{P}_1+\tilde{P}_2+\tilde{P}_3$ comme dans le Théorème 0.4.2.

La méthode du Chapitre 1 ne s'applique pas aux polynômes qui ne sont pas de la forme (17), tel $P_N(X_1,\dots,X_N) = X_2X_3$, ni à ceux qui sont de la forme (17) avec $\tilde{P}(X_1,\dots,X_\beta)$ qui ne possède pas de monôme divisible par X_1X_β, typiquement $\tilde{P}(X_1,X_2,X_3) = X_1X_2 + X_2X_3$. Notons que dans ce cas $\tilde{P}$ possède trois variables, donc $\beta - 1 = 2$ et alors si P est à coefficients dans $\mathbb{F}_2$:

$$\begin{aligned} P(X_1,\dots,X_N) &= \sum_{i=1}^{N-2} \tilde{P}_1(X_i,X_{i+1},X_{i+2}) \\ &= \sum_{i=1}^{N-2} (X_iX_{i+1} + X_{i+1}X_{i+2}) \\ &= X_1X_2 + X_{N-1}X_N + 2\sum_{i=2}^{N-2} X_iX_{i+1} \\ &= X_1X_2 + X_{N-1}X_N. \end{aligned}$$

On pouvait donc s'attendre à ne pas pouvoir obtenir une estimation par cette méthode.

Pour démontrer qu'une fonction f issue d'une suite définie sur les chiffres satisfait à un théorème des nombres premiers et un principe d'aléa de Möbius, une approche est possible : elle consiste à vérifier qu'elle possède les propriétés de Fourier et de propagation.

Par exemple, la fonction $f = e(\alpha b_d(\cdot))$ vérifie facilement la propriété de propagation. L'objet de [MR15, Section 10.2] est de montrer qu'elle vérifie également la propriété de Fourier, c'est-à-dire, substantiellement, que la quantité

$$\left| \sum_{n<q^N} f(n)e(-nt) \right| \tag{22}$$

est petite (pour plus de précision, voir la Définition 1.2.2). Pour obtenir ce résultat, Mauduit et Rivat associent la fonction au graphe de la Figure 1 :

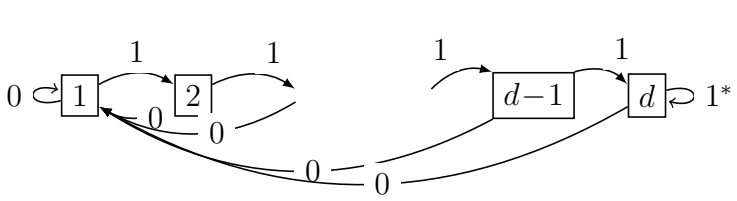


Figure 1

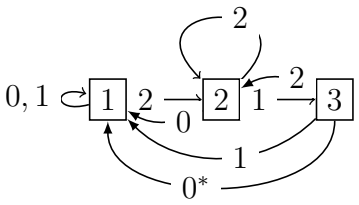
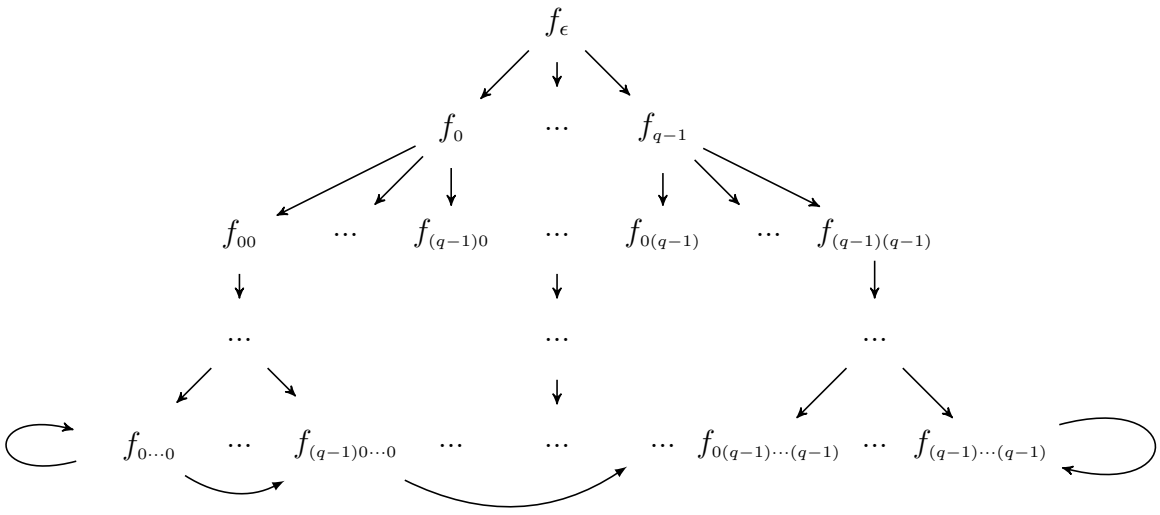


Figure 2

Il se comprend ainsi : à l'état 1, si on voit un 0 on reste à l'état 1, si on voit un 1 on passe à l'état 2. A l'état 2, si on voit un 1 on passe à l'état 3, si on voit un 0 on retourne à l'état 1, etc. A l'état d, si on voit un 1, on reste à l'état d, si on voit un 0 on retourne à l'état 1. L'étoile signifie que voir un 1 à l'état d est

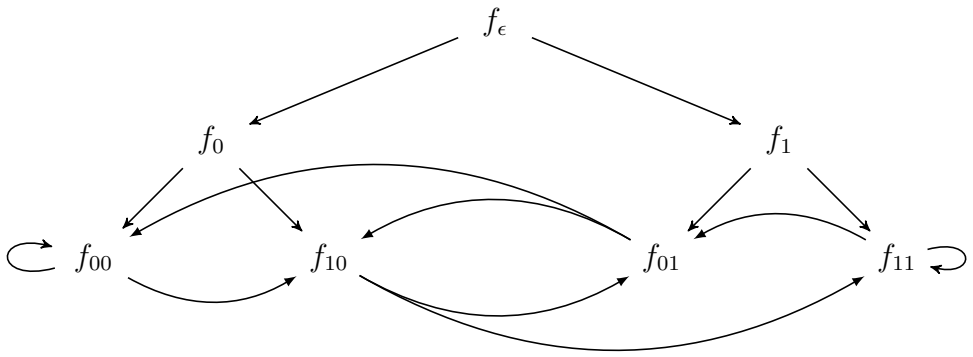
particulier par rapport aux autres changements d'états. Le fait de passer d'un état à un autre est une transition, ainsi 1^* est la transition de l'état d à l'état d. Pour obtenir que (22) est petite, Mauduit et Rivat montrent qu'elle est majorée par la norme infinie d'un vecteur, qu'on nomme $S(N)$. Par suite, ils trouvent une formule de type $S(N) = \|A\|_\infty S(N-d)$, où A est une matrice. Le coefficient $A_{i,j}$ de la matrice est une somme d'exponentielle dont les arguments sont liés aux transitions 0, 1 et 1^* : à chaque transition correspond l'ajout d'un terme précis à l'argument, passer par plusieurs transitions successives revient à cumuler cette altération d'argument, la transition 1^* fournit un terme particulier, et $A_{i,j}$ est la somme d'exponentielle correspondant à tous les arguments possibles pour aller de l'état i à j en d étapes. La clé de la démonstration consiste à dire que, quel que soit l'état initial, en parcourant le graphe d fois, il y a une possibilité de passer une fois par la transition 1^*.

De même, dans le cas où $q = 3$ et $f := e(\alpha\#012_3(\cdot))$, où $(\#012_3(n))_{n\geq 0}$ est la suite qui compte le nombre de blocs '012' dans l'écriture *finie* de n en base 3, nous pouvons associer la propriété de Fourier de f au graphe de la Figure 2, et, de même que pour Mauduit et Rivat, la "transformée de Fourier" de $e(\alpha\#012_3(\cdot))$ s'altère différemment selon que la transition est $0, 1, 2$ ou 0^*. Dans le Chapitre 1, nous avons généralisé l'argument et explicité un graphe $\mathbb{G}$ qui a la forme générale suivante :



A chaque flèche correspond une altération de l'argument tel qu'expliqué précédemment, l'altération se fait selon une instruction précise qui dépend de l'état de départ, de l'état d'arrivée et de la suite associée. Nous donnons aux flèches partant de la dernière ligne des instructions "potentiellement différentes" de celles des autres : ces instructions "encodent" la suite β-récursive. Si l'argument donné à une flèche de la dernière ligne n'a pas cette différence, qui n'était que potentielle, c'est que le chemin parcouru était inutile, et il est alors possible de contracter le graphe. C'est pourquoi les graphes des Figures 1 et 2 possèdent une forme différente de $\mathbb{G}$, mais sont bien en connexion avec un graphe de cette forme.

Dans le cas $q = 2$, $\beta = 3$ et g quelconque, $\mathbb{G}$ se présente sous la forme :



L'étude du graphe $\mathbb{G}$, dont le fonctionnement est détaillé dans la preuve de la Proposition 1.6.8, permet d'obtenir la propriété de Fourier pour $f(n) := e(\alpha a(n))$ où $(a(n))_{n\geq 0}$ est une suite β-récursive.

Une nouveauté de ce graphe, par rapport aux Figures 1 et 2 est que les états f_ω, où ω est un mot et ϵ est le mot vide, correspondent à des transformations de la fonction f en procédant ainsi : $f_\epsilon(n) := f(n)$, $f_0(n) := f(qn)$, $f_1(n) = f(qn+1), \ldots, f_{q-1}(n) := f(qn+q-1)$, $f_{00}(n) := f(q^2n)$, $f_{01}(n) := f(q^2n+1)$, etc. Puisque $f(n) = f_\epsilon(n)$, l'obtention de la propriété de Fourier découlera d'une majoration du majorant de (22) suivant :

$$\left\| \sum_{n<q^N} V_n \right\|_\infty ,$$

où les coordonnées du vecteur V_n sont les $f_\omega(n)e(-nt)$ et la norme est la norme infinie.

Pour une suite β-récursive, avec une fonction g donnée, on remarque alors que ce vecteur vérifie une récurrence linéaire : il existe une matrice carrée $M(\alpha, r, t)$ dépendant de α et de t telle que $V_{qn+r} = M(\alpha, r, t)V_n$. Les coefficients de la matrice $M(\alpha, r, t)$ peuvent alors se lire sur le graphe, et il est possible en parcourant le graphe un certain nombre de fois, si la fonction g intervenant dans (14) est non triviale, de démontrer la propriété de Fourier.

Il reste à vérifier la propriété de propagation. Malheureusement, les fonctions associées aux suites β-récursives ne possèdent pas la propriété de propagation, mais une propriété plus faible, et ceci nous pousse à reprendre les calculs de [MR15] en altérant certaines estimations.

Le Théorème 0.4.1 est non trivial si $\beta \leq c \log N$ avec $c < 1/\log 2$. Cependant, les suites $(b_d(n))_{n\geq 0}$ et $(\beta_\delta(n))_{n\geq 0}$ qui correspondent aux suites polynomiales respectives $(P_N^{b_d})_{N\geq d}$ et $(P_N^{\beta_\delta})_{N\geq d}$ définies par

$$P_N^{b_d}(X_1, \ldots, X_N) = \sum_{i=1}^{N-d} X_i \cdots X_{i+d}$$

et

$$P_N^{\beta_\delta}(X_1, \ldots, X_N) = \sum_{i=1}^{N-d} X_i X_{i+d}$$

vérifient pour tout N supérieur à d, tout N' supérieur à N et tout n inférieur à 2^N,

$$P_N^{b_d}(\epsilon_0(n), \dots, \epsilon_{N-1}(n)) = P_{N'}^{b_d}(\epsilon_0(n), \dots, \epsilon_{N'-1}(n)) \tag{23}$$

et de même pour $P_N^{\beta_\delta}$. Sous l'écriture

$$P_N(n) = P(\epsilon_0(n), \dots, \epsilon_{N-1}(n)),$$

la propriété (23) nous permet d'identifier complètement la suite $(b_d(n))_{n\geq 0}$ (respectivement $(\beta_\delta(n))_{n\geq 0}$) avec les valuations de la suite polynomiale $(P_N^{b_d})_{N\geq d}$ (respectivement $(P_N^{\beta_\delta})_{N\geq d}$). On peut écrire $(b_d(n))_{n\leq N} = (P_N^{b_d}(n))_{n\leq N}$. La propriété (23) n'existe plus lorsque le degré des polynômes augmente selon l'indice de la suite.

Soit, par exemple, la suite de polynômes $(P_N)_{N\geq 0}$, définie par

$$P_N(X_1, \dots, X_N) = \sum_{i=1}^{N-\lfloor \log N/(2\log 2)\rfloor} X_i \dots X_{i+\lfloor \log N/(2\log 2)\rfloor}.$$

Comme $\lfloor \log 2/(2\log 2)\rfloor = 0$, nous avons $P_2(X_1, X_2) = X_1 + X_2$ et donc

$$P_2(\epsilon_0(2), \epsilon_1(2)) = P_2(0, 1) = 0 + 1 = 1.$$

Comme à présent $(\log 4)/(2\log 2) = 1$, nous avons

$$P_4(X_1, X_2, X_3, X_4) = \sum_{i=1}^{4-1} X_i X_{i+1}$$

et donc

$$P_4(\epsilon_0(2), \epsilon_1(2), \epsilon_2(2), \epsilon_3(2)) = P_4(0, 1, 0, 0) = 0 \times 1 + 1 \times 0 + 0 \times 0 = 0$$

et finalement (23) n'est pas vérifiée pour cette suite polynomiale. Il n'est alors pas possible de créer une suite d'entiers à partir de la suite polynomiale en imitant le processus permettant de créer la suite $(b_d(n))_{n\geq 0}$ à partir de la suite $(P_N^{b_d})_{N\geq 0}$. Une manière de pallier ce problème, tout en regardant une suite polynomiale aux degrés croissants, est d'imposer à la suite, pour tout entier n, de prendre ses valeurs sur le polynôme $P_{T_q(n)}$ correspondant.

Soit à présent P ne désignant plus un polynôme mais une fonction croissante. Dans le Chapitre 2, nous montrons un théorème des nombres premiers et un principe d'aléa de Möbius pour les suites $(e(\alpha a_P(n)))_{n\geq 0}$, avec $(a_P(n))_{n\geq 0}$ définie par :

$$a_P(n) := \sum_{i\geq 0} \epsilon_i(n) \dots \epsilon_{i+P(T_2(n))}(n),$$

où $P : \mathbb{N} \to \mathbb{N}$ ne croît pas trop rapidement.

Si P est une fonction constante valant d, $(a_P(n))_{n\geq 0}$ correspond à la suite $(b_d(n))_{n\geq 0}$, et les résultats du Chapitre 2 découlent des travaux de Mauduit et Rivat. En revanche, si $P(x) = x$, alors notre suite $(a_P(n))_{n\geq 0}$ vaut

$$\begin{aligned} a_P(n) &= \sum_{i\geq 0} \epsilon_i(n)\dots\epsilon_{i+T_2(n)}(n) \\ &= \epsilon_0(n)\dots\epsilon_{T_2(n)}(n) \\ &= \begin{cases} 1 & \text{si } n = 2^{T_2(n)+1}-1, \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Il est ainsi illusoire d'espérer obtenir un quelconque résultat pour les fonctions P à croissance linéaire, tant la question de l'infinité du nombre de nombres premiers s'écrivant sous cette forme semble inaccessible par les moyens actuels. Toutefois il est intéressant de connaître la croissance maximale que l'on peut donner à P. Le Théorème 0.4.1 suggère que cette croissance est au moins $c\log x$ avec $c < 1/\log 2$. Nous démontrons dans le Chapitre 2 un théorème des nombres premiers et un principe d'aléa de Möbius pour les suites $(a_P(n))_{n\geq 0}$ pour toute fonction P satisfaisant à $P(x) \leq c\log x$ avec $c < 1/\log 2$. Soit désormais $f_P = e(\alpha a_P(\cdot))$, où α est un réel qui n'est pas un nombre entier. Nous obtenons le théorème suivant :

Théorème 0.4.3. *Soit P une fonction croissante, positive, et à valeurs entières pour laquelle il existe une constante strictement positive $c < 1/\log 2$ telle que $P(y) \leq c\log y$ pour tout réel y assez grand. Alors uniformément en $\alpha \in \mathbb{R}\backslash\mathbb{Z}$ et $\vartheta \in \mathbb{R}$:*

$$\left|\sum_{n\leq x} \Lambda(n) f_P(n) e(\vartheta n)\right| \ll (\log x)^{c_1'} \cdot x 2^{-\frac{1}{64}\gamma_P\left(\frac{1}{120}\lfloor\frac{\log x}{\log 2}\rfloor, \lfloor\frac{\log x}{\log 2}\rfloor\right)}, \tag{24}$$

avec

$$\gamma_P(l,k) = l\left(1 - \frac{\log\left(2^{P(k)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(k)\log 2}\right),$$

c_1' est une constante strictement positive ne dépendant ni de f_P ni de α ni de ϑ et la constante implicite est absolue et effective. De plus le théorème reste valable avec μ en lieu et place de Λ.

Remarque 0.4.4. *Si $P(x)$ vérifie les conditions du théorème, alors le majorant de l'équation (24) est $o(x)$ si $x \to \infty$. Par exemple si $\alpha = 1/2$, comme $\log(1-u) \leq -u$ si $u \in [0,1[$:*

$$\begin{aligned} \gamma_P\left(\frac{1}{120}\left\lfloor\frac{\log x}{\log 2}\right\rfloor, \left\lfloor\frac{\log x}{\log 2}\right\rfloor\right) &= -\frac{1}{120}\left\lfloor\frac{\log x}{\log 2}\right\rfloor \log\left(1 - \frac{8\left(\sin\pi/8\right)^2}{2^{P\left(\lfloor\frac{\log x}{\log 2}\rfloor\right)}}\right) \cdot \frac{1}{P\left(\left\lfloor\frac{\log x}{\log 2}\right\rfloor\right)\log 2} \\ &\geq \frac{1}{120}\left\lfloor\frac{\log x}{\log 2}\right\rfloor \frac{8\left(\sin\pi/8\right)^2}{2^{P\left(\lfloor\frac{\log x}{\log 2}\rfloor\right)}} \cdot \frac{1}{P\left(\left\lfloor\frac{\log x}{\log 2}\right\rfloor\right)\log 2} \end{aligned}$$

et si

$$P(x) = \left\lfloor\frac{2}{3}\frac{\log x}{\log 2}\right\rfloor \leq \frac{2}{3}\frac{\log x}{\log 2},$$

nous obtenons :

$$\gamma_P\left(\frac{1}{120}\left\lfloor\frac{\log x}{\log 2}\right\rfloor, \left\lfloor\frac{\log x}{\log 2}\right\rfloor\right) \geq \frac{1}{120}\left\lfloor\frac{\log x}{\log 2}\right\rfloor \frac{8\left(\sin \pi/8\right)^2}{\left\lfloor\log x/\log 2\right\rfloor^{2/3}} \cdot \frac{1}{2/3 \log\left(\left\lfloor\log x/\log 2\right\rfloor\right)}.$$

En posant $c_2' = \frac{3\cdot 8(\sin \pi/8)^2}{2\cdot 64\cdot 120} > 0$*, nous trouvons que dans ce cas précis, le membre de droite de l'équation* (24) *est majoré par*

$$x(\log x)^{c_1'} 2^{-c_2' \frac{\lfloor \log x/\log 2\rfloor^{1/3}}{\log\lfloor \log x/\log 2\rfloor}}$$

qui est $o(x)$ *si* $x \to \infty$*. Une démonstration plus générale de ce fait est donnée dans la Partie 2.9. En réalité, nous obtenons ce type de théorème pour une base* q *quelconque, mais nous les présentons ici dans le cas* $q = 2$ *pour d'une part simplifier l'écriture, d'autre part, parce que dans ce cas le résultat a une interprétation arithmétique évidente : on compte le nombre de blocs composés de '*1*'.*

Les résultats du Chapitre 2 ne résultent pas de [Mül16], qui traite des suites engendrées par un automate fini. Une démonstration est donnée dans la Partie 2.10.

Comme dans le Chapitre 1, il n'est pas possible au Chapitre 2 d'obtenir la propriété de propagation de Mauduit et Rivat (Définition 1.2.1). Cela provient dans les deux cas de l'utilisation de la taille de n dans l'argumentation. Mais alors qu'au Chapitre 1 nous pouvions altérer très légérement cette définition (le terme d'erreur trouvé ne correspondait pas à la définition de Mauduit et Rivat, mais il restait contrôlable), nous ne pouvons pas espérer une telle possibilité dans ce nouveau cas (les raisons sont détaillées dans la Partie 2.3). Nous définissons alors, pour une fonction P croissante

$$a_P(x, y) = \sum_{i\geq 0} \epsilon_i(x) \cdots \epsilon_{i+P(y)}(x)$$

et notre problème consiste alors à étudier $a_P(n, T_q(n))$ et à montrer que la fonction $(x \mapsto a_P(x, y))$ vérifie la propriété de propagation.

Cette modification entraîne de nombreuses difficultés techniques, notamment en ce qui concerne la double troncation qui permet de ne considérer que les chiffres du milieu. Ces difficultés sont résolues à l'aide de résultats classiques (théorème de Kusmin-Landau, comportement en moyenne de la fonction τ, etc.)

Finalement nous obtenons un théorème des nombres premiers et un principe d'aléa de Möbius pour $a_P(n, T_q(n))$ sous condition que $P(x) < \log x/\log 2$.

Les estimations de ce chapitre reposent sur la croissance de P et sur le fait que cette fonction intervient dans $a_P(n)$ sous la forme $P(T_2(n))$, c'est-à-dire que la croissance n'intervient que lorsqu'il y a une augmentation du nombre de chiffres. L'écriture spécifique de a_P, notamment le fait qu'elle compte les blocs constitués de $P(T_2(n))$ '1' en base 2, n'intervient pas, ou très faiblement. Il serait donc possible, quitte à faire quelques ajustements, les mêmes faits dans le Chapitre 1 par rapport à l'article [MR15], de considérer pour tout entier β une suite β-récursive donnée $(\tilde{a}_\beta(n))_{n\geq 0}$ et de prendre comme suite $(a_P(n))_{n\geq 0}$ définie par :

$$a_P(n) := \tilde{a}_{P(T_q(n))}(n)$$

et de conserver nos résultats. Dans le Chapitre 2, nous avons fait le choix particulier

$$\tilde{a}_{\beta+1}(n) = \sum_{i=0}^{T_2(n)-\beta} \epsilon_i(n)\dots\epsilon_{i+\beta}(n),$$

et nous avons donc pris $\beta = P(T_2(n))$.

Cependant ce résultat est insuffisant pour déterminer la croissance optimale de P. Dans le Chapitre 3 nous nous intéressons au cas $q = 2$ et, si N est un entier positif, pour tout $n < 2^N$, nous regardons la valeur

$$a(n) = \sum_{i\geq 0} \epsilon_i(n)\dots\epsilon_{i+k}(n)$$

dans le cas où $k \geq c\log N$ avec $c > 1/\log 2$. Nous démontrons alors que la propriété de Fourier n'est pas vérifiée dans ce cas. Nous démontrons tout de même un principe d'aléa de Möbius en obtenant la majoration suivante :

$$\left|\sum_{n<2^N} \mu(n)(-1)^{a(n)}\right| \leq \left|\sum_{n<2^N} \mu(n)\right| + 2^{N+1}N^{1-A} + o(2^{N+1}N^{1-A}),$$

où A est tel que $c = A/\log 2$. En particulier $A > 1$. La démonstration repose sur une construction probabiliste et consiste à dire que le nombre d'entiers n tels que $a(n)$ soit non nulle est en nombre très petit.

Le même argument permet de montrer

$$\sum_{n<2^N} \Lambda(n)(-1)^{a(n)} = \sum_{n<2^N} \Lambda(n) + h(N)$$

avec $|h(N)| < 2^{N+1}N^{2-A} + o(2^{N+1}N^{2-A})$. Ce dernier terme est un $o(2^N)$ si

$$a(n) = \sum_{i\geq 0} \epsilon_i(n)\dots\epsilon_{i+k}(n),$$

avec $k > c\log N$ et $c \geq 2/\log 2$, permettant de conclure que la vitesse optimale dans le problème est plus grande que $c\log N$, avec $c < 1/\log 2$ mais plus petite que $c\log N$ avec $c > 2/\log 2$. En effet, si le principe d'aléa de Möbius pouvait être démontré en partant de l'identité de Vaughan utilisée par Mauduit et Rivat, nous aurions obtenu également

$$\sum_{n<2^N} \Lambda(n)(-1)^{a(n)} = o(2^N).$$

À la fin de cette thèse se trouvent deux annexes. L'Annexe A répertorie, après les avoir mis en contexte, des résultats nécessaires à l'élaboration des différentes preuves des trois chapitres, résultats que nous avons choisi de ne pas insérer dans le corps de cette thèse afin de ne pas interrompre l'argumentation principale. Dans cette annexe, certaines démonstrations ne sont qu'esquissées, d'autres ne sont pas faites, mais une référence à un texte contenant une démonstration complète est alors donnée. L'Annexe B est consacrée à des questions et des problèmes donnant des pistes pour poursuivre ce travail.

Chapitre 1

Blocs de taille constante

1.1 Introduction

L'objectif de l'article de Mauduit et Rivat [MR15] est de donner un théorème des nombres premiers et un principe d'aléa de Möbius pour la suite de Rudin-Shapiro. Cette suite est liée à la suite qui compte le nombre de blocs '11' en base 2 : si $(a(n))_{n\geq 0}$ désigne cette dernière suite, alors $((-1)^{a(n)})_{n\geq 0}$ désigne la suite de Rudin-Shapiro.

La suite de Rudin-Shapiro a été introduite par Shapiro dans le cadre de sa thèse [Sha51]. On peut aussi la rattacher à Golay suite à [Gol51]. Elle a été créée par Shapiro comme suite des coefficients de polynômes définis par une double récursivité,

$$P_{n+1}(x) = P_n(x) + x^{2^n} Q_n(x), \quad Q_{n+1}(x) = P_n(x) - x^{2^n} Q_n(x)$$

avec comme condition initiale $P_0(x) = Q_0(x) = 1$. En remarquant que $P_n(x)$ est de degré $2^n - 1$ et en écrivant

$$P_n(x) = \sum_{r=0}^{2^n-1} a(r) x^r$$

la suite en question est $(a(r))_{r\geq 0}$. Le lien avec les chiffres binaires a été remarqué par Brillhart et Carlitz [BC70]. Les polynômes introduits par Shapiro sont particulièrement importants dans la recherche des grandeurs des sommes trigonométriques. Ces polynômes sont notamment utilisés par Kahane et Salem dans [KS94] pour démontrer de nombreux théorèmes autour des séries trigonométriques. La suite $(a(r))_{r\geq 0}$, quant à elle, répond elle-même à un certain nombre de problèmes d'optimisation. Dans le but d'expliciter des suites possédant les mêmes propriétés que la suite de Rudin-Shapiro, cette dernière a été étendue de nombreuses manières. En effet, M.Queffélec a cherché des suites dont la mesure de corrélation est celle de Lebesgues [Que87], Grant, Shallit et Stoll ont cherché à trouver des optimisations dans des problèmes de corrélation discrète [GSS09], et Allouche et Liardet ont explicité des suites possédant une petite transformée de Fourier discrète [AL91].

Soient q et β deux entiers supérieurs ou égaux à 2. Dans ce chapitre, qui fait l'objet de l'article [Han16b] nous obtenons un principe d'aléa de Möbius et un théorème

des nombres premiers pour toutes les suites $(a(n))_{n\geq 0}$ qui vérifient si $n \geq q^{\beta-1}$

$$a(n) = a\left(\left\lfloor n/q^{T_q(n)-\beta+2}\right\rfloor\right) + \sum_{i=0}^{T_q(n)-\beta+1} g(\epsilon_i(n), \dots, \epsilon_{i+\beta-1}(n))$$

où g est une fonction quelconque et $T_q(n) = \lfloor \log n / \log q \rfloor$, et les valeurs $(a(n))_{n<q^{\beta-1}}$ sont librement assignées. La forme de ces suites, que nous nommons β-récursives, généralise (12) et (13), ainsi que les généralisations de M.Queffélec et celles de Grant, Shallit et Stoll. Elle généralise également le cas des suites digitales, parfois nommées blocs-additives, qu'on peut trouver dans [Cat92]. La recherche d'un principe d'aléa de Möbius pour les suites blocs-additives a été traitée parallèlement à notre travail par Müllner.

Le lecteur trouvera dans la Partie 1.3 une introduction aux suites β-récursives et aux différentes notations qui seront utilisées dans ce chapitre. Dans la Partie 1.4 nous développons plus précisément les conséquences du théorème principal (Théorème 1.2.5). La faible propriété de propagation obtenue, et l'explication de l'altération de la condition initiale sont situées dans la Partie 1.5 de ce travail. Comme nous altérons les définitions de [MR15], nous sommes obligé de reprendre partiellement leur article, c'est ce qui est fait dans la Partie 1.7. Pour terminer l'étude des suites β-récursives, la condition de Fourier est vérifiée dans la Partie 1.6. Pour ce faire, nous sommes amené à contrôler la norme infinie d'une matrice reliée à la suite β-récursive étudiée. Nous donnons la formule exacte de la norme infinie de cette matrice (Proposition 1.6.8) en exhibant un graphe. La Partie 1.8 est dédiée à la collecte de résultats.

1.2 Travaux de Mauduit-Rivat et résultat principal

Dans cette partie consacrée aux travaux de Mauduit et Rivat, nous introduirons précisément les propriétés de Fourier et de propagation. Nous altérerons la propriété de propagation en une *faible* propriété de propagation au cours de cette étude. D'autre part, nous énoncerons un analogue du théorème principal de [MR15] que nous démontrerons dans une partie ultérieure. Si nous nommons $\mathbb{U}$ le cercle unité, pour une fonction $f : \mathbb{N} \to \mathbb{U}$ donnée, nous définissons la fonction tronquée $f^{(\lambda)}$ définie par $f^{(\lambda)}(n) = f(n \bmod q^\lambda)$ et nous notons $e(x) = \exp(2\mathrm{i}\pi x)$. Nous sommes à même de définir les propriétés centrales des travaux de Mauduit et Rivat [MR15, Definition $1-2$] :

Définition 1.2.1 (Propriété de propagation)**.** *On dit qu'une application $f : \mathbb{N} \to \mathbb{U}$ a la propriété de propagation si, uniformément pour $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ avec $\rho < \lambda$, le nombre d'entiers l satisfaisant à $0 \leq l < q^\lambda$ tels qu'il existe $(k_1, k_2) \in \{0, \dots, q^\kappa - 1\}^2$ avec*

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)} \tag{1.1}$$

est $O\left(q^{\lambda-\rho}\right)$, la constante ne dépendant que de q et f.

Définition 1.2.2 (Propriété de Fourier)**.** *On dit qu'une application $f : \mathbb{N} \to \mathbb{U}$ a la propriété de Fourier s'il existe une fonction γ croissante, avec $\lim_{\lambda\to+\infty} \gamma(\lambda) = +\infty$ et une constante absolue $c > 0$ tels que pour tous entiers positifs λ, κ avec $\kappa \leq c\lambda$ et tout réel t, on ait :*

$$\left|\frac{1}{q^\lambda} \sum_{0\leq n<q^\lambda} f(q^\kappa n)e(-nt)\right| \leq q^{-\gamma(\lambda)}.$$

Avec ces deux définitions, Mauduit et Rivat obtiennent le théorème suivant :

Théorème 1.2.3. *Soit f une application vérifiant la propriété de propagation (Définition 1.2.1) et la propriété de Fourier (Définition 1.2.2). Alors f vérifie uniformément en $\vartheta \in \mathbb{R}$:*

$$\left|\sum_{n\leq x} \Lambda(n)f(n)e(\vartheta n)\right| \ll c_1(q)(\log x)^{c_2(q)} x q^{-\gamma(2\lfloor(\log x)/80\log q\rfloor)/20}, \tag{1.2}$$

avec

$$c_1(q) = \max(\tau(q)\log q, \log^{10} q)^{1/4}(\log q)^{2-2c_2(q)},$$
$$c_2(q) = 2 + \max((1+\omega(q))/4, 2).$$

La preuve du Théorème 1.2.3 consiste à majorer le terme à gauche de (1.2) en utilisant les sommes de type I et de type II. La propriété de propagation permet d'introduire dans ces sommes la fonction tronquée afin de relier les deux sommes à la transformée de Fourier de f. La propriété de Fourier permet alors de conclure.

Soit $(a(n))_{n\geq 0}$ une suite β-récursive. Une approche naturelle pour ce chapitre est de montrer que l'application associée $f(n) := e(\alpha a(n))$ vérifie les propriétés de propagation et de Fourier. Cependant, comme nous allons le voir, la forme des suites β-récursives nous pousse à modifier la Définition 1.2.1 en

Définition 1.2.4 (Faible propriété de propagation)**.** *On dit qu'une application $f : \mathbb{N} \to \mathbb{U}$ a la faible propriété de propagation si, uniformément pour $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ avec $\rho < \lambda$, le nombre d'entiers l satisfaisant à $0 \leq l < q^\lambda$ tels qu'il existe $(k_1, k_2) \in \{0, \ldots, q^\kappa - 1\}^2$ avec*

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)} \tag{1.3}$$

est $O\left(q^{\lambda-\rho+\log\rho}\right)$, la constante ne dépendant que de q et f.

L'apparition du $\log\rho$ vient du fait que $T_q(n)$ apparaît dans l'écriture des suites β-récursives. Cette apparition sera plus détaillée dans la Remarque 1.5.3. Ces modifications entraînent une altération de l'estimation (1.2). Cette altération est explicitée dans le théorème suivant qui est le théorème principal du Chapitre 1.

Théorème 1.2.5. *Soit f une application vérifiant la faible propriété de propagation (Définition 1.2.4) et la propriété de Fourier (Définition 1.2.2). Alors f vérifie uniformément en $\vartheta \in \mathbb{R}$:*

$$\left|\sum_{n\leq x} \Lambda(n)f(n)e(\vartheta n)\right| \ll c_1(q)(\log x)^{c_2(q)} x q^{-\gamma(2\lfloor(\log x)/80\log q\rfloor)/20+\log(\gamma(2\lfloor(\log x)/80\log q\rfloor)/20)}, \tag{1.4}$$

avec

$$c_1(q) = \max(\tau(q)\log q, \log^{10} q)^{1/4}(\log q)^{2-2c_2(q)},$$
$$c_2(q) = 4 + \frac{\log q}{4} + \frac{1}{4}\max(\omega(q), 2).$$

Cet énoncé diffère du Théorème 1.2.3 par une altération dans la Définition 1.2.4 de $O(q^{\lambda-\rho})$ en $O(q^{\lambda-\rho+\log\rho})$ et par l'altération des constantes $c_1(q)$ et $c_2(q)$. L'apparition du $\log q$ dans $c_1(q)$ et $c_2(q)$ provient directement du $\log\rho$ dans l'estimation de la Définition 1.2.4.

Remarque 1.2.6. *Comme nous l'avons remarqué dans l'introduction, l'approche utilisée pour cette démonstration permet de remplacer dans l'énoncé du Théorème 1.2.5 la fonction de von Mangoldt Λ par la fonction de Möbius μ.*

1.3 Introduction aux suites β-récursives

Dans cette partie, nous introduisons la notion de suite β-récursive à travers les propriétés qui nous permettront de conclure à un théorème des nombres premiers. Nous explicitons également le lien les unissant avec différentes suites classiques liées aux chiffres. Nous commençons cette partie en introduisant certaines notations qui seront couramment utilisés dans ce chapitre.

Soit q un entier supérieur ou égal à 2. On note $\mathcal{A}$ l'alphabet sur $\mathbb{Z}/q\mathbb{Z}$, c'est-à-dire $\mathcal{A} = \{0, \dots, q-1\}$. On note Σ l'ensemble des mots sur $\mathcal{A}$, Σ^* l'ensemble des mots finis, Σ_k l'ensemble des mots de taille k, Σ_k^* l'ensemble des mots de taille au plus k, et ϵ le mot de taille 0. Ainsi $\Sigma_0 = \{\epsilon\}$, $\Sigma_1 = \{0, \dots, q-1\}$, $\Sigma_1^* = \{\epsilon, 0, \dots, q-1\}$, etc.

Si ω et ω' sont deux mots finis sur $\mathcal{A}$, on note $\omega\cdot\omega'$ leur concaténation. On omettra parfois le symbole $\cdot$, toutefois sans risque de confusion. Pour ω un mot fini, nous notons $|\omega|$ sa taille, pour un entier k positif et inférieur ou égal à $|\omega|$, on note $\overline{\omega}^k$, le préfixe de ω de taille k, et $\underline{\omega}_k$ son suffixe de taille k. On a par convention $\overline{\omega}^0 = \underline{\omega}_0 = \epsilon$. Ainsi, pour tout entier k entre 0 et $|\omega|$, on a la décomposition $\omega = \overline{\omega}^{|\omega|-k} \cdot \underline{\omega}_k$. On note $\epsilon_i(\omega)$ la i-ième lettre de ω, lorsque ω est lu de droite à gauche. Le mot ω possède ainsi la décomposition $\omega = \epsilon_{|\omega|-1}(\omega)\cdots\epsilon_0(\omega)$.

On définit l'application $\varphi : \Sigma^* \to \mathbb{N}$ par

$$\varphi(\omega) = \sum_{i=0}^{|\omega|-1} \epsilon_i(\omega) q^i.$$

Pour $r \in \mathcal{A}$, une lettre de l'alphabet, on utilisera la notation $\hat{r}$ pour l'entier $\varphi(r)$. Pour un entier x compris entre 0 et $q-1$, on note $\dot{x} = \varphi^{-1}(x)$ pour désigner la lettre correspondante.

Ainsi, pour $\omega = 280163$, on a $\epsilon_0(\omega) = 3$, $\epsilon_1(\omega) = 6$, $\epsilon_2(\omega) = 1$. Nous avons également $|\omega| = 6$, $\overline{\omega}^2 = 28$, $\underline{\omega}_3 = 163$. Enfin, si $\mathcal{A} = \{0, \dots, 10\}$ et $q = 11$, nous

avons :

$$\begin{aligned}\varphi(\omega) &= \varphi(280163)\\ &= 2\times 11^5 + 8\times 11^4 + 0\times 11^3 + 1\times 11^2 + 6\times 11^1 + 3\times 11^0\\ &= 439420.\end{aligned}$$

Une fonction aura une place importante dans ce chapitre : l'indicatrice des mots. Si ω', est un mot fini, nous la notons $\mathbb{1}_{\omega'}$. Elle va de Σ^* à $\{0,1\}$ et vaut

$$\mathbb{1}_{\omega'}(\omega) = \begin{cases} 1 & \text{si } \omega = \omega' \\ 0 & \text{sinon.}\end{cases}$$

Nous introduisons maintenant l'objet central de l'étude de ce chapitre : la notion de suite β-récursive. Nous ne donnons pas ici la définition qui permet la meilleure représentation des suites β-récursives, mais celle que nous donnons met en exergue les propriétés principales qui ont motivé l'étude de ces suites.

Définition 1.3.1. *Soient $(a(n))_{n\geq 0}$ une suite à valeurs dans $\mathbb{Z}$ et β un entier supérieur ou égal à 2. On dit que $(a(n))_{n\geq 0}$ est β-récursive s'il existe une application $g : \Sigma_\beta \to \mathbb{N}$ telle que pour tout $n \geq 1$ et pour tout ω dans Σ_β, on ait :*

$$a(q^\beta n + \varphi(\omega)) = a(q^{\beta-1}n + \varphi(\overline{\omega}^{|\omega|-1})) + g(\omega), \tag{1.5}$$

et telle que si $\overline{\omega}^1 \neq 0$:

$$a(\varphi(\omega)) = a(\varphi(\overline{\omega}^{|\omega|-1})) + g(\omega). \tag{1.6}$$

Nous dirons que g est la fonction de propagation de a.

Comme ω est un élément de Σ_β, donc comme il possède β lettres, si $\overline{\omega}^1 = 0$ il existe $\tilde{\omega}$ dans $\Sigma^*_{\beta-1}$ tel que

$$\varphi(\omega) = \varphi(\tilde{\omega}) = \sum_{i=0}^{\beta-2} \epsilon_i(\omega) q^i \leq q^{\beta-1} - 1 < q^{\beta-1}.$$

Ainsi la notion de β-récursivité n'impose de contraintes que pour les entiers au moins égaux à $q^{\beta-1}$.

Citons ici trois exemples de suites β-récursives :

(E1) **Suites de Rudin–Shapiro généralisées.** Les suites de type Rudin-Shapiro, constituées des généralisations proposées par M. Queffélec [Que87], par Grant, Shallit et Stoll [GSS09], ou encore Allouche et Liardet [AL91] sont des suites β-récursives.

(E2) **Suites blocs-additives.** Les suites digitales, qui sont parfois nommées blocs-additives [AS03, Cat92] définies par

$$a(n) = \sum_{i\geq 0} g(\epsilon_{i+\beta-1}(n)\cdots\epsilon_i(n))$$

avec $g(0\cdot\ldots\cdot 0) = 0$ et (3) sont des suites β-récursives. Les exemples de (E1) sont des suites digitales particulières.

(E3) **Suites blocs-additives finies.** On peut se passer de la condition $g(0\cdots 0) = 0$ et prendre la suite

$$a(n) = \sum_{i=0}^{T_q(n)-\beta+1} g(\epsilon_{i+\beta-1}(n)\cdots\epsilon_i(n)),$$

ce qui est fondamental si on veut compter les blocs de chiffres en écriture finie (par exemple la suite blocs-additives qui compte le nombre de 01 vaudra 2 pour 101, ce qui est contraire à l'intuition). Cette suite est également une suite β-récursive.

Notons que notre méthode ne permet pas d'obtenir un théorème des nombres premiers pour toutes les suites β-récursives : elle nécessite une condition de non trivialité sur la fonction g. Toutefois cette condition est assez peu restrictive : si elle n'est pas satisfaite, cela veut dire en quelque sorte que la fonction g n'était pas vraiment définie sur un bloc de taille β. En particulier, pour tous les exemples proposés en (E1), notre méthode s'applique.

L'objet de la proposition suivante est de donner une forme aux suites β-récursives telle que leur représentation s'en trouve facilitée. L'explicitation des exemples mentionnés ci-dessus est faite dans la Remarque 1.3.3 qui s'appuie sur la Proposition 1.3.2.

Proposition 1.3.2. *Soient un entier β supérieur ou égal à 2 et $(a(n))_{n\geq 0}$ une suite β-récursive. Soit n un entier, nous considérons sa décomposition en base q,*

$$n = \sum_{i=0}^{N} \epsilon_i(n)q^i = \varphi\Big(\epsilon_N(n)\cdots\epsilon_1(n)\cdot\epsilon_0(n)\Big),$$

où $N = T_q(n)$. Alors, si $n \geq q^{\beta-1}$, on a $N \geq \beta - 1$ et

$$a(n) = a\bigg(\varphi\Big(\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+2}(n)\Big)\bigg) + \sum_{l=0}^{N-\beta+1} g\Big(\epsilon_{l+\beta-1}(n)\cdots\epsilon_{l+1}(n)\cdot\epsilon_l(n)\Big).$$

Remarquons que $|\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+2}(n)| = \beta - 1$ et que $\epsilon_N(n) \neq 0$.

Démonstration. Le cas $N = \beta - 1$ est immédiat, nous pouvons désormais supposer $N > \beta - 1$.

Nous allons montrer par récurrence sur r que pour tout entier r compris entre 0 et $N - \beta$,

$$a\left(\sum_{i=0}^{N}\epsilon_i(n)q^i\right) = a\bigg(q^{\beta-1}\sum_{i=\beta+r}^{N}\epsilon_i(n)q^{i-\beta-r} + \varphi\Big(\epsilon_{\beta-1+r}(n)\cdots\epsilon_{r+1}(n)\Big)\bigg) + \sum_{l=0}^{r} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)). \tag{1.7}$$

Pour $r = 0$, on a par (1.5) :

$$a\left(\sum_{i=0}^{N}\epsilon_i(n)q^i\right) = a\Bigg(q^\beta\sum_{i=\beta}^{N}\epsilon_i(n)q^{i-\beta} + \varphi\Big(\epsilon_{\beta-1}(n)\cdots\epsilon_1(n)\cdot\epsilon_0(n)\Big)\Bigg)$$
$$= a\Bigg(q^{\beta-1}\sum_{i=\beta}^{N}\epsilon_i(n)q^{i-\beta} + \varphi\Big(\epsilon_{\beta-1}(n)\cdots\epsilon_1(n)\Big)\Bigg) + g(\epsilon_{\beta-1}(n)\cdots\epsilon_0(n)).$$

Supposons l'hypothèse de récurrence (1.7) satisfaite pour un certain $r \leq N-\beta-1$ et montrons (1.7) pour $r+1$. Comme $\beta+r+1 \leq N$ et $\epsilon_N(n) \neq 0$,

$$\sum_{i=\beta+r+1}^{N}\epsilon_i(n)q^{i-\beta-r-1} \geq 1.$$

Alors, en utilisant l'hypothèse de récurrence (1.7), puis la première propriété des suites β-récursives (1.5) on obtient :

$$\begin{aligned}
a\left(\sum_{i=0}^{N}\epsilon_i(n)q^i\right) &= a\Bigg(q^{\beta-1}\sum_{i=\beta+r}^{N}\epsilon_i(n)q^{i-\beta-r} + \varphi\Big(\epsilon_{\beta-1+r}(n)\cdots\epsilon_{r+1}(n)\Big)\Bigg) \\
&\qquad + \sum_{l=0}^{r} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)) \\
&= a\Bigg(q^{\beta}\sum_{i=\beta+r+1}^{N}\epsilon_i(n)q^{i-\beta-r-1} + \varphi\Big(\epsilon_{\beta+r}(n)\cdot\epsilon_{\beta-1+r}(n)\cdots\epsilon_{r+2}(n)\cdot\epsilon_{r+1}(n)\Big)\Bigg) \\
&\qquad + \sum_{l=0}^{r} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)) \\
&= a\Bigg(q^{\beta-1}\sum_{i=\beta+r+1}^{N}\epsilon_i(n)q^{i-\beta-r-1} + \varphi\Big(\epsilon_{\beta+r}(n)\cdot\epsilon_{\beta-1+r}(n)\cdots\epsilon_{r+2}(n)\Big)\Bigg) \\
&\qquad + \sum_{l=0}^{r+1} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)),
\end{aligned}$$

ce qui conclut la récurrence. En appliquant (1.7) à $r = N-\beta$, on obtient :

$$\begin{aligned}
a(n) &= a\Bigg(q^{\beta-1}\sum_{i=N}^{N}\epsilon_i(n)q^{i-N} + \varphi\Big(\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+1}(n)\Big)\Bigg) + \sum_{l=0}^{N-\beta} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)) \\
&= a\Bigg(q^{\beta-1}\epsilon_N(n) + \varphi\Big(\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+1}(n)\Big)\Bigg) + \sum_{l=0}^{N-\beta} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)) \\
&= a\Bigg(\varphi\Big(\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+1}(n)\Big)\Bigg) + \sum_{l=0}^{N-\beta} g(\epsilon_{l+\beta-1}(n)\cdots\epsilon_l(n)),
\end{aligned}$$

et on conclut par la deuxième propriété des suites β-récursives (1.6). On peut le faire parce qu'ici N désigne l'indice du dernier terme non nul dans la décomposition de n, ce qui veut dire $\epsilon_N(n) \neq 0$, et enfin $\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+1}(n) \in \Sigma_\beta$. □

Remarque 1.3.3. *Avec l'écriture de la proposition précédente, il suffit, pour retrouver les exemples de (E1), de prendre la fonction g correspondante. Par exemple, on pose*

$$g(\omega) = \widehat{\epsilon_\delta(\omega)}\widehat{\epsilon_0(\omega)},$$

nous obtenons $a(n) = \sum_{i\geq 0} \epsilon_{i+\delta}(n)\epsilon_i(n) = \beta_\delta(n)$*, la suite d'Allouche et Liardet. Pour obtenir une suite digitale, ou blocs-additives (E2) à partir d'une suite* β*-récursive, il suffit de poser*

$$a(\varphi(\omega)) = \sum_{l=1}^{\beta-1} g(0^{\beta-l}\cdot\overline{\omega}^l), \tag{1.8}$$

où 0^k *désigne le mot composé de* k *'* 0*'. Par exemple si a compte les blocs* 011 *dans l'écriture infinie de* n *en base* 2*, on définit* $a(n)$ *pour* $0 \leq n < 4$ *par* $a(0) = a(\varphi(00)) = g(000) = 0, a(1) = a(\varphi(01)) = g(001) = 0$ *et de même* $a(2) = 0$ *mais* $a(3) = a(\varphi(11)) = g(011) = 1$*. En effet, si on définit* $a(n)$ *par* (1.8) *si* $n < q^{\beta-1}$*, nous avons alors :*

$$\begin{aligned} a(n) &= a\Big(\varphi\Big(\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+2}(n)\Big)\Big) + \sum_{i=0}^{N-\beta+1} g\Big(\epsilon_{i+\beta-1}(n)\cdots\epsilon_{i+1}(n)\cdot\epsilon_i(n)\Big) \\ &= \sum_{l=1}^{\beta-1} g(0^{\beta-l}\cdot\overline{\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+2}(n)}^l) + \sum_{i=0}^{N-\beta+1} g\Big(\epsilon_{i+\beta-1}(n)\cdots\epsilon_{i+1}(n)\cdot\epsilon_i(n)\Big), \end{aligned}$$

et comme $\overline{\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdots\epsilon_{N-\beta+2}(n)}^l = \epsilon_N(n)\cdots\epsilon_{N-l+1}(n)$ *et que pour tout* k *supérieur ou égal à* 1*,* $\epsilon_{N+k}(n) = 0$*, nous avons :*

$$\begin{aligned} a(n) &= \sum_{l=1}^{\beta-1} g(0^{\beta-l}\cdot\epsilon_N(n)\cdots\epsilon_{N-l+1}(n)) + \sum_{i=0}^{N-\beta+1} g\Big(\epsilon_{i+\beta-1}(n)\cdots\epsilon_{i+1}(n)\cdot\epsilon_i(n)\Big) \\ &= \sum_{i=0}^{N} g\Big(\epsilon_{i+\beta-1}(n)\cdots\epsilon_{i+1}(n)\cdot\epsilon_i(n)\Big) \\ &= \sum_{i\geq 0} g\Big(\epsilon_{i+\beta-1}(n)\cdots\epsilon_{i+1}(n)\cdot\epsilon_i(n)\Big) \end{aligned}$$

parce que $g(0\cdots 0) = 0$*.*

1.4 Troncation et conséquences du Théorème 1.2.5

Nous énonçons ici les propriétés relatives aux nombres premiers que les suites β-récursives possèdent. Ces résultats sont des conséquences du Théorème 1.2.5 et sont issus de [MR15]. Nous définissons également rigoureusement la notion de troncation.

Pour cette partie nous rappelons que $\tau(n)$ désigne le nombre de diviseurs de n, et $\omega(n)$ le nombre de facteurs premiers dans la décomposition de n (ainsi $\omega(2^2\times 3) = 2$). Les deux notations ω pour désigner un mot et la fonction arithmétique $\omega(n)$ ne se recoupent pas dans le chapitre, et nous pouvons utiliser conjointement ces deux notations sans risque de confusion. De plus nous rappelons que $\pi(x; a, m)$ désigne le nombre de nombres premiers inférieurs ou égaux à x et congrus à a modulo m.

Nous définissons à présent la notion de troncation.

Définition 1.4.1. *Soit $(a(n))_{n\geq 0}$ une suite β-récursive, et soit λ un entier naturel. On définit $(a^{(\lambda)}(n))_{n\geq 0}$, la suite tronquée en λ, par*

$$a^{(\lambda)}(n) = a(n \bmod q^{\lambda}),$$

où $n \bmod q^{\lambda}$ désigne le reste de la division euclidienne de n par q^{λ}. Soit α un nombre réel. On définit les applications $f : \mathbb{N} \to \mathbb{U}$ et $f^{(\lambda)} : \mathbb{N} \to \mathbb{U}$ par

$$f(n) = e\Big(\alpha a(n)\Big) \quad et \quad f^{(\lambda)}(n) = e\Big(\alpha a^{(\lambda)}(n)\Big).$$

On dit qu'elles sont associées aux suites $(a(n))_{n\geq 0}$ et $(a^{(\lambda)}(n))_{n\geq 0}$.

Le fait de prendre la réduction modulo q^{λ} d'un entier n consiste à regarder ses chiffres d'indice inférieur à λ. Le terme 'troncation' prend ici son sens. De plus les notions de propriété de propagation (Définition 1.2.2), de faible propriété de propagation (Définition 1.2.4), ainsi que les Théorèmes 1.2.3 et 1.2.5 prennent ici un sens rigoureux. Tout comme Mauduit et Rivat, nous déduisons du Théorème 1.2.5 trois corollaires, dont les preuves sont identiques à [MR15, Corollary 1–3] :

Corollaire 1.4.2. *Soit $b : \mathbb{N} \to \mathbb{N}$ une application telle que pour tout α irrationnel, la fonction $f = e(\alpha b(\cdot))$ vérifie les Définitions 1.2.2 et 1.2.4. Alors pour tout entier relatif a et tout entier naturel m premier avec a, la suite $(\alpha b(p))_{p\in\mathcal{P}(a,m)}$, où $\mathcal{P}(a,m)$ désigne les nombres premiers congrus à a modulo m, est uniformément distribuée si et seulement si α est irrationnel.*

Corollaire 1.4.3. *Soit $b : \mathbb{N} \to \mathbb{N}$ une application et m et m' des entiers supérieurs ou égaux à 1 tels que pour tout $1 \leq j' < m'$, la fonction $f = e\left(\frac{j'}{m'}b(\cdot)\right)$ vérifie les Définitions 1.2.2 et 1.2.4. Alors, pour tous a et a' tel que a soit premier avec m, on a :*

$$\#\{p \leq x,\ p \in \mathcal{P}(a,m),\ b(p) \equiv a' \bmod m'\} \sim \frac{\pi(x;a,m)}{m'} \qquad (x \to \infty).$$

Corollaire 1.4.4. *Soit $b : \mathbb{N} \to \mathbb{N}$ et m et m' des entiers plus grands que 1, tels que pour tout $1 \leq j' < m'$, la fonction $f = e\left(\frac{j'}{m'}b(\cdot)\right)$ vérifie les Définitions 1.2.2 et 1.2.4. Alors, pour tout a et a' tel que a soit premier avec m, la suite $(\vartheta p)_{\{p\in\mathcal{P}(a,m),\ b(p)\equiv a' \bmod m'\}}$ est uniformément distribuée si et seulement si ϑ est irrationnel.*

1.5 Faible propriété de propagation

Ici, et désormais, nous fixons q et β des entiers supérieurs ou égaux à 2. Le but de cette partie est de démontrer que les fonctions associées aux suites β-récursives vérifient la faible propriété de propagation (Définition 1.2.4). L'idée principale consiste à exploiter la Proposition 1.3.2 pour dire que sous certaines conditions, il n'y a pas de différence entre $f(n)$ et $f^{(\lambda)}(n)$.

Proposition 1.5.1. *Soient α un réel, $(a(n))_{n\geq 0}$ une suite β-récursive et $f(n) = e(\alpha a(n))$ sa fonction associée, alors f a la faible propriété de propagation.*

Autrement dit, uniformément pour $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ avec $\rho < \lambda$, le nombre d'entiers l satisfaisant à $0 \leq l < q^\lambda$ tels qu'il existe $(k_1, k_2) \in \{0, \dots, q^\kappa - 1\}^2$ avec

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)}$$

est $O\left(q^{\lambda-\rho+\log\rho}\right)$, la constante implicite ne dépend que de q et de β.

Pour démontrer ce point nous commençons par donner une condition suffisante sur les entiers l pour qu'on puisse remplacer f par $f^{(\kappa+\rho)}$, sa version tronquée, dans la corrélation. Ensuite nous démontrerons que cette condition est suffisamment faible pour assurer le contrôle attendu. Dans la Remarque 1.5.3 nous expliquons pourquoi nous avons eu besoin d'utiliser cette démarche, pourquoi elle n'est pas nécessaire dans le cas de la suite qui compte le nombre de '11' en base 2, et pourquoi l'exposant du terme d'erreur est augmenté d'un $\log\rho$ à sa puissance.

Proposition 1.5.2. *Soient $(a(n))_{n\geq 0}$ une suite β-récursive, et f sa fonction associée. Soient $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ avec $\rho < \lambda$ et $\kappa \geq 1$. Soient des entiers $l > q^\rho$ et $k_1 < q^\kappa$. Supposons qu'il existe un entier m tel que $0 \leq m < \rho - \beta + 2$ avec $\epsilon_{\kappa+m}(lq^\kappa + k_1) \neq q - 1$ et que, si on note i le plus petit de ces m, il existe un entier j vérifiant $i + \beta - 2 < j < \rho$ et $\epsilon_{\kappa+j}(lq^\kappa + k_1) \neq 0$.*

Alors pour tout entier $k_2 < q^\kappa$:

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} = f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)}.$$

Démonstration. Nous commençons par démontrer que, sous ces conditions, la valeur $a(n)$ a bien la forme donnée par la Proposition 1.3.2. Il est en effet possible que les entiers considérés n'aient pas assez de chiffres.

On note $n_1 = lq^\kappa + k_1$, $n_1' = n_1 \bmod q^{\kappa+\rho}, N_1 = T_q(n_1)$ et $N_1' = T_q(n_1')$, autrement dit N_1 (respectivement N_1') est l'indice du dernier chiffre non nul de n_1 (respectivement n_1'). Par définition de n_1', nous avons pour tout entier $0 \leq k < \kappa + \rho$ que $\epsilon_k(n_1) = \epsilon_k(n_1')$ et nous avons également $N_1 \geq N_1'$.

Par hypothèse, il existe un entier j, avec $i + \beta - 2 < j < \rho$ et $\epsilon_{\kappa+j}(n_1) \neq 0$. Comme $i \geq 0$, nous pouvons dire que j vérifie $\beta - 2 < j < \rho$. Nous obtenons donc $N_1 \geq N_1' \geq \kappa + j > \kappa + \beta - 2 \geq \beta - 2$, donc $N_1 \geq N_1' \geq \beta - 1$.

On pose à présent $n_2 = n_1 + k_2$ de sorte à perturber n_1 dans les conditions voulues, $n_2' = n_2 \bmod q^{\kappa+\rho}$ ainsi que $N_2 = T_q(n_2)$ et $N_2' = T_q(n_2')$ leur dernier chiffre respectif. Il ne peut y avoir de différence entre les grands chiffres de n_1 et n_2 que dans le cas d'une propagation de retenue sur les chiffres de n_1. Or, si on veut une propagation jusqu'au chiffre $\kappa + r$, il faut que les chiffres compris entre κ et $\kappa + r - 1$ de n_1 soient tous égaux à $q - 1$. Ainsi, par hypothèse, une propagation éventuelle de retenue s'arrête à $\kappa + i$. Nous avons donc que pour tout $k > i$,

$$\epsilon_{\kappa+k}(n_1) = \epsilon_{\kappa+k}(n_2). \tag{1.9}$$

Cependant, nous avons $\beta \geq 2$, et donc $N_1, N_1' \geq \kappa + j > \kappa + i + \beta - 2 \geq \kappa + i$. Ceci veut donc dire que le dernier chiffre significatif de n_1' n'a pas été affecté par la

propagation, et donc entre autres que $N_1' = N_2'$ et $N_1 = N_2$. La Proposition 1.3.2 s'applique donc, si bien que :

$$\begin{aligned}
a(n_1) =& a\Big(\varphi\Big(\epsilon_{N_1}(n_1)\cdot\epsilon_{N_1-1}(n_1)\cdots\epsilon_{N_1-\beta+2}(n_1)\Big)\Big)\\
&+\sum_{l=0}^{N_1-\beta+1} g\Big(\epsilon_{l+\beta-1}(n_1)\cdots\epsilon_{l+1}(n_1)\cdot\epsilon_l(n_1)\Big),\\
a(n_1') =& a\Big(\varphi\Big(\epsilon_{N_1'}(n_1')\cdot\epsilon_{N_1'-1}(n_1')\cdots\epsilon_{N_1'-\beta+2}(n_1')\Big)\Big)\\
&+\sum_{l=0}^{N_1'-\beta+1} g\Big(\epsilon_{l+\beta-1}(n_1')\cdots\epsilon_{l+1}(n_1')\cdot\epsilon_l(n_1')\Big),\\
a(n_2) =& a\Big(\varphi\Big(\epsilon_{N_1}(n_2)\cdot\epsilon_{N_1-1}(n_2)\cdots\epsilon_{N_1-\beta+2}(n_2)\Big)\Big)\\
&+\sum_{l=0}^{N_1-\beta+1} g\Big(\epsilon_{l+\beta-1}(n_2)\cdots\epsilon_{l+1}(n_2)\cdot\epsilon_l(n_2)\Big)
\end{aligned}$$

et

$$\begin{aligned}
a(n_2') =& a\Big(\varphi\Big(\epsilon_{N_1'}(n_2')\cdot\epsilon_{N_1'-1}(n_2')\cdots\epsilon_{N_1'-\beta+2}(n_2')\Big)\Big)\\
&+\sum_{l=0}^{N_1'-\beta+1} g\Big(\epsilon_{l+\beta-1}(n_2')\cdots\epsilon_{l+1}(n_2')\cdot\epsilon_l(n_2')\Big).
\end{aligned}$$

Ceci conduit à :

$$\begin{aligned}
f(n_1)\overline{f(n_2)f(n_1')}f(n_2') = e\Bigg(\alpha\Bigg(& a\Big(\varphi\Big(\epsilon_{N_1}(n_1)\cdot\epsilon_{N_1-1}(n_1)\cdots\epsilon_{N_1-\beta+2}(n_1)\Big)\Big) && (1.10)\\
&- a\Big(\varphi\Big(\epsilon_{N_1}(n_2)\cdot\epsilon_{N_1-1}(n_2)\cdots\epsilon_{N_1-\beta+2}(n_2)\Big)\Big) && (1.11)\\
&- a\Big(\varphi\Big(\epsilon_{N_1'}(n_1')\cdot\epsilon_{N_1'-1}(n_1')\cdots\epsilon_{N_1'-\beta+2}(n_1')\Big)\Big) && (1.12)\\
&+ a\Big(\varphi\Big(\epsilon_{N_1'}(n_2')\cdot\epsilon_{N_1'-1}(n_2')\cdots\epsilon_{N_1'-\beta+2}(n_2')\Big)\Big) && (1.13)\\
&+\sum_{l=N_1'-\beta+2}^{N_1-\beta+1}\Big[g\Big(\epsilon_{l+\beta-1}(n_1)\cdots\epsilon_{l+1}(n_1)\cdot\epsilon_l(n_1)\Big) && (1.14)\\
&\qquad -g\Big(\epsilon_{l+\beta-1}(n_2)\cdots\epsilon_{l+1}(n_2)\cdot\epsilon_l(n_2)\Big)\Big]\Bigg)\Bigg).
\end{aligned}$$

Il ne nous reste plus qu'à démontrer que le membre de droite vaut 1. Ceci vient du fait que la retenue ne s'est pas propagée assez loin. En effet, comme $N_1' \geq \kappa+j > \kappa+i+\beta-2$, on a $N_1'-\beta+2 > \kappa+i$, et donc, pour tout $N_1'-\beta+2 \leq l \leq N_1$, par (1.9), nous avons $\epsilon_l(n_1) = \epsilon_l(n_2)$, et donc :

$$\sum_{l=N_1'-\beta+2}^{N_1-\beta+1} \Big[g\Big(\epsilon_{l+\beta-1}(n_1)\cdots\epsilon_{l+1}(n_1)\cdot\epsilon_l(n_1)\Big) - g\Big(\epsilon_{l+\beta-1}(n_2)\cdots\epsilon_{l+1}(n_2)\cdot\epsilon_l(n_2)\Big)\Big] = 0.$$

En appliquant le même raisonnement pour (1.10) à (1.13), on trouve

$$f(n_1)\overline{f(n_2)f(n_1')}f(n_2') = 1,$$

ce qui est bien le résultat voulu. □

Preuve de la Proposition 1.5.1. Pour commencer, on remarque que si $lq^\kappa + 2(q^\kappa - 1) < q^{\kappa+\rho}$, on a $f(lq^\kappa+k_1+k_2)\overline{f(lq^\kappa+k_1)} = f^{(\kappa+\rho)}(lq^\kappa+k_1+k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa+k_1)}$. En effet, comme $k_1, k_2 \in \{0,\dots,q^\kappa-1\}$, on a toujours $lq^\kappa+k_1+k_2 < q^{\kappa+\rho}$ et donc $lq^\kappa+k_1+k_2 = lq^\kappa+k_1+k_2 \mod q^{\kappa+\rho}$.

Soit maintenant $l \geq q^\rho$. La Proposition 1.5.2 donne des conditions à vérifier pour que (1.3) ne soit pas réalisée. On peut donc écrire que l'ensemble

$$\Big\{0 \leq l < q^\lambda : \exists\, 0 \leq k_1, k_2 < q^\kappa : \\ f(lq^\kappa+k_1+k_2)\overline{f(lq^\kappa+k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa+k_1+k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa+k_1)}\Big\}$$

est inclus dans l'union $A \cup B \cup C$ avec

$$\begin{aligned}
A &:= \Big\{q^\rho \leq l < q^\lambda :\ \exists\, 0 \leq k_1 < q^\kappa : \forall\, 0 \leq i < \rho-\beta+2,\ \epsilon_{\kappa+i}(lq^\kappa+k_1) = q-1\Big\},\\
B &:= \Big\{q^\rho \leq l < q^\lambda :\ \exists\, 0 \leq k_1 < q^\kappa : \exists\, 0 \leq i < \rho-\beta+2,\ \epsilon_{\kappa+i}(lq^\kappa+k_1) \neq q-1,\\
&\qquad \forall m < i, \epsilon_{\kappa+m}(lq^\kappa+k_1) = q-1, \qquad \forall j\ :\ i+\beta-2 < j < \rho,\\
&\qquad\qquad \epsilon_{\kappa+j}(lq^\kappa+k_1) = 0\},\\
C &:= \Big\{l :\ lq^\kappa \leq q^{\kappa+\rho} \leq lq^\kappa + 2(q^\kappa-1)\Big\}.
\end{aligned}$$

Cependant $(q^\rho-2)q^\kappa + 2(q^\kappa-1) = q^{\kappa+\rho}-2 < q^{\kappa+\rho}$ implique $l \geq q^\rho-1$, et on déduit que $C = \{q^\rho-1, q^\rho\}$.
Il nous reste donc à évaluer les cardinaux de A et B. Pour ce faire on remarque que, quel que soit $k_1 < q^\kappa$, nous avons $\epsilon_{\kappa+i}(lq^\kappa+k_1) = \epsilon_i(l)$, ce qui nous permet de dire que :

$$\begin{aligned}
A &= \{q^\rho \leq l < q^\lambda :\ \exists\, 0 \leq k_1 < q^\kappa :\ \forall\, 0 \leq i < \rho-\beta+2,\ \epsilon_{\kappa+i}(lq^\kappa+k_1) = q-1\}\\
&= \{q^\rho \leq l < q^\lambda :\ \forall\, 0 \leq i < \rho-\beta+2,\ \epsilon_i(l) = q-1\},
\end{aligned}$$

donc

$$\#A = \frac{q^\lambda - q^\rho}{q^{\rho-\beta+2}} = q^{\beta-2}\left(q^{\lambda-\rho}-1\right).$$

On peut d'autre part écrire $B = \cup_{i=0}^{\rho-\beta+1} B_i$ avec

$$\begin{aligned} B_i = \Big\{ & q^\rho \leq l < q^\lambda : \ \exists\, 0 \leq k_1 < q^\kappa : \ 0 < \epsilon_{\kappa+i}(lq^\kappa + k_1) < q-1, \\ & \forall\, m < i, \epsilon_{\kappa+m}(lq^\kappa + k_1) = q-1, \\ & \text{et pour tout } j \text{ tel que } i+\beta-2 < j < \rho,\ \epsilon_{\kappa+j}(lq^\kappa + k_1) = 0\} \\ = \Big\{ & q^\rho \leq l < q^\lambda : \ \exists\, 0 \leq k_1 < q^\kappa : \ 0 < \epsilon_i(l) < q-1, \quad \forall\, m < i, \epsilon_m(l) = q-1, \\ & \text{et pour tout } j \text{ tel que } i+\beta-2 < j < \rho,\ \epsilon_j(l) = 0\}\,. \end{aligned}$$

Mais comme tous les B_i sont en bijection entre eux, on a $\#B = (\rho-\beta+2)\#B_0$. Enfin, on a

$$\begin{aligned} \#B_0 &= \#\{q^\rho \leq l < q^\lambda : \forall j : \ \beta-2 < j < \rho,\ \epsilon_j(l) = 0\} \\ &= \frac{q^\lambda - q^\rho}{q^{\rho-\beta+1}} = q^{\beta-1}\left(q^{\lambda-\rho} - 1\right). \end{aligned}$$

En mettant les trois estimations ensemble, on trouve :

$$\begin{aligned} \#\Big\{ & 0 \leq l < q^\lambda : \exists\, 0 \leq k_1, k_2 < q^\kappa : \\ & f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)}\Big\} \\ & \leq q^{\beta-2}\left(q^{\lambda-\rho} - 1\right) + (\rho-\beta+2)q^{\beta-1}\left(q^{\lambda-\rho} - 1\right) + 2 \ll q^\beta(q^{\lambda-\rho+\log\rho}). \end{aligned}$$

Comme q^β est une constante ne dépendant que de q et β, la fonction est bien de faible propagation.

□

Remarque 1.5.3. *Dans [MR15], Mauduit et Rivat étudient le cas particulier de la suite de Rudin-Shapiro. Pour cette suite, la décomposition de la Proposition 1.3.2 se fait automatiquement car*

(A) $a(k) = 0$ *pour tout* $0 \leq k < q$

(B) $g(a \cdot b) \neq 0 \Leftrightarrow a = b = 1$.

Ainsi on peut écrire, en notant $N = T_q(n)$ *et* $N_\lambda = T_q(n \mod q^\lambda)$ *:*

$$\begin{aligned} a(n) - a^{(\lambda)}(n) &= a(\epsilon_N(n)) - a(\epsilon_{N_\lambda}(n)) + \sum_{i=N_\lambda}^{N-1} g(\epsilon_{i+1}(n)\cdot\epsilon_i(n)) \\ &= \sum_{i=\lambda}^{N-1} g(\epsilon_{i+1}(n)\cdot\epsilon_i(n)), \end{aligned}$$

car on sait qu'alors, pour tout $N_\lambda < i < \lambda$, $\epsilon_i(n) = 0$, *et donc* $g(\epsilon_{i+1}(n)\cdot\epsilon_i(n)) = 0$, *en vertu de (B). Ceci permet alors de dire, en reprenant les notations de la démonstration de la Proposition 1.5.2, que*

$$a(n_1) - a(n_2) - a(n_1') + a(n_2') = \sum_{i=\lambda}^{N-1} g(\epsilon_{i+1}(n_1)\cdot\epsilon_i(n_1)) - \sum_{i=\lambda}^{N-1} g(\epsilon_{i+1}(n_2)\cdot\epsilon_i(n_2)), \quad (1.15)$$

et pour avoir (1.15) = 0*, il suffit de s'assurer que* $\epsilon_i(n_1) = \epsilon_i(n_2)$ *dès que* i *dépasse* λ*.*

Si on suppose uniquement l'existence d'un chiffre d'indice $\kappa \leq m < \lambda$ *tel que* $\epsilon_m(n_1) \neq q-1$*, alors cette condition est assurée (car la propagation ne pourra se faire au-delà du* m*, et on a effectivement* $\lambda > m$*).*

Ce raisonnement tient dès que l'on demande

$$a(\epsilon_{N_\lambda}(n)) = \sum_{i=N_\lambda}^{\lambda-1} g(\epsilon_{i+1}(n) \cdot \epsilon_i(n)), \tag{1.16}$$

et s'étend assez facilement pour la forme des suites blocs-additives (1.8)*.*

Dans le cas général on peut autoriser $g(0\cdots0) \neq 0$ *(par exemple si on compte le nombre de blocs* 00*). Il faut alors nous assurer que la décomposition de la Proposition 1.3.2 s'arrête au bon endroit, c'est-à-dire au dernier chiffre non nul, et c'est en partie pour ceci qu'on passe par les conditions (1.5) et (1.6).*

Il y a de grandes possibilités que la condition (1.16) ne soit pas vérifiée. La condition sur j *dans la Proposition 1.5.2 devient nécessaire pour obtenir* (1.14) = 1 *: elle assure que les chiffres entre* $N_1' - \beta + 2$ *et* N_1' *de* n_1 *et* n_2 *sont identiques.*

Si i *est l'indice du premier chiffre non égal à* $q-1$*, la propagation de retenue s'arrête à* i *et si* N_1' *est le dernier chiffre non nul de* n_1'*, les chiffres de* n_1 *et* n_2 *sont identiques si* $i \leq N_1' - \beta + 2$*. L'introduction d'un chiffre non nul entre* $i + \beta - 2$ *et* N_1' *permet de s'assurer cette condition. C'est une fenêtre de sécurité.*

Cette fenêtre de sécurité fait apparaître l'ensemble B *dans la preuve de la Proposition 1.5.1 (l'ensemble* A *est issu de la condition sur* m*, et l'ensemble* C*, lui, est un ensemble exceptionnel). Enfin, c'est cet ensemble* B *qui donne la majoration en* $q^{\log \rho}$*.*

Il convient désormais de montrer que les fonctions associées aux suites β-récursives vérifient l'équation

$$\left| \frac{1}{q^N} \sum_{n<q^N} f(q^\kappa n) e(nt) \right| \leq q^{-\gamma(N)}, \tag{1.17}$$

pour tout entier positif κ, avec $\gamma(N)$ tendant vers l'infini de manière croissante. La partie suivante sert à introduire des notions qui permettent ce genre de contrôle.

1.6 Généalogie des fonctions

La preuve de la propriété de Fourier pour la suite $(b_d(n))_{n\geq 0}$ développée dans [MR15] explicite un graphe et l'étudie (Figure 1 de l'introduction). Il est possible d'imiter cette preuve dans le cas où on compte le nombre de blocs '012', c'est-à-dire de trouver un graphe associé à cette suite (Figure 2 de l'introduction) et de l'étudier. Il s'avère que ce graphe est directement lié à la fonction regardée $\mathbb{1}_{012}$ et que le graphe qu'ont trouvé Mauduit et Rivat est directement lié à la fonction $\mathbb{1}_{1\cdots1}$.

Dans cette partie, nous donnons un graphe $\mathbb{G}$ qui lie une suite β-récursive, quelle qu'elle soit, à sa propriété de Fourier. Dans le but d'expliciter ce lien, nous définissons tout un panel d'objets liés aux suites β-récursives. Ces objets interviennent explicitement dans $\mathbb{G}$. Les sommets de $\mathbb{G}$ sont par exemple, et contrairement à [MR15],

directement liés à la fonction, et sont en bijection avec $\Sigma_{\beta-1}^*$, les mots de taille au plus $\beta-1$.

Nous définissons en premier lieu les sommets de $\mathbb{G}$:

Définition 1.6.1. *Soient $f : \mathbb{N} \to \mathbb{U}$ une application et ω un mot. On pose*

$$f_\omega(n) := f\Big(q^{|\omega|}n + \varphi(\omega)\Big), \tag{1.18}$$

où φ a été introduite dans la Partie 1.3.

Le lemme suivant permet de donner une formule de récurrence pour $f_\omega(n)$ si f est associée à une suite β-récursive : il fournit les arêtes de $\mathbb{G}$.

Lemme 1.6.2. *Si f est la fonction associée d'une suite β-récursive, alors :*

$$f_\omega(qn+r) = \begin{cases} f_{\hat{r}\cdot\omega}(n) & si \quad |\omega| < \beta-1; \\ f_{\hat{r}\cdot\overline{\omega}^{|\omega|-1}}(n)e\Big(\alpha g(\hat{r}\cdot\omega)\Big) & si \quad |\omega| = \beta-1. \end{cases} \tag{1.19}$$

Démonstration. Par (1.18) :

$$\begin{aligned} f_\omega(qn+r) &= f\Big(q^{|\omega|}(qn+r) + \varphi(\omega)\Big) \\ &= f\Big(q^{|\omega|+1}n + q^{|\omega|}r + \varphi(\omega)\Big) \\ &= f\Big(q^{|\hat{r}\cdot\omega|}n + \varphi(\hat{r}\cdot\omega)\Big). \end{aligned}$$

Puisque $f(n) = e(\alpha a(n))$, on conclut en utilisant (1.18) si $|\omega| < \beta-1$ (donc $|\hat{r}\cdot\omega| < \beta$), et en utilisant (1.5) ainsi que (1.18) si $|\omega| = \beta-1$, donc $|\hat{r}\cdot\omega| = \beta$. □

Soit n un entier et γ un mot tel que $\varphi(\gamma) = n$. En définissant

$$f_\omega(n) = f(q^{|\omega|}n + \varphi(\omega)) = f(\varphi(\gamma\cdot\omega)),$$

on isole le suffixe ω. Le Lemme 1.6.2 décrit l'évolution des valeurs de f lorsqu'on change n en $qn+r$, c'est-à-dire lorsqu'on insère la lettre $\hat{r}$ dans le mot $\gamma\cdot\omega$ juste avant le suffixe ω ($\gamma\cdot\omega \mapsto \gamma\cdot\hat{r}\cdot\omega$).Tant que la taille du suffixe $\hat{r}\cdot\omega$ ne dépasse pas $\beta-1$, on ne modifie pas f mais on isole le suffixe $\hat{r}\cdot\omega$ en considérant $f_{\hat{r}\cdot\omega}$.

Si en revanche $|\hat{r}\cdot\omega| = \beta$, on remplace le suffixe ω par $\hat{r}\cdot\overline{\omega}^{|\omega|-1}$ (on efface la dernière lettre de ω et on insère $\hat{r}$ à la première lettre) et f est altéré par une multiplication par $e(\alpha g(\hat{r}\cdot\omega))$.

Par exemple, si $(a(n))_{n\geq 0}$ est la suite 3-récursive qui compte les blocs '011' dans l'écriture *finie* de n en base 2, nous avons $f_\epsilon(n) = e(\alpha a(n))$, $f_0(n) = e(\alpha a(2n))$, $f_1(n) = e(\alpha a(2n+1))$, etc. Puis $f_{011}(n) = f_{11}(2n+0) = e(\alpha)f_{01}(n) = e(\alpha)e(\alpha a(4n+1))$.

Nous introduisons à présent un ordre pseudo-lexicographique dans le but d'expliciter la correspondance entre l'équation (1.19) et le graphe $\mathbb{G}$ à travers une formule de récurrence.

Définition 1.6.3. *On munit Σ^* de l'ordre $\preceq$ suivant. Si $|\omega| \leq |\omega'|$, alors $\omega \preceq \omega'$. Si les deux tailles sont égales, on compare les deux mots par leur ordre lexicographique lu de gauche à droite.* Si ψ désigne la fonction qui énumère Σ^*, alors on définit $\phi : \mathbb{N} \to \Sigma^*$ par $\phi = \psi^{-1}$.*

*. Ainsi $00 \preceq 01 \preceq 10 \preceq 000$.

Le Lemme 1.6.2 ne peut pas être exploité directement. Cependant, nous pouvons assembler un ensemble de valeurs possibles de la suite β-récursive dans un même vecteur, et ce vecteur vérifiera une propriété de récurrence.

Définition 1.6.4. *Soit $f : \mathbb{N} \to \mathbb{U}$ une application associée à une suite β-récursive, on définit le vecteur V_n de taille $(q^\beta - 1)/(q-1)$ par*

$$V_n[l] = f_{\phi(l)}(n), \quad 0 \leq l \leq (q^\beta - 1)/(q-1) - 1.$$

On dira que V_n est le n-ième vecteur généalogique de f. On remarque qu'il est de la taille du cardinal de $\Sigma^*_{\beta-1}$.

Nous sommes à présent à même de démontrer la propriété de Fourier pour une fonction f associée à une suite β-récursive. Nous allons exploiter le Lemme 1.6.2 dans le but d'obtenir une formule de récurrence, non pas directement pour

$$\sum_{n<q^N} f(n)e(nt),$$

mais pour

$$S(N,t) := \sum_{n<q^N} V_n e(nt),$$

où V_n est le n-ième vecteur généalogique de f. Il s'en suivra que la propriété de Fourier de f découlera de la majoration de la norme infinie d'une matrice (Corollaire 1.6.7), majoration obtenue par l'étude de $\mathbb{G}$. Nous commençons par expliciter la formule de récurrence.

Par le Lemme 1.6.2, il existe une matrice $M_l(\alpha,t)$ telle que

$$V_{qn+l}e((qn+l)t) = M_l(\alpha,t)V_n e(qnt),$$

et donc il existe une matrice $\widetilde{M}(\alpha,t)$ telle que $S(N,t) = \widetilde{M}(\alpha,t)S(N-\beta, q^\beta t)$. En effet, on peut écrire :

$$\begin{aligned}
S(N,t) &= \sum_{0\leq n<q^N} V_n e(nt) \\
&= \sum_{0\leq n<q^{N-1}} \sum_{0\leq l<q} V_{qn+l}e((qn+l)t) \\
&= \sum_{0\leq n<q^{N-1}} \sum_{0\leq l<q} M_l(\alpha,t)V_n e(qnt) \\
&= \sum_{0\leq l<q} M_l(\alpha,t) \sum_{0\leq n<q^{N-1}} V_n e(qnt) \\
&= M(\alpha,t)S(N-1,qt) \\
&= \dots \\
&= \left(\prod_{0\leq k<\beta} M(\alpha,q^k t)\right) S(N-\beta,q^\beta t) \\
&= \widetilde{M}(\alpha,t)S(N-\beta,q^\beta t),
\end{aligned}$$

où on a posé $M(\alpha,t)=\sum_{0\le l<q} M_l(\alpha,t)$ et $\widetilde{M}(\alpha,t)=\prod_{0\le k<\beta} M(\alpha,q^k t)$. On dit que $\widetilde{M}(\alpha,t)$ est la matrice généalogique de f. En itérant cette propriété avec $q^\beta t$ à la place de t, en passant par la norme infinie et en remarquant que $N-N \bmod \beta=\beta\lfloor N/\beta\rfloor$, on obtient :

$$\begin{aligned}\left\|\sum_{0\le n<q^N} V_n e(nt)\right\|_\infty &\le \prod_{i=0}^{\lfloor N/\beta\rfloor-1}\left\|\widetilde{M}(\alpha,q^{i\beta}t)\right\|_\infty \left\|\sum_{n<q^{N \bmod \beta}} V_n e(q^{\beta\lfloor N/\beta\rfloor}nt)\right\|_\infty\\ &\le \prod_{i=0}^{\lfloor N/\beta\rfloor-1}\left\|\widetilde{M}(\alpha,q^{i\beta}t)\right\|_\infty \sum_{n<q^{N \bmod \beta}}\left\|V_n e(q^{\beta\lfloor N/\beta\rfloor}nt)\right\|_\infty\\ &\le \prod_{i=0}^{\lfloor N/\beta\rfloor-1}\left\|\widetilde{M}(\alpha,q^{i\beta}t)\right\|_\infty q^{N \bmod \beta}. \qquad (1.20)\end{aligned}$$

Les deux propositions suivantes sont destinées à faire le lien entre la matrice généalogique et l'estimation (1.17).

Proposition 1.6.5. *Pour tout entier $\kappa\ge\beta$, on a*

$$\left|\sum_{n<q^N} f(q^\kappa n)e(-nt)\right|=\left|\sum_{n<q^N} f(q^{\beta-1}n)e(-nt)\right|.$$

Démonstration. Nous allons montrer par récurrence que, pour tout $0\le r\le\kappa-\beta+1$: $a(q^\kappa n)=a(q^{\kappa-r}n)+rg(0\cdot 0\cdots 0)$ où $0\cdot 0\cdots 0$ est de taille β.

Le cas $r=0$ est clair.

Montrons l'hérédité. Supposons qu'on ait l'hypothèse de récurrence pour un certain $r\le\kappa-\beta$. Alors :

$$\begin{aligned}a(q^\kappa n)&=a(q^{\kappa-r}n)+rg(0\cdots 0)\\ &=a(q^{\kappa-r}n+\varphi(0\cdot 0\cdots 0))+rg(0\cdots 0)\\ &=a(q^{\kappa-r-1}n+\varphi(0\cdots 0))+(r+1)g(0\cdots 0),\end{aligned}$$

où à la dernière étape, on a appliqué (1.5), ce qui est licite parce que $\kappa-r>\beta-1$. La récurrence est donc terminée.

Le cas $r=\kappa-\beta+1$ dans la formule que l'on vient de montrer correspond à $a(q^\kappa n)=a(q^{\beta-1}n)+(\kappa-\beta+1)g(0\cdots 0)$, et comme le second terme est indépendant en n, on a :

$$\begin{aligned}\left|\sum_{n<q^N} f(q^\kappa n)e(-nt)\right|&=\left|\sum_{n<q^N} e(\alpha a(q^\kappa n))e(-nt)\right|\\ &=\left|\sum_{n<q^N} e(\alpha a(q^{\beta-1}n)+\alpha(\kappa-\beta+1)g(0\ldots 0))e(-nt)\right|\\ &=\left|\sum_{n<q^N} e(\alpha a(q^{\beta-1}n))e(-nt)\right|\\ &=\left|\sum_{n<q^N} f(q^{\beta-1}n)e(-nt)\right|.\end{aligned}$$

□

Proposition 1.6.6. *Pour tout entier κ inférieur à β nous avons :*

$$\left|\sum_{n<q^N} f(q^\kappa n)e(-nt)\right| \leq \left\|\sum_{n<q^N} V_n e(-nt)\right\|_\infty .$$

Démonstration. La quantité $f(q^\kappa n)$ correspond à $f_{0^\kappa}(n)$ avec 0^κ le mot de taille κ et n'ayant que des 0 : c'est donc la $(q^\kappa-1)/(q-1)$-ième coordonnée de V_n. □

De ceci on déduit :

Corollaire 1.6.7. *Pour tout entier κ positif, la majoration suivante est valide :*

$$\left|\frac{1}{q^N}\sum_{0\leq n<q^N} f(q^\kappa n)e(-nt)\right| \leq \frac{1}{q^{\beta\lfloor N/\beta\rfloor}} \prod_{i=0}^{\lfloor N/\beta\rfloor-1} \left\|\widetilde{M}(\alpha, q^{i\beta}t)\right\|_\infty .$$

Démonstration. Par les Propositions 1.6.5 et 1.6.6, il vient que, pour tout κ positif :

$$\left|\frac{1}{q^N}\sum_{0\leq n<q^N} f(q^\kappa n)e(-nt)\right| \leq \left\|\sum_{n<q^N} V_n e(-nt)\right\|_\infty .$$

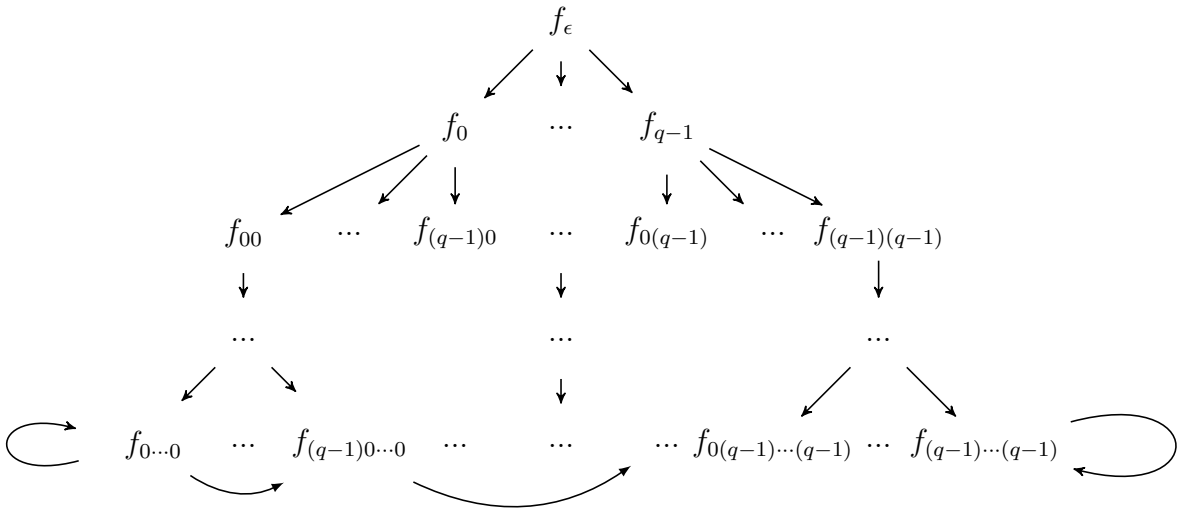
L'équation (1.20) permet donc de conclure. □

D'après le Corollaire 1.6.7, il est désormais important d'avoir un contrôle sur la norme infinie de la matrice $\widetilde{M}(\alpha,t)$. C'est l'objet du résultat suivant.

Proposition 1.6.8.

$$\|\widetilde{M}(\alpha,t)\|_\infty = \sup_{\gamma\in\Sigma^*_{\beta-1}} \sum_{\omega\,\in\,\Sigma_{\beta-1}} \left|\sum_{k\in\Sigma_1} e\left(t(\hat{k}+q\varphi(\omega)) + \alpha\left(\sum_{m\leq|\gamma|} g(\underline{\omega}_{|\omega|-m}\cdot k\cdot\overline{\gamma}^m)\right)\right)\right|. \tag{1.21}$$

Démonstration. Soit $\mathbb{G}$ le graphe suivant :



Soit β un entier supérieur ou égal à 2, γ un mot de taille au plus β-1 donné et f une fonction associée à une suite β-récursive. Le graphe $\mathbb{G}$ représente la manière dont peut évoluer en k étapes (k arbitraire) une fonction f_γ, selon le Lemme 1.6.2. Décrivons-le.

$\mathbb{G}$ est un graphe qui possède β lignes (de 0 à $\beta - 1$) et qui va en descendant. À chaque flèche correspond une altération de l'argument de $f(n)e(-nt)$. Les flèches qui descendent relient une fonction f_γ avec une fonction $f_{\hat{r}\cdot\gamma}$ sans altération d'argument lié à f. Les flèches de la dernière ligne relient une fonction f_γ à une fonction $f_{\hat{r}\overline{\gamma}^{|\gamma|-1}}$ avec une altération de l'argument lié à f de $\alpha g(\hat{r}\cdot\gamma)$. Ce sont les modifications décrites par le Lemme 1.6.2. Chaque élément donne donc q descendants, ainsi le graphe possède $\frac{q^\beta-1}{q-1}$ sommets. Le graphe $\mathbb{G}$ est régi par les règles suivantes.

(i) On suit le sens des flèches.

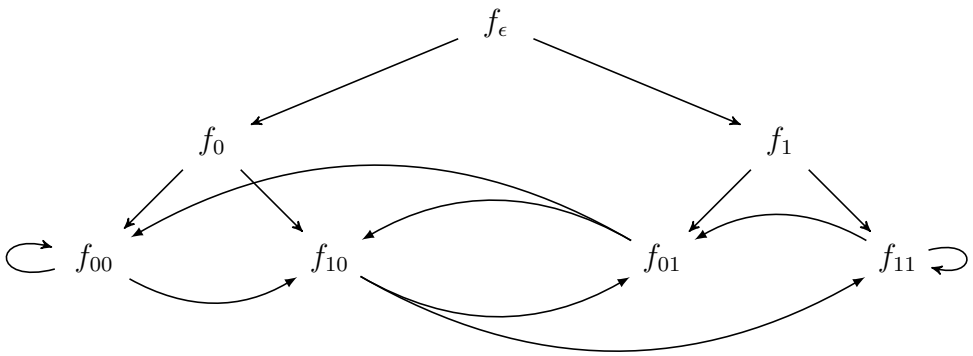
(ii) Si à la k-ième étape, on passe d'un mot γ à un mot γ', avec la taille de γ strictement plus petite que $\beta - 1$, on ajoute $q^{k-1}\hat{\overline{\gamma'}^1}t$ à l'argument.

(iii) Si à la k-ième étape, on passe d'un mot γ à un mot γ', avec la taille de γ égale à $\beta - 1$, on ajoute $q^{k-1}\hat{\overline{\gamma'}^1}t + \alpha g(\overline{\gamma'}^1\cdot\gamma)$ à l'argument.

Désormais, nous appelons encodage d'un chemin la valeur $e(x)$, où x est l'argument total du chemin lorsque ce dernier est soumis aux règles ci-dessus.

Soit à présent $\mathrm{Enc}_k(\gamma,\omega)$, la somme des encodages concernant tous les chemins possibles en k étapes reliant γ à ω.

Exemple 1.6.9. *Le graphe suivant correspond au cas $q = 2$, $\beta = 3$.*



Dans ce graphe il y a deux manières d'aller du mot ϵ au mot 00 en trois étapes (sous les flèches et entre parenthèses correspond l'altération de l'argument) : en faisant le chemin

$$\epsilon \underset{0(+0)}{\to} 0 \underset{0(+0)}{\to} 00 \underset{0(+0)}{\to} 00$$

et en faisant le chemin

$$\epsilon \underset{1(+t)}{\to} 1 \underset{0(+0)}{\to} 01 \underset{0(+0)}{\to} 00.$$

Ceci nous donne donc :

$$Enc_3(\epsilon, 00) = e(\alpha g(000)) + e(t + \alpha g(001)).$$

Ainsi, si $(a(n))_{n\geq 0}$ est la suite qui compte les blocs '011' dans l'écriture finie de n en base 2, pour passer de f_ϵ à f_0, on n'ajoute rien à l'argument, mais pour passer de f_ϵ à f_1, on rajoute t à l'argument ; pour passer de f_0 à f_{00}, on n'ajoute rien à l'argument, de f_0 à f_{10}, on rajoute t à l'argument, etc. La seule flèche qui ajoute un α à l'argument est la flèche qui va de f_{11} à f_{01} : la fonction $g : \Sigma_3 \to \mathbb{N}$ n'est non nulle dans ce cas que pour le mot $\omega = 011$.

Nous avons par exemple $Enc_3(\epsilon, 01) = e(t+qt+\alpha)+e(qt)$ ainsi que $Enc_3(\epsilon, 11) = e(t + qt + q^2t) + e(qt + q^2t)$.

Comme $M_l(\alpha, t)$ est la matrice de passage de V_n à V_{qn+l}, sommer sur l (c'est à dire regarder $M(\alpha, t)$) revient alors à déterminer tous les chemins à une étape possible. Et comme $\widetilde{M}(\alpha, t) = \prod_{l<\beta} M(\alpha, q^l t)$, le coefficient $\widetilde{M}(\alpha, t)[i, j]$ correspond à la somme des encodages de tous les chemins possibles en β étapes reliant $\phi(i)$ à $\phi(j)$.

Nous avons donc :

$$\|\widetilde{M}(\alpha, t)\|_\infty = \sup_i \sum_j |\mathrm{Enc}_\beta(\phi(i), \phi(j))| . \tag{1.22}$$

Comme $\phi(i)$ et $\phi(j)$ parcourent l'ensemble des mots de taille au plus $\beta - 1$, cette formule s'écrit :

$$\|\widetilde{M}(\alpha, t)\|_\infty = \sup_{\gamma\in\Sigma^*_{\beta-1}} \sum_{\omega\,\in\,\Sigma^*_{\beta-1}} |\mathrm{Enc}_\beta(\gamma, \omega)| . \tag{1.23}$$

Cependant, par le Lemme 1.6.2, pour tout mot γ, un descendant de γ à la β-ieme génération est forcément de taille $\beta - 1$.

En effet, la taille du mot va croissant, strictement si la taille est strictement plus petite que $\beta-1$, et devient constante dès que cette taille est atteinte. Or cette taille est atteinte, dans le cas le plus long, au bout de la $\beta - 1$ ième étape. Donc (1.23) se transforme en :

$$\|\widetilde{M}(\alpha, t)\|_\infty = \sup_{\gamma\in\Sigma^*_{\beta-1}} \sum_{\omega\,\in\,\Sigma_{\beta-1}} |\mathrm{Enc}_\beta(\gamma, \omega)| . \tag{1.24}$$

Il reste donc à comprendre $\mathrm{Enc}_\beta(\gamma, \omega)$.

Pour aller à un mot de taille $\beta-1$ en β étapes, il est nécessaire un moment où un autre "d'écraser de l'information". Dans l'exemple, le mot '1' de la première étape du deuxième chemin possible a été effacé dans l'étape finale, et les deux chemins ne diffèrent que par cette première étape. Il arrive dans le cas général un processus similaire, et la preuve de notre proposition consiste à le décrire.

Soit $\gamma \in \Sigma^*_{\beta-1}$. Soient $R \in \Sigma_{\beta-1-|\gamma|}$ et $S \in \Sigma_{|\gamma|+1}$ des mots qui interviendront dans le processus pour aller de γ à ω et seront déterminés ultérieurement. Arriver à un mot de taille $\beta - 1$ se fait en $\beta - 1 - |\gamma|$ étapes, c'est-à-dire par l'adjonction de R. Nous avons donc, en suivant la règle (ii), le chemin suivant :

$$\begin{aligned} \gamma \underset{\epsilon_0(R)t}{\longrightarrow} \underline{R}_1 \cdot \gamma \to \quad \ldots \quad &\to \underline{R}_{i-1} \cdot \gamma \underset{\epsilon_{i-1}(R)q^{i-1}t}{\longrightarrow} \underline{R}_i \cdot \gamma \\ \to \quad \ldots \quad &\to \underline{R}_{|R|-1} \cdot \gamma \underset{\epsilon_{|R|-1}(R)q^{|R|-1}t}{\longrightarrow} R \cdot \gamma. \end{aligned} \tag{1.25}$$

Il nous reste alors $\beta - (\beta - 1 - |\gamma|) = |\gamma| + 1$ étapes à parcourir pour parvenir à ω. Cela ce fait en concaténant S. Cependant comme on a atteint un mot de taille $\beta - 1$, la fonction de propagation g s'adjoint à l'argument (il s'agit de la règle (iii)). Nous avons donc, en suivant cette règle, la chaîne suivante (on ajoute à l'argument ce qui est en bas de la flèche) :

$$
\begin{aligned}
&R \cdot \gamma \underset{\epsilon_0(S) q^{|R|} t + \alpha g(\underline{S}_1 \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|})}{\longrightarrow} \underline{S}_1 \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-1} \qquad (1.26)\\
&\cdots\\
&\underline{S}_i \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-i} \underset{\epsilon_i(S) q^{i+|R|} t + \alpha g(\underline{S}_{i+1} \cdot \overline{R\cdot\gamma}^{|R\cdot\gamma|-i})}{\longrightarrow} \underline{S}_{i+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-i-1}\\
&\cdots\\
&\underline{S}_{|\gamma|} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-|\gamma|} \underset{\epsilon_{|\gamma|}(S) q^{|\gamma|+|R|} t + \alpha g(\underline{S}_{|\gamma|+1} \cdot \overline{R\cdot\gamma}^{|R\cdot\gamma|-|\gamma|})}{\longrightarrow} S \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-|\gamma|-1} = S \cdot \overline{R}^{|R|-1} = \omega.
\end{aligned}
$$

De la dernière ligne on conclut que $S \cdot R = \omega \cdot k$, avec k un mot de taille 1. Il suit donc que :

$$
\begin{aligned}
\underline{S}_{i+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-i} &= \underline{S}_{i+1} \cdot R \cdot \overline{\gamma}^{|\gamma|-i}\\
&= \underline{S \cdot R}_{|R|+i+1} \cdot \overline{\gamma}^{|\gamma|-i}\\
&= \underline{\omega \cdot k}_{\beta-(|\gamma|+1)+i+1} \cdot \overline{\gamma}^{|\gamma|-i}\\
&= \underline{\omega \cdot k}_{|\omega|+1-(|\gamma|+1)+i+1} \cdot \overline{\gamma}^{|\gamma|-i}\\
&= \underline{\omega}_{|\omega|-|\gamma|+i} \cdot k \cdot \overline{\gamma}^{|\gamma|-i}.
\end{aligned}
$$

Comme $0 \leq i \leq |\gamma|$, on a

$$
\begin{aligned}
\{\underline{S}_{i+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-i},\, 0 \leq i \leq |\gamma|\} &= \{\underline{\omega}_{|\omega|-|\gamma|+i} \cdot k \cdot \overline{\gamma}^{|\gamma|-i},\, 0 \leq i \leq |\gamma|\}\\
&= \{\underline{\omega}_{|\omega|-i} \cdot k \cdot \overline{\gamma}^{i},\, 0 \leq i \leq |\gamma|\}. \qquad (1.27)
\end{aligned}
$$

En réunissant (1.25) et (1.26), et en utilisant (1.27), nous obtenons qu'un encodage, suivant le chemin $S \cdot R$ est égal à

$$
\begin{aligned}
&e\left(t\left(\sum_{i=0}^{|R|-1} \epsilon_i(R) q^i + q^{|R|} \sum_{i=0}^{|S|-1} \epsilon_i(S) q^i\right) + \alpha \sum_{m=0}^{|\gamma|} g\left(\underline{S}_{m+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-m}\right)\right)\\
&\qquad = e\left(t\varphi(S \cdot R) + \alpha \sum_{m=0}^{|\gamma|} g\left(\underline{S}_{m+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-m}\right)\right)\\
&\qquad = e\left(t\varphi(\omega \cdot k) + \alpha \sum_{m=0}^{|\gamma|} g\left(\underline{\omega}_{|\omega|-m} \cdot k \cdot \overline{\gamma}^{m}\right)\right)\\
&\qquad = e\left(t\left(\hat{k} + q\varphi(\omega)\right) + \alpha \sum_{m=0}^{|\gamma|} g\left(\underline{\omega}_{|\omega|-m} \cdot k \cdot \overline{\gamma}^{m}\right)\right).
\end{aligned}
$$

En utilisant (1.24), et le fait que k prend toutes les valeurs de Σ_1, on obtient bien (1.21). □

Nous utilisons à présent cette estimation pour obtenir un contrôle uniforme en t de la norme infinie de $\widetilde{M}(\alpha,t)$.

Corollaire 1.6.10. *Soient $\omega_1,\omega_2\in\Sigma_{\beta-1}$, tels que $\underline{\omega_1}_{(\beta-2)}=\underline{\omega_2}_{(\beta-2)}$ mais $\omega_1\neq\omega_2$ [†] et k_1,k_2 deux mots de taille 1 tels que $k_1\neq k_2$. Alors*

$$\|\widetilde{M}(\alpha,t)\|_\infty\leq q^\beta-8\left(\sin\frac{\pi\|\alpha\left(g(\omega_1\cdot k_1)-g(\omega_1\cdot k_2)-g(\omega_2\cdot k_1)+g(\omega_2\cdot k_2)\right)\|_{\mathbb{Z}}}{4}\right)^2. \tag{1.28}$$

Tout d'abord, présentons un lemme trigonométrique, dont on peut retrouver la démonstration dans [MR15]. Nous donnons la preuve pour une meilleure lisibilité. Rappelons que $\|x\|_{\mathbb{Z}}$ représente la distance du réel x au plus proche entier.

Lemme 1.6.11. *Soient x,x',ξ,α des nombres réels. Alors :*

$$|e(x+\alpha')+e(x)|+|e(x'+\xi)+e(x')|\leq 4-8\left(\sin\frac{\pi\|\xi-\alpha'\|_{\mathbb{Z}}}{4}\right)^2. \tag{1.29}$$

Démonstration. En prenant le carré du module et en utilisant $\cos(2\theta)=2(\cos(\theta))^2-1$, on obtient $|e(x+\alpha')+e(x)|\leq 2|\cos(\pi\alpha')|$.

Enfin, en posant

$$\xi'=\begin{cases}\xi & \text{si } \cos(\pi\alpha') \text{ et } \cos(\pi\xi) \text{ sont de même signe}\\ \xi+1 & \text{sinon,}\end{cases}$$

on obtient en utilisant $\cos a+\cos b=2\cos\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right)$:

$$\begin{aligned}|\cos(\pi\alpha')|+|\cos(\pi\xi)|&\leq 2\left|\cos\pi\frac{\xi'-\alpha'}{2}\right|\\&\leq 2\cos\pi\frac{\|\xi-\alpha'\|_{\mathbb{Z}}}{2}.\end{aligned}$$

On conclut en utilisant $\cos 2\theta=1-2(\sin\theta)^2$. □

Démonstration du Corollaire 1.6.10. En majorant trivialement (1.21), dans les cas où on a $\omega\neq\omega_1,\omega_2$, $k\neq k_1,k_2$, nous obtenons :

$$\|\widetilde{M}(\alpha,t)\|_\infty=\sup_{\gamma\in\Sigma^*_{\beta-1}}\left(q^\beta-4+\sum_{i=1,2}\left|\sum_{j=1,2}e\left(t(\hat{k_j}+q\varphi(\omega_i))+\alpha\left(\sum_{m\leq|\gamma|}g(\underline{\omega_i}_{|\omega_i|-m}\cdot k_j\cdot\overline{\gamma}^m)\right)\right)\right|\right).$$

†. Les mots ω_1 et ω_2 diffèrent par leur première lettre $\epsilon_{\beta-2}$, par exemple $\omega_1=10000000$ et $\omega_2=00000000$

On pose alors

$$\begin{aligned} x &= t(\hat{k_1} + q\varphi(\omega_1)) + \alpha \sum_{m\leq|\gamma|} g(\underline{\omega_1}_{|\omega_1|-m} \cdot k_1 \cdot \overline{\gamma}^m), \\ \alpha' &= t(\hat{k_2} - \hat{k_1}) + \alpha \sum_{m\leq|\gamma|} \left(g(\underline{\omega_1}_{|\omega_1|-m} \cdot k_2 \cdot \overline{\gamma}^m) - g(\underline{\omega_1}_{|\omega_1|-m} \cdot k_1 \cdot \overline{\gamma}^m)\right), \\ x' &= t(\hat{k_1} + q\varphi(\omega_2)) + \alpha \sum_{m\leq|\gamma|} g(\underline{\omega_2}_{|\omega_2|-m} \cdot k_1 \cdot \overline{\gamma}^m) \\ \text{et} \quad \xi &= t(\hat{k_2} - \hat{k_1}) + \alpha \sum_{m\leq|\gamma|} \left(g(\underline{\omega_2}_{|\omega_2|-m} \cdot k_2 \cdot \overline{\gamma}^m) - g(\underline{\omega_2}_{|\omega_2|-m} \cdot k_1 \cdot \overline{\gamma}^m)\right). \end{aligned} \tag{1.30}$$

Si bien que

$$\|\widetilde{M}(\alpha,t)\|_\infty = \sup_{\gamma\in\Sigma^*_{\beta-1}} \Big(q^\beta - 4 + |e(x) + e(\alpha' + x)| + |e(x') + e(x' + \xi)|\Big). \tag{1.31}$$

Or

$$\begin{aligned} \xi - \alpha' = \alpha \Bigg(&\sum_{m\leq|\gamma|} \left(g(\underline{\omega_2}_{|\omega_2|-m} \cdot k_2 \cdot \overline{\gamma}^m) - g(\underline{\omega_2}_{|\omega_2|-m} \cdot k_1 \cdot \overline{\gamma}^m)\right) \\ &- \sum_{l\leq|\gamma|} \left(g(\underline{\omega_1}_{|\omega_1|-l} \cdot k_2 \cdot \overline{\gamma}^l) - g(\underline{\omega_1}_{|\omega_1|-l} \cdot k_1 \cdot \overline{\gamma}^l)\right)\Bigg). \end{aligned} \tag{1.32}$$

Pour tout $1 \leq m \leq |\omega_1|$, nous avons par hypothèse $\underline{\omega_1}_{|\omega_1|-m} = \underline{\omega_2}_{|\omega_1|-m}$. Ainsi le seul terme non nul dans (1.32) est le terme en $m = 0$, et donc :

$$\xi - \alpha' = \alpha \left(g(\omega_1 \cdot k_1) - g(\omega_1 \cdot k_2) - g(\omega_2 \cdot k_1) + g(\omega_2 \cdot k_2)\right). \tag{1.33}$$

On majore donc (1.31) en utilisant le Lemme 1.6.11, ce qui donne $\|\tilde{M}(\alpha,t)\|_\infty \leq q^\beta - 8\left(\sin\dfrac{\pi\|\xi-\alpha'\|_\mathbb{Z}}{4}\right)^2$ et on conclut avec (1.33). □

1.7 Preuve du Théorème 1.2.5

La preuve du Théorème 1.2.3 de Mauduit et Rivat est technique. Notre Théorème 1.2.5 étant une déclinaison du Théorème 1.2.3, nous ne présentons pas ici toute la preuve, mais seulement les éléments modifiés. Nous suivrons pas à pas, mais en étant elliptique, la démonstration de Mauduit et Rivat.

Pour cette partie, si μ_0 et μ_2 sont des entiers avec $\mu_0 \leq \mu_2$, en considérant l'écriture unique suivante :

$$n = u_2 q^{\mu_2} + u_1 q^{\mu_0} + u_0,$$

avec u_0, u_1, u_2 des entiers tels que $0 \leq u_0 < q^{\mu_0}$ et $0 \leq u_1 < q^{\mu_2-\mu_0}$ alors nous définissons

$$r_{\mu_0,\mu_2}(n) = u_1. \tag{1.34}$$

La preuve du Théorème 1.2.3 consiste à évaluer des sommes de type I et de type II et à utiliser une identité de Vaughan. La modification de la Définition 1.2.1 altère l'estimation de ces deux sommes. Nous allons dans un premier temps traiter, en indiquant seulement les modifications, les sommes $S_I(\vartheta)$ et $S_{II}(\vartheta)$, puis nous évaluerons $\sum_{n<N}\Lambda(n)f(n)e(\vartheta n)$ avec ces deux nouvelles estimations. Les sommes de type I et de type II sont régulièrement utilisées pour estimer des sommes avec la fonction de von Mangoldt.

Une des idées principales que nous pouvons dégager des travaux de Mauduit et Rivat pourrait être résumée ainsi : on peut très souvent remplacer une fonction définie à l'aide des chiffres par une fonction tronquée (au sens où nous l'avons défini peu avant la Définition 1.2.1). La Définition 1.2.1 est une formalisation de cette idée. Le fait de pouvoir tronquer nous permet d'utiliser l'analyse de Fourier dans les évaluations des sommes de type I et II.

1.7.1 Sommes de type I

Soient M et N des entiers, avec $1 \leq M \leq N$ et $M \leq (MN)^{1/3}$. Nous notons μ et ν les entiers tels que $T_q(M) = \mu - 1$ et $T_q(N) = \nu - 1$.

Soient $\vartheta \in \mathbb{R}$ et $I(M,N) \subset [0, MN]$ un intervalle. Notre but est d'estimer

$$S_I(\vartheta) := \sum_{M/q \leq m < M} \left| \sum_{\substack{n \\ mn \in I(M,N)}} f(mn)e(\vartheta mn) \right|. \tag{1.35}$$

Dans [MR15], le contrôle de $S_I(\vartheta)$ utilise uniquement la Définition 1.2.1, à travers un ensemble apparaissant lors de l'équation [MR15, (35)], que Mauduit et Rivat notent $\widetilde{\mathcal{W}_\kappa}$. Cet ensemble désigne l'ensemble des couples d'entiers $(u,v) \in \{0,\dots,q^\kappa - 1\} \times \{0,\dots,q^{\mu+\nu-\kappa}-1\}$ pour lesquels

$$f(u+vq^\kappa)\overline{f(vq^\kappa)} \neq f^{(\kappa+\rho_1)}(u+vq^\kappa)\overline{f^{(\kappa+\rho_1)}(vq^\kappa)}.$$

Ici, κ est un entier tel que $1 \leq \kappa \leq \frac{\mu+\nu}{3}$ et ρ_1 est un paramètre entier vérifiant $1 \leq \rho_1 \leq \mu+\nu-\kappa$ que l'on optimisera ultérieurement.

Avec ces notations, Mauduit et Rivat estiment le cardinal de $\widetilde{\mathcal{W}_\kappa}$ par

$$\operatorname{card} \widetilde{\mathcal{W}_\kappa} \ll q^{\mu+\nu-\rho_1}. \tag{1.36}$$

Lorsque nous estimons ce cardinal avec nos modifications nous obtenons donc :

$$\operatorname{card} \widetilde{\mathcal{W}_\kappa} \ll q^{\mu+\nu-\rho_1+\log\rho_1}. \tag{1.37}$$

Étudions l'incidence de cette modification dans $S_I(\vartheta)$. Les auteurs séparent la somme S_I en deux parties, qu'ils nomment $S'_{I,1}(\vartheta')$ et $S'_{I,2}(\vartheta')$. Plus précisément, ils utilisent [MR15, equations (31), (32), (36)],

$$S_I(\vartheta) \ll q^{\mu+\nu}\log(q^{\mu+\nu})(S'_{I,1}(\vartheta') + S'_{I,2}(\vartheta')). \tag{1.38}$$

Dans la première somme, $S'_{I,1}$, la fonction f est remplacée par sa fonction tronquée, la seconde somme $S'_{I,2}$ prend en compte l'erreur engendrée par cette substitution et c'est ici que l'estimation (1.36) est utile. Estimons ces deux sommes avec nos définitions.

Pour estimer $S'_{I,1}(\vartheta')$, Mauduit et Rivat n'utilisent pas l'estimation (1.36), nous conservons donc leur majoration

$$S'_{I,1}(\vartheta') \ll \mu(\log q)^{3/2} q^{\frac{\rho_1}{2}-\gamma(\frac{\mu+\nu}{3})}. \tag{1.39}$$

En revanche, pour estimer $S'_{I,2}(\vartheta')$, les auteurs font appel à une famille de sommes dépendantes de $\widetilde{\mathcal{W}_\kappa}$. Ils obtiennent :

$$S'_{I,2}(\vartheta') \leq \sum_{1\leq d\leq M} \frac{S''_{I,2}(M,d)}{dq^{\mu+\nu}}, \tag{1.40}$$

et les $S''_{I,2}$ satisfont à :

$$\left|S''_{I,2}(M,d)\right|^2 \ll (\log q)\left(q^{\mu+\nu}+\frac{M^2}{d^2}\right)\sum_{\omega\in\mathcal{W}_{\kappa_d}} 2^2, \tag{1.41}$$

où κ_d est choisi de sorte que $q^{\kappa_d-1} \leq M^2/d^2 < q^{\kappa_d}$, $\mathcal{W}_\kappa$ est défini par $\mathcal{W}_\kappa := \{u+vq^\kappa, (u,v)\in\widetilde{\mathcal{W}_\kappa}\}$. L'équation (1.41) vient du fait que $S'_{I,2}$ est la contribution de l'erreur commise lorsqu'on remplace la fonction par la fonction tronquée, ainsi les termes n'existent que s'ils se trouvent dans $\mathcal{W}_{\kappa_d}$, et le cas échéant, le module au carré de ces termes est majoré par 4 : on regarde une différence de deux termes de modules 1.

Comme $M < q^\mu, d \geq 1$ et $\mu \leq \nu$, nous obtenons $\dfrac{M^2}{d^2} \ll q^{\mu+\nu}$, et donc par (1.37), nous avons :

$$S''_{I,2}(M,d) \ll (\log q)^{1/2} q^{\mu+\nu-\rho_1/2+(\log\rho_1)/2}, \tag{1.42}$$

ce qui nous permet de dire que

$$S'_{I,2}(\vartheta') \ll \mu(\log q)^{3/2} q^{-\rho_1/2+(\log\rho_1)/2}, \tag{1.43}$$

et finalement en combinant (1.38), (1.39) et (1.43) avec le choix $\rho_1 = \gamma((\mu+\nu)/3)$, nous obtenons :

$$S_I(\vartheta) \ll (\log q)^{5/2}(\mu+\nu)^2 q^{\mu+\nu-\frac{\gamma((\mu+\nu)/3)}{2}+\frac{\log(\gamma((\mu+\nu)/3))}{2}}. \tag{1.44}$$

Avant de passer à la somme de type II, remarquons que, eu égard à l'existence de la propriété $\gamma(\lambda) \leq \lambda/2$ [MR15, equation (25)], on peut réécrire (1.44) sous la forme

$$S_I(\vartheta) \ll (\log q)^{5/2}(\mu+\nu)^{2+\log q} q^{\mu+\nu-\frac{\gamma((\mu+\nu)/3))}{2}}.$$

Remarque 1.7.1. *Un choix plus fin de ρ_1 conduirait probablement à de meilleurs résultats, mais le terme principal restera donné par $S_{II}(\vartheta)$.*

1.7.2 Sommes de type II

Dans cette sous-partie, nous reprenons les notations introduites pour les sommes de type I. Nous faisons l'hypothèse supplémentaire que μ et ν sont liés par

$$\frac{1}{4}(\mu+\nu) \leq \mu \leq \nu \leq \frac{3}{4}(\mu+\nu).$$

Cette contrainte sur la taille des variables regardées découle de la définition des sommes de type II. Nous introduisons de plus $a_m \in \mathbb{C}$ et $b_n \in \mathbb{C}$ avec $|a_m|, |b_n| \leq 1$. Les sommes de type II sont définies par

$$S_{II}(\vartheta) := \sum_{M/q \leq m < M} \sum_{N/q \leq n < N} a_m b_n f(mn) e(\vartheta mn). \tag{1.45}$$

Pour $S_{II}(\vartheta)$, la notion de propagation n'intervient pas directement, mais par le biais de deux lemmes [MR15, Lemma 8-9], que nous remplaçons par les deux lemmes suivant :

Lemme 1.7.2. *Si $f : \mathbb{N} \to \mathbb{U}$ vérifie la Définition 1.2.4, alors pour $(\mu, \nu, \rho) \in \mathbb{N}^3$ avec $2\rho < \nu$, l'ensemble $\mathcal{E}$ des couples $(m, n) \in \{q^{\mu-1}, \dots, q^\mu - 1\} \times \{q^{\nu-1}, \dots, q^\nu - 1\}$ tels qu'il existe $k < q^{\mu+\rho}$ avec $f(mn+k)\overline{f(mn)} \neq f^{(\mu+2\rho)}(mn+k)\overline{f^{(\mu+2\rho)}(mn)}$ satisfait à*

$$card\,\mathcal{E} \ll (\log q) q^{\mu+\nu-\rho+\log\rho}. \tag{1.46}$$

Lemme 1.7.3. *Soient $f : \mathbb{N} \to \mathbb{U}$ une fonction qui vérifie la Définition 1.2.4 et $(\mu, \nu, \mu_0, \mu_1, \mu_2) \in \mathbb{N}^5$ avec $\mu_0 \leq \mu_1 \leq \mu \leq \mu_2$, $\mu \leq \nu$ et $2(\mu_2 - \mu_0) \leq \mu_0$. Pour $(a, b, c) \in \mathbb{N}^3$, l'ensemble $\mathcal{E}(a, b, c)$ des couples $(m, n) \in \{q^{\mu-1}, \dots, q^\mu - 1\}$ tels que*

$$\begin{aligned} &f^{(\mu_2)}(mn + am + bn + c)\overline{f^{(\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + am + bn + c))} \\ &\quad \neq f^{(\mu_1)}(mn + am + bn + c)\overline{f^{(\mu_1)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + am + bn + c))} \end{aligned}$$

satisfait à

$$card\,\mathcal{E}(a, b, c) \ll \max(\tau(q), \log q)\mu_2^{\omega(q)} q^{\mu+\nu+\mu_0-\mu_1+\log\mu_1}. \tag{1.47}$$

Les énoncés ne diffèrent de [MR15] que pour les estimations (1.46) et (1.47). En effet, dans [MR15] les termes d'erreurs sont respectivement

$$O((\log q)\, q^{\mu+\nu-\rho}) \text{ et } O(\max(\tau(q), \log q)\mu_2^{\omega(q)} q^{\mu+\nu+\mu_0-\mu_1}).$$

Ces modifications viennent de la perturbation de la propagation, et plus précisément de l'utilisation de la Définition 1.2.1 avec $\rho = \rho$ dans [MR15, Lemma 8] et avec $\rho = \mu_1 - \mu_0$ dans [MR15, Lemma 9]. Les [MR15, Lemma 8-9] n'interviennent dans [MR15] qu'une fois chacun dans l'estimation de $S_{II}(\vartheta)$, nous allons indiquer ici à quel endroit et en quoi les calculs sont modifiés.

Le [MR15, Lemma 8] apparaît au début de la démonstration, afin d'introduire une première troncation. Il permet de dire que le nombre de couples (m, n) pour lesquels $f(mn + mr)\overline{f(mn)} \neq f^{(\mu_2)}(mn + mr)\overline{f^{(\mu_2)}(mn)}$ est un $O(q^{\mu+\nu-\rho})$. Cette estimation conduit aux estimations (52) puis (55) de [MR15], que l'on peut réunir sous la forme

$$|S_{II}(\vartheta)|^4 \ll q^{4(\mu+\nu)-2\rho} + q^{3(\mu+\nu-\rho)} \sum_{1 \leq r < q^\rho} \sum_{1 \leq s < q^{2\rho}} |S_2'(r, s)|,$$

où ρ est un paramètre vérifiant $7\rho \leq \mu$ et qui sera choisi à la fin des estimations, et $S_2'(r, s)$ est une somme qui sera évaluée tout au long de la preuve.

Avec notre Lemme 1.7.2, nous sommes amené à avoir, en gardant les mêmes notations, l'équation

$$|S_{II}(\vartheta)|^4 \ll q^{4(\mu+\nu)-2\rho+2\log\rho} + q^{3(\mu+\nu-\rho)} \sum_{1\leq r<q^\rho} \sum_{1\leq s<q^{2\rho}} |S_2'(r,s)|. \tag{1.48}$$

Regardons maintenant à quel endroit dans [MR15] le [MR15, Lemma 9] apparaît. Soit $r_{\mu_0,\mu_2}(n)$ défini par (1.34). Afin d'estimer $S_2'(r,s)$, Mauduit et Rivat introduisent la fonction doublement tronquée

$$f^{(\mu_1,\mu_2)}(n) := f^{(\mu_2)}(n)\overline{f^{(\mu_1)}(n)}$$

et la quantité

$$f^{(\mu_1,\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(n)).$$

Ceci les amènent à estimer le cardinal de $\mathcal{E}_{\mu_0,\mu_1,\mu_2}(r,s)$, l'ensemble des couples (m,n), avec $M/q < m \leq M$ et $N/q < n \leq N$ (avec $T_q(M) = \mu - 1$ et $T_q(N) = \nu - 1$) pour lesquels

$$f^{(\mu_1,\mu_2)}(mn + q^{\mu_1}sn + q^{\mu_1}sr) \neq f^{(\mu_1,\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1}sn + q^{\mu_1}sr)),$$

c'est à dire

$$\begin{aligned} &f^{(\mu_2)}(mn + q^{\mu_1}sn + q^{\mu_1}sr)\overline{f^{(\mu_1)}(mn + q^{\mu_1}sn + q^{\mu_1}sr)} \\ &\quad \neq f^{(\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1}sn + q^{\mu_1}sr))\overline{f^{(\mu_1)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1}sn + q^{\mu_1}sr))}, \end{aligned}$$

ou encore

$$\begin{aligned} &f^{(\mu_2)}(mn + q^{\mu_1}sn + q^{\mu_1}sr)\overline{f^{(\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1}sn + q^{\mu_1}sr))} \\ &\quad \neq f^{(\mu_1)}(mn + q^{\mu_1}sn + q^{\mu_1}sr)\overline{f^{(\mu_1)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1}sn + q^{\mu_1}sr))}. \end{aligned}$$

Mauduit et Rivat utilisent alors [MR15, Lemma 9] avec $\mu_2 = \mu + 2\rho$, $\mu_1 = \mu - 2\rho$, et pour $0 \leq \rho' \leq \rho$, $\mu_0 = \mu_1 - 2\rho'$ pour contrôler le cardinal de $\mathcal{E}_{\mu_0,\mu_1,\mu_2}(r,s)$. Nous, nous utilisons les mêmes valeurs (et nous les utiliserons tout le long de la preuve) mais avec le Lemme 1.7.3 et du fait que $7\rho \leq \mu \leq \nu$, ceci nous conduit à l'estimation :

$$\operatorname{card} \mathcal{E}_{\mu_0,\mu_1,\mu_2}(r,s) \ll \max(\tau(q), \log q)(\mu+\nu)^{\omega(q)} q^{\mu+\nu-2\rho'+\log\mu_1}. \tag{1.49}$$

Mauduit et Rivat estiment alors $S_2'(r,s)$ en substituant $f^{(\mu_1,\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1}sn + q^{\mu_1}sr))$ à $f^{(\mu_1,\mu_2)}(mn + q^{\mu_1}sn + q^{\mu_1}sr)$ et en introduisant le terme correctif résultant, ce qui induit

$$S_2'(r,s) = S_3(r,s) + O(\operatorname{card} \mathcal{E}_{\mu_0,\mu_1,\mu_2}(r,s)). \tag{1.50}$$

En réunissant (1.48), (1.49) et (1.50), nous obtenons finalement :

$$\begin{aligned} |S_{II}(\vartheta)|^4 \ll\ & q^{4(\mu+\nu)-2\rho+2\log\rho} + \max(\tau(q), \log q)(\mu+\nu)^{\omega(q)} q^{4(\mu+\nu)-2\rho'+\log\mu_1} \\ &+ q^{3(\mu+\nu-\rho)} \sum_{1\leq r<q^\rho} \sum_{1\leq s<q^{2\rho}} |S_3(r,s)|. \end{aligned} \tag{1.51}$$

Mauduit et Rivat majorent $|S_3(r,s)|$ sans utiliser [MR15, Lemma 8-9], mais en utilisant directement la Définition 1.2.1. Plus précisément elle apparaît dans [MR15, Lemma 10]. Nous allons d'abord expliquer comment ils procèdent pour arriver à ce dernier, puis modifier l'énoncé du lemme pour qu'il corresponde à notre cas, puis nous conclurons.

La quantité $S_3(r,s)$ est une somme qui dépend des chiffres du milieu de mn et de $m(n+r)$. De manière à introduire des transformées de Fourier de $f^{(\mu_1,\mu_2)}$, Mauduit et Rivat identifient la décomposition en base q avec un sous-ensemble de l'intervalle $[0,1)$ translaté sur l'ensemble des entiers : c'est la formule

$$r_{\mu_0,\mu_2}(n) = u \Leftrightarrow \frac{n}{q^{\mu_2}} \in \left[\frac{u}{q^{\mu_2-\mu_0}}, \frac{u+1}{q^{\mu_2-\mu_0}}\right) + \mathbb{Z}.$$

Ils introduisent alors des fonctions indicatrices d'intervalles qu'ils contrôlent à l'aide des polynômes de Vaaler (voir Partie A.3). Ceci est repris dans notre thèse sous la forme du Lemme A.3.2, lemme que l'on peut retrouver dans [MR15, Lemma 1]. Mauduit et Rivat trouvent une nouvelle décomposition de $S_3(r,s)$, qu'ils nomment $S_4(r,s)$, constituée du terme principal des polynômes de Vaaler. Les termes d'erreurs du Lemme A.3.2 sont contrôlés par les méthodes usuelles et ne sont pas affectés par notre modification. Le calcul explicite est fait dans notre thèse dans le Lemme A.3.4. Mauduit et Rivat peuvent alors conclure que

$$S_3(r,s) = S_4(r,s) + O(\max(\log q^{\mu_0}, \tau(q^{\mu_0}))q^{\mu+\nu-2\rho}). \tag{1.52}$$

Le fait d'avoir introduit les polynômes de Vaaler permet de travailler sur les transformées de Fourier de $g(n) := f^{(\mu_1,\mu_2)}(q^{\mu_0}n)$, si bien que $S_4(r,s)$ s'écrit :

$$\begin{aligned} S_4(r,s) = q^{2(\mu_2-\mu_0)} \sum_{|h_0|,|h_1|\leq H} a_{h_0}(q^{\mu_0-\mu_2},H)a_{h_1}(q^{\mu_0-\mu_2},H) \sum_{0\leq h_2,h_3<q^{\mu_2-\mu_0}} e\left(\frac{h_3sr}{q^{\mu_2-\mu_1}}\right) \\ \hat{g}(h_0-h_2)\overline{\hat{g}(h_3-h_1)\hat{g}(-h_2)}\hat{g}(h_3) \\ \sum_{m,n} e\left(\frac{(h_0+h_1)mn + h_1mr + (h_2+h_3)q^{\mu_1}sn}{q^{\mu_2}}\right), \end{aligned}$$

où

$$a_0(\alpha,H) = \alpha, \quad |a_h(\alpha,H)| \leq \min\left(\alpha, \frac{1}{\pi|h|}\right),$$

selon le Lemme A.3.2. Ce lemme induit le choix $H = q^{\mu_2-\mu_0+2\rho}$, mais pour des raisons de simplifications d'écritures, nous conserverons la notation H tant que le choix de celui-ci n'est pas déterminant.

Il convient d'isoler les termes diagonaux, satisfaisant à $h_0+h_1=0$, des autres termes. Nous noterons la contribution des termes diagonaux par $S_4'(r,s)$, l'autre terme sera noté $S_4''(r,s)$. La plus grande contribution proviendra des termes diagonaux.

Dans l'estimation de $S_4''(r,s)$, le [MR15, Lemma 10] n'intervient pas, et nous avons donc, comme Mauduit et Rivat :

$$|S_4''(r,s)| \ll (\log q)^3(\mu+\nu)^3 q^{\mu+\nu+3(\mu_2-\mu_0)+2\rho}(q^{-\mu_2}+q^{-\nu}). \tag{1.53}$$

Pour $S_4'(r,s)$, en faisant la moyenne sur les s, en utilisant certaines observations sur les objets et l'inégalité de Cauchy-Schwarz, Mauduit et Rivat se ramènent à étudier

$$S_8(r) = q^{2(\mu_2-\mu_0)} \sum_{|h_1|\leq H} |a_{h_1}(q^{\mu_0-\mu_2}, H)|^2 \min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right) S_7(h_1), \tag{1.54}$$

avec

$$S_7(h_1) = \sum_{0\leq h'<q^{\mu_2-\mu_0}} |\hat{g}(h'-h_1)\hat{g}(h')|^2. \tag{1.55}$$

La somme $S_8(r)$ est liée aux quantités précédentes par

$$\frac{1}{S}\sum_{1\leq s<S} |S_4'(r,s)| \ll q^{\nu+\mu_1-\mu_0}(\tau(q^{\mu_2-\mu_1}) + q^{\mu_2-\mu_1}\log q^{\mu_2-\mu_1})S_8(r). \tag{1.56}$$

Par la suite Mauduit et Rivat découpent $S_8(r)$ en $S_8'(r)$, qui correspond au cas où $|h_1| \leq q^{2\rho}$, en $S_8''(r)$ pour $q^{2\rho} < |h_1| \leq q^{\mu_2-\mu_0}$ et en $S_8'''(r)$ pour $q^{\mu_2-\mu_0} < |h_1| \leq H$. La variable H sera choisie avec un ordre de $q^{\mu_2-\mu_0+2\rho}$.

Pour $S_8''(r)$, en utilisant $|a_h(\alpha, H)| \leq \min(\alpha, 1/|H|)$ et le fait que

$$\sum_{0\leq h<q^{\mu_2-\mu_0}} |\hat{g}(h)|^2 = 1, \tag{1.57}$$

nous avons, parce que h_1 va jusqu'à $q^{\mu_2-\mu_0}$, $S_8''(r) \leq q^{\mu_2-2\rho}/r$. Le même procédé fonctionne pour $S_8'''(r)$. En revanche, si h_1 est petit il faut faire appel au [MR15, Lemma 10], qui est une estimation plus fine de (1.55) que peut donner (1.57), et qui se déduit du [MR15, Lemma 11]. Pour nous, le [MR15, Lemma 11] aura la forme suivante :

Lemme 1.7.4. *On définit*

$$G_{\mu_0,\lambda}(t) = \frac{1}{q^{\lambda}} \sum_{0\leq u<q^{\lambda}} f^{(\mu_1,\mu_2)}(uq^{\mu_0}) e\left(-\frac{ut}{q^{\lambda}}\right).$$

Soient μ et ρ des entiers tels que $\mu \leq (2+4c/3)\rho$, où c est la constante introduite dans la Définition 1.2.2. Alors, uniformément pour λ entier compris entre $(\mu_2-\mu_0)/3$ et $4(\mu_2-\mu_0)/5$ et t réel, on a

$$\sum_{0\leq k<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0}(k+t)|^2 \ll (\gamma(\lambda)-\mu_1+\mu_0)\, q^{(\mu_1-\mu_0-\gamma(\lambda))/2}(\log q^{\mu_2-\mu_1})^2.$$

Indiquons comment ce lemme est utilisé. On remarque que

$$G_{\mu_0,\lambda}(t) = \frac{1}{q^{\lambda}} \sum_{0\leq u<q^{\lambda}} g(u) e\left(-\frac{ut}{q^{\lambda}}\right)$$

est la transformée de Fourier de g. Puisque le contrôle est uniforme en t nous utilisons le lemme avec $\lambda = \mu_2-\mu_0-2\rho$, et par (1.57) :

$$\sum_{0\leq h<q^{\mu_2-\mu_0}} \sum_{0\leq k<q^{2\rho}} |\hat{g}(h+k)\hat{g}(h)|^2$$
$$\ll (\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)\, q^{-\frac{\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0}{2}}(\log q^{\mu_2-\mu_1})^2.$$

Mais ceci permet de dire, par la définition de S_7 faite en (1.55) que

$$\sum_{|h_1|\leq q^{2\rho}} S_7(h_1) \ll (\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)\, q^{-\frac{\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0}{2}}$$

ou encore par (1.54) et la définition sous-jacente de S_8' :

$$S_8'(r) \ll (\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)\, q^{\mu-\frac{\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0}{2}} \tag{1.58}$$

ce qui finalement, en écrivant $S_8(r) = S_8'(r) + S_8''(r) + S_8'''(r)$, nous permet de dire

$$\frac{1}{q^\rho}\sum_{1\leq r<q^\rho} S_8(r) \ll (\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)\, q^{\mu-\frac{\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0}{2}} + q^{\mu-\rho}\log q^\rho,$$

et donc, par (1.56) :

$$\begin{aligned}&\frac{1}{q^{3\rho}}\sum_{1\leq r<q^\rho}\sum_{1\leq s<q^{2\rho}} |S_4'(r,s)| \\ &\quad\ll q^{\mu+\nu+\mu_1-\mu_0}\Big(\big(\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0\big)\, q^{-\frac{\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0}{2}} + q^{-\rho}\log q^\rho\Big) \\ &\qquad(\tau(q^{\mu_2-\mu_1}) + q^{\mu_2-\mu_1-\nu}\log q^{\mu_2-\mu_1}).\end{aligned} \tag{1.59}$$

Nous allons maintenant démontrer le Lemme 1.7.4.

Preuve du Lemme 1.7.4. Soit $0\leq\lambda\leq\mu_2-\mu_0$. Nous séparons la somme définissant $G_{\mu_0,\mu_2-\mu_0}(t)$ selon les restes de la division euclidienne de u par q^λ. Si on suppose $\mu_1-\mu_0\leq\lambda\leq\mu_2-\mu_0$, comme $(u+vq^\lambda)q^{\mu_0}\equiv uq^{\mu_0} \bmod q^{\mu_1}$, nous pouvons écrire en remplaçant dans cette somme uq^{μ_0} par $vq^{\mu_0+\lambda}+uq^{\mu_0}$, avec $0\leq u<q^\lambda$, de sorte à séparer les variables modulo q^{μ_1} :

$$\begin{aligned}&G_{\mu_0,\mu_2-\mu_0}(t) \\ &= \frac{1}{q^{\mu_2-\mu_0-\lambda}}\sum_{0\leq v<q^{\mu_2-\mu_0-\lambda}} f(vq^{\mu_0+\lambda})e\left(-\frac{vt}{q^{\mu_2-\mu_0-\lambda}}\right) \\ &\qquad\frac{1}{q^\lambda}\sum_{0\leq u<q^\lambda} f(uq^{\mu_0}+vq^{\mu_0+\lambda})\overline{f(vq^{\mu_0+\lambda})f^{(\mu_1)}(uq^{\mu_0})}e\left(-\frac{ut}{q^{\mu_2-\mu_0}}\right).\end{aligned}$$

Dans la ligne du bas, Mauduit et Rivat remplacent f par la fonction tronquée $f^{(\mu_0+\lambda+\rho_3)}$ associée, où ρ_3 est un paramètre qui sera optimisé. Ils décomposent donc $G_{\mu_0,\mu_2-\mu_0}(t) = G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t) + G_{\mu_0,\mu_2-\mu_0,\lambda,2}(t)$, où $G_{\mu_0,\mu_2-\mu_0,\lambda,2}(t)$ est le terme d'erreur correspondant au changement de fonctions. L'estimation du cas $G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t)$ se traite dans notre cas exactement comme dans le leur et on a l'estimation, uniforme en t :

$$\sum_{0\leq k<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0,\lambda,1}(k+t)|^2 \ll q^{3\rho_3+2(\mu_1-\mu_0)-2\gamma(\lambda)}(\log q^{\mu_2-\mu_1})^2. \tag{1.60}$$

Si à présent, on note $\mathcal{W}_\lambda$ l'ensemble des entiers $w = u + vq^\lambda$ tels que

$$f(uq^{\mu_0} + vq^{\mu_0+\lambda})\overline{f(vq^{\mu_0+\lambda})} \neq f^{(\mu_0+\lambda+\rho_3)}(uq^{\mu_0} + vq^{\mu_0+\lambda})\overline{f^{(\mu_0+\lambda+\rho_3)}(vq^{\mu_0+\lambda})},$$

alors nous avons par la faible propriété de propagation, l'estimation

$$|\mathcal{W}_\lambda| \ll q^{\mu_2-\mu_0-\rho_3+\log\rho_3}.$$

De plus,

$$G_{\mu_0,\mu_2-\mu_0,\lambda,2}(t) = \frac{1}{q^{\mu_2-\mu_0}} \sum_{w<q^{\mu_2-\mu_0}} c'_\lambda(w) e\left(-\frac{wt}{q^{\mu_2-\mu_0}}\right),$$

où $c'_\lambda(w)$ désigne la différence entre la fonction et la fonction tronquée. Ainsi $|c'_\lambda(w)| \leq 2$ pour tout w et $c'_\lambda(w) = 0$ si $w \notin \mathcal{W}_\lambda$: en effet, les fonctions étant de module 1, le module de la différence est majoré par 2 si la différence se fait, c'est-à-dire si $w \in \mathcal{W}_\lambda$. Mais alors on peut écrire en complétant la somme :

$$\begin{aligned}
&\sum_{0\leq k<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0,\lambda,2}(k+t)|^2 \\
&\qquad \leq \frac{1}{q^{2(\mu_2-\mu_0)}} \sum_{w<q^{\mu_2-\mu_0}} \sum_{w'<q^{\mu_2-\mu_0}} c'_\lambda(w)\overline{c'_\lambda(w')} e\left(-\frac{(w-w')t}{q^{\mu_2-\mu_0}}\right) \\
&\qquad\qquad \sum_{k<q^{\mu_2-\mu_0}} e\left(-\frac{(w-w')k}{q^{\mu_2-\mu_0}}\right) \\
&\qquad = \frac{1}{q^{\mu_2-\mu_0}} \sum_{w<q^{\mu_2-\mu_0}} |c'_\lambda(w)|^2 \ll \frac{|\mathcal{W}_\lambda|}{q^{\mu_2-\mu_0}} \\
&\qquad \ll q^{-\rho_3+\log\rho_3}.
\end{aligned}$$

De ceci combiné avec (1.60), nous obtenons

$$\sum_{k<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0}(k+t)|^2 \ll q^{3\rho_3+2(\mu_1-\mu_0)-2\gamma(\lambda)}(\log q^{\mu_2-\mu_1})^2 + q^{-\rho_3+\log\rho_3},$$

nous concluons en choisissant, comme Mauduit et Rivat, $\rho_3 = \max(1, \lfloor \frac{1}{2}(\gamma(\lambda) - \mu_1 + \mu_0)\rfloor)$.

□

Nous n'avons plus qu'à réunir les équations (1.51), (1.52), (1.53) et (1.59) pour

obtenir :

$$
\begin{aligned}
&|S_{II}(\vartheta)|^4 \\
&\ll q^{4(\mu+\nu)-2\rho+2\log\rho} + \max(\tau(q),\log q)(\mu+\nu)^{\omega(q)} q^{4(\mu+\nu)-2\rho'+\log\mu_1} \\
&\quad + q^{3(\mu+\nu-\rho)} \sum_{r<q^\rho} \sum_{s<q^{2\rho}} \Big(|S_4(r,s)| + \max(\log q^{\mu_0}, \tau(q^{\mu_0})) q^{\mu+\nu-2\rho} \Big) \\
&\ll \max(\log(q^{\mu_0}), \tau(q^{\mu_0})) q^{4(\mu+\nu)-2\rho+2\log\rho} && (1.61) \\
&\quad + \max(\tau(q),\log q)(\mu+\nu)^{\omega(q)} q^{4(\mu+\nu)-2\rho'+\log\mu_1} && (1.62) \\
&\quad + q^{3(\mu+\nu)} (\log q)^3 (\mu+\nu)^3 q^{\mu+\nu+3(\mu_2-\mu_0)+2\rho} (q^{-\nu} + q^{-\mu_2}) && (1.63) \\
&\quad + q^{3\mu+3\nu} \Big[q^{\mu+\nu+\mu_1-\mu_0} (\gamma(\mu_2-\mu_0-2\rho) - \mu_1 + \mu_0)\, q^{-\frac{\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0}{2}} + q^{-\rho}\log q^\rho) && (1.64) \\
&\qquad (\tau(q^{\mu_2-\mu_1}) + q^{\mu_2-\mu_1-\nu} \log q^{\mu_2-\mu_1}) \Big].
\end{aligned}
$$

Nous rappelons, pour faire notre choix de ρ, que $\mu_2 = \mu + 2\rho$, $\mu_1 = \mu - 2\rho$ et $\mu_0 = \mu_1 - 2\rho'$ et que $7\rho \le \mu$ et $\rho' \le \rho$.

Puisque la fonction γ est croissante, nous avons $\gamma(\mu_2-\mu_0-2\rho) \ge \gamma(\mu_2-\mu_1-2\rho) = \gamma(2\rho)$. De plus, comme $\gamma(x) \le x/2$ (remarque (26) de [MR15]), on a

$$\gamma(\mu_2-\mu_0-2\rho) - \mu_1 + \mu_0 \le \gamma(4\rho) \le 2\rho \ll \rho \ll \log(q^\rho).$$

Nous constatons également que $\tau(q^{\mu_2-\mu_1}) \le (\mu_2-\mu_1)^{\omega(q)}\tau(q)$ et $\mu_2-\mu_1 \le \mu-2\rho \le \nu-2\rho$ de sorte que $q^{\mu_2-\mu_1-\nu}\log q^{\mu_2-\mu_1}$ est borné et donc le terme (1.64) est

$$O(q^{4(\mu+\nu)+3/2(\mu_1-\mu_0)-\gamma(2\rho)} \log(q^\rho)\tau(q)(\mu_2-\mu_1)^{\omega(q)}). \tag{1.65}$$

Puis, du fait de la forme de μ_1, le terme (1.62) est

$$O(\max(\tau(q),\log q)(\mu+\nu)^{\omega(q)+1} q^{4(\mu+\nu)-2\rho'}) \tag{1.66}$$

Notre estimation de $|S_{II}|^4$ devient de la même forme que celle trouvée dans [MR15], on peut alors déduire, en faisant les mêmes choix que les auteurs :

$$|S_{II}(\vartheta)|^4 \ll \max(\tau(q)\log q, (\log q)^3)(\mu+\nu)^{2+\log q+\max(\omega(q),2)} q^{4\mu+4\nu-\gamma(2\lfloor\mu/15\rfloor)/5}. \tag{1.67}$$

En rappelant $q^{\mu+\nu-4} \le x < q^{\mu+\nu}$, en utilisant les Lemmes A.1.2 et A.1.3 avec les estimations (1.44) et (1.67), nous obtenons :

$$\left| \sum_{x/q<n\le x} \Lambda(n) f(n) e(\vartheta n) \right| \ll (\log x)^2 \left(|S_I(\vartheta)| + |S_{II}(\vartheta)| \right),$$

et

$$\left| \sum_{x/q<n\le x} \mu(n) f(n) e(\vartheta n) \right| \ll (\log x)^2 \left(|S_I(\vartheta)| + |S_{II}(\vartheta)| \right).$$

Comme les estimations (1.44) et (1.67) fournissent

$$|S_I(\vartheta)| \ll (\log q)^{5/2}(\mu+\nu)^{2+\log q} q^{\mu+\nu-\frac{\gamma((\mu+\nu)/3))}{2}}$$

ainsi que

$$|S_{II}(\vartheta)| \ll \max(\tau(q)\log q, (\log q)^3)^{1/4}(\mu+\nu)^{1/2+\log q/4+\max(\omega(q),2)/4} q^{\mu+\nu-\gamma(2\lfloor \mu/15\rfloor)/20},$$

nous pouvons conclure la preuve de ce théorème comme le font Mauduit et Rivat.

1.8 Applications

Dans cette partie nous appliquons les résultats des Parties 1.5 et 1.6 pour obtenir une large classe de fonctions qui vérifient un théorème des nombres premiers.

Nous avons vu que si une fonction vérifiait la faible propriété de propagation et la propriété de Fourier, alors elle vérifiait la majoration (3.2). De plus, nous avons vu dans la Partie 1.5 que les fonctions associées aux suites β-récursives vérifiaient la faible propriété de propagation (Proposition 1.5.1). Enfin, nous avons vu dans la Partie 1.6, que, pour une fonction associée à une suite β-récursive, pour vérifier la propriété de Fourier (1.17), il suffisait de trouver α réel et ω_1, ω_2 de taille $\beta-1$ de même suffixe, et k_1 et k_2 de sorte que

$$\alpha\left(g(\omega_1\cdot k_1) - g(\omega_1\cdot k_2) - g(\omega_2\cdot k_1) + g(\omega_2\cdot k_2)\right) \notin \mathbb{Z}. \tag{1.68}$$

Nous notons

$$K = K(g,\omega_1,\omega_2,k_1,k_2) = g(\omega_1\cdot k_1) - g(\omega_1\cdot k_2) - g(\omega_2\cdot k_1) + g(\omega_2\cdot k_2). \tag{1.69}$$

Nous allons ici donner des exemples de suites β-récursives, et montrer que pour certains $k_1,k_2,\omega_1,\omega_2$ leurs fonctions de propagations vérifient (1.68) si et seulement si α n'est pas un entier. Il y a deux grandes classes de fonctions, que nous traitons séparément :

1.8.1 Nombre d'occurences

Proposition 1.8.1. *Soit β un entier supérieur ou égal à 2, et soit B un sous-ensemble de Σ_β tel qu'il existe un mot ω dans B de sorte que pour chaque extrémité de ω, il existe une lettre telle qu'en remplaçant l'extrémité par cette lettre, le nouveau mot obtenu ne soit pas dans B. Il est donc demandé qu'il existe $l_1 \neq \epsilon_{|\omega|-1}(\omega)$ et $l_2 \neq \epsilon_0(\omega)$ des lettres telles que*

$$l_1\cdot \underline{\omega}_{(\beta-1)} \notin B, \tag{1.70}$$

$$\overline{\omega}^{(\beta-1)}\cdot l_2 \notin B, \tag{1.71}$$

et

$$l_1\cdot\epsilon_{\beta-2}(\omega)\ldots\cdot\epsilon_1(\omega)\cdot l_2 \notin B. \tag{1.72}$$

Soit à présent $(a(n))_{n\geq 0}$ une suite β-récursive de fonction de propagation $g = \sum_{\chi\in B}\mathbb{1}_\chi$. Alors $K=1$ et $(e(\alpha a(n)))_{n\geq 0}$ vérifie un théorème des nombres premiers et un principe d'aléa de Möbius si et seulement si $\alpha\in\mathbb{R}\backslash\mathbb{Z}$.

Démonstration. En choisissant dans (1.69), $\omega_1 = \overline{\omega}^{(\beta-1)}$, $\omega_2 = l_1 \cdot \epsilon_{\beta-2}(\omega) \dots \cdot \epsilon_1(\omega)$, $k_1 = \epsilon_0(\omega)$ et $k_2 = l_2$, on a $\omega_1 \cdot k_1 = \omega$ et donc :

$$K = g(\omega) - g(\overline{\omega}^{(\beta-1)} \cdot l_2) - g(l_1 \cdot \underline{\omega}_{(\beta-1)}) + g(l_1 \cdot \epsilon_{\beta-2}(\omega) \dots \cdot \epsilon_1(\omega) \cdot l_2) = 1.$$

□

De ce résultat à première vue tautologique, on tire de nombreuses conséquences. Le fait que K soit égal à 1 implique que (1.68) est équivalente à α non entier, ou encore que les suites β-récursives ayant une fonction de propagation correspondant aux conditions de la Proposition 1.8.1 vérifient la propriété de Fourier (1.17) si et seulement si α n'est pas un entier.

Or ce type de fonction recouvre de nombreux cas classiques. Par exemple :

(I) Si on prend $B = \{\omega\}$, alors il existe $\omega \in B$ vérifiant (1.70), (1.71) et (1.72) (n'importe quelle lettre convient), et si on pose $a(k) = 0$ pour tout $k < q^{|\omega|-1}$, on trouve les suites qui comptent le nombre d'occurrences d'un mot quelconque de taille supérieure ou égale à 2.

(II) Soit $k \geq 1$. Si on prend $B = \{a \cdot \gamma \cdot b, \gamma \in \Sigma_k\}$, on trouve alors que $g = \mathbb{1}_{a \cdot Z \cdot b}$, et donc le nombre d'occurrences des mots de la forme aZb où Z est un mot arbitraire. En particulier $q = 2, a = 1, b = 1$ donne la suite introduite par Allouche et Liardet dans [AL91]. On peut l'améliorer de sorte à assigner des lettres fixes entre les deux extremités en posant $B = \{a_0 \cdot \gamma_0 \cdot a_1 \cdots \gamma_k \cdot a_{k+1},\ \gamma_i \in \Sigma_{\varsigma(i)}\ \forall 0 \leq i \leq k\}$, où ς est une fonction de $\mathbb{N}$ dans $\mathbb{N}$ arbitraire.

(III) Si on suppose qu'on n'est pas dans le cas $q = \beta = 2$, on peut prendre $B = \bigcup_{a \in \Sigma_1} \{a \cdots a\}$ pour compter le nombre d'occurrences des mots de même taille et ayant une seule lettre, comme 000, 111 et 222 pour $q = 3$ et $k = 3$.

Notre condition (1.68) permet de traiter de nombreux cas classiques. En revanche la suite $(a(n))_{n \geq 0}$ qui compte le nombre de mots 00 et 11 dans l'écriture de n en base 2 n'entre pas dans ce cadre. En effet, sous ces conditions, la fonction de propagation $g(a \cdot b)$ vaut 1 si et seulement si $a = b = 0$ ou $a = b = 1$ et alors quels que soient ω_1, ω_2 de taille 1 et k_1, k_2 de taille 1, on a

$$\begin{aligned} |K| &= |g(\omega_1 \cdot k_1) - g(\omega_2 \cdot k_1) - g(\omega_1 \cdot k_2) + g(\omega_2 \cdot k_2)| \\ &= |g(00) - g(01) - g(10) + g(11)| \\ &= 2 \equiv 0 \bmod 2, \end{aligned}$$

et $\alpha = 1/2$ implique forcément que pour tout $\omega_1, \omega_2, k_1, k_2$

$$\alpha K(g, \omega_1, \omega_2, k_1, k_2) \in \mathbb{Z},$$

ce qui est censé être proscrit.

1.8.2 Polynômes sur les chiffres

Dans cette sous-partie, nous résolvons partiellement la question posée par Kalai [Kal12] à travers la démonstration du Théorème 0.4.1 et du Théorème 0.4.2.

Soit r un entier supérieur ou égal à 1. Nous associons à tout polynôme R de $\mathbb{Z}[X_1, \ldots, X_r]$ une fonction $\dot{R} : \mathcal{A}^r \to \mathbb{Z}$ par $\dot{R}(\gamma) := R(\epsilon_0(\gamma), \ldots, \epsilon_{r-1}(\gamma))$.

Nous rappelons le Théorème 0.4.1.

Théorème 1.8.2. *Soient N un entier supérieur ou égal à 3, β un entier compris entre 2 et $N-1$. Soient $i_1, \ldots, i_d$ tels que $1 = i_1 < i_2 < \ldots < i_d = \beta$. Nous définissons alors un polynôme $\tilde{P}_1$ de $\mathbb{Z}[Y_1, \ldots, Y_\beta]$ par*

$$\tilde{P}_1(Y_1, \ldots, Y_\beta) = Z_{i_1} \ldots Z_{i_{d-1}} Y_{i_d},$$

où la variable Z_i signifie Y_i ou $1 - Y_i$. Soit le polynôme à N variables

$$P_N(X_1, \ldots, X_N) := \sum_{i=1}^{N-\beta+1} \tilde{P}_1(X_i, \ldots, X_{i+\beta-1}),$$

alors il existe des constantes absolues strictement positives C_1 et C_2 telles que

$$\sum_{n<2^N} \mu(n)(-1)^{P_N(n)} \ll N^{C_1} 2^{N - C_2 N \frac{1}{\beta 2^\beta} + o\left(\frac{N}{\beta 2^\beta}\right)} \qquad (N \to \infty), \tag{1.73}$$

où $P_N(n) = P_N(\epsilon_0(n), \ldots, \epsilon_{N-1}(n))$.

Démonstration. La suite β-récursive $(a(n))_{n\geq 0}$ de fonction de propagation $g : \Sigma_\beta \to \mathbb{N}$ qui a comme valeurs

$$g(\omega) = \dot{P}_1(\omega),$$

et elle vérifie pour tout n inférieur à 2^N, du fait que $\tilde{P}_1(x_1, \ldots, x_{\beta-1}, 0) = 0$ pour tout $(x_1, \ldots, x_{\beta-1})$, :

$$\begin{aligned} a(n) &= \sum_{i=0}^{T_2(n)-\beta} g(\epsilon_{i+\beta-1}(n) \cdots \epsilon_i(n)) \\ &= \sum_{i=0}^{N-\beta} g(\epsilon_{i+\beta-1}(n) \cdots \epsilon_i(n)). \end{aligned}$$

Soient $(x_{i_2}, \ldots, x_{i_{d-1}}) \in \{0,1\}^{d-2}$ de sorte que $Z_{i_k}(x_{i_k}) = 1$ pour tout k. Si ω est un mot de taille $\beta - 2$ tel que $\epsilon_{i_k-1}(\omega) = x_{i_k}$ pour tout $2 \leq k \leq d-2$, en se rappelant que $i_1 = 1$ et $i_d = \beta$, il vient que

$$\begin{aligned} &g(1\cdot\omega\cdot 1) - g(0\cdot\omega\cdot 1) - g(1\cdot\omega\cdot 0) + g(0\cdot\omega\cdot 0) \\ &= Z_{i_1}(\epsilon_{i_1-1}(\omega)) \cdots Z_{i_{d-1}} \\ &\quad \cdot (\epsilon_{i_{d-1}-1}(\omega)) \left(Z_{i_1}(1)Y_{i_d}(1) - Z_{i_1}(1)Y_{i_d}(0) - Z_{i_1}(0)Y_{i_d}(1) + Z_{i_1}(0)Y_{i_d}(0)\right) \\ &= Z_1(1)Y_\beta(1) - Z_1(1)Y_\beta(0) - Z_1(0)Y_\beta(1) + Z_1(0)Y_\beta(0) \\ &= Z_1(1) - Z_1(0), \end{aligned}$$

et comme $Z_i = Y_i$ ou $(1 - Y_i)$, on conclut que

$$|g(1\cdot\omega\cdot 1) - g(0\cdot\omega\cdot 1) - g(1\cdot\omega\cdot 0) + g(0\cdot\omega\cdot 0)| = 1.$$

Donc par le Corollaire 1.6.7, qui relie la propriété de Fourier à la norme infinie de la matrice généalogique, la Proposition 1.6.8 et le Corollaire 1.6.10, qui, mis ensemble, fournissent une majoration de cette norme en fonction de K, la fonction $f(n) = e\left(\frac{1}{2}P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))\right)$ associée au polynôme P_N vérifie

$$\frac{1}{2^N}\left|\sum_{n<2^N} f(nq^\kappa)e(nt)\right| \leq \frac{1}{2^{\beta\lfloor N/\beta\rfloor}}\left(2^\beta - 8(\sin\pi/8)^2\right)^{\lfloor N/\beta\rfloor}$$

ceci a pour conséquence qu'elle vérifie la propriété de Fourier avec

$$\begin{aligned}-\gamma(\lambda) &= \lfloor N/\beta\rfloor\left(\frac{\log(2^\beta - 8(\sin\pi/8)^2)}{\log 2} - \beta\right)\\ &= \lfloor N/\beta\rfloor\frac{\log(1-2^{3-\beta}(\sin\pi/8)^2)}{\log 2}.\end{aligned}$$

Nous avons alors, par le Théorème 1.2.5, qu'il existe une constante $c > 0$ telle que

$$\begin{aligned}&\sum_{n<2^N}\mu(n)f(n)\\ &\quad\ll N^c 2^{N+\lfloor\lfloor N/80\rfloor/\beta\rfloor\log(1-2^{3-\beta}(\sin\pi/8))^2)/20\log 2+o(\lfloor\lfloor N/80\rfloor/\beta\rfloor\log(1-2^{3-\beta}(\sin\pi/8))^2)/20\log 2)}\\ &\quad\ll N^c 2^{N-N\frac{(\sin\pi/8)^2}{200\beta 2^\beta\log 2}+o(N/\beta 2^\beta)},\end{aligned}$$

où la dernière ligne a été obtenue en utilisant le fait que $\log(1-x) \leq -x$ pour $x \in [0,1)$. Notre théorème est ainsi démontré.

□

Nous allons à présent démontrer le Théorème 0.4.2, que nous rappelons

Théorème 1.8.3. *Soient N un entier supérieur ou égal à 3, β un entier compris entre 2 et $N-1$. Soient $i_1, \dots, i_d$, telles que $1 = i_1 < i_2 < \dots < i_d = \beta$. Nous définissons alors un polynôme $\tilde{P}_1$ de $\mathbb{Z}[Y_1, \dots, Y_\beta]$ par*

$$\tilde{P}_1(Y_1, \dots, Y_\beta) = Z_{i_1}\dots Z_{i_d},$$

où la variable Z_i signifie Y_i ou $1 - Y_i$. Soit le polynôme à N variables

$$\begin{aligned}&P_N(X_1, \dots, X_N) :=\\ &\quad\sum_{i=1}^{N-\beta+1}\left[\tilde{P}_1(X_i, \dots, X_{i+\beta-1}) + \tilde{P}_2(X_i, \dots, X_{i+\beta-2}) + \tilde{P}_3(X_{i+1}, \dots, X_{i+\beta-1})\right],\end{aligned}$$

avec $\tilde{P}_2$ et $\tilde{P}_3$ des polynômes de $\mathbb{Z}[X_1, \dots, X_{\beta-1}]$ quelconques. Alors, il existe des constantes absolues C_1 et C_2 (les mêmes que celles du Théorème 0.4.1) strictement positives telles que

$$\sum_{2^{N-1}\leq n<2^N}\mu(n)(-1)^{P_N(n)} \ll N^{C_1}2^{N-C_2N\frac{1}{\beta 2^\beta}+o\left(\frac{N}{\beta 2^\beta}\right)} \qquad (N\to\infty), \tag{1.74}$$

où $P_N(n) = P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$.

Démonstration. Puisque $2^{N-1} \leq n < 2^N$, n a exactement N chiffres dans son écriture binaire finie. La suite β-récursive $(a(n))_{n\geq 0}$ de fonction de propagation $g : \Sigma_\beta \to \mathbb{N}$ qui a comme valeurs

$$g(\omega) = \dot{P}_1(\omega) + \dot{P}_2\left(\underline{\omega}_{|\omega|-1}\right) + \dot{P}_3\left(\overline{\omega}_{|\omega|-1}\right)$$

vérifie pour tout $2^{N-1} \leq n < 2^N$

$$\begin{aligned} a(n) &= \sum_{i=0}^{T_2(n)-\beta} g(\epsilon_{i+\beta-1}(n)\cdots\epsilon_i(n)) \\ &= \sum_{i=0}^{N-\beta} g(\epsilon_{i+\beta-1}(n)\cdots\epsilon_i(n)). \end{aligned}$$

La preuve du Théorème 0.4.1 se transpose alors à notre cas. □

Chapitre 2

Blocs de taille croissante

2.1 Introduction

Dans le chapitre précédent, nous avons étendu les travaux que Mauduit et Rivat ont effectués dans [MR15] en démontrant un théorème des nombres premiers et un principe d'aléa de Möbius pour une suite $(a(n))_{n\geq 0}$, où $a(n)$ vérifie

$$a(n) = a\left(\left\lfloor n/q^{T_q(n)-\beta+2}\right\rfloor\right) + \sum_{i=0}^{T_q(n)-\beta+1} g(\epsilon_i(n),\dots,\epsilon_{i+\beta-1}(n))$$

avec $g : \{0,\dots,q-1\}^\beta \to \mathbb{N}$ une fonction possédant une contrainte peu restrictive et $T_q(n)$ valant $\lfloor \log n/\log q\rfloor$, et où $\epsilon_0(n),\epsilon_1(n),\dots$ sont les chiffres de n en base q. Une conséquence de la méthode employée est l'obtention du théorème suivant (Théorème 0.4.1) :

Théorème. *Soient N un entier supérieur ou égal à 3, β un entier compris entre 2 et $N-1$. Soient $i_1,\dots,i_d$ tels que $1 = i_1 < i_2 < \dots < i_d = \beta$. Nous définissons alors un polynôme $\tilde{P}_1$ de $\mathbb{Z}[Y_1,\dots,Y_\beta]$ par*

$$\tilde{P}_1(Y_1,\dots,Y_\beta) = Z_{i_1}\dots Z_{i_{d-1}}Y_{i_d},$$

où la variable Z_i signifie Y_i ou $1-Y_i$. Soit le polynôme à N variables

$$P_N(X_1,\dots,X_N) := \sum_{i=1}^{N-\beta+1} \tilde{P}_1(X_i,\dots,X_{i+\beta-1}),$$

alors il existe des constantes absolues strictement positives C_1 et C_2 telles que

$$\sum_{n<2^N} \mu(n)(-1)^{P_N(n)} \ll N^{C_1} 2^{N-C_2 N\frac{1}{\beta 2^\beta}+o\left(\frac{N}{\beta 2^\beta}\right)} \qquad (N\to\infty), \tag{2.1}$$

où $P_N(n) = P_N(\epsilon_0(n),\dots,\epsilon_{N-1}(n))$, et où $\epsilon_0(n),\epsilon_1(n),\dots$ sont les chiffres de n en base 2.

Ce théorème est non trivial pour tout $\beta \leq c\log N$ avec $c < 1/\log q$. Il suggère donc qu'il est possible d'obtenir un théorème des nombres premiers pour des fonctions qui comptent des blocs dont la taille varie en fonction de $T_q(n)$. Le cas le plus

simple d'une fonction comptant les blocs est celle qui compte en base 2 des blocs exclusivement composés de '1', aussi nous nous sommes concentrés dans ce chapitre sur ce cas particulier (en réalité un cas un peu plus général, mais restant dans l'esprit de ce cas).

Soit $P : \mathbb{N} \to \mathbb{N}$ une application croissante. Si

$$n = \sum_{i=0}^{T_q(n)} \epsilon_i(n) q^i$$

est l'écriture de n en base q, nous définissons une suite $(a_P(n))_{n\geq 0}$ par,

$$a_P(n) = \sum_{i\geq 0} \epsilon_i(n) \dots \epsilon_{i+P(T_q(n))}(n).$$

et pour α réel, nous définissons $f_P(n) = e(\alpha a_P(n))$ la fonction associée à a_P.

Le cas $P(x) = x$ en base $q = 2$ donne

$$\begin{aligned} a_P(n) &= \epsilon_0(n) \cdots \epsilon_{T_2(n)}(n) \\ &= \begin{cases} 1 & \text{si} \quad n = \displaystyle\sum_{i=0}^{T_2(n)} 2^i = 2^{T_2(n)+1} - 1 \\ 0 & \text{sinon,} \end{cases} \end{aligned}$$

aussi il est intéressant de se demander quelle fonction est admissible pour que la méthode de Mauduit et Rivat s'applique.

Dans ce chapitre, nous démontrons les théorèmes suivants :

Théorème 2.1.1. *Soit P une fonction croissante, positive, et à valeurs entières pour laquelle il existe une constante strictement positive $c < 1/\log q$ telle que $P(y) \leq c \log y$ pour tout réel y assez grand. Alors uniformément en $\vartheta \in \mathbb{R}$:*

$$\left| \sum_{n\leq x} \Lambda(n) f_P(n) e(\vartheta n) \right| \ll c_1'(q) (\log x)^{3+\frac{\omega(q)}{4}} x q^{-\frac{1}{64}\gamma_P(\frac{1}{120}\lfloor \frac{\log x}{\log q}\rfloor, \lfloor \frac{\log x}{\log q}\rfloor)},$$

avec

$$\gamma_P(l,k) = l\left(1 - \frac{\log\left(q^{P(k)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(k)\log q}\right) \tag{2.2}$$

et $c_1'(q) = q^{26/128} \max\left((\log q)^3, \tau(q)^{1/4}\right) (\log q)^{-3-\frac{\omega(q)}{4}}$.

Théorème 2.1.2. *Soit P une fonction croissante, positive, et à valeurs entières pour laquelle il existe une constante strictement positive $c < 1/\log q$ telle que $P(y) \leq c \log y$ pour tout réel y assez grand. Alors uniformément en $\vartheta \in \mathbb{R}$:*

$$\left| \sum_{n\leq x} \mu(n) f_P(n) e(\vartheta n) \right| \ll c_1'(q) (\log x)^{3+\frac{\omega(q)}{4}} x q^{-\frac{1}{64}\gamma_P(\frac{1}{120}\lfloor \frac{\log x}{\log q}\rfloor, \lfloor \frac{\log x}{\log q}\rfloor)},$$

avec γ_P et définie par (2.2) et $c_1'(q)$ définie dans le théorème précédent.

Le Théorème 0.4.3 présenté dans l'introduction de cette thèse est l'exemplification des résultats de ce chapitre au cas $q = 2$. Dans le cas particulier où P est l'application constante égale à d, et $q = 2$, la suite $(a_P(n))_{n\geq 0}$ correspond à la suite $(b_d(n))_{n\geq 0}$ et notre résultat est traité dans l'article de Mauduit et Rivat [MR15].

Il serait possible de combiner les idées du chapitre précédent avec celles de ce chapitre, sans négliger un certain nombre de contraintes techniques, pour obtenir ce type de résultat pour toute classe de polynômes $(Q_{N,P(N)})_{N\geq 0}$ de $\mathbb{Z}[X_1, \dots, X_N]$ de degré $P(N)$ et de la forme des polynômes introduits dans le Théorème 0.4.2, et ceci pour toute fonction P à valeurs entières satisfaisant à $P(y) \leq c \log y$ et $c < 1/\log q$: les contraintes ne portent pas tant sur la forme précise du polynôme considéré que sur la vitesse de croissance de P.

Certaines hypothèses semblent plus indispensables : le fait que P soit croissante est utilisé dans de nombreuses et importantes estimations. Par ailleurs, P n'apparaît dans $a_P(n)$ que sous la forme $P(T_q(n))$: ceci veut dire que les blocs ne sont de taille potentiellement différentes que si les entiers ont un nombre de chiffres en *écriture finie* différents. Cette propriété est fondamentale dans notre raisonnement.

La technique utilisée ici repose sur un contrôle uniforme de la transformée de Fourier de f_P. Un meilleur contrôle de celle-ci entraînerait une amélioration immédiate et sans difficulté de la vitesse de croissance de P. Remarquons toutefois que la vitesse maximale pour que a_P soit non nulle, $P(x) = x$ est hors d'atteinte car les conclusions du théorème seraient alors fausses. En effet, le Théorème 2.1.1 implique (par intégration par partie) une équirépartition des nombres premiers selon les classes de congruences de a_P (résultat démontré dans la Proposition 3.2.1). Une conséquence du théorème pour $P(x) = x$, serait que la moitié des nombres premiers seraient des nombres de Mersenne. Nous verrons dans le Chapitre 3 que la vitesse $P(x) < \log x/\log q$ est la limite au-delà de laquelle la méthode ne permet plus de conclure.

Ce chapitre et le suivant font l'objet d'un article en cours de préparation [Han16a].

2.2 Notations

Pour des raisons techniques nous ne regarderons pas la suite $(a_P(n))_{n\geq 0}$ mais une application $a_P : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ à deux variables définie par :

$$a_P(x, y) := \sum_{i\geq 0} \epsilon_{i+P(y)}(x) \cdots \epsilon_i(x), \tag{2.3}$$

la première variable nous donne des informations sur les valeurs des chiffres, tandis que la seconde porte sur la taille de l'entier. Nous définissons alors $a_P^{(\rho)}(x, y) := a_P(x \bmod q^\rho, y)$. Avec ces définitions, nous avons $a_P(n) = a_P(n, T_q(n))$ et $a_P^{(\rho)}(n) = a_P^{(\rho)}(n, T_q(n)) = a_P(n \bmod q^\rho, T_q(n))$.

Si α est un nombre réel, nous définissons $f_P(x, y) := e(\alpha a_P(x, y))$, $f_P(n) := f_P(n, T_q(n))$, *etc.* Nous définissons également

$$f_P^{(\mu_1,\mu_2)}(x, y) := f_P^{(\mu_2)}(x, y)\overline{f_P^{(\mu_1)}(x, y)}.$$

Il s'agit d'une fonction doublement tronquée qui jouera un rôle crucial dans les estimations des sommes de type II.

Remarque 2.2.1. *La fonction γ_P définie par* (2.2) *intervient dans le contrôle de la transformée de Fourier de f_P. Ainsi, tout comme dans [MR15] nous avons*

$$1 = \sum_{0\leq h<q^\lambda} \left| \frac{1}{q^\lambda} \sum_{0\leq u<q^\lambda} f_P(uq^\kappa, k) e(-u(h+t)) \right|^2 \leq q^{\lambda - 2\gamma_P(\lambda,k)}$$

et donc $\gamma_P(\lambda, k) \leq \lambda/2$.

2.3 Panorama de la preuve

Comme au Chapitre 1, la preuve des Théorèmes 2.1.1 et 2.1.2 repose essentiellement sur la méthode que Mauduit et Rivat ont développée au cours d'une série d'articles (voir [MMR15, MR10, MR15]).

Leur idée consiste à montrer qu'un contrôle de la norme infinie de la transformée de Fourier d'une fonction f, définie d'une certaine manière sur les chiffres, permet de montrer une orthogonalité asymptotique entre f et les fonctions Λ et μ, via l'identité de Vaughan (ou son pendant). Ce contrôle a été formalisé par la Définition 1.2.2.

Afin de rendre cette connexion avec la transformée de Fourier possible nous avons besoin de la Définition 1.2.1 qui est une formalisation : pour les fonctions qui nous intéressent, seuls les chiffres du milieu de la décomposition en base q sont significatifs.

Une tentative naturelle pour montrer un principe d'aléa de Möbius et un théorème des nombres premiers pour une fonction basée sur les chiffres consiste à essayer de vérifier l'une et l'autre définition. Dans le cas où P est constante, Mauduit et Rivat le vérifient dans [MR15] pour notre fonction a_P. Seulement, si P n'est plus une application constante, la vérification de ces deux conditions devient délicate. L'obtention de la propriété de Fourier dans le cas P constante est due au fait que, la taille du bloc étant un moment donné "petite" par rapport à la taille d'un entier n, l'application $f(n) = e(\alpha a(n))$ s'avère vérifier une formule proche de $f(qn+r) = e(\alpha)f(n)$. Il est ainsi possible de trouver une formule de récurrence de la forme

$$\sum_{n<q^\lambda} V(n)e(n\theta) = M(\theta) \sum_{n<q^{\lambda-1}} V(n)e(n\theta),$$

où M est une matrice carrée dont la taille dépend de q et de f, et V est un vecteur dont les coordonnées dépendent de f.

Trouver ce type de récurrence dans notre cas est ardu, parce que, si τ est tel que $P(\tau) \neq P(\tau-1)$, et n_1, n_2 de la forme

$$n_1 = \sum_{i=0}^{\tau-1} \epsilon_i(n_1)q^i, \quad n_2 = \sum_{i=0}^{\tau} \epsilon_i(n_2)q^i$$

nous avons

$$a_P(n_1) = \sum_{i\geq 0} \epsilon_{i+P(\tau-1)}(n_1)\dots\epsilon_i(n_1)$$

et

$$\begin{aligned} a_P(n_2) &= \sum_{i\geq 0} \epsilon_{i+P(\tau)}(n_2)\dots\epsilon_i(n_2) \\ &= \sum_{i\geq 0} \epsilon_{i+P(\tau)}(n_2)\dots\epsilon_{i+P(\tau-1)+1}(n_2)\epsilon_{i+P(\tau-1)}(n_2)\dots\epsilon_i(n_2). \end{aligned}$$

Au vu de ces deux écritures, le nombre de chiffres considérés n'étant pas le même pour n_1 et pour n_2, il semble difficile de trouver une récurrence de la forme

$$\sum_{n<q^k} V_P(n)e(n\theta) = M(\theta) \sum_{n<q^{k-1}} V_P(n)e(n\theta).$$

Ce principe fournit néanmoins une propriété de Fourier légèrement altérée, en regardant les n qui possèdent le même nombre de chiffres, et en sommant ensuite sur toutes les tailles possibles.

En revanche, dès que P n'est plus constante, il est impossible d'avoir la propriété de propagation. Si nous reprenons notre τ tel que $P(\tau) \neq P(\tau-1)$; alors, pour n tel que $T_q(n) = \tau$ et $n \bmod q^\rho < n$,

$$a_P(n \bmod q^\rho) = \sum_{i\geq 0} \epsilon_{i+P(T_q(n \bmod q^\rho))}(n \bmod q^\rho)\dots\epsilon_i(n \bmod q^\rho), \tag{2.4}$$

et alors nécessairement $P(T_q(n)) = P(\tau) \neq P(T_q(n \bmod q^\rho))$. Le nombre de chiffres considérés pour n_1 et $n_1 \bmod q^\rho$ n'est pas le même et on ne peut pas espérer de simplification dans l'expression $a_P(n) - a_P(n \bmod q^\rho)$. Il n'y a donc *a priori* aucune raison de pouvoir contrôler le nombre de l tels que

$$a_P(lq^\kappa + k_1) - a_P(lq^\kappa + k_1 + k_2) \neq a_P((lq^\kappa + k_1) \bmod q^\rho) - a_P((lq^\kappa + k_1 + k_2) \bmod q^\rho)$$

si lq^κ est "beaucoup plus grand" que q^ρ. Nous nous trouvons alors dans l'obligation de redéfinir la propagation de manière à contourner ce problème, ce qui modifie considérablement la preuve de [MR15].

Ainsi l'écriture d'un entier en base q nécessite deux informations : sa taille, $T_q(n)$, et ses chiffres significatifs, c'est-à-dire ceux situés avant sa taille. L'idée principale de ce chapitre consiste alors à regarder, non pas une fonction à une variable $a_P(n)$ mais une fonction à deux variables $a_P(n_1, n_2)$ la première variable codant l'information digitale, la seconde l'information de taille, $T_q(n)$, et notre problème consiste à regarder $a_P(n, T_q(n))$. Dès lors, la troncation ne portera que sur la première variable, et une propriété de propagation altérée devient possible (Lemmes 2.4.2 et 2.6.8). Nous sommes ainsi loin de la démonstration donnée dans le chapitre précédent, où seules certaines modifications numériques de [MR15] suffisaient.

Comme dit précédemment, la preuve de [MR15] utilise l'identité de Vaughan, qui relie

$$\sum_{n\leq x} \Lambda(n)f(n)$$

à des sommes plus faciles à estimer :

$$S_I(\vartheta) := \sum_{M/q<m\leq M} \left| \sum_{\substack{n \\ mn\in I(M,N)}} f(mn)e(\vartheta mn) \right|$$

et

$$S_{II}(\vartheta) := \sum_{\frac{M}{q}<m\leq M} \sum_{N/q<n\leq N} a_m b_n f(mn) e(\vartheta mn),$$

où ici $|a_m|, |b_n| \leq 1$, M et N sont des entiers reliés l'un à l'autre de manières différentes selon S_I et S_{II}, m et n des entiers tels que $M/q \leq m < M$, $N/q \leq n < N$, $\vartheta \in \mathbb{R}$ et $I(M,N) \subset [0, MN)$.

Après avoir complété S_I, nous introduisons (modulo un terme d'erreur) la fonction tronquée dans l'espoir de relier S_I à la transformée de Fourier. Ici deux difficultés surgissent.

Premièrement il est plus difficile, malgré le travail préliminaire déjà mentionné, de séparer la structure digitale de la structure multiplicative du problème. Mauduit et Rivat procèdent de la sorte : si n est écrit sous la forme $u + vq^\kappa$ avec $u < q^\kappa$, si $w = v \bmod q^\rho$ et si P est constante, il résulte que

$$f_P^{(\kappa+\rho)}(u + vq^\kappa) = f_P^{(\kappa+\rho)}(u + wq^\kappa),$$

mais si P n'est plus constante, ce n'est plus le cas, car $T_q(u+vq\kappa) \neq T_q(u+wq^\kappa)$ en général. Pour contourner le problème, nous passons par l'idée suivante : pour n un entier en considérant l'écriture $n = u + vq^\kappa$ avec $0 \leq u < q^\kappa$, en posant $T_q(n) = l$, et $w = v \bmod q^\rho$, nous introduisons $n' = u + wq^\kappa + q^{\kappa+\rho}\lfloor q^{l-\rho} \rfloor$. Alors nous avons pour tout $0 \leq i < \kappa + \rho$:

$$\begin{cases} T_q(n') & = T_q(u + wq^\kappa + q^{\kappa+\rho}\lfloor q^{l-\rho}\rfloor) & = T_q(vq^\kappa) \\ \epsilon_i(n') & = \epsilon_i(u + wq^\kappa + q^{\kappa+\rho}\lfloor q^{l-\rho}\rfloor \bmod q^{\kappa+\rho}) & = \epsilon_i(u + vq^\kappa). \end{cases}$$

D'une certaine manière, n' est mieux adapté au processus de séparation des informations digitales et de taille d'un entier n. Le rôle de $q^{\kappa+\rho}\lfloor q^{l-\rho}\rfloor$ est de continuer à indiquer la taille de n.

D'autre part pour les petits entiers le contrôle de la transformée de Fourier se révèle impossible. Nous différencions donc notre estimation selon les cas où un tel contrôle est possible et ceux où il ne l'est pas, et afin de majorer proprement les occurrences du second cas, nous exploitons le fait que la croissance de P ne saurait Ãªtre trop forte. Ces difficultés techniques mises à part, le traitement de S_I suit la méthode utilisée dans [MR15].

Le contrôle de S_{II} commence comme dans [MR15] ; à savoir que la première étape consiste à lisser la somme, c'est-à-dire à se rapporter à une somme où n'interviennent pas les coefficients a_m et b_n. Cette opération conduit à regarder une double corrélation :

$$\sum_m \sum_n f_P^{(\mu_2)}((m + sq^{\mu_1})(n + r))\overline{f_P^{(\mu_2)}(m(n + r))f_P^{(\mu_2)}((m + sq^{\mu_1})n)}f_P^{(\mu_2)}(mn). \quad (2.5)$$

A ce stade de la preuve, Mauduit et Rivat introduisent une fonction doublement tronquée $f_P^{(\mu_1,\mu_2)}$ dans le but d'effectuer le reste des calculs uniquement sur les chiffres du milieu :

$$S_2''(r,s) := \sum_m \sum_n f_P^{(\mu_1,\mu_2)}((m + sq^{\mu_1})(n + r))\overline{f_P^{(\mu_1,\mu_2)}(m(n + r))} \cdot \overline{f_P^{(\mu_1,\mu_2)}((m + sq^{\mu_1})n)}f_P^{(\mu_1,\mu_2)}(mn). \quad (2.6)$$

Une motivation possible de cet acte est que, contrairement à la situation dans (2.5), les entiers considérés dans (2.6) se trouvent "indépendants" : les chiffres compris entre μ_1 et μ_2 de mn sont différents de ceux de $m(n+r)$ (du fait de l'ajout de r).

Une autre raison de faire ce calcul est qu'il permet d'utiliser tout un panel d'objets liés à l'analyse harmonique. Toutefois si la perturbation est trop forte (typiquement $\mu_1 > T_q(m)$), la taille des entiers considérés peut en Ã^atre altérée, et le passage d'une fonction simplement tronquée à doublement tronquée, peut, dans notre cas, Ã^atre compromis (des raisons détaillées de ce fait se trouvent dans la Partie 2.7).

Fort heureusement, si la perturbation est petite, ceci n'arrive que très rarement, et nous majorons le terme d'erreur dans le Lemme 2.6.4. Il suffit alors de déterminer une perturbation acceptable (on prendra $\mu_1 = T_q(m) - 3\rho$ et $s < q^{2\rho}$). Ce dernier fait est, selon nous, avec le fait de séparer dès le départ les notions de tailles et de chiffres, la nouveauté principale de ce chapitre. Nous pouvons démontrer le Lemme 2.6.4 au moins de deux différentes manières. La première, suggérée par O.Robert, consiste à remarquer que la fonction T_q est croissante, et à obtenir une majoration de la quantité désirée à l'aide des sommes d'exponentielles. La seconde, présentée ici car plus élémentaire, plus courte et de meilleur terme d'erreur, a été suggérée par T.Stoll. Elle utilise également les sommes d'exponentielles, mais de manière cachée, dans un lemme ici admis. Selon nous, la première idée possède toutefois l'avantage de s'inscrire dans une plus large catégorie de problèmes.

Une fois ce lemme établi, nous nous trouvons dans une situation très proche de celle de [MR15], à la différence près que les quantités regardées restent liées, mais si faiblement que nous pouvons continuer à exercer sur elles un contrôle similaire à celui opéré dans [MR15] en prenant toutefois des précautions au niveau des calculs. Ce sont ces précautions qui nous poussent à démontrer les Lemmes 2.6.2 et 2.6.3.

Ce chapitre est présenté comme suit. Les Parties 2.4 et 2.6 sont dédiées à la collecte de résultats utiles, respectivement, au traitement des sommes de type I et de type II. Ces résultats sont de différentes natures (analytiques, digitaux et harmoniques) et leur démonstration est assez différente du schéma global de la preuve principale : les inclure nuirait à la compréhension structurelle du traitement des sommes. Dans la Partie 2.5 nous exerÃ§ons un contrôle sur les sommes de type I, et dans la Partie 2.7, sur les sommes de type II. Dans la Partie 2.8 nous réunissons les résultats des Parties 2.5 et 2.7 afin d'obtenir les théorèmes. Enfin dans la Partie 2.9, nous réunissons les différentes contraintes sur la fonction P obtenues dans les parties précédentes afin de déterminer une croissance possible de P. Nous obtenons notamment que pour toute fonction à valeurs entières P, telle qu'il existe une constante strictement positive $c < 1/\log q$ telle que $P(x) \leq c \log x$ pour tout réel x, la fonction $f_P(n) = e(\alpha a_P(n))$ vérifie un théorème des nombres premiers et un principe d'aléa de Möbius pour tout α non entier. Enfin, nous fournissons dans la Partie 2.10 une preuve que les suites que nous étudions ne sont pas automatiques. Dans tout ce chapitre, P désigne une fonction à valeurs entières.

2.4 Travail préparatoire pour les sommes de type I

L'essentiel des résultats présentés ici servent à la Partie 2.5. Le Lemme 2.4.2 sert aussi à la Partie 2.6. Ce lemme est de nature digitale. Les Lemmes 2.4.3 et 2.4.4 eux sont de l'ordre de l'analyse harmonique.

L'énoncé du lemme suivant est le résultat final d'un (assez) long calcul voué à apparaÃ®tre plusieurs fois dans la Partie 2.5.

Lemme 2.4.1. *Soient μ, ν, $q \geq 2$ et d des entiers. Soit M un entier tel que $q^{\mu-1} \leq M < q^{\mu}$ et κ_d un entier tel que $1 \leq \kappa_d \leq \frac{2}{3}(\mu+\nu)$ et $q^{\kappa_d-1} < M^2/d^2 \leq q^{\kappa_d}$. Considérons enfin $0 \leq \rho_1 \leq \mu+\nu-\kappa_d$, $0 \leq h < q^{\rho_1}$ et $0 \leq u < q^{\kappa_d}$ des entiers ainsi que ϑ' un réel. Nous posons pour l un entier quelconque*

$$c_{\kappa_d,\rho_1,l}(u,h) = \frac{1}{q^{\rho_1}} \sum_{w<q^{\rho_1}} f_P^{(\kappa_d+\rho_1)}(u + wq^{\kappa_d} + q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor) \cdot \overline{f_P^{(\kappa_d+\rho_1)}(wq^{\kappa_d} + q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor)} e\left(-\frac{hw}{q^{\rho_1}}\right),$$

et

$$S(M,d,l) = \sum_{0\leq h<q^{\rho_1}} \sum_{\frac{M}{qd}\leq m'<\frac{M}{d}} \frac{1}{m'} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \left| \sum_{0\leq u<q^{\kappa_d}} c_{\kappa_d,\rho_1,l}(u,h) e\left(-\frac{u\vartheta'}{q^{\mu+\nu}} + \frac{uk'}{m'}\right)\right|.$$

Alors

$$|S(M,d,l)| \ll (\log q) q^{\rho_1/2+\kappa_d}.$$

Démonstration. Nous assemblons des parties éparses de la démonstration des sommes de type I de [MR15].

Pour commencer

$$\sum_{\frac{M}{qd}\leq m'<\frac{M}{d}} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \frac{1}{m'^2} \leq \sum_{\frac{M}{qd}\leq m'<\frac{M}{d}} \frac{1}{m'} \ll \log q,$$

donc par l'inégalité de Cauchy-Schwarz, nous avons

$$|S(M,d,l)|^2 \ll (\log q) q^{\rho_1} \sum_{0\leq h<q^{\rho_1}} \sum_{\frac{M}{qd}\leq m'<\frac{M}{d}} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \left| \sum_{0\leq u<q^{\kappa_d}} c_{\kappa_d,\rho_1,l}(u,h) e\left(-\frac{u\vartheta'}{q^{\mu+\nu}} + \frac{uk'}{m'}\right)\right|^2.$$

Nous utilisons alors l'inégalité du Grand Crible (Théorème A.2.4) pour affirmer

$$|S(M,d,l)|^2 \ll (\log q) q^{\rho_1} \sum_{0\leq h<q^{\rho_1}} \left(q^{\kappa_d} + \frac{M^2}{d^2}\right) \sum_{0\leq u<q^{\kappa_d}} |c_{\kappa_d,\rho_1,l}(u,h)|^2.$$

Cependant

$$\begin{aligned}
&\sum_{0\le h<q^{\rho_1}} |c_{\kappa_d,\rho_1,l}(u,h)|^2\\
&= \sum_{0\le h<q^{\rho_1}} \frac{1}{q^{2\rho_1}} \sum_{0\le w,w'<q^{\rho_1}} e\left(-\frac{h(w-w')}{q^{\rho_1}}\right)\\
&\qquad f_P^{(\kappa_d+\rho_1)}(u+wq^{\kappa_d}+q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor)\overline{f_P^{(\kappa_d+\rho_1)}(u+w'q^{\kappa_d}+q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor)}\\
&\qquad \overline{f_P^{(\kappa_d+\rho_1)}(wq^{\kappa_d}+q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor)} f_P^{(\kappa_d+\rho_1)}(w'q^{\kappa_d}+q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor)\\
&= \frac{1}{q^{\rho_1}} \sum_{0\le w<q^{\rho_1}} \left|f_P^{(\kappa_d+\rho_1)}(wq^{\kappa_d}+q^{\kappa_d+\rho_1}\lfloor q^l/q_1^{\rho}\rfloor)\right|^2 \left|f_P^{(\kappa_d+\rho_1)}(u+wq^{\kappa_d}+q^{\kappa_d+\rho_1}\lfloor q^l/q^{\rho_1}\rfloor)\right|^2\\
&= 1
\end{aligned}$$

par définition de f_P. Ainsi

$$\begin{aligned}
|S(M,d,l)|^2 &\ll (\log q)q^{\rho_1}\left(q^{\kappa_d}+\frac{M^2}{d^2}\right)\sum_{0\le u<q^{\kappa_d}}\sum_{0\le h<q^{\rho_1}}|c_{\kappa_d,\rho_1,l}(u,h)|^2\\
&\ll (\log q)q^{\rho_1}\left(q^{\kappa_d}+\frac{M^2}{d^2}\right)q^{\kappa_d},
\end{aligned}$$

et comme $q^{\kappa_d-1} < M^2/d^2 \le q^{\kappa_d}$ le résultat est obtenu. □

Nous démontrons à présent un pendant de la propriété de petite propagation.

Lemme 2.4.2. *Soit ρ, λ et κ des entiers tels que $P(\lambda+\kappa+1) \le \rho$ et $\rho \le \frac{3}{4}\lambda$. Soit B l'ensemble des $0 \le l < q^\lambda$ tels qu'il existe $0 \le k_1, k_2 < q^\kappa$ tels que*

$$a_P(lq^\kappa+k_1+k_2) - a_P(lq^\kappa+k_1) \ne a_P^{(\kappa+\rho)}(lq^\kappa+k_1+k_2) - a_P^{(\kappa+\rho)}(lq^\kappa+k_1).$$

Alors

$$\#B \ll q^{\lambda-\rho+P(\lambda+\kappa+1)}.$$

Démonstration. Nous rappelons qu'ici *a priori*

$$\begin{aligned}
a_P^{(\rho)}(n) &= \sum_{i\ge 0}\epsilon_{i+T_q(n)}(n \bmod q^\rho)\dots\epsilon_i(n \bmod q^\rho)\\
&\ne \sum_{i\ge 0}\epsilon_{i+T_q(n \bmod q^\rho)}(n \bmod q^\rho)\dots\epsilon_i(n \bmod q^\rho).
\end{aligned}$$

Commençons par montrer que le nombre de $l < q^\lambda$ tels que $T_q(lq^\kappa+k_1+k_2) \ne T_q(lq^\kappa+k_1)$ est majoré par $\lambda+1$. En effet, cela n'arrive que s'il existe un m de sorte que $lq^\kappa+k_1 < q^m < lq^\kappa+k_1+k_2$. Ceci implique $0 \le l < q^{m-\kappa} < l+2$ et donc $l = q^{m-\kappa}-1$ si $m \ge \kappa$ et $l = 0$ si $m \le \kappa$. Les valeurs de l possibles sont donc $\{0, q-1, q^2-1, \dots, q^\lambda-1\}$ soient $\lambda+1$ valeurs.

Nous pouvons à présent supposer que $T_q(lq^\kappa+k_1+k_2) = T_q(lq^\kappa+k_1)$ quels que soient l, k_1, k_2.

Soit à présent $y \le \lambda+\kappa+1$ fixé. Pour tout entier n nous avons par (2.3),

$$a_P(n,y) = \sum_{i\ge 0}\epsilon_{i+P(y)}(n)\dots\epsilon_i(n)$$

et

$$a_P^{(\rho)}(n,y) = \sum_{i\geq 0} \epsilon_{i+P(y)}(n \bmod q^\rho)\dots\epsilon_i(n \bmod q^\rho) = \sum_{i\leq \rho - P(y)} \epsilon_{i+P(y)}(n)\dots\epsilon_i(n).$$

Ceci nous donne

$$\begin{aligned} &a_P(lq^\kappa + k_1 + k_2, y) - a_P(lq^\kappa + k_1, y) - a_P^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2, y) + a_P^{(\kappa+\rho)}(lq^\kappa + k_1, y) \\ &= \sum_{i>\kappa+\rho-P(y)} \left[\epsilon_{i+P(y)}(lq^\kappa + k_1 + k_2)\dots\epsilon_i(lq^\kappa + k_1 + k_2) - \epsilon_{i+P(y)}(lq^\kappa + k_1)\dots\epsilon_i(lq^\kappa + k_1)\right]. \end{aligned}$$

Pour que cette quantité soit non nulle, puisque $P(y) \leq \rho$, il est donc nécessaire que

$$\epsilon_{\kappa+\rho-P(y)}(lq^\kappa + k_1 + k_2) \neq \epsilon_{\kappa+\rho-P(y)}(lq^\kappa + k_1),$$

(sinon, cela veut dire que la propagation s'est arrÃªtée avant le chiffre d'indice $\kappa + \rho - P(y)$), ce qui signifie

$$\epsilon_{\rho-P(y)}(l + \lfloor (k_1 + k_2)/q^\kappa \rfloor) \neq \epsilon_{\rho-P(y)}(l).$$

Comme $\lfloor (k_1 + k_2)/q^\kappa \rfloor \leq 1$, ceci ne peut être vérifié que si $\epsilon_i(l) = q - 1$ pour tout $0 \leq i < \rho - P(y)$. Nous avons donc que le nombre de l tels que la quantité soit non nulle est $O(q^{\lambda-\rho+P(y)})$. Nous appliquons alors ce résultat avec $y = T_q(lq^\kappa + k_1) = T_q(lq^\kappa + k_1 + k_2) \leq \lambda + \kappa + 1$, et nous exploitons la croissance de P pour obtenir

$$\#B \ll q^{\lambda-\rho+P(\lambda+\kappa+1)} + \lambda + 1$$

et comme $\rho \leq 3/4\lambda$, nous avons $\lambda + 1 \ll q^{\lambda-\rho}$, et le résultat est prouvé. □

Le lemme suivant fournit la propriété de Fourier.

Lemme 2.4.3. *Soient $l \geq 0$ et κ des entiers tel que $P(\kappa+l) \leq l$, alors uniformément en $t \in \mathbb{R}$:*

$$\left| \sum_{q^{l-1}\leq u<q^l} f_P(uq^\kappa, T_q(uq^\kappa))e(-ut) \right| \leq q^{\gamma(l,\kappa)},$$

avec

$$\gamma(l,\kappa) := l\frac{\log\left(q^{P(\kappa+l)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(\kappa+l)\log q}. \tag{2.7}$$

Nous remarquons que la différence avec la transformée de Fourier introduite dans le chapitre précédent consiste essentiellement dans l'intervalle de sommation.

Démonstration. Dans cette démonstration, nous serons amenés à utiliser des objets introduits dans le chapitre précédent, notamment dans la Définition 1.6.4. Nous commenÃ§ons par remarquer que, à κ fixé, $T_q(uq^\kappa)$ est constante sur $q^{l-1} \leq u < q^l$ et donc $P(T_q(uq^\kappa)) = P(\kappa + l - 1)$. Soit donc $\beta = P(\kappa + l - 1)$ et V_u le u-ième vecteur généalogique lié à la fonction β-récursive $a(n) = \sum_{i\geq 0} \epsilon_{i+\beta}(n)\dots\epsilon_i(n)$; alors

$$\left| \sum_{q^{l-1}\leq u<q^l} f_P(uq^\kappa, T_q(uq^\kappa))e\left(-ut\right) \right| \leq \left\| \sum_{q^{l-1}\leq u<q^l} V_u e(-ut) \right\|_\infty.$$

Nous obtenons donc, de manière similaire aux Corollaires 1.6.7 et 1.6.10,

$$\left|\sum_{q^{l-1}\leq u<q^l} f_P(uq^\kappa, T_q(uq^\kappa))e\left(-ut\right)\right| \leq \left(q^{P(l+\kappa)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)^{\left\lfloor\frac{l}{P(\kappa+l)}\right\rfloor}$$
$$\leq \left(q^{P(l+\kappa)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)^{\frac{l}{P(\kappa+l)}},$$

ce qui achève la preuve. □

Proposition 2.4.4. *Si $P(0) \geq 3$, la fonction $(l,\kappa) \mapsto \gamma(l,\kappa)/l$ est une fonction croissante en l et en κ sur $[0,\infty)$. De plus la fonction γ vérifie $\gamma(l,\kappa) = \gamma(l+k,\kappa-k)$ pour tout k réel.*

Démonstration. Nous avons, par définition :

$$\frac{\gamma(l,\kappa)}{l} := \frac{\log\left(q^{P(\kappa+l)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(\kappa+l)\log q},$$

mais pour tout $K > 0$, l'application

$$x \mapsto \frac{\log(x-K)}{\log x}$$

a pour dérivée

$$\frac{1}{(\log x)^2}\cdot\left(\frac{\log x}{x-K} - \frac{\log(x-K)}{x}\right) = \frac{1}{(\log x)^2}\cdot\frac{x\log x - (x-K)\log(x-K)}{x(x-K)}$$

qui est positive si $x \geq K$ par croissance de la fonction $f(x) = x\log x$. Ici $x = q^{P(\kappa+l)}$ et $K = 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2$. La condition est donc vérifiée si $P(0) \geq 3$ par croissance de P. □

Nous sommes maintenant en mesure de contrôler les sommes de type I.

2.5 Sommes de type I

Soient $1 \leq M \leq N$ tels que

$$M \leq (MN)^{1/3} \tag{2.8}$$

et μ et ν les uniques entiers tels que $q^{\mu-1} \leq M < q^\mu$ et $q^{\nu-1} \leq N < q^\nu$ (ou encore $T_q(M) = \mu - 1, T_q(N) = \nu - 1$).

Soient également $\vartheta \in \mathbb{R}$ et $I := I(M,N) \subset [0, MN]$ un intervalle. Nous posons alors

$$S_I(\vartheta) := \sum_{M/q<m\leq M}\left|\sum_{\substack{n:\\ mn\in I(M,N)}} f_P(mn)e(\vartheta mn)\right|.$$

Théorème 2.5.1. *Soit P tel que*

$$P(\mu+\nu+1) \leq \gamma_P\left(\frac{1}{3}(\mu+\nu),\, \mu+\nu\right), \tag{2.9}$$

alors nous avons uniformément en $\vartheta \in \mathbb{R}$:

$$S_I(\vartheta) \ll (\mu+\nu)^3 (\log q)^3 q^{\mu+\nu-\frac{1}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)},$$

où $\gamma_P(k,l)$ est définie en (2.2).

Démonstration. Nous commenÃ§ons par réécrire et compléter la somme de sorte à nous ramener à une somme S_I' plus simple à manipuler. Soit $0 \leq l < q^{\mu+\nu}$ entier. Pour $\frac{M}{q} < m \leq M$, nous pouvons écrire $l = mn$ avec $mn \in I$ si et seulement si $l \in I$ et $l \equiv 0 \bmod m$. Ainsi nous pouvons écrire la somme interne de $S_I(\vartheta)$ sous la forme

$$\begin{aligned}
&\sum_{\substack{n:\\ mn\in I(M,N)}} f_P(mn)e(\vartheta mn) \\
&\quad= \sum_{0\leq l<q^{\mu+\nu}} f_P(l)e(\vartheta l) \sum_{u\in I} \frac{1}{q^{\mu+\nu}} \sum_{0\leq h<q^{\mu+\nu}} e\left(\frac{h(u-l)}{q^{\mu+\nu}}\right) \frac{1}{m} \sum_{0\leq k<m} e\left(\frac{kl}{m}\right) \\
&\quad= \sum_{0\leq h<q^{\mu+\nu}} \left(\sum_{u\in I} e\left(\frac{hu}{q^{\mu+\nu}}\right)\right) \frac{1}{m} \sum_{0\leq k<m} \frac{1}{q^{\mu+\nu}} \sum_{0\leq l<q^{\mu+\nu}} f_P(l)e\left(\vartheta l - \frac{hl}{q^{\mu+\nu}} + \frac{kl}{m}\right).
\end{aligned}$$

Nous en déduisons que,

$$\begin{aligned}
S_I(\vartheta) = \sum_{M/q<m\leq M} \Bigg| &\sum_{0\leq h<q^{\mu+\nu}} \left(\sum_{u\in I(M,N)} e\left(\frac{hu}{q^{\mu+\nu}}\right)\right) \\
&\cdot \frac{1}{m} \sum_{0\leq k<m} \frac{1}{q^{\mu+\nu}} \sum_{0\leq l<q^{\mu+\nu}} f_P(l)e\left(\vartheta l - \frac{hl}{q^{\mu+\nu}} + \frac{kl}{m}\right)\Bigg|.
\end{aligned}$$

En posant

$$S_I'(\vartheta) = \sum_{M/q<m\leq M} \frac{1}{m} \sum_{0\leq k<m} \left| \frac{1}{q^{\mu+\nu}} \sum_{0\leq l<q^{\mu+\nu}} f_P(l)e\left(-\frac{l\left(\vartheta - \frac{k}{m}q^{\mu+\nu}\right)}{q^{\mu+\nu}}\right)\right|,$$

et en remarquant que $|I(M,N)| \leq q^{\mu+\nu}$, on a :

$$S_I(\vartheta) \leq \sum_{h<q^{\mu+\nu}} \min\left(q^{\mu+\nu}, \left|\sin\frac{\pi h}{q^{\mu+\nu}}\right|^{-1}\right) S_I'(h-\vartheta q^{\mu+\nu}),$$

ce qui nous donne, par le Lemme A.2.10,

$$S_I(\vartheta) \ll q^{\mu+\nu}\log q^{\mu+\nu} \left(\max_{\vartheta'\in\mathbb{R}} S_I'(\vartheta')\right). \tag{2.10}$$

Nous introduisons à présent la fonction tronquée. Pour ce faire, pour tout $1 \leq \kappa \leq \frac{2}{3}(\mu+\nu)$, nous introduisons $1 \leq \rho \leq \mu+\nu-\kappa$, que l'on choisira explicitement par

la suite. En posant $g(t) = \dfrac{1}{q^{\mu+\nu}} \sum_{l<q^{\mu+\nu}} f_P(l) e\left(-\dfrac{lt}{q^{\mu+\nu}}\right)$, et en écrivant $l = u + vq^\kappa$, on obtient

$$g(t) = \frac{1}{q^{\mu+\nu-\kappa}} \sum_{v<q^{\mu+\nu-\kappa}} f_P(vq^\kappa) e\left(-\frac{vt}{q^{\mu+\nu-\kappa}}\right) \frac{1}{q^\kappa} \sum_{u<q^\kappa} f_P(u+vq^\kappa)\overline{f_P(vq^\kappa)} e\left(-\frac{ut}{q^{\mu+\nu}}\right)$$

$$= \frac{1}{q^{\mu+\nu-\kappa}} \sum_{v<q^{\mu+\nu-\kappa}} f_P(vq^\kappa) e\left(-\frac{vt}{q^{\mu+\nu-\kappa}}\right) \frac{1}{q^\kappa} \sum_{u<q^\kappa} f_P^{(\kappa+\rho)}(u+vq^\kappa)\overline{f_P^{(\kappa+\rho)}(vq^\kappa)} e\left(-\frac{ut}{q^{\mu+\nu}}\right) \tag{2.11}$$

$$+ \frac{1}{q^{\mu+\nu-\kappa}} \sum_{v<q^{\mu+\nu-\kappa}} f_P(vq^\kappa) e\left(-\frac{vt}{q^{\mu+\nu-\kappa}}\right) \tag{2.12}$$

$$\cdot \frac{1}{q^\kappa} \sum_{u<q^\kappa} \left[f_P(u+vq^\kappa)\overline{f_P(vq^\kappa)} - f_P^{(\kappa+\rho)}(u+vq^\kappa)\overline{f_P^{(\kappa+\rho)}(vq^\kappa)}\right] e\left(-\frac{ut}{q^{\mu+\nu}}\right).$$

On rappelle qu'ici

$$f_P^{(\kappa+\rho)}(n) = e\left(\alpha a_P\Big(n \bmod q^{\kappa+\rho}, T_q(n)\Big)\right).$$

Nous incorporons (2.11), qu'on nomme $G_{\kappa,1}(t)$, et (2.12), qu'on nomme $G_{\kappa,2}(t)$, dans $S_I'(\vartheta)$ avec la valeur $\kappa = \kappa_d$ définie par

$$q^{\kappa_d - 1} < M^2/d^2 \le q^{\kappa_d}. \tag{2.13}$$

Ici le choix de κ_d intervient avant tout pour des raisons techniques. En posant $t = \vartheta - \frac{k}{m} q^{\mu+\nu}$, la majoration devient :

$$S_I'(\vartheta) \le \sum_{1\le d\le M} \sum_{\frac{M}{q}<m\le M} \frac{1}{m} \sum_{\substack{0\le k<m\\(k,m)=d}} \left|G_{\kappa_d,1}\left(\vartheta - \frac{k}{m}q^{\mu+\nu}\right) + G_{\kappa_d,2}\left(\vartheta - \frac{k}{m}q^{\mu+\nu}\right)\right|, \tag{2.14}$$

ainsi S_I' est séparée en deux sommes :

$$S_{I,1}'(\vartheta) = \sum_{1\le d\le M} \sum_{\frac{M}{q}<m\le M} \frac{1}{m} \sum_{\substack{0\le k<m\\(k,m)=d}} \left|G_{\kappa_d,1}\left(\vartheta - \frac{k}{m}q^{\mu+\nu}\right)\right|$$

et

$$S_{I,2}'(\vartheta) := \sum_{1\le d\le M} \sum_{\frac{M}{q}<m\le M} \frac{1}{m} \sum_{\substack{0\le k<m\\(k,m)=d}} \left|G_{\kappa_d,2}\left(\vartheta - \frac{k}{m}q^{\mu+\nu}\right)\right|.$$

Contrôlons à présent le terme d'erreur $S_{I,2}'(\vartheta)$. Supposons

$$P(\mu+\nu+1) \le \rho, \tag{2.15}$$

et

$$\rho \le \frac{\mu+\nu}{4}. \tag{2.16}$$

Par (2.8) et (2.13), nous avons $\frac{2}{3}(\mu+\nu) \geq \kappa_d$, et alors ρ satisfait à $\rho \leq \frac{3}{4}(\mu+\nu-\kappa_d)$ de sorte que le Lemme 2.4.2 s'applique avec $\lambda = \mu+\nu-\kappa_d$, $\kappa = \kappa_d$ et $\rho = \rho$. Il vient donc que le nombre de $0 \leq v < q^{\mu+\nu-\kappa_d}$ tels qu'il existe $0 \leq u < q^{\kappa_d}$ avec

$$f_P(u+vq^{\kappa_d})\overline{f_P(vq^{\kappa_d})} \neq f_P^{(\kappa_d+\rho)}(u+vq^{\kappa_d})\overline{f_P^{(\kappa_d+\rho)}(vq^{\kappa_d})}$$

est $O(q^{\mu+\nu-\kappa_d-\rho+P(\mu+\nu+1)})$. En nommant $\widetilde{\mathcal{W}}_{\kappa_d}$ l'ensemble des couples (u,v) vérifiant cette propriété, on a

$$\#\widetilde{\mathcal{W}}_{\kappa_d} \ll q^{\mu+\nu-\rho+P(\mu+\nu+1)}. \tag{2.17}$$

Nous posons à présent

$$\mathcal{W}_{\kappa_d} := \{w = u+vq^{\kappa_d} : (u,v) \in \widetilde{\mathcal{W}}_{\kappa_d}\},$$

de sorte que $v = r_{\kappa_d,\mu+\nu}(w)$, ce qui est une écriture admissible puisque $\frac{2}{3}(\mu+\nu) \geq \kappa_d$. La quantité $G_{\kappa_d,2}(t)$ satisfait par ces considérations à

$$G_{\kappa_d,2}(t) = \frac{1}{q^{\mu+\nu}} \sum_{0\leq w<q^{\mu+\nu}} c'_{\kappa_d,\rho_1}(w) e\left(-\frac{wt}{q^{\mu+\nu}}\right),$$

avec

$$\begin{aligned}
&|c'_{\kappa_d,\rho_1}(w)| \\
&= \left| f_P(q^{\kappa_d} r_{\kappa_d,\mu+\nu}(w)) \left(f_P(w)\overline{f_P(q^{\kappa_d} r_{\kappa_d,\mu+\nu}(w))} - f_P^{(\kappa+\rho)}(w)\overline{f_P^{(\kappa+\rho)}(q^{\kappa_d} r_{\kappa_d,\mu+\nu}(w))} \right) \right| \\
&\leq 2 \cdot \mathbb{1}_{w\in\mathcal{W}_{\kappa_d}}.
\end{aligned} \tag{2.18}$$

Cette notation nous permet d'écrire

$$\begin{aligned}
S'_{I,2}(\vartheta) &= \sum_{1\leq d\leq M} \sum_{\frac{M}{q}<m\leq M} \frac{1}{m} \sum_{\substack{0\leq k<m \\ (k,m)=d}} \left| G_{\kappa_d,2}(\vartheta - q^{\mu+\nu}k/m) \right| \\
&\leq \sum_{1\leq d\leq M} \frac{S''_{I,2}(M,d)}{dq^{\mu+\nu}},
\end{aligned} \tag{2.19}$$

où on a posé

$$S''_{I,2}(M,d) = \sum_{\frac{M}{qd}<m'\leq\frac{M}{d}} \frac{1}{m'} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \left| \sum_{w<q^{\mu+\nu}} c'_{\kappa_d,\rho_1}(w) e\left(-\frac{w\vartheta}{q^{\mu+\nu}} + \frac{wk'}{m'}\right) \right|.$$

Comme

$$\sum_{\frac{M}{qd}<m'\leq\frac{M}{d}} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \frac{1}{m'^2} \leq \sum_{\frac{M}{qd}<m'\leq\frac{M}{d}} \frac{1}{m'} \ll \log q, \tag{2.20}$$

par l'inégalité de Cauchy-Schwarz, il vient que

$$\left|S''_{I,2}(M,d)\right|^2 \ll \log q \sum_{\frac{M}{qd}<m'\leq\frac{M}{d}} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \left| \sum_{w<q^{\mu+\nu}} c'_{\kappa_d,\rho_1}(w) e\left(-\frac{w\vartheta}{q^{\mu+\nu}} + \frac{wk'}{m'}\right) \right|^2,$$

ce qui, par le Grand Crible (Théorème A.2.4), les équations (2.17) et (2.18) et le fait que $M^2 \leq q^{2\mu} \leq q^{\mu+\nu}$, nous donne :

$$\begin{aligned}\left|S''_{I,2}(M,d)\right|^2 &\ll (\log q)(q^{\mu+\nu}+M^2/d^2)\sum_{w<q^{\mu+\nu}}|c'_{\kappa_d,\rho_1}(w)|^2\\ &\ll (\log q)(q^{\mu+\nu}+M^2/d^2)\#\widetilde{\mathcal{W}}_{\kappa_d}\\ &\ll (\log q)\, q^{2(\mu+\nu)-\rho+P(\mu+\nu+1)}.\end{aligned}$$

Enfin, par (2.19), nous concluons au fait que

$$S'_{I,2}(\vartheta') \ll (\log q)^{1/2}\sum_{1\leq d\leq M}\frac{1}{d}\,q^{-\rho/2+P(\mu+\nu+1)/2} \ll \mu(\log q)^{3/2}q^{-\rho/2+P(\mu+\nu+1)/2}. \quad (2.21)$$

Contrôlons à présent le terme principal $S'_{I,1}(\vartheta)$. Pour ce faire nous rappelons l'élément principal consituant cette somme :

$$G_{\kappa_d,1}(t) = \frac{1}{q^{\mu+\nu-\kappa_d}}\sum_{v<q^{\mu+\nu-\kappa_d}} f_P(vq^{\kappa_d})e\left(-\frac{vt}{q^{\mu+\nu-\kappa_d}}\right) \quad (2.22)$$

$$\cdot\,\frac{1}{q^{\kappa_d}}\sum_{u<q^{\kappa_d}} f_P^{(\kappa_d+\rho)}(u+vq^{\kappa_d})\overline{f_P^{(\kappa_d+\rho)}(vq^{\kappa_d})}e\left(-\frac{ut}{q^{\mu+\nu}}\right). \quad (2.23)$$

Le fait d'avoir introduit la fonction tronquée nous facilite la tâche : (2.23) est de ce fait moins liée à (2.22) (qui correspond à la transformée de Fourier discrète). Afin d'expliciter le lien entre ces équations, Mauduit et Rivat introduisent le reste de la division euclidienne de v par q^ρ de manière à rendre les deux lignes indépendantes. Nous ne pouvons pas le faire directement : notre définition de $f_P^{(\kappa+\rho)}$ ne correspond pas exactement à la fonction basée sur les restes modulo $q^{\kappa+\rho}$, mais à (2.4). Ainsi, si $w = v \bmod q^\rho$, on a clairement $T_q(w) \neq T_q(v)$ si $\rho < T_q(v)$.

Pour contourner ce problème on définit $l = T_q(v)$ et on pose $0 \leq u < q^{\kappa_d}$. Alors on a, toujours si $w = v \bmod q^\rho$:

$$\begin{cases} T_q(u+wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^{l-\rho}\rfloor) & = T_q(vq^{\kappa_d})\\ \epsilon_i((u+wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^{l-\rho}\rfloor) \bmod (q^{\kappa_d+\rho})) & = \epsilon_i(u+vq^{\kappa_d}),\end{cases}$$

et ce pour tout $0 \leq i < \kappa_d+\rho$.

En effet, si $\rho > l$, alors $w = v$ et $\lfloor q^{l-\rho}\rfloor = 0$ et donc $u+wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^{l-\rho}\rfloor = u+vq^{\kappa_d}$. Inversement, si $\rho \leq l$, comme $0 \leq w \leq q^\rho-1$ et $0 \leq u \leq q^{\kappa_d}-1$, nous avons $u+wq^{\kappa_d} \leq q^{\kappa_d}-1+q^{\kappa_d+\rho}-q^{\kappa_d} = q^{\kappa_d+\rho}-1$ et donc $T_q(u+wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^{l-\rho}\rfloor) = T_q(q^{l+\kappa_d}) = l+\kappa_d = T_q(vq^{\kappa_d}) = T_q(u+vq^{\kappa_d})$, et comme $q^{l+\kappa_d} \equiv 0 \bmod (q^{\rho+\kappa_d})$, on a la seconde ligne.

Ainsi si on isole les entiers selon leur taille, nous obtenons une indépendance entre (2.22) et (2.23). Plus précisément :

$$
\begin{aligned}
&G_{\kappa_d,1}(t)\\
&= \frac{1}{q^{\mu+\nu-\kappa_d}} \sum_{w<q^\rho} \sum_{0\le l<\mu+\nu-\kappa_d} \sum_{q^{l-1}\le v<q^l} f_P(vq^{\kappa_d}) e\left(-\frac{vt}{q^{\mu+\nu-\kappa_d}}\right) \frac{1}{q^\rho} \sum_{h<q^\rho} e\left(h\frac{v-w}{q^\rho}\right) \qquad (2.24)\\
&\quad \cdot \frac{1}{q^{\kappa_d}} \sum_{u<q^{\kappa_d}} f_P^{(\kappa_d+\rho)}(u+wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^{l-\rho}\rfloor)\overline{f_P^{(\kappa_d+\rho)}(wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^{l-\rho}\rfloor)} e\left(-\frac{ut}{q^{\mu+\nu}}\right).\\
&= \sum_{0\le l<\mu+\nu-\kappa_d} \sum_{h<q^\rho} \left[\frac{1}{q^{\kappa_d}} \sum_{u<q^{\kappa_d}} c_{\kappa_d,\rho,l}(u,h) e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right] \qquad (2.25)\\
&\qquad \cdot \left[\frac{1}{q^{\mu+\nu-\kappa_d}} \sum_{q^{l-1}\le v<q^l} f_P(vq^{\kappa_d}) e\left(-\frac{vt}{q^{\mu+\nu-\kappa_d}}+\frac{hv}{q^\rho}\right)\right], \qquad (2.26)
\end{aligned}
$$

avec

$$
\begin{aligned}
&c_{\kappa_d,\rho,l}(u,h)\\
&= \frac{1}{q^\rho} \sum_{w<q^\rho} f_P^{(\kappa_d+\rho)}(u+wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^l/q^\rho\rfloor)\overline{f_P^{(\kappa_d+\rho)}(wq^{\kappa_d}+q^{\kappa_d+\rho}\lfloor q^l/q^\rho\rfloor)} e\left(-\frac{hw}{q^\rho}\right).
\end{aligned}
$$

Il reste désormais à isoler définitivement (2.25) de (2.26). On remarque d'abord que dans (2.25), certains l doivent être traité à part. Si $P(l+\kappa_d) > l$ et n est tel que $T_q(n) = l$, alors $\epsilon_{i+P(l+\kappa_d)}(n)\dots\epsilon_i(n) = 0$ car $l = T_q(n)$ est l'indice du dernier chiffre non nul de n, et la somme composée des $e(\alpha a(n))$ est alors triviale.

Soit donc

$$M_d = \max\{0 \le l \le \mu+\nu-\kappa_d : P(l+\kappa_d) > l\}.$$

La borne triviale de M_d est $\mu+\nu-\kappa_d$, mais nous majorerons cette quantité plus finement. Nous séparons la somme dans (2.25) selon que $l \le M_d$ notée $G'_{\kappa_d,1}(t)$) ou que $l > M_d$ notée $G''_{\kappa_d,1}(t)$.

En majorant la seconde somme trivialement dans $G'_{\kappa_d,1}(t)$, nous avons

$$
\begin{aligned}
|G'_{\kappa_d,1}(t)| &\le \sum_{0\le l\le M_d} q^{l-(\mu+\nu-\kappa_d)} \sum_{h<q^\rho} \frac{1}{q^{\kappa_d}} \left| \sum_{u<q^{\kappa_d}} c_{\kappa_d,\rho,l}(u,h) e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right|\\
&\ll q^{M_d-(\mu+\nu)} \sum_{0\le l\le M_d} \sum_{h<q^\rho} \left| \sum_{u<q^{\kappa_d}} c_{\kappa_d,\rho,l}(u,h) e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right|,
\end{aligned}
$$

mais par le Lemme 2.4.1 , nous obtenons

$$\begin{aligned}
&\sum_{1\le d\le M}\frac{1}{d}\sum_{\frac{M}{qd}\le m'<\frac{M}{d}}\frac{1}{m'}\sum_{\substack{0\le k'<m'\\(k',m')=1}}\left|G'_{\kappa_d,1}\left(\vartheta'-\frac{k}{m}q^{\mu+\nu}\right)\right| \qquad (2.27)\\
&\quad\ll\sum_{1\le d\le M}\frac{1}{d}\sum_{\frac{M}{qd}\le m'<\frac{M}{d}}\frac{1}{m'}q^{M_d-(\mu+\nu)}\\
&\qquad\cdot\sum_{0\le l\le M_d}\sum_{\substack{0\le k'<m'\\(k',m')=1}}\sum_{h<q^\rho}\left|\sum_{u<q^{\kappa_d}}c_{\kappa_d,\rho,l}(u,h)e\left(-\frac{u(\vartheta'-\frac{k}{m}q^{\mu+\nu})}{q^{\mu+\nu}}\right)\right|\\
&\quad\ll\frac{\log q}{q^{\mu+\nu}}\sum_{1\le d\le M}\frac{1}{d}\,q^{M_d+\kappa_d+\rho/2}\,M_d.
\end{aligned}$$

Cependant, comme la fonction P est croissante et que, par (2.8) et (2.13), $1\le\kappa_d\le\kappa_1\le\frac{2}{3}(\mu+\nu)$, nous avons

$$\begin{aligned}
M_d&=\max\{0\le l\le\mu+\nu-\kappa_d : P(l+\kappa_d)>l\}\\
&\le\max\left\{0\le l\le\mu+\nu-\kappa_d : P\left(l+\frac{2}{3}(\mu+\nu)\right)>l\right\}.
\end{aligned}$$

Supposons maintenant que $P(x)\le x/10$ (les prochaines estimations marchent pour $P(x)\le x\left(\frac{1}{3}-\epsilon\right)$ pour tout $0<\epsilon<\frac{1}{3}$, mais le choix final de ρ devra Ãªtre alors très fin et de toute manière d'autres conditions plus restrictives sur la taille de P seront prises), ceci implique

$$\frac{1}{10}\left(l+\frac{2}{3}(\mu+\nu)\right)>l,\ \text{c'est-à-dire}: l<\frac{2}{27}(\mu+\nu),$$

et donc $M_d\le\frac{2}{27}(\mu+\nu)$. Comme $\kappa_d\le\frac{2}{3}(\mu+\nu)$, nous obtenons quel que soit d :

$$M_d+\kappa_d\le\frac{20}{27}(\mu+\nu),$$

et donc

$$\sum_{1\le d\le M}\frac{1}{d}\sum_{\frac{M}{qd}\le m'<\frac{M}{d}}\frac{1}{m'}\sum_{\substack{0\le k'<m'\\(k',m')=1}}\left|G'_{\kappa_d,1}\left(\vartheta'-\frac{k}{m}q^{\mu+\nu}\right)\right|\ll(\mu+\nu)^2(\log q)^2q^{-\frac{7}{27}(\mu+\nu)+\rho/2}. \qquad (2.28)$$

À présent contrôlons le terme restant. Il nous fournira la contribution principale de notre estimation. Rappelons que la somme à contrôler est essentiellement liée à

$$\begin{aligned}
G''_{\kappa_d,1}(t)=&\sum_{M_d<l\le\mu+\nu-\kappa_d}\sum_{h<q^\rho}\left[\frac{1}{q^{\kappa_d}}\sum_{u<q^{\kappa_d}}c_{\kappa_d,\rho,l}(u,h)e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right]\\
&\cdot\left[\frac{1}{q^{\mu+\nu-\kappa_d}}\sum_{q^{l-1}\le v<q^l}f_P(vq^{\kappa_d})e\left(-\frac{vt}{q^{\mu+\nu-\kappa_d}}+\frac{hv}{q^\rho}\right)\right].
\end{aligned}$$

Comme $l > M_d$, nous pouvons à présent utiliser le Lemme 2.4.3 pour la seconde ligne, ce qui nous donne :

$$|G''_{\kappa_d,1}(t)| \leq \sum_{M_d<l\leq\mu+\nu-\kappa_d} q^{\gamma(l,\kappa_d)-(\mu+\nu-\kappa_d)} \sum_{h<q^\rho} \frac{1}{q^{\kappa_d}} \left| \sum_{u<q^{\kappa_d}} c_{\kappa_d,\rho,l}(u,h) e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right|.$$

Soit à présent $h(l,k) = \gamma(l,k)/l$. En nous rappelant la Proposition 2.4.4, et en remarquant que quelque soit k, l'application $l \mapsto lh(k,0)$ est croissante (quitte à supposer $P(0) \geq 4$), nous avons :

$$lh(\mu+\nu-\kappa_d,\kappa_d) - (\mu+\nu-\kappa_d) = lh(\mu+\nu,0) - (\mu+\nu-\kappa_d)$$

mais

$$\begin{aligned} m\,(1-h(k,0)) &= m\left(1 - \frac{\log\left(q^{P(k)} - 8\sin\left(\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(k)\log q}\right) \\ &= \gamma_P(m,k). \end{aligned}$$

En effet, comme $l \leq \mu+\nu-\kappa_d$, nous avons $lh(\mu+\nu,0) - (\mu+\nu-\kappa_d) \leq (\mu+\nu-\kappa_d)(h(\mu+\nu,0)-1)$, et donc :

$$|G''_{\kappa_d,1}(t)| \leq q^{-\gamma_P(\mu+\nu-\kappa_d,\,\mu+\nu)} \sum_{M_d<l\leq\mu+\nu-\kappa_d} \sum_{h<q^\rho} \frac{1}{q^{\kappa_d}} \left| \sum_{u<q^{\kappa_d}} c_{\kappa_d,\rho,l}(u,h) e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right|.$$

L'application $m \mapsto \gamma_P(m,k)$ est croissante (linéaire de coefficient directeur strictement positif), ainsi par le Lemme 2.4.1, nous obtenons

$$\begin{aligned} &\sum_{1\leq d\leq M} \frac{1}{d} \sum_{\frac{M}{qd}\leq m'<\frac{M}{d}} \frac{1}{m'} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \left|G''_{\kappa_d,1}\left(\vartheta' - \frac{k}{m}q^{\mu+\nu}\right)\right| \qquad (2.29) \\ &\quad\leq \sum_{1\leq d\leq M} \frac{q^{-\gamma_P(\mu+\nu-\kappa_d,\,\mu+\nu)}}{dq^{\kappa_d}} \\ &\qquad\cdot \sum_{M_d<l\leq\mu+\nu-\kappa_d} \sum_{\frac{M}{qd}\leq m'<\frac{M}{d}} \frac{1}{m'} \sum_{\substack{0\leq k'<m' \\ (k',m')=1}} \sum_{h<q^\rho} \left| \sum_{u<q^{\kappa_d}} c_{\kappa_d,\rho,l}(u,h) e\left(-\frac{ut}{q^{\mu+\nu}}\right)\right| \\ &\quad\ll q^{-\gamma_P(\frac{1}{3}(\mu+\nu),\,\mu+\nu)} \sum_{1\leq d\leq M} \frac{q^{\rho/2}}{d}(\mu+\nu)\log q, \end{aligned}$$

ce qui nous donne

$$(2.29) \ll q^{\rho/2-\gamma_P(\frac{1}{3}(\mu+\nu),\,\mu+\nu)}(\mu+\nu)^2(\log q)^2. \qquad (2.30)$$

Nous avons donc par les équations (2.14), (2.21), (2.28) et (2.30) :

$$\begin{aligned} S'_I(\vartheta) \ll& \mu(\log q)^{3/2} q^{-\rho/2+P(\mu+\nu+1)/2} \\ &+ (\mu+\nu)^2(\log q)^2 q^{-\frac{7}{27}(\mu+\nu)+\rho/2} \\ &+ q^{\rho/2-\gamma_P(\frac{1}{3}(\mu+\nu),\,\mu+\nu)}(\mu+\nu)^2(\log q)^2, \end{aligned}$$

et donc par (2.10) :

$$\begin{aligned}S_I(\vartheta) \ll &(\log q^{\mu+\nu})\Big(\mu(\log q)^{3/2}q^{\mu+\nu-\rho/2+P(\mu+\nu+1)/2}\\ &+(\mu+\nu)^2(\log q)^2q^{\frac{20}{27}(\mu+\nu)+\rho/2}\\ &+q^{\mu+\nu+\rho/2-\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)}(\mu+\nu)^2(\log q)^2\Big).\end{aligned}$$

Nous choisissons $\rho = \frac{P(\mu+\nu+1)}{2} + \gamma_P(\frac{1}{3}(\mu+\nu),\, \mu+\nu)$, et par (2.9) nous trouvons que (2.15) est vérifié. En effet, par (2.9) :

$$P(\mu+\nu+1) \leq \gamma_P\left(\frac{1}{3}(\mu+\nu), \mu+\nu\right) \leq \rho.$$

De plus :

$$\begin{aligned}S_I(\vartheta) &\ll q^{\mu+\nu}(\mu+\nu)^3(\log q)^3\left(q^{\frac{P(\mu+\nu+1)}{4}-\frac{1}{2}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)} + q^{\frac{3}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)-\frac{7}{27}(\mu+\nu)}\right)\\ &\ll q^{\mu+\nu}(\mu+\nu)^3(\log q)^3\left(q^{-\frac{1}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)} + q^{\frac{3}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)-\frac{7}{27}(\mu+\nu)}\right)\end{aligned}$$

Cependant, par la Remarque 2.2.1, $\gamma_P(\frac{1}{3}(\mu+\nu),\, \mu+\nu) \leq \frac{\mu+\nu}{6}$ et ainsi, comme $\rho \leq \frac{3}{2}\gamma_P(\frac{1}{3}(\mu+\nu),\, \mu+\nu)$, (2.16) est également vérifiée. De plus

$$\frac{3}{4}\gamma_P\left(\frac{1}{3}(\mu+\nu),\, \mu+\nu\right) - \frac{7}{27}(\mu+\nu) \leq (\mu+\nu)\left(\frac{1}{8}-\frac{7}{27}\right) = -(\mu+\nu)\frac{29}{216}$$

et

$$-\frac{1}{4}\gamma_P\left(\frac{1}{3}(\mu+\nu),\, \mu+\nu\right) \geq -\frac{\mu+\nu}{24} \geq -(\mu+\nu)\frac{29}{216},$$

ainsi finalement

$$S_I(\vartheta) \ll (\mu+\nu)^3(\log q)^3 q^{\mu+\nu-\frac{1}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)},$$

ce qui finit la preuve. □

2.6 Travail préparatoire pour les sommes de type II

De même que pour les sommes de type I, le traitement des sommes de type II nécessite un certain nombre de résultats préliminaires. La stratégie pour contrôler les sommes de type II consiste à introduire une fonction doublement tronquée et à exploiter sa structure pour mettre en exergue dans nos estimations la propriété de Fourier de $e(\alpha a_P(\cdot))$. Les Lemmes 2.6.4, 2.6.6 et 2.6.7 permettent d'introduire la fonction doublement tronquée. Ces lemmes sont des redites de résultats se trouvant dans [MR15]. Le Lemme 2.6.10 nous permet de faire apparaître la propriété de Fourier dans l'estimation des sommes de type II, pour conclure, dans la Partie 2.7, nous serons amenés à évaluer des sommes d'exponentielles pondérées de deux différents types. Le Lemme 2.6.1 transforme cette pondération en une somme d'exponentielle classique. Les Lemmes 2.6.2 et 2.6.3 sont les estimations des sommes d'exponentielles que nous serons amenés à regarder par la suite.

Lemme 2.6.1. *Soit f une fonction réelle, $(b_n)_{n\geq 0}$ une suite réelle, μ et q deux entiers supérieurs ou égaux à 2, $q^{\mu-1} \leq M < q^{\mu}$ et $I_1 \subseteq [M/q, M[$ un intervalle. Alors*

$$\left|\sum_{m\in I_1} e(f(m))b_m\right| \ll \max\left(|b_{\max I_1+1}|\left|\sum_{m\in I_1} e(f(m))\right|, \sup_{M/q<K\leq M}\left|\sum_{l\in I_1\cap[M/q,K)} e(f(l))\right| \sum_{m\in I_1}|b_{m+1}-b_m|\right).$$

Démonstration. Par sommation d'Abel :

$$\begin{aligned}
\left|\sum_{m\in I_1} e(f(m))b_m\right| &= \left|b_{\max I_1+1}\sum_{m\in I_1} e(f(m)) - \sum_{m\in I_1}(b_{m+1}-b_m)\sum_{l\in I_1\cap[M/q,m]} e(f(l))\right| \\
&\leq \left|b_{\max I_1+1}\sum_{m\in I_1} e(f(m))\right| + \left|\sum_{m\in I_1}(b_{m+1}-b_m)\sum_{l\in I_1\cap[M/q,m]} e(f(l))\right| \\
&\leq \left|b_{\max I_1+1}\sum_{m\in I_1} e(f(m))\right| + \sum_{m\in I_1}|b_{m+1}-b_m|\left|\sum_{l\in I_1\cap[M/q,m]} e(f(l))\right| \\
&\leq \left|b_{\max I_1+1}\sum_{m\in I_1} e(f(m))\right| \\
&\quad + \sup_{M/q<K\leq M}\left\{\left|\sum_{l\in I_1\cap[M/q,K)} e(f(l))\right|\right\}\sum_{m\in I_1}|b_{m+1}-b_m|.
\end{aligned}$$

□

Lemme 2.6.2. *Soient μ, ν, M, N, q des entiers tels que $2\mu \leq \nu$, $q^{\mu-1} \leq M < q^{\mu}$ et $q^{\nu-1} \leq N < q^{\nu}$. Soient $k \in \{\mu+\nu-4, \ldots, \mu+\nu-1\}$ et $M/q \leq m < M$ des entiers. Définissons*

$$I(k,m) = \left\{\frac{N}{q} \leq n < N : \frac{q^k}{m} \leq n < \frac{q^{k+1}}{m}\right\},$$

alors, si $I_1 \subseteq [M/q, M[$ est un intervalle, nous avons :

$$\left|\sum_{m\in I_1} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| \ll q^{\nu}\min\left(q^{\mu}, \left|\sin\pi\frac{h_1 r}{q^{\mu_2}}\right|^{-1}\right).$$

Démonstration. Commençons par remarquer que

$$I(k,m) = \begin{cases} \left[\frac{N}{q}, \frac{q^{k+1}}{m}\right[\cap \mathbb{N} & \text{si} \quad m \geq \frac{q^{k+1}}{N} \\ \left[\frac{q^k}{m}, N\right[\cap \mathbb{N} & \text{si} \quad m < \frac{q^{k+1}}{N}, \end{cases}$$

et donc

$$\#I(k,m) = \begin{cases} 0 & \text{si} \quad m \leq \dfrac{q^k}{N} \quad \text{ou} \quad m \geq \dfrac{q^{k+2}}{N} \\ \left\lceil \dfrac{q^{k+1}}{m} \right\rceil - \left\lceil \dfrac{N}{q} \right\rceil & \text{si} \quad \dfrac{q^{k+1}}{N} \leq m < \dfrac{q^{k+2}}{N} \\ N - \left\lfloor \dfrac{q^k}{m} \right\rfloor & \text{si} \quad \dfrac{q^k}{N} \leq m < \dfrac{q^{k+1}}{N} \end{cases}$$

Nous allons d'abord effectuer la preuve du lemme dans le cas $(M,N) = (q^{\mu-1}, q^{\nu-1})$ qui est un cas particulier et qui permet de bien comprendre la démonstration : dans le cas général, seules quelques difficultés techniques supplémentaires interviennent.

Puisque $(M,N) = (q^{\mu-1}, q^{\nu-1})$, nous avons $q^{\mu-2} \leq m < q^{\mu-1}$ et $q^{\nu-2} \leq n < q^{\nu-1}$, de sorte que $q^{\mu+\nu-4} \leq mn < q^{\mu+\nu-2}$.

CommenÃ§ons par une simple étude de cas. Si $k = \mu+\nu-4$, alors

$$\frac{q^{k+1}}{N} = q^{\mu-2} \leq m < q^{\mu-1} = \frac{q^{k+2}}{N}$$

et $\lceil N/q \rceil = q^{\nu-2}$. De plus si $k = \mu+\nu-3$, nous avons

$$\frac{q^k}{N} = q^{\mu-2} \leq m < \frac{q^{k+1}}{N},$$

et donc :

$$\#I(\mu+\nu-4, m) = \left\lceil \frac{q^{\mu+\nu-3}}{m} \right\rceil - q^{\nu-2} \tag{2.31}$$

et

$$\#I(\mu+\nu-3, m) = \quad q^{\nu-1} - \left\lfloor \frac{q^{\mu+\nu-3}}{m} \right\rfloor. \tag{2.32}$$

Pour $k \geq \mu+\nu-2$, $\#I(k,m)$ est nul, car $(M,N) = (q^{\mu-1}, q^{\nu-1})$.

La technique de majoration étant quasi identique, nous nous contenterons de majorer pour $\#I(\mu+\nu-3,m)$. Nous appliquons le Lemme 2.6.1 pour pouvoir dire

$$\begin{aligned} &\left| \sum_{m \in I_1} e\left(m\frac{h_1 r}{q^{\mu_2}}\right) \left| q^{\nu-1} - \left\lfloor \frac{q^{\mu+\nu-3}}{m} \right\rfloor \right| \right| \\ &\ll \max\left(\left| q^{\nu-1} - \left\lfloor \frac{q^{\mu+\nu-3}}{\max I_1 + 1} \right\rfloor \right| \left| \sum_{m \in I_1} e\left(m\frac{h_1 r}{q^{\mu_2}}\right) \right|, \right. \\ &\qquad \left. \sup_{q^{\mu-2} < K \leq q^{\mu-1}} \left| \sum_{m \in I_1 \cap [q^{\mu-2}, K)} e\left(m\frac{h_1 r}{q^{\mu_2}}\right) \right| \sum_{m \in I_1} \left| \left\lfloor \frac{q^{\mu+\nu-3}}{m+1} \right\rfloor - \left\lfloor \frac{q^{\mu+\nu-3}}{m} \right\rfloor \right| \right). \end{aligned} \tag{2.33}$$

Majorons d'abord le premier terme du max. Comme $I_1 \subseteq [q^{\mu-2}, q^{\mu-1}[$, nous avons

$$\left| q^{\nu-1} - \left\lfloor \frac{q^{\mu+\nu-3}}{\max I_1 + 1} \right\rfloor \right| \ll q^{\nu}$$

et comme $\left|\sum_{m\in I_1} e(\alpha m)\right| \leq \min\left(|I_1|, \frac{1}{|\sin \pi\alpha|}\right)$, nous avons la majoration désirée car $|I_1| \ll q^\mu$.

Pour le second terme, on trouve que

$$\sum_{m\in I_1} \left|\left\lfloor \frac{q^{\mu+\nu-3}}{m+1}\right\rfloor - \left\lfloor \frac{q^{\mu+\nu-3}}{m}\right\rfloor\right| = \sum_{m\in I_1} \left(\left\lfloor \frac{q^{\mu+\nu-3}}{m}\right\rfloor - \left\lfloor \frac{q^{\mu+\nu-3}}{m+1}\right\rfloor\right)$$

qui est une somme télescopique, donc

$$\sum_{m\in I_1} \left|\left\lfloor \frac{q^{\mu+\nu-3}}{m+1}\right\rfloor - \left\lfloor \frac{q^{\mu+\nu-3}}{m}\right\rfloor\right| \leq \left\lfloor \frac{q^{\mu+\nu-3}}{\min I_1}\right\rfloor \ll q^\nu$$

car $I_1 \subseteq [q^{\mu-2}, q^{\mu-1}[$ et nous concluons en utilisant le fait que

$$\left|\sum_{m\in I} e(\alpha m)\right| \leq \min\left(|I|, \frac{1}{|\sin \pi\alpha|}\right).$$

Supposons à présent $(M, N) \neq (q^{\mu-1}, q^{\nu-1})$.Nous avons

$$m \geq \frac{q^{k+2}}{N} \Rightarrow q^{k+2} \leq MN < q^{\mu+\nu} \Rightarrow k \leq \mu+\nu-3$$

et

$$m \leq \frac{q^k}{N} \Rightarrow q^{k+1} \geq MN > q^{\mu+\nu-2} \Rightarrow k \geq \mu+\nu-2.$$

Enfin, nous avons

$$N \leq \frac{q^k}{m} \Leftrightarrow m \leq \frac{q^k}{N} \qquad \text{et} \qquad \frac{q^{k+1}}{m} \leq \frac{N}{q} \Leftrightarrow m \geq \frac{q^{k+2}}{N}.$$

Comme $\#I(k,m) = 0$ si $m \leq q^k/N$ ou si $m \geq q^{k+2}/N$, nous avons :

$$\left|\sum_{m\in I_1} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| = \left|\sum_{m\in I_1\cap\left[\frac{M}{q}, \frac{q^{k+2}}{N}\right[} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| \tag{2.34}$$

si $k \in \{\mu+\nu-4, \mu+\nu-3\}$ et

$$\left|\sum_{m\in I_1} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| = \left|\sum_{m\in I_1\cap\left]\frac{q^k}{N}, M\right[} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right|$$

si $k \in \{\mu+\nu-2, \mu+\nu-1\}$. Si m vérifie $m < q^{k+1}/N < m+1$, donc tel que l'expression donnant $\#I(k,m)$ ne soit pas de la même forme que celle donnant $\#I(k,m+1)$, alors $m = \left\lfloor q^{k+1}/N\right\rfloor$.

Soit $k \in \{\mu+\nu-2, \mu+\nu-1\}$ fixé, si on note J_k l'intervalle de sommation de (2.34), nous avons alors en notant $J'_k = J_k \cap \left]\frac{M}{q}, \frac{q^{k+1}}{N} - 1\right[$ et $J''_k = J_k \cap \left]\frac{q^{k+1}}{N}, M\right[$:

$$\begin{aligned}\left|\sum_{m\in J_k} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| \leq &\left|\sum_{m\in J'_k} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| \\ &+ \left|\sum_{m\in J''_k} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| \\ &+ \#I\left(k, \left\lfloor\frac{q^{k+1}}{N}\right\rfloor\right).\end{aligned}$$

Maintenant $\#I\left(k, \left\lfloor\frac{q^{k+1}}{N}\right\rfloor\right) \leq \#\{N/q \leq n < N\} \ll q^\nu$, et la technique utilisée pour contrôler (2.33) s'applique pour J'_k et J''_k, ce qui nous fournit le résultat dans le cas $k \in \{\mu+\nu-2, \mu+\nu-1\}$. Le cas $k \in \{\mu+\nu-4, \mu+\nu-3\}$ se traite de la même manière.

Nous avons donc démontré

$$\left|\sum_{m\in I_1} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\#I(k,m)\right| \ll q^\nu \min\left(q^\mu, \left|\sin\pi\frac{h_1 r}{q^{\mu_2}}\right|^{-1}\right),$$

ce qui est le résultat annoncé.

□

Lemme 2.6.3. *Soient μ, ν des entiers tels que $\frac{1}{4}(\mu+\nu) \leq \mu \leq \nu \leq \frac{3}{4}(\mu+\nu)$. Soient M, m, k et $I(k,m)$ définis dans le Lemme 2.6.2. Alors si $h, h_1, \mu_0, \mu_1, \mu_2, s$ sont des entiers tels que $\mu_0 < \mu_1 < \mu_2$ et $hq^{\mu_1-\mu_2}s \notin \mathbb{Z}$, nous avons pour tout $I_1 \subseteq [q^{\mu-2}, q^\mu[$:*

$$\left|\sum_{m\in I_1} e\left(\frac{h_1 rm}{q^{\mu_2}}\right)\sum_{n\in I(k,m)} e(hsnq^{\mu_1-\mu_2})\right| \ll \left(shq^{3(\mu_2-\mu_1)}\right)^{1/2} q^{\frac{7}{8}(\mu+\nu)}$$

Démonstration. Soient a_m et b_m des entiers tels que $I(k,m) = [a_m, b_m[$ (les entiers dépendent de k, mais pour ne pas alourdir les notations nous ne le marquons pas). Comme $hq^{\mu_1-\mu_2}s \notin \mathbb{Z}$, nous pouvons écrire :

$$\begin{aligned}\sum_{n\in I(k,m)} e(hq^{\mu_1-\mu_2}sn) &= \frac{e(hq^{\mu_1-\mu_2}sa_m) - e(hq^{\mu_1-\mu_2}sb_m)}{1 - e(hq^{\mu_1-\mu_2}s)} \\ &= e\left(hq^{\mu_1-\mu_2}s\frac{a_m+b_m}{2}\right)\frac{\sin\left(\pi hq^{\mu_1-\mu_2}s(b_m-a_m)\right)}{\sin\left(\pi hq^{\mu_1-\mu_2}s\right)}\end{aligned}$$

donc

$$\begin{aligned}&\left|\sum_{m\in I_1} e\left(\frac{h_1 rm}{q^{\mu_1}}\right)\sum_{n\in I(k,m)} e(hq^{\mu_1-\mu_2}sn)\right| \\ &\ll \frac{1}{|\sin(\pi hq^{\mu_1-\mu_2}s)|}\left|\sum_{m\in I_1} e\left(\frac{h_1 rm}{q^{\mu_1}}\right) e\left(hq^{\mu_1-\mu_2}s\frac{a_m+b_m}{2}\right)\sin\left(\pi hq^{\mu_1-\mu_2}s(b_m-a_m)\right)\right|.\end{aligned}$$

Rappelons que $|\sin(\pi x)| \geq 2\|x\|_{\mathbb{Z}}$. Comme $q^{\mu_1-\mu_2}hs \notin \mathbb{Z}$, nous pouvons écrire $hs = kq^{\mu_2-\mu_1} + l$ avec $1 \leq l \leq q^{\mu_2-\mu_1} - 1$, et donc $\|q^{\mu_1-\mu_2}hs\|_{\mathbb{Z}} \geq q^{\mu_1-\mu_2}$. Ainsi

$$\begin{aligned}\left|\sum_{m\in I_1} e\left(\frac{h_1rm}{q^{\mu_1}}\right)\sum_{n\in I(k,m)} e(hq^{\mu_1-\mu_2}sn)\right| \\ \ll q^{\mu_2-\mu_1}\left|\sum_{m\in I_1} e\left(\frac{h_1rm}{q^{\mu_1}}\right) e\left(hq^{\mu_1-\mu_2}s\frac{a_m+b_m}{2}\right)\sin\left(\pi hq^{\mu_1-\mu_2}s(b_m-a_m)\right)\right|.\end{aligned}$$

Quitte à découper l'intervalle comme dans la démonstration du Lemme 2.6.2, nous pouvons nous ramener à estimer

$$\sum_{m\in J_1} e\left(\frac{h_1rm}{q^{\mu_1}} + hq^{\mu_1-\mu_2}s\frac{q^k}{m}\right)\sin\left(\pi hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right),$$

avec $J_1 \subseteq I_1 \subseteq [q^{\mu-2}, q^{\mu})$.

Nous utilisons alors le Lemme 2.6.1 pour dire

$$\begin{aligned}&\left|\sum_{m\in J_1} e\left(\frac{h_1rm}{q^{\mu_1}} + hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\sin\left(\pi hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\right| \\ &\ll \max\left(\left|\sum_{m\in J_1} e\left(\frac{h_1rm}{q^{\mu_1}} + hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\right|,\right. \\ &\qquad \sup_{M/q<K\leq M}\left|\sum_{l\in J_1\cap[M/q,K)} e\left(\frac{h_1rm}{q^{\mu_1}} + hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\right| \\ &\qquad \left.\sum_{m\in I_1}\left|\sin\left(\pi hq^{\mu_1-\mu_2}s\frac{q^k}{m+1}\right) - \sin\left(\pi hq^{\mu_1-\mu_2}s\frac{q^k}{m}\right)\right|\right).\end{aligned}$$

La fonction

$$f(x) := \frac{h_1r}{q^{\mu_2}}x + \frac{1}{2x}hsq^{\mu_1-\mu_2+k}$$

est $\mathcal{C}^\infty$ sur $[q^{\mu-2}, q^{\mu})$ et de plus sa dérivée seconde vérifie

$$\lambda := shq^{\mu_1-\mu_2+k-3\mu} \leq f^{(2)}(x) = \frac{shq^{\mu_1-\mu_2+k}}{x^3} \leq shq^{\mu_1-\mu_2+k-3\mu+3} = \lambda q^3,$$

nous pouvons alors utiliser le Théorème A.2.8 pour obtenir :

$$\left|\sum_{l\in J_1\cap[q^{\mu-1},K)} e\left(\frac{h_1r}{q^{\mu_1}}l + \frac{1}{2l}hsq^{\mu_1-\mu_2+k}\right)\right| \ll q^\mu\left(shq^{\mu_1-\mu_2+k-3\mu}\right)^{1/2} + \left(shq^{\mu_1-\mu_2+k-3\mu}\right)^{-1/2}.$$

En exploitant le fait que $\mu+\nu-4 \leq k \leq \mu+\nu-1$ dans l'estimation précédente, nous obtenons :

$$\begin{aligned}\left|\sum_{l\in J_1\cap[q^{\mu-1},K)} e\left(\frac{h_1r}{q^{\mu_1}}l + \frac{1}{2l}hsq^{\mu_1-\mu_2+k'}\right)\right| &\ll q^\mu\left(shq^{\mu_1-\mu_2+\nu-2\mu}\right)^{1/2} + \left(shq^{\mu_1-\mu_2+\nu-2\mu}\right)^{-1/2} \\ &\ll \left(shq^{\mu_1-\mu_2}\right)^{1/2}q^{\nu/2} + \left(shq^{\mu_1-\mu_2}\right)^{-1/2}q^{\mu-\nu/2}.\end{aligned}$$

En majorant trivialement le terme de la somme sur les sinus, et en utilisant $J_1 \subseteq I_1 \subseteq [q^{\mu-2}, q^\mu)$, nous obtenons la majoration :

$$\begin{aligned}\left|\sum_{m\in J_1} e\left(\frac{h_1 rm}{q^{\mu_1}} + hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\sin\left(\pi hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\right| \\ \ll \left(shq^{\mu_2-\mu_1}\right)^{1/2} q^{\mu+\nu/2} + \left(shq^{\mu_1-\mu_2}\right)^{-1/2} q^{2\mu-\nu/2}.\end{aligned}$$

Cependant, nous avons $\frac{1}{4}(\mu+\nu) \leq \mu \leq \nu \leq \frac{3}{4}(\mu+\nu)$, ce qui donne

$$2\mu - \frac{\nu}{2} \leq \mu + \nu - \frac{\nu}{2} \leq (\mu+\nu) - \frac{\mu+\nu}{8} = \frac{7}{8}(\mu+\nu)$$

ainsi que

$$\mu + \frac{\nu}{2} = \frac{\mu+\nu}{2} + \frac{\mu}{2} \leq \frac{\mu+\nu}{2} + \frac{3(\mu+\nu)}{8} = \frac{7}{8}(\mu+\nu)$$

ce qui nous donne

$$\left|\sum_{m\in J_1} e\left(\frac{h_1 rm}{q^{\mu_1}} + hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\sin\left(\pi hq^{\mu_1-\mu_2}s\frac{q^k}{2m}\right)\right| \ll \left(shq^{\mu_2-\mu_1}\right)^{1/2} q^{\frac{7}{8}(\mu+\nu)},$$

et le lemme est démontré. □

Le lemme ci dessous est le lemme crucial du présent chapitre. Il dit en quelque sorte que si on ne perturbe pas trop des entiers m et n en m' et n', le produit $m'n'$ aura la mÃªme taille que le produit mn. Ceci nous permet d'introduire dans S_{II} la notion essentielle de fonction doublement tronquée. Les explications de la nécessité d'un tel résultat se trouvent dans la Partie 2.7.

Lemme 2.6.4. *Soient μ, ν, ρ des entiers tels que $2\rho \leq \nu - 1$. Soient $q^{\mu-2} \leq m < q^\mu$ et $q^{\nu-2} \leq n < q^\nu$ des entiers. Posons $m' = m + q^{\mu-\rho}$ et $n' = n + q^\rho$.*

Alors :

$$\#\{q^{\mu-1} \leq m < q^\mu, q^{\nu-1} \leq n < q^\nu : T_q(mn) \neq T_q(m'n')\} \ll \log(q^{\mu+\nu})q^{\mu+\nu-\rho}.$$

Démonstration. Observons que $m'n' = mn + mq^\rho + nq^{\mu-\rho} + q^\mu$. Par ailleurs

$$\begin{aligned}mq^\rho + nq^{\mu-\rho} + q^\mu &< q^{\mu+\rho} + nq^{\mu-\rho} + q^\mu \\ &\leq q^{\mu+\rho+1} + nq^{\mu-\rho} \\ &\leq q^{\mu+\nu+1-\rho}.\end{aligned}$$

Comme $mn \geq q^{\mu+\nu-4}$, pour que la taille de mn soit perturbée par l'ajout d'un terme inférieur à $q^{\mu+\nu+1-\rho}$, il faut que les chiffres de mn d'indice entre $\mu+\nu+1-\rho$ et $\mu+\nu-4$ soient égaux à $q-1$. Soit $\mathcal{M}$ le nombre des (m,n) tels que $T_q(mn) \neq T_q(m'n')$. Si

$$\chi(a) = \begin{cases} 1 & \text{si} \quad \epsilon_i(a) = q-1, \quad \mu+\nu+1-\rho \leq i \leq \mu+\nu-4 \\ 0 & \text{sinon,}\end{cases}$$

alors

$$\begin{aligned}\mathcal{M} &\leq \sum_{q^{\mu+\nu+1-\rho}\leq a<q^{\mu+\nu}} \tau(a)\chi(a)\\ &\leq \sum_{b<q^{\mu+\nu+1-\rho}} \sum_{c<q^4} \tau(b+(q-1)q^{\mu+\nu+1-\rho}+\ldots+(q-1)q^{\mu+\nu-4}+q^{\mu+\nu-3}c).\end{aligned}$$

Nous pouvons alors appliquer le Lemme A.2.9, avec $x = q^{\mu+\mu+1-\rho} - 1 + (q-1)q^{\mu+\nu+1-\rho} + \ldots + (q-1)q^{\mu+\nu-2} + q^{\mu+\nu-1}c \leq q^{\mu+\nu+1}$ et $y = q^{\mu+\nu+1-\rho}$ pour pouvoir dire

$$\mathcal{M} \ll q^{\mu+\nu-\rho}\log q^{\mu+\nu}.$$

□

Le Lemme 2.6.6 fait la transition entre la fonction f_P et la fonction tronquée $f_P^{(\mu_2)}$. Pour le démontrer, nous avons besoin d'un résultat intermédiaire, qui correspond à [MR15, Lemma 7] :

Lemme 2.6.5. *Soient $\mu \geq 1, \nu \geq 1, \mu' \geq 1$ des entiers avec $\mu' \leq \mu+\nu$. Pour $\mathcal{B} \subset \{0,\ldots,q^{\mu+\nu-\mu'}-1\}$, le nombre $\mathcal{N}$ de couples $(m,n) \in \{q^{\mu-2},\ldots,q^{\mu}-1\} \times \{q^{\nu-2},\ldots,q^{\nu}-1\}$ tels que $mn = a + q^{\mu'}b$ avec $0 \leq a < q^{\mu'}$ et $b \in \mathcal{B}$ satisfait à*

$$\mathcal{N} \leq (q^{\mu'}\log q + q^{\mu} + q^{\mu'-\mu+1})\#\mathcal{B}.$$

Démonstration. Pour tout $m \in \{q^{\mu-1},\ldots,q^{\mu}-1\}$, le nombre $\mathcal{N}_m$ des entiers n tels que $mn = a + q^{\mu'}b$ avec $0 \leq a < q^{\mu'}$ et $b \in \mathcal{B}$ satisfait à

$$\mathcal{N}_m \leq \sum_{b\in\mathcal{B}} \#\{a \in \mathbb{N} : 0 \leq a < q^{\mu'}, a + q^{\mu'}b \equiv 0 \bmod m\}.$$

Ceci donne

$$\mathcal{N}_m \leq \sum_{b\in\mathcal{B}} \left(1 + \frac{q^{\mu'}}{m}\right) = \left(1 + \frac{q^{\mu'}}{m}\right)\#\mathcal{B}.$$

Il suit que

$$\mathcal{N} = \sum_{q^{\mu-2}\leq m<q^{\mu}} \mathcal{N}_m \leq \sum_{q^{\mu-2}\leq m<q^{\mu}} \left(1 + \frac{q^{\mu'}}{m}\right)\#\mathcal{B}$$

et donc

$$\mathcal{N} \leq (q^{\mu} - q^{\mu-2})\#\mathcal{B} + q^{\mu'}\left(\frac{1}{q^{\mu-2}} + \int_{q^{\mu-2}}^{q^{\mu}} \frac{dt}{\log t}\right)\#\mathcal{B}$$

et le résultat suit. □

Lemme 2.6.6. *Soient $(\mu,\nu,\rho) \in \mathbb{N}^3$ avec $2\rho < \nu$ et tels que $P(\mu+\nu) \leq \rho$. L'ensemble $\mathcal{E}$ des couples $(m,n) \in \{q^{\mu-2},\ldots,q^{\mu}-1\} \times \{q^{\nu-2},\ldots,q^{\nu}-1\}$ tels qu'il existe $k < q^{\mu+\rho}$ avec $f_P(mn+k)\overline{f_P(mn)} \neq f_P^{(\mu+2\rho)}(mn+k)\overline{f_P^{(\mu+2\rho)}(mn)}$ satisfait à*

$$\#\mathcal{E} \ll (\log q)q^{\mu+\nu-\rho+P(\mu+\nu+1)}.$$

Démonstration. Soit $\mathcal{B}$ l'ensemble des $l < q^{\nu-\rho}$ tels qu'il existe $(k_1, k_2) \in \{0, \dots, q^{\mu+\rho}-1\}^2$ avec

$$a_P(lq^\kappa + k_1 + k_2) - a_P(lq^\kappa + k_1) \neq a_P^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2) - a_P^{(\kappa+\rho)}(lq^\kappa + k_1).$$

Alors nous utilisons le Lemme 2.4.2 avec $\lambda = \nu - \rho$, $\kappa = \mu + \rho$ et $\rho = \rho$ pour obtenir $\#\mathcal{B} \ll q^{\nu-2\rho+P(\mu+\nu+1)}$.

Il suffit donc de compter le nombre $\mathcal{N}$ de couples $(m, n) \in \{q^{\mu-2}, \dots, q^\mu - 1\} \times \{q^{\nu-2}, \dots, q^\nu - 1\}$ tels que $mn = k_1 + lq^{\mu+\rho}$ avec $l \in \mathcal{B}$, k_2 jouera le rôle du k de l'énoncé. Par le Lemme 2.6.5, avec $\mu' = \mu + \rho$, nous obtenons

$$\#\mathcal{E} \ll (q^{\mu+\rho}\log q + q^\mu + q^{\mu+\rho-\mu+2})\#\mathcal{B} \ll (\log q)q^{\mu+\nu-\rho+P(\mu+\nu+1)}.$$

□

Lorsque nous tronquons deux fois la fonction f_P, des problèmes techniques peuvent surgir. Pour les pallier, il nous faut introduire une fenÃªtre de sécurité qui grandit selon la taille des entiers regardés. Le but de ce lemme est de mesurer l'erreur produite en regardant cette fenÃªtre. Notons qu'il ressemble très fortement au [MR15, Lemma 9], et la preuve en est d'ailleurs similaire. Seulement les objets spécifiques à cet article imposent une nouvelle démonstration.

Lemme 2.6.7. *Soient $(\mu, \nu, \mu_0, \mu_1, \mu_2) \in \mathbb{N}^5$ avec $\mu_0 \leq \mu_1 \leq \mu \leq \mu_2$, $\mu_1 - \mu_0 \leq \frac{3}{4}(\mu_2 - \mu_0)$ et $2(\mu_2 - \mu) \leq \mu_0$. Supposons également que $P(\mu_2) \leq \mu_1 - \mu_0$. Alors, pour $(a, b, c) \in \mathbb{N}^3$ l'ensemble $\mathcal{E}(a, b, c)$ des couples $(m, n) \in \{q^{\mu-2}, \dots, q^\mu - 1\} \times \{q^{\nu-2}, \dots, q^\nu - 1\}$ tels que*

$$\begin{aligned} &\frac{f_P^{(\mu_2)}\Big(mn + am + bn + c, T_q(mn + am + bn + c)\Big)}{f_P^{(\mu_1)}\Big(mn + am + bn + c, T_q(mn + am + bn + c)\Big)} \\ &\neq \frac{f_P^{(\mu_2)}\Big(q^{\mu_0} r_{\mu_0,\mu_2}(mn + am + bn + c), T_q(mn + am + bn + c)\Big)}{f_P^{(\mu_1)}\Big(q^{\mu_0} r_{\mu_0,\mu_2}(mn + am + bn + c), T_q(mn + am + bn + c)\Big)} \end{aligned} \tag{2.35}$$

vérifie

$$\#\mathcal{E}(a, b, c) \ll \max(\tau(q), \log q)\mu_2^{\omega(q)} q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)}. \tag{2.36}$$

Démonstration. Soit $\mathcal{B}$ l'ensemble des $l \in \{0, \dots, q^{\mu_2-\mu_0}-1\}$ tel qu'il existe $(k_1, k_2) \in \{0, \dots, q^{\mu_0} - 1\}^2$ avec

$$f_P^{(\mu_2)}(q^{\mu_0}l + k_1 + k_2)\overline{f_P^{(\mu_2)}(q^{\mu_0}l + k_1)} \neq f_P^{(\mu_1)}(q^{\mu_0}l + k_1 + k_2)\overline{f_P^{(\mu_1)}(q^{\mu_0}l + k_1)}.$$

Pour $0 \leq l \leq q^{\mu_2-\mu_0} - 2$, nous avons $0 \leq q^{\mu_0}l + k_1 + k_2 \leq q^{\mu_2} - 2$ et ainsi

$$f_P^{(\mu_2)}(q^{\mu_0}l + k_1 + k_2)\overline{f_P^{(\mu_2)}(q^{\mu_0}l + k_1)} = f_P(q^{\mu_0}l + k_1 + k_2)\overline{f_P(q^{\mu_0}l + k_1)}$$

sauf possiblement si $l = q^{\mu_2-\mu_0} - 1$. Comme $\mu_1 - \mu_0 \leq 3/4(\mu_2 - \mu_0)$, nous pouvons utiliser le Lemme 2.4.2 avec $\lambda = \mu_2 - \mu_0$, $\kappa = \mu_0$, $\rho = \mu_1 - \mu_0$, et donc

$$\#\mathcal{B} = O(q^{\mu_2-\mu_0-(\mu_1-\mu_0)+P(\mu_2-\mu_0+\mu_0+1)}) = O(q^{\mu_2-\mu_1+P(\mu_2+1)}). \tag{2.37}$$

Si on écrit $k = mn + am + bn + c$ sous la forme $k = r_{0,\mu_0}(k) + q^{\mu_0} r_{\mu_0,\mu_2}(k) + q^{\mu_2} k'$, nous avons

$$\mathcal{E}(a,b,c) \subset \mathcal{E}'(a,b,c),$$

avec $\mathcal{E}'(a,b,c)$ l'ensemble des couples (m,n) tels que $r_{\mu_0,\mu_2}(mn+am+bn+c) \in \mathcal{B}$.

En effet, l'équation (2.35) implique que

$$\frac{f_P^{(\mu_2)}\Big(q^{\mu_0} r_{\mu_0,\mu_2}(mn+am+bn+c) + r_{0,\mu_0}(mn+am+bn+c), T_q(mn+am+bn+c)\Big)}{f_P^{(\mu_1)}\Big(q^{\mu_0} r_{\mu_0,\mu_2}(mn+am+bn+c) + r_{0,\mu_0}(mn+am+bn+c), T_q(mn+am+bn+c)\Big)}$$
$$\neq \frac{f_P^{(\mu_2)}\Big(q^{\mu_0} r_{\mu_0,\mu_2}(mn+am+bn+c), T_q(mn+am+bn+c)\Big)}{f_P^{(\mu_1)}\Big(q^{\mu_0} r_{\mu_0,\mu_2}(mn+am+bn+c), T_q(mn+am+bn+c)\Big)},$$

et on pose $k_1 = 0$, $k_2 = r_{0,\mu_0}(mn+am+bn+c)$.

Nous pouvons écrire

$$\#\mathcal{E}'(a,b,c) = \sum_{l\in\mathcal{B}} \sum_{m,n} \chi_{q^{\mu_0-\mu_2}} \left(\frac{mn+am+bn+c}{q^{\mu_2}} - \frac{l}{q^{\mu_2-\mu_0}} \right).$$

Par le lemme de Vaaler, qui est énoncé dans notre thèse sous la forme du Théorème A.3.2 il suit que pour tout entier $H \geq 1$ il existe $a_h(q^{\mu_0-\mu_2}, H)$ et $b_h(q^{\mu_0-\mu_2}, H)$ vérifiant (A.23) tels que

$$\#\mathcal{E}'(a,b,c) = \sum_{l\in\mathcal{B}} \sum_{m,n} \sum_{|h|\leq H} a_h(q^{\mu_0-\mu_2}, H) e\left(\frac{h(mn+am+bn+c)}{q^{\mu_2}} - \frac{hl}{q^{\mu_2-\mu_0}} \right)$$
$$+ \sum_{l\in\mathcal{B}} \sum_{m,n} \sum_{|h|\leq H} b_h(q^{\mu_0-\mu_2}, H) e\left(\frac{h(mn+am+bn+c)}{q^{\mu_2}} - \frac{hl}{q^{\mu_2-\mu_0}} \right).$$

En posant $H = q^{\mu_2-\mu_0}$ et en utilisant (2.37), la contribution des termes $h = 0$ est bornée par $q^{\mu+\nu+\mu_0-\mu_2}\#\mathcal{B} \ll q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)}$. Par ailleurs, avec cette valeur de H, les coefficients $b_h(q^{\mu_0-\mu_2}, H)$ sont bornés en valeur absolue par $q^{\mu_0-\mu_2}$. Comme les coefficients $a_h(q^{\mu_0-\mu_2}, H)$ vérifient la mÃªme propriété, toujours en utilisant (2.37), nous avons :

$$\#\mathcal{E}'(a,b,c)$$
$$\ll q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)} + \frac{\#\mathcal{B}}{q^{\mu_2-\mu_0}} \sum_{1\leq|h|\leq q^{\mu_2-\mu_0}} \sum_n \left| \sum_m e\left(\frac{h(mn+am+bn+c)}{q^{\mu_2}} \right) \right|$$
$$\ll q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)} + \frac{q^{\mu_2-\mu_1+P(\mu_2+1)}}{q^{\mu_2-\mu_0}} \sum_{1\leq|h|\leq q^{\mu_2-\mu_0}} \sum_n \min\left(q^{\mu}, \left| \sin \pi \frac{h(n+a)}{q^{\mu_2}} \right|^{-1} \right).$$

Cependant la sommation sur n se fait sur au plus $\lceil q^{\nu-\mu_2} \rceil \leq q^{\nu-\mu_2} + 1$ périodes modulo q^{μ_2}, aussi en utilisant (A.16), on trouve

$$\#\mathcal{E}'(a,b,c) \ll q^{\mu+\nu+P(\mu_2+1)+\mu_0-\mu_1} + q^{\mu_2-\mu_1+P(\mu_2+1)}(q^{\nu-\mu_2}+1)(q^{\mu}\tau(q^{\mu_2}) + q^{\mu_2}\log q^{\mu_2})$$
$$\ll q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)}(1 + q^{-\mu_0}(1+q^{\mu_2-\nu})(\tau(q)\mu_2^{\omega(q)} + q^{\mu_2-\mu}\log q^{\mu_2})),$$

où à la seconde ligne on a utilisé la multiplicité de la fonction $\tau(n)$ qui donne $\tau(q^{\mu_2}) \leq \tau(q)\mu_2^{\omega(q)}$. En utilisant $\mu_1 \leq \mu \leq \nu$ nous obtenons

$$\#\mathcal{E}'(a,b,c) \ll q^{\mu+\nu+P(\mu_2+1)+\mu_0-\mu_1}\left(1+\mu_2^{\omega(q)}\max(\tau(q),\log q)q^{2\mu_2-2\mu-\mu_0}\right),$$

et en utilisant $2(\mu_2-\mu) \leq \mu_0$ nous obtenons le résultat désiré. □

Le lemme suivant est un pendant du Lemme 2.4.2 pour le cas des sommes de type II, dans le cas où la taille des entiers est fixée, ce cas de figure est une conséquence du Lemme 2.6.4.

Lemme 2.6.8. *Soient $(y,\lambda,\kappa,\rho) \in \mathbb{N}^4$ et soit B l'ensemble des $0 \leq l < q^\lambda$ tels qu'il existe $0 \leq k_1, k_2 < q^\kappa$ satisfaisant à*

$$a_P(lq^\kappa+k_1+k_2,y)-a_P(lq^\kappa+k_1,y) \neq a_P^{(\kappa+\rho)}(lq^\kappa+k_1+k_2,y)-a_P^{(\kappa+\rho)}(lq^\kappa+k_1,y). \quad (2.38)$$

Alors

$$\#B \ll q^{\lambda-\rho+P(y)} \quad (2.39)$$

Démonstration. Remarquons que si $P(y) > \rho$ alors la majoration est triviale. Supposons à présent $P(y) \leq \rho$. Pour tout entier n nous avons

$$a_P(n,y) = \sum_{i\geq 0} \epsilon_{i+P(y)}(n)\dots\epsilon_i(n)$$

et

$$a_P^{(\rho)}(n,y) = \sum_{i\geq 0} \epsilon_{i+P(y)}(n \bmod q^\rho)\dots\epsilon_i(n \bmod q^\rho) = \sum_{i\leq \rho-P(y)} \epsilon_{i+P(y)}(n)\dots\epsilon_i(n).$$

Ceci nous donne

$$\begin{aligned} &a_P(lq^\kappa+k_1+k_2,y)-a_P(lq^\kappa+k_1,y)-a_P^{(\kappa+\rho)}(lq^\kappa+k_1+k_2,y)+a_P^{(\kappa+\rho)}(lq^\kappa+k_1,y)\\ &= \sum_{i>\kappa+\rho-P(y)} \Big[\epsilon_{i+P(y)}(lq^\kappa+k_1+k_2)\dots\epsilon_i(lq^\kappa+k_1+k_2)\\ &\qquad -\epsilon_{i+P(y)}(lq^\kappa+k_1)\dots\epsilon_i(lq^\kappa+k_1)\Big]. \end{aligned}$$

Pour que cette quantité soit non nulle, il est donc nécessaire que

$$\epsilon_{\kappa+\rho-P(y)}(lq^\kappa+k_1+k_2) \neq \epsilon_{\kappa+\rho-P(y)}(lq^\kappa+k_1),$$

(sinon, cela veut dire que la propagation s'est arrÃªtée avant ce chiffre), mais comme $P(y) \leq \rho$, ceci veut dire

$$\epsilon_{\rho-P(y)}(l) \neq \epsilon_{\rho-P(y)}(l+\lfloor (k_1+k_2)/q^\kappa \rfloor).$$

Comme $\lfloor (k_1+k_2)/q^\kappa \rfloor \leq 1$, cette dernière n'est vérifiée que si $\epsilon_i(l) = q-1$ pour tout $0 \leq i < \rho - P(y)$, ce qui montre le résultat. □

De mÃªme que pour les sommes de type I, nous aurons besoin d'une propriété de Fourier, et nos besoins sont légèrement différents. Toutefois, la démonstration du lemme suivant est très similaire à celle du Lemme 2.4.3, aussi nous nous contenterons d'énoncer le résultat. La forme que prendra le contrôle de la transformée de Fourier est l'objet du Lemme 2.6.10.

Lemme 2.6.9. *Soient $l \geq 0$ et k deux entiers tels que $P(k) \leq l$, alors uniformément en $t \in \mathbb{R}$:*

$$\left|\frac{1}{q^l}\sum_{0\leq u<q^l} f_P(uq^\kappa, k)e(-ut)\right| \leq q^{-\gamma_P(l,k)}$$

avec γ_P définie dans (2.2).

L'objet du lemme suivant est de dire que la fonction doublement tronquée a une transformée de Fourier qui décroît. Pour l'expliciter nous introduisons un objet intermédiaire.

Soit $G_{\mu_0,\lambda}(t,k) = \dfrac{1}{q^\lambda}\displaystyle\sum_{0\leq u<q^\lambda} f_P^{(\mu_1,\mu_2)}(uq^{\mu_0},k)e\left(-\frac{ut}{q^\lambda}\right)$.

Lemme 2.6.10. *Uniformément pour $\lambda \in \mathbb{N}$ tel que*

$$\frac{1}{3}(\mu_2-\mu_0) \leq \lambda \leq \frac{4}{5}(\mu_2-\mu_0), \tag{2.40}$$

et tout entier k tel que

$$P(k) \leq \frac{1}{3}(\mu_1-\mu_0) \tag{2.41}$$

et $t \in \mathbb{R}$, nous avons :

$$\sum_{0\leq h<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0}(h+t,k)|^2 \ll q^{1/2(\mu_1-\mu_0-\gamma_P(\lambda,k))+3P(k)/4}(\log q^{\mu_2-\mu_1})^2. \tag{2.42}$$

La preuve est similaire à [MR15], mais les modifications des éléments entrant en compte dans la démonstration imposent de reprendre la preuve. Le fil de la preuve consiste à se ramener à une écriture de la forme de (2.22).

Démonstration. Pour commencer modifions l'écriture de $G_{\mu_0,\mu_2-\mu_0}(h+t,k)$. Pour $0 \leq \lambda \leq \mu_2-\mu_0$ et $t \in \mathbb{R}$, nous pouvons écrire

$$G_{\mu_0,\mu_2-\mu_0}(t,k) = \frac{1}{q^{\mu_2-\mu_0}}\sum_{0\leq u<q^\lambda}\sum_{0\leq v<q^{\mu_2-\mu_0-\lambda}} f_P^{(\mu_1,\mu_2)}(q^{\mu_0}(u+vq^\lambda),k)e\left(-\frac{(u+vq^\lambda)t}{q^{\mu_2-\mu_0}}\right).$$

Mais si $\mu_1-\mu_0 \leq \lambda \leq \mu_2-\mu_0$, alors $0 \leq u+vq^\lambda < q^{\mu_2-\mu_0}$ et $(u+vq^\lambda)q^{\mu_0} \equiv uq^{\mu_0} \bmod q^{\mu_1}$, et pour $0 \leq u < q^\lambda$ et $0 \leq v < q^{\mu_2-\mu_0-\lambda}$, on a :

$$\begin{aligned} f_P^{(\mu_1,\mu_2)}(q^{\mu_0}(u+vq^\lambda),k) &= f_P^{(\mu_2)}(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P^{(\mu_1)}(q^{\mu_0}(u+vq^\lambda),k)} \\ &= f_P(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P^{(\mu_1)}(q^{\mu_0}u,k)} \end{aligned}$$

ce qui mène à

$$G_{\mu_0,\mu_2-\mu_0}(t,k) = \frac{1}{q^{\mu_2-\mu_0-\lambda}} \sum_{0\le v<q^{\mu_2-\mu_0-\lambda}} f_P(vq^{\mu_0+\lambda},k)e\left(-\frac{vq^\lambda t}{q^{\mu_2-\mu_0}}\right)$$
$$\frac{1}{q^\lambda}\sum_{0\le u<q^\lambda} f_P(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P(vq^{\mu_0+\lambda},k)f_P^{(\mu_1)}(uq^{\mu_0},k)}e\left(-\frac{ut}{q^{\mu_2-\mu_0}}\right).$$

Introduisons une autre troncation. Pour cela, nous posons

$$1 \le \rho_3 \le \mu_2-\mu_0-\lambda. \tag{2.43}$$

Par le Lemme 2.6.8, le nombre de $v \in \{0,\dots,q^{\mu_2-\mu_0-\lambda}\}$ tels qu'il existe $u \in \{0,\dots,q^\lambda-1\}$ pour lequel

$$f_P(uq^{\mu_0}+vq^{\mu_0+\lambda},k)\overline{f_P(vq^{\mu_0+\lambda},k)} \neq f_P^{(\mu_0+\lambda+\rho_3)}(uq^{\mu_0}+vq^{\mu_0+\lambda},k)\overline{f_P^{(\mu_0+\lambda+\rho_3)}(vq^{\mu_0+\lambda},k)} \tag{2.44}$$

est $O\left(q^{\mu_2-\mu_0-\lambda-\rho_3+P(k)}\right)$. Ainsi, en sommant sur u, l'ensemble $\widetilde{\mathcal{W}_\lambda}$ des couples (u,v) satisfaisant à (2.44) vérifie

$$\#\widetilde{\mathcal{W}_\lambda} \ll q^{\mu_2-\mu_0-\rho_3+P(k)}. \tag{2.45}$$

Ceci nous mène à considérer pour tout $t \in \mathbb{R}$ la décomposition suivante :

$$G_{\mu_0,\mu_2-\mu_0}(t,k) = G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t,k) + G_{\mu_0,\mu_2-\mu_0,\lambda,2}(t,k),$$

avec

$$G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t,k) := \frac{1}{q^{\mu_2-\mu_0-\lambda}} \sum_{0\le v<q^{\mu_2-\mu_0-\lambda}} f_P(vq^{\mu_0+\lambda},k)e\left(-\frac{vq^\lambda t}{q^{\mu_2-\mu_0}}\right)$$
$$\cdot \frac{1}{q^\lambda}\sum_{0\le u<q^\lambda} f_P^{(\mu_0+\lambda+\rho_3)}(q^{\mu_0}(u+vq^\lambda),k)$$
$$\overline{f_P^{(\mu_0+\lambda+\rho_3)}(vq^{\mu_0+\lambda},k)f_P^{(\mu_1)}(uq^{\mu_0},k)}e\left(-\frac{ut}{q^{\mu_2-\mu_0}}\right),$$

qui est le terme principal, et

$$G_{\mu_0,\mu_2-\mu_0,\lambda,2}(t,k) := \frac{1}{q^{\mu_2-\mu_0}} \sum_{(u,v)\in\widetilde{\mathcal{W}_\lambda}} f_P(vq^{\mu_0+\lambda},k)f_P^{(\mu_1)}(uq^{\mu_0},k)e\left(-\frac{(u+vq^\lambda)t}{q^{\mu_2-\mu_0}}\right)$$
$$\cdot\Bigg(f_P(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P(vq^{\mu_0+\lambda},k)}$$
$$- f_P^{(\mu_0+\lambda+\rho_3)}(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P^{(\mu_0+\lambda+\rho_3)}(vq^{\mu_0+\lambda},k)}\Bigg),$$

qui est le terme d'erreur. Si nous introduisons dans $G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t,k)$ le résidu w de v mod q^{ρ_3} dans le but de rendre les variables u et v indépendantes (notons que

contrairement aux sommes de type I il n'y a pas de difficultés ici : la taille est fixée), nous obtenons

$$\begin{aligned}
&G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t,k)\\
&= \sum_{0\le w<q^{\rho_3}} \frac{1}{q^{\mu_2-\mu_0-\lambda}} \sum_{0\le v<q^{\mu_2-\mu_0-\lambda}} f_P(vq^{\mu_0+\lambda},k)e\left(-\frac{vq^\lambda t}{q^{\mu_2-\mu_0}}\right)\frac{1}{q^{\rho_3}}\sum_{0\le l<q^{\rho_3}} e\left(l\frac{v-w}{q^{\rho_3}}\right)\\
&\quad\cdot\frac{1}{q^\lambda}\sum_{0\le u<q^\lambda} f_P^{(\mu_0+\lambda+\rho_3)}(q^{\mu_0}(u+wq^\lambda),k)\\
&\qquad\cdot\overline{f_P^{(\mu_0+\lambda+\rho_3)}(wq^{\mu_0+\lambda},k)f_P^{(\mu_1)}(uq^{\mu_0},k)}e\left(-\frac{ut}{q^{\mu_2-\mu_0}}\right),
\end{aligned}$$

ce qui nous donne

$$G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t,k)=\sum_{0\le l<q^{\rho_3}}\frac{\tilde{c}_l(t)}{q^{\mu_2-\mu_0-\lambda}}\sum_{0\le v<q^{\mu_2-\mu_0-\lambda}} f_P(vq^{\mu_0+\lambda},k)e\left(-\frac{vt}{q^{\mu_2-\mu_0-\lambda}}+\frac{vl}{q^{\rho_3}}\right)$$

où on a posé

$$\tilde{c}_l(t)=\frac{1}{q^{\rho_3}}\sum_{0\le w<q^{\rho_3}} c_\lambda(w,t)e\left(-\frac{wl}{q^{\rho_3}}\right)$$

et

$$\begin{aligned}
&c_\lambda(w,t)=\\
&\frac{1}{q^\lambda}\sum_{0\le u<q^\lambda} f_P^{(\mu_0+\lambda+\rho_3)}(q^{\mu_0}(u+wq^\lambda),k)\overline{f_P^{(\mu_0+\lambda+\rho_3)}(wq^{\mu_0+\lambda},k)f_P^{(\mu_1)}(uq^{\mu_0},k)}e\left(-\frac{ut}{q^{\mu_2-\mu_0}}\right).
\end{aligned}$$

Par l'inégalité de Cauchy-Schwarz nous obtenons :

$$\begin{aligned}
&|G_{\mu_0,\mu_2-\mu_0,\lambda,1}(t,k)|^2\\
&\le\left(\sum_{0\le l<q^{\rho_3}}|\tilde{c}_l(t)|^2\right)\sum_{0\le l<q^{\rho_3}}\left|\frac{1}{q^{\mu_2-\mu_0-\lambda}}\sum_{0\le v<q^{\mu_2-\mu_0-\lambda}} f_P(vq^{\mu_0+\lambda},k)e\left(-\frac{vt}{q^{\mu_2-\mu_0-\lambda}}+\frac{vl}{q^{\rho_3}}\right)\right|^2.
\end{aligned}$$

Mais en développant les modules au carré, nous obtenons

$$\sum_{0\le l<q^{\rho_3}}|\tilde{c}_l(t)|^2=\frac{1}{q^{\rho_3}}\sum_{0\le w<q^{\rho_3}}|c_\lambda(w,t)|^2, \tag{2.46}$$

et puisque $f_P^{(\mu_1)}(u_0q^{\mu_0}+u_1q^{\mu_1},k)=f_P^{(\mu_1)}(u_0q^{\mu_0},k)$ pour $0\le u_0<q^{\mu_1-\mu_0}$ et $0\le u_1<q^{\lambda-\mu_1+\mu_0}$, nous pouvons écrire en posant $u=u_0+u_1q^{\mu_1-\mu_0}$,

$$\begin{aligned}
c_\lambda(w,t)&=\overline{f_P^{(\mu_0+\lambda+\rho_3)}(wq^{\mu_0+\lambda},k)}e\left(\frac{wq^\lambda t}{q^{\mu_2-\mu_0}}\right)\frac{1}{q^{\mu_1-\mu_0}}\sum_{0\le u_0<q^{\mu_1-\mu_0}}\overline{f_P^{(\mu_1)}(u_0q^{\mu_0},k)}\\
&\quad\cdot\frac{1}{q^{\lambda-\mu_1+\mu_0}}\sum_{0\le u_1<q^{\lambda-\mu_1+\mu_0}} f_P^{(\mu_0+\lambda+\rho_3)}(u_0q^{\mu_0}+u_1q^{\mu_1}+wq^{\mu_0+\lambda},k)\\
&\qquad\cdot e\left(-\frac{(u_0q+u_1q^{\mu_1-\mu_0}+wq^\lambda)t}{q^{\mu_2-\mu_0}}\right).
\end{aligned}$$

Afin de retirer la restriction de la troncation, la somme sur u_1 peut Ã[a]tre écrite comme une somme sur les u' tels que $0 \leq u' < q^{\lambda+\rho_3}$ et $u' = u_0 + u_1 q^{\mu_1-\mu_0} + wq^{\lambda}$ pour un certain u_1. Nous pouvons donc réécrire la dernière ligne

$$\sum_{0\leq l'<q^{\lambda+\rho_3}} \frac{1}{q^{\lambda-\mu_1+\mu_0}} \sum_{0\leq u_1<q^{\lambda-\mu_1+\mu_0}} e\left(l'\frac{(u_0+u_1q^{\mu_1-\mu_0}+wq^{\lambda})}{q^{\lambda+\rho_3}}\right) \cdot \frac{1}{q^{\lambda+\rho_3}} \sum_{0\leq u'<q^{\lambda+\rho_3}} f_P(u'q^{\mu_0},k)e\left(-\frac{u't}{q^{\mu_2-\mu_0}}-\frac{l'u'}{q^{\lambda+\rho_3}}\right).$$

Si nous supposons

$$P(k) \leq \lambda + \rho_3, \tag{2.47}$$

nous pouvons alors utiliser le Lemme 2.6.9 avec $l = \lambda + \rho_3$, ce qui nous donne l'estimation uniforme suivante

$$\left|\frac{1}{q^{\lambda+\rho_3}} \sum_{0\leq u'<q^{\lambda+\rho_3}} f_P(u'q^{\mu_0},k)e\left(-\frac{u't}{q^{\mu_2-\mu_0}}-\frac{l'u'}{q^{\lambda+\rho_3}}\right)\right| \leq q^{-\gamma_P(\lambda+\rho_3,k)},$$

ainsi :

$$|c_\lambda(w,t)| \ll \frac{q^{-\gamma_P(\lambda+\rho_3,k)}}{q^{\lambda-\mu_1+\mu_0}} \sum_{0\leq l'<q^{\lambda+\rho_3}} \min\left(q^{\lambda-\mu_1+\mu_0}, \left|\sin\pi\frac{l'q^{\mu_1-\mu_0}}{q^{\lambda+\rho_3}}\right|^{-1}\right).$$

L'équation (2.2) nous informe que $\gamma_P(l,k)$ est strictement croissante en l, et en utilisant le Lemme A.2.11, et en remarquant qu'il y a $q^{\mu_1-\mu_0}$ périodes modulo $q^{\lambda+\rho_3-\mu_1+\mu_0}$ et que $q^{\lambda-\mu_1+\mu_0} \leq q^{\lambda+\rho_3}$, nous obtenons

$$\begin{aligned}|c_\lambda(w,t)| &\ll \frac{q^{-\gamma_P(\lambda+\rho_3,k)}}{q^{\lambda-\mu_1+\mu_0}} q^{\lambda+\rho_3}\log q^{\lambda+\rho_3-\mu_1+\mu_0} \\ &\ll q^{\rho_3+\mu_1-\mu_0-\gamma_P(\lambda,k)}\log q^{\lambda+\rho_3-\mu_1+\mu_0}.\end{aligned}$$

Nous en déduisons, par (2.43) et (2.46), que

$$\sum_{0\leq l<q^{\rho_3}} |\tilde{c}_l(t)|^2 \ll q^{2\rho_3+2(\mu_1-\mu_0)-2\gamma_P(\lambda,k)}(\log q^{\mu_2-\mu_1})^2,$$

et

$$\begin{aligned}&\sum_{0\leq h<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0,\lambda,1}(h+t,k)|^2 \\ &\quad\ll q^{2\rho_3+2(\mu_1-\mu_0)-2\gamma_P(\lambda,k)}(\log q^{\mu_2-\mu_1})^2 \\ &\quad\quad\cdot \sum_{0\leq l<q^{\rho_3}} \frac{1}{q^{2(\mu_2-\mu_0-\lambda)}} \sum_{0\leq v,v'<q^{\mu_2-\mu_0-\lambda}} f_P(vq^{\mu_0+\lambda},k)\overline{f_P(v'q^{\mu_0+\lambda},k)} \\ &\quad\quad\cdot e\left(-\frac{(v-v')t}{q^{\mu_2-\mu_0-\lambda}}+\frac{(v-v')l}{q^{\rho_3}}\right) \sum_{0\leq h<q^{\mu_2-\mu_0-\lambda}} e\left(-\frac{(v-v')h}{q^{\mu_2-\mu_0-\lambda}}\right),\end{aligned}$$

c'est-à-dire

$$\sum_{0\leq h<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0,\lambda,1}(h+t,k)|^2 \ll q^{3\rho_3+2(\mu_1-\mu_0)-2\gamma_P(\lambda,k)}(\log q^{\mu_2-\mu_1})^2. \tag{2.48}$$

Traitons à présent le terme d'erreur. Nous rappelons que

$$\begin{aligned}
&G_{\mu_0,\mu_2-\mu_0,\lambda,2}(t,k)\\
&= \frac{1}{q^{\mu_2-\mu_0}} \sum_{(u,v)\in\widetilde{\mathcal{W}_\lambda}} f_P(vq^{\mu_0+\lambda}) f_P^{(\mu_1)}(uq^{\mu_0},k) e\left(-\frac{(u+vq^\lambda)t}{q^{\mu_2-\mu_0}}\right)\\
&\quad\cdot\Bigg(f_P(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P(vq^{\mu_0+\lambda},k)}\\
&\qquad - f_P^{(\mu_0+\lambda+\rho_3)}(q^{\mu_0}(u+vq^\lambda),k)\overline{f_P^{(\mu_0+\lambda+\rho_3)}(vq^{\mu_0+\lambda},k)}\Bigg)\\
&= \frac{1}{q^{\mu_2-\mu_0}} \sum_{w<q^{\mu_2-\mu_0}} c'_{\lambda,k}(w) e\left(-\frac{wt}{q^{\mu_2-\mu_0}}\right),
\end{aligned}$$

où $|c'_{\lambda,k}(w)| \le 2$ et $c'_{\lambda,k}(w) = 0$ si $w \notin \mathcal{W}_\lambda$, où $\mathcal{W}_\lambda$ est l'ensemble des $w = u + vq^\lambda, (u,v) \in \widetilde{\mathcal{W}_\lambda}$. Il vient donc

$$\begin{aligned}
\sum_{0\le h<q^{\mu_2-\mu_0}} |G_{\mu_0,\mu_2-\mu_0,\lambda,2}(h+t,k)|^2 &= \frac{1}{q^{2(\mu_2-\mu_0)}} \sum_{0\le w,w'<q^{\mu_2-\mu_0}} c'_{\lambda,k}(w)\overline{c'_{\lambda,k}(w')} e\left(-\frac{(w-w')t}{q^{\mu_2-\mu_0}}\right)\\
&\quad\cdot \sum_{0\le h<q^{\mu_2-\mu_0}} e\left(-\frac{(w-w')h}{q^{\mu_2-\mu_0}}\right)\\
&= \frac{1}{q^{\mu_2-\mu_0}} \sum_{w<q^{\mu_2-\mu_0}} |c'_{\lambda,k}(w)|^2.
\end{aligned}$$

Nous pouvons donc conclure, en utilisant (2.45), que

$$\sum_{0\le h<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0,\lambda,2}(h+t,k)|^2 \ll q^{-\rho_3+P(k)}. \tag{2.49}$$

En rassemblant (2.48) et (2.49), nous obtenons

$$\sum_{0\le h<q^{\mu_2-\mu_0-\lambda}} |G_{\mu_0,\mu_2-\mu_0}(h+t,k)|^2 \ll q^{-\rho_3+P(k)} + q^{3\rho_3+2(\mu_1-\mu_0)-2\gamma_P(\lambda,k)}(\log q^{\mu_2-\mu_1})^2,$$

et en posant $\rho_3 = \max(1, \frac{1}{2}(\gamma_P(\lambda,k) - \mu_1 + \mu_0) + P(k)/4)$, nous avons le résultat demandé. Par ailleurs

$$\begin{aligned}
&\frac{1}{2}(\gamma_P(\lambda,\kappa) - \mu_1 + \mu_0) + \frac{P(k)}{4} \le \mu_2 - \mu_0 - \lambda\\
&\qquad\Leftrightarrow \lambda + \frac{\gamma_P(\lambda,k)}{2} \le (\mu_2-\mu_0) + \frac{1}{2}(\mu_1-\mu_0) - \frac{P(k)}{4},
\end{aligned}$$

or, comme $\gamma_P(\lambda,k) \le \lambda/2$, par (2.40) nous avons $\lambda + \frac{\gamma_P(\lambda,k)}{2} \le (\mu_2-\mu_0)$. La condition (2.41) permet de conclure à (2.43).

Enfin, toujours par (2.41), nous avons

$$P(k) \le \frac{1}{3}(\mu_1-\mu_0) \le \frac{1}{3}(\mu_2-\mu_0) \le \lambda,$$

où la dernière inégalité résulte de (2.40), et donc (2.47) est vérifiée. □

Nous allons maintenant contrôler les sommes de type II.

2.7 Sommes de type II

Soient M et N des entiers tels que $1 \leq M \leq N$, nous notons, tout comme dans la Partie 2.5, $\mu - 1 = T_q(M)$ et $\nu - 1 = T_q(N)$. Nous supposons ici en outre

$$\frac{1}{4}(\mu+\nu) \leq \mu \leq \nu \leq \frac{3}{4}(\mu+\nu). \tag{2.50}$$

Soit $\vartheta \in \mathbb{R}, a_m \in \mathbb{C}, b_n \in \mathbb{C}$ avec $|a_m| \leq 1, |b_n| \leq 1$. Nous écrivons alors

$$S_{II}(\vartheta) := \sum_{\frac{M}{q}<m\leq M} \sum_{\frac{N}{q}<n\leq N} a_m b_n f_P(mn) e(\vartheta mn).$$

Nous allons prouver le

Théorème 2.7.1. *Soit $P : \mathbb{N} \to \mathbb{N}$ telle que*

$$P(\mu+\nu+1) \leq \frac{2}{3}\Big\lfloor \frac{1}{16}\gamma_P\left(\frac{\mu+\nu}{640},\, \mu+\nu-2\right)\Big\rfloor. \tag{2.51}$$

Alors nous avons uniformément en $\vartheta \in \mathbb{R}$

$$|S_{II}(\vartheta)| \ll \left(\max\left(\tau(q), (\log q)^3\right)(\mu+\nu)^{\omega(q)+3}\right)^{1/4} q^{\mu+\nu-\frac{1}{64}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu-2)}, \tag{2.52}$$

où $\gamma_P(k,l)$ est définie en (2.2)

Démonstration. Nous commenÃ§ons par lisser la somme, c'est-à-dire enlever les variables a_m et b_n. Nous en profitons pour introduire la fonction tronquée dès que possible. L'idée est d'utiliser l'inégalité de Cauchy-Schwarz deux fois. Pour la seconde fois, afin d'enlever la valeur absolue, nous utilisons l'inégalité de Van der Corput (Théorème A.2.3) afin d'obtenir un contrôle plus fin que la majoration triviale.

Par l'inégalité de Cauchy-Schwarz :

$$|S_{II}(\vartheta)|^2 \leq M \sum_m \left|\sum_n b_n f_P(mn) e(\vartheta mn)\right|^2.$$

Soit ρ un entier tel que

$$1 \leq 7\rho \leq \mu. \tag{2.53}$$

On pose $R = q^\rho$ de sorte que $1 \leq R \ll N$. Par le Théorème A.2.3 :

$$|S_{II}(\vartheta)|^2 \ll \frac{M^2N^2}{R} + \frac{MN}{R}\sum_{1\leq r<R}\left(1-\frac{r}{R}\right)\Re(S_1(r)), \tag{2.54}$$

avec

$$S_1(r) := \sum_m \sum_{n\in I_1(N,r)} b_{n+r}\overline{b_n} f_P(mn+mr)\overline{f_P(mn)} e(\vartheta mr),$$

avec $I_1(N,r) = (N/q, N-r]$. Si de plus ρ vérifie

$$P(\mu+\nu) \leq \rho \tag{2.55}$$

on peut utiliser le Lemme 2.6.6 pour obtenir

$$S_1(r) = S_1'(r) + O((\log q)q^{\mu+\nu-\rho+P(\mu+\nu+1)}), \tag{2.56}$$

avec

$$S_1'(r) = \sum_m \sum_{n\in I_1(N,r)} b_{n+r}\overline{b_n} f_P^{(\mu+2\rho)}(mn+mr)\overline{f_P^{(\mu+2\rho)}(mn)}e(\vartheta mr),$$

et nous posons

$$\mu_2 := \mu + 2\rho. \tag{2.57}$$

En appliquant l'inégalité de Cauchy-Schwarz et en étendant la sommation sur n à l'intervalle $(N/q, N]$, on trouve :

$$|S_1'(r)|^2 \ll N\sum_n \left|\sum_m f_P^{(\mu_2)}(mn+mr)\overline{f_P^{(\mu_2)}(mn)}e(\vartheta mr)\right|^2,$$

et une utilisation du Lemme A.2.3 avec des paramètres μ_1 et S tels que

$$1 \le q^{\mu_1}S \ll M \tag{2.58}$$

donne :

$$\sum_{1\le r<R} |S_1'(r)|^2 \ll \frac{M^2N^2R}{S} + \frac{MN}{S}\Re(S_2), \tag{2.59}$$

où

$$S_2 := \sum_{1\le r<R}\sum_{1\le s<S}\left(1-\frac{s}{S}\right)S_2'(r,s)e\left(\vartheta q^{\mu_1}rs\right) \tag{2.60}$$

et

$$S_2'(r,s) = \sum_{m\in I_2(M,s)}\sum_n f_P^{(\mu_2)}((m+sq^{\mu_1})(n+r))\overline{f_P^{(\mu_2)}(m(n+r))f_P^{(\mu_2)}((m+sq^{\mu_1})n)}f_P^{(\mu_2)}(mn),$$

avec $I_2(M,s) = (M/q, M-sq^{\mu_1}]$.

La suite logique ici consiste à remplacer chaque fonction $f_P^{(\mu_2)}$ par la fonction doublement tronquée $f_P^{(\mu_1,\mu_2)} := f_P^{(\mu_2)}\overline{f_P^{(\mu_1)}}$ par l'intermédiaire du jeu d'écriture

$$f_P^{(\mu_2)} = f_P^{(\mu_2)}\overline{f_P^{(\mu_1)}}f_P^{(\mu_1)}.$$

Il est possible de le faire dans [MR15] car les fonctions tronquées permettent le passage aux transformées de Fourier discrètes. En effet, le raisonnement repose sur l'écriture suivante :

$$\begin{aligned} S_2'(r,s) = \sum_{m\in I_2(M,s)}\sum_n & f_P^{(\mu_1,\mu_2)}((m+sq^{\mu_1})(n+r)) \\ & \cdot \overline{f_P^{(\mu_1,\mu_2)}(m(n+r))f_P^{(\mu_1,\mu_2)}((m+sq^{\mu_1})n)}f_P^{(\mu_1,\mu_2)}(mn) \\ & \cdot f_P^{(\mu_1)}((m+sq^{\mu_1})(n+r))\overline{f_P^{(\mu_1)}(m(n+r))f_P^{(\mu_1)}((m+sq^{\mu_1})n)}f_P^{(\mu_1)}(mn), \end{aligned}$$

et il n'est pas clair que pour nous la dernière ligne vaille 1. On pourrait très bien imaginer $P(T_q((m+sq^{\mu_1})(n+r))) \neq P(T_q(m(n+r)))$ auquel cas il n'y aurait aucune raison de trouver l'identité espérée.

Cependant, si nous posons $S = q^{2\rho}$ et $\mu_1 = \mu - 3\rho$, et

$$S_2''(r,s) := \sum_{m \in I_2(M,s)} \sum_n f_P^{(\mu_1,\mu_2)}((m+sq^{\mu_1})(n+r)) \cdot \overline{f_P^{(\mu_1,\mu_2)}(m(n+r)) f_P^{(\mu_1,\mu_2)}((m+sq^{\mu_1})n)} f_P^{(\mu_1,\mu_2)}(mn),$$

nous avons $S_2'(r,s) \leq S_2''(r,s) + S_2'''(r,s)$ avec

$$|S_2'''(r,s)| \leq \#\{(m,n) : T_q(mn) \neq T_q((m+Sq^{\mu_1})(n+q^{\rho}))\}.$$

En effet, si $T_q(mn) = T_q((m+Sq^{\mu_1})(n+q^{\rho}))$, on a en particulier $T_q(mn) = T_q((m+Sq^{\mu_1})n)$ et $T_q(m(n+q^{\rho})) = T_q((m+Sq^{\mu_1})(n+q^{\rho}))$ et ces dernières identités demeurent valables pour $s \leq S$ et $r \leq q^{\rho}$ en lieu et place de S et q^{ρ}. Mais alors $m + sq^{\mu_1} \equiv m \bmod q^{\mu_1}$, et donc $f_P^{(\mu_1)}((m+sq^{\mu_1})n) = f_P^{(\mu_1)}(mn)$, et de mÃªme pour $m(n+r)$ et $(m+sq^{\mu_1})(n+r)$. En imposant

$$\rho \leq \frac{\nu - 1}{2} \tag{2.61}$$

de sorte à pouvoir utiliser le Lemme 2.6.4. Nous obtenons alors :

$$S_2'(r,s) = S_2''(r,s) + O((\mu+\nu)q^{\mu+\nu-\rho}). \tag{2.62}$$

Pour des raisons techniques, il est plus intéressant pour nous, au lieu de regarder $r_{\mu_1,\mu_2}(n)$, de regarder $r_{\mu_0,\mu_2}(n)$ avec un $\mu_0 \leq \mu_1$ bien contrôlé. C'est l'objet des calculs suivants.

Soit ρ' tel que

$$\rho' \leq \rho, \tag{2.63}$$

nous posons

$$\mu_0 = \mu_1 - 2\rho', \tag{2.64}$$

de sorte que $\mu_1 - \mu_0 \leq 2\rho' \leq 3/4(5\rho + 2\rho') = 3/4(\mu_2 - \mu_0)$.

Si nous avons

$$P(\mu + 2\rho) = P(\mu_2) \leq \mu_1 - \mu_0 = 2\rho' \tag{2.65}$$

par le Lemme 2.6.7 :

$$S_2''(r,s) = S_3(r,s) + O\left(\max(\tau(q), \log q)\mu_2^{\omega(q)} q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)}\right) \tag{2.66}$$

avec

$$S_3(r,s) = \sum_m \sum_n \varphi_P\Big(r_{\mu_0,\mu_2}((m+sq^{\mu_1})(n+r)), T_q((m+sq^{\mu_1})(n+r))\Big) \cdot \overline{\varphi_P\Big((r_{\mu_0,\mu_2} m(n+r)), T_q(m(n+r))\Big)} \cdot \overline{\varphi_P\Big(r_{\mu_0,\mu_2}((m+sq^{\mu_1})n), T_q((m+sq^{\mu_1})n)\Big)} \cdot \varphi_P\Big(r_{\mu_0,\mu_2}(mn), T_q(mn)\Big),$$

où on a posé

$$\varphi_P(x,y) := e\left(\sum_{i=\mu_1-P(y)}^{\mu_2-P(y)} \epsilon_{i+P(y)}(q^{\mu_0}x)\cdots\epsilon_i(q^{\mu_0}x)\right).$$

Nous pouvons à présent rendre les entiers considérés "indépendants". Pour ce faire nous nous intéressons aux différents restes. On remarque que $\varphi_P(x,y)$ est $q^{\mu_2-\mu_0}$ périodique en x. Ainsi en posant $u_0 := r_{\mu_0,\mu_2}(mn)$ et $u_1 := r_{\mu_0,\mu_2}(mn+mr)$, on a

$$r_{\mu_0,\mu_2}(mn+q^{\mu_1}sn) = r_{\mu_2-\mu_0}(u_0+q^{\mu_1-\mu_0}sn) = u_0+q^{\mu_1-\mu_0}sn \bmod q^{\mu_2-\mu_0}$$

et

$$\begin{aligned} r_{\mu_0,\mu_2}(mn+mr+q^{\mu_1}sn+q^{\mu_1}sr) &= r_{\mu_2-\mu_0}(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr) \\ &= u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr \bmod q^{\mu_2-\mu_0}. \end{aligned}$$

Et donc, comme $\varphi_P(x,y) = \varphi_P(x \bmod q^{\mu_2-\mu_0}, y)$, nous avons :

$$\begin{aligned} &\varphi_P\Big(r_{\mu_0,\mu_2}((m+sq^{\mu_1})n), T_q((m+sq^{\mu_1})n)\Big) \\ &\qquad = \varphi_P\Big(r_{\mu_2-\mu_0}(u_0+q^{\mu_1-\mu_0}sn), T_q((m+sq^{\mu_1})n)\Big) \\ &\qquad = \varphi_P\Big(u_0+q^{\mu_1-\mu_0}sn, T_q((m+sq^{\mu_1})n)\Big) \end{aligned}$$

et

$$\begin{aligned} &\varphi_P\Big(r_{\mu_0,\mu_2}(m(n+r)+nsq^{\mu_1}+rsq^{\mu_1}), T_q((m+sq^{\mu_1})(n+r))\Big) \\ &\qquad = \varphi_P\Big(r_{\mu_2-\mu_0}(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr), T_q((m+sq^{\mu_1})(n+r))\Big) \\ &\qquad = \varphi_P\Big(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr, T_q((m+sq^{\mu_1})(n+r))\Big). \end{aligned}$$

Nous rappelons que

$$r_{\mu_0,\mu_2}(n) = u \Leftrightarrow \frac{n}{q^{\mu_2}} \in \left[\frac{u}{q^{\mu_2-\mu_0}}, \frac{u+1}{q^{\mu_2-\mu_0}}\right) + \mathbb{Z}$$

et que $\chi_\alpha(x)$ désigne la fonction caractéristique de l'intervalle $[0,\alpha)$ translaté dans $\mathbb{Z}$, si bien que

$$\begin{aligned} S_3(r,s) = \sum_{m\in I_2(M,s)}\sum_{n}\sum_{0\le u_0,u_1<q^{\mu_2-\mu_0}} &\chi_{q^{\mu_0-\mu_2}}\left(\frac{mn}{q^{\mu_2}}-\frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ &\cdot \chi_{q^{\mu_0-\mu_2}}\left(\frac{mn+mr}{q^{\mu_2}}-\frac{u_1}{q^{\mu_2-\mu_0}}\right)\overline{\varphi_P\Big(u_1, T_q(mn+mr)\Big)}\varphi_P\Big(u_0, T_q(mn)\Big) \\ &\cdot \varphi_P\Big(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr, T_q((m+sq^{\mu_1})(n+r))\Big) \\ &\cdot \overline{\varphi_P\Big(u_0+q^{\mu_1-\mu_0}sn, T_q((m+sq^{\mu_1})n)\Big)}. \end{aligned}$$

De mÃªme que dans [MR15], on peut dire en utilisant le Lemme A.3.4 avec l'expression $A_{q^{\mu_0-\mu_2},q^{\mu_2-\mu_0+2\rho}}$ donnée en (A.22) avec le choix $H = q^{\mu_2-\mu_0+2\rho}$ (pour simplifier la rédaction, nous conserverons la notation H tant que les calculs ne nécessitent pas la valeur $H = q^{\mu_2-\mu_0+2\rho}$ choisie), que

$$S_3(r,s) = S_4(r,s) + O(\max(\log q^{\mu_0}, \tau(q^{\mu_0}))q^{\mu+\nu-2\rho}), \tag{2.67}$$

avec

$$\begin{aligned} S_4(r,s) = \sum_{m\in I_2(M,s)} \sum_n \sum_{0\le u_0,u_1<q^{\mu_2-\mu_0}} \sum_{|h_0|\le H} a_{h_0}\left(q^{\mu_0-\mu_2},H\right) e\left(h_0\frac{mn}{q^{\mu_2}} - h_0\frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ \cdot \sum_{|h_1|\le H} a_{h_1}(q^{\mu_0-\mu_2},H) e\left(h_1\frac{mn+mr}{q^{\mu_2}} - h_1\frac{u_1}{q^{\mu_2-\mu_0}}\right) \varphi_P\Big(u_0, T_q(mn)\Big) \\ \cdot \varphi_P\Big(u_1 + q^{\mu_1-\mu_0}sn + q^{\mu_1-\mu_0}sr, T_q((m+sq^{\mu_1})(n+r))\Big) \\ \cdot \overline{\varphi_P\Big(u_1, T_q(mn+mr)\Big)\varphi_P\Big(u_0+q^{\mu_1-\mu_0}sn, T_q((m+sq^{\mu_1})n)\Big)}. \end{aligned}$$

En écrivant $u_0 + q^{\mu_1-\mu_0}sn \equiv u_2 \bmod q^{\mu_2-\mu_0}$ et $u_1 + q^{\mu_1-\mu_0}sn + q^{\mu_1-\mu_0}sr \equiv u_3 \bmod q^{\mu_2-\mu_0}$, nous avons :

$$\begin{aligned} S_4(r,s) = \sum_{m\in I_2(M,s)} \sum_n \sum_{0\le u_0,u_1<q^{\mu_2-\mu_0}} \sum_{|h_0|\le H} a_{h_0}\left(q^{\mu_0-\mu_2},H\right) e\left(h_0\frac{mn}{q^{\mu_2}} - h_0\frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ \cdot \sum_{|h_1|\le H} a_{h_1}(q^{\mu_0-\mu_2},H) e\left(h_1\frac{mn+mr}{q^{\mu_2}} - h_1\frac{u_1}{q^{\mu_2-\mu_0}}\right) \sum_{0\le u_2,u_3<q^{\mu_2-\mu_0}} \frac{1}{q^{2(\mu_2-\mu_0)}} \\ \cdot \sum_{0\le h_2,h_3<q^{\mu_2-\mu_0}} e\left(h_2\frac{u_0+q^{\mu_1-\mu_0}sn-u_2}{q^{\mu_2-\mu_0}}\right) e\left(h_3\frac{u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr-u_3}{q^{\mu_2-\mu_0}}\right) \\ \cdot \varphi_P\Big(u_3, T_q((m+sq^{\mu_1})(n+r))\Big)\overline{\varphi_P\Big(u_1, T_q(mn+mr)\Big)} \\ \cdot \overline{\varphi_P\Big(u_2, T_q((m+sq^{\mu_1})n)\Big)}\varphi_P\Big(u_0, T_q(mn)\Big). \end{aligned}$$

Nous rappelons que nous pouvons supposer $T_q(mn) = T_q((m+sq^{\mu_1})(n+r))$; mais comme

$$q^{T_q(m)} \le m < q^{T_q(m)+1}, \quad q^{T_q(n)} \le n < q^{T_q(n)+1} \Rightarrow q^{T_q(m)+T_q(n)} \le mn < q^{T_q(m)+T_q(n)+2},$$

ceci veut dire $T_q(m)T_q(n) \le T_q(mn) \le T_q(m)T_q(n)+1$. Comme m et n sont pris de sorte que

$$q^{\mu-2} \le M/q \le m < M < q^{\mu}$$

et

$$q^{\nu-2} \le N/q \le n < N < q^{\nu},$$

nous avons

$$\mu+\nu-4 \le T_q(mn) \le \mu+\nu-1,$$

ce qui fait qu'en posant

$$\widetilde{\varphi_P}(h,y) := \frac{1}{q^{\mu_2-\mu_0}} \sum_{0\le u<q^{\mu_2-\mu_0}} \varphi_P(u,y) e\left(\frac{-uh}{q^{\mu_2-\mu_0}}\right),$$

nous avons l'écriture suivante, toujours si $m \in I_2(M,s)$:

$$\begin{aligned} S_4(r,s) &= q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_0|\le H} a_{h_0}\left(q^{\mu_0-\mu_2},H\right) \sum_{|h_1|\le H} a_{h_1}(q^{\mu_0-\mu_2},H) \\ &\cdot \sum_{0\le h_2,h_3<q^{\mu_2-\mu_0}} e\left(\frac{h_3 sr}{q^{\mu_1-\mu_0}}\right) \widetilde{\varphi_P}\big(h_3,k\big)\overline{\widetilde{\varphi_P}(h_3-h_1,k)\widetilde{\varphi_P}(-h_2,k)}\widetilde{\varphi_P}(h_0-h_2,k) \\ &\cdot \sum_{\substack{m,n \\ T_q(mn)=k}} e\left(h_0\frac{mn}{q^{\mu_2}} + h_1\frac{mn+mr}{q^{\mu_2}} + h_2\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}} + h_3\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}}\right). \end{aligned}$$

Nous pouvons remarquer que les variables de $\widetilde{\varphi_P}$ sont "indépendantes". Nous séparons ici la double somme sur h_0, h_1, $S_4(r,s)$ en deux sommes : $S_4'(r,s)$ qui correspond au cas où $h_0+h_1=0$, qui consiste en la contribution principale (du fait que $e(0)=1$) et $S_4''(r,s)$ qui rassemble les autres termes. Dans [MR15], Mauduit et Rivat traitent le cas $S_4'(r,s)$ en sommant d'abord sur n puis sur m et utilisent que dans ce cas les deux sommations sont indépendantes (puisque h_0+h_1, le terme les reliant, est nul). Nous ne pouvons pas appliquer leur méthode textuellement, car mÃªme dans ce cas m et n sont reliés par la taille.

Plus précisément, nous avons

$$\sum_{M/q\le m<M} \sum_{\substack{N/q\le n<N \\ T_q(mn)=k}} = \sum_{M/q\le m<M} \sum_{\substack{N/q\le n<N \\ q^k/m\le n<q^{k+1}/m}} = \sum_{N/q\le n<N} \sum_{\substack{M/q\le m<M \\ q^k/n\le m<q^{k+1}/n}}. \tag{2.68}$$

Nous allons commencer par estimer $S_4''(r,s)$, dont le contrôle est le plus proche de [MR15].

2.7.1 Estimation de $S_4''(r,s)$

Le fait que $h_0+h_1\neq 0$ entraÃ®ne que la sommation sur n fera apparaÃ®tre un terme en sinus, et donc la sommation sera naturellement petite. Nous pouvons nous permettre de contrôler le reste de manière relativement triviale.

Passant la valeur absolue à l'intérieur, nous avons, si la sommation sur m se fait sur $I_2(M,s)$,

$$\begin{aligned} S_4''(r,s) &\ll \sum_{k=\mu+\nu-4}^{\mu+\nu-1} q^{2(\mu_2-\mu_0)} \sum_{|h_0|\le H} \sum_{h_1\neq -h_0} \left|a_{h_0}\left(q^{\mu_0-\mu_2},H\right)\right| \left|a_{h_1}\left(q^{\mu_0-\mu_2},H\right)\right| \\ &\cdot \sum_{0\le h_3<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}\big(h_3,k\big)\widetilde{\varphi_P}(h_3-h_1,k)\right| \sum_{0\le h_2<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}(-h_2,k)\widetilde{\varphi_P}(h_0-h_2,k)\right| \\ &\cdot \left|\sum_{\substack{m,n \\ T_q(mn)=k}} e\left(h_0\frac{mn}{q^{\mu_2}} + h_1\frac{mn+mr}{q^{\mu_2}} + h_2\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}} + h_3\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}}\right)\right|. \end{aligned}$$

Soit $k \in \{\mu+\nu-4, \mu+\nu-1\}$ fixé, nous traitons d'abord la sommation sur m et n comme suit :

$$\left| \sum_{m\in I_2(M,s)} \sum_{\substack{N/q\le n<N \\ T_q(mn)=k}} e\left(h_0\frac{mn}{q^{\mu_2}} + h_1\frac{mn+mr}{q^{\mu_2}} + h_2\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}} + h_3\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}}\right)\right|$$

$$= \left| \sum_{N/q\le n<N} e\Big((h_2+h_3)q^{\mu_1-\mu_2}sn\Big) \sum_{m\in I_2(M,s)\cap\left[\frac{q^k}{n},\frac{q^{k+1}}{n}\right)} e\left(m\left[\frac{n(h_0+h_1)}{q^{\mu_2}} + \frac{h_1 r}{q^{\mu_2}}\right]\right)\right|$$

et comme $I_2(M,s) \subseteq [M/q, M) \subseteq [q^{\mu-2}, q^\mu)$, la dernière ligne est

$$\begin{aligned}
&\le \sum_{N/q\le n<N} \min\left(\left|[M/q, M)\cap\left[\frac{q^k}{n}, \frac{q^{k+1}}{n}\right)\right|, \left|\sin\pi\frac{(h_0+h_1)n+h_1 r}{q^{\mu_2}}\right|^{-1}\right)\\
&\le \sum_{q^{\nu-1}\le n<q^\nu} \min\left(q^\mu, \left|\sin\pi\frac{(h_0+h_1)n+h_1 r}{q^{\mu_2}}\right|^{-1}\right)\\
&\ll \lceil q^{\nu-\mu_2}\rceil((h_0+h_1, q^{\mu_2})q^\mu + q^{\mu_2}\log q^{\mu_2}),
\end{aligned}$$

par le Lemme A.2.10. Mais $|h_0+h_1| \le 2H$ et donc

$$\sum_{q^{\nu-1}\le n<q^\nu} \min\left(q^\mu, \left|\sin\pi\frac{(h_0+h_1)n+h_1 r}{q^{\mu_2}}\right|^{-1}\right) \ll \lceil q^{\nu-\mu_2}\rceil(Hq^\mu + q^{\mu_2}\log q^{\mu_2}),$$

mais en ayant choisi $H = q^{\mu_2-\mu_0+2\rho}$, nous avons $Hq^\mu \ge q^{\mu+\mu_2-\mu_0} \ge q^{\mu_2}$, et donc

$$\sum_{q^{\nu-1}\le n<q^\nu} \min\left(q^\mu, \left|\sin\pi\frac{(h_0+h_1)n+h_1 r}{q^{\mu_2}}\right|^{-1}\right) \ll \lceil q^{\nu-\mu_2}\rceil Hq^\mu\log q^{\mu_2}.$$

Par orthogonalité des caractères, nous avons pour tout k et y :

$$\sum_{0\le h<q^{\mu_2-\mu_0}} |\widetilde{\varphi_P}(h+y,k)|^2 = 1 \tag{2.69}$$

et nous obtenons donc par l'inégalité de Cauchy-Schwarz :

$$\begin{aligned}
&\sum_{0\le h_3<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}\Big(h_3,k\Big)\widetilde{\varphi_P}(h_3-h_1,k)\right|\\
&\le \left(\sum_{0\le h_3<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}\Big(h_3,k\Big)\right|^2\right)^{1/2}\left(\sum_{0\le h_3<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}(h_3-h_1,k)\right|^2\right)^{1/2} \le 1
\end{aligned}$$

et de manière similaire

$$\sum_{0\le h_2<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}(-h_2,k)\widetilde{\varphi_P}(h_0-h_2,k)\right| \le 1.$$

De plus, d'après (A.23) et le choix de H :

$$\sum_{|h|\le H}|a_h(q^{\mu_0-\mu_2},H)|\le\sum_{|h|\le q^{\mu_2-\mu_0}}\frac{1}{q^{\mu_2-\mu_0}}+\sum_{q^{\mu_2-\mu_0}<|h|\le H}\frac{1}{\pi|h|}\ll\log(H/q^{\mu_2-\mu_0})=\log q^{\rho}.$$

Ainsi nous avons

$$|S_4''(r,s)|\ll(\log q)^2\rho^2q^{2(\mu_2-\mu_0)}\lceil q^{\nu-\mu_2}\rceil Hq^{\mu}\log q^{\mu_2},$$

et avec le choix $H=q^{\mu_2-\mu_0+2\rho}$, et comme $\lceil x\rceil\le x+1$,

$$|S_4''(r,s)|\ll(\log q)^3(\mu+\nu)^3q^{\mu+\nu+3(\mu_2-\mu_0)+2\rho}(q^{-\mu_2}+q^{-\nu}). \tag{2.70}$$

2.7.2 Estimation de $S_4'(r,s)$

Nous avons, par définition, puisque $h_0+h_1=0$:

$$\begin{aligned}S_4'(r,s)=q^{2(\mu_2-\mu_0)}&\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{|h_1|\le H}a_{h_1}\left(q^{\mu_0-\mu_2},H\right)a_{-h_1}\left(q^{\mu_0-\mu_2},H\right)\\&\cdot\sum_{0\le h_2,h_3<q^{\mu_2-\mu_0}}e\left(\frac{h_3sr}{q^{\mu_2-\mu_1}}\right)\widetilde{\varphi_P}\Big(h_3,k\Big)\overline{\widetilde{\varphi_P}(h_3-h_1,k)\widetilde{\varphi_P}(-h_2,k)}\widetilde{\varphi_P}(-h_1-h_2,k)\\&\cdot\sum_{m\in I_2(M,s)}\sum_{\substack{N/q\le n<N\\T_q(mn)=k}}e\left(h_1\frac{mr}{q^{\mu_2}}+h_2\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}}+h_3\frac{q^{\mu_1-\mu_0}sn}{q^{\mu_2-\mu_0}}\right).\end{aligned}$$

Posons $h=h_2+h_3$, de sorte à unifier les termes en n. Ceci nous donne

$$\begin{aligned}S_4'(r,s)\ll q^{2(\mu_2-\mu_0)}&\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{|h_1|\le H}\left|a_{h_1}\left(q^{\mu_0-\mu_2},H\right)\right|^2\\&\sum_{0\le h<2q^{\mu_2-\mu_0}}\sum_{0\le h_3<q^{\mu_2-\mu_0}}\left|\widetilde{\varphi_P}\Big(h_3,k\Big)\widetilde{\varphi_P}(h_3-h_1,k)\widetilde{\varphi_P}(h_3-h,k)\widetilde{\varphi_P}(h_3-h_1-h,k)\right|\\&\left|\sum_{m\in I_2(M,s)}\sum_{\substack{q^{\nu-1}\le n<q^{\nu}\\T_q(mn)=k}}e\left(m\frac{h_1r}{q^{\mu_2}}+n\frac{sh}{q^{\mu_2-\mu_1}}\right)\right|.\end{aligned}$$

Il s'agit à présent de rendre les lignes indépendantes les unes des autres. Si nous posons

$$S_6(h,h_1,k)=\sum_{0\le h_3<q^{\mu_2-\mu_0}}\left|\widetilde{\varphi_P}\Big(h_3,k\Big)\widetilde{\varphi_P}(h_3-h_1,k)\widetilde{\varphi_P}(h_3-h,k)\widetilde{\varphi_P}(h_3-h_1-h,k)\right|$$

par l'inégalité de Cauchy-Schwarz nous avons :

$$\begin{aligned}|S_6(h,h_1,k)|&\le\left(\sum_{0\le h_3<q^{\mu_2-\mu_0}}\left|\widetilde{\varphi_P}\Big(h_3,k\Big)\widetilde{\varphi_P}(h_3-h_1,k)\right|^2\right)^{1/2}\\&\qquad\cdot\left(\sum_{0\le h_3<q^{\mu_2-\mu_0}}|\widetilde{\varphi_P}(h_3-h,k)\widetilde{\varphi_P}(h_3-h_1-h,k)|^2\right)^{1/2}\\&\le\sum_{0\le h_3<q^{\mu_2-\mu_0}}\left|\widetilde{\varphi_P}\Big(h_3,k\Big)\widetilde{\varphi_P}(h_3-h_1,k)\right|^2=:S_6'(h_1,k)\end{aligned}$$

par $q^{\mu_2-\mu_0}$ périodicité. Nous avons alors :

$$S_4'(r,s) \ll q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2},H\right)\right|^2 S_6'(h_1,k) \cdot \sum_{1\leq h<2q^{\mu_2-\mu_0}} \left| \sum_{m\in I_2(M,s)} \sum_{\substack{N/q\leq n<N \\ T_q(mn)=k}} e\left(m\frac{h_1 r}{q^{\mu_2}}+n\frac{sh}{q^{\mu_2-\mu_1}}\right)\right|.$$

Nous constatons qu'il y a essentiellement deux termes : ceux où n a une contribution dans l'argument de la somme d'exponentielles ($q^{\mu_2-\mu_1} \nmid hs$) et les autres :

$$\sum_{1\leq s<S} |S_4'(r,s)| \ll \sum_{\substack{1\leq s<S \\ 0\leq h<2q^{\mu_2-\mu_0} \\ q^{\mu_2-\mu_1}\mid hs}} S_5(r,h) + \sum_{\substack{1\leq s<S \\ 0\leq h<2q^{\mu_2-\mu_0} \\ q^{\mu_2-\mu_1}\nmid hs}} S_5'(r,h,s), \tag{2.71}$$

avec

$$S_5(r,h) := q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2},H\right)\right|^2 S_6'(h_1,k) \left| \sum_{\substack{m,n \\ T_q(mn)=k}} e\left(m\frac{h_1 r}{q^{\mu_2}}\right)\right|,$$

et

$$S_5'(r,h,s) := q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2},H\right)\right|^2 S_6'(h_1,k) \left| \sum_{\substack{m,n \\ T_q(mn)=k}} e\left(m\frac{h_1 r}{q^{\mu_2}}+n\frac{hs}{q^{\mu_2-\mu_1}}\right)\right|$$

où la sommation sur m se fait sur l'intervalle $I_2(M,s)$.

Les termes où n a une grande contribution (c'est-à-dire ceux où l'argument n'est pas altéré, donc maximal) sont les plus faciles à traiter. D'après le Lemme 2.6.3, nous avons

$$S_5'(r,h,s) \ll q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2},H\right)\right|^2 \cdot S_6'(h_1,k) q^{\mu_2-\mu_1} \left(Sq^{\mu_1-\mu_0}q^{\mu_2-\mu_1}\right)^{1/2} q^{\frac{7}{8}(\mu+\nu)}.$$

Cependant

$$\sum_{0\leq h_1<q^{\mu_2-\mu_0}} S_6'(h_1,k) = \sum_{0\leq h_1<q^{\mu_2-\mu_0}} \sum_{0\leq h_3<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}\big(h_3,k\big)\widetilde{\varphi_P}(h_3-h_1,k)\right|^2 = 1. \tag{2.72}$$

Nous séparons donc $S_5'(r,h,s)$ selon $|h_1| \leq q^{\mu_2-\mu_0}$, qu'on nomme $S_{7,1}(r,h,s)$ et selon $q^{\mu_2-\mu_0} < |h_1| \leq H$ qu'on nomme $S_{7,1}'(r,h,s)$. Par (2.72), en utilisant $|a_{h_1}(q^{\mu_0-\mu_2},H)| \leq q^{\mu_0-\mu_2}$, nous avons l'estimation

$$S_{7,1}(r,h,s) \ll q^{\mu_2-\mu_1}\left(Sq^{\mu_1-\mu_0}q^{\mu_2-\mu_1}\right)^{1/2} q^{\frac{7}{8}(\mu+\nu)} \ll q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{1}{2}(\mu_2-\mu_0)} S^{1/2}. \tag{2.73}$$

Si $q^{\mu_2-\mu_0} < |h_1| \leq H$, alors $|a_{h_1}(q^{\mu_0-\mu_2}, H)| \leq \frac{1}{\pi|h_1|}$, et donc

$$S'_{7,1}(r,h,s) \ll q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{q^{\mu_2-\mu_0}\leq|h_1|\leq H} \frac{S'_6(h_1,k)}{|h_1|^2} q^{\frac{7}{8}(\mu+\nu)} q^{\mu_2-\mu_1} \left(Sq^{\mu_1-\mu_0}q^{\mu_2-\mu_1}\right)^{1/2}.$$

Mais $S'_6(h_1,k)$ est $q^{\mu_2-\mu_0}$ périodique en h_1. Nous pouvons séparer la sommation en $jq^{\mu_2-\mu_0} \leq |h| \leq (j+1)q^{\mu_2-\mu_0}$ avec $1 \leq j \leq H/q^{\mu_2-\mu_0}$ et borner $|h_1|^{-2}$ par $j^{-2}q^{2(\mu_0-\mu_2)}$. Ceci nous mène à dire que

$$\begin{aligned} &S'_{7,1}(r,h,s) \\ &\ll q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+2(\mu_2-\mu_0)} \left(Sq^{\mu_1-\mu_0}\right)^{1/2} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{j\geq 1} \frac{1}{j^2 q^{2(\mu_2-\mu_0)}} \sum_{0\leq|h_1|<q^{\mu_2-\mu_0}} S'_6(h_1,k) \\ &\ll q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{1}{2}(\mu_2-\mu_0)} S^{1/2}, \end{aligned}$$

et par (2.73), nous obtenons

$$S'_5(r,h,s) \ll q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{1}{2}(\mu_2-\mu_0)} S^{1/2},$$

ou encore

$$\sum_{\substack{1\leq s<S \\ 0\leq h<q^{\mu_2-\mu_0} \\ q^{\mu_2-\mu_1}\nmid hs}} S'_5(r,h,s) \ll q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{3}{2}(\mu_2-\mu_0)} S^{3/2}. \tag{2.74}$$

À présent contrôlons $S_5(r,h)$ où on rappelle

$$\begin{aligned} &S_5(r,h) := \\ &q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 S'_6(h_1,k) \left| \sum_{m\in I_2(M,s)} \sum_{\substack{N/q\leq n<N \\ T_q(mn)=k}} e\left(h_1 \frac{mr}{q^{\mu_2}}\right)\right|. \end{aligned}$$

Nous utilisons le Lemme 2.6.2 pour pouvoir dire

$$\left| \sum_{m\in I_2(M,s)} \sum_{\substack{N/q\leq n<N \\ T_q(mn)=k}} e\left(h_1 \frac{mr}{q^{\mu_2}}\right)\right| \ll q^{\nu} \min\left(q^{\mu}, \left|\sin \pi \frac{h_1 r}{q^{\mu_2}}\right|^{-1}\right), \tag{2.75}$$

ce qui amène à

$$\begin{aligned} &S_5(r,h) \\ &\ll q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 S'_6(h_1,k) q^{\nu} \min\left(q^{\mu}, \left|\sin \pi \frac{h_1 r}{q^{\mu_2}}\right|^{-1}\right). \end{aligned}$$

Notons que $|h_1 r| \leq HR = q^{\mu_2-\mu_0+3\rho} = q^{\mu_2-\mu+6\rho+2\rho'} \leq q^{\mu_2-\mu+8\rho}$. Si l'on suppose

$$8\rho < \mu, \tag{2.76}$$

nous avons $|h_1 r| < q^{\mu_2}$ et donc $\left|\sin \pi \frac{h_1 r}{q^{\mu_2}}\right|^{-1} \leq \frac{q^{\mu_2}}{r|h_1|}$, ce qui donne

$$S_5(r,h) \ll q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 S_6'(h_1,k) q^{\nu} \min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right).$$

Nous séparons cette dernière somme en $S_{7,2}(r,h)$, $S'_{7,2}(r,h)$ et $S''_{7,2}(r,h)$ selon $|h_1| \leq q^{2\rho}$, $q^{2\rho} < |h_1| \leq q^{\mu_2-\mu_0}$ et $q^{\mu_2-\mu_0} < |h_1| \leq H$. En effet, si $|h_1| < q^{\rho}$, $\min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right) = q^{\mu}$, alors que $\min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right) = \frac{q^{\mu_2}}{r|h_1|}$ sinon. Notons ici un enjeu dans le fait que la sommation sur n soit maximale.

Nous traitons d'abord les sommes $S'_{7,2}(r,h)$ et $S''_{7,2}(r,h)$ pour lesquelles la méthode ne diffère pas beaucoup des sommes $S_{7,1}(r,h,s)$ et $S'_{7,1}(r,h,s)$. Plus précisément nous avons

$$\begin{aligned}
S'_{7,2}(r,h) &:= q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{q^{2\rho}<|h_1|\leq q^{\mu_2-\mu_0}} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 \\
&\qquad \cdot S_6'(h_1,k) q^{\nu} \min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right) \\
&= q^{\nu+2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{q^{2\rho}<|h_1|\leq q^{\mu_2-\mu_0}} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 S_6'(h_1,k) \frac{q^{\mu_2}}{r|h_1|} \\
&\ll \frac{q^{\nu+\mu_2}}{r} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{q^{2\rho}<|h_1|\leq q^{\mu_2-\mu_0}} \frac{S_6'(h_1,k)}{|h_1|} \\
&\ll \frac{q^{\nu+\mu_2-2\rho}}{r} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{0<|h_1|\leq q^{\mu_2-\mu_0}} S_6'(h_1,k),
\end{aligned}$$

ce qui nous mène à

$$S'_{7,2}(r,h) \ll \frac{q^{\nu+\mu}}{r}. \tag{2.77}$$

A présent

$$\begin{aligned}
S''_{7,2}(r,h) &:= q^{2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{q^{\mu_2-\mu_0}<|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 S_6'(h_1) q^{\nu} \min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right) \\
&= q^{\nu+2(\mu_2-\mu_0)} \sum_{k=\mu+\nu-4}^{\mu+\nu-1} \sum_{q^{\mu_2-\mu_0}<|h_1|\leq H} \left|a_{h_1}\left(q^{\mu_0-\mu_2}, H\right)\right|^2 S_6'(h_1) \frac{q^{\mu_2}}{r|h_1|}.
\end{aligned}$$

Nous utilisons la majoration $|a_{h_1}(q^{\mu_0-\mu_2}, H)| \leq \frac{1}{\pi|h_1|}$ et le mÃªme découpage que

pour $S'_{7,1}(r,h)$ pour dire

$$\begin{aligned}
S''_{7,2}(r,h) &\ll q^{\nu+2(\mu_2-\mu_0)}\frac{q^{\mu_2}}{r}\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{q^{\mu_2-\mu_0}<|h_1|\leq H}\frac{S'_6(h_1,k)}{|h_1|^3}\\
&\ll q^{\nu+2(\mu_2-\mu_0)}\frac{q^{\mu_2}}{r}\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{j\geq 1}\frac{1}{j^3q^{3(\mu_2-\mu_0)}}\sum_{0\leq h_1<q^{\mu_2-\mu_0}}S'_6(h_1,k)\\
&\ll q^{\nu-(\mu_2-\mu_0)}\frac{q^{\mu_2}}{r}\\
&\ll \frac{q^{\nu+\mu_0}}{r},
\end{aligned}$$

et finalement

$$S''_{7,2}(r,h) \ll \frac{q^{\nu+\mu}}{r}. \tag{2.78}$$

Nous pouvons alors écrire

$$\begin{aligned}
\frac{1}{RS}\sum_{1\leq r<R}\sum_{\substack{1\leq s<S\\0\leq h<q^{\mu_2-\mu_0}\\q^{\mu_2-\mu_1}|hs}}\Big(S'_{7,2}(r,h)+S''_{7,2}(r,h)\Big) &\ll \frac{1}{RS}\sum_{1\leq r<R}\sum_{\substack{1\leq s<S\\0\leq h<q^{\mu_2-\mu_0}\\q^{\mu_2-\mu_1}|hs}}\frac{q^{\nu+\mu}}{r}\\
&\ll q^{\mu+\nu}\frac{\log R}{R}\frac{\#\{1\leq s<S, 0\leq h<q^{\mu_2-\mu_0}: q^{\mu_2-\mu_1}|hs\}}{S}\\
&\ll q^{\mu+\nu}\frac{\log R}{R}\frac{\#\{0\leq k<q^{\mu_2-\mu_0}S: q^{\mu_2-\mu_1}|k\}}{S}\\
&\ll q^{\mu+\nu}\frac{\log R}{R}\frac{\#\{0\leq q^{\mu_2-\mu_1}k'<q^{\mu_2-\mu_0}S\}}{S}\\
&\ll q^{\mu+\nu}\frac{\log R}{R}\frac{q^{\mu_2-\mu_0-\mu_2+\mu_1}S}{S},
\end{aligned}$$

ce qui revient à dire

$$\frac{1}{RS}\sum_{1\leq r<R}\sum_{\substack{1\leq s<S\\0\leq h<q^{\mu_2-\mu_0}\\q^{\mu_2-\mu_1}|hs}}\Big(S'_{7,2}(r,h)+S''_{7,2}(r,h)\Big) \ll q^{\mu+\nu+\mu_1-\mu_0}\frac{\log R}{R}. \tag{2.79}$$

Traitons maintenant le cas $S_{7,2}(h,r,s)$. Nous rappelons que

$$\begin{aligned}
S_{7,2}(h,r) &:= q^{2(\mu_2-\mu_0)}\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{|h_1|\leq q^{2\rho}}\Big|a_{h_1}\Big(q^{\mu_0-\mu_2},H\Big)\Big|^2 S'_6(h_1,k)q^{\nu}\min\left(q^{\mu},\frac{q^{\mu_2}}{r|h_1|}\right)\\
&\ll q^{\mu+\nu}\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{|h_1|\leq q^{2\rho}}S'_6(h_1,k)\\
&\ll q^{\mu+\nu}\sum_{k=\mu+\nu-4}^{\mu+\nu-1}\sum_{|h_1|\leq q^{2\rho}}\sum_{0\leq h_3<q^{\mu_2-\mu_0}}\Big|\widetilde{\varphi_P}\Big(h_3,k\Big)\widetilde{\varphi_P}(h_3-h_1,k)\Big|^2.
\end{aligned}$$

Soit

$$P(\mu+\nu+1)\leq\frac{1}{3}(\mu_1-\mu_0) \tag{2.80}$$

Nous utilisons ici le Lemme 2.6.10 avec $\lambda = \mu_2 - \mu_0 - 2\rho$ pour pouvoir dire

$$\sum_{|h_1|\leq q^{2\rho}} \sum_{0\leq h_3<q^{\mu_2-\mu_0}} \left|\widetilde{\varphi_P}\big(h_3,k\big)\ \widetilde{\varphi_P}(h_3-h_1,k)\right|^2 \\ \ll q^{\frac{1}{2}(\mu_1-\mu_0-\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3P(k)}{4}}(\log q^{\mu_2-\mu_1})^2,$$

donc nous obtenons par croissance de P :

$$\frac{1}{RS}\sum_{1\leq r<R}\sum_{\substack{1\leq s<S\\0\leq h<q^{\mu_2-\mu_0}\\q^{\mu_2-\mu_1}\nmid hs}} S_7(h,r) \ll q^{(\mu+\nu)+\frac{1}{2}(\mu_1-\mu_0-\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}(\log q^{\mu_2-\mu_1})^2 \\ \cdot\frac{\#\{1\leq s<S, 0\leq h<q^{\mu_2-\mu_0}: q^{\mu_2-\mu_1}|hs\}}{S},$$

ce qui nous permet de dire

$$\frac{1}{RS}\sum_{1\leq r<R}\sum_{\substack{1\leq s<S\\0\leq h<q^{\mu_2-\mu_0}\\q^{\mu_2-\mu_1}|hs}} S_7(h,r) \ll (\log q^{\mu_2-\mu_1})^2 q^{(\mu+\nu)+\frac{3}{2}(\mu_1-\mu_0)-\frac{1}{2}\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}. \tag{2.81}$$

En posant $S = q^{2\rho}$, par les équations (2.71), (2.74), (2.79) et (2.81), nous avons

$$\begin{aligned}\frac{1}{RS}\sum_{1\leq r<R}\sum_{1\leq s<S}|S_4'(r,s)| \ll&(\log q^{\mu_2-\mu_1})^2 q^{(\mu+\nu)+\frac{3}{2}(\mu_1-\mu_0)-\frac{1}{2}\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+q^{\mu+\nu+\mu_1-\mu_0-\rho}\log q^\rho\\ &+q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{3}{2}(\mu_2-\mu_0)+\rho}.\end{aligned}$$

Ceci nous donne en utilisant (2.60), (2.62), (2.66), (2.67) et (2.70) :

$$\begin{aligned}\frac{1}{RS}\sum_{1\leq r<R}\sum_{1\leq s<S}|S_2'(r,s)| \ll&(\log q^{\mu_2-\mu_1})^2 q^{(\mu+\nu)+\frac{3}{2}(\mu_1-\mu_0)-\frac{1}{2}\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+q^{\mu+\nu+\mu_1-\mu_0-\rho}\log q^\rho\\ &+q^{\frac{7}{8}(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{3}{2}(\mu_2-\mu_0)+\rho}\\ &+(\log q)^3(\mu+\nu)^3q^{\mu+\nu+3(\mu_2-\mu_0)+2\rho}(q^{-\mu_2}+q^{-\nu})\\ &+\max(\log q^{\mu_0},\tau(q^{\mu_0}))q^{\mu+\nu-2\rho}\\ &+\max(\tau(q),\log q)\mu_2^{\omega(q)}q^{\mu+\nu+\mu_0-\mu_1+P(\mu_2+1)}\\ &+q^{\mu+\nu-\rho}(\mu+\nu).\end{aligned}$$

Puis par (2.54), (2.56) et (2.59) :

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll{}& (\log q^{\mu_2-\mu_1})^2 q^{4(\mu+\nu)+\frac{3}{2}(\mu_1-\mu_0)-\frac{1}{2}\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+ q^{4(\mu+\nu)+\mu_1-\mu_0-\rho}\log q^\rho\\ &+ q^{(4-\frac{1}{8})(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{3}{2}(\mu_2-\mu_0)+\rho}\\ &+ (\log q)^3(\mu+\nu)^3 q^{4(\mu+\nu)+3(\mu_2-\mu_0)+2\rho}(q^{-\mu_2}+q^{-\nu})\\ &+ \max(\log q^{\mu_0},\tau(q^{\mu_0}))q^{4(\mu+\nu)-2\rho}\\ &+ \max(\tau(q),\log q)\mu_2^{\omega(q)}q^{4(\mu+\nu)+\mu_0-\mu_1+P(\mu_2+1)}\\ &+ q^{4(\mu+\nu)-\rho}(\mu+\nu)+q^{4(\mu+\nu)-2\rho}+q^{4(\mu+\nu)-2\rho}.\end{aligned}$$

Nous faisons quelques réductions élémentaires pour pouvoir dire

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll{}& (\log q^{\mu_2-\mu_1})^2 q^{4(\mu+\nu)+\frac{3}{2}(\mu_1-\mu_0)-\frac{1}{2}\gamma_P(\mu_2-\mu_0-2\rho,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+ q^{(4-\frac{1}{8})(\mu+\nu)+\frac{3}{2}(\mu_2-\mu_1)+\frac{3}{2}(\mu_2-\mu_0)+\rho}\\ &+ (\log q)^3(\mu+\nu)^3 q^{4(\mu+\nu)+3(\mu_2-\mu_0)+2\rho}(q^{-\mu_2}+q^{-\nu})\\ &+ \max(\log q^{\rho},\log q^{\mu_0},\tau(q^{\mu_0}),(\mu+\nu))q^{4(\mu+\nu)+\mu_1-\mu_0-\rho}\\ &+ \max(\tau(q),\log q)\mu_2^{\omega(q)}q^{4(\mu+\nu)+\mu_0-\mu_1+P(\mu_2+1)}.\end{aligned}$$

Nous rappelons à présent que nous avons posé $\mu_2=\mu+2\rho$, $\mu_1=\mu-3\rho$ et $\mu_0=\mu_1-2\rho'=\mu-3\rho-2\rho'$ de sorte que $\mu_2-\mu_1=5\rho$, $\mu_1-\mu_0=2\rho'$ et $\mu_2-\mu_0=5\rho+2\rho'$, ce qui nous donne, quitte à choisir $2\rho<\nu$ (ce qui sera le cas) :

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll{}& q^{4(\mu+\nu)}\Big[(\log q^{5\rho})^2 q^{\frac{3}{2}(2\rho')-\frac{1}{2}\gamma_P(3\rho+2\rho',\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+ q^{-\frac{1}{8}(\mu+\nu)+\frac{3}{2}(5\rho)+\frac{3}{2}(5\rho+2\rho')+\rho}\\ &+ (\log q)^3(\mu+\nu)^3 q^{3(5\rho+2\rho')+2\rho}(q^{-\mu-2\rho}+q^{-\nu})\\ &+ \max(\log q^{\rho},\log q^{\mu-3\rho-2\rho'},\tau(q^{\mu-3\rho-2\rho'}),(\mu+\nu))q^{2\rho'-\rho}\\ &+ \max(\tau(q),\log q)(\mu+2\rho)^{\omega(q)}q^{-2\rho'+P(\mu+\nu+1)}\Big].\end{aligned}$$

Remarquons à présent que par (2.80), nous avons $P(\mu+\nu+1)\leq 2\rho'/3$. Par ailleurs, comme $\rho\leq\mu$, nous pouvons écrire

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll{}& q^{4(\mu+\nu)}\Big[(\log q^{5\rho})^2 q^{3\rho'-\frac{1}{2}\gamma_P(3\rho+2\rho',\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+ q^{-\frac{1}{8}(\mu+\nu)+16\rho+3\rho'}\\ &+ (\log q)^3(\mu+\nu)^3 q^{17\rho+6\rho'}(q^{-\mu-2\rho}+q^{-\nu})\\ &+ \max\Big(\tau(q^{\mu-3\rho-2\rho'}),\mu+\nu\Big)q^{2\rho'-\rho}\\ &+ \max(\tau(q),\log q)(\mu+2\rho)^{\omega(q)}q^{-\frac{4}{3}\rho'}\Big],\end{aligned}$$

et en nous rappelant que $\rho' \leq \rho$, et que $\gamma_P(l,k)$ est croissante en l, nous avons la simplification suivante :

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll q^{4(\mu+\nu)} \Big[&(\log q^{5\rho})^2 q^{3\rho'-\frac{1}{2}\gamma_P(3\rho,\,\mu+\nu-2)+\frac{3}{4}P(\mu+\nu)}\\ &+ q^{-\frac{1}{8}(\mu+\nu)+19\rho}\\ &+ (\log q)^3(\mu+\nu)^3 q^{23\rho}(q^{-\mu-2\rho}+q^{-\nu})\\ &+ \max\Big(\tau(q^{\mu-3\rho-2\rho'}),\mu+\nu\Big)q^{2\rho'-\rho}\\ &+ \max(\tau(q),\log q)(\mu+2\rho)^{\omega(q)}q^{-\frac{4}{3}\rho'}\Big].\end{aligned}$$

Si nous supposons

$$P(\mu+\nu) \leq \gamma_P(3\rho,\mu+\nu)/3, \tag{2.82}$$

alors par décroissance de $\gamma_P(l,\kappa)$ en κ, nous obtenons

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll q^{4(\mu+\nu)} \Big[&(\log q^{5\rho})^2 q^{3\rho'-\frac{1}{4}\gamma_P(3\rho,\,\mu+\nu-2)}\\ &+ q^{-\frac{1}{8}(\mu+\nu)+19\rho}\\ &+ (\log q)^3(\mu+\nu)^3 q^{23\rho}(q^{-\mu-2\rho}+q^{-\nu})\\ &+ \max\Big(\tau(q^{\mu-3\rho-2\rho'}),\mu+\nu\Big)q^{2\rho'-\rho}\\ &+ \max(\tau(q),\log q)(\mu+2\rho)^{\omega(q)}q^{-\frac{4}{3}\rho'}\Big].\end{aligned}$$

Nous faisons alors le choix de prendre $\rho = \lfloor \frac{\mu}{160} \rfloor = \lfloor \frac{\mu}{20\times 8} \rfloor \leq \frac{\mu}{160} \leq \frac{3}{4\times 160}(\mu+\nu)$ (on voit aisément que ρ vérifie (2.61)).

Ainsi

$$19\rho \leq 21\rho \leq 23\rho \leq \frac{23}{8\times 20}\nu \leq \frac{3\times 23}{4\times 8\times 20}(\mu+\nu).$$

Plus précisément nous obtenons

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll q^{4(\mu+\nu)} \Big[&(\log q^{5\rho})^2 q^{3\rho'-\frac{1}{4}\gamma_P(3\rho,\,\mu+\nu-2)}\\ &+ q^{-\frac{184}{5120}(\mu+\nu)} + (\log q)^3(\mu+\nu)^3 q^{-\frac{139}{160}\mu} + (\log q)^3(\mu+\nu)^3 q^{-\frac{137}{160}\nu}\\ &+ \max\Big(\tau(q^{\mu-3\rho-2\rho'}),\mu+\nu\Big)q^{2\rho'-\rho}\\ &+ \max(\tau(q),\log q)(\mu+2\rho)^{\omega(q)}q^{-\frac{4}{3}\rho'}\Big].\end{aligned}$$

Nous posons alors $\rho' = \lfloor \frac{1}{16}\gamma_P(3\rho,\,\mu+\nu-2))\rfloor \leq \frac{3}{32}\rho$ d'après la Remarque 2.2.1, de sorte que, par (2.51), nous sommes certains que (2.80) est vérifiée, et de plus :

$$\begin{aligned}|S_{II}(\vartheta)|^4 \ll q^{4(\mu+\nu)} \Big[&(\log q^{5\rho})^2 q^{-\frac{1}{16}\gamma_P(3\lfloor\frac{\mu}{160}\rfloor,\,\mu+\nu-2)}\\ &+ q^{-\frac{184}{5120}(\mu+\nu)} + (\log q)^3(\mu+\nu)^3 q^{-\frac{139}{160}\mu} + (\log q)^3(\mu+\nu)^3 q^{-\frac{137}{160}\nu}\\ &+ \max\Big(\tau(q^{\mu-3\rho-2\rho'}),\mu+\nu\Big)q^{-\frac{26}{32}\lfloor\frac{\mu}{160}\rfloor}\\ &+ \max(\tau(q),\log q)(\mu+2\rho)^{\omega(q)}q^{-\frac{4}{3}\lfloor\frac{1}{16}\gamma_P(3\lfloor\frac{\mu}{160}\rfloor,\,\mu+\nu-2)\rfloor}\Big].\end{aligned}$$

Ceci dit, avec la condition (2.50) et les estimations classiques des parties entières, nous pouvons écrire :

$$\begin{aligned}|S_{II}(\vartheta)|^4 &\ll q^{4(\mu+\nu)}\Big[\max\Big(\tau(q),\log q)(\mu+\nu)^{\omega(q)},(\log q^{5\rho})^2\Big)q^{-\frac{1}{16}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu-2)}\\ &\quad+q^{-\frac{184}{5120}(\mu+\nu)}+(\log q)^3(\mu+\nu)^3q^{-\frac{139}{4\times160}(\mu+\nu)}\\ &\quad+(\log q)^3(\mu+\nu)^3q^{-\frac{137}{4\times160}(\nu+\mu)}\\ &\quad+q^{\frac{26}{32}}\max\Big(\tau(q^{\mu-3\rho-2\rho'}),\mu+\nu\Big)q^{-\frac{26}{32\times4\times160}(\mu+\nu)}\Big]\\ &\ll q^{4(\mu+\nu)}q^{\frac{26}{32}}\Big(q^{-\frac{26}{20480}(\mu+\nu)}+q^{-\frac{1}{16}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu-2))}\Big)\\ &\quad\max\Big(\tau(q)(\mu+\nu)^{\omega(q)},\log q(\mu+2\rho)^{\omega(q)}\\ &\qquad,(\log q^{5\rho})^2\tau(q^{\mu-3\rho-2\rho'}),(\log q)^3(\mu+\nu)^3\Big).\end{aligned}$$

Cependant, par la remarque 2.2.1 :

$$\frac{1}{16}\gamma_P\left(\frac{\mu+\nu}{640},\,\mu+\nu-2\right)\leq\frac{\mu+\nu}{160\times32}\leq\frac{26}{20480}(\mu+\nu)$$

et donc finalement :

$$S_{II}(\vartheta)\ll q^{\frac{26}{128}}\Big(\max\Big(\tau(q),(\log q)^3\Big)(\mu+\nu)^{\omega(q)+3}\Big)^{1/4}q^{\mu+\nu-\frac{1}{64}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu-2)}.$$

□

2.8 Fin de l'estimation

Nous avons par la Partie 2.5

$$S_I(\vartheta)\ll(\mu+\nu)^3(\log q)^3q^{\mu+\nu-\frac{1}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)},$$

et par la Partie 2.7

$$S_{II}(\vartheta)\ll q^{\frac{26}{128}}\Big(\max\Big(\tau(q),(\log q)^3\Big)(\mu+\nu)^{\omega(q)+3}\Big)^{1/4}q^{\mu+\nu-\frac{1}{64}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu-2)}.$$

On rappelle que $\gamma_P(l,k)=l\left(1-\dfrac{\log\left(q^{P(k)}-8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(k)\log q}\right)$ est croissante en l et décroissante en k du fait de la Proposition 2.4.4. Ainsi nous pouvons écrire

$$\begin{aligned}S_I(\vartheta)&\ll(\mu+\nu)^3(\log q)^3q^{\mu+\nu-\frac{1}{4}\gamma_P(\frac{1}{3}(\mu+\nu),\mu+\nu)}\\ &\ll(\mu+\nu)^3(\log q)^3q^{\mu+\nu-\frac{1}{4}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu)}\\ &\ll q^{26/128}(\mu+\nu)^{3+\frac{\omega(q)}{4}}\max\Big((\log q)^3,\tau(q)^{1/4}\Big)q^{\mu+\nu-\frac{1}{64}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu)}\end{aligned}$$

et de mÃªme

$$S_{II}(\vartheta)\ll q^{26/128}(\mu+\nu)^{3+\frac{\omega(q)}{4}}\max\Big((\log q)^3,\tau(q)^{1/4}\Big)q^{\mu+\nu-\frac{1}{64}\gamma_P(\frac{\mu+\nu}{640},\mu+\nu)}.$$

Posons $c_1(q) = q^{26/128}\max\left((\log q)^3, \tau(q)^{1/4}\right)(\log q)^{-3-\frac{\omega(q)}{4}}$. En rappelant que $x = q^{\mu+\nu}$, nous pouvons alors utiliser les Lemmes A.1.2 et A.1.3 pour obtenir

$$\left|\sum_{x/q<n\leq x}\Lambda(n)f_P(n)e(\vartheta n)\right| \ll c_1(q)(\log x)^{3+\frac{\omega(q)}{4}}xq^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log x}{\log q}\rfloor)}$$

et

$$\left|\sum_{x/q<n\leq x}\mu(n)f_P(n)e(\vartheta n)\right| \ll c_1(q)(\log x)^{3+\frac{\omega(q)}{4}}xq^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log x}{\log q}\rfloor)}.$$

Il reste à remplacer x par xq^{-k} et sommer sur k. Soit $K\in\mathbb{N}$ tel que $q^K \leq x^{1/4} < q^{K+1}$. Comme $\gamma_P(l,k)$ est croissante en l et décroissante en k, nous avons

$$\begin{aligned}\sum_{k\leq K}xq^{-k}q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log xq^{-k}}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log xq^{-k}}{\log q}\rfloor)} &\leq \sum_{k\leq K}xq^{-k}q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log xq^{-k}}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log x}{\log q}\rfloor)}\\ &\leq \sum_{k\leq K}xq^{-k}q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log xq^{-k}}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log x}{\log q}\rfloor)}\\ &\leq q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x^{3/4}}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log x}{\log q}\rfloor)}\sum_{k\leq K}xq^{-k}\\ &\ll xq^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{120},\lfloor\frac{\log x}{\log q}\rfloor)},\end{aligned}$$

tandis que

$$\begin{aligned}\sum_{k>K}\frac{x}{q^k}q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log xq^{-k}}{\log q}\rfloor\frac{1}{160},\lfloor\frac{\log xq^{-k}}{\log q}\rfloor)} &\leq \sum_{k>K}\frac{x}{q^k}\\ &\ll \frac{x}{q^{K+1}} \ll x^{3/4} \ll xq^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{120},\lfloor\frac{\log x}{\log q}\rfloor)}\end{aligned}$$

et finalement

$$\left|\sum_{n\leq x}\Lambda(n)f_P(n)e(\vartheta n)\right| \ll c_1(q)(\log x)^{3+\frac{\omega(q)}{4}}xq^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{120},\lfloor\frac{\log x}{\log q}\rfloor)} \tag{2.83}$$

et

$$\left|\sum_{n\leq x}\mu(n)f_P(n)e(\vartheta n)\right| \ll c_1(q)(\log x)^{3+\frac{\omega(q)}{4}}xq^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{120},\lfloor\frac{\log x}{\log q}\rfloor)}. \tag{2.84}$$

2.9 Conditions sur P

Nous devons à présent choisir P de sorte que (2.9) et (2.51) et (2.82) soient satisfaites.

Ceci nous donne $P(\mu+\nu+1) \leq \frac{2}{3}\left\lfloor\frac{1}{16}\gamma_P\left(\frac{\mu+\nu}{640},\, \mu+\nu-2\right)\right\rfloor$ et $P(\mu+\nu) \leq \gamma_P(\frac{1}{3}(\mu+\nu),\, \mu+\nu)$.

Comme la fonction P est croissante, que $\lfloor x \rfloor \geq x/2$, et que $\rho \leq \frac{3}{4\times 160}(\mu+\nu)$, les trois équations sont impliquées par

$$P(2(\mu+\nu)) \leq \frac{1}{48}\gamma_P\left(\frac{\mu+\nu}{640}, \mu+\nu\right) \tag{2.85}$$

Constatons que

$$\gamma_P(l,k) = l\left(1 - \frac{\log\left(q^{P(k)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(k)\log q}\right) = -l\frac{\log\left(1 - \frac{8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2}{q^{P(k)}}\right)}{P(k)\log q},$$

et que pour tout $0 \leq x < 1$, nous avons $\log(1-x) \leq -x$, ce qui implique que

$$\gamma_P(l,k) \geq l\frac{8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2}{q^{P(k)}P(k)\log q},$$

et donc il suffit que la fonction P vérifie

$$P(2(\mu+\nu)) \leq \frac{\mu+\nu}{640\times 48}\frac{8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2}{q^{P(\mu+\nu)}P(\mu+\nu)\log q}$$

ou encore

$$P(2x)q^{P(x)}P(x)\log q \leq \frac{x}{640\times 48}8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2. \tag{2.86}$$

et nous constatons que pour tout $0 < c < 1/\log q$, toute fonction $P(x)$ vérifiant $P(x) \leq c\log x$ vérifie (2.86).

Pour que les équations (2.83) et (2.84) ne soient pas triviales, il faut que

$$c_1(q)(\log x)^{3+\frac{\omega(q)}{4}} x q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{120},\lfloor\frac{\log x}{\log q}\rfloor)} = o(x)$$

ce qui revient à dire

$$c_1(q)(\log x)^{3+\frac{\omega(q)}{4}} q^{-\frac{1}{64}\gamma_P(\lfloor\frac{\log x}{\log q}\rfloor\frac{1}{120},\lfloor\frac{\log x}{\log q}\rfloor)} = o(1)$$

ou encore

$$\frac{12+\omega(q)}{4\log q}\log\log x - \frac{1}{64\times 120}\left\lfloor\frac{\log x}{\log q}\right\rfloor\left(1 - \frac{\log\left(q^{P(\lfloor\frac{\log x}{\log q}\rfloor)} - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{P(\lfloor\frac{\log x}{\log q}\rfloor)\log q}\right) \underset{x\to\infty}{\to} -\infty,$$

mais là encore, il suffit que P vérifie

$$\frac{12+\omega(q)}{4\log q}\log\log x - \frac{1}{64\times 120}\left\lfloor\frac{\log x}{\log q}\right\rfloor \cdot \frac{8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2}{q^{P(\lfloor\frac{\log x}{\log q}\rfloor)}P(\lfloor\frac{\log x}{\log q}\rfloor)\log q} \underset{x\to\infty}{\to} -\infty \tag{2.87}$$

et là encore, si $0 < c < 1/\log q$ et si $P(x) < c \log x$, nous avons

$$\frac{12+\omega(q)}{4\log q}\log\log x - \frac{1}{64\times 120}\left\lfloor \frac{\log x}{\log q}\right\rfloor \cdot \frac{8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2}{q^{c\log(\lfloor\frac{\log x}{\log q}\rfloor)}c\log(\lfloor\frac{\log x}{\log q}\rfloor)\log q}$$
$$= \frac{12+\omega(q)}{4\log q}\log\log x - \frac{\left(8\sin\frac{\pi\|\alpha\|}{4}\right)^2}{64\times 120 c\log q}\cdot\frac{1}{\log(\lfloor\frac{\log x}{\log q}\rfloor)}\cdot\left\lfloor\frac{\log x}{\log q}\right\rfloor^{1-c\log q}$$

et comme pour tout $\epsilon > 0$, nous avons $\log\log x = o\left(\frac{(\log x)^\epsilon}{\log\log x}\right)$, (2.87) est vérifiée pour toutes les fonctions $P(x)$ vérifiant $P(x) \leq c\log x$.

2.10 Non automaticité

Dans cette partie, nous montrons que les suites $((-1)^{a_P(n)})_{n\geq 0}$ étudiées ne sont pas automatiques dans le cas $q = 2$. Ceci nous permet d'affirmer que les résultats de ce chapitre ne sont pas recouverts par [Mül16]. La preuve que nous présentons est due à Julien Cassaigne, suite à une volonté de simplifier une preuve initiale.

Soit $P : \mathbb{N} \to \mathbb{N}$ une fonction croissante majorÃ©e par $\log n/\log 2$. Nous allons montrer que l'ensemble E des entiers possÃ©dant un nombre pair de blocs de taille $P(T_2(n))$ "1" consécutifs en base 2 n'est reconnaissable par aucun automate fini.

Supposons que E est reconnu par un automate à k états. Parmi les $k+1$ mots $x_l = 0^{k-l}1^l$, pour l de 0 à k, il y en a donc deux qui conduisent au même état, disons x_i et $x_j, i < j$. Soit m un entier suffisamment grand pour que $P(m) > k$ et $m > P(m) + k$. Soit $y = 1^{P(m)-j}0^{m-P(m)+j-k}$. Alors les mots $x_i \cdot y$ et $x_j \cdot y$ sont deux mots de longueur m qui conduisent au même état, et pourtant le premier code un Ã©lÃ©ment de E (il ne contient aucun bloc de taille $P(m)$) et pas le second (il contient exactement un bloc de taille $P(m)$). Le choix de m est valable puisque $\min(P(m), m - P(m))$ est non majoré dans notre cas.

Chapitre 3

Blocs de grande taille

3.1 Introduction

Dans ce dernier chapitre, nous essayons de prendre du recul sur les deux précédents chapitres, en leur donnant une interprétation arithmétique. De plus nous évoquons un argument probabiliste (fourni par Régine Marchand) pour donner une limite à la méthode de Mauduit-Rivat concernant les problèmes qui ont été traités au cours de cette thèse. Nous invoquons le même argument probabiliste pour compléter notre réponse à la question de Kalai concernant les objets étudiés au cours de cette thèse en montrant que si

$$P_N(X_1, \dots, X_N) = \sum_{i=1}^{N-k+1} X_i \cdots X_{i+k-1}$$

avec $k \geq c \log N$ et $c > 1/\log 2$, alors

$$\sum_{n<2^N} \mu(n)(-1)^{P_N(n)} = o(2^N)$$

avec $P_N(n) = P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$, où les ϵ_i désignent les chiffres binaires de n. De plus nous démontrons le résultat suivant :

Théorème 3.1.1. *Soient $f : \mathbb{N} \to \mathbb{N}$ une application, $A > 1$ un réel, N un entier positif, et*

$$P_N(X_1, \dots, X_N) = \sum_{i=1}^{N-k} X_i \dots X_{i+k-1}$$

un polynôme, avec k un entier supérieur ou égal à $A \log N/\log 2$. Alors, si pour tout entier n inférieur à 2^N, nous notons $P_N(n) := P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$ où les ϵ_i désignent les chiffres binaires de n, nous avons

$$\sum_{n<2^N} f(n)(-1)^{P_N(n)} = \sum_{n<2^N} f(n) + \varepsilon(N),$$

avec $|\varepsilon(N)| \leq 2^{N+1} N^{1-A} \sup_{n<2^N} |f(n)|(1 + o(1))$.

3.2 Réflexion sur les deux premiers chapitres

Dans le Chapitre 1, les résultats de [MR15] ont été étendus à toutes les suites de la forme

$$a(n) = a(\lfloor n/q^{T_q(n)-k} \rfloor) + \sum_{0\leq i\leq T_q(n)-k} g(\epsilon_i(n), \epsilon_{i+1}(n), \dots, \epsilon_{i+k-1}(n)), \tag{3.1}$$

où k a été fixé et $g : \{0, \dots, q-1\}^k \to \mathbb{N}$ est une fonction non triviale dans un sens qui a été précisé. Plus précisément nous avons obtenu la formule asymptotique suivante :

$$\left|\sum_{n\leq x} \mu(n) f(n) e(\vartheta n)\right| \ll c_1(q)(\log x)^{c_2(q)} x q^{-\gamma(2\lfloor(\log x)/80\log q\rfloor)/20+\log(\gamma(2\lfloor(\log x)/80\log q\rfloor)/20)}, \tag{3.2}$$

où $f(n) = e(\alpha a(n))$, $\alpha \in \mathbb{R}/\mathbb{Z}$, $\vartheta \in \mathbb{R}$, $c_1(q), c_2(q)$ des constantes définies dans le Théorème 1.2.5 ne dépendant que de q et de f, et

$$\gamma(N) := \lfloor N/k \rfloor \cdot \frac{\log\left(q^k - 8\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)}{N\log q}.$$

En particulier, en prenant $q = 2, \alpha = 1/2, \vartheta = 0$, l'équation (3.2) nous fournit

$$\sum_{n\leq x} \mu(n)(-1)^{a(n)} = o(x)$$

dans le cas où $(a(n))_{n\geq 0}$ est une suite de la forme (3.1). L'estimation du Chapitre 1 reste valable, dans le cas $x = 2^N$, pour tout $k \leq c\log N$ avec $c < 1/\log 2$. Cependant la suite $(a(n))_{n\geq 0}$ concernée n'est pas alors bien définie : selon la valeur de N, un même entier n inférieur à 2^N peut avoir plusieurs images différentes par l'application concernée, comme il a été vu dans l'introduction.

Dans l'objectif de formaliser cette remarque, au cours du Chapitre 2 nous avons démontré un théorème des nombres premiers et un principe d'aléa de Möbius pour la suite $(e(\alpha a_P(n)))_{n\geq 0}$ où α est un réel non entier, a_P définie par

$$a_P(n) := \sum_{i\geq 0} \epsilon_i(n) \dots \epsilon_{i+P(T_q(n))}(n),$$

avec $P : \mathbb{N} \to \mathbb{N}$ une application croissante vérifiant $P(x) \leq c\log x$ avec $c < 1/\log q$, $T_q(n) = \lfloor \log n/\log q \rfloor$ et

$$n = \sum_{i\geq 0} \epsilon_i(n) q^i$$

l'écriture *infinie* de n en base q. La forme de a_P, et notamment l'utilisation de l'écriture *infinie* de n, n'a été utilisée que dans le but de simplifier les calculs. Il est possible de généraliser notre suite de la manière suivante : soit k un entier strictement positif, pour tout intervalle $[q^{k-1}, q^k - 1]$ on fait correspondre une suite $P(k)$-récursive $\tilde{a}_{P(k)}$; nous pouvons alors définir $(a_P(n))_{n\geq 0}$ la suite qui a pour valeur

$$a_P(n) = \tilde{a}_{P(T_q(n))}(n).$$

Les résultats du Chapitre 2 peuvent alors s'adapter pour cette nouvelle suite : quelques ajustements de constantes - les mêmes effectués entre l'article de Mauduit et Rivat [MR15] et le Chapitre 1 - permettent de conclure à la validité des résultats. Le cas que nous avons regardé au Chapitre 2 correspond aux suites $P(k)$-récursives

$$\tilde{a}_{P(k)}(n) = \sum_{i=0}^{T_q(n)-P(k)} \epsilon_i(n)\dots\epsilon_{i+P(k)}(n).$$

Il existe une interprétation arithmétique des résultats du Chapitre 1 et du Chapitre 2 qui résulte du résultat (classique) suivant :

Proposition 3.2.1. *Soit $a : \mathbb{N} \to \mathbb{N}$ une application et m un entier supérieur ou égal à 2 tel que pour tout entier k satisfaisant à $1 \leq k < m$ on ait,*

$$\left|\sum_{n<N} \Lambda(n) e\left(\frac{k}{m}a(n)\right)\right| \leq C(N), \tag{3.3}$$

avec $C(N)$ une fonction croissante et étant $o(N)$ lorsque N tend vers l'infini, alors

$$\#\{p \leq x, \quad a(p) \equiv k \pmod m\} \sim \frac{\pi(x)}{m} \qquad (x \to \infty). \tag{3.4}$$

Démonstration. On a

$$\begin{aligned}\sum_{\substack{p\leq x\\ a(p)\equiv k \pmod m}} 1 &= \sum_{p\leq x} \frac{1}{m} \sum_{0\leq j<m} e\left(\frac{j(a(p)-k)}{m}\right)\\ &= \frac{\pi(x)}{m} + \sum_{p\leq x}\frac{1}{m}\sum_{1\leq j<m} e\left(\frac{j(a(p)-k)}{m}\right).\end{aligned}$$

Par ailleurs, par le Lemme A.1.1, pour toute $f : \mathbb{N} \to \mathbb{C}$ telle que $|f(n)| \leq 1$:

$$\left|\sum_{p\leq x} f(p)\right| \leq \frac{2}{\log x} \max_{t\leq x}\left|\sum_{n\leq t}\Lambda(n)f(n)\right| + O(\sqrt{x}),$$

en utilisant cette estimation avec $f(n) = e\left(\frac{j\cdot a(n)}{m}\right)$ nous obtenons :

$$\begin{aligned}\left|\sum_{p\leq x}\frac{1}{m}\sum_{1\leq j<m} e\left(\frac{j(a(p)-k)}{m}\right)\right| &= \frac{1}{m}\left|\sum_{1\leq j<m} e\left(\frac{-jk}{m}\right)\sum_{p\leq x} e\left(\frac{ja(p)}{m}\right)\right|\\ &\leq \sup_{1\leq j<m}\left|\sum_{p\leq x} e\left(\frac{ja(p)}{m}\right)\right|\\ &\leq \sup_{1\leq j<m}\left(\frac{2}{\log x}\max_{t\leq x}\left|\sum_{n\leq t}\Lambda(n)e\left(\frac{ja(n)}{m}\right)\right|\right) + O(\sqrt{x})\\ &\leq \sup_{1\leq j<m}\left(\frac{2}{\log x}\max_{t\leq x} C(t)\right) + O(\sqrt{x})\end{aligned}$$

et comme C est croissante et vérifie $C(N) = o(N)$ la dernière estimation est un $o(\pi(x))$ par le théorème des nombres premiers, ce qui achève la preuve. □

Ainsi, les estimations obtenues donnent une équirépartition des nombres premiers selon les classes de congruences. Dans le cas du Chapitre 1, on montre que les nombres premiers sont bien répartis selon la congruence du nombre de mot ω dans leurs chiffres, quelque soit ω. Ce résultat est à rapprocher du problème de Gelfond [MR10] : Mauduit et Rivat avaient démontré que les nombres premiers étaient bien répartis selon la congruence du nombre de '1' dans leurs chiffres binaires. Avec Martin ils avaient étendu ce résultat à n'importe quelle base et n'importe quel chiffre [MMR15]. Si l'estimation du Chapitre 1 reste valable pour $\beta < \log N/\log 2$ lorsque $x = 2^N$, il n'est pas possible de donner une interprétation dans ce cas : la taille du bloc considéré dépend de la borne de l'intervalle de sommation.

Par le Chapitre 2, nous pouvons dire, sous la condition $P(x) < \log_2(x)$, qu'il existe autant de nombres premiers possédant dans leur écriture binaire un nombre de $P(T_2(p))$ '1' consécutifs pair, que de nombre premier possédant un nombre de $P(T_2(p))$ '1' consécutifs impair.

Ainsi, si les résultats du Chapitre 2 avaient pu s'étendre à $P(x) = x$, nous aurions pu dire que la densité des nombres de Mersenne dans les nombre premiers était de $1/2$. En effet, le cas $P(x) = x$ correspond au produit des chiffres en base 2, et ce produit est impair si et seulement s'il vaut 1 si et seulement si tous les chiffres valent 1, si et seulement si l'entier correspondant est de la forme $2^k - 1$.

Nous avons donc un sens arithmétique, mais aussi une importante obstruction dans le cas extrême. Il est naturel de se demander quelle est la vitesse maximale à donner à P pour que la méthode de Mauduit et Rivat s'applique, et au delà de cette vitesse, s'il est possible d'obtenir un principe d'aléa de Möbius et/ou un théorème des nombres premier.

3.3 Cas de blocs de grande taille

Les résultats obtenus dans le Chapitre 1 (tout comme ceux obtenus dans [MR15]) sont très dépendants de ce qui est nommé la propriété de Fourier, qui implique notamment qu'il existe une application γ tendant vers l'infini à l'infini telle que, si k est un entier supérieur ou égal à 1,

$$\frac{1}{2^N}\left|\sum_{n<2^N} e\left(\alpha\sum_{i\geq 0}\epsilon_i(n)\cdots\epsilon_{i+k}(n)\right)\right| \leq 2^{-\gamma(N)}. \tag{3.5}$$

En prenant $\alpha = 1/2$, ce qui correspond à la question de Kalai, nous cherchons donc à montrer que

$$\frac{1}{2^N}\left|E_k(2^N) - I_k(2^N)\right| \leq 2^{-\gamma(N)},$$

où $E_k(m)$ désigne le nombre de $u < m$ tels que u a un nombre pair de blocs de taille $k+1$ de '1' dans son écriture binaire, et $I_k(m)$, un nombre impair. Elémentairement :

$$\left|E_k(2^N) - I_k(2^N)\right| = 2^N - 2\min(E_k(2^N), I_k(2^N)) = 2\max(E_k(2^N), I_k(2^N)) - 2^N. \tag{3.6}$$

Nous allons montrer dans la Partie 3.4 le résultat négatif suivant :

Proposition 3.3.1. *Soient N et k deux entiers, et $E_k(2^N)$ et $I_k(2^N)$ définis comme précédemment .*

Nous avons pour tout $1 < A < 2$, et pour tout entier $k \geq A\log_2(N)$:

$$\frac{E_k(2^N)}{2^N} \geq 1 - 2N^{1-A} + o(N^{1-A}) \qquad \textit{et donc} \qquad \frac{I_k(2^N)}{2^N} \leq 2N^{1-A} + o(N^{1-A}).$$

Par (3.6), ceci veut dire que sous les conditions de la proposition, on a pour N assez grand

$$\begin{aligned}\frac{1}{2^N}\left|\sum_{u<2^N} e\left(\frac{1}{2}\sum_{i\geq 0}\epsilon_{i+k}(u)\cdots\epsilon_i(u)\right)\right| &= \frac{2\max(E_k(2^N), I_k(2^N)) - 2^N}{2^N} \\ &\geq 2\frac{E_k(2^N)}{2^N} - 1 \\ &\geq 2(1-2N^{1-A}) + o(N^{1-A}) - 1 \\ &= 1 - 4N^{1-A} + o(N^{1-A})\end{aligned}$$

et en particulier (3.5) n'a aucune chance de se réaliser. Le Théorème 3.1.1 découle facilement de la Proposition 3.3.1.

Démonstration du Théorème 3.1.1. Soient E_k et I_k définis comme précédemment. Sous les conditions de la Proposition 3.3.1, nous avons pour $N \gg_A 1$:

$$I_k(2^N) = \min(E_k(2^N), I_k(2^N)) = 2^N - \max(E_k(2^N), I_k(2^N)) \tag{3.7}$$

et

$$\begin{aligned}\sum_{n<2^N} f(n)(-1)^{P_N(n)} &= \sum_{\substack{n<2^N \\ 2|P_N(n)}} f(n) - \sum_{\substack{n<2^N \\ 2\nmid P_N(n)}} f(n) \\ &= \sum_{n<2^N} f(n) - 2\sum_{\substack{n<2^N \\ 2\nmid P_N(n)}} f(n).\end{aligned}$$

À présent remarquons que

$$\begin{aligned}\left|\sum_{\substack{n<2^N \\ 2\nmid P_N(n)}} f(n)\right| &\leq \sup_{n<2^N}|f(n)|\#\{n<2^N : P_N(n) \not\equiv 0 \bmod 2\} \\ &= \sup_{n<2^N}|f(n)|I_k(2^N)\end{aligned}$$

et la Proposition 3.3.1 permet de conclure. □

En appliquant la proposition avec $f(n) = \mu(n)$ et en utilisant le théorème des nombres premiers sous la forme (8), nous obtenons que pour tout $A > 1$,

$$\sum_{n<2N} \mu(n)(-1)^{P_N(n)} = o(2^N)$$

avec

$$P_N(X_1, \dots, X_N) = \sum_{i=1}^{N-k} X_i \cdots X_{i+k-1}$$

un polynôme, avec $k \geq A \log N / \log 2$ et $P_N(n) = P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$. De même, avec cette définition de $P_N(n)$, le théorème des nombres premiers permet de conclure que pour tout $A > 2$ et $k \geq A \log N / \log 2$,

$$\sum_{n<2N} \Lambda(n)(-1)^{P_N(n)} \sim 2^N.$$

En effet, $\sup_{n<2^N} \Lambda(n) \leq N \log 2 < N$ et $|\varepsilon(N)| \leq N^{1-A} 2^{N+1} \sup_{n<2^N} \Lambda(n)(1 + o(1)) = o(2^N)$, car $A > 2$.

3.4 Un résultat probabiliste

La preuve de la Proposition 3.3.1 repose sur un résultat probabiliste. Ce n'est pas si étonnant si on tient compte du fait que, pour un entier n pris aléatoirement entre 0 et $2^N - 1$, en écrivant

$$n = \sum_{i=0}^{N-1} \epsilon_i(n) 2^i,$$

où $\epsilon_{N-1}(n)$ peut être égal à 0, les ϵ_i suivent des lois de Bernoulli et sont indépendantes et uniformémement distribuées.

Introduisons des notations : soit $\mathcal{A} := \{0, 1\}$ l'alphabet à deux éléments, $\mathcal{A}^N$ les mots sur $\mathcal{A}$ de taille N. Nous identifions totalement $\{0, \dots, 2^N - 1\}$ à $\mathcal{A}^N$. Pour ω un mot de taille N, nous notons $\mathcal{N}(\omega)$ son nombre de blocs constitués du même chiffre, pour chaque i-ième bloc, $X_i(\omega)$ sa taille. Nous notons enfin $\mathcal{M}(\omega)$ la taille du plus grand bloc constitué du même chiffre.

Ainsi $\omega := 111000011$ est constitué de trois blocs : '111' de taille 3, '0000' de taille 4 et '11' de taille 2. Donc dans ce cas $\mathcal{N}(\omega) = 3$, $X_1(\omega) = 3, X_2(\omega) = 4, X_3(\omega) = 2$ et $\mathcal{M}(\omega) = 4$.

Nous commençons cette partie en générant un mot aléatoire de taille N. Cette construction est standard et peut être retrouvée dans [MZA07].

Construction 3.4.1. *Soient $(Z_i)_{i\geq 0}$ des lois géométriques de paramètre $1/2$ définies sur un espace de probabilités $(\Omega, \mathcal{F}, \mathbb{P})$. Supposons-les indépendantes et identiquement distribuées. Soit ϵ une loi de Bernoulli de paramètre $1/2$ définie sur Ω et indépendante des Z_i. Alors nous construisons une suite infinie de 0 et de 1 de la manière suivante :*

- *si $\epsilon = 1$ nous écrivons Z_1 '0', puis Z_2 '1' puis Z_3'0' etc.*
- *si $\epsilon = 0$ nous écrivons Z_1 '1', puis Z_2 '0' puis Z_3'1' etc.*

Gardant les premiers symboles, nous obtenons un mot aléatoire de taille N. Avec ces notations, nous avons

$$\mathcal{N}(\omega) = \inf \left\{ k \in \mathbb{N}, \quad \sum_{i=1}^{k} Z_i(\omega) \geq N \right\}$$

et

$$\forall i \in \{1, \dots, \mathcal{N}(\omega) - 1\} : X_i(\omega) = Z_i \quad \text{et} \quad X_{\mathcal{N}(\omega)}(\omega) = N - \sum_{i=1}^{\mathcal{N}(\omega)-1} Z_i \leq Z_{\mathcal{N}(\omega)}. \tag{3.8}$$

Nous avons alors le résultat suivant :

Proposition 3.4.2. *Pour tout $1 < A < 2$, tout $N \geq 2$ et tout $\omega \in \mathcal{A}^l$:*

$$\mathbb{P}(\mathcal{M}(\omega) \geq A \log N / \log 2) \leq 2N^{1-A}.$$

Démonstration. Soit $y > 0$, comme pour tout i, $X_i \leq Z_i$ et que $\mathcal{N}(\omega) \leq N$, nous avons

$$\begin{aligned}
\mathbb{P}(\mathcal{M}(\omega) < y) &= \mathbb{P}(\forall 1 \leq i \leq \mathcal{N}(\omega) : X_i(\omega) < y) \\
&\geq \mathbb{P}(\forall 1 \leq i \leq \mathcal{N}(\omega) : Z_i < y) \\
&\geq \mathbb{P}(\forall 1 \leq i \leq N : Z_i < y) \\
&\geq (1 - 2^{-\lfloor y \rfloor})^N.
\end{aligned}$$

En appliquant ce résultat à $y = A \log N / \log 2$, ceci montre que

$$\begin{aligned}
\mathbb{P}(\mathcal{M}(\omega) \geq A \log N / \log 2) &= 1 - \mathbb{P}(\mathcal{M}(\omega) < A \log N / \log 2) \\
&\leq 1 - (1 - 2^{-\lfloor A \log N / \log 2 \rfloor})^N \\
&= 1 - \exp(N \log(1 - 2^{-\lfloor A \log N / \log 2 \rfloor})) \\
&\leq -N \log(1 - 2^{-\lfloor A \log N / \log 2 \rfloor}) \\
&\leq N 2^{-\lfloor A \log N / \log 2 \rfloor} + o(N 2^{-\lfloor A \log N / \log 2 \rfloor}) \\
&\leq N 2^{1 - A \log N / \log 2} + o(N 2^{-\lfloor A \log N / \log 2 \rfloor}) \\
&= 2N^{1-A} + o(N^{1-A}).
\end{aligned}$$

□

Voyons maintenant comment la Proposition 3.4.2 nous donne la Proposition 3.3.1.

Démonstration de la Proposition 3.3.1. Nous avons clairement, comme 0 est pair :

$$\begin{aligned}
E_k(2^N) &\geq 2^l \cdot \mathbb{P}(\mathcal{M}(\omega) < k) \\
&\geq 2^l \cdot \mathbb{P}(\mathcal{M}(\omega) < A \log N / \log 2) \\
&= 2^l \cdot (1 - \mathbb{P}(\mathcal{M}(\omega) \geq A \log N / \log 2)) \\
&\geq 2^N \cdot \left(1 - 2N^{1-A}\right) + o(2^N N^{1-A}),
\end{aligned}$$

ce qui conclut notre preuve et ce chapitre. □

Annexe A

Résultats annexes

A.1 Sommation sur les nombres premiers

Dans cette annexe, nous démontrons deux résultats, dont nous avons eu besoin, permettant pour une fonction arithmétique g d'évaluer la somme $\sum_{p\leq x} g(p)$. Ces deux résultats sont démontrés dans [MR10, Lemme 1, Lemme 11].

La difficulté à évaluer une telle somme, du fait du comportement imprévisible des nombres premiers, nous pousse à regarder une sommation différente. Il convient d'introduire la fonction de von Mangoldt. Le poids logarithmique ainsi posé, du fait du théorème fondamental de l'arithmétique, nous permet d'avoir

$$\log n = \sum_{d|n} \Lambda(d),$$

rendant les calculs plus simples. Le premier résultat que nous présentons est une des manières de relier la somme sur les premiers à Λ.

Lemme A.1.1. *Soit g une fonction arithmétique telle que $|g(n)| \leq 1$ pour tout entier n, alors*

$$\left|\sum_{p\leq x} g(p)\right| \leq \frac{2}{\log x} \max_{t\leq x} \left|\sum_{n\leq t} \Lambda(n)g(n)\right| + O(\sqrt{x}).$$

Démonstration. Par sommation par parties,

$$\sum_{p\leq x} g(p) = \frac{1}{\log x} \sum_{p\leq x} \log(p)g(p) + \int_2^x \left(\sum_{p\leq t} \log(p)g(p)\right) \frac{dt}{t(\log t)^2},$$

d'où en coupant l'intégrale en $\sqrt{x}$, et en utilisant l'inégalité $\sum_{p\leq t} \log p = O(t)$ (par

exemple [HW79, Theorem 414]),

$$\begin{aligned}\left|\sum_{p\le x} g(p)\right| &\le \left|\frac{1}{\log x}\sum_{p\le x}\log(p)g(p)\right| + \left|\int_{\sqrt{x}}^{x}\left(\sum_{p\le t}\log(p)g(p)\right)\frac{dt}{t(\log t)^2}\right| \\ &\quad + \left|\int_{2}^{\sqrt{x}}\left(\sum_{p\le t}\log(p)g(p)\right)\frac{dt}{t(\log t)^2}\right| \\ &\le \left|\frac{1}{\log x}\sum_{p\le x}\log(p)g(p)\right| + \left|\int_{\sqrt{x}}^{x}\left(\sum_{p\le t}\log(p)g(p)\right)\frac{dt}{t(\log t)^2}\right| \\ &\quad + O\left(\left|\int_{2}^{\sqrt{x}}\frac{dt}{(\log t)^2}\right|\right) \\ &\le \left(\frac{1}{\log x} + \int_{\sqrt{x}}^{x}\frac{dt}{t(\log t)^2}\right)\max_{\sqrt{x}<t\le x}\left|\sum_{p\le t}\log(p)g(p)\right| + O(\sqrt{x}).\end{aligned}$$

Or, du fait de l'inégalité de Tchébychev, $\pi(t) = O(t/\log t)$ [HW79, Theorem 7], nous obtenons pour $t \le x$,

$$\begin{aligned}\left|\sum_{n\le t}\Lambda(n)g(n) - \sum_{p\le t}\log(p)g(p)\right| &\le \sum_{p\le\sqrt{x}}\log p \sum_{2\le a\le\lfloor\log x/\log p\rfloor} 1 \\ &\le \pi(\sqrt{x})\log x = O(\sqrt{x}).\end{aligned}$$

□

Ainsi nous avons réduit le problème à l'évaluation de la somme

$$\sum_{n\le x}\Lambda(n)g(n). \tag{A.1}$$

Une méthode classique pour évaluer une telle somme consiste à utiliser une identité combinatoire permettant de transformer (A.1) en sommes multiples

$$\sum_{n_1,\dots,n_k} a_1(n_1)\dots a_k(n_k)g(n_1\dots n_k)$$

où les n_i sont liés par des conditions multiplicatives.

Le lemme que nous présentons ici s'inscrit dans cette direction. La preuve étant technique, nous n'en présentons qu'une esquisse, il est toutefois possible de la trouver dans [MR10, Lemme 1].

Lemme A.1.2. *Soient $q \ge 2$, $x \ge q^2$, $0 < \beta_1 < 1/3$, $1/2 < \beta_2 < 1$ et g une fonction arithmétique. On suppose que pour tous réels $M \le x$ et tous nombres complexes a_m, b_n avec $|a_m| \le 1$, $|b_n| \le 1$, on a*

$$\left|\sum_{\frac{M}{q}<m\le M}\sum_{\frac{x}{qm}<n\le\frac{x}{m}} a_m b_n g(mn)\right| \le U \quad \textit{pour} \quad x^{\beta_1} \le M \le x^{\beta_2} \tag{A.2}$$

et

$$\sum_{\frac{M}{q}<m\leq M} \max_{\frac{x}{qm}\leq t\leq \frac{x}{m}} \left| \sum_{t<n\leq \frac{x}{m}} g(mn) \right| \leq U \quad \textit{pour} \quad M \leq x^{\beta_1}. \tag{A.3}$$

Alors :

$$\left| \sum_{\frac{x}{q}<n\leq x} \Lambda(n)g(n) \right| \ll U(\log x)^2.$$

Démonstration. Pour $u \geq 1$ et $s \in \mathbb{C}$ posons

$$G(s) = \sum_{n\leq u} \frac{\mu(n)}{n^s}, \quad F(s) = \sum_{n\leq u} \frac{\Lambda(n)}{n^s}$$

et considérons pour $\Re(s) > 1$ l'égalité

$$-\frac{\zeta'}{\zeta} = F - \zeta' G - \zeta F G + \zeta \left(\frac{1}{\zeta} - G\right)\left(-\frac{\zeta'}{\zeta} - F\right)$$

où ζ est la fonction zêta de Riemann définie par $\zeta(s) = \sum_{n\geq 1} n^{-s}$.

Alors, pour x assez grand, en identifiant les coefficients de n^{-s} nous pouvons obtenir pour $u = x^{\beta_1}$ de sorte que $1 \leq u \leq \sqrt{x}$

$$\sum_{x/q<n\leq x} \Lambda(n)g(n) = S_1 - S_2 + S_3$$

avec

$$S_1 = \sum_{\substack{m\leq u \\ x/q<mn\leq x}} \mu(m)\log(n)g(mn)$$

$$S_2 = \sum_{\substack{m_1\leq u \\ m_2\leq u \\ x/q<m_1m_2n\leq x}} \mu(m_1)\Lambda(m_2)g(m_1m_2n)$$

$$S_3 = \sum_{\substack{u<m\leq x \\ u<n_1\leq x \\ x/q<mn_1n_2\leq x}} \mu(m)\Lambda(n_1)g(mn_1n_2).$$

En faisant des manipulations techniques usuelles (découpage de somme, interversion de somme, majoration classique, etc.) et en utilisant (A.3) pour S_1, (A.2) et (A.3) pour S_2 et (A.2) pour S_3, on arrive à démontrer le résultat.

□

En utilisant [IK04, equation (13.40)] :

$$\mu(m) = -\sum_{\substack{bc|m \\ b\leq u \\ c\leq u}} \mu(b)\mu(c) + \sum_{\substack{bc|m \\ b>u \\ c>u}} \mu(b)\mu(c)$$

nous obtenons

$$\sum_{x/q<n\leq x}\mu(n)g(n) = -S_1' + S_2'$$
$$= -\sum_{\substack{x/q<n_1n_2\leq x\\ n_1,n_2<u}}\mu(n_1)\mu(n_2)g(n_1n_2) + \sum_{\substack{x/q<n_1n_2\leq x\\ n_1,n_2>u}}\mu(n_1)\mu(n_2)g(n_1n_2)$$

et en utilisant la technique de la majoration de S_3 dans [MR10, Lemme 1] pour S_2' et (A.3) après un découpage selon les puissances de q pour n_1 pour traiter S_1', nous obtenons le pendant du Lemme A.1.2 pour la fonction de Möbius :

Lemme A.1.3. *Soient $q \geq 2$, $x \geq q^2$, $0 < \beta_1 < 1/3$, $1/2 < \beta_2 < 1$. Soit g une fonction arithmétique. On suppose que pour tous réels $M \leq x$ et tous nombres complexes a_m, b_n avec $|a_m| \leq 1$, $|b_n| \leq 1$, on a*

$$\left|\sum_{M/q<m\leq M}\sum_{\frac{x}{qm}<n\leq\frac{x}{m}} a_m b_n g(mn)\right| \leq U \quad \textit{pour} \quad x^{\beta_1} \leq M \leq x^{\beta_2} \tag{A.4}$$

et

$$\sum_{M/q<m\leq M}\max_{\frac{x}{qm}\leq t\leq\frac{x}{m}}\left|\sum_{t<n\leq\frac{x}{m}} g(mn)\right| \leq U. \tag{A.5}$$

Alors

$$\left|\sum_{x/q<n\leq x}\mu(n)g(n)\right| \ll U(\log x)^2.$$

A.2 Sommes d'exponentielles

Dans cette partie, nous commenterons et démontrerons plusieurs résultats classiques en lien avec les sommes d'exponentielles. Nous avons vu au cours de cette thèse que ces dernières pouvaient avoir un rôle primordial en théorie analytique des nombres. Leur intérêt dépasse largement le cadre des problèmes vus ici. Elles apparaissent par exemple dans l'estimation du terme d'erreur de la moyenne des diviseurs (problème de Dirichlet), dans la majoration de la quantité $|\zeta(1/2+it)|$, où ζ désigne la fonction zêta de Riemann (hypothèse de Lindelöf) ou dans la résolution de certains systèmes diophantiens. Pour un aperçu, voir par exemple [Rob16] ou [GK91].

Notre but ici n'est pas d'être exhaustif, mais d'introduire et/ou démontrer les résultats dont nous avons eu besoin. On trouvera dans [GK91], [Rob16] ou [IK04] un exposé plus complet.

Dans un premier temps nous énoncerons et démontrerons deux résultats qui ne concernent pas uniquement les sommes d'exponentielles : les inégalités de Cauchy-Schwarz et de Van der Corput. Ensuite, nous discuterons des sommes d'exponentielles et nous énoncerons les théorèmes de Kusmin-Landau (Théorème A.2.5) et de Van der Corput (Théorème A.2.8). Pour ces théorèmes, nous suivrons l'approche de [GK91], une approche différente peut être trouvée dans [Ten08].

Théorème A.2.1 (Inégalité de Cauchy-Schwarz)**.** *Soient $(a_m)_{m\geq 1}$ et $(b_m)_{m\geq 1}$ deux suites de nombres complexes. Alors, nous avons pour tout entier N strictement positif :*

$$\left|\sum_{i=1}^{N} a_i b_i\right|^2 \leq \left(\sum_{i=1}^{N} |a_i|^2\right)\left(\sum_{i=1}^{N} |b_i|^2\right). \tag{A.6}$$

Nous avons vu que cette identité apparaissait à plusieurs reprises lors du Chapitre 2, notamment pour le lissage des sommes de type II. Elle peut s'énoncer de manière plus générale dans le cadre d'un espace Hilbertien sous la forme suivante :

Théorème A.2.2 (Inégalité de Cauchy-Schwarz : cas Hilbertien)**.** *Soit $(E, \langle\cdot,\cdot\rangle)$ un espace préhilbertien réel ou complexe. Alors pour tous vecteurs x et y de E,*

$$|\langle x, y\rangle| \leq \|x\| \cdot \|y\|,$$

de plus il y a égalité si et seulement si x et y sont linéairements dépendants.

Une jolie preuve de ce dernier résultat repose sur une résolution d'une équation polynomiale de second degré. Plutôt que cette démonstration, nous préférons présenter ici une preuve élémentaire de l'inégalité de Cauchy-Schwarz, reposant sur une identité de Lagrange.

Preuve élémentaire dans le cas complexe. Soient $(a_m)_{m\geq 1}$ et $(b_n)_{n\geq 1}$ deux suites de nombres complexes. Alors nous avons :

$$\begin{aligned}
\sum_{1\leq i<j\leq N} |a_i b_j - a_j b_i|^2 &= \sum_{1\leq i<j\leq N} (|a_i|^2|b_j|^2 - 2a_i b_j \overline{a_j b_i} + |a_j|^2|b_i|^2) \\
&= \sum_{\substack{1\leq i,j\leq N \\ i\neq j}} (|a_i|^2|b_j|^2 - a_i b_j \overline{a_j b_i}) \\
&= \sum_{1\leq i,j\leq N} (|a_i|^2|b_j|^2 - a_i b_j \overline{a_j b_i}) \\
&= \left(\sum_{i=1}^{N} |a_i|^2\right)\left(\sum_{j=1}^{N} |b_j|^2\right) - \left(\sum_{i=1}^{N} a_i \overline{b_i}\right)\left(\sum_{j=1}^{N} \overline{a_j} b_j\right),
\end{aligned}$$

qui est l'identité de Lagrange dans le cas complexe. Comme le membre de gauche est positif, l'inégalité est démontrée. □

Nous voyons ainsi clairement apparaître le cas d'égalité. Il s'avère que parfois l'inégalité de Cauchy-Schwarz est trop imprécise (ou bien que le terme d'erreur est trop compliqué à contrôler). Appliquant (A.6) avec $b_i = 1$ pour tout i, nous obtenons :

$$\left|\sum_{i=1}^{N} a_i\right|^2 \leq N \sum_{i=1}^{N} |a_i|^2. \tag{A.7}$$

L'inégalité de Van der Corput raffine ce résultat.

Théorème A.2.3 (Inégalité de Van der Corput)**.** *Soient $z_1, \dots, z_N$ des nombres complexes. Pour tout entier $R \geq 1$, on a :*

$$\left| \sum_{1 \leq n \leq N} z_n \right|^2 \leq \frac{N+R-1}{R} \sum_{|r|<R} \left(1 - \frac{|r|}{R}\right) \sum_{\substack{1 \leq n \leq N \\ 1 \leq n+r \leq N}} z_{n+r}\overline{z_n}. \tag{A.8}$$

Démonstration. Nous reprenons ici la preuve donnée dans [MR10, Lemme 4]. Par commodité, on pose $z_n = 0$ pour $n \leq 0$ et $n \geq N+1$. Pour tout entier $R \geq 1$, on a les égalités

$$R \sum_{n \in \mathbb{Z}} z_n = \sum_{r=0}^{R-1} \sum_{n \in \mathbb{Z}} z_{n+r} = \sum_{n \in \mathbb{Z}} \sum_{r=0}^{R-1} z_{n+r}.$$

Les entiers n pour lesquels la dernière somme est potentiellement non nulle vérifient $1-(R-1) \leq n \leq N$ et leur nombre ne dépasse pas $N+R-1$. En appliquant l'inégalité de Cauchy-Schwarz, nous obtenons :

$$\begin{aligned} R^2 \left| \sum_{n \in \mathbb{Z}} z_n \right|^2 &\leq (N+R-1) \sum_{n \in \mathbb{Z}} \left| \sum_{r=0}^{R-1} z_{n+r} \right|^2 \\ &\leq (N+R-1) \sum_{r_1=0}^{R-1} \sum_{r_2=0}^{R-1} \sum_{n \in \mathbb{Z}} z_{n+r_1} \overline{z_{n+r_2}} \\ &\leq (N+R-1) \sum_{r_1=0}^{R-1} \sum_{r_2=0}^{R-1} \sum_{m \in \mathbb{Z}} z_{m+r_1-r_2} \overline{z_m} \\ &\leq (N+R-1) \sum_{-R<r<R} (R-|r|) \sum_{m \in \mathbb{Z}} z_{m+r} \overline{z_m} \end{aligned}$$

et nous obtenons le résultat annoncé en divisant par R^2. □

L'avantage de (A.8) par rapport à (A.7) consiste en l'introduction des corrélations $z_{n+r}\overline{z_n}$. En imaginant que $z_n = e(U_n)$, alors on a $z_{n+r}\overline{z_n} = e(U_{n+r} - U_n)$. C'est cette différence qui permet d'introduire la fonction tronquée. Un autre exemple (marquant et originel) consiste à prendre pour suite $U_n := P(n)$ où $P : \mathbb{N} \to \mathbb{N}$ est une fonction polynomiale. Ce faisant, avec cette manipulation, nous réduisons le degré du polynôme.

Un autre résultat important de majoration de sommes en théorie analytique des nombres est la version arithmétique du grand crible. Nous ne faisons pas ici sa démonstration, mais elle peut être trouvée dans [Mon78].

Théorème A.2.4 (Grand Crible)**.** *Pour tout $(z_1, \dots, z_N) \in \mathbb{C}^N$ et tout entier $Q \geq 1$ nous avons*

$$\sum_{q \leq Q} \sum_{a=1}^{q} \left| \sum_{n=1}^{N} z_n e\left(\frac{an}{q}\right) \right|^2 \leq (N-1+Q^2) \sum_{n=1}^{N} |z_n|^2, \tag{A.9}$$

où $e(x) = \exp(2i\pi x)$.

Le point de départ de l'étude des sommes d'exponentielles est l'identité de la série géométrique :

$$\sum_{i=0}^{N} q^i = \frac{1-q^{N+1}}{1-q}. \tag{A.10}$$

Si nous l'appliquons à $q = e\left(\frac{a}{N}i\right)$ $(N \nmid a)$, du fait que pour tout entier n, $e(n) = 1$ nous obtenons

$$\sum_{i=0}^{N-1} e\left(\frac{a}{N}i\right) = \frac{1-e\left(N\cdot\frac{a}{N}\right)}{1-e\left(\frac{a}{N}\right)} = 0,$$

a contrario si nous avions supposé $a = Nk$ nous aurions obtenu

$$\sum_{i=0}^{N-1} e\left(\frac{a}{N}i\right) = \sum_{i=0}^{N-1} e\left(ki\right) = N,$$

ce qui donne finalement

$$\frac{1}{N}\sum_{i=0}^{N-1} e\left(\frac{a}{N}i\right) = \begin{cases} 1 \text{ si } & N|a \\ 0 \text{ si } & N \nmid a. \end{cases} \tag{A.11}$$

Si à présent nous utilisons la formule (A.10) avec $q = e(\alpha)$ pour $\alpha \in \mathbb{R}\backslash\mathbb{Z}$ quelconque, nous trouvons :

$$\sum_{i=0}^{N-1} e(\alpha i) = \frac{1-e(\alpha N)}{1-e(\alpha)} = \frac{e(-\alpha N/2)-e(\alpha N/2)}{e(-\alpha/2)-e(\alpha/2)}\cdot\frac{e(\alpha N/2)}{e(\alpha/2)},$$

ce qui donne

$$\left|\sum_{i=0}^{N-1} e(\alpha i)\right| = \left|\frac{\sin(\pi\alpha N)}{\sin(\pi\alpha)}\right| \leq \frac{1}{|\sin\pi\alpha|},$$

et comme par l'inégalité triangulaire :

$$\left|\sum_{i=0}^{N-1} e(\alpha i)\right| \leq N$$

nous avons finalement

$$\left|\sum_{i=0}^{N-1} e(\alpha i)\right| \leq \min\left(N, \frac{1}{|\sin\pi\alpha|}\right). \tag{A.12}$$

Nous pouvons simplifier (A.12) en remarquant que $|\sin\pi\alpha|$ est 1-périodique en α et que $\sin(\pi(1-\alpha)) = \sin\pi\alpha$. Nous pouvons supposer que $\alpha \in [0, 1/2)$ et dans cet intervalle, $\sin\pi\alpha \geq 2\alpha$. En effectuant l'opération nécessaire pour se ramener au cas $\alpha \notin [0, 1/2)$ nous pouvons dire $|\sin\pi\alpha| \geq 2\|\alpha\|_{\mathbb{Z}}$ et donc finalement :

$$\left|\sum_{n=0}^{N-1} e(\alpha n)\right| \ll \min\left(N, \frac{1}{\|\alpha\|_{\mathbb{Z}}}\right). \tag{A.13}$$

Nous voyons sans peine que les arguments se généralisent à un intervalle quelconque (et non plus l'intervalle $[\![0, N-1]\!]$) et que nous pouvons prendre $\alpha k+\beta$ sans rien perdre de l'estimation.

Il semble alors naturel de penser que, pour une fonction $f : \mathbb{R} \to \mathbb{R}$ possédant des propriétés semblables et I un intervalle, la somme

$$\sum_{n\in I} e(f(n))$$

est petite. Nous présentons un premier résultat dans cette direction [GK91, Theorem 2.1] :

Théorème A.2.5 (Kusmin-Landau)**.** *Si $I = (a, b]$ est un intervalle et si f est continûment dérivable sur cet intervalle, f' monotone et $\|f'\|_{\mathbb{Z}} \geq \lambda > 0$ sur I, alors :*

$$\sum_{n\in I} e(f(n)) \ll \lambda^{-1}.$$

Démonstration. Comme $e(-x) = \overline{e(x)}$, nous avons

$$\left|\sum_{n\in I} e(f(n))\right| = \left|\sum_{n\in I} e(-f(n))\right|$$

et nous pouvons supposer f croissante. Par hypothèse, il existe un entier k tel que

$$k + \lambda \leq f'(n) \leq k + 1 - \lambda$$

mais comme

$$\sum_{n\in I} e(f(n)) = \sum_{n\in I} e(f(n) - kn)$$

nous pouvons supposer $\lambda \leq f'(n) \leq 1 - \lambda$.

Soit $g(n) = f(n + 1) - f(n)$. Par le théorème des accroissements finis, comme f est continûment dérivable, il existe $n < x_n < n + 1$ tel que

$$g(n) = f(n + 1) - f(n) = \frac{f(n + 1) - f(n)}{n + 1 - n} = f'(x_n).$$

En conséquence g est croissante et vérifie $\lambda \leq g(n) \leq 1 - \lambda$. Cependant

$$e(f(n)) = \frac{e(f(n)) - e(f(n + 1))}{1 - e(g(n))} = (e(f(n)) - e(f(n + 1)))\, C_n$$

avec $C_n = \frac{1}{2}(1 + i \cot \pi g(n))$. En effet,

$$\begin{aligned}
\frac{1}{1 - e(g(n))} &= \frac{e(-g(n)/2)}{e(-g(n)/2) - e(g(n)/2)} \\
&= \frac{\cos(-\pi g(n)) + i \sin(-\pi g(n))}{2i \sin(-\pi g(n))} \\
&= \frac{1}{2} + \frac{1}{2i} \cot(-\pi g(n)) \\
&= \frac{1}{2}(1 - i \cot(-\pi g(n))) \\
&= \frac{1}{2}(1 + i \cot(\pi g(n))).
\end{aligned}$$

Avec ces considérations, nous avons donc, en considérant $I =]a, b]$:

$$\begin{aligned}\sum_{n\in I} e(f(n)) &= \sum_{n=a+1}^{b-1} (e(f(n)) - e(f(n+1)))\, C_n + e(f(b)) \\ &= \sum_{n=a+2}^{b-1} e(f(n))\,(C_n - C_{n-1}) + e(f(a+1))C_{a+1} + e(f(b))(1 - C_{b-1})\end{aligned}$$

et ainsi nous avons

$$\left|\sum_{n\in I} e(f(n))\right| \leq \frac{1}{2} \sum_{n=a+2}^{b-1} |\cot(\pi g(n-1)) - \cot(\pi g(n))| + |C_{a+1}| + |1 - C_{b-1}|.$$

Mais la fonction cotangente est décroissante, et la somme de droite est télescopique, de sorte que

$$\left|\sum_{n\in I} e(f(n))\right| \leq \frac{1}{2} (\cot(\pi g(a+1)) - \cot(\pi g(b-1))) + |C_{a+1}| + |1 - C_{b-1}|, \quad \text{(A.14)}$$

et comme nous avons

$$|\cot \pi x| = \left|\frac{\cos \pi x}{\sin \pi x}\right| \leq |\sin \pi x|^{-1} \ll \|x\|_{\mathbb{Z}}^{-1}$$

en nous rappelant que $C_n = \frac{1}{2}(1 + i \cot \pi g(n))$, nous avons par (A.14) :

$$\left|\sum_{n\in I} e(f(n))\right| \ll \sup_{n\in I} |\cot(\pi g(n))| \ll \sup_{n\in I} \|g(n)\|_{\mathbb{Z}}^{-1}$$

et nous concluons le théorème en rappelant $1 - \lambda > g(n) > \lambda$ pour tout n dans I. □

Remarque A.2.6. *Une autre démonstration possible est d'utiliser des intégrales de Stieltjes et de relier les sommes trigonométriques à ces intégrales. Nous pouvons trouver une preuve avec cette méthode dans [Ten08, Chapitre I.6].*

Avant de démontrer le théorème de Van der Corput, nous allons démontrer le lemme suivant [Hux96, Lemma 3.1.2] :

Lemme A.2.7. *Soit f une fonction dérivable sur un intervalle I telle qu'il existe $\lambda > 0$ et $\alpha \geq 1$ des réels de sorte que $\lambda \leq |f'(x)| \leq \alpha\lambda$ pour tout x dans I. Alors pour tout $\delta > 0$,*

$$\#\{m \in I : \|f(m)\|_{\mathbb{Z}} \leq \delta\} \ll \left(1 + \frac{\delta}{\lambda}\right)(\alpha\lambda|I| + 1).$$

Démonstration. Sans perte de généralité nous pouvons supposer f croissante sur I. Si $I = [a, b]$, nous définissons $f(I) = [f(a), f(b)]$. Comme $|f(b) - f(a)| \leq \alpha\lambda(b - a)$, nous avons $|f(I) \cap \mathbb{Z}| \leq \alpha\lambda(b - a) + 1$. À présent

$$\begin{aligned}\#\{m \in I : \|f(m)\|_{\mathbb{Z}} \leq \delta\} &= \sum_{v\in f(I)\cap\mathbb{Z}} \#\{m \in I : |f(m) - v| \leq \delta\} \\ &=: \sum_{v\in f(I)\cap\mathbb{Z}} \#A_v,\end{aligned}$$

Si m et m' sont dans A_v, ils vérifient $\lambda|m - m'| \leq |f(m) - f(m')| \leq |f(m) - v| + |v - f(m')| \leq 2\delta$, et donc $\#A_v \leq 1 + \frac{2\delta}{\lambda}$ et le résultat est prouvé. □

Nous sommes à présent à même de démontrer le théorème de Van der Corput [GK91, Theorem 2.2]. Il présente l'avantage d'avoir des conditions à vérifier moins restrictives que le théorème de Kusmin-Landau (c'est pourquoi nous l'avons utilisé dans le Chapitre 2).

Théorème A.2.8 (Van der Corput)**.** *Soit f une fonction réelle deux fois dérivable dans un intervalle I. Supposons en outre qu'il existe un certain $\lambda > 0$ et un $\alpha \geq 1$ tels que*

$$\lambda \leq |f''(x)| \leq \alpha\lambda$$

sur I. Alors

$$\sum_{n\in I} e(f(n)) \ll \alpha|I|\lambda^{1/2} + \lambda^{-1/2}.$$

Démonstration. Soit $\delta(< 1/2)$ un paramètre qui sera choisi plus tard. Nous séparons alors la somme selon

$$\sum_{n\in I} e(f(n)) = \sum_{\substack{n\in I \\ \|f'(n)\|\leq\delta}} e(f(n)) + \sum_{\substack{n\in I \\ \|f'(n)\|>\delta}} e(f(n)).$$

La première somme est contrôlée par le Lemme A.2.7, et la seconde somme est composée d'intervalles, de sorte qu'on peut appliquer le théorème de Kusmin-Landau pour pouvoir dire que

$$\sum_{n\in I} e(f(n)) \ll \left(1 + \frac{\delta}{\lambda}\right)(\alpha\lambda|I| + 1) + \delta^{-1}.$$

Si $\lambda > 1/4$, la majoration désirée découle de la majoration triviale. Nous pouvons donc supposer $\lambda \leq 1/4$. Nous choisissons alors $\delta = \lambda^{1/2}$ et nous obtenons

$$\sum_{n\in I} e(f(n)) \ll (1 + \lambda^{-1/2})(\alpha\lambda|I| + 1) + \lambda^{-1/2} \ll \alpha\lambda|I| + \alpha\lambda^{1/2}|I| + \lambda^{-1/2} + 1.$$

Comme nous avons alors $\lambda^{1/2} \geq \lambda$, le résultat désiré est obtenu. □

Donnons ici une application (qui nous est utile dans notre thèse) des sommes d'exponentielles. Le résultat suivant évalue la somme des diviseurs sur un intervalle court. Il s'agit de [DMR09, Lemma 3.5] (nous renvoyons à la référence pour la démonstration).

Lemme A.2.9. *Pour $x^{27/82} \leq y \leq x$, nous avons*

$$\sum_{x-y<n\leq x} \tau(n) = O(y \log x).$$

Il est bien souvent utile d'avoir des connaissances sur la moyenne de l'équation (A.12). Le lemme suivant, correspond à [MR10, Lemme 6].

Lemme A.2.10. *Pour tout couple d'entiers (a, m) avec $m \geq 1$, et pour tous $b \in \mathbb{R}$, $U \in \mathbb{R}$ et $U > 0$ nous avons*

$$\sum_{0 \leq n \leq m-1} \min\left(U, \left|\sin \pi \frac{an+b}{m}\right|^{-1}\right) \ll \operatorname{pgcd}(a, m)U + m \log m. \tag{A.15}$$

La preuve de ce lemme est faite dans [MR10] nous n'en donnerons ici qu'un aperçu.

Idée de preuve. Notons S la somme à estimer. Nous remarquons que nous pouvons supposer $d = \operatorname{pgcd}(a, m) \neq m$ (sans quoi l'inégalité est triviale), nous réduisons le membre de gauche par le pgcd, par l'opération précédemment faite, le a' trouvé est inversible dans $\mathbb{Z}/m'\mathbb{Z}$ avec $m' = m/d$, et nous nous ramenons au cas où $a = 1$. Nous isolons alors les cas extrêmes (qui correspondent à $\operatorname{pgcd}(a, m)U$) pour nous concentrer sur une somme de type

$$\sum_{1 \leq n \leq m'-2} \min\left(M, \left|\sin \frac{\pi}{m'}\left(n + \frac{r}{d}\right)\right|^{-1}\right).$$

Nous utilisons alors la méthode des trapèzes et la convexité de $t \mapsto 1/(\sin t)$ sur $]0, \pi[$ pour pouvoir dire qu'il faut avant tout estimer

$$h(x) = \left(\sin \frac{\pi}{m'}(1-x)\right)^{-1} + \int_{1/2}^{m'-3/2} \left(\sin \frac{\pi}{m'}(t+x)\right)^{-1} dt.$$

Cependant par convexité de l'application $t \mapsto 1/(\sin t)$ la fonction h est convexe sur $[0, 1/2]$, donc elle atteint son maximum sur les extrémités, et on remarque que $h(1/2) - h(0) \geq 0$. Les identités trigonométriques permettent alors de conclure. □

Le lemme suivant est [MR15, Lemma 5].

Lemme A.2.11. *Soient $A \geq 1$, $m \geq 1$ des entiers et $b \in \mathbb{R}$. Pour tout nombre réel $U > 0$ nous avons*

$$\frac{1}{A} \sum_{1 \leq a \leq A} \sum_{0 \leq n < m} \min\left(U, \left|\sin \frac{an+b}{m}\right|^{-1}\right) \ll \tau(m)U + m \log m. \tag{A.16}$$

Démonstration. Il suffit d'exploiter (A.15) en remarquant que

$$\sum_{1 \leq a \leq A} \operatorname{pgcd}(a, m) = \sum_{\substack{d \mid m \\ d \leq A}} d \sum_{\substack{1 \leq a \leq A \\ (a,m)=d}} 1 \leq \sum_{\substack{d \mid m \\ d \leq A}} d \sum_{\substack{1 \leq a \leq A \\ d \mid a}} 1 = \sum_{\substack{d \mid m \\ d \leq A}} d \left\lfloor \frac{A}{d} \right\rfloor \leq A\tau(m).$$

□

A.3 Approximation par polynômes trigonométriques

L'article [Vaa85] traite d'un certain nombre de résultats d'analyse harmonique qui possèdent des applications en théorie des nombres. Nous allons présenter ici un théorème qui fournit un résultat d'approximation. Pour commencer définissons certaines fonctions qui nous serons utiles par la suite. Ces fonctions sont liées aux noyaux fondamentaux (dont le noyau de Féjer).

Soit

$$K(z) := \left(\frac{\sin \pi z}{\pi z}\right)^2 = \int_{-1}^{1} (1-|t|)e(tz)dt$$

alors,

$$\hat{K}(t) := \int_{-\infty}^{\infty} K(x)e(-tx)dx = (1-|t|)\mathbb{1}_{t\in[-1,1]}.$$

Posons à présent

$$H(z) = \left(\frac{\sin \pi z}{\pi}\right)^2 \left\{ \sum_{m=-\infty}^{\infty} \operatorname{sgn}(m)(z-m)^{-2} + 2z^{-1} \right\} \quad \text{et} \quad J(z) = \frac{1}{2}H'(z),$$

alors par [Vaa85, Theorem 6], nous avons :

$$\hat{J}(t) = \begin{cases} 1 & \text{si} \quad t = 0, \\ \pi t(1-|t|)\cot \pi t + |t| & \text{si} \quad 0 < |t| < 1, \\ 0 & \text{si} \quad 1 \leq |t|. \end{cases}$$

Nous définissons alors [Vaa85, page 199] $f_\delta(t) = \delta f(\delta t)$ de sorte que $\hat{f}_\delta(t) = \hat{f}(t/\delta)$ et pouvons alors définir les deux objets centraux du résultat :

$$\begin{aligned} j_N(x) &= \sum_{n=-N}^{N} \hat{J}_{N+1}(n)e(nx) \\ &= \sum_{n=-N}^{N} \left(\pi \frac{n}{N+1}\left(1 - \frac{|n|}{N+1}\right)\cot\left(\pi\frac{n}{N+1}\right) + \frac{|n|}{N+1}\right)e(nx) \end{aligned} \tag{A.17}$$

et

$$k_N(x) := \sum_{n=-N}^{N} \hat{K}_{N+1}(n)e(nx) = \sum_{n=-N}^{N} \left(1 - \frac{|n|}{N+1}\right)e(nx). \tag{A.18}$$

Nous finissons les définitions par la notion de produit de convolution de [Vaa85, page 208], c'est-à-dire

$$f * g(x) = \int_{-1/2}^{1/2} f(t)g(x-t)dt.$$

Nous rappelons que $V_f(x)$ est la variation totale de la fonction f sur l'intervalle $[-1/2, x)$. Nous posons

$$(dV_f) * k_N(x) = \int_{-1/2}^{1/2} (dV_f)(t)k_N(x-t)dt.$$

Nous avons alors le [Vaa85, Theorem 19]

Théorème A.3.1. *Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de période 1 et de variation bornée pour tout intervalle fermé de longueur 1. Supposons en outre que f vérifie*

$$\lim_{h\to 0+} \frac{1}{2}\{f(x+h) + f(x-h)\} = f(x). \tag{A.19}$$

Alors les polynômes trigonométriques $f * j_N(x)$ et $(dV_f) * k_N(x)$ vérifient

$$|f(x) - f * j_N(x)| \leq (2N+2)^{-1}(dV_f) * k_N(x) \tag{A.20}$$

La démonstration de ce résultat nécessite de redémontrer l'essentiel des résultats de [Vaa85], nous ne le ferons donc pas ici. Regardons comment appliquer le Théorème A.3.1 avec $\chi_\alpha = \lfloor x \rfloor - \lfloor x - \alpha \rfloor = \mathbb{1}_{\{x\}\in[0,\alpha)}$. Pour commencer il faut normaliser la fonction. Nous prenons donc

$$\widetilde{\chi_\alpha}(x) = \lim_{t\to 0+} \frac{1}{2}(\chi_\alpha(x-t) + \chi_\alpha(x+t)).$$

L'équation (A.20) nous dit donc que

$$|\widetilde{\chi_\alpha}(x) - \widetilde{\chi_\alpha} * j_N(x)| \leq (2N+2)^{-1} dV_{\widetilde{\chi_\alpha}} * k_N(x).$$

Remarquons que $j_0(x) = \hat{J}(0)e(0\cdot x) = 1$, donc $\widetilde{\chi_\alpha} * j_N(x) = \alpha$. Supposons à présent $N > 0$, alors :

$$\begin{aligned}
\widetilde{\chi_\alpha} * j_N(x) &= \int_{-1/2}^{1/2} \widetilde{\chi_\alpha}(t) j_N(x-t)dt \\
&= \int_{-1/2}^{1/2} \widetilde{\chi_\alpha}(t) j_N(x) e(-nt)dt \\
&= j_N(x) \int_{-1/2}^{1/2} \widetilde{\chi_\alpha}(t) e(-nt)dt.
\end{aligned}$$

Si $\alpha \leq 1/2$, l'intégrale vaut

$$\int_{-1/2}^{1/2} \widetilde{\chi_\alpha}(t)e(-nt)dt = \int_0^\alpha e(-nt)dt = \left[\frac{e(-nt)}{-2i\pi n}\right]_0^\alpha = \frac{e(-n\alpha)-1}{-2i\pi n} = e(-n\alpha/2)\frac{\sin(\pi n\alpha)}{\pi n}$$

et si $\alpha > 1/2$ elle vaut

$$\int_{-1/2}^{1/2} \widetilde{\chi_\alpha}(t)e(-nt)dt = \int_0^{1/2} e(-nt)dt + \int_{-1/2}^{\alpha-1} e(-nt)dt = e(-n\alpha/2)\frac{\sin(\pi n\alpha)}{\pi n}.$$

Nous en déduisons donc

$$\begin{aligned}
\widetilde{\chi_\alpha} * j_N(x) &= j_N(x)e(-n\alpha/2)\frac{\sin(\pi n\alpha)}{\pi n} \\
&= \sum_{n=-N}^{N} \left(\pi \frac{n}{N+1}\left(1 - \frac{|n|}{N+1}\right)\cot\left(\pi\frac{n}{N+1}\right) + \frac{|n|}{N+1}\right) e(nx)e(-n\alpha/2)\frac{\sin(\pi n\alpha)}{\pi n}.
\end{aligned}$$

Cependant nous avons

$$\left(\pi \frac{n}{N+1}\left(1 - \frac{|n|}{N+1}\right)\cot\left(\pi\frac{n}{N+1}\right) + \frac{|n|}{N+1}\right) \leq 1.$$

En effet, par développement limité en 0 de la fonction cotangente, nous notons $\cot(\pi t) \leq \frac{1}{\pi t}$ sur $(0,1]$ et donc

$$\pi t(1-t)\cot \pi t + t \leq \pi t(1-t)\frac{1}{\pi t} + t = 1.$$

Par cette majoration, nous obtenons

$$\begin{aligned}\left(\pi\frac{n}{N+1}\left(1-\frac{|n|}{N+1}\right)\cot\left(\pi\frac{n}{N+1}\right)+\frac{|n|}{N+1}\right)e(nx)e(-n\alpha/2)\frac{\sin(\pi n\alpha)}{\pi n}&\\ \leq \frac{|\sin(\pi n\alpha)|}{|\pi n|}&\\ \leq \min\left(\alpha, \frac{1}{\pi|n|}\right).&\end{aligned}$$

Regardons à présent $dV_{\widetilde{\chi_\alpha}} * k_N(x)$. Si $\alpha < 1/2$ il existe deux points de variation pour la fonction $\widetilde{\chi_\alpha}$: en 0 et en α. Ceci nous donne donc

$$\begin{aligned}dV_{\widetilde{\chi_\alpha}} * k_N(x) &= \int_{-1/2}^{1/2}(dV_{\widetilde{\chi_\alpha}})(t)k_N(x-t)dt\\ &= k_N(x) + k_N(x-\alpha)\\ &= \sum_{n=-N}^{N}\left(1-\frac{|n|}{N+1}\right)e(nx)\left(1+e(-n\alpha)\right)\\ &= \sum_{n=-N}^{N}\left(1-\frac{|n|}{N+1}\right)e(-n\alpha/2+nx)\cdot 2\cos(\pi n\alpha).\end{aligned}$$

Soit à présent $\alpha > 1/2$. Puisque sur $[-1/2, 0)$, $\{x\} = x+1$, la fonction $\widetilde{\chi_\alpha}$ possède sur l'intervalle $[-1/2, 1/2]$ deux points de variations : 0 et $\alpha - 1$. Nous avons donc

$$\begin{aligned}dV_{\widetilde{\chi_\alpha}} * k_N(x) &= \int_{-1/2}^{1/2}(dV_{\widetilde{\chi_\alpha}})(t)k_N(x-t)dt\\ &= k_N(x) + k_N(x-\alpha+1)\\ &= \sum_{n=-N}^{N}\left(1-\frac{|n|}{N+1}\right)e(nx)\left(1+e(-n\alpha+n)\right)\\ &= \sum_{n=-N}^{N}\left(1-\frac{|n|}{N+1}\right)e(nx)\left(1+e(-n\alpha)\right)\\ &= \sum_{n=-N}^{N}\left(1-\frac{|n|}{N+1}\right)e(-n\alpha/2)\cdot 2\cos(\pi n\alpha).\end{aligned}$$

Nous avons donc obtenu qu'il existe deux polynômes trigonométriques à valeurs réelles $A_{\alpha,H}$ et $B_{\alpha,H}$ tels que pour tout $x \in \mathbb{R}$,

$$|\widetilde{\chi_\alpha}(x) - A_{\alpha,H}(x)| \leq B_{\alpha,H}(x).$$

En particulier

$$|\widetilde{\chi_\alpha}(x+t) - A_{\alpha,H}(x+t)| \leq B_{\alpha,H}(x+t),$$

et en faisant tendre t vers 0, par continuité des polynômes trigonométriques, nous avons le lemme suivant [MR15, Lemma 1] :

Lemme A.3.2. *Pour tout $\alpha \in \mathbb{R}$ tel que $0 \leq \alpha < 1$ et tout entier $H \geq 1$ il existe des polynômes trigonométriques à valeurs réelles $A_{\alpha,H}$ et $B_{\alpha,H}$ tels que pour tout $x \in \mathbb{R}$,*

$$|\chi_\alpha(x) - A_{\alpha,H}(x)| \leq B_{\alpha,H}(x), \tag{A.21}$$

avec

$$A_{\alpha,H}(x) = \sum_{|h|\leq H} a_h(\alpha, H)e(hx), \quad B_{\alpha,H}(x) = \sum_{|h|\leq H} b_h(\alpha, H)e(hx) \tag{A.22}$$

dont les coefficients $a_h(\alpha, H)$ et $b_h(\alpha, H)$ vérifient

$$a_0(\alpha, H) = \alpha, \quad |a_h(\alpha, H)| \leq \min\left(\alpha, \frac{1}{\pi|h|}\right), \quad |b_h(\alpha, H)| \leq \frac{1}{H+1}. \tag{A.23}$$

Il était possible d'obtenir ce lemme avec l'approximation trigonométrique de la fonction $\psi(x)$ fournie par [Vaa85, Theorem 18] : notre fonction χ_α est définie directement à partir de la partie entière. Comme [Vaa85, Theorem 19] est une conséquence de [Vaa85, Theorem 18], les calculs auraient été peu ou prou les mêmes.

Du Lemme A.3.2, on en tire aisément un cas bidimensionnel [MR15, Lemma 2] :

Corollaire A.3.3. *Pour tout $(\alpha_1, \alpha_2) \in [0, 1)^2$, tout entiers $H_1, H_2 \geq 1$ et tout $(x, y) \in \mathbb{R}^2$ nous avons :*

$$\begin{aligned}|\chi_{\alpha_1}(x)\chi_{\alpha_2}(y) - A_{\alpha_1,H_1}(x)A_{\alpha_2,H_2}(y)| \\ \leq \chi_{\alpha_1}(x)B_{\alpha_2,H_2}(y) + B_{\alpha_1,H_1}(x)\chi_{\alpha_2}(y) + B_{\alpha_1,H_1}(x)B_{\alpha_2,H_2}(y).\end{aligned} \tag{A.24}$$

Démonstration. Pour $(x, y) \in \mathbb{R}^2$ nous avons

$$\begin{aligned}\chi_{\alpha_1}(x)\chi_{\alpha_2}(y) - A_{\alpha_1,H_1}(x)A_{\alpha_2,H_2}(y) \\ = \chi_{\alpha_1}(x)(\chi_{\alpha_2}(y) - A_{\alpha_2,H_2}(y)) + \chi_{\alpha_2}(y)(\chi_{\alpha_1}(x) - A_{\alpha_1,H_1}(x)) \\ - (\chi_{\alpha_2}(y) - A_{\alpha_2,H_2}(y))(\chi_{\alpha_1}(x) - A_{\alpha_1,H_1}(x)).\end{aligned}$$

Puisque $\chi_{\alpha_1}(x), \chi_{\alpha_2}(y) \geq 0$, (A.24) résulte de (A.21). □

Nous sommes à présent à même de démontrer un résultat central de notre thèse. Il est technique et se démontre exactement à la manière de [MR15] à la différence toutefois que dans [MR15] il n'apparaît pas explicitement sous la forme d'un lemme, mais se trouve être la conclusion d'un long calcul visant à estimer un terme d'erreur [MR15, pages $2614 - 2616$, Parties 6.1 et 6.2].

Plus précisément, la clé de [MR15] consiste à regarder les chiffres du milieu des entiers concernés. Pour ce faire, il existe une formule qui relie $r_{\mu_0,\mu_2}(n)$, le nombre tel que $n = kq^{\mu_2} + q^{\mu_0}r_{\mu_0,\mu_2}(n) + n \bmod q^{\mu_0}$, avec $0 \leq r_{\mu_0,\mu_2}(n) < q^{\mu_2-\mu_0}$, à la position d'un certain nombre dans l'intervalle $[0, 1)$: le Lemme A.3.2 apparaît sous la forme du Corollaire A.3.3. L'estimation du terme d'erreur est difficile : c'est l'objet du prochain résultat. Les conditions de l'énoncé sont purement techniques et nous permettent de nous placer dans les conditions dans lesquelles apparaît le Corollaire A.3.3 dans le Chapitre 2.

Lemme A.3.4. *Soient $r, s, q, \mu, \mu_0, \mu_1\mu_2, M, N$ des entiers tels que $q \geq 2$, $q^{\mu-1} \leq M < q^{\mu}$, $q^{\nu-1} \leq N < q^{\nu}$, $6\rho \leq \mu$, $\mu - 4\rho \leq \mu_0 \leq \mu \leq \mu_1 \leq \mu_2$, $1 \leq r < q^{\rho}$ et $1 \leq s < q^{2\rho}$. Soient à présent $I_2(M,s) = [M/q, M - sq^{\mu_1})$, g une application quelconque et*

$$\begin{aligned} S_3(r,s) = \sum_{m\in I_2(M,s)} \sum_{n} \sum_{0\leq u_0<q^{\mu_2-\mu_0}} \chi_{q^{\mu_0-\mu_2}}\left(\frac{mn}{q^{\mu_2}} - \frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ \times \sum_{0\leq u_1<q^{\mu_2-\mu_0}} \chi_{q^{\mu_2-\mu_0}}\left(\frac{mn+mr}{q^{\mu_2}} - \frac{u_1}{q^{\mu_2-\mu_0}}\right) \\ \times g(u_1 + q^{\mu_1-\mu_0}sn + q^{\mu_1-\mu_0}sr)\overline{g}(u_1)\overline{g}(u_0 + q^{\mu_1-\mu_0}sn)g(u_0). \end{aligned}$$

Alors nous avons

$$S_3(r,s) = S_4(r,s) + O(\max(\log q^{\mu_0}, \tau(q^{\mu_0}))q^{\mu+\nu-2\rho})$$

avec

$$\begin{aligned} S_4(r,s) = \sum_{m\in I_2(M,s)} \sum_{n} \sum_{0\leq u_0<q^{\mu_2-\mu_0}} A_{q^{\mu_0-\mu_2},q^{\mu_2-\mu_0+2\rho}}\left(\frac{mn}{q^{\mu_2}} - \frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ \times \sum_{0\leq u_1<q^{\mu_2-\mu_0}} A_{q^{\mu_0-\mu_2},q^{\mu_2-\mu_0+2\rho}}\left(\frac{mn+mr}{q^{\mu_2}} - \frac{u_1}{q^{\mu_2-\mu_0}}\right) \\ \times g(u_1 + q^{\mu_1-\mu_0}sn + q^{\mu_1-\mu_0}sr)\overline{g}(u_1)\overline{g}(u_0 + q^{\mu_1-\mu_0}sn)g(u_0), \end{aligned}$$

où $A_{q^{\mu_0-\mu_2},q^{\mu_2-\mu_0+2\rho}}$ est défini par (A.22) *avec $H = q^{\mu_2-\mu_0+2\rho}$.*

Démonstration. Nous utilisons (A.24) avec le choix $H = q^{\mu_2-\mu_0+2\rho}$ sur $S_3(r,s)$ en remarquant que $S_4(r,s)$ correspond au terme approchant. Il nous faut donc borner les termes d'erreurs : les sommes comprenant les termes en $B_{q^{\mu_0-\mu_2},q^{\mu_2-\mu_0+2\rho}}$. Pour alléger les notations, nous conserverons la notation $B_{q^{\mu_0-\mu_2},H}$ tant que le choix de H n'intervient pas dans les calculs.

Nous posons donc

$$\begin{aligned} E_4(r,r') = \sum_{m\in I_2(M,s)} \sum_{n} \sum_{0\leq u_0<q^{\mu_2-\mu_0}} B_{q^{\mu_0-\mu_2},H}\left(\frac{mn+mr}{q^{\mu_2}} - \frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ \times \sum_{0\leq u_1<q^{\mu_2-\mu_0}} \chi_{q^{\mu_0-\mu_2}}\left(\frac{mn+mr'}{q^{\mu_2}} - \frac{u_1}{q^{\mu_2-\mu_0}}\right) \end{aligned}$$

et

$$\begin{aligned} E_4'(r) = \sum_{m\in I_2(M,s)} \sum_{n} \sum_{0\leq u_0<q^{\mu_2-\mu_0}} B_{q^{\mu_0-\mu_2},H}\left(\frac{mn}{q^{\mu_2}} - \frac{u_0}{q^{\mu_2-\mu_0}}\right) \\ \times \sum_{0\leq u_1<q^{\mu_2-\mu_0}} B_{q^{\mu_0-\mu_2},H}\left(\frac{mn+mr}{q^{\mu_2}} - \frac{u_1}{q^{\mu_2-\mu_0}}\right). \end{aligned}$$

Comme $B_{q^{\mu_0-\mu_2},H}$ et $\chi_{q^{\mu_0-\mu_2}}$ sont positives, il est possible détendre la sommation sur tous les entiers m dans $[M/q, M)$. Les termes d'erreurs de (A.24) correspondent à $E_4(r,0)$, $E_4(0,r)$ et $E_4'(r)$.

Commençons par estimer $E_4(r,r')$. À m,n,r' fixés, il ne peut y avoir qu'un seul u_1 tel que $u_1 = r_{\mu_0,\mu_2}(mn+mr')$. En particulier ceci implique

$$\sum_{0\le u_1<q^{\mu_2-\mu_0}} \chi_{q^{\mu_0-\mu_2}}\left(\frac{mn+mr'}{q^{\mu_2}} - \frac{u_1}{q^{\mu_2-\mu_0}}\right) = 1$$

et nous pouvons alors regarder

$$E_4(r,r') = \sum_m \sum_n \sum_{0\le u_0<q^{\mu_2-\mu_0}} B_{q^{\mu_0-\mu_2},H}\left(\frac{mn+mr}{q^{\mu_2}} - \frac{u_0}{q^{\mu_2-\mu_0}}\right)$$

ou encore

$$E_4(r,r') = \sum_{|h_0|\le H} b_{h_0}(q^{\mu_0-\mu_2},H) \sum_m \sum_n \sum_{0\le u_0<q^{\mu_2-\mu_0}} e\left(h_0\frac{mn+mr}{q^{\mu_2}} - h_0\frac{u_0}{q^{\mu_2-\mu_0}}\right).$$

Par (A.23), $|b_{h_0}(q^{\mu_0-\mu_2},H)| \ll 1/H$. En utilisant

$$\frac{1}{q^{\mu_2-\mu_0}} \sum_{0\le u_0<q^{\mu_2-\mu_0}} e\left(-\frac{h_0u_0}{q^{\mu_2-\mu_0}}\right) = \begin{cases} 1 & \text{si } q^{\mu_2-\mu_0}|h_0 \\ 0 & \text{sinon} \end{cases}$$

sous l'écriture $h_0 = h_0' q^{\mu_2-\mu_0}$ nous avons $|E_4(r,r')| \ll E_5$ avec

$$E_5 = \frac{q^{\mu_2-\mu_0}}{H} \sum_{|h_0'|\le H/q^{\mu_2-\mu_0}} \sum_m \left|\sum_n e\left(\frac{h_0'mn}{q^{\mu_0}}\right)\right|.$$

Après sommation sur n nous avons

$$E_5 \ll \frac{q^{\mu_2-\mu_0}}{H} \sum_{|h_0'|\le H/q^{\mu_2-\mu_0}} \sum_m \min\left(N, \left|\sin\pi\frac{h'm}{q^{\mu_0}}\right|^{-1}\right).$$

La sommation sur m se fait à travers au plus $q^{\mu-\mu_0}$ périodes modulo q^{μ_0} et ainsi

$$E_5 \ll q^{\mu-\mu_0}\frac{q^{\mu_2-\mu_0}}{H} \sum_{|h'|\le H/q^{\mu_2-\mu_0}} \sum_{0\le m'<q^{\mu_0}} \min\left(N, \left|\sin\pi\frac{h'm'}{q^{\mu_0}}\right|^{-1}\right).$$

En utilisant l'estimation triviale si $h'=0$ et (A.16) avec $A = \frac{H}{q^{\mu_2-\mu_0}}$ dans le cas contraire, nous obtenons :

$$E_5 \ll q^{\mu+\nu}\frac{q^{\mu_2-\mu_0}}{H} + q^{\mu-\mu_0}(\tau(q^{\mu_0})N + q^{\mu_0}\log q^{\mu_0}).$$

Le choix de H de notre énoncé est

$$H = q^{\mu_2-\mu_0+2\rho} \tag{A.25}$$

avec ce choix, nous obtenons, comme $N \le q^\nu$

$$E_5 \ll q^{\mu+\nu-2\rho} + q^{\mu+\nu-\mu_0}\tau(q^{\mu_0}) + q^\mu \log q^{\mu_0}$$

comme nous avons $\mu_0 \geq \mu - 4\rho$ et $\nu \geq 2\rho$ ceci nous donne :

$$E_4(r,r') \ll E_5 \ll \max(\log q^{\mu_0}, \tau(q^{\mu_0}))q^{\mu+\nu-2\rho}. \tag{A.26}$$

Majorons à présent $E_4'(r)$. Nous rappelons que

$$E_4'(r) = \sum_{|h_0|\leq H}\sum_{|h_1|\leq H} b_{h_0}(q^{\mu_0-\mu_2},H)b_{h_1}(q^{\mu_0-\mu_2},H) \times \sum_m\sum_n \sum_{\substack{0\leq u_0<q^{\mu_2-\mu_0}\\ 0\leq u_1<q^{\mu_2-\mu_0}}} e\left(h_0\frac{mn}{q^{\mu_2}} - h_0\frac{u_0}{q^{\mu_2-\mu_0}}\right) e\left(h_1\frac{mn+mr}{q^{\mu_2}} - h_1\frac{u_1}{q^{\mu_2-\mu_0}}\right).$$

Nous rappelons que si $q^{\mu_2-\mu_0} \nmid h_0$, nous avons $\sum_{0\leq u_0<q^{\mu_2-\mu_0}} e(-h_0u_0/q^{\mu_2-\mu_0}) = 0$ si bien que nous pouvons supposer $h_0 \equiv h_1 \equiv 0 \bmod q^{\mu_2-\mu_0}$. En notant h_0' et h_1' leur quotient respectif dans la division par $q^{\mu_2-\mu_0}$, et en utilisant (A.23), nous obtenons

$$E_4'(r) \ll \frac{q^{2(\mu_2-\mu_0)}}{H^2} \sum_{|h_0'|\leq H/q^{\mu_2-\mu_0}} \sum_{|h_1'|\leq H/q^{\mu_2-\mu_0}} \left|\sum_{m,n} e\left(\frac{(h_0'+h_1')mn + h_1'mr}{q^{\mu_0}}\right)\right|.$$

Classiquement, il convient d'évaluer la somme selon que $h_0' + h_1' = 0$ ($E_{4,1}'(r)$) ou non ($E_{4,2}'(r)$). Si $h_0' + h_1' = 0$, nous obtenons après sommation sur m et n

$$E_{4,1}'(r) \ll \frac{q^{2(\mu_2-\mu_0)}}{H^2} N \sum_{|h_1'|\leq H/q^{\mu_2-\mu_0}} \min\left(M, \left|\sin\pi\frac{h_1'r}{q^{\mu_0}}\right|^{-1}\right).$$

Puisque $1 \leq r \leq q^\rho$ et $H \leq q^\mu$, nous avons $|h_1'r| < q^{\mu-\mu_2+\mu_0+\rho} = q^{\mu_0-\rho}$ de sorte que les valeurs de $h_1'r$ sont toutes distinctes modulo q^{μ_0}. Nous pouvons donc conclure que

$$E_{4,1}'(r) \ll \frac{q^{2(\mu_2-\mu_0)}}{H^2} N(M + q^{\mu_0}\log q^{\mu_0}) \ll \frac{q^{2(\mu_2-\mu_0)}}{H^2} q^{\mu+\nu}(1 + q^{\mu_0-\mu}\log q^{\mu_0}). \tag{A.27}$$

Pour $E_{4,2}'(r)$ nous sommons d'abord sur n :

$$E_{4,2}'(r) \ll \frac{q^{2(\mu_2-\mu_0)}}{H^2} \sum_{h_0'+h_1'\neq 0} \sum_m \min\left(N, \left|\sin\pi\frac{(h_0'+h_1')m}{q^{\mu_0}}\right|^{-1}\right),$$

ce qui en écrivant $h' = h_0' + h_1'$ donne

$$E_{4,2}'(r) \ll \frac{q^{\mu_2-\mu_0}}{H} \sum_{1\leq|h'|\leq 2H/q^{\mu_2-\mu_0}} \sum_m \min\left(N, \left|\sin\pi\frac{h'm}{q^{\mu_0}}\right|^{-1}\right).$$

La sommation sur m parcourt au plus $q^{\mu-\mu_0}$ périodes modulo q^{μ_0} de sorte que

$$E_{4,2}'(r) \ll q^{\mu-\mu_0}\frac{q^{\mu_2-\mu_0}}{H} \sum_{1\leq|h'|\leq 2H/q^{\mu_2-\mu_0}} \sum_{0\leq m'<q^{\mu_0}} \min\left(N, \left|\sin\pi\frac{h'm'}{q^{\mu_0}}\right|^{-1}\right).$$

Nous utilisons alors (A.16) pour dire que

$$E'_{4,2}(r) \ll q^{\mu-\mu_0}(\tau(q^{\mu_0})N + q^{\mu_0}\log q^{\mu_0}) \ll q^{\mu+\nu-\mu_0}\tau(q^{\mu_0}) + q^{\mu}\log q^{\mu_0}. \tag{A.28}$$

Nous réunissons alors (A.27) et (A.28) pour dire

$$E'_4(r) \ll \frac{q^{2(\mu_2-\mu_0)}}{H^2}q^{\mu+\nu}(1+q^{\mu_0-\mu}\log q^{\mu_0}) + q^{\mu+\nu-\mu_0}\tau(q^{\mu_0}) + q^{\mu}\log q^{\mu_0}.$$

Nous avons $\mu_0 \geq \mu - 4\rho \geq 2\rho$ de sorte que, par (A.25)

$$E'_4(r) \ll \max(\log q^{\mu_0}, \tau(q^{\mu_0}))q^{\mu+\nu-2\rho} \tag{A.29}$$

et nous concluons la preuve en réunissant (A.26) et (A.29). □

Remarque A.3.5. *Pour que le terme d'erreur du Lemme A.3.4 soit non trivial, c'est à dire plus petit que $q^{\mu+\nu}$, il est nécessaire de choisir H significativement plus grand que $q^{\mu_2-\mu_0+\log(\mu_0)}$. Ceci vient des sommes en u_0 et u_1 qui sont apparues en cours de calcul dans le Chapitre 2 et qui donnent l'ensemble des valeurs possibles des chiffres du milieu de mn et $mn+mr$. Tout choix de H de la forme $q^{\mu_2-\mu_0+g(\mu+\nu)}$ avec g une fonction linéaire permet d'obtenir que le terme d'erreur est un $o(q^{\mu+\nu})$. Le choix de ρ du Chapitre 2 fait en sorte que H est pris de cette forme.*

Annexe B

Perspectives

Dans cette annexe, nous discutons les différents résultats obtenus dans ces travaux, nous proposons quelques idées d'extension de ces travaux ainsi que quelques conjectures motivées. Certaines pistes semblent relativement faciles à explorer, d'autres plus ardues et sont exposées comme pistes plausibles.

B.1 Sur le Chapitre 1

Concernant la recherche d'un principe d'aléa de Möbius pour les suites définies à partir de valeurs polynomiales sur les chiffres des entiers, utiliser la méthode de Mauduit et Rivat pour couvrir un large cas de ces suites semble raisonnable. Le Théorème 0.4.1 laisse suggérer la conjecture suivante :

Conjecture B.1.1. *Soit $P_N(X_1, \dots, X_N)$ un polynôme à coefficient dans $\mathbb{Z}/2\mathbb{Z}$ de degré k (il y a au plus k variables X_i dans chaque monôme). Alors, en écrivant un entier inférieur à 2^N sous la forme*

$$n = \sum_{i=0}^{N-1} \epsilon_i(n) 2^i$$

et en écrivant $P_N(n) = P_N(\epsilon_0(n), \dots, \epsilon_{N-1}(n))$, il existe des constantes c_1, c_2, c_3 strictement positives ne dépendant pas de N telles que

$$\left| \sum_{n<2^N} \mu(n)(-1)^{P_N(n)} \right| \leq c_1 N^{c_2} 2^{N - c_3 \frac{N}{k 2^k} + o\left(\frac{N}{k2^k}\right)}. \tag{B.1}$$

Un tel polynôme s'écrit

$$P(X_1, \dots, X_N) = \sum_{1 \leq i_1 \leq \dots \leq i_k \leq N} \alpha_{i_1, i_2, \dots, i_k} X_{i_1} \cdots X_{i_k}, \qquad \alpha_{i_1, i_2, \dots, i_k} \in \{0, 1\},$$

où deux coefficients différents peuvent donner le même monôme (par exemple $\alpha_{1,1,2} = \alpha_{1,2,2}$). Une première étape consisterait à simplifier cette écriture, suite à quoi il serait possible de déterminer des conditions sur les $\alpha_{i_1, i_2, \dots, i_k}$ pour que la suite associée au polynôme satisfasse aux propriétés de propagation et de Fourier à l'aide des techniques décrites dans le Chapitre 1.

Si la propriété de Fourier n'était pas satisfaite, on pourrait imaginer qu'il n'y a pas assez de coefficients $\alpha_{i_1,i_2,\dots,i_k}$ non nuls. S'il n'y a qu'un petit nombre de coefficients $\alpha_{i_1,i_2,\dots,i_k}$ non nuls, adapter les méthodes que Green a employées dans [Gre12] semble être une stratégie. Si la propriété de Fourier est vérifiée, mais pas la propriété de propagation, peut-être est-il envisageable de considérer la formule à obtenir comme une conséquence d'un résultat obtenu pour une suite satisfaisant aux deux conditions.

B.2 Sur le Chapitre 2

Il serait intéressant d'élargir les résultats obtenus dans ce chapitre dans le cas où P n'est pas strictement croissante (on pourrait l'imaginer oscillante), où encore regarder la suite

$$a_P(n) = \sum_{i\geq 0} \epsilon_i(n)\dots\epsilon_{i+P(n)}(n),$$

où les changements de blocs ne se fassent pas forcément sur les tailles des entiers. Les idées que nous avons développées au Chapitre 2 pourraient être utiles pour traiter ces questions.

B.3 Sur le Chapitre 3

Les résultats du Chapitre 3 reposent sur le contrôle du nombre de n inférieurs à 2^N possédant k '1' consécutifs dans leur écriture binaire, où $k > \log N/\log 2$. Considérons donc la question suivante : si N est un entier, ω est un mot de taille $k > \log N/\log q$ sur l'alphabet $\{0,\dots,q-1\}$, que peut-on dire, si on note $\epsilon_i(n)$ le i-ième chiffre de n en base q, de

$$\#\{n < q^N : \omega \quad \text{soit un facteur de} \quad \hat{\epsilon}_{N-1}(n)\cdots\hat{\epsilon}_0(n)\} \quad ?$$

On dit qu'un mot ω est un facteur de ω' s'il existe $\hat{\epsilon}_k(\omega'),\dots,\hat{\epsilon}_{k+|\omega|-1}(\omega')$, $|\omega|$ lettres de ω' telles que $\omega = \hat{\epsilon}_k(\omega')\cdots\hat{\epsilon}_{k+|\omega|-1}(\omega')$. Dans le cas $q=2$, un article de Odlyzko [Odl85] fournit un résultat concernant la probabilité qu'un mot ω soit dans un mot ω'.

Par ailleurs, toujours dans l'optique d'un principe d'aléa de Möbius, si un polynôme $P(X_1,\dots,X_N)$ est de degré $k > \log N/\log 2$, et si $\epsilon_i(n)$ désigne le i-ième chiffre de n en base 2, a-t-on

$$\#\{n < 2^N : P(\epsilon_0(n),\dots,\epsilon_{N-1}(n)) \neq 0\} = o(2^N) \quad ? \tag{B.2}$$

Cette question est motivée par le fait que cette identité a été vérifiée dans le Chapitre 3 dans le cas où

$$P(X_1,\dots,X_N) = \sum_{i=1}^{N-k+1} X_i\cdots X_{i+k-1} \tag{B.3}$$

et est toujours vérifiée si $P(X_1,\dots,X_N)$ est composé d'un seul monôme de degré k. En effet, si $\epsilon_{i_1},\dots,\epsilon_{i_k}$ sont tous non nuls, ils sont tous égaux à 1. Les entiers

satisfaisant à cette condition sont au nombre de 2^{N-k}, et comme $k > \log N/\log 2$, ceci est bien un $o(2^N)$.

Enfin, si P est un polynôme de la forme (B.3), tel que

$$\log N/\log 2 \leq k \leq 2\log N/\log 2,$$

que peut-on dire de

$$\sum_{n<2^N} \Lambda(n)(-1)^{P(n)},$$

où $P(n) = P(\epsilon_0(n), \ldots, \epsilon_{N-1}(n))$? Dans le cas $k < \log N/\log 2$, on sait que cette quantité est un $o(2^N)$ et dans le cas $k > 2\log N/\log 2$, on sait par le théorème des nombres premiers et les résultats du Chapitre 3, que c'est équivalent à 2^N.

Bibliographie

[AL91] J-P. Allouche et P. Liardet : Generalized Rudin-Shapiro sequences. *Acta Arith.*, 60(1):1–27, 1991.

[AMF85] J-P. Allouche et M. Mendès France : On an extremal property of the Rudin-Shapiro sequence. *Mathematika*, 32(1):33–38, 1985.

[AS03] J-P. Allouche et J. Shallit : *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, Applications, Generalizations.

[BC70] J. Brillhart et L. Carlitz : Note on the Shapiro polynomials. *Proc. Amer. Math. Soc.*, 25:114–118, 1970.

[Bés72] J. Bésineau : Indépendance statistique d'ensembles liés à la fonction "somme des chiffres". *Acta Arith.*, 20:401–416, 1972.

[BK16] D. Berend et G. Kolesnik : Joint distribution of completely q-additive functions in residue classes. *J. Number Theory*, 160:716–738, 2016.

[Bla] P. Black : Dictionary of algorithms and data structures.

[Bor09] E. Borel : Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, 27:247–271, 1909.

[Bou13] J. Bourgain : Möbius-Walsh correlation bounds and an estimate of Mauduit and Rivat. *J. Anal. Math.*, 119:147–163, 2013.

[Bou15] J. Bourgain : Prescribing the binary digits of primes, II. *Israel J. Math.*, 206(1):165–182, 2015.

[Brü95] J. Brüdern : *Einführung in die analytische Zahlentheorie*. Springer-Verlag Berlin Heidelberg, 1995.

[Cat92] E. Cateland : *Suites digitales et suites k-régulières*. Thèse de doctorat, Université Bordeaux I, 1992.

[CE46] A.H. Copeland et P. Erdős : Note on normal numbers. *Bull. Amer. Math. Soc.*, 52:857–860, 1946.

[CG05] C.Dartyge et G.Tenenbaum : Sommes des chiffres de multiples d'entiers. *Ann. Inst. Fourier (Grenoble)*, 55(7):2423–2474, 2005.

[Cha33] D. G. Champernowne : The construction of decimals normal in the scale of ten. *J. London Math. Soc.*, S1-8(4):254, 1933.

[Dav80] H. Davenport : *Multiplicative Number Theory*. Graduate Texts in Mathematics 74. Springer New York, 2 édition, 1980.

[DMR09] M. DRMOTA, C. MAUDUIT et J. RIVAT : Primes with an average sum of digits. *Compos. Math.*, 145(2):271–292, 2009.

[DMR11] M. DRMOTA, C. MAUDUIT et J. RIVAT : The sum-of-digits function of polynomial sequences. *J. Lond. Math. Soc. (2)*, 84(1):81–102, 2011.

[DMR16] M. DRMOTA, C. MAUDUIT et J. RIVAT : The Thue–Morse sequence along squares is normal (http ://www.dmg.tuwien.ac.at/drmota/). 2016.

[FM96] E. FOUVRY et C. MAUDUIT : Sommes des chiffres et nombres presque premiers. *Math. Ann.*, 305(3):571–599, 1996.

[GK91] S. W. GRAHAM et G. KOLESNIK : *van der Corput's method of exponential sums*, volume 126 de *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[Gol51] M. J. E. GOLAY : Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Am.*, 41(7):468–472, Jul 1951.

[Gre12] B. GREEN : On (not) computing the Möbius function using bounded depth circuits. *Combin. Probab. Comput.*, 21(6):942–951, 2012.

[GSS09] E. GRANT, J. SHALLIT et T. STOLL : Bounds for the discrete correlation of infinite sequences on k symbols and generalized Rudin-Shapiro sequences. *Acta Arith.*, 140(4):345–368, 2009.

[Han16a] G. HANNA : Blocs de chiffres de taille croissante dans les nombres premiers. 2016+.

[Han16b] G. HANNA : Sur les occurrences des mots dans les nombres premiers (http ://arxiv.org/abs/1511.02068). *Acta Arithmetica*, accepté, Août 2016.

[Hux96] M. N. HUXLEY : *Area, lattice points, and exponential sums*, volume 13 de *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1996. Oxford Science Publications.

[HW79] G. H. HARDY et E. M. WRIGHT : *An Introduction to the Theory of Numbers, Fifth edition*. Oxford Univ.Press, New York, 1979.

[IK04] H. IWANIEC et E. KOWALSKI : *Analytic number theory*, volume 53 de *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Kal11] G. KALAI : Walsh Fourier Transform of the Möbius function (mathoverflow), 2011.

[Kal12] G. KALAI : Möbius randomness of the Rudin–Shapiro sequence (mathoverflow), 2012.

[Kim99] D-H. KIM : On the joint distribution of q-additive functions in residue classes. *J. Number Theory*, 74(2):307–336, 1999.

[KS94] J-P. KAHANE et R. SALEM : *Ensembles parfaits et séries trigonométriques*. Hermann, Paris, second édition, 1994. With notes by Kahane, Thomas W. Körner, Russell Lyons and Stephen William Drury.

[Mad14] M. MADRITSCH : Construction of normal numbers via pseudo-polynomial prime sequences. *Acta Arith.*, 166(1):81–100, 2014.

[May16] J. MAYNARD : Primes with restricted digits (arxiv), 2016.

[MMR15] B. MARTIN, C. MAUDUIT et J. RIVAT : Fonctions digitales le long des nombres premiers. *Acta Arith.*, 170(2):175–197, 2015.

[Mon78] H. L. MONTGOMERY : The analytic principle of the large sieve. *Bull. Amer. Math. Soc.*, 84(4):547–567, 1978.

[MR09] C. MAUDUIT et J. RIVAT : La somme des chiffres des carrés. *Acta Math.*, 203(1):107–148, 2009.

[MR10] C. MAUDUIT et J. RIVAT : Sur un problème de Gelfond : la somme des chiffres des nombres premiers. *Ann. of Math. (2)*, 171(3):1591–1646, 2010.

[MR15] C. MAUDUIT et J. RIVAT : Prime numbers along Rudin-Shapiro sequences. *J. Eur. Math. Soc. (JEMS)*, 17(10):2595–2642, 2015.

[Mül16] C. MÜLLNER : Automatic sequences fulfill the full Sarnak conjecture (http ://arxiv.org/abs/1602.03042). Février 2016.

[MZA07] R. MARCHAND et E. ZOHOORIAN AZAD : Limit law of the length of the standard right factor of a Lyndon word. *Combin. Probab. Comput.*, 16(3):417–434, 2007.

[Odl85] A. M. ODLYZKO : Enumeration of strings. *In Combinatorial algorithms on words (Maratea, 1984)*, volume 12 de *NATO Adv. Sci. Inst. Ser. F Comput. Systems Sci.*, pages 205–228. Springer, Berlin, 1985.

[Que87] M. QUEFFÉLEC : Une nouvelle propriété des suites de Rudin-Shapiro. *Ann. Inst. Fourier (Grenoble)*, 37(2):115–138, 1987.

[Rob16] O. ROBERT : On van der Corput's k-th derivative test for exponential sums. *à paraitre dans Indagationes Mathematicae*, 2016+.

[Sha51] H. S. SHAPIRO : *Extremal Problems for Polynomials and Power Series.* Thèse de doctorat, M.I.T., 1951.

[Sha16] J. SHALLIT : Communication privée, 2016.

[Sie17] W. SIERPIŃSKI : Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'une tel nombre. *Bull. Soc. Math. France*, 45:125–132, 1917.

[Sie59] W. SIERPIŃSKI : Sur les nombres premiers ayant des chiffres initiaux et finals donnés. *Acta Arith.*, 5:265–266 (1959), 1959.

[Tao12] T. TAO : The Chowla conjecture and the Sarnak conjecture (wordpress of Terry Tao), 2012.

[Ten08] G. TENENBAUM : *Introduction à la théorie analytique et probabiliste des nombres*, volume 1 de *Cours Spécialisés.* Belin, troisième édition, 2008.

[Vaa85] J.D. VAALER : Some extremal functions in Fourier analysis. *Bull. Amer. Math. Soc. (N.S.)*, 12(2):183–216, 1985.

Résumé

Blocs des chiffres des nombres premiers

Résumé

Au cours de cette thèse nous nous intéressons à des orthogonalités asymptotiques (au sens ou le produit scalaire dans le tore discret de taille N tend vers 0 lorsque N tend vers l'infini) entre certaines fonctions liées aux blocs des chiffres des entiers et la fonction de Möbius (ainsi qu'avec la fonction de von Mangoldt). Ces travaux prolongent ceux de Mauduit et Rivat et répondent partiellement à une question de Kalai posée en 2012. Au cours du Chapitre 1 nous établissons ces estimations asymptotiques dans le cas où la fonction étudiée est une fonction exponentielle d'une fonction qui compte les blocs de chiffres consécutifs ou espacés de taille k fixé dans l'écriture de n en base q. Nous donnons aussi une grande classe de polynômes agissant sur les blocs de chiffres qui nous fournissent un théorème des nombres premiers et une orthogonalité asymptotique avec la fonction de Möbius. Dans le Chapitre 2, nous obtenons un principe d'aléa de Möbius avec dans le cas où notre fonction est une fonction exponentielle d'une fonction qui compte les blocs de '1' consécutifs dans l'écriture de n en base 2, où la taille du bloc est une application croissante tendant vers l'infini, mais avec une certaine restriction de croissance. Dans le cas extrémal, que nous ne pouvons pas traiter, ce problème est lié à l'estimation du nombre de nombres premiers dans la suite des nombres de Mersenne. Dans le Chapitre 3, nous donnons des estimations dans le cas où la fonction est l'exponentielle d'une fonction qui compte les blocs de k '1' dans l'écriture de n en base 2 où k est grand par rapport à log N. Une conséquence du Chapitre 3 est que les résultats du Chapitre 1 sont quasi optimaux.

Mots-clefs

Chiffres, nombres premiers, transformée de Fourier discrète, identité de Vaughan.

Blocks of digits of prime numbers

Abstract

Throughout this thesis, we are interested in asymptotic orthogonality (in the sense that the scale product of the discrete torus of length N tends to zero as N tend to infinity) between some functions related to the blocks of digits of integers and the Möbius function (and also the von Mangoldt function). Our work extends previous results of Mauduit and Rivat, and gives a partial answer to a question posed by Kalai in 2012. Chapter 1 provides estimates in the case of the function is the exponential of a function taking values on the blocks (with and without wildcards) of length k (k fixed) in the digital expansion of n in base q. We also give a large class of polynomials acting on the digital blocks that allow to get a prime number theorem and asymptotic orthogonality with the Möbius function. In Chapter 2, we get an asymptotic formula in the case of our function is the exponential of the function which counts blocks of consecutive '1's in the expansion of n in base 2, where the length of the block is an increasing function that tends (slowly) to infinity. In the extremal case, which we cannot handle, this problem is connected to estimating the number of primes in the sequences of Mersenne numbers. In Chapter 3, we provides estimates on the case of the function is the exponential of a function which count the blocks of k '1's in the expansion of n in base 2 where k is large with respect to log N. A consequence of Chapter 3 is that the results of Chapter 1 are quasi-optimal.

Keywords

Digits, prime numbers, discrete Fourier transform, Vaughan's identity.