UNIVERSITÉ DE LORRAINE | BIBLIOTHÈQUES UNIVERSITAIRES

AVERTISSEMENT
DROIT D'AUTEUR

Ce document est le fruit d'un long travail approuvé par le jury de soutenance et mis à disposition de l'ensemble de la communauté universitaire élargie.

Il est soumis à la propriété intellectuelle de l'auteur. Ceci implique une obligation de citation et de référencement lors de l'utilisation de ce document. Toute contrefaçon, plagiat ou reproduction illicite encourt une poursuite pénale.

Contact bibliothèque : ddoc-theses-contact@univ-lorraine.fr
(Cette adresse ne permet pas de contacter les auteurs)

Code de la Propriété Intellectuelle. articles L 122. 4
Code de la Propriété Intellectuelle. articles L 335.2- L 335.10

UNIVERSITÉ DE LORRAINE
34 COURS LÉOPOLD — CS 25233
54052 NANCY CEDEX
TÉL : 03 54 50 54 00
CONTACT@UNIV-LORRAINE.FR
WWW.UNIV-LORRAINE.FR

UNIVERSITÉ DE LORRAINE

École doctorale IAEM

THÈSE DE DOCTORAT DE L'UNIVERSITÉ DE LORRAINE

Mention : **Mathématiques**

Présentée et soutenue publiquement le 03 juin 2026 par

Nathan Toumi

Polynômes, facteurs premiers et chiffres

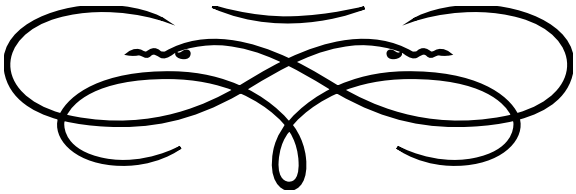
Composition du jury

Président du jury :	Sary Drappeau Professeur, Université Clermont-Auvergne
Rapporteurs :	Sary Drappeau Professeur, Université Clermont-Auvergne Lukas Spiegelhofer Senior Scientist, Montanuniversität Leoben
Examinateurs :	Anne De Roton Maîtresse de conférences, Université de Lorraine Joël Rivat Professeur, Université d'Aix-Marseille Cathy Swaenepoel Maîtresse de conférences, Université Paris-Cité
Directrice et directeur de thèse :	Cécile Dartyge Professeure, Université de Lorraine Thomas Stoll Professeur, Université de Lorraine

Institut Élie Cartan de Lorraine (IECL) – UMR 7502

À Nèpe et Kali. ♡

Remerciements



Se lancer dans une thèse est synonyme de voguer vers un horizon qui nous est inconnu. On ne connaît ni les tenants ni les aboutissants de ce périple, mais il y a à chaque instant ces rayons de soleil – dont la dorure adoucit au contact n'importe quelle personne – qui nous éclairent le chemin au fur et à mesure du voyage. Ces quelques lignes sont ainsi présentes afin de remercier toutes les personnes m'ayant aidé à réaliser cette thèse.

Je tiens à remercier sincèrement *Thomas* et *Cécile* pour m'avoir, d'une part, proposé ce sujet de thèse et, d'autre part, pour vos enseignements ainsi que pour votre présence constante, notamment dans les périodes difficiles. Votre pédagogie est vraiment intègre et complémentaire. Vous avez su m'accompagner dans ce monde qui m'était quasiment inconnu : la recherche. J'ai beaucoup appris à vos côtés, aussi bien sur le plan mathématique que sur le plan pédagogique. Travailler avec vous a été un réel plaisir.

Un remerciement à *Sary Drappeau* pour avoir accepté d'être rapporteur de ma thèse et pour l'intérêt porté à mes travaux. Ich danke *Lukas Spiegelhofer* herzlich dafür, dass er meinen Arbeiten Interesse entgegengebracht und das Gutachten meiner Dissertation übernommen hat. Enfin, un remerciement à *Anne de Roton*, *Joël Rivat* et *Cathy Swaenepoel* et pour l'intérêt porté à mes travaux, en ayant accepté de faire partie de mon jury de thèse.

J'aimerais également remercier les doctorants de l'IECL, à commencer par Sérénouille, la fripouille. Ta solarité étant très contagieuse, j'ai adoré converser et parler de tout avec toi. J'ai également beaucoup apprécié nos « séances de travail ». C'était également très drôle de te voir te battre contre cinquante ennemis dans Minecraft avec ton épée en bois ! Sache que je serai toujours là pour toi. Merci également à Kilian – le sportif frénétique – pour la bonne humeur que tu apportes ainsi que pour les conversations infinies sur des problèmes de maths qui n'avaient pas vraiment de lien avec nos thèses respectives. On arrivait parfois à entraîner Amine dans nos bêtises chronophages. En parlant de toi, Amine, j'aimerais te remercier pour ta gentillesse et ton calme exemplaire, bien que tu as quitté notre bureau ! Un immense merci à toi Aurélie pour toutes ces années depuis notre rencontre en classe prépa. Le fait de « suivre tes pas » était d'une part assez drôle mais en réalité cela m'a beaucoup

aidé. Tu as toujours été là quand j'avais des interrogations que ce soit au niveau de la thèse ou au niveau de l'Éducation Nationale et pour cela : Merci infiniment. Merci à toi, Amine H., pour nos discussions sur divers sujets, parfois profonds. J'admire réellement ta force d'esprit. On peut toujours compter sur toi. J'aimerais également remercier mes co-bureaux, à commencer par Victor – Monsieur V –. Je ne sais même pas si tu liras ces lignes, mais merci pour tout. Je pense avoir été le meilleur co-bureau dans le domaine de l'absentéisme et je le regrette car nos conversations, bien que brèves, m'étaient vraiment enrichissantes. J'admire ton calme et ton efficacité au travail et j'espère que tu t'épanouis dans ton « nouvel » environnement. Merci à toi Hugo – gogoat – pour toutes ces heures face au tableau noir, à écrire, effacer puis réécrire des choses floues. Se poser sur un banc avec toi en fin de journée et parler de tout et de rien était une réelle bouffée d'air, merci. Merci également à Valentin pour ton immense partage des mathématiques ; tu incarnes selon moi le passionné dévoué à la matière. Vous deux ensemble dans le bureau, c'était quelque chose, mais quelque chose de vraiment agréable. Merci à Nathan G. pour ton soutien moral sans précédent ainsi que pour les nombreuses réponses à mes questions. Je te remercie également, Benjamin, pour nos nombreuses discussions très enrichissantes, dans lesquelles j'en apprenais davantage sur ton domaine de recherche. J'ai encore en tête cette fois où l'on est rentrés ensemble après la formation sur la cybersécurité, lors d'un beau jour de printemps rayonnant. Ensuite, j'aimerais te remercier, Marie, pour ton humour et ton altruisme – notamment quand je n'ai plus d'eau, n'est-ce pas ? –. Le fait que l'on ait Loulou en ami commun ne m'étonne finalement pas tant que ça ! Vous êtes de très belles personnes. Merci à toi, Aurélien G., pour ta sympathie et ta bienveillance. J'ai grandement apprécié travailler avec toi. Enfin, un merci sincère à Rodolphe, Aurélien M., Amélie, Julia et Mabrouk. J'ai apprécié partager ces quelques moments avec vous ; cela représente beaucoup pour moi.

Un laboratoire ne peut pas fonctionner sans personnel. J'aimerais remercier le personnel d'appui, notamment Paola, pour ton aide sans précédent à chaque fois que je dois plonger dans les abysses de Notilus. Ta réactivité est exemplaire. Merci également à Élodie et Laurence pour votre bonne humeur constante et votre bienveillance à mon égard, surtout quand j'ai des interrogations. Un immense merci à tous les membres de l'équipe de théorie des nombres pour les nombreux échanges formateurs que nous avons pu avoir. Merci à Jean-Marc pour ta sagesse rassurante ainsi que pour ces conversations dans ta voiture entre Metz et Nancy.

En dehors du laboratoire, j'ai eu la chance d'avoir un entourage omniprésent. Un grand merci à toi Cyril – Bichon – pour tous les moments passés avec toi depuis la Terminale. Il y en a tellement que je ne peux pas tous les citer, mais chacun d'entre eux est encore gravé dans ma mémoire. Tu as été rejoint par Marion – la Pipsouille – ou la meuf qui dort 18h par jour. Nos soirées tous les trois sur Squid Game ou Koh-Lanta sur Roblox étaient vraiment mémorables. Je suis content d'avoir pu souffler ma 28e bougie avec Panpan, à vos côtés. Merci également au groupe des M.C, à savoir Fak, Loulou, Bégbenne et Maxou, pour ces moments inoubliables à la cafét' ainsi que dans différents bars, à raconter vraiment n'importe quoi dans la joie et l'allégresse. Un merci inconditionnel à toutes les personnes que j'ai pu rencontrer en ligne, notamment Jannou, Jadou et Marion. Vous avez grandement contribué à préserver ma santé mentale tout au long de cette thèse, et converser avec vous a toujours été un immense vent de fraîcheur.

Je remercie les professeurs de mathématiques que j'ai pu avoir lors de ma scolarité. Un merci éternel à toi, Olivier, pour avoir changé ma vie et m'avoir fait aimer les mathématiques. Tu es littéralement l'une des genèses de toute cette thèse.

Quand la santé mentale était là, la santé physique ne l'était pas forcément. Je remercie grandement les médecins qui me suivent pour ma pathologie d'avoir toujours été présents dès que je rencontrais un problème. Un immense merci à vous, Dr. Guffroy, Dr. Herber ainsi que Dr. Lenormand, pour tout. Merci également au Dr. Erbstein pour m'avoir toujours motivé et pour avoir toujours cru en moi, malgré les nombreuses difficultés rencontrées au cours de ma vie.

Merci également à Soupi d'avoir enduré mes ronchonneries quotidiennes, de m'avoir rassuré dans mes craintes et de m'avoir tout simplement soutenu. J'en ai de la chance !

J'aimerais conclure ces remerciements en remerciant ma famille, qui a toujours été derrière moi tout au long de ces quatre années. Merci notamment à Mamounet, Papounet, Mimi et Yaya pour tout ce que vous m'avez apporté. Merci également à Lorinda et Dalila pour votre douceur qui apaise n'importe quel cœur.

Table des matières

Introduction **1**
1 Introduction en français 1
1 Les contributions de cette thèse 6
2 Applications à l'études de valeurs polynomiales sous contraintes 7
2 Introduction in English 8
1 Contributions of this thesis 13
2 Applications to the study of polynomial values under constraints 13

Plan de la thèse **15**

Notations **19**

Chapitre 1 Autour des normes de Gowers **21**
1 Naissance des normes de Gowers 21
1 Progressions arithmétiques dans un ensemble 21
2 Définition et comportement polynomial 22
2 Normes de Gowers de la fonction somme des chiffres 23
1 Normes de Gowers de la suite de Thue–Morse ($q = 2$) 23
2 Le cas $q \geq 2$ général 24
3 Preuve du Théorème **1.2.5** 24
1 Formule de récurrence et mise en place du graphe 24
2 Une valeur explicite de η_0 32

Chapitre 2 Le niveau de répartition de la fonction somme des chiffres **41**
1 Définition 41
2 Niveau de répartition de s_2 42
3 Résultats principaux 44
4 Propagation des retenue et troncature 47
5 Preuve du Théorème **2.3.5** 50
1 Étape 1 : Itérations de l'inégalité de van der Corput 50
2 Étape 2 : Décalage et découpage 56
6 Preuve du Théorème **2.3.3** 71
7 Preuve du Théorème **2.3.1** 74
8 Choix des paramètres 76
9 Graphe de la fonction $\varepsilon \mapsto \log \eta(\varepsilon)$ 81

Chapitre 3 Valeurs polynomiales sous contraintes digitales **83**
1 Historique 83
1 Facteurs premiers des valeurs polynomiales 83
2 Le cas général 85
3 Résultats principaux 87

2 Résultats auxiliaires 88
3 Le plus grand facteur premier de $n^2 + 1$ sous contraintes digitales . . 90
1 Définitions et notations spécifiques 91
2 Preuve du Théorème **3.1.13** 91
4 Valeurs polynomiales avec peu de facteurs premiers 99
1 Définitions et premières propriétés 99
2 Preuve du Théorème **3.1.15** 100
5 Valeurs friables de F 103
1 Cadre d'étude 103
2 Preuve du Théorème **3.1.16** 104

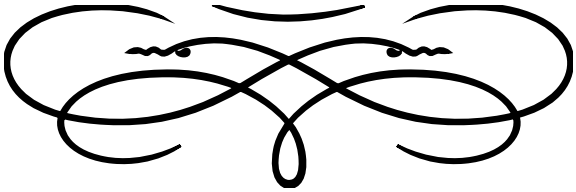
Annexe A : Fractions de Farey 107

Annexe B : Discrépance d'un nombre réel 109

Annexe C : Propriétés de la fonction partie entière 111

Bibliographie 115

Introduction



0.1. Introduction en français

Un rapide retour à l'école.

«Un nombre est divisible par 9 *si et seulement si la somme de ses chiffres est divisible par* 9*.»*

Cette propriété fait rencontrer pour la première fois (et pour la dernière fois dans la plupart des cas) nos écoliers et écolières avec la fonction *somme des chiffres*. Pour beaucoup d'entre eux, ce n'est qu'une règle assez obscure mais très pratique pour justifier si un nombre est divisible par 9 ou non. En réalité, ce critère de divisibilité est un des nombreux résultats concernant cette fonction qui va irriguer l'ensemble de cette thèse.

Comment compter correctement ?

La propriété mise entre guillemets est en fait incomplète dans sa formulation. Il nous faut préciser que le nombre en question est écrit en *base* 10. Cela peut nous paraître naturel étant donné que la majeure partie de la population mondiale actuelle utilise le système de numération décimal (la base 10). Néanmoins, on pouvait compter différemment selon la période dans laquelle on vivait. Au Moyen Âge, on utilisait le système de numération vicésimal (base 20), un héritage gaulois, selon les linguistes. Ce système laisse des traces encore aujourd'hui, notamment dans l'usage du mot «quatre-vingts» pour le nombre 80, ou encore l'hospice des *Quinze-Vingts*, fondé en 1260, qui pouvait accueillir 300 lits. Enfin, en informatique la base 2, la base 16 et la base 32 sont largement utilisés.

Peu importe la base de numération $q \geq 2$ que l'on se donne, chaque entier naturel y trouvera sa représentation. Par exemple, quatre-vingts s'écrit en base 10

$$80 = 8 \times 10^1$$

et s'écrit en base 2

$$1010000 = 1 \times 2^6 + 1 \times 2^4.$$

La fonction somme des chiffres et le théorème de Gelfond.

Pour $q \geq 2$, tout entier n peut être écrit de manière unique comme

$$n = \sum_{k=0}^{L} n_k q^k,$$

où pour tout $k \in \{0, \dots, L-1\}$ on a $n_k \in \{0, \dots, q-1\}$ et $n_L \in \{1, \dots, q-1\}$. Les entiers n_k sont appelés *chiffres*. L'entier $L \geq 0$ est appelé *longueur* de n. La fonction somme des chiffres s_q est définie pour tout $n \in \mathbb{N}$ par

$$s_q(n) = s_q\left(\sum_{k=0}^{L} n_k q^k\right) = \sum_{k=0}^{L} n_k.$$

Par exemple, $s_{10}(123456) = 6+5+4+3+2+1 = 21$. Lors d'une première rencontre avec une fonction, une question que l'on peut se poser est la monotonie de cette dernière. Ici, on peut rapidement se convaincre que la fonction s_q est non monotone. En effet, la valeur 1 est atteinte une infinité de fois (considérer la suite $(q^n)_{n\in\mathbb{N}}$). En considérant de plus pour tout $n > 0$ le nombre de longueur n uniquement composé du chiffre $(q-1)$, on ne peut espérer un comportement asymptotique de s_q. Une propriété importante que vérifie la fonction somme des chiffres est la propriété de q-additivité. En effet, pour $q \geq 2$ fixé et pour $a, b \in \mathbb{N}$ tels que $b < q$, on a

$$s_q(qa + b) = s_q(a) + s_q(b).$$

La q-additivité de s_q nous permet d'avoir la q-multiplicativité de la fonction (pour ℓ, b des entiers et $b \neq 0$)

$$t_q \ : n \mapsto \mathrm{e}\left(\frac{\ell}{b} s_q(n)\right),$$

avec pour tout $t \in \mathbb{R}$, $\mathrm{e}(t) = \exp(2i\pi t)$. La q-multiplicativité de cette fonction se traduit de la manière suivante. Pour tout $a, b \in \mathbb{N}$ tels que $b < q$, on a

$$t_q(qa + b) = t_q(a) t_q(b).$$

La propriété de q-additivité de s_q nous invite dans un premier temps à étudier la répartition de s_q le long des progressions arithmétiques.

En 1968, Gelfond **[Gel68]** a proposé une méthode pour étudier la fonction somme des chiffres à l'aide de sommes d'exponentielles et de représentations sous forme de produits. Il prouva que pour deux entiers $b, q \geq 2$ tels que $(b, q-1) = 1$, on a l'estimation [1]

$$|\{n < N \ : \ s_q(n) \equiv a \pmod b, \ n \equiv r \pmod m\}| = \frac{N}{bm} + \mathcal{O}(N^\lambda), \qquad (1)$$

où

$$\lambda = \frac{1}{2\log q} \log\left(\frac{q \sin(\pi/2b)}{\sin(\pi/2bq)}\right) < 1,$$

avec $m \geq 2$ un entier, $a \in \{0, \dots, b-1\}$ et $r \in \{0, \dots, m-1\}$. Il est important de noter que la constante implicite est indépendante de a, b, m, r. Ce résultat montre que, à module $m \geq 2$ fixé, la fonction s_q se répartit « correctement » dans les classes

1. La condition $(b, q-1) = 1$ peut être retirée au prix d'un terme principal différent.

de congruences modulo b, lorsque l'argument de la fonction est lui-même dans une progression arithmétique. L'étude de la répartition de la fonction somme des chiffres va au-delà des progressions arithmétiques. À la fin de son article, Gelfond **[Gel68]** propose comme ouverture trois problèmes supplémentaires, qu'il serait intéressant de résoudre.

1. **Répartition conjointe.** Soient $b_1, b_2, q_1, q_2 \in \mathbb{N}$ tels que $(b_1, q_1 - 1) = (b_2, q_2 - 1) = 1$. Soient $a_1 \in \{0, \dots, b_1 - 1\}$ et $a_2 \in \{0, \dots, b_2 - 1\}$. Existe-t-il $\lambda < 1$ tel que

$$|\{n < N \ : \ s_{q_1}(n) \equiv a \pmod{b_1}, \ s_{q_2}(n) \equiv a \pmod{b_2}\}| = \frac{N}{b_1 b_2} + \mathcal{O}(N^{\lambda}) \ ?$$

   Kim **[Kim99]** apporta en 1999 une réponse positive à ce premier problème, en améliorant et en généralisant à n'importe quelle fonction q-additive l'estimation asymptotique de Bésineau **[Bes71]** suivante (pour $N \to +\infty$) :

$$|\{n \leq N \ : \ s_{q_i}(n) \equiv a_i \pmod{b_i}, \ (i \in \{1, \dots, \ell\})\}| \sim \frac{N}{q_1 \times \cdots \times q_\ell},$$

   où pour tout $i \in \{1, \dots, \ell\}$, on a $(b_i, q_i - 1) = 1$, $a_i \in \{0, \dots, b_i - 1\}$ et $q_i \neq q_j$ pour $i \neq j$.

2. **Répartition de s_q des nombres premiers.** Il s'agit de s'intéresser au cardinal de l'ensemble des nombres $p \in \mathbb{P}$ inférieurs à x tels $s_q(p) \equiv a \pmod{b}$ (avec $b, q \geq 2$ deux entiers et $a \in \{0, \dots, b-1\}$). Heuristiquement, on s'attend à ce que l'on ait pour $x \to +\infty$,

$$|\{p \leq x \ : \ s_q(p) \equiv a \pmod{b}\}| \sim \frac{(b, q-1)}{b} \pi(x; a, (b, q-1)).$$

   Une première approche consiste à remplacer la condition de primalité par une condition de quasi-primalité. En 1996, Fouvry et Mauduit **[FM96a]** se sont intéressés au deuxième problème de Gelfond pour l'ensemble P_2 des nombres ayant au plus deux facteurs premiers. Plus précisément, lls montrèrent, pour $b, q \geq 2$ tels que $(b, q-1) = 1$ et $a \in \{0, \dots, b-1\}$, l'inégalité suivante :

$$|\{n \leq x \ : \ s_q(n) \equiv a \pmod{b}, \ n = P_2\}| \gg_{b,q} \frac{x}{\log x}.$$

   En 2005, Dartyge et Tenenbaum **[DT05]** généralisèrent ce résultat aux nombres $n \leq x$ ayant *exactement* $r \geq 2$ facteurs premiers, comptés avec multiplicité (notons $\mathcal{E}_r(x)$ cet ensemble). Avec les mêmes hypothèses sur b et q, on a l'inégalité

$$|\{n \in \mathcal{E}_r(x) \ : \ s_q(n) \equiv a \pmod{b}\}| \gg_{r,b,q} \frac{x(\log\log x)^{r-2}}{(\log x)\log\log\log x}.$$

   En 2010, Mauduit et Rivat **[MR10]** résolvèrent le deuxième problème de Gelfond en montrant l'existence d'un réel $c_{b,q} > 0$ tel que

$$|\{p \leq x \ : \ s_q(p) \equiv a \pmod{b}\}| = \frac{(b, q-1)}{b} \pi(x; a, (b, q-1)) + \mathcal{O}_{b,q}\left(x^{1-c_{b,q}}\right).$$

3. **Répartition de s_q des valeurs polynomiales.** Étant donné un polynôme $P \in \mathbb{Z}[X]$, comment estimer l'ensemble des entiers $n \leq x$ tels que $s_q(P(n)) \equiv a \pmod b$? Le problème général est toujours ouvert aujourd'hui. Mauduit et Rivat **[MR95]** ont obtenu un résultat pour la répartition de la fonction s_q le long des suites de la forme $(\lfloor n^c \rfloor)_{n\in\mathbb{N}}$ pour $c \in [1, 4/3[$ (les suites dites de Piatetski–Shapiro). Concernant le cas $b = q = 2$, Müllner et Spiegelhofer **[MS17]** parvinrent à obtenir $3/2$ comme borne supérieure et les techniques actuelles semblent permettre d'obtenir ce résultat pour tout $1 < c < 2$ (voir **[Sha23]**). Concernant le cas du degré 2, une première réponse fut apportée en 2006 par Dartyge et Tenenbaum **[DT06]**. Ils montrèrent l'existence d'une constante $C = C(b, q) > 0$ (avec toujours la condition $(b, q-1) = 1$) telle que pour N suffisamment grand, on a la minoration

$$|\{n < N \ : \ s_q(n^2) \equiv a \pmod b\}| \geq CN.$$

Par ailleurs, dans ce même article, ils proposèrent une première piste de réponse au troisième problème de Gelfond pour un polynôme P quelconque. En effet, pour $P \in \mathbb{Z}[X]$ de degré d, ils prouvèrent l'existence d'une constante $C = C(P, b, q) > 0$ telle que l'on a la minoration (pour N suffisamment grand)

$$|\{0 \leq n \leq N \ : \ s_q(P(n)) \equiv a \pmod b\}| \geq CN^{2/d!}.$$

L'exposant fut amélioré en 2011 par Stoll **[Sto11]**, qui parvint à le faire passer de $2/d!$ à $4/(3d+1)$. Le cas $P = X^2$ fut résolu en 2009 par Mauduit et Rivat **[MR09]**. On a l'estimation asymptotique

$$|\{n \leq x \ : \ s_q(n^2) \equiv a \pmod b\}| = \frac{x}{b}|\{0 \leq n < d \ : \ n^2 \equiv a \pmod d\}| + \mathcal{O}_{b,q}(x^{1-\sigma})$$

où $d = (b, q-1)$ et $\sigma = \sigma(b, q) > 0$ est explicite. Récemment, Spiegelhofer **[Spi23]** résolut le cas $P = X^3$ avec la condition $b = q = 2$. Drmota, Mauduit et Rivat **[DMR11]** ont montré que lorsque la base de numération q est grande, alors le troisième problème de Gelfond est résolu. Si $P \in \mathbb{Z}[X]$ de degré $k \geq 2$ est tel que $P(\mathbb{N}) \subset \mathbb{N}$ et tel que le coefficient dominant de P est premier avec q, alors il existe $\sigma = \sigma(b, q) > 0$ tel que :

$$|\{n \leq x \ : \ s_q(P(n)) \equiv a \pmod b\}| = \frac{x}{b}|\{0 \leq n < d \ : \ P(n) \equiv a \pmod d\}| + \mathcal{O}_{b,q}(x^{1-\sigma}),$$

où $d = (b, q-1)$.

Notion de niveau de répartition

Analysons les limites du théorème de Gelfond donné par **(1)**. Dès lors que m devient très grand (proche de N par exemple), ce théorème ne donne plus d'information, étant donné que le terme principal rentre dans le terme d'erreur. Ce phénomène apparaît dans d'autres études, le plus connu étant le théorème de Siegel–Walfisz, présent dans **[Wal35]**. Ce dernier fournit le comportement asymptotique (pour x suffisamment grand),

$$\sum_{\substack{n\leq x \\ n\equiv a \pmod m}} \Lambda(n) = \frac{x}{\varphi(m)} + \mathcal{O}\left(x \exp\left(-C\sqrt{\log(x)}\right)\right),$$

où $C > 0$ est une constante, $m \geq 2$ et $0 \leq a < m$ tels que $(a, m) = 1$. À l'instar du théorème de Gelfond, il y a une limite pour les valeurs des modules m (donnée dans ce cas par l'inégalité $x \geq \exp\left(m^{1/A}\right)$, où $A > 0$ est un réel). Lorsque l'on étudie des problèmes qui font intervenir des modules proches de x, il est préférable d'avoir des *estimations en moyenne*.
Une première approche afin de comprendre la notion de niveau de répartition est de s'intéresser au théorème ci-dessus. Comme

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

on s'attend à ce que pour presque tout $m \geq 2$ et pour tout $0 \leq a < m$ tels que $(a, m) = 1$ on ait

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{m}}} \Lambda(n) \sim \frac{x}{\varphi(m)}.$$

Afin de comprendre la répartition moyenne de Λ le long des progressions arithmétiques, l'idée est de s'intéresser à la quantité E définie sur $\mathbb{R}^* \times]0, 1[$ par

$$E(x, \theta) := \sum_{m \leq x^\theta} \max_{y \leq x} \max_{\substack{0 \leq a < m \\ (a,m)=1}} \left| \sum_{\substack{n \leq y \\ n \equiv a \pmod{m}}} \Lambda(n) - \frac{y}{\varphi(m)} \right|.$$

L'objectif est ainsi de trouver $0 < \theta < 1$ le plus grand possible afin que l'on ait une inégalité par exemple du type

$$E(x, \theta) \leq x^{1-\eta},$$

avec $\eta > 0$.
En 1965, Bombieri **[Bom65]** et Vinogradov **[Vin65]** publièrent deux articles fondateurs. Dans ces derniers se trouve ce qu'on appellera par la suite le *théorème de Bombieri–Vinogradov*. Ce théorème fournit l'inégalité

$$\sum_{m \leq D} \max_{y \leq x} \max_{\substack{0 \leq a < m \\ (a,m)=1}} \left| \sum_{\substack{n \leq y \\ n \equiv a \pmod{m}}} \Lambda(n) - \frac{y}{\varphi(m)} \right| \ll x^{1/2} D (\log x)^5,$$

pour tout $A > 0$ et pour $x^{1/2}(\log x)^{-A} \leq D \leq x^{1/2}$. On dit alors que la fonction de von Mangoldt a un *niveau de répartition* de (d'au moins) $1/2$. Ceci dit, il n'existe pas encore d'améliorations connues de cet exposant. La conjecture d'Elliott–Halberstam (1968) suggère que l'on peut pousser l'exposant jusqu'à $1 - \varepsilon$ (pour $0 < \varepsilon < 1$).

Une répartition de s_q globalement satisfaisante.

Fouvry et Mauduit **[FM96a]** ont initié l'étude du niveau de répartition de la suite s_q le long des progressions arithmétiques. En effet, ils montrèrent que s_2 possède un niveau de répartition d'au moins 0.5924. Plus précisément, on a, pour tout $A \in \mathbb{R}_+$, l'existence d'un réel $C > 0$ tel que

$$\sum_{1 \leq m \leq x^{0.5924}} \max_{1 \leq z \leq x} \max_{0 \leq r < m} \left| \sum_{\substack{n < z \\ s_2(n) \equiv 0 \pmod 2 \\ n \equiv r \pmod m}} 1 - \frac{z}{2m} \right| \leq C x (\log 2x)^{-A}, \qquad x \to +\infty.$$

Ils ont également étudié le niveau de répartition de s_q pour une base de numération q quelconque. Dans **[FM96b,** p. 340**]**, ils ont explicité un exposant de répartition admissible de s_q et ont montré que ce dernier tendait vers 1 lorsque $q \to +\infty$:

$$\sum_{1\leq m\leq x^{\theta_q-\varepsilon}} \max_{1\leq z\leq x} \max_{0\leq r<m} \left| \sum_{\substack{n<z\\ s_q(n)\equiv a \pmod b\\ n\equiv r \pmod m}} 1-\frac{1}{m} \sum_{\substack{n<z\\ s_q(n)\equiv a \pmod b}} 1\right| = \mathcal{O}(x(\log 2x)^{-A}),$$

avec $b, q \geq 2$, deux entiers tels que $(b, q-1) = 1$, $0 < \varepsilon < 1$ et pour un certain $A > 0$. En 2020, Spiegelhofer **[Spi20]** a amélioré le résultat principal de **[FM96a]**. Il a en effet montré que la suite s_2 admet un niveau de répartition égal à 1. Cela signifie que pour tout $\varepsilon > 0$, il existe $\eta > 0$ tel que

$$\sum_{1\leq m\leq x^{1-\varepsilon}} \max_{\substack{y,z\geq 0\\ z-y\leq x}} \max_{0\leq r<m} \left| \sum_{\substack{y\leq n<z\\ s_2(n)\equiv 0 \pmod 2\\ n\equiv r \pmod m}} 1-\frac{z-y}{2m}\right| \ll x^{1-\eta}, \qquad x \to +\infty.$$

0.1.1. Les contributions de cette thèse

Le résultat central de cette thèse repose sur une estimation en moyenne de la répartition de la fonction s_q. En effet, on montre que pour $0 < \varepsilon < 1$ et $b, q \geq 2$ deux entiers tels que $(b, q-1) = 1$, il existe une constante $C = C(\varepsilon, b, q) > 0$ et un exposant $\eta = \eta(\varepsilon, b, q) > 0$ tels que

$$\sum_{1\leq m\leq x^{1-\varepsilon}} \max_{\substack{y,z\\ 0\leq y<z\\ z-y\leq x}} \max_{r\geq 0} \left| \sum_{\substack{y\leq n<z\\ s_q(n)\equiv a \pmod b\\ n\equiv r \pmod m}} 1-\frac{z-y}{bm}\right| \leq Cx^{1-\eta}.$$

De surcroît, une valeur explicite de l'exposant η est également fournie. L'idée sous-jacente est de passer par les sommes d'exponentielles et d'appliquer l'inégalité de van der Corput un certain nombre de fois. Nous sommes amenés à étudier la suite $(t_q(n))_{n\geq 0}$ définie par

$$t_q(n) = \mathrm{e}\left(\frac{\ell}{b} s_q(n)\right), \tag{2}$$

où $b, \ell \in \mathbb{N}$ sont tels que $1 \leq \ell < b$. Cette généralisation de la suite classique de (Prouhet–)Thue–Morse a fait l'objet d'études depuis longtemps sous divers angles. La première apparition de cette suite remonte au cadre des suites q-multiplicatives dans les travaux de Bellman et Shapiro **[BS48]** en 1948. Nous mentionnons Queffélec (1979) (voir **[Que79]**) ou Coquet la même année (voir **[Coq79]**).
Après divers opérations et remaniements, on se retrouve à devoir estimer la norme de Gowers associée à s_q. Une définition plus complète des normes de Gowers est donnée dans le Chapitre 1. Nous pouvons donc appliquer le premier résultat présenté dans cette thèse, à savoir une estimation des normes de Gowers pour la fonction s_q. On montre que l'on a l'inégalité (pour $(b, q-1) = 1$) et $\rho \to +\infty$,

$$\frac{1}{q^{(k+1)\rho}} \sum_{\substack{0\leq n<q^\rho\\ 0\leq h_0,\dots,h_{k-1}<q^\rho}} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q(n+\mathbf{w}\cdot\mathbf{h})\right) \ll q^{-\eta_0\rho},$$

avec $\eta_0 > 0$ étant explicite.
La principale difficulté de la généralisation des travaux de **[Spi20]** en base q réside

notamment dans l'estimation de la norme de Gowers associée à la fonction somme des chiffres. En effet, pour pouvoir estimer la norme de Gowers de s_2 (en base 2), l'idée de **[Kon19]** est de se ramener à l'étude d'un certain graphe probabiliste, afin de pouvoir appliquer les théorèmes ergodiques pour les chaînes de Markov. Dans notre étude, nous n'avons plus un tel graphe, étant donné que nous obtenons des poids (et non des probabilités) de transition complexes non nécessairement réels. S'intéresser à la combinatoire des mots est un élégant moyen de court-circuiter ce problème et, par ailleurs, nous verrons qu'il nous permettra d'obtenir une valeur explicite pour l'exposant dans l'estimation de la norme de Gowers.

0.1.2. Applications à l'études de valeurs polynomiales sous contraintes

L'étude des valeurs polynomiales premières est encore aujourd'hui un problème qui voit fleurir un grand nombre d'avancées. Elle repose sur une question simple de compréhension : étant donné un polynôme $P \in \mathbb{Z}[X]$ irréductible sans diviseur fixe, existe-t-il une infinité d'entiers n tels que $P(n)$ soit premier ?
A contrario de sa formulation, la résolution de ce problème est très difficile. Actuellement, seul le degré 1 est résolu, par Dirichlet en 1838. Nous étudions les valeurs polynomiales premières $P(n)$, avec une contrainte du type

$$s_q(n) \equiv a \pmod{b},$$

avec la condition $(b, q-1) = 1$. Le premier résultat concerne le polynôme $F = X^2 + 1$. On montre, à l'aide du résultat concernant la répartition de s_q le long des progressions arithmétiques, qu'il existe une infinité d'entiers $n \geq 1$ tels que $s_q(n) \equiv a \pmod{b}$ et tels que le plus grand facteur premier de $F(n)$ est plus grand que n^{θ_b}, où $\theta_b > 1$ est solution de l'équation :

$$1 - \theta_b - 2\log(2 - \theta_b) = \frac{1}{4b}.$$

La preuve s'inspire de celle proposée dans **[DI82]**.

Pour un polynôme $F \in \mathbb{Z}[X]$ de degré $k \geq 2$ quelconque, nous montrons, à l'aide du crible à poids de Richert **[HR13]**, l'inégalité

$$|\{n \leq x \,:\, F(n) = P_{k+1},\ s_q(n) \equiv a \pmod{b}\}| \geq \frac{22k+1}{33bk} \left(\prod_p \frac{1 - \varrho(p)/p}{1 - 1/p} \right) \frac{x}{\log x},$$

où, pour $d \geq 1$, on pose

$$\varrho(d) = |\{m \in \{0, \dots, d-1\},\ F(m) \equiv 0 \pmod{d}\}|.$$

Enfin, pour $F \in \mathbb{Z}[X]$ ayant un discriminant non nul, on s'intéressera à l'étude des valeurs friables de $F(n)$. On rappelle qu'un nombre $n \in \mathbb{N}$ est dit *y-friable* ($y > 2$) si

$$P^+(n) \leq y,$$

où pour $n \geq 2$, $P^+(n)$ désigne le plus grand facteur premier de n. À l'aide des travaux de Mounier **[Mou24]**, on montre l'inégalité

$$|\{n \leq x \,:\, P^+(F(n)) \leq y\,,\ s_q(n) \equiv a \pmod{b}\}| \geq (1 - (k - 1 + \varepsilon)u + o(1))\frac{x}{b},$$

où $x \to +\infty$, $y > x^{k-1+2\varepsilon}$ $(0 < \varepsilon < 1)$ et $u = \log x / \log y$.

La preuve concernant le niveau de répartition de s_q repose en grande partie sur une estimation des normes de Gowers pour la fonction s_q. Récemment, Jelinek **[Jel25]** s'est intéressé à l'obtention d'une estimation concernant la fonction somme des chiffres dans un système de numération $G = (G_i)_{i\in\mathbb{N}}$ plus général (système de numération récurrent linéaire). Il serait intéressant d'étudier le niveau de répartition de la fonction s_G le long des progressions arithmétiques. Cela conduirait à des applications équivalentes à l'études des valeurs polynomiales sous contraintes digitales. Par ailleurs, lors de l'Étape 1 de la preuve du Théorème **3.1.13**, nous retirons la condition portant sur la somme des chiffres, afin d'appliquer le résultat de **[DI82]**. Il serait intéressant d'adapter les résultats auxiliaires de **[DI82]** avec la contrainte

$$s_q(n) \equiv a \pmod{b},$$

notamment ceux portant sur les sommes de Kloosterman. Ceci aurait comme conséquence une amélioration de l'exposant final.

0.2. Introduction in English

A quick return to school.

«*An integer is divisible by* 9 *if and only if the sum of its digits is divisible by* 9.»

This property introduces, for the first time (and in most cases the last time), schoolchildren to the *sum-of-digits* function. For many of them, it is merely a somewhat obscure but very convenient rule to determine whether a number is divisible by 9 or not. In reality, this divisibility criterion is one of many results concerning this function that will permeate the entirety of this thesis.

How should one count properly ?

The property stated above is actually incomplete in its formulation. We have to specify that the number in question is written in *base* 10. This may seem natural, given that the vast majority of the world's population currently uses the decimal numeral system (base 10). Nevertheless, counting methods have varied throughout history. In the Middle Ages, the vigesimal system (base 20) was used, a Gallic legacy according to linguists. This system still leaves traces today, notably in the use of the word «quatre-vingts» for the number 80, or in the poorhouse *des Quinze-Vingts*, founded in 1260, which could accommodate 300 beds. Finally, in computer science, bases 2, 16, and 32 are widely used.

Regardless of the numeral base $q \geq 2$, every natural number admits a representation in that base. For example, eighty is written in base 10 as

$$80 = 8 \times 10^1,$$

and in base 2 as

$$1010000 = 1 \times 2^6 + 1 \times 2^4.$$

The sum-of-digits function and Gelfond's theorem.

For $q \geq 2$, every integer n can be written uniquely as

$$n = \sum_{k=0}^{L} n_k q^k,$$

where for all $k \in \{0, \dots, L-1\}$ we have $n_k \in \{0, \dots, q-1\}$ and $n_L \in \{1, \dots, q-1\}$. The integers n_k are called *digits*, and the integer $L \geq 0$ is called the *length* of n. The sum-of-digits function s_q is defined for all $n \in \mathbb{N}$ by

$$s_q(n) = s_q\left(\sum_{k=0}^{L} n_k q^k\right) = \sum_{k=0}^{L} n_k.$$

For instance, $s_{10}(123456) = 6+5+4+3+2+1 = 21$. When first encountering a function, one natural question concerns its monotonicity. Here, one quickly sees that s_q is not monotonic. Indeed, the value 1 is attained infinitely often (consider the sequence $(q^n)_{n\in\mathbb{N}}$). Moreover, by considering numbers of length n consisting solely of the digit $(q-1)$, no simple asymptotic behavior can be expected for s_q. An important property satisfied by the sum-of-digits function is q-additivity. Indeed, for fixed $q \geq 2$ and for $a, b \in \mathbb{N}$ with $b < q$, one has

$$s_q(qa+b) = s_q(a) + s_q(b).$$

The q-additivity of s_q yields the q-multiplicativity of the function (for integers ℓ, b with $b \neq 0$)

$$t_q : n \mapsto \mathrm{e}\left(\frac{\ell}{b} s_q(n)\right),$$

where for all $t \in \mathbb{R}$, $\mathrm{e}(t) = \exp(2i\pi t)$. The q-multiplicativity of this function means that for all $a, b \in \mathbb{N}$ such that $b < q$, one has

$$t_q(qa+b) = t_q(a)t_q(b).$$

The q-additivity of s_q naturally leads us to study the distribution of s_q along arithmetic progressions.

In 1968, Gelfond **[Gel68]** proposed a method to study the sum-of-digits function using exponential sums and product representations. He proved that for two integers $b, q \geq 2$ such that $(b, q-1) = 1$, we have

$$|\{n < N \,:\, s_q(n) \equiv a \pmod b,\ n \equiv r \pmod m\}| = \frac{N}{bm} + \mathcal{O}(N^\lambda), \tag{3}$$

where

$$\lambda = \frac{1}{2\log q} \log\left(\frac{q\sin(\pi/2b)}{\sin(\pi/2bq)}\right) < 1,$$

with $m \geq 2$, $a \in \{0, \dots, b-1\}$, and $r \in \{0, \dots, m-1\}$. It is important to note that the implied constant is independent of a, b, m, r. This result shows that, for fixed modulus $m \geq 2$, the function s_q is « properly distributed » in congruence classes modulo b, when its argument runs over an arithmetic progression. The study of the distribution of the sum-of-digits function goes beyond arithmetic progressions. At the end of his article, Gelfond proposed three additional open problems.

1. **Joint distribution.** Let b_1, b_2, q_1, q_2 be four integers such that$(b_1, q_1 - 1) = (b_2, q_2 - 1) = 1$. Let $a_1 \in \{0, \dots, b_1 - 1\}$ and $a_2 \in \{0, \dots, b_2 - 1\}$. Does it exist $\lambda < 1$ such that

$$|\{n < N \,:\, s_{q_1}(n) \equiv a_1 \pmod{b_1},\ s_{q_2}(n) \equiv a_2 \pmod{b_2}\}| = \frac{N}{b_1 b_2} + \mathcal{O}(N^\lambda)\ ?$$

Kim **[Kim99]** answered this positively in 1999, generalizing Bésineau's result :

$$|\{n \leq N \ : \ s_{q_i}(n) \equiv a_i \pmod{b_i}, \ (i \in \{1, \dots, \ell\})\}| \sim \frac{N}{q_1 \times \cdots \times q_\ell},$$

where for all $i \in \{1, \dots, \ell\}$, we have $(b_i, q_i - 1) = 1$, $a_i \in \{0, \dots, b_i - 1\}$ and $q_i \neq q_j$ if $i \neq j$.

2. **Distribution of s_q over prime numbers.** We are interested in the cardinality of the set of prime numbers $p \in \mathbb{P}$ less than x such that $s_q(p) \equiv a \pmod{b}$ (where $b, q \geq 2$ are integers and $a \in 0, \dots, b-1$). Heuristically, we expect that as $x \to +\infty$,

$$|\{p \leq x \ : \ s_q(p) \equiv a \pmod{b}\}| \sim \frac{(b, q-1)}{b} \pi(x; a, (b, q-1)).$$

It is natural to first replace the condition of primality with a condition of almost-primality. In 1996, Fouvry and Mauduit **[FM96a]** studied the second problem of Gelfond for the set P_2 of numbers having at most two prime factors. More precisely, they proved, for $b, q \geq 2$ such that $(b, q-1) = 1$ and $a \in \{0, \dots, b-1\}$, the following inequality :

$$|\{n \leq x \ : \ s_q(n) \equiv a \pmod{b}, \ n = P_2\}| \gg_{b,q} \frac{x}{\log x}.$$

In 2005, Dartyge and Tenenbaum **[DT05]** generalized this result to integers $n \leq x$ having *exactly* $r \geq 2$ prime factors, counted with multiplicity (denote this set by $\mathcal{E}_r(x)$). Under the same assumptions on b and q, we have the inequality

$$|\{n \in \mathcal{E}_r(x) \ : \ s_q(n) \equiv a \pmod{b}\}| \gg_{r,b,q} \frac{x(\log\log x)^{r-2}}{(\log x)\log\log\log x}.$$

In 2010, Mauduit and Rivat **[MR10]** solved the second problem of Gelfond by proving that there is an effectively computable real number $c_{b,q} > 0$ such that

$$|\{p \leq x \ : \ s_q(p) \equiv a \pmod{b}\}| = \frac{(b, q-1)}{b} \pi(x; a, (b, q-1)) + \mathcal{O}_{b,q}\left(x^{1-c_{b,q}}\right).$$

3. **Distribution of s_q over polynomial values.** Given a polynomial $P \in \mathbb{Z}[X]$, how can we estimate the set of integers $n \leq x$ such that $s_q(P(n)) \equiv a \pmod{b}$? The problem remains open today. Mauduit and Rivat **[MR95]** obtained a result on the distribution of the function s_q along sequences of the form $(\lfloor n^c \rfloor)_{n \in \mathbb{N}}$ for $c \in [1, 4/3[$ (the so-called Piatetski–Shapiro sequences). In the case $b = q = 2$, Müllner and Spiegelhofer **[MS17]** managed to obtain $3/2$ as an upper bound and current techniques seem to allow to get the result for all $1 < c < 2$ (see **[Sha23]**).

Concerning the degree 2 case, a first answer was given in 2006 by Dartyge and Tenenbaum **[DT06]**. They proved the existence of a constant $C = C(b, q) > 0$ (still under the condition $(b, q-1) = 1$) such that for sufficiently large N, one has the lower bound

$$|\{n < N \ : \ s_q(n^2) \equiv a \pmod{b}\}| \geq CN.$$

Moreover, in the same article, they proposed a first approach to the third problem of Gelfond for a general polynomial P. Indeed, for $P \in \mathbb{Z}[X]$ of degree d, they proved the existence of a constant $C = C(P, b, q) > 0$ such that (for sufficiently large N) one has the lower bound

$$|0 \leq n \leq N \ : \ s_q(P(n)) \equiv a \pmod{b}| \geq CN^{2/d!}.$$

The exponent was improved in 2011 by Stoll **[Sto11]**, who increased it from $2/d!$ to $4/(3d+1)$. The case $P = X^2$ was resolved in 2009 by Mauduit and Rivat **[MR09]**. We have the asymptotic estimate

$$|n \leq x \ : \ s_q(n^2) \equiv a \pmod{b}| = \frac{x}{b}|0 \leq n < d \ : \ n^2 \equiv a \pmod{d}| + \mathcal{O}_{b,q}(x^{1-\sigma})$$

where $d = (b, q-1)$ and $\sigma = \sigma(m, q) > 0$ is explicit. Recently, Spiegelhofer **[Spi23]** solved the case $P = X^3$ under the condition $b = q = 2$. Drmota, Mauduit, and Rivat **[DMR11]** showed that when the base q is large, the third problem of Gelfond is solved. Suppose $P \in \mathbb{Z}[X]$ (with degree $k \geq 2$) such that $P(\mathbb{N}) \subset \mathbb{N}$ and such that its leading coefficient is coprime with q, then there exists $\sigma = \sigma(m, q) > 0$ such that :

$$|\{n \leq x \ : \ s_q(P(n)) \equiv a \pmod{b}\}| = \frac{x}{b}|0 \leq n < d \ : \ P(n) \equiv a \pmod{d}| + \mathcal{O}_{b,q}(x^{1-\sigma}),$$

where $d = (b, q-1)$.

Notion of level of distribution

Let us analyze the limitations of Gelfond's theorem given by **(3)**. As soon as m becomes very large (for instance, close to N), the theorem no longer provides useful information, since the main term is absorbed into the error term. This phenomenon also appears in other contexts, the most well-known being the Siegel–Walfisz theorem (see **[Wal35]**). The latter provides the asymptotic behavior (for sufficiently large x),

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{m}}} \Lambda(n) = \frac{x}{\varphi(m)} + \mathcal{O}\left(x \exp\left(-C\sqrt{\log x}\right)\right),$$

where $C > 0$ is a constant, $m \geq 2$, and $0 \leq a < m$ with $(a, m) = 1$. As in Gelfond's theorem, there is a limitation on the size of the moduli m (in this case given by the inequality $x \geq \exp\left(m^{1/A}\right)$, where $A > 0$ is a real number). When studying problems involving moduli close to x, it is preferable to work with *average estimates*. A first approach to understanding the notion of level of distribution is to examine the theorem above. Since

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

we expect that for almost all $m \geq 2$ and for all $0 \leq a < m$ with $(a, m) = 1$,

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{m}}} \Lambda(n) \sim \frac{x}{\varphi(m)}.$$

To understand the average distribution of Λ along arithmetic progressions, we consider the quantity E, defined on $\mathbb{R}^* \times]0,1[$ by

$$E(x,\theta) := \sum_{m \leq x^\theta} \max_{y \leq x} \max_{\substack{0 \leq a < m \\ (a,m)=1}} \Big| \sum_{\substack{n \leq y \\ n \equiv a \pmod m}} \Lambda(n) - \frac{y}{\varphi(m)} \Big|.$$

The goal is then to find the largest possible $0 < \theta < 1$ such that we have an inequality of the form

$$E(x,\theta) \leq x^{1-\eta},$$

for some $\eta > 0$. In 1965, Bombieri **[Vin65]** and Vinogradov **[Bom65]** proved what is now known as the Bombieri–Vinogradov theorem. *Bombieri–Vinogradov theorem.* This theorem provides the bound

$$\sum_{m \leq Q} \max_{y \leq x} \max_{\substack{0 \leq a < m \\ (a,m)=1}} \Big| \sum_{\substack{n \leq y \\ n \equiv a \pmod m}} \Lambda(n) - \frac{y}{\varphi(m)} \Big| \ll x^{1/2} Q (\log x)^5,$$

where $A > 0$ and $x^{1/2}(\log x)^{-A} \leq Q \leq x^{1/2}$. We then say that the von Mangoldt function has a *level of distribution* (at least) $1/2$. Currently, no improvement of this exponent is known. The Elliott–Halberstam conjecture (1968) suggests that the exponent could be pushed up to $1 - \varepsilon$ (for $0 < \varepsilon < 1$).

The distribution of s_q.

Fouvry and Mauduit **[FM96a]** initiated the study of the level of distribution of the sequence s_q along arithmetic progressions. In particular, they showed that s_2 has a level of distribution of at least 0.5924. More precisely, for $A \in \mathbb{R}$, there exists a constant $C > 0$ such that

$$\sum_{1 \leq m \leq x^{0.5924}} \max_{1 \leq z \leq x} \max_{0 \leq r < m} \Big| \sum_{\substack{n < z \\ s_2(n) \equiv 0 \pmod 2 \\ n \equiv r \pmod m}} 1 - \frac{z}{2m} \Big| \leq C x (\log 2x)^{-A}, \qquad x \to +\infty.$$

They also studied the level of distribution of s_q for an arbitrary base q. In **[FM96b,** p. 340**]**, they provided an explicit admissible exponent θ_q and showed that it tends to 1 as $q \to +\infty$:

$$\sum_{1 \leq m \leq x^{\theta_q - \varepsilon}} \max_{1 \leq z \leq x} \max_{0 \leq r < m} \Big| \sum_{\substack{n < z \\ s_q(n) \equiv a \pmod b \\ n \equiv r \pmod m}} 1 - \frac{1}{m} \sum_{\substack{n < y \\ s_q(n) \equiv a \pmod b}} 1 \Big| = \mathcal{O}(x (\log 2x)^{-A}),$$

where $b, q \geq 2$ with $(b, q-1) = 1$, $0 < \varepsilon < 1$, and for some $A > 0$.
In 2020, Spiegelhofer **[Spi20]** considerably improved the main result of **[FM96a]**, showing that the sequence s_2 has level of distribution 1, which is optimal. This means that for every $\varepsilon > 0$, there exists $\eta > 0$ such that

$$\sum_{1 \leq m \leq x^{1-\varepsilon}} \max_{\substack{y,z \geq 0 \\ z - y \leq x}} \max_{0 \leq r < m} \Big| \sum_{\substack{y \leq n < z \\ s_2(n) \equiv 0 \pmod 2 \\ n \equiv r \pmod m}} 1 - \frac{z-y}{2m} \Big| \ll x^{1-\eta}, \qquad x \to +\infty.$$

0.2.1. Contributions of this thesis

The main result of this thesis is based on an average estimate for the distribution of the function s_q. More precisely, for $0 < \varepsilon < 1$ and integers $b, q \geq 2$ with $(b, q-1) = 1$, we show that there exist constants $C = C(\varepsilon, b, q) > 0$ and $\eta = \eta(\varepsilon, b, q) > 0$ such that

$$\sum_{1 \leq m \leq x^{1-\varepsilon}} \max_{\substack{y,z \\ 0 \leq y < z \\ z-y \leq x}} \max_{r \geq 0} \left| \sum_{\substack{y \leq n < z \\ s_q(n) \equiv a \pmod b \\ n \equiv r \pmod m}} 1 - \frac{z-y}{bm} \right| \leq C x^{1-\eta}.$$

Moreover, an explicit value of the exponent η is provided. The underlying idea is to use exponential sums and apply van der Corput's inequality repeatedly. This naturally leads to the study of the sequence $(t_q(n))_{n \geq 0}$ defined by

$$t_q(n) = \mathrm{e}\left(\frac{\ell}{b} s_q(n)\right), \tag{4}$$

where $b, \ell \in \mathbb{N}$ with $1 \leq \ell < b$. This generalization of the classical (Prouhet–)Thue–Morse sequence has been studied for a long time from various perspectives. It first appeared in the context of q-multiplicative sequences in the work of Bellman and Shapiro **[BS48]** (1948). We also mention Queffélec (1979) **[Que79]** and Coquet (1979) **[Coq79]**. After several transformations, we are led to estimate the Gowers norm associated with s_q. A more complete definition of Gowers norms is given in CHAPTER 1. We then apply the first main result of this thesis, namely an estimate of Gowers norms for the function s_q. We prove that (for $(b, q-1) = 1$ and $\rho \to +\infty$)

$$\frac{1}{q^{(k+1)\rho}} \sum_{\substack{0 \leq n < q^\rho \\ 0 \leq h_0, \ldots, h_{k-1} < q^\rho}} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\ldots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q(n + \mathbf{w} \cdot \mathbf{h})\right) \ll q^{-\eta_0 \rho},$$

with $\eta_0 > 0$ explicit. The main difficulty in extending the work of Spiegelhofer **[Spi20]** to base q lies in estimating the Gowers norm of the sum-of-digits function. Indeed, in base 2, the approach of Konieczny **[Kon19]** reduces the problem to the study of a probabilistic graph, allowing the use of ergodic theorems for Markov chains. In our setting, such a graph no longer exists, since the transition weights are complex and not necessarily real probabilities. Studying the combinatorics of words provides a way to bypass this issue and, moreover, allows us to obtain an explicit exponent in the Gowers norm estimate.

0.2.2. Applications to the study of polynomial values under constraints

The study of prime values of polynomials remains, currently, a problem that continues to see numerous advances. It is based on a simple question of understanding : given an irreducible polynomial $P \in \mathbb{Z}[X]$ with no fixed divisor, does there exist an infinite number of integers n such that $P(n)$ is prime ? Despite its simple formulation, solving this problem is very difficult. At present, only the degree 1 case has been resolved, by Dirichlet in 1838. We study prime polynomial values $P(n)$ under a constraint of the form

$$s_q(n) \equiv a \pmod b,$$

with the condition $(b, q-1) = 1$. The first result concerns the polynomial $F = X^2+1$. Using results on the distribution of s_q along arithmetic progressions, we show that there exist infinitely many integers $n \geq 1$ such that $s_q(n) \equiv a \pmod b$ and such that

the largest prime factor of $F(n)$ is greater than n^{θ_b}, where $\theta_b > 1$ is the solution of the equation :

$$1 - \theta_b - 2\log(2 - \theta_b) = \frac{1}{4b}.$$

The proof is inspired by **[DI82]**. For a general polynomial $F \in \mathbb{Z}[X]$ of degree $k \geq 2$, we show, using Richert's weighted sieve **[HR13]**, the inequality

$$|\{n \leq x \,:\, F(n) = P_{k+1},\, s_q(n) \equiv a \pmod b\}| \geq \frac{22k+1}{33bk} \left(\prod_p \frac{1 - \varrho(p)/p}{1 - 1/p} \right) \frac{x}{\log x},$$

where, for $d \geq 1$, we define

$$\varrho(d) = |\{m \in \{0, \dots, d-1\},\, F(m) \equiv 0 \pmod d\}|.$$

Finally, for $F \in \mathbb{Z}[X]$ with nonzero discriminant, we consider the study of friable values of $F(n)$. Recall that an integer $n \in \mathbb{N}$ is said to be *y-friable* ($y > 2$) if

$$P^+(n) \leq y,$$

where for $n \geq 2$, $P^+(n)$ denotes the largest prime factor of n. Using results of Mounier **[Mou24]**, we obtain the inequality

$$|\{n \leq x \;:\; P^+(F(n)) \leq y\,,\, s_q(n) \equiv a \pmod b\}| \geq (1 - (k - 1 + \varepsilon)u + o(1))\frac{x}{b},$$

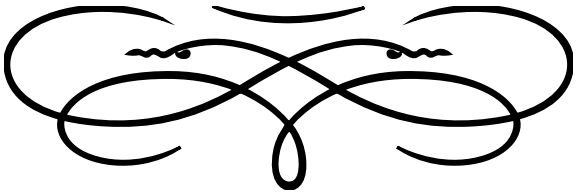
where $x \to +\infty$, $y > x^{k-1+2\varepsilon}$ ($0 < \varepsilon < 1$), and $u = \log x / \log y$.

The proof concerning the level of distribution of s_q relies largely on an estimate of the Gowers norms for the function s_q. Recently, Jelinek **[Jel25]** investigated obtaining an estimate for the sum-of-digits function in a more general numeration system $G = (G_i)_{i \in \mathbb{N}}$ (linear recurrent numeration system). It would be interesting to study the level of distribution of the function s_G along arithmetic progressions. This would lead to applications equivalent to the study of polynomial values under digital constraints. Furthermore, in Étape 1 of the proof of Theorem **3.1.13**, we remove the condition involving the sum of digits in order to apply the result of **[DI82]**. It would be interesting to adapt the auxiliary results of **[DI82]** to include the constraint

$$s_q(n) \equiv a \pmod b,$$

in particular those concerning Kloosterman sums. This would result in an improvement of the final exponent.

Plan de la thèse



Cette thèse est scindée en diverses parties. Il y a des chapitres d'exposition, qui amènent des outils, des définitions et des notations afin de donner un cadre bien défini aux chapitres qui apportent des nouveautés. Pour chaque chapitre, nous donnons la ou les contribution(s) apportée(s) dans cette thèse. Celles-ci proviennent des articles **[Tou25]** (publié) et **[Tou26+]** (soumis).

- Chapitre 1 : Nous nous intéressons à la notion de normes de Gowers de la fonction somme des chiffres. Un rapide historique est donné, afin de comprendre la naissance de ces dernières. Nous y donnons une définition formelle ainsi que des résultats permettant de les évaluer. Le résultat principal de ce chapitre, s'inspirant des travaux de **[Kon19]**, est l'estimation de la norme de Gowers de s_q et de s_q^ρ, avec une proposition d'une formule explicite pour l'exposant. L'entier $s_q^\rho(n)$ est la somme des chiffres tronquée de l'entier n : on ne considère que les ρ premiers chiffres dans l'écriture en base q de n.

  Théorème 1.2.5 : ***[Toumi [Tou25], 2025]***

  Soient b, q deux entiers tels que $(b, q-1) = 1$. Soit $k \geq 3$ un entier et $0 < \ell < b$. Posons
  $$K = \left\lfloor \frac{\log(k)}{\log(q)} \right\rfloor + 1.$$
  On définit
  $$\eta_0 := \frac{1}{\log(q)(K + (k+1)b)q^{(k+1)(K+b(k+1))}}.$$
  Alors, lorsque $\rho \to +\infty$,
  $$\frac{1}{q^{(k+1)\rho}} \sum_{\substack{0 \leq n < q^\rho \\ 0 \leq h_0, \dots, h_{k-1} < q^\rho}} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q(n + \mathbf{w} \cdot \mathbf{h}) \right) \ll q^{-\eta_0 \rho}.$$
  De plus, on dispose de la même formule pour la fonction s_q^ρ : pour $\rho \to +\infty$,
  $$\frac{1}{q^{(k+1)\rho}} \sum_{\substack{0 \leq n < q^\rho \\ 0 \leq h_0, \dots, h_{k-1} < q^\rho}} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^\rho(n + \mathbf{w} \cdot \mathbf{h}) \right) \ll q^{-\eta_0 \rho}.$$

▶ Chapitre 2 : Ce chapitre est dédié à la notion de niveau de répartition d'une suite arithmétique. Il s'ouvre sur des définitions et des résultats concernant le niveau de répartition de certaines suites spécifiques. On généralise à n'importe quelle base de numération le travail de Spiegelhofer **[Spi20]** en prouvant à l'aide du résultat central du Chapitre 1 que la fonction somme des chiffres possède un niveau de répartition égal à 1.

Théorème 3.1.13 : ***[Toumi [Tou25], 2025]***

Soit $0 < \varepsilon < 1$. Soient $b, q \geq 2$ deux entiers tels que $(b, q-1) = 1$. Il existe une constante $C = C(\varepsilon, b, q) > 0$ et un exposant $\eta = \eta(\varepsilon)$, tels que

$$\sum_{1 \leq m \leq x^{1-\varepsilon}} \max_{\substack{y,z \\ 0 \leq y < z \\ z-y \leq x}} \max_{r \geq 0} \left| \sum_{\substack{y \leq n < z \\ s_q(n) \equiv a \pmod b \\ n \equiv r \pmod m}} 1 - \frac{z-y}{bm} \right| \leq C x^{1-\eta}.$$

Une valeur admissible pour η est donnée pour $\varepsilon < \frac{2}{3}(1-\lambda)$ (avec λ défini dans le Théorème 2.7.1) par

$$\eta(\varepsilon) = \frac{\varepsilon^3 \min\left(1/4, 3\log_q(P^-(q))\right)}{7200 \times 8^{1/\varepsilon}\left(\log(4q/\varepsilon) + 5b\log(q)/\varepsilon\right)} \times \exp\left(-\frac{5}{\varepsilon}\left(\log(4q/\varepsilon) + \frac{5b\log(q)}{\varepsilon}\right)\right).$$

▶ Chapitre 3 : Ce dernier chapitre met en lumière quelques applications du résultat du niveau de répartition de la fonction somme des chiffres établi dans le Chapitre 2. On s'intéresse à l'étude des valeurs polynomiales $F(n)$ d'un polynôme F quelconque de degré $k \geq 2$ ayant peu de facteurs premiers avec la condition

$$s_q(n) \equiv a \pmod b,$$

avec l'hypothèse classique $(b, q-1) = 1$. Le premier résultat concerne l'étude du plus grand facteur premier de $n^2 + 1$ sous contraintes digitales.

Théorème 3.1.13 : ***[Toumi [Tou26+], 2026+]***

Soient $b, q \geq 2$ tels que $(b, q-1) = 1$. Pour tout $\varepsilon > 0$, il existe une infinité d'entiers $n \geq 1$ tels que $s_q(n) \equiv a \pmod b$ et tels que le plus grand facteur premier de $n^2 + 1$ est plus grand que $n^{\theta_b - \varepsilon}$, où $\theta_b > 1$ est solution de l'équation :

$$(E_b) \ : \ 1 - \theta_b - 2\log(2 - \theta_b) = \frac{1}{4b}.$$

Concernant le cas d'un polynôme F de degré $k \geq 2$ quelconque irréductible dans $\mathbb{Z}[X]$ et sans diviseur fixe, on a dans un second temps le résultat suivant.

Théorème 3.1.15 : ***[Toumi [Tou26+], 2026+]***

Soit F un polynôme irréductible dans $\mathbb{Z}[X]$ de degré $k \geq 2$ sans diviseur fixe. Il existe une infinité d'entiers n tels que $s_q(n) \equiv a \pmod b$ et tels que $F(n)$ a au plus $(k+1)$ facteurs premiers. Plus précisément, pour $x \to +\infty$

on a :

$$|\{n \leq x \,:\, F(n) = P_{k+1},\, s_q(n) \equiv a \pmod b\}| \geq \frac{22k+1}{33bk} \left(\prod_p \frac{1-\varrho(p)/p}{1-1/p} \right) \frac{x}{\log x},$$

où, pour $d \geq 1$, on pose

$$\varrho(d) = |\{m \in \{0, \ldots, d-1\},\, F(m) \equiv 0 \pmod d\}|.$$

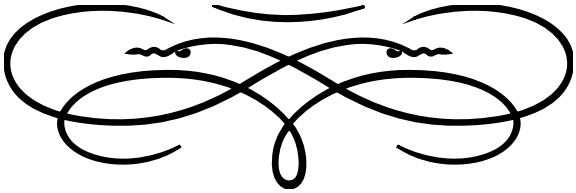
Le chapitre se conclura par l'étude de la proportion d'entiers friables parmi les entiers du type $F(n)$. Le dernier résultat de ce chapitre s'énonce comme suit.

Théorème 3.1.16 : ***[Toumi [Tou26+], 2026+]***

Soit $x > 0$. Soit F un polynôme irréductible de $\mathbb{Z}[X]$ de degré $k \geq 2$ et de discriminant $D \neq 0$. Soient $b, q \in \mathbb{Z}$ tels que $(b, q-1) = 1$. Soit $\varepsilon > 0$. Supposons que $y \geq 1$ est tel que $y > x^{k-1+2\varepsilon}$. Posons $u = \log x / \log y$. Alors, pour $x \to +\infty$, on a la minoration

$$\left|\left\{n \leq x \,:\, P^+(F(n)) \leq y\,,\, s_q(n) \equiv a \pmod b\right\}\right| \geq (1-(k-1+\varepsilon)u+o(1))\frac{x}{b}.$$

Notations



Nous regroupons les notations utilisées dans cette thèse. Certaines sont d'ordre général (non liées spécifiquement au chapitre en cours) et d'autres sont spécifiques à un chapitre.

Notations ensemblistes

- $\mathbb{N}$ désigne l'ensemble des entiers positifs.
- $\mathbb{N}^*$ désigne l'ensemble des entiers strictement positifs.
- L'anneau des polynômes en l'indéterminée X à coefficients entiers est noté $\mathbb{Z}[X]$.
- $\mathbb{P}$ désigne l'ensemble des nombres premiers.
- Pour $n \geq 2$, on note $\mathbb{Z}/n\mathbb{Z}$ l'anneau des classes de congruences modulo n. L'ensemble des inversibles pour la loi $\times$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$.
- Pour $N \geq 1$, on note $[N] := \{1, \dots, N\}$.
- Soit A un ensemble fini. On note $|A|$ son cardinal.
- Pour une famille d'ensembles $A_i \subset \mathbb{R}$ ($i \in \mathbb{N}$) on écrit $\biguplus_{i\geq 0} A_i$ à la place de $\bigcup_{i\geq 0} A_i$ lorsque $A_i \cap A_j = \emptyset$ pour tout $i \neq j$.

Notations fonctionnelles

- La fonction μ est la fonction de Möbius.
- La fonction Λ est la fonction de von Mangoldt.
- La fonction indicatrice d'Euler est notée φ.
- Pour $n \in \mathbb{N}^*$, $\omega(n)$ désigne le nombre de diviseurs premiers de n sans multiplicité.
- Pour $d \geq 2$, $\nu(d)$ désigne le nombre de facteurs premiers de d, comptés avec multiplicité.
- Pour $a, q \in \mathbb{N}^*$ et $x > 0$, on note $\pi(x; q, a)$ le nombre de nombres premiers inférieurs à x qui sont congrus à a modulo q.

- On écrit, de manière usuelle, pour tout $t \in \mathbb{R}$, $\mathrm{e}(t) = e^{2\pi i t}$.
- Pour $z \in \mathbb{C}$, on écrit $\mathcal{C}(z) := \overline{z}$. le conjugué de z.
- Pour $A \subset \mathbb{R}$ et $x \in \mathbb{R}$, on note $\mathbb{1}_A(x) = 1$ si $x \in A$ et 0 sinon.
- Pour $x \in \mathbb{R}$, on pose $\{x\} = x - \lfloor x \rfloor$ (partie fractionnaire de x) et $\langle x \rangle = \left\lfloor x + \frac{1}{2} \right\rfloor$ (entier le plus proche de x).
- Pour $x \in \mathbb{R}$, on définit $\|x\| = \min_{n \in \mathbb{Z}} |x - n|$ (distance à l'entier le plus proche de x).
- Pour $x > 0$, on pose $\log^+(x) = \max(1, \log x)$.
- Pour $x > 0$ et $q > 0$, on écrit $\log_q x = \dfrac{\log x}{\log q}$.
- L'opérateur de conjugaison $z \mapsto \bar{z}$ sera noté $\mathcal{C}$.

Notations générales

- Pour $n \geq 2$, $P^-(n)$ est le plus petit diviseur premier de n.
- Pour $n \geq 2$, $P^+(n)$ désigne le plus grand facteur premier de n.
- Pour $r \in \mathbb{N}^*$, P_r désigne un entier ayant au plus r facteurs premiers.
- Pour $n \geq 2$ et pour $p \in \mathbb{P}$, $v_p(n)$ est le plus grand entier $s \in \mathbb{N}$ tel que $p^s \mid n$.
- Pour $n \in \mathbb{N}$, $u_q(n)$ désigne le chiffre des unités de n dans la base q.
- Soient $a, b \in \mathbb{N}^*$. On note $a \mid b$ lorsque a divise b.
- Pour deux entiers a et b, le nombre (a, b) désigne le plus grand diviseur commun de a et b.
- Pour $w = \sum_{i=0}^{k-1} w_i 2^i$, avec $w_i \in \{0, 1\}$, on écrit de manière concise

$$\mathbf{w} = (w_0, \ldots, w_{k-1}).$$

  ▷ On basculera souvent entre la notation vectorielle $\mathbf{w}$ et l'écriture classique de w en base 2.

- Soient $\mathbf{w}$ et $\mathbf{h}$ deux vecteurs de $\mathbb{R}^k$. On utilise l'écriture du produit scalaire usuel $\mathbf{w} \cdot \mathbf{h}$:

$$\mathbf{w} \cdot \mathbf{h} = \sum_{i=0}^{k-1} w_i h_i.$$

- Sauf mention contraire, p désigne un nombre premier.
- Sauf mention explicite, une somme indexée par p désigne une somme portant sur les nombres premiers.

Chapitre 1

Autour des normes de Gowers

1 Naissance des normes de Gowers **21**
1 Progressions arithmétiques dans un ensemble 21
2 Définition et comportement polynomial 22
2 Normes de Gowers de la fonction somme des chiffres **23**
1 Normes de Gowers de la suite de Thue–Morse ($q = 2$) 23
2 Le cas $q \geq 2$ général 24
3 Preuve du Théorème **1.2.5** **24**
1 Formule de récurrence et mise en place du graphe 24
2 Une valeur explicite de η_0 32

Dans ce chapitre, on démontre le Théorème 1.2.5, relatif aux normes de Gowers de s_q. Les pages 24 à 40 correspondent aux pages **2375** à **2391** de **[Tou25]**.

1.1. Naissance des normes de Gowers

1.1.1. Progressions arithmétiques dans un ensemble

Soit $A \subset \mathbb{N}$ et soit $k \geq 3$. Quelles sont les hypothèses à fournir afin que A contienne une progression arithmétique de longueur k ? Une première réponse fut apportée par Roth **[Rot53]** en 1953. En effet, si on suppose que

$$\limsup_{n \to +\infty} \frac{|A \cap \{1, \dots, n\}|}{n} > 0,$$

alors A contient au moins une progression arithmétique de longueur 3. En 1975, Szemerédi **[Sze75]** généralisa, sous les mêmes hypothèses, à n'importe quelle longueur. Sa preuve est combinatoire et technique. Une approche plus directe est l'utilisation de l'analyse de Fourier (discrète). En effet, pour le cas $k = 3$ (Théorème de Roth) on a, pour $N > 1$,

$$\sum_{n,r \in \mathbb{Z}/n\mathbb{Z}} \mathbb{1}_A(n)\mathbb{1}_A(n+r)\mathbb{1}_A(n+2r) = N^2 \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \widehat{\mathbb{1}_A}(k)\widehat{\mathbb{1}_A}(-2k)\widehat{\mathbb{1}_A}(k).$$

Bien que très élégante, cette approche ne permet pas de traiter les progressions arithmétiques plus grandes que 4. Pour pallier ce problème, Gowers **[Gow01]** présenta

en 2001 une nouvelle approche concernant la preuve du théorème de Szemerédi pour le cas $k = 4$. C'est dans cet article que naissent ce que l'on appelera par la suite les *normes de Gowers*. Une des idées sous-jacentes est de transformer l'étude des progressions arithmétiques en une étude des parallélépipèdes

$$(n + \mathbf{w} \cdot \mathbf{h})_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k}.$$

1.1.2. Définition et comportement polynomial

Définition 1.1.1. Soient $(G, +)$ un groupe abélien fini, $f : G \to \mathbb{C}$ une fonction et $k \geq 1$ un entier. On définit la norme de Gowers d'ordre k de f, notée $\|f\|_{U^k(G)}$, par

$$\|f\|_{U^k(G)}^{2^k} = \frac{1}{|G|^{k+1}} \sum_{\substack{n\in G \\ h_0,\dots,h_{k-1}\in G}} \prod_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} \mathcal{C}^{s_2(w)} \left(f(n + \mathbf{w} \cdot \mathbf{h})\right).$$

Remarque 1.1.2. On peut étendre cette définition à des ensembles qui ne sont pas nécessairement munis d'une structure de groupe. Par exemple, dans notre étude, on s'intéressera à l'intervalle $\{0, \dots, q^\rho - 1\}$, où ρ est un entier positif.

Il est particulièrement intéressant d'étudier les fonctions f du type

$$f = \exp(2i\pi g),$$

avec $g : G \to \mathbb{R}$ une fonction, via sa norme de Gowers. En effet, dans ce cas, on a

$$\|f\|_{U^k(G)}^{2^k} = \frac{1}{|G|^{k+1}} \sum_{\substack{n\in G \\ h_0,\dots,h_{k-1}\in G}} \mathrm{e}\left(\sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} g(n + \mathbf{w} \cdot \mathbf{h}) \right).$$

On observe une alternance de signes selon le nombre de phases $(h_0, h_1, \dots, h_{k-1})$ que l'on ajoute dans l'argument. Cette alternance résulte, dans beaucoup d'études, directement de plusieurs itérations de l'inégalité de van der Corput. Cela sera mis en lumière lors du Chapitre 2.

Les compensations liées aux alternances de signes peuvent révéler le comportement polynomial d'une fonction. Pour le voir, pour tout $h \in G$, on définit l'opérateur $\partial_h : \widehat{G} \to \widehat{G}$ (avec $\widehat{G} = \{f : G \to \mathbb{C}\}$) par :

$$\forall f \in \widehat{G}, \forall x \in G, (\partial_h(f))(x) = f(x + h) - f(x).$$

L'opérateur ∂_h apparaît naturellement lorsque l'on applique l'inégalité de van der Corput. L'utilisation de cette inégalité permet d'obtenir des estimations sur certaines sommes d'exponentielles, nous invitons le lecteur à consulter **[KI04]** pour plus de détails. Pour $f \in \widehat{G}$ donnée, on peut montrer que

$$\forall h_1, h_2 \in G,\ \partial_{h_1}\partial_{h_2} f = 0 \iff \forall x \in G,\ f(x) = a(x) + b,$$

avec a un morphisme de $G \to \mathbb{C}$ et $b \in \mathbb{C}$. Dans ce cas, on dit que f est une fonction « polynomiale » de degré au plus 1. On peut généraliser cette définition à une fonction polynomiale de degré au plus d.

Définition 1.1.3. Une application $\varphi : G \to \mathbb{C}$ est appelée application polynomiale de degré au plus d si pour tout $x, h_1, \dots h_{d+1} \in G$, on a

$$(\partial_{h_1}\partial_{h_2} \cdots \partial_{h_{d+1}}\varphi)(x) = 0.$$

Le lecteur est invité à consulter l'ouvrage de Tao **[Tao12]** pour un voyage plus approfondi autour de l'opérateur ∂_h.
Les normes de Gowers peuvent donc être perçues comme une mesure du comportement d'une fonction f par rapport au comportement polynomial. Pour appuyer ce dire, on peut montrer que pour tout $f \in \widehat{G}$ donnée telle que $\sup\{f(x) \ : \ x \in G\} \leq 1$ on a, pour tout $k > 0$,

$$\|f\|_{U^k(G)} \leq 1,$$

avec égalité si et seulement si

$$f = \exp(\varphi),$$

avec φ une fonction polynomiale de $G \to \mathbb{R}/\mathbb{Z}$ de degré au plus $k-1$.

1.2. Normes de Gowers de la fonction somme des chiffres

1.2.1. Normes de Gowers de la suite de Thue–Morse ($q = 2$)

La suite de Thue–Morse $(\mathtt{t}(n))_{n\in\mathbb{N}}$ est une des suites (binaires) les plus élémentaires en théorie des nombres. Elle peut se construire en considérant la substitution

$$0 \mapsto 01, \ 1 \mapsto 10$$

et en considérant la graine 0. On obtient, par une infinité d'itérations de la substitution, le mot

$$\mathtt{t} = 0110100110010110\ldots.$$

Le $n-$ième terme de la suite de Thue–Morse $\mathtt{t}(n)$ est par définition la n-ième lettre de $\mathtt{t}$. Une propriété, qui nous servira à définir une version algébrique de la suite de Thue–Morse est la suivante (voir **[AS99]** pour plus de détails).

Proposition 1.2.1. *Soit $n \in \mathbb{N}$. Alors $\mathtt{t}(n) = 0$ si et seulement si $s_2(n) \equiv 0 \pmod 2$.*

La suite $((-1)^{s_2(n)})_{n\in\mathbb{N}}$ est donc une définition alternative de la suite de Thue–Morse $\mathtt{t}$.

Remarque 1.2.2. On gardera par la suite l'écriture $\mathtt{t} = ((-1)^{s_2(n)})_{n\in\mathbb{N}}$.

En 2019, Konieczny **[Kon19]** estima la norme de Gowers d'ordre $k \geq 1$ sur l'intervalle $[N] := \{1, \ldots, N\}$ pour $N \to +\infty$ concernant la suite de Thue–Morse.

Théorème 1.2.3 (**[Kon19]**, Theorem A)**.** *Pour tout $k \geq 0$, il existe $\eta_0 = \eta_0(k) > 0$ tel que pour $N \to +\infty$, on a*

$$\|\mathtt{t}\|_{U^k[N]} \ll_k N^{-\eta_0}.$$

Remarque 1.2.4. L'idée de Konieczny est d'interpréter la formule de récurrence que vérifie une certaine suite (que l'on explicitera dans la suite du chapitre) comme des coefficients d'une « matrice de probabilités de transition » d'une chaîne de Markov. Cela nous invitera à nous intéresser au graphe sous-jacent et à étudier les structures types, comme la finitude, l'irréductibilité ou l'apériodicité du graphe. En effet, ces informations permettent à Konieczny d'appliquer les théorèmes ergodiques pour les chaînes de Markov afin d'avoir une convergence (de vitesse exponentielle) de la chaîne de Markov vers une probabilité stationnaire. C'est dans la vitesse de convergence que réside η_0.

1.2.2. Le cas $q \geq 2$ général

Le but de cette section est de proposer puis démontrer une généralisation du Théorème 1.2.3. Le résultat central de ce chapitre est le suivant.

Théorème 1.2.5. *Soient b, q deux entiers tels que $(b, q-1) = 1$. Soient $k \geq 3$ un entier et $0 < \ell < b$. Posons*

$$K = \left\lfloor \frac{\log(k)}{\log(q)} \right\rfloor + 1.$$

On définit

$$\eta_0 := \frac{1}{\log(q)(K + (k+1)b)q^{(k+1)(K+b(k+1))}}.$$

Alors, lorsque $\rho \to +\infty$,

$$\frac{1}{q^{(k+1)\rho}} \sum_{\substack{0 \leq n < q^\rho \\ 0 \leq h_0, \dots, h_{k-1} < q^\rho}} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q(n + \mathbf{w} \cdot \mathbf{h}) \right) \ll q^{-\eta_0 \rho}.$$

De plus, on dispose de la même formule pour la fonction s_q^ρ : pour $\rho \to +\infty$,

$$\frac{1}{q^{(k+1)\rho}} \sum_{\substack{0 \leq n < q^\rho \\ 0 \leq h_0, \dots, h_{k-1} < q^\rho}} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^\rho(n + \mathbf{w} \cdot \mathbf{h}) \right) \ll q^{-\eta_0 \rho}.$$

Ce théorème généralise le résultat obtenu par Konieczny dans son article **[Kon19]** de 2019. Comme l'a commenté Konieczny dans **[Kon19,** Remark 2.5**]**, le calcul du trou spectral de la matrice $(p_{\mathbf{r_0},\mathbf{r_1}})_{(\mathbf{r_0},\mathbf{r_1}) \in \mathfrak{R}^2}$, où $p_{\mathbf{r_0},\mathbf{r_1}}$ est défini en (1.11) et $\mathfrak{R}$ est défini dans le Lemme 1.3.5, donne une autre valeur admissible pour $b = q = 2$. Toutefois, nous utilisons une approche différente, car $p_{\mathbf{r_0},\mathbf{r_1}}$ n'est pas nécessairement un nombre réel pour des valeurs générales de q et b. Le cas $b = q = 2$ nous conduit à l'estimation de la norme de Gowers pour la suite classique de Thue–Morse. Nous mentionnons également le résultat de Byszewski, Konieczny et Müllner [**[BKM23]**, Theorem A]. Les auteurs prouvèrent que toute suite automatique orthogonale aux suites périodiques est fortement uniforme au sens de Gowers (au sens de [**[BKM23]**, (1), p.2]). Notons que η_0 n'est pas explicite dans leur travail (à l'instar du résultat de Konieczny dans **[Kon19]**), et que le cas s_q mod b n'est pas mentionné explicitement.

1.3. Preuve du Théorème 1.2.5

1.3.1. Formule de récurrence et mise en place du graphe

Dans cette section, en vue d'une utilisation ultérieure du Lemme 2.5.7, nous supposons $k \geq 3$ (les arguments de cette section restent néanmoins valables pour $k = 2$). Rappelons que nous faisons, tout au long de l'étude, l'hypothèse suivante :

$$(b, q-1) = 1 \quad \text{et} \quad 0 < \ell < b.$$

Pour tout $w \in \{0, \dots, 2^k - 1\}$, on écrit

$$w = \sum_{0 \leq i \leq k-1} w_i 2^i,$$

avec $w_i \in \{0, 1\}$, et $\mathbf{w} = (w_0, \dots, w_{k-1})$ est le vecteur des chiffres binaires de l'entier w (nous passerons souvent de la représentation vectorielle à l'entier sans indication au préalable). Nous notons

$$t_q^{(w)}(n) = \mathrm{e}\left((-1)^{s_2(w)}\frac{\ell}{b}s_q(n)\right). \tag{1.1}$$

Observons que **(1.1)** est une généralisation de **(4)**. Le facteur $(-1)^{s_2(w)}$ apparaît naturellement dans le contexte de normes de Gowers, comme nous le verrons plus tard.
Soit $\mathbf{r_0} = (r_{0,w})_{w\in\{0,\dots,2^k-1\}} \in \mathbb{Z}^{2^k}$. Pour $\rho \geq 0$, on considère

$$A(\rho, \mathbf{r_0}) = \frac{1}{q^{(k+1)\rho}} \sum_{\substack{0\leq n<q^\rho \\ \mathbf{h}=(h_0,\dots,h_{k-1})\in\{0,\dots,q^\rho-1\}^k}} \prod_{w=0}^{2^k-1} t_q^{(w)}(n+\mathbf{w}\cdot\mathbf{h}+r_{0,w}), \tag{1.2}$$

où $\mathbf{w}\cdot\mathbf{h}$ est le produit scalaire usuel définit par

$$\mathbf{w}\cdot\mathbf{h} = \sum_{i=0}^{k-1} w_i h_i.$$

Dans un premier temps, nous établissons une formule de récurrence pour $A(\rho, \mathbf{r_0})$ en nous basant sur la q-multiplicativité de la suite $(t_q^{(w)}(n))_{n\in\mathbb{N}}$. Cette relation de récurrence peut être interprétée comme une relation de récurrence du type

$$X_\rho = MX_{\rho-1},$$

où X_ρ est un vecteur et M une matrice telle que $|M|$ est stochastique[1].
Cela nous conduit à examiner le « graphe probabiliste » sous-jacent associé à M. Pour cette première étape, nous suivons l'argument donné par Konieczny dans la démonstration de **[Kon19,** Lemma 2.1, p. 1902**]**.

Lemme 1.3.1. *Soit $k \geq 3$ un entier. Pour tout $\mathbf{r_0} \in \mathbb{Z}^{2^k}$ fixé, la suite $(A(\rho, \mathbf{r_0}))_{\rho\geq 1}$ satisfait la relation de récurrence*

$$A(\rho, \mathbf{r_0}) = \frac{1}{q^{k+1}}\,\mathrm{e}\left(\frac{\ell}{b}\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}r_{0,w}\right) \times \sum_{\mathbf{e}=(e_0,\dots,e_k)\in\{0,\dots,q-1\}^{k+1}} A(\rho-1, \delta(\mathbf{r_0};\mathbf{e}))\,\mathrm{e}\left(-\frac{q\ell}{b}\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}\delta(\mathbf{r_0};\mathbf{e})_w\right),$$

où $\delta(\mathbf{r_0};\mathbf{e}) = (\delta(\mathbf{r_0};\mathbf{e})_w)_{w\in\{0,\dots,2^k-1\}} \in \mathbb{Z}^{2^k}$ est le vecteur défini par

$$\delta(\mathbf{r_0};\mathbf{e})_w = \left\lfloor \frac{r_{0,w} + (1,\mathbf{w})\cdot\mathbf{e}}{q} \right\rfloor, \tag{1.3}$$

pour tout $w \in \{0,\dots,2^k-1\}$, avec la notation raccourcie $(1,\mathbf{w})\cdot\mathbf{e} = e_0 + \sum_{i=1}^{k} w_{i-1}e_i$.

1. Une matrice $M = (m_{i,j})_{(i,j)\in\{1,\dots,n\}^2} \in \mathcal{M}_n(\mathbb{R})$ est dite stochastique si M est à coefficients positifs et que pour tout $i \in \{1,\dots,n\}$ on a

$$\sum_{j=1}^{n} m_{i,j} = 1.$$

Démonstration. Soient $0 \leq n < q^\rho$ et $h = (h_0, \dots, h_{k-1})$ avec $0 \leq h_i < q^\rho$ pour $0 \leq i \leq k-1$. En effectuant une division euclidienne, il existe un unique $(2k+2)$-uplet d'entiers $(n', h'_0, \dots, h'_{k-1}, e_0, \dots, e_k)$ tels que $0 \leq n' < q^{\rho-1}$, $0 \leq h'_i < q^{\rho-1}$ $(1 \leq i \leq k-1)$, et $0 \leq e_i < q$ $(0 \leq i \leq k)$, et tels que

$$\begin{cases} n & = qn' + e_0, \\ h_0 & = qh'_0 + e_1, \\ & \vdots \\ h_{k-1} & = qh'_{k-1} + e_k. \end{cases}$$

Ainsi, pour tout $\mathbf{w} = (w_0, \dots, w_{k-1})$, on a

$$n + \mathbf{w} \cdot \mathbf{h} = q(n' + \mathbf{w} \cdot \mathbf{h}') + (1, \mathbf{w}) \cdot \mathbf{e}.$$

Par unicité des paramètres de la division euclidienne, on observe que

$$\begin{aligned} Q &:= \{n + \mathbf{w} \cdot \mathbf{h} \,|\, w \in \{0, \dots, 2^k - 1\} \\ &= \{q(n' + \mathbf{w} \cdot \mathbf{h}') + (1, \mathbf{w}) \cdot \mathbf{e} \,|\, w \in \{0, \dots, 2^k - 1\}\} \end{aligned}$$

est en bijection avec le cube

$$Q' = \{n' + \mathbf{w} \cdot \mathbf{h}' \,|\, w \in \{0, \dots, 2^k - 1\}\}.$$

Par définition de $A(\rho, \mathbf{r_0})$ (voir **(1.2)**),

$$A(\rho, \mathbf{r_0}) = \frac{1}{q^{(k+1)\rho}} \sum_{\substack{0 \leq n' < q^{\rho-1} \\ \mathbf{h}' = (h'_0, \dots, h'_{k-1}) \in \{0, \dots, q^{\rho-1}-1\}^k \\ \mathbf{e} = (e_0, \dots, e_k) \in \{0, \dots, q-1\}^{k+1}}} \prod_{w=0}^{2^k-1} t_q^{(w)}(q(n' + \mathbf{w} \cdot \mathbf{h}') + (1, \mathbf{w}) \cdot \mathbf{e} + r_{0,w}). \tag{1.4}$$

Pour tout $0 \leq n' < q^{\rho-1}$, $\mathbf{h}' \in \{0, \dots, q^{\rho-1} - 1\}^k$ et $\mathbf{e} \in \{0, \dots, q-1\}^{k+1}$, on rappelle que

$$t_q^{(w)}(q(n' + \mathbf{w} \cdot \mathbf{h}') + (1, \mathbf{w}) \cdot \mathbf{e} + r_{0,w}) = \mathrm{e}\left((-1)^{s_2(w)} \frac{\ell}{b} s_q(q(n' + \mathbf{w} \cdot \mathbf{h}') + (1, \mathbf{w}) \cdot \mathbf{e} + r_{0,w}) \right).$$

Comme pour tout $n \in \mathbb{N}$ on a

$$s_q(n) = s_q\left(\left\lfloor \frac{n}{q} \right\rfloor \right) + u_q(n), \tag{1.5}$$

où $u_q(n)$ désigne le chiffre des unités de n en base-q, on obtient

$$\begin{aligned} t_q^{(w)}(q(n' + \mathbf{w} \cdot \mathbf{h}') + (1, \mathbf{w}) \cdot \mathbf{e} + r_{0,w}) = \\ \mathrm{e}\left((-1)^{s_2(w)} \frac{\ell}{b} (s_q(n' + \mathbf{w} \cdot \mathbf{h}' + \delta(\mathbf{r_0}; \mathbf{e})_w) + u_q((1, \mathbf{w}) \cdot \mathbf{e} + r_{0,w})) \right), \end{aligned} \tag{1.6}$$

avec

$$\delta(\mathbf{r_0}; \mathbf{e})_w = \left\lfloor \frac{r_{0,w} + (1, \mathbf{w}) \cdot \mathbf{e}}{q} \right\rfloor.$$

En insérant (1.6) dans (1.4), on a

$$A(\rho,\mathbf{r_0}) = \frac{1}{q^{(k+1)\rho}} \sum_{\substack{0\le n'<q^{\rho-1}\\ \mathbf{h}'=(h'_0,\dots,h'_{k-1})\in\{0,\dots,q^{\rho-1}-1\}^k\\ \mathbf{e}=(e_0,\dots,e_k)\in\{0,\dots,q-1\}^{k+1}}} \prod_{w=0}^{2^k-1} \mathrm{e}\left((-1)^{s_2(w)}\frac{\ell}{b}u_q((1,\mathbf{w})\cdot\mathbf{e}+r_{0,w})\right) \times \prod_{w=0}^{2^k-1} t_q^{(w)}(n'+\mathbf{w}\cdot\mathbf{h}'+\delta(\mathbf{r_0};\mathbf{e})_w).$$

Le premier produit étant indépendant de n' et $\mathbf{h}'$, il s'ensuit que

$$A(\rho,\mathbf{r_0}) = \frac{1}{q^{k+1}} \sum_{\mathbf{e}=(e_0,\dots,e_k)\in\{0,\dots,q-1\}^{k+1}} \mathrm{e}\left(\frac{\ell}{b}S(\mathbf{r_0},\mathbf{e})\right) A(\rho-1,\delta(\mathbf{r_0};\mathbf{e})), \tag{1.7}$$

où

$$S(\mathbf{r_0},\mathbf{e}) = \sum_{w=0}^{2^k-1}(-1)^{s_2(w)}u_q((1,\mathbf{w})\cdot\mathbf{e}+r_{0,w}).$$

Remarquons que l'on a le résultat suivant.

Lemme 1.3.2. *Soit $\rho\ge 2$. Pour tout $n\in\mathbb{N}$, on a*

$$s_q^\rho(n) = s_q^{\rho-1}\left(\left\lfloor\frac{n}{q}\right\rfloor\right) + u_q(n).$$

Le Lemme 1.3.2 entraîne l'obtention de la même formule de récurrence (1.7). De ce fait, jusqu'à la fin de la démonstration, nous ne considérerons que s_q, en sachant que toute occurrence de s_q peut être remplacée par s_q^ρ.
Nous réécrivons à présent la somme $S(\mathbf{r_0},\mathbf{e})$ d'une manière plus commode. D'après (1.3),

$$u_q((1,\mathbf{w})\cdot\mathbf{e}+r_{0,w}) = (1,\mathbf{w})\cdot\mathbf{e}+r_{0,w}-q\delta(\mathbf{r_0};\mathbf{e})_w$$

et donc

$$\begin{aligned} S(\mathbf{r_0},\mathbf{e}) &= \sum_{w=0}^{2^k-1}(-1)^{s_2(w)}((1,\mathbf{w})\cdot\mathbf{e}+r_{0,w}-q\delta(\mathbf{r_0};\mathbf{e})_w)\\ &= \sum_{w=0}^{2^k-1}(-1)^{s_2(w)}(r_{0,w}-q\delta(\mathbf{r_0};\mathbf{e})_w) - \sum_{\substack{w=0\\ 2\nmid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e} + \sum_{\substack{w=0\\ 2\mid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e}. \end{aligned}$$

Remarquons que

$$\sum_{\substack{w=0\\ 2\mid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e} = \sum_{\substack{w=0\\ 2\nmid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e}.$$

En effet, pour voir cela, écrivons

$$\sum_{\substack{w=0\\2\nmid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e}=e_0\,|\{0\le w<2^k\ :\ 2\nmid s_2(w)\}|+\sum_{\substack{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k\\2\nmid\sum_{i=0}^{k-1}w_i}}\sum_{r=1}^{k}w_{r-1}e_r$$

$$=e_0\,|\{0\le w<2^k\ :\ 2\nmid s_2(w)\}|+\sum_{r=1}^{k}e_r\sum_{\substack{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k\\2\nmid\sum_{i=0}^{k-1}w_i}}w_{r-1}$$

$$=e_0\,|\{0\le w<2^k\ :\ 2\nmid s_2(w)\}|+\sum_{r=1}^{k}e_r\sum_{\substack{w_0,\dots,w_{k-1}\in\{0,1\}\\w_{r-1}=1\\2\mid\sum_{i\neq r-1}w_i}}1. \tag{1.8}$$

De manière analogue, on a

$$\sum_{\substack{w=0\\2\mid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e}=e_0|\ \{0\le w<2^k\ :\ 2\mid s_2(w)\}|+\sum_{r=1}^{k}e_r\sum_{\substack{w_0,\dots,w_{k-1}\in\{0,1\}\\w_{r-1}=1\\2\nmid\sum_{i\neq r-1}w_i}}1. \tag{1.9}$$

On remarque que les ensembles $\{0\le w<2^k\ :\ 2\mid s_2(w)\}$ et $\{0\le w<2^k\ :\ 2\nmid s_2(w)\}$ sont en bijection. En effet, en modifiant, par exemple, le chiffre des unités binaire de w, on peut passer d'un ensemble à l'autre. De manière équivalente, on peut utiliser l'égalité

$$\sum_{0\le j<2^k}(-1)^{s_2(j)}=0.$$

Un argument similaire basé sur le changement de chiffre (en remarquant que $k\ge 2$) permet de montrer que, pour un r fixé, les deux sommes internes dans (1.8) et (1.9) sont égales.
On obtient donc

$$\sum_{\substack{w=0\\2\mid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e}=\sum_{\substack{w=0\\2\nmid s_2(w)}}^{2^k-1}(1,\mathbf{w})\cdot\mathbf{e}$$

et

$$S(\mathbf{r_0},\mathbf{e})=\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}(r_{0,w}-q\delta(\mathbf{r_0};\mathbf{e})_w).$$

En insérant cela dans (1.7) on obtient la formule de récurrence désirée. □

Remarque 1.3.3. Dans le cas $b=q=2$, qui correspond à la suite de Thue–Morse, la formule de récurrence du Lemme 1.3.1 devient

$$A(\rho,\mathbf{r_0})=\frac{(-1)^{|\mathbf{r_0}|}}{2^{k+1}}\sum_{\mathbf{e}=(e_0,\dots,e_{k-1})\in\{0,1\}^{k+1}}A(\rho-1,\delta(\mathbf{r_0};\mathbf{e})),$$

où $|\mathbf{r_0}|:=\sum_{w\in\{0,\dots,2^{k-1}\}}r_{0,w}$. Il s'agit de la même formule que dans l'article de Konieczny [Kon19, (2.1)] et de Spiegelhofer [Spi20, (5.13)].

Nous remarquons que, dans notre cas plus général, la formule correspondante est plus complexe en raison de la présence de poids multiplicatifs supplémentaires (racines b-ièmes de l'unité) attachés à la somme et aux arguments. Il est quelque peu surprenant de constater que ces racines b-ièmes de l'unité sont reliées à la somme des chiffres binaires de l'indice de sommation w.

Afin d'obtenir une somme portant sur l'ensemble entier $\mathbb{Z}^{2^k}$, nous regroupons les $\mathbf{e} \in \{0,\dots,q-1\}^{k+1}$ tels que $\mathbf{r_1} = \delta(\mathbf{r_0};\mathbf{e})$. La formule du Lemme 1.3.1 devient alors une relation de récurrence avec des poids normalisés attachés à ses termes.

Lemme 1.3.4. *Pour $\mathbf{r_0} \in \mathbb{Z}^{2^k}$, la suite $(A(\rho,\mathbf{r_0}))_{\rho>0}$ vérifie la relation de récurrence*

$$A(\rho,\mathbf{r_0}) = \sum_{\mathbf{r_1}\in\mathbb{Z}^{2^k}} A(\rho-1,\mathbf{r_1})p_{\mathbf{r_0},\mathbf{r_1}}, \tag{1.10}$$

où

$$p_{\mathbf{r_0},\mathbf{r_1}} = \mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r_1}) - \tilde{S}(\mathbf{r_0})\right)\right)\frac{\left|\{\mathbf{e}\in\{0,\dots,q-1\}^{k+1} \,:\, \delta(\mathbf{r_0};\mathbf{e})=\mathbf{r_1}\}\right|}{q^{k+1}}, \tag{1.11}$$

avec

$$\tilde{S}(\mathbf{r}) = -\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}r_w$$

pour

$$\mathbf{r} = (r_w)_{w\in\{0,\dots,2^k-1\}} \in \mathbb{Z}^{2^k}.$$

Le vecteur $\mathbf{r} = (r_w)_{w\in\{0,1\}^k}$ tel que $r_w = 0$ pour tout $w \in \{0,\dots,2^k-1\}$ sera noté

$$\mathbf{0} := (0,0,\dots,0) \in \mathbb{Z}^{2^k}.$$

La formule de récurrence (1.10), ainsi que les poids pouvant être interprétés comme des variables aléatoires complexes de transition, nous invitent à considérer un graphe orienté défini sur l'ensemble $\mathbb{Z}^{2^k}$, constitué des vecteurs $\mathbf{r}$ comme sommets, lesquels sont connectés entre eux dès qu'une condition spécifique sur les poids associés est vérifiée : il existe une arête entre $\mathbf{r_0}$ et $\mathbf{r_1}$ si et seulement s'il existe un $\mathbf{e} \in \{0,\dots,q-1\}^{k+1}$ tel que

$$\delta(\mathbf{r_0};\mathbf{e}) = \mathbf{r_1}.$$

Un sommet $\mathbf{r_1} = (r_{1,w})_w$ est dit « atteignable » à partir d'un sommet $\mathbf{r_0}$ s'il existe un entier $d > 0$ et une suite de vecteurs $\mathbf{r^{(1)}},\dots,\mathbf{r^{(d)}} \in \mathbb{Z}^{2^k}$ tels que

$$p_{\mathbf{r_0},\mathbf{r^{(1)}}} \times p_{\mathbf{r^{(1)}},\mathbf{r^{(2)}}} \times \cdots \times p_{\mathbf{r^{(d-1)}},\mathbf{r^{(d)}}} \times p_{\mathbf{r^{(d)}},\mathbf{r_1}} \neq 0.$$

On écrit

$$\mathbf{r_0} \to \mathbf{r^{(1)}} \to \mathbf{r^{(2)}} \to \cdots \to \mathbf{r^{(d)}} \to \mathbf{r_1},$$

lorsque $\mathbf{r_1}$ est atteignable depuis $\mathbf{r_0}$ via $\mathbf{r^{(1)}},\mathbf{r^{(2)}},\dots,\mathbf{r^{(d)}}$. Intéressons-nous maintenant au graphe formé par les éléments $\mathbf{r_1} \in \mathbb{Z}^{2^k}$ atteignables à partir de $\mathbf{0}$. Le résultat suivant montre qu'il s'agit d'un sous-graphe fini du graphe défini précédemment.

Lemme 1.3.5. *Soit $\mathfrak{R}$ l'ensemble des éléments $\mathbf{r} \in \mathbb{Z}^{2^k}$ atteignables depuis $\mathbf{0}$. Alors $\mathfrak{R}$ est fini, et pour tout $\mathbf{r} = (r_w)_{w\in\{0,\dots,2^k-1\}}$ atteignable depuis $\mathbf{0}$ et pour tout $0 \le w < 2^k$, on a*

$$0 \leq r_w \leq s_2(w).$$

De plus

$$|\mathfrak{R}| \leq \prod_{i=0}^{k} (i+1)^{\binom{k}{i}}.$$

Démonstration. Supposons que

$$\mathbf{0} \to \mathbf{r^{(1)}} \to \mathbf{r^{(2)}} \to \cdots \to \mathbf{r^{(d)}} \to \mathbf{r_1}.$$

Comme $p_{\mathbf{r^{(d)}},\mathbf{r_1}} \neq 0$, il existe un élément $\mathbf{e^{(d)}} \in \{0,\ldots,q-1\}^{k+1}$ tel que pour tout $w \in \{0,\ldots,2^k-1\}$,

$$\delta(\mathbf{r^{(d)}};\mathbf{e^{(d)}})_w = \left\lfloor \frac{r_w^{(d)} + (1,\mathbf{w})\cdot\mathbf{e^{(d)}}}{q} \right\rfloor = r_{1,w}.$$

Dans la même veine, si $d \geq 2$ et si $p_{\mathbf{r^{(d-1)}},\mathbf{r^{(d)}}} \neq 0$, on en déduit l'existence de $\mathbf{e^{(d-1)}} \in \{0,\ldots,q-1\}^{k+1}$ tel que

$$r_{1,w} = \left\lfloor \frac{\left\lfloor \frac{r_w^{(d-1)} + (1,\mathbf{w})\cdot\mathbf{e^{(d-1)}}}{q} \right\rfloor + (1,\mathbf{w})\cdot\mathbf{e^{(d)}}}{q} \right\rfloor.$$

Pour tout $\mathbf{e} \in \{0,\ldots,q-1\}^{k+1}$ et pour tout $0 \leq w < 2^k$ on a la majoration élémentaire

$$(1,\mathbf{w})\cdot\mathbf{e} \leq (q-1)(1+s_2(w)).$$

En itérant le processus ci-dessus, on atteint le point $\mathbf{0}$ après un nombre fini d'étapes. On obtient donc la borne

$$r_{1,w} < (q-1)(1+s_2(w)) \sum_{r=1}^{+\infty} \frac{1}{q^r} = 1 + s_2(w),$$

et on en déduit que $r_{1,w} \leq s_2(w)$. De plus, on remarque que pour tout $w \in \{0,\ldots,2^k-1\}$, on a

$$r_w^{(1)} = \left\lfloor \frac{(1,\mathbf{w})\cdot\mathbf{e^{(0)}}}{q} \right\rfloor \geq 0,$$

et donc $r_w^{(2)},\ldots,r_w^{(d)},r_{1,w} \geq 0$ pour tout $w \in \{0,\ldots,2^k-1\}$. Cela implique que l'ensemble $\mathfrak{R}$ des sommets atteignables à partir de $\mathbf{0}$ est fini, et que pour tout $\mathbf{r} = (r_w)_w \in \mathfrak{R}$, on a

$$0 \leq r_w \leq s_2(w).$$

Concernant le cardinal de $\mathfrak{R}$, on observe que pour tout $\mathbf{r} = (r_w)_{w\in\{0,\ldots,2^k-1\}} \in \mathfrak{R}$ et pour tout $0 \leq i \leq k$ fixé, il y a $\binom{k}{i}$ choix possibles pour les éléments w tels que $s_2(w) = i$. Ainsi, il y a $(i+1)^{\binom{k}{i}}$ choix possibles pour les coordonnées de $\mathbf{r}$ indexées par un w tel que $s_2(w) = i$, ce qui conduit à la borne annoncée. □

En plus de la finitude, notre graphe est fortement connexe. Pour le démontrer, nous introduisons une nouvelle notation. Pour $\mathbf{e} \in \{0,\ldots,q-1\}^{k+1}$, on définit la fonction $\delta_{\mathbf{e}} : \mathbb{Z}^{2^k} \to \mathbb{Z}^{2^k}$ par

$$\delta_{\mathbf{e}}(\mathbf{r}) = \delta(\mathbf{r};\mathbf{e}).$$

Lemme 1.3.6. *Pour* $K := \left\lfloor \frac{\log(k)}{\log(q)} \right\rfloor + 1$ *on a pour tout* $\mathbf{r} \in \mathfrak{R}$ *:*

$$\underbrace{(\delta_{\mathbf{0}} \circ \delta_{\mathbf{0}} \circ \cdots \circ \delta_{\mathbf{0}})}_{K \text{ fois}}(\mathbf{r}) = \mathbf{0}.$$

Démonstration. Soit $\mathbf{r} \in \mathfrak{R}$ et $w \in \{0, \ldots, 2^k - 1\}$. Alors

$$0 \leq \delta_{\mathbf{0}}(\mathbf{r})_w = \left\lfloor \frac{r_w}{q} \right\rfloor \leq \frac{r_w}{q}.$$

Donc,

$$0 \leq \delta_{\mathbf{0}}(\delta_{\mathbf{0}}(\mathbf{r}))_w \leq \frac{r_w}{q^2}.$$

Par récurrence sur le nombre d'itérations de $\delta_{\mathbf{0}}$ et en utilisant le fait que $r_w \leq s_2(w) \leq k$, on obtient

$$0 \leq \underbrace{(\delta_{\mathbf{0}} \circ \delta_{\mathbf{0}} \circ \cdots \circ \delta_{\mathbf{0}})}_{K \text{ fois}}(\mathbf{r})_w \leq \frac{k}{q^K}.$$

Comme $k < q^K$ et $\underbrace{(\delta_{\mathbf{0}} \circ \delta_{\mathbf{0}} \circ \cdots \circ \delta_{\mathbf{0}})}_{K \text{ fois}}(\mathbf{r})_w \in \mathbb{N}$, on a

$$\underbrace{(\delta_{\mathbf{0}} \circ \delta_{\mathbf{0}} \circ \cdots \circ \delta_{\mathbf{0}})}_{K \text{ fois}}(\mathbf{r})_w = 0.$$

□

Le Lemme 1.3.6 nous assure qu'après avoir appliqué K fois l'opérateur $\delta_{\mathbf{0}}$ à n'importe quel sommet du graphe, on atteint inexorablement le sommet $\mathbf{0}$ (ce que l'on décrit parfois aussi comme la propriété de *synchronicité* du graphe).

Proposition 1.3.7. *Soient* $\mathbf{r_0}, \mathbf{r_1} \in \mathfrak{R}$*. Alors,* $\mathbf{r_1}$ *est atteignable à partir de* $\mathbf{r_0}$*.*

Démonstration. Le Lemme 1.3.6 permet d'**atteindre** le point $\mathbf{0}$ en un nombre fini d'étapes. Ensuite, la définition du graphe nous permet d'**atteindre** $\mathbf{r_1}$ en un nombre fini d'étapes à partir de $\mathbf{0}$.

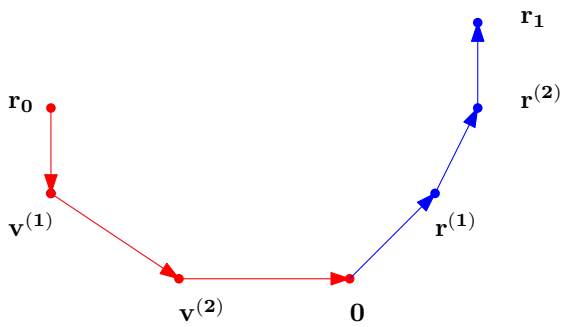


FIGURE 1.1 – Visualisation du parcours de $\mathbf{r_0}$ à $\mathbf{r_1}$.

On peut donc concaténer les deux chemins précédents et ainsi relier $\mathbf{r_0}$ à $\mathbf{r_1}$.

□

Nous pouvons maintenant interpréter la formule (1.10) du Lemme 1.3.4 de manière récursive dans le cadre de notre graphe. Pour $1 \leq j \leq \rho$, et pour tout $\mathbf{r_0} \in \mathfrak{R}$, on a

$$A(\rho, \mathbf{r_0}) = \sum_{\mathbf{r_j} \in \mathfrak{R}} A(\rho - j, \mathbf{r_j})\, p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}, \tag{1.12}$$

où $p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}$ désigne la somme des poids de tous les chemins reliant $\mathbf{r_0}$ à $\mathbf{r_j}$ de longueur j. Rappelons que le poids $p(\gamma)$ d'un chemin γ reliant $\mathbf{r_0}$ à $\mathbf{r_j}$,

$$\gamma \ : \ \mathbf{r_0} \to \mathbf{r^{(1)}} \to \mathbf{r^{(2)}} \to \cdots \to \mathbf{r^{(d)}} \to \mathbf{r_j}$$

est défini par

$$p(\gamma) = p_{\mathbf{r_0},\mathbf{r^{(1)}}} \times p_{\mathbf{r^{(1)}},\mathbf{r^{(2)}}} \times \cdots \times p_{\mathbf{r^{(d-1)}},\mathbf{r^{(d)}}} \times p_{\mathbf{r^{(d)}},\mathbf{r_j}}.$$

Comme $\mathfrak{R}$ est fini, la quantité $v_\rho = \max_{\mathbf{r} \in \mathfrak{R}}(|A(\rho, \mathbf{r})|) < +\infty$ est bien définie. Pour tout $1 \leq j \leq \rho$, on obtient

$$v_\rho \leq v_{\rho - j} \max_{\mathbf{r_0} \in \mathfrak{R}} \left(\sum_{\mathbf{r_j} \in \mathfrak{R}} |p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}| \right). \tag{1.13}$$

Afin de poursuivre la démonstration du Théorème 1.2.5, nous montrons dans la section suivante qu'il existe un entier $j \geq 1$ tel que

$$\sum_{\mathbf{r_j} \in \mathfrak{R}} |p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}| < 1 \tag{1.14}$$

pour tout $\mathbf{r_0} \in \mathfrak{R}$.

1.3.2. Une valeur explicite de η_0

Le but de cette section est de démontrer (1.14), et plus précisément de fournir une valeur effective pour η_0. Cela nous permettra d'obtenir la version effective du Théorème 1.2.5 avec une valeur explicite de η_0 à la fin.
Nous allons montrer qu'il existe un entier $j \geq 1$ tel que

$$M := \max_{\mathbf{r_0} \in \mathfrak{R}} \left(\sum_{\mathbf{r_j} \in \mathfrak{R}} \left| p^{(j)}_{\mathbf{r_0},\mathbf{r_j}} \right| \right) < 1$$

avec une borne effective sur M donnée par une constante strictement inférieure à 1. Soient k et j deux entiers. Soit K défini comme dans le Lemme 1.3.6. On suppose que $j \geq K + b(k+1)$. Nous utilisons deux chemins reliant $\mathbf{0}$ à $\mathbf{0}$ de longueur $(k+1)$ avec des poids différents afin d'obtenir un gain.

Rappelons qu'un chemin de longueur $(k+1)$ reliant un point $\mathbf{r^{(0)}}$ à $\mathbf{r^{(k+1)}}$ via l'opérateur δ (défini en (1.3)) est spécifié par $(k+1)$ vecteurs $\mathbf{e^{(0)}}, \ldots, \mathbf{e^{(k)}} \in \{0, \ldots, q-1\}^{k+1}$ et k vecteurs $\mathbf{r^{(1)}}, \ldots, \mathbf{r^{(k)}} \in \mathbb{Z}^{2^k}$ tels que $\mathbf{r^{(1)}} = \delta(\mathbf{r^{(0)}}; \mathbf{e^{(0)}})$, …, $\mathbf{r^{(k+1)}} = \delta(\mathbf{r^{(k)}}; \mathbf{e^{(k)}})$.
Cela peut être représenté comme suit :

$$\mathbf{r^{(0)}} \xrightarrow{\mathbf{e^{(0)}}} \mathbf{r^{(1)}} \xrightarrow{\mathbf{e^{(1)}}} \cdots \xrightarrow{\mathbf{e^{(k-2)}}} \mathbf{r^{(k-1)}} \xrightarrow{\mathbf{e^{(k-1)}}} \mathbf{r^{(k)}} \xrightarrow{\mathbf{e^{(k)}}} \mathbf{r^{(k+1)}}.$$

Chemin trivial et chemin de Konieczny

▶ Concernant le *premier chemin (chemin trivial)*, on effectue $(k+1)$ *petites* boucles à $\mathbf{0}$, i.e. à chaque étape $1 \leq t \leq k+1$ on choisit $\mathbf{e^{(t)}} = \mathbf{0}$,

$$\mathbf{0} \xrightarrow{\mathbf{0}} \mathbf{0} \xrightarrow{\mathbf{0}} \cdots \xrightarrow{\mathbf{0}} \mathbf{0} \xrightarrow{\mathbf{0}} \mathbf{0} \xrightarrow{\mathbf{0}} \mathbf{0}. \tag{1.15}$$

▶ Pour le *second chemin (chemin de Konieczny)*, nous allons utiliser une *grande* boucle. Pour ce faire, on adapte la construction de la boucle proposée dans la preuve de la Proposition 2.3 **[Kon19]** par Konieczny. On pose $\mathbf{r^{(0)}} = \mathbf{0} = \mathbf{r^{(k+1)}}$. Pour $1 \leq t \leq k$, on définit $\mathbf{r^{(t)}} = (r_w^{(t)})_w$ par

$$\forall w \in \{0, \dots, 2^k - 1\}, \qquad r_w^{(t)} = \begin{cases} 1, & \text{si } w_0 = \cdots = w_{t-1} = 1; \\ 0, & \text{sinon.} \end{cases}$$

▷ Cas $t = 0$. On choisit $\mathbf{e_{Ko}^{(0)}} = (q-1, 1, 0, \dots, 0)$. Nous avons

$$\delta(\mathbf{r^{(0)}}; \mathbf{e_{Ko}^{(0)}}) = \mathbf{r^{(1)}}.$$

Pour prouver cela, on observe que pour $w \in \{0, \dots, 2^k - 1\}$ on a

$$\delta(\mathbf{r^{(0)}}; \mathbf{e_{Ko}^{(0)}})_w = \left\lfloor \frac{0 + q - 1 + w_0}{q} \right\rfloor.$$

C'est égal 1 si $w_0 = 1$, et 0 si $w_0 = 0$. Ainsi, dans ce cas

$$\delta(\mathbf{r^{(0)}}; \mathbf{e_{Ko}^{(0)}})_w = r_w^{(1)}.$$

Le poids de transition de $\mathbf{r_0}$ à $\mathbf{r_1}$ est donné par

$$\mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r^{(1)}}) - \tilde{S}(\mathbf{r^{(0)}})\right)\right),$$

où

$$\tilde{S}(\mathbf{r^{(1)}}) = -\sum_{w=0}^{2^k-1} (-1)^{s_2(w)} r_w^{(1)} = -\sum_{\substack{w=0 \\ w_0=1}}^{2^k-1} (-1)^{s_2(w)} = 0$$

et

$$\tilde{S}(\mathbf{r^{(0)}}) = -\sum_{w=0}^{2^k-1} (-1)^{s_2(w)} r_w^{(0)} = 0.$$

Ainsi,

$$\boxed{\mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r^{(1)}}) - \tilde{S}(\mathbf{r^{(0)}})\right)\right) = 1.}$$

▷ Cas $1 \leq t < k-1$. On choisit $\mathbf{e_{Ko}^{(t)}} = (q-2, 0, \dots, 0, 1, 0, \dots, 0)$, où 1 est en position $(t+1)$. Pour $w \in \{0, \dots, 2^k - 1\}$, on a

$$\delta(\mathbf{r^{(t)}}; \mathbf{e_{Ko}^{(t)}})_w = \left\lfloor \frac{r_w^{(t)} + (1, \mathbf{w}) \cdot \mathbf{e_{Ko}^{(t)}}}{q} \right\rfloor = \left\lfloor \frac{r_w^{(t)} + q - 2 + w_t}{q} \right\rfloor.$$

Ainsi, $\delta(\mathbf{r^{(t)}}; \mathbf{e_{Ko}^{(t)}})_w = 1$ si et seulement si $r_w^{(t)} = 1$ et $w_t = 1$. Par définition de $r_w^{(t)}$,

$$\delta(\mathbf{r^{(t)}}; \mathbf{e_{Ko}^{(t)}})_w = 1 \iff w_0 = \cdots = w_t = 1.$$

On en déduit que

$$\delta(\mathbf{r^{(t)}}; \mathbf{e_{Ko}^{(t)}}) = \mathbf{r^{(t+1)}}.$$

D'après (1.11), le poids lié à la transition de $\mathbf{r^{(t)}}$ à $\mathbf{r^{(t+1)}}$ est donné par

$$\mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r^{(t+1)}}) - \tilde{S}(\mathbf{r^{(t)}})\right)\right),$$

où

$$\tilde{S}(\mathbf{r^{(t+1)}}) = -\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}r_w^{(t+1)} = -\sum_{\substack{w=0\\ w_0=\cdots=w_t=1}}^{2^k-1}(-1)^{s_2(w)} = 0$$

et

$$\tilde{S}(\mathbf{r^{(t)}}) = -\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}r_w^{(t)} = -\sum_{\substack{w=0\\ w_0=\cdots=w_{t-1}=1}}^{2^k-1}(-1)^{s_2(w)} = 0.$$

Ainsi,

$$\boxed{\mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r^{(t+1)}}) - \tilde{S}(\mathbf{r^{(t)}})\right)\right) = 1.}$$

▷ Cas $t = k-1$. On pose $\mathbf{e_{Ko}^{(k-1)}} = (q-2, 0, \ldots, 0, 0, 1)$.
Pour $w \in \{0, \ldots, 2^k-1\}$, on a

$$\delta(\mathbf{r^{(t)}}; \mathbf{e_{Ko}^{(t)}})_w = \left\lfloor \frac{r_w^{(k-1)} + (1, \mathbf{w}) \cdot \mathbf{e_{Ko}^{(k-1)}}}{q} \right\rfloor = \left\lfloor \frac{r_w^{(k-1)} + q - 2 + w_{k-1}}{q} \right\rfloor.$$

Ainsi, $\delta(\mathbf{r^{(k-1)}}; \mathbf{e_{Ko}^{(k-1)}})_w = 1$ si et seulement si $r_w^{(k-1)} = 1$ et $w_{k-1} = 1$. D'après la définition de $r_w^{(k-1)}$ on a

$$\delta(\mathbf{r^{(k-1)}}; \mathbf{e_{Ko}^{(k-1)}})_w = 1 \quad \Longleftrightarrow \quad w_0 = \cdots = w_{k-1} = 1.$$

On en déduit que

$$\delta(\mathbf{r^{(k-1)}}; \mathbf{e_{Ko}^{(k-1)}}) = \mathbf{r^{(k)}}.$$

Ici apparaît le premier changement concernant les poids de transitions. On a dans un premier temps

$$\tilde{S}(\mathbf{r^{(k-1)}}) = -\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}r_w^{(t)} = \sum_{\substack{w=0\\ w_0=\cdots=w_{k-2}=1}}^{2^k-1}(-1)^{s_2(w)} = 0.$$

En revanche,

$$\tilde{S}(\mathbf{r^{(k)}}) = -\sum_{w=0}^{2^k-1}(-1)^{s_2(w)}r_w^{(t)} = -\sum_{\substack{w=0\\ w_0=\cdots=w_{k-1}=1}}^{2^k-1}(-1)^{s_2(w)} = -(-1)^k = (-1)^{k+1}.$$

Ainsi, le poids lié à la transition de $\mathbf{r^{(k-1)}}$ à $\mathbf{r^{(k)}}$ est égal à

$$\boxed{\mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r^{(k)}}) - \tilde{S}(\mathbf{r^{(k-1)}})\right)\right) = \mathrm{e}\left((-1)^{k+1}\frac{q\ell}{b}\right).}$$

▷ Cas $t = k$. On pose $\mathbf{e}_{\mathbf{Ko}}^{(\mathbf{k})} = \mathbf{0}$. Ainsi,

$$\delta(\mathbf{r}^{(\mathbf{k})}; \mathbf{e}_{\mathbf{Ko}}^{(\mathbf{k})}) = \mathbf{0} = \mathbf{r}^{(\mathbf{k+1})}.$$

Le poids lié à la transition de $\mathbf{r}^{(\mathbf{k})}$ à $\mathbf{r}^{(\mathbf{k+1})}$ est donné par

$$\boxed{\mathrm{e}\left(\frac{\ell}{b}\left(q\tilde{S}(\mathbf{r}^{(\mathbf{k+1})}) - \tilde{S}(\mathbf{r}^{(\mathbf{k})})\right)\right) = \mathrm{e}\left((-1)^k \frac{\ell}{b}\right).}$$

Remarquons que les poids $\tilde{S}$ ne dépendent que $\mathbf{r}^{(\mathbf{t})}$ (et non de $\mathbf{e}$). En rassemblant les poids (encadrés) connectant chaque sommet de notre *grande boucle*, on obtient

$$\begin{aligned}
p_{\mathbf{r}^{(\mathbf{t})},\mathbf{r}^{(\mathbf{t+1})}} &= \frac{|\{\mathbf{e} \in \{0,\dots,q-1\}^{k+1} \,:\, \delta(\mathbf{r}^{(\mathbf{t})}; \mathbf{e}) = \mathbf{r}^{(\mathbf{t+1})}\}|}{q^{k+1}}, \qquad 0 \le t < k, \\
p_{\mathbf{r}^{(\mathbf{k-1})},\mathbf{r}^{(\mathbf{k})}} &= \mathrm{e}\left((-1)^{k+1}\frac{q\ell}{b}\right) \frac{|\{\mathbf{e} \in \{0,\dots,q-1\}^{k+1} \,:\, \delta(\mathbf{r}^{(\mathbf{k-1})}; \mathbf{e}) = \mathbf{r}^{(\mathbf{k})}\}|}{q^{k+1}}, \quad (1.16) \\
p_{\mathbf{r}^{(\mathbf{k})},\mathbf{r}^{(\mathbf{k+1})}} &= \mathrm{e}\left((-1)^{k}\frac{\ell}{b}\right) \frac{|\{\mathbf{e} \in \{0,\dots,q-1\}^{k+1} \,:\, \delta(\mathbf{r}^{(\mathbf{k})}; \mathbf{e}) = \mathbf{r}^{(\mathbf{k+1})}\}|}{q^{k+1}}.
\end{aligned}$$

Un codage des chemins par les mots

Soient $\mathbf{r_0}, \mathbf{r_j} \in \mathfrak{R}$. Considérons l'ensemble de tous les chemins de longueur j reliant $\mathbf{r_0}$ à $\mathbf{r_j}$. La Proposition 1.3.7 montre que cet ensemble est non vide. Un chemin γ appartenant à cet ensemble peut être décrit par des mots ω_γ de longueur j sur l'alphabet $\{0, 1, \dots, q^{k+1}-1\}$, où l'on identifie $\mathbf{e}^{(\mathbf{i})} \in \{0,\dots,q-1\}^{k+1}$ à la lettre $\sum_{j=0}^{k+1} e_j^{(i)} q^j$. Il convient de noter qu'il peut exister plusieurs mots différents qui décrivent un même chemin. Nous illustrons ce mot par

$$\omega_\gamma \;:\; \boxed{\mathbf{e}^{(\mathbf{0})}} \; \boxed{\mathbf{e}^{(\mathbf{1})}} \; \dots \; \boxed{\mathbf{e}^{(\mathbf{j-1})}}$$

qui est identifié au chemin

$$\mathbf{r_0} \longrightarrow \mathbf{r_1} \longrightarrow \cdots \longrightarrow \mathbf{r_{j-1}} \longrightarrow \mathbf{r_j},$$

via

$$\mathbf{r_1} = \delta(\mathbf{r_0}; \mathbf{e}^{(\mathbf{0})}), \quad \dots, \quad \mathbf{r_j} = \delta(\mathbf{r_{j-1}}; \mathbf{e}^{(\mathbf{j-1})}).$$

Nous définissons dans un premier temps la *concaténation* de deux mots.

Définition 1.3.8. Soient ω et ω' deux mots de longueurs respectives $\alpha > 0$ et $\beta > 0$.

$$\omega \;:\; \boxed{\mathbf{e}^{(\mathbf{0})}} \; \boxed{\mathbf{e}^{(\mathbf{1})}} \; \dots \; \boxed{\mathbf{e}^{(\alpha-\mathbf{1})}}$$

$$\omega' \;:\; \boxed{\mathbf{e}'^{(\mathbf{0})}} \; \boxed{\mathbf{e}'^{(\mathbf{1})}} \; \dots \; \boxed{\mathbf{e}'^{(\beta-\mathbf{1})}}$$

On définit $\omega \circ \omega'$ par

$$\omega \circ \omega' \;:\; \boxed{\mathbf{e}^{(\mathbf{0})}} \; \boxed{\mathbf{e}^{(\mathbf{1})}} \; \dots \; \boxed{\mathbf{e}^{(\alpha-\mathbf{1})}} \; \boxed{\mathbf{e}'^{(\mathbf{0})}} \; \boxed{\mathbf{e}'^{(\mathbf{1})}} \; \dots \; \boxed{\mathbf{e}'^{(\beta-\mathbf{1})}}$$

De manière analogue on définit, pour un mot ω et pour $n \in \mathbb{N}^*$, le mot ω^n par

$$\omega^n = \begin{cases} \omega, & \text{si } n = 1; \\ \omega^{n-1} \circ \omega, & \text{si } n \geq 2. \end{cases}$$

Concentrons-nous sur quelques mots spécifiques. Premièrement, on définit le mot élémentaire ω_0 de longueur 1 par

$$\omega_0 : \boxed{\mathbf{0}}$$

Lorsque $\mathbf{r_0} = \mathbf{0}$, ce mot code une *petite* boucle de $\mathbf{0}$ à $\mathbf{0}$ et ω_0^{k+1} encode le *chemin trivial* constitué de $(k+1)$ *petites* boucles en $\mathbf{0}$. De manière similaire, nous définissons le mot ω_1 codant le *chemin de Konieczny*, en utilisant la définition des vecteurs $\mathbf{e_{Ko}^{(t)}}$ précedemment établie :

$$\omega_1 : \boxed{\mathbf{e_{Ko}^{(0)}}} \boxed{\mathbf{e_{Ko}^{(1)}}} \ldots \boxed{\mathbf{e_{Ko}^{(k)}}}$$

Le mot fondamental de longueur $(K + b(k+1))$

$$\omega_0^{K+b(k+1)} : \boxed{\mathbf{0}} \ldots \boxed{\mathbf{0}} \boxed{\mathbf{0}} \boxed{\mathbf{0}} \ldots \boxed{\mathbf{0}}$$

va jouer un rôle crucial par la suite. Séparons deux phases très importantes de ce mot.

▶ Les K premières occurrences de $\mathbf{0}$ apparaissant à gauche dans $\omega_0^{K+b(k+1)}$ (jusqu'à la ligne **verticale**) indiquent la « chute libre » de notre chemin, c'est-à-dire le chemin menant au sommet $\mathbf{0}$.

▶ Les $b(k+1)$ autres $\mathbf{0}$ correspondent à b répétitions du *premier chemin* (*chemin trivial*) allant de $\mathbf{0}$ à lui-même, tel que défini en **(1.15)**.

Une partition de l'ensemble des mots

Supposons que $j \geq K + b(k+1)$. Le cardinal de l'ensemble W^* des mots de longueur j qui **ne contiennent pas** le sous-mot $\omega_0^{K+b(k+1)}$ vérifie l'inégalité suivante

$$|W^*| \leq \left(q^{(k+1)(K+b(k+1))} - 1\right)^{\frac{j}{K+b(k+1)}}. \tag{1.17}$$

En effet, lorsqu'on subdivise un mot de longueur j en sous-mots contigus de longueur $K + b(k+1)$ (en laissant éventuellement un court sous-mot à la fin), chaque mot ne contenant pas le mot $\omega_0^{K+b(k+1)}$ ne doit contenir ce mot sur chaque emplacement interne contigu de taille j. Il y a $q^{(k+1)(K+b(k+1))} - 1$ choix possibles de sous-mots distincts de $\omega_0^{K+b(k+1)}$, et il y a strictement moins de $j/(K + b(k+1))$ sous-mots complets. Dans ce qui suit, nous allons nous concentrer sur les mots contenant $\omega_0^{K+b(k+1)}$, les mots ne contenant pas ce sous-mot seront estimés de manière triviale. Nous avons

$$p^{(j)}_{\mathbf{r_0},\mathbf{r_j}} = \frac{1}{q^{(k+1)j}} \sum_{\substack{\mathbf{e}=(\mathbf{e^{(1)}},\ldots,\mathbf{e^{(j)}}) \in (\{0,\ldots,q-1\}^{k+1})^j \\ \mathbf{r_j} = \delta_{\mathbf{e^{(j)}}} \circ \cdots \circ \delta_{\mathbf{e^{(1)}}}(\mathbf{r_0})}} W(\mathbf{e}),$$

où

$$W(\mathbf{e}) = \mathrm{e}\left(\frac{\ell}{b}\sum_{t=1}^{j}\left(q\tilde{S}(\delta_{\mathbf{e^{(t)}}}\circ\cdots\circ\delta_{\mathbf{e^{(1)}}}(\mathbf{r_0})) - \tilde{S}(\delta_{\mathbf{e^{(t-1)}}}\circ\cdots\circ\delta_{\mathbf{e^{(1)}}}(\mathbf{r_0}))\right)\right), \quad (1.18)$$

avec l'initialisation, pour $t = 1$:

$$\delta_{\mathbf{e^{(t-1)}}}\circ\cdots\circ\delta_{\mathbf{e^{(1)}}}(\mathbf{r_0}) = \mathbf{r_0}.$$

Définissons $F(\mathbf{r_j})$ (égal à $F(\mathbf{r_0},\mathbf{r_j})$, mais afin d'alléger les notations, nous omettons la dépendance en $\mathbf{r_0}$) comme l'ensemble des éléments $\mathbf{e} = (\mathbf{e^{(1)}},\ldots,\mathbf{e^{(j)}})$ tels qu'il existe un entier $1 \leq m \leq j - K - b(k+1) + 1$ pour lequel

$$\mathbf{e^{(m)}} = \cdots = \mathbf{e^{(m+K+b(k+1)-1)}} = \mathbf{0}.$$

Pour $0 < m \leq j - K - b(k+1) + 1$, on note $F_m(\mathbf{r_j}) \subset F(\mathbf{r_j})$ l'ensemble des éléments $\mathbf{e} = (\mathbf{e^{(1)}},\ldots,\mathbf{e^{(j)}})$ tels que m soit le plus petit entier satisfaisant

$$\mathbf{e^{(m)}} = \cdots = \mathbf{e^{(m+K+b(k+1)-1)}} = \mathbf{0}.$$

Avec ces définitions, on a la partition suivante :

$$F(\mathbf{r_j}) = \biguplus_{m=1}^{j-K-b(k+1)} F_m(\mathbf{r_j}).$$

Dans la sous-section suivante, nous allons associer à chaque $\mathbf{e}$ contenant le sous-mot $\omega_0^{K+b(k+1)}$, $(b-1)$ mots $\varphi_1(\mathbf{e}),\ldots,\varphi_{b-1}(\mathbf{e})$ tels que pour $\lambda = 1,\ldots,b-1$, le mot φ_λ remplace les λ premiers sous-mots ω_0^{k+1} par λ sous-mots ω_1. De manière informelle, φ_λ remplace λ *petites* boucles en $\mathbf{0}$ par λ *grandes* boucles en $\mathbf{0}$. Nous verrons ensuite qu'il existe des compensations (annulations) entre les poids associés à tous ces mots.

Substitution et couplage avec le chemin de Konieczny

Définition 1.3.9 (fonction λ-switching)**.** Pour $\lambda \in \{1,\ldots,b-1\}$, on définit la fonction $\varphi_\lambda : F(\mathbf{r_j}) \longrightarrow (\{0,\ldots,q-1\}^{k+1})^j$ de la manière suivante.
Pour $\mathbf{e} = (\mathbf{e^{(1)}},\ldots,\mathbf{e^{(j)}}) \in F_m(\mathbf{r_j})$, on pose $\varphi_\lambda(\mathbf{e}) = (\mathbf{g^{(1)}},\ldots,\mathbf{g^{(j)}})$, avec

$$\begin{cases} \mathbf{g^{(m+K+t)}} = \mathbf{e_{Ko}^{t \bmod (k+1)}} & \text{si } t \in \{0,\ldots,\lambda(k+1)-1\}; \\ \mathbf{g^{(t)}} = \mathbf{e^{(t)}} & \text{si } t \in \{0,\ldots,m-1\} \cup \{m+K+b(k+1),\ldots,j\}, \end{cases}$$

où $\mathbf{e_{Ko}^{(0)}},\ldots,\mathbf{e_{Ko}^{(k)}}$ sont les vecteurs définis au début de la Section 2 et correspondent au *chemin de Konieczny*.

▷ Par exemple, la fonction φ_2 remplace deux *petites boucles* par deux *grandes* boucles, après la « chute libre ».
On écrit

$$p_{\mathbf{r_0},\mathbf{r_j}}^{(j)} = \frac{1}{q^{(k+1)j}} \sum_{\mathbf{e}\in F(\mathbf{r_j})\cup\varphi_1(F(\mathbf{r_j}))\cup\cdots\cup\varphi_{b-1}(F(\mathbf{r_j}))} W(\mathbf{e}) + \frac{1}{q^{(k+1)j}} \sum_{\mathbf{e}\notin F(\mathbf{r_j})\cup\varphi_1(F(\mathbf{r_j}))\cup\cdots\cup\varphi_{b-1}(F(\mathbf{r_j}))} W(\mathbf{e}). \quad (1.19)$$

Pour tout $1 \leq m \leq j-K-b(k+1)+1$, notons $H_m(\mathbf{r_j})$ l'ensemble des éléments

$$\mathbf{e} = (\mathbf{e^{(1)}}, \dots, \mathbf{e^{(j)}})$$

appartenant à

$$F(\mathbf{r_j}) \cup \varphi_1(F(\mathbf{r_j})) \cup \cdots \cup \varphi_{b-1}(F(\mathbf{r_j})),$$

tels que m soit le plus petit entier pour lequel le mot associé à

$$(\mathbf{e^{(m)}}, \dots, \mathbf{e^{(m+K+b(k+1)-1)}})$$

appartienne à l'ensemble

$$\left\{\omega_0^{K+k+1}, \omega_0^K \circ \omega_1 \circ \omega_0^{(k+1)(b-1)}, \dots, \omega_0^K \circ \omega_1^{b-1} \circ \omega_0\right\}.$$

Avec cette définition, on a la partition

$$F(\mathbf{r_j}) \cup \varphi_1(F(\mathbf{r_j})) \cup \cdots \cup \varphi_{b-1}(F(\mathbf{r_j})) = \biguplus_{m=1}^{j-K-b(k+1)+1} H_m(\mathbf{r_j}).$$

Ainsi,

$$\begin{aligned}\sum_{\mathbf{e} \in F(\mathbf{r_j}) \cup \varphi_1(F(\mathbf{r_j})) \cup \cdots \cup \varphi_{b-1}(F(\mathbf{r_j}))} W(\mathbf{e}) &= \sum_{m=1}^{j-K-b(k+1)+1} \sum_{\mathbf{e} \in H_m(\mathbf{r_j})} W(\mathbf{e}) \\ &= \sum_{m=1}^{j-K-b(k+1)+1} \sum_{\mathbf{e} \in F_m(\mathbf{r_j})} \\ &\qquad \times (W(\mathbf{e}) + W(\varphi_1(\mathbf{e})) + \cdots + W(\varphi_{b-1}(\mathbf{e}))).\end{aligned}$$

De plus, nous avons le lemme suivant.

Lemme 1.3.10. *Pour tout* $\mathbf{e} \in F_m(\mathbf{r_j})$ *et pour* $1 \leq m \leq j-K-b(k+1)+1$, *on a*

$$W(\mathbf{e}) + W(\varphi_1(\mathbf{e})) + \cdots + W(\varphi_{b-1}(\mathbf{e})) = 0. \tag{1.20}$$

Démonstration. Nous démontrons le cas $2 \leq m \leq j-K-b(k+1)$. Les cas $m=1$ et $m = j-K-b(k+1)+1$ se prouvent de la même manière. La seule différence réside dans le nombre de parties inchangées par notre fonction (une seule partie inchangée). D'après (1.18) et la définition de φ_λ, on a, pour $2 \leq m \leq j-K-b(k+1)$, $\lambda \in \{0, \dots, b-1\}$ et pour $t \in \{0, \dots, m-1\} \cup \{m+K+b(k+1), \dots, j\}$,

$$\begin{aligned}&q\tilde{S}(\delta_{\varphi_\lambda(\mathbf{e^{(t)}})} \circ \cdots \circ \delta_{\varphi_\lambda(\mathbf{e^{(1)}})}(\mathbf{r_0})) - \tilde{S}(\delta_{\varphi_\lambda(\mathbf{e^{(t-1)}})} \circ \cdots \circ \delta_{\varphi_\lambda(\mathbf{e^{(1)}})}(\mathbf{r_0})) \\ &\quad = q\tilde{S}(\delta_{\mathbf{e^{(t)}}} \circ \cdots \circ \delta_{\mathbf{e^{(1)}}}(\mathbf{r_0})) - \tilde{S}(\delta_{\mathbf{e^{(t-1)}}} \circ \cdots \circ \delta_{\mathbf{e^{(1)}}}(\mathbf{r_0})).\end{aligned} \tag{1.21}$$

Ces deux quantités, qui sont inchangées par la fonction φ_λ, constitueront les poids communs (de module 1) pour les termes $W(\mathbf{e}), W(\varphi_1(\mathbf{e})), \dots, W(\varphi_{b-1}(\mathbf{e}))$. Elles n'interviendront pas dans le calcul de la quantité

$$|W(\mathbf{e}) + W(\varphi_1(\mathbf{e})) + \cdots + W(\varphi_{b-1}(\mathbf{e}))|.$$

Par ailleurs, la partie modifiée par la fonction φ_λ (qui correspond à λ chemins de Konieczny) possède, d'après la Définition 1.3.9 et (1.16), un poids égal à

$$\mathrm{e}\left((-1)^{k+1}\lambda(q-1)\ell/b\right),$$

puisqu'un chemin de Konieczny possède un poids égal à $\mathrm{e}\left((-1)^{k+1}(q-1)\ell/b\right)$. On en déduit alors que

$$\begin{aligned}\Big|W(\mathbf{e})+W(\varphi_1(\mathbf{e}))+\cdots+W(\varphi_{b-1}(\mathbf{e}))\Big| &\\ &= \left|1+\mathrm{e}\left((-1)^{k+1}\frac{(q-1)\ell}{b}\right)+\mathrm{e}\left((-1)^{k+1}\frac{2(q-1)\ell}{b}\right)\right.\\ &\qquad \left.+\cdots+\mathrm{e}\left((-1)^{k+1}\frac{(b-1)(q-1)\ell}{b}\right)\right|\\ &= 0.\end{aligned}$$

□

Comme $(b, q-1)=1$ et $0<\ell<b$, le nombre $(q-1)\ell/b$ n'est **pas** un entier. Ainsi,

$$\sum_{\mathbf{e}\in F(\mathbf{r_j})\cup\varphi_1(F(\mathbf{r_j}))\cup\cdots\cup\varphi_{b-1}(F(\mathbf{r_j}))} W(\mathbf{e})=0.$$

Majorations finales

On écrit $F=\bigcup_{\mathbf{r_j}} F(\mathbf{r_j})$ et on réconsidère l'équation (1.19). On majore trivialement la seconde somme dans (1.19). On a, d'après l'inégalité (1.17),

$$\begin{aligned}\sum_{\mathbf{r_j}\in\mathfrak{R}}\Big|\sum_{\mathbf{e}\notin F(\mathbf{r_j})\cup\varphi_1(F(\mathbf{r_j}))\cup\cdots\cup\varphi_{b-1}(F(\mathbf{r_j}))} W(\mathbf{e})\Big| &\le \sum_{\mathbf{r_j}\in\mathfrak{R}}\sum_{\mathbf{e}\notin F(\mathbf{r_j})\cup\varphi_1(F(\mathbf{r_j}))\cup\cdots\cup\varphi_{b-1}(F(\mathbf{r_j}))} 1\\ &\le \Big|\sum_{\mathbf{e}\notin F\cup\varphi_1(F)\cup\cdots\cup\varphi_{b-1}(F)} 1\Big|\\ &\le (q^{(k+1)(K+b(k+1))}-1)^{\frac{j}{K+b(k+1)}}.\end{aligned}$$

On injecte cette inégalité dans (1.19) et on obtient

$$\sum_{\mathbf{r_j}\in\mathfrak{R}}|p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}|\le\frac{1}{q^{(k+1)j}}(q^{(k+1)(K+b(k+1))}-1)^{\frac{j}{K+b(k+1)}}.$$

Désormais, on choisit

$$j=K+b(k+1).$$

En prenant le maximum sur $\mathbf{r_0}\in\mathfrak{R}$, on a

$$M=\max_{\mathbf{r_0}\in\mathfrak{R}}\left(\sum_{\mathbf{r_j}\in\mathfrak{R}}|p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}|\right)\le 1-\frac{1}{q^{(k+1)(K+b(k+1))}}. \tag{1.22}$$

En utilisant l'inégalité (1.13), on a, pour chaque terme de la suite

$$(v_\rho)_{\rho\ge0}=(\max_{\mathbf{r}\in\mathfrak{R}}|A(\rho,\mathbf{r})|)_{\rho\ge0},$$

la majoration

$$\begin{aligned}v_\rho &\le v_{\rho-j}\max_{\mathbf{r_0}\in\mathfrak{R}}\left(\sum_{\mathbf{r_j}\in\mathfrak{R}}|p^{(j)}_{\mathbf{r_0},\mathbf{r_j}}|\right)\\ &\le Mv_{\rho-j}.\end{aligned}$$

Ainsi, par récurrence et en utilisant le fait que pour tout $r \geq 0$ on a $v_r \leq 1$, on obtient

$$v_\rho \leq M^{\lfloor \frac{\rho}{K+b(k+1)} \rfloor} \tag{1.23}$$

et

$$A(\rho, \mathbf{r_0}) \leq \left(1 - \frac{1}{q^{(k+1)(K+b(k+1))}}\right)^{\lfloor \frac{\rho}{K+b(k+1)} \rfloor} \leq 2\left(1 - \frac{1}{q^{(k+1)(K+b(k+1))}}\right)^{\frac{\rho}{K+b(k+1)}} \ll q^{-\eta_0 \rho},$$

avec

$$\eta_0 = -\frac{\log(1 - \frac{1}{q^{(k+1)(K+b(k+1))}})}{(\log q)(K + b(k+1))}.$$

L'inégalité $\log(1-x) \leq -x$ (valide pour tout $0 \leq x < 1$) nous permet d'avoir

$$\eta_0 \geq \frac{1}{(\log q)(K + b(k+1))q^{(k+1)(K+b(k+1))}}.$$

Chapitre 2

Le niveau de répartition de la fonction somme des chiffres

1 Définition 41
2 Niveau de répartition de s_2 42
3 Résultats principaux 44
4 Propagation des retenue et troncature 47
5 Preuve du Théorème **2.3.5** 50
  1 Étape 1 : Itérations de l'inégalité de van der Corput 50
  2 Étape 2 : Décalage et découpage 56
6 Preuve du Théorème **2.3.3** 71
7 Preuve du Théorème **2.3.1** 74
8 Choix des paramètres 76
9 Graphe de la fonction $\varepsilon \mapsto \log \eta(\varepsilon)$ 81

Le dessein de ce chapitre est d'établir, à l'instar du théorème principal de **[Spi20]**, un résultat sur le niveau de répartition de s_q le long des progressions arithmétiques. Ce travail fait l'objet de l'article de **[Tou25]** remanié. Les pages 50 à 81 correspondent aux pages **2392** à **2425** de **[Tou25]**.

2.1. Définition

Il existe des définitions du niveau de répartition d'une suite, la suivante étant proposée dans l'article **[Spi20]**, s'inspirant de **[FM96b]**. Soit $(c_n)_{n\in\mathbb{N}}$ une suite à valeurs complexes. Soient $\mathcal{Q}$ et $\mathcal{R}$ deux applications qui à tout entier $m \geq 1$ associent deux sous-ensembles $\mathcal{Q}(m) \neq \emptyset$ et $\mathcal{R}(m)$ de $\mathbb{Z}/m\mathbb{Z}$ tels que $\mathcal{Q}(m) \subseteq \mathcal{R}(m)$.

Le réel θ est appelé niveau (ou exposant) de répartition de la suite $(c_n)_{n\in\mathbb{N}}$ relativement aux applications $\mathcal{Q}$ et $\mathcal{R}$ si pour tout $\varepsilon > 0$, pour tout $A > 0$, on a, pour

$x \geq 1$, l'inégalité

$$\sum_{m<x^{\theta-\varepsilon}} \max_{y\leq x} \max_{\substack{0\leq a<m\\ a+m\mathbb{Z}\in\mathcal{Q}(m)}} \Big| \sum_{\substack{n<y\\ n\equiv a \pmod m}} c_n - \frac{1}{|\mathcal{R}(m)|} \sum_{\substack{n<y\\ n+m\mathbb{Z}\in\mathcal{R}(m)}} c_n \Big| \ll \log(2x)^{-A} \sum_{n\leq x} |c_n|.$$

Il est courant de considérer $\mathcal{R}(m) = \mathbb{Z}/m\mathbb{Z} = \mathcal{Q}(m)$. Par exemple, dans le cas du théorème de Bombieri–Vinogradov, on a $\mathcal{R}(m) = (\mathbb{Z}/m\mathbb{Z})^* = \mathcal{Q}(m)$. 0

2.2. Niveau de répartition de s_2

Fouvry et Mauduit **[FM96a]** ont initié l'étude du niveau de répartition de la suite de Thue–Morse (base $q = 2$) et de ses généralisations le long des progressions arithmétiques. En effet, ils montrèrent le théorème suivant.

Théorème 2.2.1 (Fouvry/Mauduit, 1996)**.** *Soit $C_b > 0$ une constante telle que pour tout $\xi \in \{1/b, \dots, (b-1)/b\}$ on a*

$$\int_0^1 \prod_{0\leq n<N} |\cos(\pi(2^n t + \xi))| dt = \mathcal{O}(C_b^N), \qquad N \to +\infty.$$

Soit

$$\gamma(\alpha) = 1 + \frac{\log \beta(\alpha)}{\log 2},$$

où

$$\beta(\alpha) := \sqrt{\max_{t\in\mathbb{R}} |\cos(\pi\,(t+\alpha))\cos(\pi(2t+\alpha))|},$$

et soit

$$\gamma_b = \max\{\gamma(\alpha) \ : \ \mathrm{e}(\alpha)^b = 1\ ,\ \alpha \notin \mathbb{Z}\}.$$

Pour $A \in \mathbb{R}$, posons $D = x^{1/2}(\log x)^{-A}$. Alors, pour $x \to +\infty$,

$$\sum_{1\leq m\leq D} \max_{1\leq z\leq x} \max_{0\leq r<m} \Big| \sum_{\substack{n<z\\ s_2(n)\equiv 0 \pmod b\\ n\equiv r \pmod m}} 1 - \frac{z}{bm} \Big| = \mathcal{O}\Big(x^{1+\log C_b/\log 2} D + x^{\gamma_b}\Big(D^{3-2\gamma_b+2\log C_b/\log 2} + \log x \Big)\Big).$$

Le Théorème 2.2.1 leur a permis de montrer que 0.5924 est un niveau de répartition de la suite de Thue–Morse $\mathtt{t}$. Plus précisément, ils ont démontré dans **[FM96a]** le théorème ci-après :

Théorème 2.2.2 (Fouvry/Mauduit, 1996)**.** *Soit $A \in \mathbb{R}$ et $D = x^{0.5924}$. Il existe $C > 0$ tel que*

$$\sum_{1\leq m\leq D} \max_{1\leq z\leq x} \max_{0\leq r<m} \Big| \sum_{\substack{n<z\\ s_2(n)\equiv 0 \pmod 2\\ n\equiv r \pmod m}} 1 - \frac{z}{2m} \Big| \leq Cx(\log 2x)^{-A}, \qquad x \to +\infty.$$

Ils ont également étudié le niveau de répartition de la suite $(s_q(n))_{n\in\mathbb{N}}$ pour une base de numération q quelconque. Dans **[FM96b,** p. 340**]**, ils ont démontré le résultat suivant.

Théorème 2.2.3 (Fouvry/Mauduit, 1996). *Soient $b, q \geq 2$, deux entiers tels que*

$$(b, q-1) = 1.$$

Soit $a \in \{0, \dots, b-1\}$. Alors, pour tout $x \geq 1$, pour tout $A \in \mathbb{R}$ et pour tout $\varepsilon > 0$, on a

$$\sum_{1 \leq m \leq x^{\theta_q - \varepsilon}} \max_{1 \leq z \leq x} \max_{0 \leq r < m} \left| \sum_{\substack{n<z \\ s_q(n) \equiv a \pmod b \\ n \equiv r \pmod m}} 1 - \frac{1}{m} \sum_{\substack{n<z \\ s_q(n) \equiv a \pmod b}} 1 \right| = \mathcal{O}(x(\log 2x)^{-A}),$$

où θ_q est défini par

$$\theta_q = 1 - \frac{\log(M(q))}{\log(q)},$$

où

$$M(q) = \begin{cases} \dfrac{1}{n} \displaystyle\sum_{k=0}^{n-1} \cos\left(\tfrac{2k+1}{4n}\pi\right)\Big)^{-1}, & \text{si } q = 2n; \\ \dfrac{1}{2n+1}\left(1 + 2\displaystyle\sum_{k=1}^{n} \cos\left(\tfrac{k}{2n+1}\pi\right)^{-1}\right), & \text{si } q = 2n+1. \end{cases}$$

De plus, $\theta_q \to 1$ pour $q \to +\infty$.

En 2020, Spiegelhofer **[Spi20]** a amélioré le Théorème 2.2.2 dans le cadre de la suite de Thue–Morse. Il a en effet montré que la suite de Thue–Morse admet un niveau de répartition égal à 1, ce qui peut être considéré comme un résultat optimal. Cela signifie que pour tout $\varepsilon > 0$, il existe un $\eta > 0$ tel que

$$\sum_{1 \leq m \leq x^{1-\varepsilon}} \max_{\substack{y,z \geq 0 \\ z-y \leq x}} \max_{0 \leq r < m} \left| \sum_{\substack{y \leq n < z \\ n \equiv r \pmod m}} (-1)^{s_2(n)} \right| \ll_\varepsilon x^{1-\eta}. \tag{2.1}$$

Comme pour tout $n \geq 0$, $(-1)^{s_2(n)} = 1 - 2s_2(n) \bmod 2$, la borne (2.1) découle immédiatement de **[Spi20,** Theorem 2.1**]**, rappelé ci-dessous.

Théorème 2.2.4 (Spiegelhofer, 2020). *Soit $\varepsilon > 0$. Il existe $\eta > 0$ tel que*

$$\sum_{1 \leq m \leq x^{1-\varepsilon}} \max_{\substack{y,z \geq 0 \\ z-y \leq x}} \max_{0 \leq r < m} \left| \sum_{\substack{y \leq n < z \\ s_2(n) \equiv 0 \pmod 2 \\ n \equiv r \pmod m}} 1 - \frac{z-y}{2m} \right| \ll x^{1-\eta}, \qquad x \to +\infty.$$

Des résultats explicites existaient avant le travail de Spiegelhofer **[Spi20]**. En 2014, Martin, Mauduit et Rivat **[MMR14,** Proposition 3**]** ont établi une estimation pour des sommes de type II.

Théorème 2.2.5 (Martin/Mauduit/Rivat, 2014). *Soit $\alpha \in \mathbb{R}/\mathbb{Z}$ et $q \geq 2$ un entier. Soient $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ deux suites à valeurs complexes telles que pour tout $n \geq 1$, on a $|a_n| \leq 1$ et $|b_n| \leq 1$. Soit $x \geq 2$, $0 < \varepsilon \leq 1/2$, $x^\varepsilon \leq M, N \leq x$ et $MN \leq x$. On pose*

$$\Theta_q := \left(1 - \frac{1}{q}\right)\left(1 - \sqrt{1 - \frac{2q-1}{3q(q-1)}}\right),$$

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

et soit $\gamma_q \in \mathbb{R}$ *tel que*

$$q^{\gamma_q} := 2 \max_{t\in\mathbb{R}} \sqrt{\left|\frac{\sin\left(q(\alpha-qt)\pi\right)\sin\left(q(\alpha-t)\pi\right)}{\sin\left((\alpha-qt)\pi\right)\sin\left((\alpha-t)\pi\right)}\right|}.$$

Enfin, on pose

$$\xi_{q,\varepsilon} := \min\left(\frac{\varepsilon}{6}, \frac{1}{20}\right) \min\left(\frac{1}{2} - \eta_q, 2(1-\gamma_q)\right). \tag{2.2}$$

Alors

$$\sum_{M<m\leq 2M} \sum_{N<n\leq 2N} a_m b_n \mathrm{e}(\alpha s_q(mn)) \ll x^{1-\xi_{q,\varepsilon}} \log x.$$

Remarque 2.2.6. En prenant, pour tout $M < m \leq 2M$,

$$a_m = \exp\left(-i \arg\left(\sum_{N<n\leq 2N} b_n \mathrm{e}(\alpha s_q(mn))\right)\right),$$

on obtient l'estimation

$$\sum_{M<m\leq 2M} \left|\sum_{N<n\leq 2N} b_n \mathrm{e}(\alpha s_q(mn))\right| \ll x^{1-\xi_{q,\varepsilon}} \log(x).$$

Cette idée permit à Spiegelhofer **[Spi20]** d'obtenir une version plus faible du théorème principal de **[Spi20]**. Pour $0 < \varepsilon < 1/2$ et pour $D = x^{\varepsilon}$ on a

$$\sum_{1\leq m\leq D} \left| \sum_{\substack{0\leq n\leq x \\ n\equiv 0 \pmod m}} (-1)^{s_2(n)} \right| \leq C x^{1-\xi'_{2,\varepsilon}},$$

où

$$\xi'_{2,\varepsilon} = \frac{1}{1+\varepsilon} \min\left(\frac{\varepsilon}{6}, \frac{1}{20}\right) \min\left(\frac{1}{2} - \eta_2, 2(1-\gamma_2)\right).$$

Bien que **[Spi20]** ne fournit pas de valeur explicite pour η, sa méthode, comme nous le verrons, permet de le faire. Le principal défi pour obtenir une valeur explicite de η est de disposer d'une version effective de l'estimation de la norme de Gowers associée à la généralisation de la suite de Thue–Morse, ce que nous proposons dans le Chapitre 1.
Puisque α, défini dans le Théorème 2.2.5, appartient à $\mathbb{R}/\mathbb{Z}$, le Théorème 2.2.5 fournit des informations pour des suites plus générales que la suite de Thue–Morse (cas où $\alpha = 1/2$).

2.3. Résultats principaux

L'objectif de cette section est de présenter notre généralisation du résultat de Spiegelhofer **[Spi20]** à la base q et à un module arbitraire. De plus, nous présentons une valeur de $\eta > 0$ qui est presque optimale (lorsque ε tend vers 0) vis-à-vis de la méthode utilisée. Le résultat principal de ce chapitre est le suivant.

Théorème 2.3.1. *Soit* $0 < \varepsilon < 1$. *Soient* $b, q \geq 2$ *deux entiers tels que* $(b, q-1) = 1$. *Il existe une constante* $C = C(\varepsilon, b, q) > 0$ *et un exposant* $\eta = \eta(\varepsilon)$, *tels que*

$$\sum_{1\le m\le x^{1-\varepsilon}} \max_{\substack{y,z\\ 0\le y<z\\ z-y\le x}} \max_{r\ge 0} \Big| \sum_{\substack{y\le m<z\\ s_q(n)\equiv a \pmod b\\ n\equiv r \pmod m}} 1-\frac{z-y}{bm}\Big| \le Cx^{1-\eta}.$$

Une valeur admissible pour η est donnée pour $\varepsilon < \frac{2}{3}(1-\lambda)$ (avec λ défini dans le Théorème 2.7.1) par

$$\eta(\varepsilon) = \frac{\varepsilon^3 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{7200\times 8^{1/\varepsilon}\left(\log(4q/\varepsilon)+5b\log(q)/\varepsilon\right)} \times \exp\left(-\frac{5}{\varepsilon}\left(\log(4q/\varepsilon)+\frac{5b\log(q)}{\varepsilon}\right)\right). \tag{2.3}$$

Spiegelhofer **[Spi20,** p. 2568, (i)**]** a posé la question suivante : peut-on choisir $D = x(\log x)^{-B}$ pour une certaine constante $B > 0$, et avoir $x(\log x)^{-A}$ comme terme d'erreur ? Dans notre résultat, il pourrait être possible d'obtenir $\varepsilon > 0$ explicite dépendant de x et tendant vers 0 (par exemple, $\varepsilon = (A\log\log x)^{-1}$ pour une certaine constante A). Toutefois, notre méthode fournit C comme une fonction de ε. Il serait intéressant d'étudier la constante C dans le Théorème 2.3.1 et son degré de dépendance en ε.

Remarque 2.3.2. Pour $\varepsilon \to 0$, on a l'équivalent pour $\eta(\varepsilon)$

$$\eta(\varepsilon) \sim \frac{\varepsilon^4 \exp(-\varepsilon^{-2}(25b\log(q)+o(1)))}{36000b\log(q)8^{\varepsilon^{-1}}} \min\left(1/4, 3\log_q\left(P^-(q)\right)\right).$$

C'est évidemment une quantité très petite. Pour $b = q = 2$, nous avons utilisé un programme écrit en Python sur machine de bureau pour calculer quelques valeurs approchées de η données par **(2.3)**. Le tableau suivant donne quelques valeurs des exposants $\eta(\varepsilon)$ (défini par **(2.3)**) et $\xi'_{2,\varepsilon}$ (défini par **(2.2)**).

ε	$\log\eta(\varepsilon)$	$\log\xi'_{2,\varepsilon}$
0.3	−270.77	−5.85
0.2	−553.97	−6.26
0.1	−1993.60	−6.95
0.05	−7504.14	−7.65
0.01	−176 866.99	−9.25
0.005	−700 973.54	−9.95
0.001	−17 375 734.08	−11.56

FIGURE 2.1 – Quelques valeurs de $\log\eta(\xi)$ et $\log\xi'_{2,\varepsilon}$ (cas $b = q = 2$)

On constate que l'exposant fourni dans **[MMR14]** est bien plus grand que le nôtre. L'une des raisons est que nous traitons le max sur les classes de résidus ainsi qu'un max sur tous les intervales $[y,z] \subset \mathbb{R}_+$ de taille au plus x, tandis que **[MMR14]** fournit une borne individuelle pour $a = 0$ sur l'intervalle $[0,x]$.

Afin de démontrer le Théorème 2.3.1, nous allons établir le théorème suivant, qui est central dans l'article de Spiegelhofer **[Spi20]**.

Théorème 2.3.3. *Soient $0 < \delta_1 \le \delta_2 < 1$ deux réels. Soient $b, q \ge 2$ deux entiers tels que $(b, q-1) = 1$. Soient $x > 0$ et $D \in \mathbb{N}$ tels que*

$$x^{\delta_1} \leq D \leq x^{\delta_2}.$$

Alors il existe une constante $C = C(\delta_1, \delta_2, b, q) > 0$ *et un exposant* $\eta = \eta(\delta_1, \delta_2, b, q) > 0$ *tels que*

$$\sum_{D<m\leq qD} \max_{\substack{y,z \\ 0\leq y<z \\ z-y\leq x}} \max_{r\geq 0} \Big| \sum_{\substack{y\leq m<z \\ s_q(n)\equiv a \pmod b \\ m\equiv r \pmod m}} 1 - \frac{z-y}{bm} \Big| \leq Cx^{1-\eta}.$$

Une valeur admissible pour η *est donnée par*

$$\begin{aligned}\eta := \frac{\delta_1(1-\delta_2)^2 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{1800 \times 8^{(1-\delta_2)^{-1}} \left(\log(4q/(1-\delta_2)) + 5b\log(q)/(1-\delta_2)\right)} \\ \times \exp\left(-\frac{5}{1-\delta_2}\left(\log(4q(1-\delta_2)^{-1}) + \frac{5b\log(q)}{1-\delta_2}\right)\right).\end{aligned} \tag{2.4}$$

Remarque 2.3.4. Pour $\delta_2 \to 1$, on a l'équivalent suivant pour η,

$$\eta \sim \frac{\delta_1(1-\delta_2)^3}{9000b\log(q)8^{(1-\delta_2)^{-1}}} \times \exp\left(\frac{-25b\log(q) + o(1))}{(1-\delta_2)^2}\right) \times \min\left(1/4, 3\log_q\left(P^-(q)\right)\right).$$

Pour démontrer ce théorème, nous suivrons l'approche de Spiegelhofer **[Spi20]**. Une méthode classique pour détecter les progressions arithmétiques consiste à utiliser des sommes exponentielles. Dans les théorèmes suivants, nous montrons une certaine annulation en moyenne sur le module de la progression arithmétique. Le Théorème 2.3.3 est une conséquence du Théorème 2.3.5 ci-dessous, lequel pourrait également avoir des applications dans d'autres problèmes.

Théorème 2.3.5. *Soient* $\rho_2 \geq \rho_1 > 0$. *Soient* $b, q \geq 2$ *deux entiers tels que* $(b, q-1) = 1$ *et soient* $N, D > 1$ *deux entiers tels que*

$$N^{\rho_1} \leq D \leq N^{\rho_2}.$$

Soit $\ell \in \{1, \ldots, b-1\}$ *et* ξ *un nombre réel. On définit* $S_0(N, D, \xi)$ *par*

$$S_0 = S_0(N, D, \xi) = \sum_{D\leq m<qD} \max_{a\geq 0} \Big| \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} s_q(nm+a)\right) \mathrm{e}(n\xi) \Big|.$$

Alors il existe $C = C(b, q, \rho_1, \rho_2) > 0$ *et* $\eta = \eta(b, q, \rho_1, \rho_2) > 0$ *tels que*

$$\left|\frac{S_0(N, D, \xi)}{D}\right| \leq CN^{1-\eta}.$$

Une valeur admissible pour η *est donnée par*

$$\begin{aligned}\eta = \frac{\rho_1 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{8^{1+\rho_2}(288\rho_2 + 300)(3\rho_2+2)\left(\log((3\rho_2+4)q) + b\log(q)(3\rho_2+5)\right)} \\ \times \exp\left(-(3\rho_2+5)\left(\log((3\rho_2+4)q) + (3\rho_2+5)b\log(q)\right)\right).\end{aligned}$$

L'idée de la démonstration consiste à appliquer l'inégalité de van der Corput (ainsi que certaines de ses variantes) un certain nombre de fois afin d'éliminer des chiffres dans les quantités sous-jacentes et de ramener l'estimation des sommes exponentielles à des estimations de normes de Gowers à l'aide du Théorème 1.2.5 du Chapitre 1 pour la suite $(t_q(n))_{n\geq 1}$ définie par (4). Ceci dit, il nous faut d'abord introduire la fonction somme des chiffres tronquée et énoncer le théorème de propagation de retenue.

2.4. Propagation des retenue et troncature

L'objet de ce paragraphe est d'introduire un ingrédient clé de l'article fondateur de Mauduit et Rivat **[MR10]** : le lemme de propagation des retenues (Proposition 2.4.5). Le lemme de propagation des retenues a joué un rôle clé dans l'étude des sommes type II concernant la fonction s_q. Une nouveauté clé de Mauduit et Rivat **[MR10]** est de combiner l'inégalité de van der Corput avec le lemme de propagation des retenues. Le fondement de leur méthode est par ailleurs utilisé dans **[Spi20]** et sera mis en lumière dans ce chapitre. Avant de l'énoncer correctement, il nous faut introduire la fonction somme des chiffres tronquée.

Définition 2.4.1. Pour $\alpha > 0$ un entier, on définit $s_q^\alpha(n)$ par

$$s_q^\alpha(n) := s_q(n'),$$

avec $n' \equiv n \bmod q^\alpha$ et $0 \leq n' < q^\alpha$. La fonction s_q^α est appelée fonction *somme des chiffres tronquée*, de rang α, dans la base q. De plus, pour $\beta > \alpha$, on définit sur $\mathbb{N}$ la fonction « doublement tronquée » $s_q^{\alpha,\beta}$ par

$$\forall n \in \mathbb{N},\ s_q^{\alpha,\beta}(n) = s_q^\beta(n) - s_q^\alpha(n).$$

Exemple 2.4.2.

- $s_{10}^3(15382) = s_{10}^3(382) = 2 + 8 + 3 = 13.$
- $s_{10}^{3,4}(15382) = 5 + 3 + 8 + 2 - (3 + 8 + 2) = 5.$

Ces fonctions de troncature permettent de réduire la taille des nombres intervenants dans notre étude. Mauduit et Rivat **[MR09]** la font intervenir dans l'étude de la répartition de s_q des carrés qui a été étudiée antérieurement par Drmota et Rivat **[DR05]**. La méthode est globablement la même que celle proposée dans **[MR10]** mais plus technique. Le lemme suivant sera utilisé lorsque nous commencerons à effectuer de nombreux décalages de chiffres, afin d'éliminer une grande portion des chiffres des entiers et de concentrer notre attention sur une petite fenêtre de chiffres uniquement (voir **[Spi20,** p.2575**]**).

Lemme 2.4.3 (Élimination de chiffres)**.** *Soient $\alpha, u_0, u_1 \geq 0$ des entiers. Soit $\beta > \alpha$. Alors, on a l'égalité suivante :*

$$s_q^\beta(u_0 + q^\alpha u_1) - s_q^\beta(u_0) = s_q^{\alpha,\beta}(u_0 + q^\alpha u_1) - s_q^{\alpha,\beta}(u_0).$$

Démonstration. Par définition de $s_q^{\alpha,\beta}$, on a

$$s_q^{\alpha,\beta}(u_0 + q^\alpha u_1) - s_q^{\alpha,\beta}(u_0) = s_q^\beta(u_0 + q^\alpha u_1) - s_q^\beta(u_0) - (s_q^\alpha(u_0 + q^\alpha u_1) - s_q^\alpha(u_0)).$$

Or, $s_q^\alpha(u_0 + q^\alpha u_1) - s_q^\alpha(u_0) = 0$, car $u_0 + q^\alpha u_1 \equiv u_0 \pmod{q^\alpha}$. □

Énonçons dans un premier temps le lemme de propagation de retenue classique.

Proposition 2.4.4 (Lemme de propagation de retenue pour les entiers en progression arithmétique)**.** *Soient $r > 0$ et N un entier supérieur ou égal à 1. Soient $a > 0$ un entier et $b \in \mathbb{N}$. Soit I un intervalle de $\mathbb{R}$ contenant N entiers consécutifs. Alors :*

$$\left|\left\{n \in I \ :\ s_q(a(n+r)+b) - s_q(an+b) \neq s_q^\lambda(a(n+r)+b) - s_q^\lambda(an+b)\right\}\right| \leq \left(\frac{N-1}{q^\lambda} + 1\right)\left(\left(1 - \frac{1}{a}\right)q^\lambda + r + \frac{b}{a}\right).$$

Démonstration. Soit $n \in I$. Écrivons

$$n = q^\lambda t + u,\ 0 \leq u < q^\lambda.$$

Alors :

$$a(n+r)+b = aq^\lambda t + a(u+r) + b.$$

► Cas 1 : si $a(u+r)+b < q^\lambda$.
D'une part,

$$s_q(a(n+r)+b) - s_q(an+b) = s_q(a(u+r)+b) - s_q(au+b).$$

D'autre part,

$$s_q^\lambda(a(n+r)+b) - s_q^\lambda(an+b) = s_q(a(u+r)+b) - s_q(au+b).$$

L'égalité est donc obtenue dans ce premier cas. Il reste à nous occuper du
► Cas 2 : si $\underbrace{\dfrac{q^\lambda - b}{a} - r}_{\alpha} \leq u < q^\lambda$.
On écrit :

$$\left|\Big\{n \in I\ :\ \alpha \leq n \pmod{q^\lambda} < q^\lambda\Big\}\right| \leq \left|\Big\{n \in I\ :\ \lfloor\alpha\rfloor \leq n \pmod{q^\lambda} < q^\lambda\Big\}\right|$$

et

$$\left|\Big\{n \in I\ :\ \lfloor\alpha\rfloor \leq n \pmod{q^\lambda} < q^\lambda\Big\}\right| = \sum_{k=\lfloor\alpha\rfloor}^{q^\lambda-1} \sum_{\substack{n\in I \\ n\equiv k \pmod{q^\lambda}}} 1 = \sum_{k=\lfloor\alpha\rfloor}^{q^\lambda-1} \sum_{\substack{n\in I \\ n\equiv k \pmod{q^\lambda}}} 1.$$

Écrivons également :

$$I \cap \mathbb{Z} = \Big\{n_0, n_0+1, \ldots, n_0+N-1\Big\}.$$

Pour $\lfloor\alpha\rfloor \leq k \leq q^\lambda - 1$ fixé et pour $n = q^\lambda t + k$, on a :

$$n \in I \iff \frac{n_0 - k}{q^\lambda} \leq t \leq \frac{n_0 + N - 1 - k}{q^\lambda}.$$

Ainsi,

$$\sum_{\substack{n\in I \\ n\equiv k \pmod{q^\lambda}}} 1 \leq \frac{n_0+N-1-k}{q^\lambda} - \frac{n_0-k}{q^\lambda} + 1 = \frac{N-1}{q^\lambda} + 1.$$

Donc :

$$\begin{aligned}\left|\Big\{n \in I\ :\ \lfloor\alpha\rfloor \leq n \pmod{q^\lambda} < q^\lambda\Big\}\right| &\leq \Big(\frac{N-1}{q^\lambda}+1\Big)\Big(q^\lambda - 1 - \lfloor\alpha\rfloor + 1\Big) \\ &\leq \Big(\frac{N-1}{q^\lambda}+1\Big)\Big(q^\lambda - \alpha\Big) \\ &= \Big(\frac{N-1}{q^\lambda}+1\Big)\Big(\Big(1-\frac{1}{a}\Big)q^\lambda + r + \frac{b}{a}\Big).\end{aligned}$$

□

Dans notre étude, nous utiliserons plutôt le lemme de propagation de retenues pour les nombres de Beatty. Müllner et Spiegelhofer **[MS17]** l'énoncent et le démontrent dans le cas $q = 2$.

Proposition 2.4.5. *Soient $r > 0$, $N \in \mathbb{N}^*$ et $\alpha, \beta > \mathbb{R}_+^*$. Soit I un intervalle de $\mathbb{R}$ contenant N entiers consécutifs. Alors :*

$$\Big|\{n \in I \ : \ s_q^\lambda(\lfloor \alpha(n+r)+\beta \rfloor) - s_q^\lambda(\lfloor \alpha n+\beta \rfloor) \neq s_q(\lfloor \alpha(n+r)+\beta \rfloor) - s_q(\lfloor \alpha n+\beta \rfloor)\}\Big| \leq r\Big(\frac{N\alpha}{q^\lambda}+2\Big).$$

Démonstration. Distinguons deux cas.

▶ Cas 1 : si $r\alpha \geq q^\lambda$, alors $r\Big(\frac{N\alpha}{q^\lambda}+2\Big) \geq N+1$ et on a trivialement :

$$\Big|\{n \in I \ : \ s(\lfloor \alpha(n+r)+\beta \rfloor) - s(\lfloor \alpha n+\beta \rfloor) \neq s_\lambda(\lfloor \alpha(n+r)+\beta \rfloor) - s_\lambda(\lfloor \alpha n+\beta \rfloor)\}\Big| \leq N+1.$$

▶ Cas 2 : si $r\alpha < q^\lambda$.
Soit $n \in I = [a, b[$ tel que $n\alpha+\beta \in [kq^\lambda, (k+1)q^\lambda[$ pour un certain $k \in \mathbb{N}$ qu'on estimera plus tard.
Si $n\alpha+\beta+r\alpha \in [kq^\lambda, (k+1)q^\lambda[$, alors n n'est pas candidat. Il reste à traiter le cas où

$$n\alpha+\beta+r\alpha \geq (k+1)q^\lambda.$$

Cette deuxième condition (couplée avec la condition $n\alpha+\beta \in [kq^\lambda, (k+1)q^\lambda]$) nous permet d'estimer n. En effet, on obtient :

$$\frac{(k+1)q^\lambda-\beta-r\alpha}{\alpha} \leq n < \frac{(k+1)q^\lambda-\beta}{\alpha}.$$

Ainsi, le nombre d'entiers $n \in I$ tels que $n\alpha+\beta \in [kq^\lambda, (k+1)q^\lambda[$ et $n\alpha+\beta+r\alpha \geq (k+1)q^\lambda$ est majoré par

$$\frac{(k+1)q^\lambda-\beta}{\alpha} - \frac{(k+1)q^\lambda-\beta-r\alpha}{\alpha} = r.$$

Il nous reste finalement à estimer k. On sait que

$$b\alpha+\beta+r\alpha \geq (k+1)q^\lambda,$$

donc

$$k \leq \frac{b\alpha+\beta+r\alpha}{q^\lambda} - 1.$$

De plus,

$$(k+1)q^\lambda > a\alpha+\beta.$$

Ainsi,

$$k > \frac{a\alpha+\beta}{q^\lambda} - 1.$$

Par conséquent, le nombre de k possibles est majoré par

$$\frac{(b-a)\alpha+r\alpha}{q^\lambda} \leq \frac{(N+1)\alpha}{q^\lambda}+1 \leq \frac{N\alpha}{q^\lambda}+2$$

car $r\alpha < q^\lambda$, donc

$$\Big|\{n \in I \ : \ s_q^\lambda(\lfloor\alpha(n+r)+\beta\rfloor) - s_q^\lambda(\lfloor\alpha n+\beta\rfloor) \neq s_q(\lfloor\alpha(n+r)+\beta\rfloor) - s_q(\lfloor\alpha n+\beta\rfloor)\}\Big| \leq r\Big(\frac{N\alpha}{q^\lambda}+2\Big).$$

□

2.5. Preuve du Théorème 2.3.5

Soient $\rho_2 \geq \rho_1 > 0$ et soient $N, D > 1$ deux entiers tels que

$$N^{\rho_1} \leq D \leq N^{\rho_2}.$$

On rappelle que

$$S_0(N, q^\nu, \xi) = \sum_{q^\nu \leq m < q^{\nu+1}} \max_{a\geq 0} \Big| \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} s_q(nm+a)\right) \mathrm{e}(n\xi)\Big|.$$

Il est suffisant de montrer qu'il existe $\eta_1 = \eta_1(\rho_1, \rho_2) > 0$ et $C = C(\rho_1, \rho_2) > 0$ tels que

$$\frac{S_0(N, q^\nu, \xi)}{Nq^\nu} \leq CN^{-\eta_1} \tag{2.5}$$

pour $\nu \in \mathbb{N}$ satisfaisant $D < q^\nu \leq qD$. En effet, si on suppose que l'inégalité (2.5) est vraie, alors on a

$$\begin{aligned}
S_0(N, D, \xi) &= \sum_{D\leq m<qD} \max_{a\geq 0} \Big| \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} s_q(nm+a)\right) \mathrm{e}(n\xi)\Big| \\
&\leq \sum_{q^{\nu-1}\leq m<q^\nu} \max_{a\geq 0} \Big| \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} s_q(nm+a)\right) \mathrm{e}(n\xi)\Big| \\
&\quad + \sum_{q^\nu\leq m<q^{\nu+1}} \max_{a\geq 0} \Big| \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} s_q(nm+a)\right) \mathrm{e}(n\xi)\Big| \\
&\leq S_0(N, q^{\nu-1}, \xi) + S_0(N, q^\nu, \xi) \\
&\leq CN^{1-\eta_1} q^{\nu-1} + CN^{1-\eta_1} q^\nu \\
&\leq (q+1)CN^{1-\eta_1} D.
\end{aligned}$$

2.5.1. Étape 1 : Itérations de l'inégalité de van der Corput

Nous suivons la méthode de démonstration de **[Spi20]**. Dans un premier temps, nous itérons l'inégalité de van der Corput k fois. Ensuite, l'étape suivante consiste à réécrire l'expression finale sous forme de norme de Gowers. Dans la dernière étape, nous choisirons les différents paramètres et utiliserons l'estimation de la norme de Gowers pour conclure la démonstration.

La première itération

Comme dans les articles portant sur la fonction somme des chiffres, l'inégalité de van der Corput et ses variantes jouent un rôle majeur. La version originale peut, par exemple, être trouvée dans l'ouvrage de Graham/Kolesnik **[GK91,** (2.3.4)**]**.

Lemme 2.5.1. *Soient $0 \leq a < b$ deux entiers et $I = [a, b[$. Soit $f : \mathbb{N} \to \mathbb{C}$ une fonction à valeurs complexes. Soit $0 < H \leq |I|$ un entier. On a*

$$\Big|\sum_{n\in I} \mathrm{e}(f(n))\Big|^2 \leq 2\frac{|I|^2}{H} + 4\frac{|I|}{H}\sum_{1\leq h<H}\Big|\sum_{\substack{n\in I\\ n+h\in I}} \mathrm{e}(f(n+h)-f(n))\Big|.$$

Mauduit et Rivat **[MR09,** Lemme 17**]** ont généralisé l'inégalité de van der Corput à des décalages arbitraires, et ont montré qu'elle peut être utilisée, de manière élégante, pour éliminer les chiffres de poids faible. Comme nous le verrons par la suite, éliminer itérativement des fenêtres de chiffres via cette inégalité permet, in fine, de ne considérer qu'une petite fenêtre de chiffres. Afin de mieux gérer ces itérations, nous réécrivons leur inégalité sous la forme d'une somme unique portant sur tous les $h \in \{0, \dots, H-1\}$, sans isoler le terme diagonal $(h = 0)$.

Lemme 2.5.2. *Soient $0 \leq a < b$ deux entiers et $I = [a, b[$. Soit $f : \mathbb{N} \to \mathbb{C}$ une fonction à valeurs complexes. Soit $K > 0$ un entier. Soit $0 < H \leq |I|$ un entier. On a*

$$\Big|\sum_{n\in I} \mathrm{e}(f(n))\Big|^2 \leq 2\frac{|I| + K(H-1)}{H}\sum_{0\leq h<H}\Big|\sum_{\substack{n\in I\\ n+Kh\in I}} \mathrm{e}(f(n+Kh)-f(n))\Big|.$$

La première itération de l'inégalité de van der Corput permet de réduire le problème initial à un problème où s_q est remplacée par la fonction périodique s_q^λ, avec

$$\lambda > \nu + 1, \tag{2.6}$$

au prix d'une erreur engendrée par la propagation des retenues (Lemme 2.4.5). Nous réécrivons le terme d'erreur sous une forme adaptée aux itérations que nous souhaitons effectuer.

Lemme 2.5.3. *Soient $1 < H_0 \leq N$ et $\lambda > \nu + 1$ deux entiers. On définit pour $h_0 \in \mathbb{N}$,*

$$S_1 = S_1(h_0) = \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}\left(s_q^\lambda((n+h_0)m+a) - s_q^\lambda(nm+a)\right)\right)$$

et

$$E_0 = \frac{3}{H_0} + \frac{4H_0}{q^{\lambda-\nu-1}} + \frac{8H_0}{N}. \tag{2.7}$$

Alors on a

$$\Big|S_0(N, q^\nu, \xi)\Big|^2 \leq (q^{\nu+1}N)^2 E_0 + \frac{2^2 N q^{\nu+1}}{H_0}\sum_{m=q^\nu}^{q^{\nu+1}} \max_{a\geq 0}\sum_{1\leq h_0<H_0} |S_1|.$$

Démonstration. D'après l'inégalité de Cauchy–Schwarz, on a

$$\begin{aligned}\Big|S_0(N, q^\nu, \xi)\Big|^2 &\leq (q^{\nu+1} - q^\nu)\sum_{m=q^\nu}^{q^{\nu+1}}\left(\max_{a\geq 0}\Big|\sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}s_q(nm+a)\right)\mathrm{e}(n\xi)\Big|\right)^2\\ &\leq q^{\nu+1}\sum_{m=q^\nu}^{q^{\nu+1}}\left(\max_{a\geq 0}\Big|\sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}s_q(nm+a)\right)\mathrm{e}(n\xi)\Big|\right)^2.\end{aligned}$$

Soit $1 < H_0 \leq N$ un entier. En utilisant le Lemme 2.5.1 on obtient

$$\begin{aligned}\Big|\sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}s_q(nm+a)\right)\mathrm{e}(n\xi)\Big|^2 &\leq \frac{2N^2}{H_0} + \frac{4N}{H_0}\sum_{1\leq h_0<H_0}\Big|\sum_{0\leq n<N-h_0}\mathrm{e}\left(\frac{\ell}{b}\left(s_q((n+h_0)m+a)-s_q(nm+a)\right)\right)\Big| \\ &\leq \frac{2N^2}{H_0} + \frac{4N}{H_0}\sum_{1\leq h_0<H_0}\Big|\sum_{0\leq n<N}\mathrm{e}\left(\frac{\ell}{b}\left(s_q((n+h_0)m+a)-s_q(nm+a)\right)\right)\Big| \\ &\quad + \frac{4N}{H_0}\sum_{1\leq h_0<H_0} h_0.\end{aligned}$$

Ainsi, d'après le lemme de propagation de retenue (Lemme 2.4.5) on a, pour $\lambda > \nu+1$,

$$\begin{aligned}\Big|\sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}s_q(nm+a)\right)\mathrm{e}(n\xi)\Big|^2 &\leq \frac{2N^2}{H_0} + \frac{4N}{H_0}\sum_{1\leq h_0<H_0}\Big|\sum_{0\leq n<N}\mathrm{e}\left(\frac{\ell}{b}\left(s_q^\lambda((n+h_0)m+a)-s_q^\lambda(nm+a)\right)\right)\Big| \\ &\quad + \frac{4N}{H_0}\sum_{1\leq h_0<H_0} h_0\left(\frac{Nm}{q^\lambda}+3\right).\end{aligned}$$

Ceci implique

$$\begin{aligned}\Big|\sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}s_q(nm+a)\right)\mathrm{e}(n\xi)\Big|^2 &\leq \frac{2N^2}{H_0} + 4NH_0\left(\frac{Nm}{q^\lambda}+3\right) \\ &\quad + \frac{4N}{H_0}\sum_{1\leq h_0<H_0}\Big|\sum_{0\leq n<N}\mathrm{e}\left(\frac{\ell}{b}\left(s_q^\lambda((n+h_0)m+a)-s_q^\lambda(nm+a)\right)\right)\Big|.\end{aligned}$$

Cela mène à

$$\Big|S_0(N,q^\nu,\xi)\Big|^2 \leq (q^{\nu+1}N)^2E_0 + \frac{2^2Nq^{\nu+1}}{H_0}\sum_{m=q^\nu}^{q^{\nu+1}}\max_{a\geq 0}\sum_{1\leq h_0<H_0}|S_1|,$$

où

$$S_1 = \sum_{0\leq n<N}\mathrm{e}\left(\frac{\ell}{b}\left(s_q^\lambda((n+h_0)m+a)-s_q^\lambda(nm+a)\right)\right)$$

et

$$E_0 = \frac{3}{H_0} + \frac{4H_0}{q^{\lambda-\nu-1}} + \frac{8H_0}{N}.$$

□

Les autres itérations

En suivant Spiegelhofer **[Spi20]**, nous continuons d'appliquer l'inégalité de van der Corput. À ce stade, pour les $(k-1)$ prochaines applications de l'inégalité de van der Corput, nous utiliserons le Lemme 2.5.2. Soit $\mu > 0$, et un autre paramètre

$$\sigma < \mu \tag{2.8}$$

que l'on choisira plus tard. Avant de passer à la suite, rappelons (voir Annexe 2, Définition A.0.8) que pour $\alpha \in \mathbb{R}$ et pour $n > 0$, on note $P_n(\alpha)/Q_n(\alpha)$ la fraction de Farey d'ordre n la plus proche de α. Pour $q^\nu \leq m \leq q^{\nu+1}$, on définit

$$\begin{aligned} K_1 &= Q_{q^{2\mu+2\sigma}}\left(\frac{m}{q^{2\mu}}\right) Q_{q^\sigma}\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}}\right), \\ M_1 &= P_{q^{2\mu+2\sigma}}\left(\frac{m}{q^{2\mu}}\right) Q_{q^\sigma}\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}}\right) \end{aligned} \tag{2.9}$$

et pour $2 \leq i < k-1$, on définit

$$\begin{aligned} K_i &= Q_{q^{\mu+2\sigma}}\left(\frac{m}{q^{(i+1)\mu}}\right) Q_{q^\sigma}\left(\frac{P_{q^{\mu+2\sigma}}(m/q^{(i+1)\mu})}{q^{(k-1-i)\mu}}\right), \\ M_i &= P_{q^{\mu+2\sigma}}\left(\frac{m}{q^{(i+1)\mu}}\right) Q_{q^\sigma}\left(\frac{P_{q^{\mu+2\sigma}}(m/q^{(i+1)\mu})}{q^{(k-i-1)\mu}}\right). \end{aligned} \tag{2.10}$$

Enfin, on définit

$$K_{k-1} = Q_{q^{\mu+\sigma}}\left(\frac{m}{q^{k\mu}}\right), \qquad M_{k-1} = P_{q^{\mu+\sigma}}\left(\frac{m}{q^{k\mu}}\right). \tag{2.11}$$

Les nombres $K_1, \ldots, K_{k-1}$ seront les décalages intervenant dans le Lemme 2.5.2. Le choix de ces décalages est motivé par notre volonté d'approcher, au cours des nombreuses phases de coupure de chiffres, les fractions qui apparaissent par des entiers (multiples de puissances de q), en utilisant la Proposition A.0.9. Des résultats classiques sur les suites de Farey nous permettront ensuite de compter le nombre de répétitions d'un élément modulo q^ρ, grâce au Lemme 2.5.7.
Pour commencer, comme $Q_n(\alpha) \leq n$ pour tout $\alpha \in \mathbb{R}$ and et pour tout $n > 0$, on observe que

$$K_1 \leq q^{2\mu+3\sigma} \tag{2.12}$$

et pour tout $2 \leq i \leq k-1$, on a

$$K_i \leq q^{\mu+3\sigma}. \tag{2.13}$$

La deuxième itération de l'inégalité de van der Corput est décrite dans le lemme suivant. Cette fois, nous utilisons le Lemme 2.5.2.

Lemme 2.5.4. *Conservons les mêmes notations que pour le Lemme 2.5.3, avec la condition supplémentaire $E_0 \leq 1$. Soit $1 < H_1 \leq N$ un entier. On définit pour $h_0, h_1 \in \mathbb{N}$,*

$$S_2 = S_2(h_0, h_1) = \sum_{0 \leq n < N} \mathrm{e}\left(\frac{\ell}{b} \sum_{w_0, w_1 \in \{0,1\}} (-1)^{w_0+w_1} s_q^\lambda((n + w_0h_0 + w_1h_1K_1)m + a)\right)$$

et

$$E_1 = \frac{3 \times 2^5 H_1 q^{2\mu+3\sigma}}{N}.$$

Alors, on a

$$\left|S_0(N, q^\nu, \xi)\right|^4 \leq 2(q^{\nu+1}N)^4(E_0 + E_1) + \frac{2^6 N^3 q^{3(\nu+1)}}{H_0 H_1} \sum_{m=q^\nu}^{q^{\nu+1}} \max_{a \geq 0} \sum_{\substack{1 \leq h_0 < H_0 \\ 0 \leq h_1 < H_1}} |S_2|.$$

Démonstration. À l'aide de l'inégalité $(a+b)^2 \le 2a^2+2b^2$, valable pour $a,b \ge 0$, nous élevons au carré les deux membres de l'inégalité du Lemme 2.5.3 pour obtenir

$$\begin{aligned}\left|S_0(N,q^\nu,\xi)\right|^4 &\le \left((q^{\nu+1}N)^2E_0 + \frac{2^2Nq^{\nu+1}}{H_0}\sum_{m=q^\nu}^{q^{\nu+1}}\max_{a\ge 0}\sum_{1\le h_0<H_0}|S_1|\right)^2\\ &\le 2(q^{\nu+1}N)^4E_0^2 + \frac{2^5N^2q^{2(\nu+1)}}{H_0^2}\left(\sum_{m=q^\nu}^{q^{\nu+1}}\max_{a\ge 0}\sum_{1\le h_0<H_0}|S_1|\right)^2.\end{aligned}$$

D'après l'inégalité de Cauchy–Schwarz (appliquée deux fois dans le but de traiter le terme "$\max_{a\ge 0}$"),

$$\left(\sum_{m=q^\nu}^{q^{\nu+1}}\max_{a\ge 0}\sum_{1\le h_0<H_0}|S_1|\right)^2 \le q^{\nu+1}H_0\sum_{m=q^\nu}^{q^{\nu+1}}\max_{a\ge 0}\sum_{1\le h_0<H_0}|S_1|^2,$$

on a

$$\left|S_0(N,q^\nu,\xi)\right|^4 \le 2(q^{\nu+1}N)^4E_0^2 + \frac{2^5N^2q^{3(\nu+1)}}{H_0}\sum_{m=q^\nu}^{q^{\nu+1}}\max_{a\ge 0}\sum_{1\le h_0<H_0}|S_1|^2. \tag{2.14}$$

Nous utiliserons cette inégalité plus tard. On applique le Lemme 2.5.2 pour S_1, $H=H_1$ et $K=K_1$, et obtenons

$$\begin{aligned}|S_1|^2 &\le 2\frac{N+K_1(H_1-1)}{H_1}\sum_{0\le h_1<H_1}\\ &\times\left(\Bigg|\underbrace{\sum_{0\le n<N}\mathrm{e}\left(\frac{\ell}{b}\sum_{w_0,w_1\in\{0,1\}}(-1)^{w_0+w_1}s_q^\lambda((n+w_0h_0+w_1h_1K_1)m+a)\right)}_{S_2}\Bigg| + h_1K_1\right)\\ &\le 2\frac{N+K_1(H_1-1)}{H_1}\left(\sum_{0\le h_1<H_1}|S_2|+H_1^2K_1\right)\\ &\le \frac{2N}{H_1}\sum_{0\le h_1<H_1}|S_2| + \frac{2}{H_1}\left(NH_1^2K_1+H_1^2K_1^2(H_1-1)+K_1(H_1-1)\sum_{0\le h_1<H_1}|S_2|\right).\end{aligned}$$

On majore trivialement

$$\sum_{0\le h_1<H_1}|S_2| \le NH_1$$

et on obtient la majoration

$$\begin{aligned}|S_1|^2 &\le \frac{2N}{H_1}\sum_{0\le h_1<H_1}|S_2| + \frac{2}{H_1}\left(NH_1^2K_1+H_1^2K_1^2(H_1-1)+NH_1K_1(H_1-1)\right)\\ &\le \frac{2N}{H_1}\sum_{0\le h_1<H_1}|S_2| + 2\left(NH_1K_1+H_1K_1^2(H_1-1)+NK_1(H_1-1)\right).\end{aligned}$$

Comme $H_1 \leq N$, $K_1 \geq 2$ et $K_1(H_1-1) < N$ on a

$$|S_1|^2 \leq \frac{2N}{H_1} \sum_{0\leq h_1<H_1} |S_2| + 6NH_1K_1.$$

En utilisant les inégalités (2.12) et (2.13), on obtient

$$\sum_{m=q^\nu}^{q^{\nu+1}} \max_{a\geq 0} \sum_{1\leq h_0<H_0} |S_1|^2 \leq \frac{2N}{H_1} \sum_{m=q^\nu}^{q^{\nu+1}} \max_{a\geq 0} \sum_{\substack{1\leq h_0<H_0\\ 0\leq h_1<H_1}} |S_2| + 6Nq^{\nu+1}H_1H_0q^{2\mu+3\sigma}. \quad (2.15)$$

Puisque $E_0 \leq 1$, on a $E_0^2 \leq E_0$. Par conséquent, en injectant cette inégalité ainsi que (2.15) dans (2.14), on obtient

$$\left|S_0(N,q^\nu,\xi)\right|^4 \leq 2(q^{\nu+1}N)^4(E_0+E_1) + \frac{2^6N^3q^{3(\nu+1)}}{H_0H_1} \sum_{m=q^\nu}^{q^{\nu+1}} \max_{a\geq 0} \sum_{\substack{1\leq h_0<H_0\\ 0\leq h_1<H_1}} |S_2|,$$

où

$$S_2 = \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} \sum_{w_0,w_1\in\{0,1\}} (-1)^{w_0+w_1} s_q^\lambda((n+w_0h_0+w_1h_1K_1)m+a)\right)$$

et

$$E_1 = \frac{3\times 2^5 H_1 q^{2\mu+3\sigma}}{N}.$$

□

Jusqu'à la fin de la preuve, on choisit

$$\rho = \lambda - k\mu. \quad (2.16)$$

Prenons $H_1 = q^\rho$. Ce choix nous permettra d'utiliser la majoration $E_1+E_0 \leq 1$, et ainsi

$$(E_1+E_0)^2 \leq E_1+E_0.$$

En appliquant exactement le même raisonnement que précédemment, nous obtenons, par une seconde application du Lemme 2.5.2, le lemme suivant :

Lemme 2.5.5. *Nous reprenons les mêmes notations que dans le Lemme 2.5.3 et le Lemme 2.5.4, avec la condition $E_0+E_1 \leq 1$. Soit $1 < H_2 \leq N$ un entier. Nous posons*

$$S_3 = \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} \sum_{w_0,w_1,w_2\in\{0,1\}} (-1)^{w_0+w_1+w_2} s_q^\lambda((n+w_0h_0+w_1h_1K_1+w_2h_2K_2)m+a)\right)$$

et

$$E_2 = \frac{3\times 2^{12} H_2K_2}{N}.$$

Alors, on a

$$\left|S_0(N,q^\nu,\xi)\right|^8 \leq 2^2(q^\nu N)^8(E_0+E_1+E_2) + \frac{2^{14}N^7q^{7(\nu+1)}}{H_0H_1H_2} \sum_{\substack{1\leq h_0<H_0\\ 0\leq h_1<H_1\\ 0\leq h_2<H_2}} \sum_{m=q^\nu}^{q^{\nu+1}} \max_{a\geq 0} |S_3|.$$

À ce stade, nous pouvons obtenir une formule de récurrence pour la k-ième itération de l'inégalité de van der Corput. Dans le lemme suivant, nous effectuons d'abord une sommation sur m. L'étape suivante consistera à réaliser certains décalages de chiffres pour un paramètre fixe m.

Lemme 2.5.6. *Soit $k \geq 2$ un entier. Soient $H_0, H_1, \dots, H_{k-1} > 1$ des entiers. On pose*

$$\begin{aligned} E_0 &= \frac{3}{H_0} + \frac{4H_0}{q^{\lambda-\nu}} + \frac{8H_0}{N}, \\ E_i &= \frac{3 \times 2^{2^{i+2}-1}}{2^{i+1}} \times \frac{H_i q^{2\mu+3\sigma}}{N}, \qquad 1 \leq i \leq k-1. \end{aligned} \tag{2.17}$$

De plus, supposons que

$$E_0 + E_1 + \cdots + E_{k-1} \leq 1. \tag{2.18}$$

Posons

$$S_4 = \sum_{0 \leq n < N} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^{\lambda}\left(nm + a + w_0 h_0 m + \sum_{i=1}^{k-1} w_i K_i m \right) \right).$$

Alors on a l'inégalité

$$\begin{aligned} \left| \frac{S_0(N, q^\nu, \xi)}{q^{\nu+1}N} \right|^{2^k} &\leq 2^{k-1}(E_0 + \cdots + E_{k-1}) \\ &\quad + \frac{2^{2^{k+2}-2}}{H_0 \cdots H_{k-1} q^{\nu+1} N} \sum_{m=q^\nu}^{q^{\nu+1}} \sum_{\substack{1 \leq h_0 < H_0 \\ 0 \leq h_i < H_i,\ 1 \leq i \leq k-1}} \max_{a \geq 0} |S_4|. \end{aligned} \tag{2.19}$$

Le Lemme 2.5.6 termine la première étape. Notre choix final des paramètres respectera bien (2.18). Nous vérifierons toutes les inégalités qui en découlent dans la Section 8.

2.5.2. Étape 2 : Décalage et découpage

L'objectif suivant est de transformer S_4 afin d'éliminer plusieurs blocs de chiffres par décalage. Nous établissons le résultat auxiliaire suivant, qui nous permettra par la suite de réduire la fenêtre d'étude dans le processus de transformation de S_4.

Lemme 2.5.7. *Soient μ, ν, σ, γ des entiers tels que $\nu + 1 \geq 3\gamma$ et soit $k \geq 3$ un entier. Pour $m \in \{0, \dots, q^{\nu+1} - 1\}$, on définit*

$$\mathfrak{M}_1 = P_{q^\sigma}\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}} \right)$$

et pour tout $1 < i < k-1$ on pose

$$\mathfrak{M}_i = P_{q^\sigma}\left(\frac{P_{q^{\mu+2\sigma}}(m/q^{(i+1)\mu})}{q^{(k-i-1)\mu}} \right).$$

Enfin, pour $i = k-1$, on pose

$$\mathfrak{M}_{k-1} = P_{q^\sigma}\left(\frac{P_{q^{\mu+\sigma}}(m/q^{k\mu})}{q^{k\mu}} \right).$$

On définit l'ensemble

$$A = \{m \in \{0, \dots, q^{\nu+1} - 1\} \,:\, \exists i \in \{1, \dots, k-1\},\ \exists p \mid q\,,\ p^{3\gamma} | \mathfrak{M}_i\}.$$

Alors

$$|A| = \mathcal{O}_q(q^{\nu+1-3\gamma \log_q(P^-(q))}). \tag{2.20}$$

Démonstration. Pour rendre la démonstration plus lisible, nous nous concentrons uniquement sur $\mathfrak{M}_1$; les autres cas ($2 \leq i \leq k-1$) se traitent de manière presque identique. Le lecteur pourra consulter l'article de Spiegelhofer **[Spi20,** Lemma 5.1**]** pour voir les légères modifications intervenant dans les cas $2 \leq i \leq k-1$. Nous considérons d'abord le cas où $(m, q) = 1$ (Cas 1). Quelques ajustements mineurs et estimations nous permettront ensuite de traiter le cas général (Cas 2).

▶ Cas 1 : $(m, q) = 1$.
Dans un premier temps, nous établissons la formule suivante pour $\mathfrak{M}_1$:

$$\mathfrak{M}_1 = P_{q^\sigma}(m_0/q^{(k-2)\mu}) + m_1 Q_{q^\sigma}(m_0/q^{(k-2)\mu}), \tag{2.21}$$

où m_0 est défini ci-après. Commençons par remarquer que $\dfrac{m}{q^{2\mu}} \in \mathcal{F}_{q^{2\mu+2\sigma}}$. Ainsi,

$$\frac{m}{q^{2\mu}} = \frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{Q_{q^{2\mu+2\sigma}}(m/q^{2\mu})}.$$

De plus, puisque $(m, q) = 1$, on a

$$P_{q^{2\mu+2\sigma}}(m/q^{2\mu}) = m. \tag{2.22}$$

En effectuant la division euclidienne de m par $q^{(k-2)\mu}$ et en utilisant la condition $m < q^{\nu+1}$, on obtient :

$$m = m_0 + q^{(k-2)\mu} m_1,$$

avec :

$$m_0 \in \{0, \dots, q^{(k-2)\mu} - 1\}, \qquad m_1 \in \{0, \dots, q^{\nu+1-(k-2)\mu} - 1\}.$$

On écrit alors :

$$\frac{P}{Q} \leq \frac{m_0}{q^{(k-2)\mu}} \leq \frac{P'}{Q'},$$

où $\dfrac{P}{Q}$ et $\dfrac{P'}{Q'}$ sont deux fractions voisines dans $\mathcal{F}_{q^\sigma}$. En ajoutant m_1 à chaque terme de cette double inégalité, on obtient :

$$\frac{P + m_1 Q}{Q} \leq \frac{m}{q^{(k-2)\mu}} \leq \frac{P' + m_1 Q'}{Q'}. \tag{2.23}$$

Puisque $(P, Q) = 1$ et $(P', Q') = 1$, toutes les fractions sont irréductibles. De plus, comme $\dfrac{P}{Q}$ et $\dfrac{P'}{Q'}$ sont voisines dans $\mathcal{F}_{q^\sigma}$, alors, par translation, $(P + m_1 Q)/Q$ et $(P' + m_1 Q')/Q'$ sont encore voisines dans $\mathcal{F}_{q^\sigma}$. On distingue deux cas selon la position de $m_0/q^{(k-2)\mu}$ par rapport au point médian de l'intervalle $[P/Q, P'/Q'[$. Supposons d'abord que :

$$\frac{m_0}{q^{(k-2)\mu}} \leq \frac{P + P'}{Q + Q'}. \tag{2.24}$$

Alors, d'après la Définition A.0.8, on a :

$$\frac{P}{Q} = \frac{P_{q^\sigma}(m_0/q^{(k-2)\mu})}{Q_{q^\sigma}(m_0/q^{(k-2)\mu})}.$$

De plus, comme :

$$\begin{aligned}\frac{m}{q^{(k-2)\mu}} &= \frac{m_0}{q^{(k-2)\mu}} + m_1,\\ &\leq \frac{P+P'}{Q+Q'} + m_1,\\ &\leq \frac{(P+m_1Q)+(P'+m_1Q')}{Q+Q'},\end{aligned}$$

le nombre $\dfrac{m}{q^{(k-2)\mu}}$ est donc inférieur au milieu de $(P+m_1Q)/Q$ et $(P'+m_1Q')/Q'$. Cela implique, grâce à (2.22) et (2.23), que :

$$\begin{aligned}\mathfrak{M}_1 &= Pq^\sigma\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}}\right)\\ &= P + m_1Q\\ &= P_{q^\sigma}(m_0/q^{(k-2)\mu}) + m_1Q_{q^\sigma}(m_0/q^{(k-2)\mu}),\end{aligned}$$

comme annoncé dans (2.21). Pour le second cas, nous supposons désormais que

$$\frac{m_0}{q^{(k-2)\mu}} > \frac{P+P'}{Q+Q'}. \tag{2.25}$$

Un calcul similaire à ce qu'on a fait au-dessus montre que

$$\begin{aligned}\mathfrak{M}_1 &= P_{q^\sigma}\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}}\right)\\ &= P' + m_1Q'\\ &= P_{q^\sigma}(m_0/q^{(k-2)\mu}) + m_1Q_{q^\sigma}(m_0/q^{(k-2)\mu}).\end{aligned}$$

Dans les deux cas on arrive à la même conclusion, l'identité (2.21). Concentrons-nous désormais sur (2.20). On suppose qu'il existe $p|q$ tel que $p^{3\gamma} \mid \mathfrak{M}_1$. On observe que $p \nmid Q_{q^\sigma}(m_0/q^{(k-2)\mu})$ car sinon, d'après (2.21), p diviserait $P_{q^\sigma}(m_0/q^{(k-2)\mu})$ ce qui contredit l'hypothèse

$$(Q_{q^\sigma}(m_0/q^{(k-2)\mu}), P_{q^\sigma}(m_0/q^{(k-2)\mu})) = 1.$$

Pour un nombre $m_0 \in \{0,\dots,q^{(k-2)\mu}-1\}$ fixé, le nombre d'entiers m_1 appartenant à l'ensemble $\left\{0,\dots,q^{\nu+1-(k-2)\mu}-1\right\}$ tels que

$$m_1Q_{q^\sigma}(m_0/q^{(k-2)\mu}) \equiv -P_{q^\sigma}(m_0/q^{(k-2)\mu}) \pmod{p^{3\gamma}}$$

est borné par $q^{\nu+1-(k-2)\mu}/p^{3\gamma}$. Donc, le nombre d'entiers $m \in \{0,\dots,q^{\nu+1}-1\}$ tels que $p^{3\gamma} \mid \mathfrak{M}_1$ est au plus égal à $q^{\nu+1}/p^{3\gamma}$.

► Cas 2 : $(m,q) > 1$.
La seule différence réside dès le départ de la preuve. La fraction $m/q^{2\mu}$ n'est plus

irréductible mais il suffit de la réduire en m'/q' (avec $(m',q')=1$) et de procéder exactement comme précédemment avec q', m' à la place de q, m.

On collecte toutes ces informations pour estimer le cardinal de A défini en amont. On obtient

$$\begin{aligned}|A| &\leq \sum_{\substack{p\in\mathbb{P}\\ p|q}} |\{m\in\{0,\dots,q^{\nu+1}-1\} : \quad \exists i\in\{1,\dots,k-1\}, \quad p^{3\gamma}|\,\mathfrak{M}_i\}| \\ &\leq q^{\nu+1}\sum_{\substack{p\in\mathbb{P}\\ p|q}} p^{-3\gamma} \\ &\leq \omega(q)q^{\nu+1}P^-(q)^{-3\gamma}.\end{aligned}$$

□

Commençons désormais les premières transformations de S_4. Nous avons le lemme suivant.

Lemme 2.5.8. *Nous reprenons les mêmes notations que dans le Lemme 2.5.6 ainsi que la définition (2.16) de ρ. Alors, nous avons*

$$S_4 = S_5 + \mathcal{O}_k\left(N\sum_{i=2}^{k-1} D_N\left(\frac{m}{q^{i\mu}}\right) + \frac{2N}{q^\sigma}\left(H_1+H_2+\cdots+H_{k-1}\right)\right), \tag{2.26}$$

où

$$S_5 = \sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b}\sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^\rho\left(\left\lfloor \frac{nm+a+w_0h_0m}{q^{k\mu}} + \sum_{i=1}^{k-1} w_ih_i\mathfrak{M}_i\right\rfloor\right)\right), \tag{2.27}$$

et $D_N(\alpha)$ est la $N-$discrépance de $\alpha\in\mathbb{R}$ dont la définition et des propriétés clés dans notre étude sont données dans l'Annexe 2.

Démonstration. D'après (2.9), et d'après la définition des suites de Farey (voir Section 2), on a

$$\frac{M_1}{K_1} = \frac{m}{q^{2\mu}}.$$

Ainsi

$$K_1m = q^{2\mu}M_1.$$

Dans S_4, définie par (2.5.6), on remplace $w_1h_1K_1m$ par $w_1h_1q^{2\mu}M_1$ et on applique le Lemme 2.4.3 avec $u_1 = h_1M_1$ et $\alpha = 2\mu$. Cela nous donne pour tout $w_0, w_2, \dots, w_{k-1}, n, h_i$:

$$\begin{aligned}-s_q^\lambda(nm+a+w_0h_0m+h_1q^{2\mu}m+\sum_{j=2}^{k-1} w_ih_iK_im)+s_q^\lambda(nm+a+w_0h_0m+\sum_{j=2}^{k-1} w_ih_iK_im)&\\ = -s_q^{2\mu,\lambda}(nm+a+w_0h_0m+h_1q^{2\mu}m+\sum_{j=2}^{k-1} w_ih_iK_im)&\\ + s_q^{2\mu,\lambda}(nm+a+w_0h_0m+\sum_{j=2}^{k-1} w_ih_iK_im).&\end{aligned}$$

Nous insérons ceci dans S_4 et rappelons que, dans la formule précédente, le premier terme du membre de droite correspond à $w_1 = 1$, le second à $w_1 = 0$, avec le signe « $-$ » associé à $(-1)^{s_2(w)}$ correspondant. De plus, dans la deuxième ligne ci-dessous, nous utiliserons le fait que pour $u \in \mathbb{N}$,

$$s_q^{2\mu,\lambda}(u) = s_q^{\lambda-2\mu}\big(\lfloor u/q^{2\mu} \rfloor\big).$$

On écrit

$$\begin{aligned}
S_4 &= \sum_{0\le n<N} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^{2\mu,\lambda}(nm + a + w_0h_0m + w_1h_1q^{2\mu}m \right.\\
&\qquad \left. + \cdots + w_{k-1}h_{k-1}K_{k-1}m)\right)\\
&= \sum_{0\le n<N} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} \right.\\
&\qquad \left. \times\, s_q^{\lambda-2\mu}\left(\left\lfloor \frac{1}{q^{2\mu}}\left(nm + a + w_0h_0m + \sum_{i=1}^{k-1} w_ih_iK_im\right)\right\rfloor\right)\right)\\
&= \sum_{0\le n<N} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^{\lambda-2\mu}\left(\left\lfloor \frac{nm + a + w_0h_0m}{q^{2\mu}} \right.\right.\right.\\
&\qquad \left.\left.\left. + w_1h_1M_1 + w_2h_2\frac{K_2m}{q^{2\mu}} + \sum_{i=3}^{k-1} w_i\frac{h_iK_im}{q^{2\mu}}\right\rfloor\right)\right). \qquad (2.28)
\end{aligned}$$

Nous souhaitons maintenant remplacer $\frac{K_2m}{q^{2\mu}}$ par un multiple d'une puissance de q. Nous utilisons d'abord la Proposition **A.0.9** pour approcher la fraction $\frac{K_2m}{q^{2\mu}}$ par l'entier $q^\mu M_2$, au prix d'une erreur admissible. D'après (**2.10**), nous avons

$$\begin{aligned}
\left|\frac{K_2m}{q^{2\mu}} - q^\mu M_2\right| &= q^\mu Q_{q^\sigma}\left(\frac{P_{q^{\mu+2\sigma}}(m/q^{3\mu})}{q^{(k-3)\mu}}\right)\left|\frac{m}{q^{3\mu}}Q_{q^{\mu+2\sigma}}\left(\frac{m}{q^{3\mu}}\right) - P_{q^{\mu+2\sigma}}\left(\frac{m}{q^{3\mu}}\right)\right|\\
&< q^{\sigma+\mu} \times \frac{1}{q^{\mu+2\sigma}}\\
&= q^{-\sigma}. \qquad (2.29)
\end{aligned}$$

De plus, nous introduisons l'ensemble

$$A = \left\{0 \le n < N \,:\, \left\|\frac{nm + a + w_0h_0m}{q^{2\mu}} + w_1h_1M_1 + \sum_{i=3}^{k-1} w_i\frac{h_iK_im}{q^{2\mu}}\right\| \ge \frac{H_2}{q^\sigma}\right\}.$$

Pour $n \in A$, l'inégalité (**2.29**) montre que

$$\left\|\frac{K_2m}{q^{2\mu}}\right\| < q^{-\sigma}.$$

À ce stade, on suppose que pour tout $1 \le i \le k-1$,

$$H_i < q^{\sigma-1}. \qquad (2.30)$$

Dans la Section 8, on choisit pour tout $1 \leq i \leq k-1$, $H_i = q^\rho$. De ce fait, on a la condition

$$\rho < \sigma - 1. \tag{2.31}$$

Comme $0 \leq h_2 \leq H_2 < q^{\sigma-1}$, nous avons, d'après l'inégalité (C.32) de la Proposition C.0.14,

$$\left\langle \frac{h_2 K_2 m}{q^{2\mu}} \right\rangle = h_2 \left\langle \frac{K_2 m}{q^{2\mu}} \right\rangle = h_2 q^\mu M_2.$$

Donc, d'après l'inégalité (C.30) de la Proposition C.0.14, on obtient

$$\begin{aligned}
&\left\lfloor \frac{nm+a+w_0h_0m}{q^{2\mu}} + w_1h_1M_1 + \sum_{i=3}^{k-1} w_i \frac{h_iK_im}{q^{2\mu}} + w_2 \frac{h_2K_2m}{q^{2\mu}} \right\rfloor \\
&\qquad = \left\lfloor \frac{nm+a+w_0h_0m}{q^{2\mu}} + w_1h_1M_1 + \sum_{i=3}^{k-1} w_i \frac{h_iK_im}{q^{2\mu}} \right\rfloor + w_2 \left\langle \frac{h_2K_2m}{q^{2\mu}} \right\rangle \\
&\qquad = \left\lfloor \frac{nm+a+w_0h_0m}{q^{2\mu}} + w_1h_1M_1 + \sum_{i=3}^{k-1} w_i \frac{h_iK_im}{q^{2\mu}} \right\rfloor + w_2h_2q^\mu M_2 \\
&\qquad = \left\lfloor \frac{nm+a+w_0h_0m}{q^{2\mu}} + w_1h_1M_1 + w_2h_2q^\mu M_2 + \sum_{i=3}^{k-1} w_i \frac{h_iK_im}{q^{2\mu}} \right\rfloor.
\end{aligned}$$

En séparant la somme dans (2.28) selon que $n \in A$ ou que $n \notin A$, et en utilisant le Lemme B.0.12 afin de majorer la somme pour $n \notin A$, nous obtenons

$$\begin{aligned}
S_4 = \sum_{0 \leq n < N} \mathrm{e}\Bigg(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^{\lambda-2\mu} \Bigg(\Bigg\lfloor \frac{nm+a+w_0h_0m}{q^{2\mu}} + w_1h_1M_1 \\
+ w_2h_2q^\mu M_2 + \sum_{i=3}^{k-1} w_i \frac{h_iK_im}{q^{2\mu}} \Bigg\rfloor \Bigg) \Bigg) + \mathcal{O}\left(ND_N\left(\frac{m}{q^{2\mu}} \right) + \frac{2H_1N}{q^\sigma} \right).
\end{aligned}$$

En répétant la même démarche, on a

$$\begin{aligned}
S_4 = \sum_{0 \leq n < N} \mathrm{e}\Bigg(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^{\lambda-3\mu} \Bigg(\Bigg\lfloor \frac{nm+a+w_0h_0m}{q^{3\mu}} + w_1h_1 \frac{M_1}{q^\mu} \\
+ w_2h_2M_2 + \sum_{i=3}^{k-1} w_i \frac{h_iK_im}{q^{3\mu}} \Bigg\rfloor \Bigg) \Bigg) + \mathcal{O}\left(N\left(D_N\left(\frac{m}{q^{2\mu}} \right) + D_N\left(\frac{m}{q^{3\mu}} \right) \right) + \frac{2N}{q^\sigma}(H_1+H_2) \right).
\end{aligned}$$

On continue le processus et on obtient

$$\begin{aligned}
S_4 = \sum_{0 \leq n < N} \mathrm{e}\Bigg(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} \\
\times s_q^{\lambda-k\mu} \Bigg(\Bigg\lfloor \frac{nm+a+w_0h_0m}{q^{k\mu}} + \sum_{i=1}^{k-1} w_i \frac{h_iM_i}{q^{(k-1-i)\mu}} \Bigg\rfloor \Bigg) \Bigg) \\
+ \mathcal{O}\left(N \sum_{i=2}^{k-1} D_N\left(\frac{m}{q^{i\mu}} \right) + \frac{2N}{q^\sigma}(H_1 + \cdots + H_{k-1}) \right).
\end{aligned}$$

Pour éliminer $\frac{M_i}{q^{(k-1-i)\mu}}$ $(1 \leq i \leq k-1)$, nous utilisons à nouveau l'approximation de Farey (Proposition A.0.9). Nous avons,

$$\left| \underbrace{\frac{P_{q^{2\mu+2\sigma}}\left(\frac{m}{q^{2\mu}}\right)}{q^{(k-2)\mu}} Q_{q^\sigma}\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}}\right)}_{M_1/q^{(k-2)\mu}} - P_{q^\sigma}\left(\frac{P_{q^{2\mu+2\sigma}}(m/q^{2\mu})}{q^{(k-2)\mu}}\right) \right| < q^{-\sigma}.$$

Pour $1 < i < k-1$, on a

$$\left| \underbrace{\frac{P_{q^{\mu+2\sigma}}\left(\frac{m}{q^{(i+1)\mu}}\right)}{q^{(k-i-1)\mu}} Q_{q^\sigma}\left(\frac{P_{q^{\mu+2\sigma}}(m/q^{(i+1)\mu})}{q^{(k-i-1)\mu}}\right)}_{M_i/q^{(k-i-1)\mu}} - P_{q^\sigma}\left(\frac{P_{q^{\mu+2\sigma}}(m/q^{(i+1)\mu})}{q^{(k-i-1)\mu}}\right) \right| < q^{-\sigma}$$

et

$$\left| \underbrace{\frac{P_{q^{\mu+\sigma}}\left(\frac{m}{q^{k\mu}}\right)}{q^{k\mu}} Q_{q^\sigma}\left(\frac{P_{q^{\mu+\sigma}}(m/q^{k\mu})}{q^{k\mu}}\right)}_{M_{k-1}/q^{k\mu}} - P_{q^\sigma}\left(\frac{P_{q^{\mu+\sigma}}(m/q^{k\mu})}{q^{k\mu}}\right) \right| < q^{-\sigma}.$$

Avec le même argument qu'auparavant, nous obtenons

$$S_4 = \underbrace{\sum_{0\leq n<N} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^{\lambda-k\mu}\left(\left\lfloor \frac{nm+a+w_0h_0m}{q^{k\mu}} + \sum_{i=1}^{k-1} w_i h_i \mathfrak{M}_i \right\rfloor\right)\right)}_{S_5}$$
$$+ \mathcal{O}_k\left(N \sum_{i=2}^{k-1} D_N\left(\frac{m}{q^{i\mu}}\right) + \frac{2N}{q^\sigma}\left(H_1 + H_2 + \cdots + H_{k-1}\right)\right),$$

ce qui termine la preuve du Lemme 2.5.8. □

Notre objectif suivant est de traiter le terme

$$\left\lfloor \frac{nm+a}{q^{k\mu}} \right\rfloor$$

présent dans S_5 afin de simplifier encore davantage l'argument de $s_q^{\lambda-k\mu}$. Rappelons que $\rho = \lambda - k\mu$, d'après (2.16).

Lemme 2.5.9. *Soient $T, h_0, m \geq 2$ des entiers. On pose*

$$\Lambda = \Lambda(h_0, m) = \left\{0 \leq t < T : \quad \left[\frac{t}{T} + \frac{h_0 m}{q^{k\mu}}, \frac{t+1}{T} + \frac{h_0 m}{q^{k\mu}}\right[\cap \mathbb{Z} = \emptyset\right\}. \tag{2.32}$$

Alors pour tout $k \geq 1$,

$$\left|\frac{S_0(N,\nu,\xi)}{q^{\nu+1}N}\right|^{2^k} \leq 2^{k-1}(E_0+\cdots+E_{k-1}) + \frac{2^{2^{k+2}-2}}{T} + \frac{2^{2^{k+2}-2}}{H_0\cdots H_{k-1}q^{\nu+1+\rho}T}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{\substack{1\leq h_0<H_0\\ 1\leq i\leq k-1,\ 0\leq h_i<H_i}}\sum_{t\in\Lambda}|S_8| + 2^{2^{k+2}-2}\mathcal{O}\left(\frac{T}{q^{\nu+1-\rho}}\sum_{m=q^\nu}^{q^{\nu+1}}D_N\left(\frac{m}{q^\lambda}\right) + \frac{1}{q^{\nu+1}}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{i=2}^{k-1}D_N\left(\frac{m}{q^{i\mu}}\right) + \frac{2(H_1+\cdots+H_{k-1})}{q^\sigma}\right),$$

où

$$S_8 = \sum_{0\leq n'<q^\rho}\mathrm{e}\left(\frac{\ell}{b}\sum_{\mathbf{w}=(w_0,\ldots,w_{k-1})\in\{0,1\}^k}(-1)^{s_2(w)}s_q^\rho\left(n' + \left\lfloor\frac{t}{T}+\frac{w_0h_0m}{q^{k\mu}}\right\rfloor + \sum_{1\leq i\leq k-1}w_ih_i\mathfrak{M}_i\right)\right).$$

Démonstration. Pour tout $0 \leq n \leq N$, il existe un unique couple (t,n') tel que $0\leq t<T$ et $0\leq n'<q^\rho$, avec $\frac{t}{T} \leq \left\{\frac{nm+a}{q^{k\mu}}\right\} < \frac{t+1}{T}$ et $\left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor \equiv n' \pmod{q^\rho}$. Nous réécrivons S_5 (cf. (2.27)) et séparons la somme en deux parties selon que les valeurs $1\leq t<T$ appartiennent à Λ ou non :

$$S_5 = \sum_{0\leq t<T}\sum_{0\leq n'<q^\rho}\sum_{\substack{0\leq n<N\\ t/T\leq\{(nm+a)/q^{k\mu}\}<(t+1)/T\\ \lfloor\frac{nm+a}{q^{k\mu}}\rfloor\equiv n' \pmod{q^\rho}}}\mathrm{e}\left(\frac{\ell}{b}\sum_{\mathbf{w}=(w_0,\ldots,w_{k-1})\in\{0,1\}^k}(-1)^{s_2(w)} \times s_q^\rho\left(\left\lfloor\frac{nm+a}{q^{k\mu}}+\frac{w_0h_0m}{q^{k\mu}}\right\rfloor + \sum_{1\leq i\leq k-1}w_ih_i\mathfrak{M}_i\right)\right)$$
$$= \sum_{t\in\Lambda} + \sum_{t\notin\Lambda} =: S_6 + S_7.$$

Comme

$$\bigcup_{t=0}^{T-1}\left[\frac{t}{T}+\frac{h_0m}{q^{k\mu}}, \frac{t+1}{T}+\frac{h_0m}{q^{k\mu}}\right[= \left[\frac{h_0m}{q^{k\mu}}, \frac{h_0m}{q^{k\mu}}+1\right[$$

est un intervalle de longueur 1, cet intervalle contient exactement un entier qui doit se trouver dans exactement l'un des T sous-intervalles. Ainsi, $|\Lambda| = T-1$.

▶ Pour $t\notin\Lambda$ (une seule valeur de t), nous majorons trivialement S_7 à l'aide de la Proposition B.0.11 :

$$|S_7| \le \sum_{0\le n'<q^\rho} \sum_{\substack{0\le n<N\\ t/T\le\{(nm+a)/q^{k\mu}\}<(t+1)/T\\ \lfloor\frac{nm+a}{q^{k\mu}}\rfloor\equiv n' \pmod{q^\rho}}} 1$$
$$\le q^\rho\left(\frac{N}{Tq^\rho}+\mathcal{O}\left(ND_N\left(\frac{m}{q^{\rho+k\mu}}\right)\right)\right)$$
$$= \frac{N}{T}+\mathcal{O}\left(Nq^\rho D_N\left(\frac{m}{q^\lambda}\right)\right).$$

► Pour $t\in\Lambda$ (qui représente $(T-1)$ valeurs de t), on écrit

$$\frac{nm+a}{q^{k\mu}} = \left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor + \underbrace{\left\{\frac{nm+a}{q^{k\mu}}\right\}}_{\in[t/T,(t+1)/T[}.$$

On en déduit que pour $w_0\in\{0,1\}$

$$\left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor+\frac{t}{T}+\frac{w_0h_0m}{q^{k\mu}} \le \frac{nm+a+w_0h_0m}{q^{k\mu}} < \left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor+\frac{t+1}{T}+\frac{w_0h_0m}{q^{k\mu}}.$$

Comme $t\in\Lambda$, on a pour $w_0=1$,

$$\left[\left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor+\frac{t}{T}+\frac{h_0m}{q^{k\mu}}, \left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor+\frac{t+1}{T}+\frac{h_0m}{q^{k\mu}}\right[\cap\mathbb{Z}=\emptyset$$

et nous avons nécessairement

$$\left\lfloor\frac{nm+a}{q^{k\mu}}+\frac{w_0h_0m}{q^{k\mu}}\right\rfloor = \left\lfloor\frac{nm+a}{q^{k\mu}}\right\rfloor+\left\lfloor\frac{t}{T}+\frac{w_0h_0m}{q^{k\mu}}\right\rfloor. \tag{2.33}$$

On remarque que (2.33) est également vraie dans le cas $w_0=0$ et pour tout $0\le t<T$, à une exception près. Ainsi, par périodicité de s_q^ρ, nous avons

$$S_6 = \sum_{t\in\Lambda}\sum_{0\le n'<q^\rho} \sum_{\substack{0\le n<N\\ t/T\le\{(nm+a)/q^{k\mu}\}<(t+1)/T\\ \lfloor(nm+a)/q^{k\mu}\rfloor\equiv n' \pmod{q^\rho}}} \mathrm{e}\left(\frac{\ell}{b}\sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k}(-1)^{s_2(w)}s_q^\rho\left(n'+\left\lfloor\frac{t}{T}+\frac{w_0h_0m}{q^{k\mu}}\right\rfloor + \sum_{1\le i\le k-1}w_ih_i\mathfrak{M}_i\right)\right)$$
$$= \sum_{t\in\Lambda}\sum_{0\le n'<q^\rho} \mathrm{e}\left(\frac{\ell}{b}\sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k}(-1)^{s_2(w)}s_q^\rho\left(n'+\left\lfloor\frac{t}{T}+\frac{w_0h_0m}{q^{k\mu}}\right\rfloor+\sum_{1\le i\le k-1}w_ih_i\mathfrak{M}_i\right)\right) \times \sum_{\substack{0\le n<N\\ t/T\le\{(nm+a)/q^{k\mu}\}<(t+1)/T\\ \lfloor(nm+a)/q^{k\mu}\rfloor\equiv n' \pmod{q^\rho}}} 1.$$

D'après la Proposition B.0.11, la somme sur n vaut $N/(Tq^\rho)+\mathcal{O}\big(ND_N(q^{\rho+k\mu})\big)$. Nous majorons trivialement $|S_8|$ par q^ρ dans l'estimation de la contribution du terme d'erreur $ND_N\left(q^{\rho+k\mu}\right)$,

$$|S_6|=\left|\sum_{t\in\Lambda}S_8\left(\frac{N}{q^\rho T}+\mathcal{O}\left(ND_N\left(\frac{m}{q^{\rho+k\mu}}\right)\right)\right)\right|\leq\frac{N}{Tq^\rho}\sum_{t\in\Lambda}|S_8|+\mathcal{O}\left(q^\rho NTD_N\left(\frac{m}{q^\lambda}\right)\right).$$

Ainsi, d'après l'inégalité triangulaire, on obtient

$$\begin{aligned}|S_4|&\leq|S_6|+|S_7|+O\left(N\sum_{i=2}^{k-1}D_N\left(\frac{m}{q^{i\mu}}\right)+\frac{2N}{q^\sigma}(H_1+\cdots+H_{k-1})\right)\\&\leq\frac{N}{Tq^\rho}\sum_{t\in\Lambda}|S_8|+\frac{N}{T}+O\left(q^\rho NTD_N\left(\frac{m}{q^\lambda}\right)+N\sum_{i=2}^{k-1}D_N\left(\frac{m}{q^{i\mu}}\right)+\frac{2N}{q^\sigma}(H_1+\cdots+H_{k-1})\right).\end{aligned}$$

Nous injectons la dernière inégalité dans l'équation (2.19) et obtenons

$$\begin{aligned}\left|\frac{S_0(N,\nu,\xi)}{q^{\nu+1}N}\right|^{2^k}&\leq 2^{k-1}(E_0+\cdots+E_{k-1})\\&\quad+\frac{2^{2^{k+2}-2}}{H_0\cdots H_{k-1}q^{\nu+1}N}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{\substack{1\leq h_0<H_0\\0\leq h_i<H_i,\ 1\leq i\leq k-1}}\max_{a\geq0}|S_4|\\&\leq 2^{k-1}(E_0+\cdots+E_{k-1})+\frac{2^{2^{k+2}-2}}{T}\\&\quad+\frac{2^{2^{k+2}-2}}{H_0\cdots H_{k-1}q^{\nu+1+\rho}T}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{\substack{1\leq h_0<H_0\\0\leq h_i<H_i,\ 1\leq i\leq k-1}}\sum_{t\in\Lambda}|S_8|\qquad(2.34)\\&\quad+2^{2^{k+2}-2}\mathcal{O}\Bigg(\frac{T}{q^{\nu+1-\rho}}\sum_{m=q^\nu}^{q^{\nu+1}}D_N\left(\frac{m}{q^\lambda}\right)+\frac{1}{q^{\nu+1}}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{i=2}^{k}D_N\left(\frac{m}{q^{i\mu}}\right)\\&\qquad\qquad+\frac{2(H_1+\cdots+H_{k-1})}{q^\sigma}\Bigg),\end{aligned}$$

où le dernier terme est majoré trivialement.

□

Jusqu'à la fin de la preuve, on prend pour tout $1\leq i\leq k-1$

$$H_i=q^\rho.\qquad(2.35)$$

(Remarquons que comme $\rho\in\mathbb{N}$, on a également $H_i\in\mathbb{N}$.) Dans l'objectif de majorer (2.34), concentrons-nous sur la quantité

$$S_9:=\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{0\leq h_1,\dots,h_{k-1}<q^\rho}|S_8|\leq\sum_{m=0}^{q^{\nu+1}}\sum_{0\leq h_1,\dots,h_{k-1}<q^\rho}|S_8|.$$

Pour $\gamma>0$ fixé (choisi plus tard), définissons

$$B:=\{m\in\{0,\dots,q^{\nu+1}\}\ :\ \exists p|q,\ \exists i\in\{1,\dots,k-1\},\ \ p^{3\gamma}|\,\mathfrak{M}_i\}.\qquad(2.36)$$

Nous commençons par scinder la somme S_9 selon que $m\in B$ ou non.
▷ Pour $m\notin B$, nous remplaçons $h_i\mathfrak{M}i$ (pour $1\leq i<k$) par h_i' et comptons le nombre de répétitions à l'aide du lemme suivant :

Lemme 2.5.10. *Soient $\rho \geq \gamma > 0$ des entiers. Soit $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \geq 2$ et $M \in \mathbb{N}^*$ tel que pour tout $1 \leq i \leq r$, on ait $\alpha_i \geq 1$ et $p_i^\gamma \nmid M$. Alors, pour tout $0 \leq a < q^\rho$, on a :*

$$|\{h \in \{0, \dots, q^\rho - 1\} \,:\, hM \equiv a \pmod{q^\rho}\}| \leq q^\gamma.$$

Démonstration. Si $(M, q^\rho) \nmid a$, alors la congruence $hM \equiv a \pmod{q^\rho}$ n'a pas de solution h. Sinon, cette congruence équivaut à

$$h\frac{M}{(M,q^\rho)} \equiv \frac{a}{(M,q^\rho)} \pmod{\frac{q^\rho}{(M,q^\rho)}}.$$

Comme

$$\left(\frac{M}{(M,q^\rho)}, \frac{q^\rho}{(M,q^\rho)}\right) = 1,$$

le nombre de solutions $h \in \{0, \dots, q^\rho - 1\}$ est égal à (M, q^ρ). Or, puisque $p_i^\gamma \nmid M$ pour tout i, on a $v_{p_i}(M) < \gamma$, tandis que $v_{p_i}(q^\rho) \geq \rho$, donc $(M, q^\rho) \leq q^\gamma$. □

▷ Pour $m \in B$, nous majorons la somme à l'aide du Lemme 2.5.7. Prenons (voir la Section 8)

$$\nu + 1 \geq 3\gamma. \tag{2.37}$$

On obtient donc

$$S_9 \leq q^{3\gamma(k-1)} \sum_{m=0}^{q^{\nu+1}} \sum_{0 \leq h_1', \dots, h_{k-1}' < q^\rho} |S_{10}| + q^{\nu+1+k\rho-3\gamma\log_q(P^-(q))}, \tag{2.38}$$

où

$$S_{10} := \sum_{0 \leq n' < q^\rho} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^\rho\left(n' + \left\lfloor \frac{t}{T} + \frac{w_0 h_0 m}{q^{k\mu}} \right\rfloor + \sum_{1 \leq i \leq k-1} w_i h_i'\right)\right).$$

Nous souhaitons désormais simplifier les termes $\theta_{h_0,m} := \left\lfloor \frac{t}{T} + \frac{w_0 h_0 m}{q^{k\mu}} \right\rfloor$ lorsque $w_0 = 1$. Puisque s_q^ρ est q^ρ-périodique, il est naturel de scinder les sommes selon les paramètres h_0 et m en fonction des classes modulo q^ρ des $\theta_{h_0,m}$:

$$\sum_{m=0}^{q^{\nu+1}} |S_{10}| = \sum_{0 \leq m' < q^\rho} a(m') \left| \sum_{0 \leq n' < q^\rho} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1}) \in \{0,1\}^k} (-1)^{s_2(w)} s_q^\rho\left(n' + w_0 m' + \sum_{1 \leq i \leq k-1} w_i h_i'\right)\right)\right|,$$

avec

$$a(m') = \left| \left\{ m \in \{0, \dots, q^{\nu+1}\} \,:\, \lfloor t/T + h_0 m / q^{k\mu} \rfloor \equiv m' \pmod{q^\rho} \right\} \right|.$$

Observons ensuite que[1] pour tout $1 \leq h_0 \leq H_0$ on a

$$\left| \left\{ m \in \{0, \dots, q^{\nu+1}\} \,:\, \lfloor t/T + h_0 m / q^{k\mu} \rfloor \equiv m' \pmod{q^\rho} \right\} \right| \ll q^{\nu+1-\rho}.$$

1. Pour $h_0 \leq q^{k\mu}$ et $w_0 = 1$, l'ensemble des entiers $m \in \{0, \dots, q^{\nu+1}\}$ tels que $\lfloor t/T + h_0 m/q^{k\mu} \rfloor \equiv m' \pmod{q^\rho}$ est l'ensemble des $m \in \{0, \dots, q^{\nu+1}\}$ tels que $\lfloor t/T + h_0 m/q^{k\mu} \rfloor = m' + \alpha q^\rho$ pour un certain $\alpha \in \mathbb{Z}$. À $\alpha \in \mathbb{Z}$ fixé, le nombre de m satisfaisant $m' + \alpha q^\rho \leq t/T + h_0 m/q^{k\mu} < m' + \alpha q^\rho + 1$ est $\mathcal{O}(q^{k\mu}/h_0)$. De plus, de par les inégalités $m' + \alpha q^\rho \leq t/T + h_0 m/q^{k\mu}$ et $m \leq q^{\nu+1}$, on obtient $\alpha \ll h_0 q^{\nu+1}/q^{k\mu+\rho}$. Ainsi, on a $\ll q^{k\mu}/h_0 \times h_0 q^{\nu+1}/q^{k\mu+\rho} = q^{\nu+1-\rho}$ entiers $m \in \{0, \dots, q^{\nu+1}\}$ tels que $\lfloor t/T + w_0 h_0 m/q^{k\mu} \rfloor \equiv m' \pmod{q^\rho}$.

Ceci nous amène à

$$\sum_{m=0}^{q^{\nu+1}} |S_{10}| \ll q^{\nu+1-\rho} \sum_{0\le m'<q^\rho} \left| \sum_{0\le n'<q^\rho} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^\rho\left(n' + m' w_0 \sum_{1\le i\le k-1} w_i h_i'\right)\right)\right|.$$

En injectant cela dans (2.38), on obtient (en remplaçant m' par h_0)

$$S_9 \ll q^{3\gamma(k-1)+\nu+1-\rho} \sum_{0\le h_0,h_1,\dots,h_{k-1}<q^\rho} |S_{10}(h_0,\dots,h_k)| + q^{\nu+1+k\rho-3\gamma\log_q(P^-(q))}, \quad (2.39)$$

avec

$$S_{10}(h_0,\dots,h_{k-1}) = \sum_{0\le n'<q^\rho} \mathrm{e}\left(\frac{\ell}{b} \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^\rho\left(n' + \sum_{0\le i\le k} w_i h_i\right)\right).$$

Choisissons

$$H_0 \le q^{k\mu}. \quad (2.40)$$

Nous avons réécrit h_i au lieu de h_i' par souci de clarté. Nous souhaitons maintenant supprimer les valeurs absolues autour de S_{10}. À cette fin, nous allons utiliser le résultat suivant.

Lemme 2.5.11. *On a*

$$\left|S_{10}(h_0,h_1,\dots,h_{k-1})\right|^2 = \sum_{0\le h_k<q^\rho} S_{10}(h_0,h_1,\dots,h_{k-1},h_k).$$

Démonstration. Pour $n' \in \{0,\dots,q^\rho-1\}$, on définit $g(n')$ par

$$g(n') = \sum_{\mathbf{w}=(w_0,\dots,w_{k-1})\in\{0,1\}^k} (-1)^{s_2(w)} s_q^\rho\left(n' + \sum_{0\le i\le k-1} w_i h_i\right).$$

$$\begin{aligned}\left|S_{10}(h_0,\dots,h_{k-1})\right|^2 &= S_{10}(h_0,\dots,h_{k-1})\overline{S_{10}(h_0,\dots,h_{k-1})} \\ &= \sum_{0\le n_1<q^\rho} \sum_{0\le n_2<q^\rho} \mathrm{e}\left(\frac{\ell}{b}(g(n_1)-g(n_2))\right).\end{aligned}$$

Pour $n_1 \in \{0,\dots,q^\rho-1\}$, on effectue la transformation linéaire $h_k = n_2 - n_1$ dans la seconde somme. De ce fait, on a

$$|S_{10}(h_0,\dots,h_{k-1})|^2 = \sum_{0\le n_1<q^\rho} \sum_{-n_1\le h_k<q^\rho-n_1} \mathrm{e}\left(\frac{\ell}{b}(g(n_1)-g(n_1+h_k))\right).$$

Pour $n_1 \in \{0,\dots,q^\rho-1\}$, la fonction $h_k \mapsto \mathrm{e}\left(\frac{\ell}{b}(g(n_1)-g(n_1+h_k))\right)$ est q^ρ-périodique, car g est q^ρ-périodique. De plus, le support de la somme sur h_k a comme longueur q^ρ. On en déduit que

$$\sum_{-n_1\le h_k<q^\rho-n_1} \mathrm{e}\left(\frac{\ell}{b}(g(n_1)-g(n_1+h_k))\right) = \sum_{0\le h_k<q^\rho} \mathrm{e}\left(\frac{\ell}{b}(g(n_1)-g(n_1+h_k))\right).$$

Ainsi, en intervertissant les deux sommes, on a

$$\begin{aligned}|S_{10}(h_0,\dots,h_{k-1})|^2 &= \sum_{0\le h_k<q^\rho}\sum_{0\le n_1<q^\rho} \mathrm{e}\left(\frac{\ell}{b}(g(n_1)-g(n_1+h_k))\right)\\ &= \sum_{0\le h_k<q^\rho}\sum_{0\le n_1<q^\rho}\\ &\qquad \times \mathrm{e}\left(\frac{\ell}{b}\sum_{\mathbf{w}=(w_0,\dots,w_k)\in\{0,1\}^{k+1}}(-1)^{s_2(w)}s_q^\rho\left(n'+\sum_{1\le i\le k}w_ih_i\right)\right)\\ &= \sum_{0\le h_k<q^\rho} S_{10}(h_0,\dots,h_{k-1},h_k).\end{aligned}$$

□

Revenons à (2.39). D'après l'inégalité de Cauchy–Schwarz et le Lemme 2.5.11, il vient que

$$\begin{aligned}\sum_{0\le h_0,\dots,h_{k-1}<q^\rho}|S_{10}(h_0,\dots,h_{k-1})| &\le q^{k\rho/2}\left(\sum_{0\le h_0,\dots,h_{k-1}<q^\rho}|S_{10}(h_0,\dots,h_{k-1})|^2\right)^{1/2}\\ &\le q^{k\rho/2}\left(\sum_{0\le h_0,\dots,h_{k-1},h_k<q^\rho}S_{10}(h_0,\dots,h_{k-1},h_k)\right)^{1/2}.\end{aligned}$$

Ainsi, d'après le Théorème 1.2.5 (pour $k+1$ à la place de k), on obtient

$$\sum_{0\le h_1,\dots,h_{k-1}<q^\rho}|S_{10}(h_1,\dots,h_{k-1})| \le q^{k\rho/2}\times q^{((k+2)\rho-\eta_0\rho)/2} = q^{k\rho+\rho-\rho\eta_0/2}. \tag{2.41}$$

En résumé, nous obtenons finalement [2] :

$$\begin{aligned}S_9 &\le q^{3\gamma(k-1)+\nu+1-\rho}\sum_{0\le h_1,\dots,h_{k-1}<q^\rho}|S_{10}(h_1,\dots,h_{k-1})| + q^{\nu+1+k\rho-3\gamma\log_q(P^-(q))}\\ &\ll q^{3\gamma(k-1)+\nu+1+k\rho-\rho\eta_0/2} + q^{\nu+1+k\rho-3\gamma\log_q(P^-(q))}.\end{aligned}$$

Comme $H_i = q^\rho$ pour tout $1\le i\le k-1$ (cf. (2.35)), on a

$$\begin{aligned}&\frac{1}{H_0\cdots H_{k-1}q^{\nu+1+\rho}T}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{\substack{1\le h_0<H_0\\ 0\le h_i<H_i,\ 1\le i\le k-1}}\sum_{t\in\Lambda}|S_8|\\ &\qquad\le \frac{1}{H_0\cdots H_{k-1}q^{\nu+1+\rho}T}\sum_{1\le h_0<H_0}\sum_{t\in\Lambda}S_9\\ &\qquad\ll q^{3\gamma(k-1)-\rho\eta_0/2}+q^{-3\gamma\log_q(P^-(q))}.\end{aligned}$$

2. À l'aide du Théorème 1.2.5 et du Lemme 2.5.11, nous parvenons à compenser le terme $q^{3\gamma(k-1)}$ avec $q^{-\rho\eta_0/2}$. En effet, le Lemme 2.5.11 nous permet de supprimer la valeur absolue sans perdre la somme complète sur $\{0,\dots,q^\rho-1\}$, ce qui est nécessaire pour appliquer le Théorème 1.2.5.

Rappelons que (cf. Lemme 2.5.9)

$$\begin{aligned}\left|\frac{S_0(N,q^\nu,\xi)}{q^{\nu+1}N}\right|^{2^k} &\le 2^{k-1}(E_0+\cdots+E_{k-1})+\frac{2^{2^{k+2}-2}}{T}\\ &+\frac{2^{2^{k+2}-2}}{H_0\cdots H_{k-1}q^{\nu+1+\rho}T}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{\substack{1\le h_0<H_0\\ 1\le i\le k-1,\ 0\le h_i<H_i}}\sum_{t\in\Lambda}|S_8|\\ &+2^{2^{k+2}-2}\mathcal{O}\Bigg(\frac{T}{q^{\nu+1-\rho}}\sum_{m=q^\nu}^{q^{\nu+1}}D_N\left(\frac{m}{q^\lambda}\right)\\ &+\frac{1}{q^{\nu+1}}\sum_{m=q^\nu}^{q^{\nu+1}}\sum_{i=2}^{k-1}D_N\left(\frac{m}{q^{i\mu}}\right)+\frac{H_1+\cdots+H_{k-1}}{q^\sigma}\Bigg),\end{aligned}$$

où $D_N(\alpha)$ est la $N-$discrépance de $\alpha\in\mathbb{R}$ (Définition B.0.10). Jusqu'à la fin de la preuve, on suppose que

$$\nu+1\ge k\mu. \tag{2.42}$$

D'après la Proposition B.0.13 on a, pour tout $2\le i\le k-1$,

$$\begin{aligned}\sum_{m=q^\nu}^{q^{\nu+1}}D_N\left(\frac{m}{q^{i\mu}}\right)&\le q^{\nu+1-i\mu}\sum_{m=0}^{q^{i\mu}}D_N\left(\frac{m}{q^{i\mu}}\right)\\ &\ll q^{\nu+1-i\mu}\frac{N+q^{i\mu}}{N}(\log^+N)^2\\ &\ll q^{\nu+1}(\log^+N)^2\left(\frac{1}{N}+\frac{1}{q^{2\mu}}\right).\end{aligned}$$

De plus,

$$\sum_{m=q^\nu}^{q^{\nu+1}}D_N\left(\frac{m}{q^\lambda}\right)\le\sum_{m=0}^{q^\lambda}D_N\left(\frac{m}{q^\lambda}\right)\ll\frac{N+q^\lambda}{N}(\log^+N)^2=q^\lambda(\log^+N)^2\left(\frac{1}{N}+\frac{1}{q^\lambda}\right).$$

D'après (2.6), on a $\lambda>\nu+1$. Finalement, en utilisant (2.7), (2.17) et (2.35), on a

$$\begin{aligned}\left|\frac{S_0(N,q^\nu,\xi)}{q^{\nu+1}N}\right|^{2^k}&\ll 2^k\left(\frac{1}{H_0}+\frac{H_0}{q^{\lambda-\nu}}+\frac{H_0}{N}+k2^{2^{k+1}}\frac{q^{\rho+2\mu+3\sigma}}{N}\right)+\frac{2^{2^{k+2}}}{T}\\ &+2^{2^{k+2}}(q^{-3\gamma\log_q P^-(q)}+q^{3\gamma(k-1)-\eta_0\rho/2})\\ &+2^{2^{k+2}}\left(Tq^{\lambda-\nu-1+\rho}(\log^+N)^2\left(\frac{1}{N}+\frac{1}{q^{2\mu}}\right)+\frac{k}{q^{\sigma-\rho}}\right).\end{aligned}\tag{2.43}$$

Il reste à choisir les paramètres introduits dans la preuve afin d'obtenir le Théorème 2.3.3 à partir de (2.43). Comme le principe de convexité appliqué à H_0 (voir [[GK91], Lemma 2.4] pour plus de détails) dans (2.43) conduit à des résultats similaires à ceux de [Spi20, p.2581], nous suivons le choix de Spiegelhofer.

Afin de définir μ, rappelons que, d'après l'hypothèse (voir le début de Section 5), nous avons

$$N^{\rho_1}<q^\nu\le qN^{\rho_2}. \tag{2.44}$$

Posons $k = 3(\lfloor \rho_2 \rfloor + 1) \geq 3$ et définissons

$$\mu = \Big\lfloor \frac{\nu - 1}{k + 1/8} \Big\rfloor.$$

Observons que $\mu \leq \nu/k$ (de ce fait, ce choix respecte (2.42)). De plus, posons

$$\sigma = \Big\lfloor \frac{\mu}{4} \Big\rfloor, \qquad \tilde{\rho} = \nu - k\mu. \tag{2.45}$$

À l'aide de la définition de $\tilde{\rho}$, on pose

$$\gamma = \Big\lfloor \frac{\eta_0 \tilde{\rho}}{12(k-1)} \Big\rfloor. \tag{2.46}$$

Ainsi, avec la définition de γ, on définit

$$T = q^{\gamma}, \qquad H_0 = \lfloor q^{\gamma/4} \rfloor.$$

Avec cette définition de H_0, la condition (2.40) est satisfaite pour γ suffisamment grand (nous renvoyons le lecteur au Corollaire 2.8.2). De plus, nous posons

$$\lambda = \nu + \Big\lfloor \frac{\gamma}{2} \Big\rfloor.$$

La condition (2.6) est satisfaite, car $\gamma \to +\infty$. On rappelle une fois de plus que

$$\rho = \lambda - k\mu. \tag{2.47}$$

Le lecteur trouvera dans la Section 8 les calculs, quelque peu fastidieux, menant à l'estimation suivante :

$$\Big| \frac{S_0(N, q^{\nu}, \xi)}{q^{\nu+1} N} \Big|^{2^k} \ll N^{-\frac{\rho_1 \eta_0}{(384k+48)(k-1)}} + N^{-\frac{3\eta_0 \log_q P^-(q)}{(k-1)(96k+12)} \rho_1}. \tag{2.48}$$

En remarquant que $384k + 48 = 4 \times (96k + 12)$, on conclut que

$$\frac{S_0(N, q^{\nu}, \xi)}{q^{\nu+1} N} \ll N^{-\eta_1},$$

où

$$\eta_1 = \frac{\rho_1 \eta_0 \min\left(1/4, 3 \log_q \left(P^-(q)\right)\right)}{2^k (k-1)(96k+12)}. \tag{2.49}$$

► Majorons η_0 fourni par le Théorème 1.2.5 (rappelons qu'on a appliqué ce théorème pour $k+1$ à la place de k). En utilisant le fait que

$$k + 1 = 3\left(\lfloor \rho_2 \rfloor + 1\right) + 1 \leq 3\rho_2 + 4,$$

On a

$$K = \Big\lfloor \frac{\log(k+1)}{\log(q)} \Big\rfloor + 1 \leq \frac{\log((3\rho_2 + 4)q)}{\log(q)}.$$

Ainsi, on obtient

$$\begin{aligned} K + (k+2)b &\leq \frac{\log((3\rho_2 + 4)q)}{\log(q)} + b(3\rho_2 + 5) \\ &\leq \frac{\log((3\rho_2 + 4)q) + b\log(q)(3\rho_2 + 5)}{\log(q)}. \end{aligned}$$

On peut donc majorer η_0 par

$$\begin{aligned}\eta_0 &= \frac{1}{\log(q)(K+(k+2)b)q^{(k+2)(K+(k+2)b)}}\\ &\geq \frac{\exp\left(-(3\rho_2+5)\left(\log((3\rho_2+4)q)+b\log(q)(3\rho_2+5)\right)\right)}{\log((3\rho_2+4)q)+b\log(q)(3\rho_2+5)}.\end{aligned}$$

En injectant toutes ces inégalités dans (2.49), on obtient

$$\begin{aligned}\eta_1 &\geq \frac{\rho_1\eta_0\min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{8^{1+\rho_2}(288\rho_2+300)(3\rho_2+2)}\\ &\geq \frac{\rho_1\min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{8^{1+\rho_2}(288\rho_2+300)(3\rho_2+2)\left(\log((3\rho_2+4)q)+b\log(q)(3\rho_2+5)\right)}\\ &\quad\times\exp\left(-(3\rho_2+5)\left(\log((3\rho_2+4)q)+(3\rho_2+5)b\log(q)\right)\right)\\ &= \eta(\rho_1,\rho_2).\end{aligned}$$

Ceci termine la preuve du Théorème 2.3.5.

2.6. Preuve du Théorème 2.3.3

Soient $0<\delta_1\leq\delta_2<1$ deux nombres réels et $0<\varepsilon_1,\varepsilon_2<1$. Soit D un entier tel que $x^{\delta_1}\leq D\leq x^{\delta_2}$ et $r\in\{0,\dots,m-1\}$. Soient y,z deux nombres réels tels que $0\leq y<z$ et $z-y\leq x$. Définissons,

$$N_{y,z}(a,b;r,m)=\Big|\{y\leq n<z\ :\ n\equiv r\ (\mathrm{mod}\ m),\quad s_q(n)\equiv a\ (\mathrm{mod}\ b)\}\Big|. \tag{2.50}$$

On a

$$N_{y,z}(a,b;r,m)-\frac{z-y}{bm}=\sum_{\substack{y\leq n<z,\\ n\equiv r\ (\mathrm{mod}\ m)}}\mathbb{1}_{b\mathbb{Z}}(s_q(n)-a)-\frac{z-y}{bm}.$$

En écrivant $n=r+km$ et en détectant la congruence portant sur la somme des chiffres à l'aide d'une somme d'exponentielles, on a

$$\begin{aligned}N_{y,z}(a,b;r,m)-\frac{z-y}{bm}&=\sum_{\frac{y-r}{m}\leq k<\frac{z-r}{m}}\mathbb{1}_{b\mathbb{Z}}(s_q(r+km)-a)-\frac{z-y}{bm}\\ &=\frac{1}{b}\sum_{\ell=1}^{b-1}\sum_{\frac{y-r}{m}\leq k<\frac{z-r}{m}}\mathrm{e}\left(\frac{\ell}{b}(s_q(r+km)-a)\right)+\mathcal{O}(1).\end{aligned} \tag{2.51}$$

À l'aide du changement de variable

$$k'=k-\left\lfloor\frac{y-r}{m}\right\rfloor,$$

on obtient

$$N_{y,z}(a,b;r,m)-\frac{z-y}{bm}=\frac{1}{b}\sum_{\ell=1}^{b-1}\sum_{0\leq k<\frac{z-y}{m}}\mathrm{e}\left(\frac{\ell}{b}\left(s_q\left(r+m\left\lfloor\frac{y-r}{m}\right\rfloor+km\right)-a\right)\right)+\mathcal{O}(1).$$

En prenant les valeurs absolues et en appliquant l'inégalité triangulaire, on obtient

$$\Big|N_{y,z}(a,b;r,m)-\frac{z-y}{bm}\Big| \le \frac{1}{b}\sum_{\ell=1}^{b-1}\Big|\sum_{k\le\frac{z-y}{m}} \mathrm{e}\left(\frac{\ell}{b}\left(s_q\left(r+m\Big\lfloor\frac{y-r}{m}\Big\rfloor+km\right)-a\right)\right)\Big|+\mathcal{O}(1)$$
$$\le \frac{1}{b}\sum_{\ell=1}^{b-1}\max_{u\le x}\max_{r'\ge 0}\Big|\sum_{k\le\frac{u}{m}}\mathrm{e}\left(\frac{\ell}{b}s_q(r'+km)\right)\Big|+\mathcal{O}(1).$$

De ce fait, en prenant le maximum sur r, on en déduit que

$$\max_{r\ge 0}\Big|N_{y,z}(a,b;r,m)-\frac{z-y}{bm}\Big| \le \frac{1}{b}\sum_{\ell=1}^{b-1}\max_{u\le x}\max_{r\ge 0}\Big|\sum_{k\le\frac{u}{m}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\Big|+\mathcal{O}(1).$$

En prenant également le maximum sur y,z et en sommant sur $m\in\{D+1,\dots,qD\}$, on a

$$\sum_{D<m\le qD}\max_{\substack{y,z\\0\le y<z\\z-y\le x}}\max_{r\ge 0}\Big|N_{y,z}(a,b;r,m)-\frac{z-y}{bm}\Big| \le \frac{1}{b}\sum_{\ell=1}^{b-1}\sum_{D<m\le qD}$$
$$\times\max_{u\le x}\max_{r\ge 0}\Big|\sum_{k\le\frac{u}{m}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\Big|+\mathcal{O}(D). \quad (2.52)$$

Pour $D<m\le qD$, on applique le lemme suivant (avec $y=u/m$ et $z=x/D$).

Lemme 2.6.1. *Soient $0\le y\le z$ des réels et $(a_n)_{n\in\mathbb{N}}\in\mathbb{C}^{\mathbb{N}}$ une suite définie pour $0\le n<z$. Alors,*

$$\Big|\sum_{0\le n<y}a_n\Big| \le \int_0^1 \min(y+1,\|\xi\|^{-1})\Big|\sum_{0\le n<z}a_n\mathrm{e}(n\xi)\Big|d\xi.$$

Démonstration. Nous renvoyons le lecteur à **[MS17,** Lemma 3.7**]**. □

On obtient alors

$$\Big|\sum_{k\le\frac{u}{m}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\Big| \le \int_0^1 \min\left(\frac{u}{m}+1,\|\xi\|^{-1}\right)\Big|\sum_{k\le\frac{x}{D}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\mathrm{e}(n\xi)\Big|d\xi.$$

L'inégalité

$$\min\left(\frac{u}{m}+1,\|\xi\|^{-1}\right)\le\min\left(\frac{x}{D}+1,\|\xi\|^{-1}\right)$$

nous permet d'écrire

$$\max_{u\le x}\Big|\sum_{k\le\frac{u}{m}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\Big| \le \int_0^1 \min\left(\frac{x}{D}+1,\|\xi\|^{-1}\right)\Big|\sum_{k\le\frac{x}{D}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\mathrm{e}(n\xi)\Big|d\xi.$$

En injectant ceci dans (2.52), on en déduit que

$$\sum_{D<m\le qD}\max_{\substack{y,z\\0\le y<z\\z-y\le x}}\max_{r\ge 0}\Big|N_{y,z}(a,b;r,m)-\frac{z-y}{bm}\Big|$$
$$\le\frac{1}{b}\sum_{1\le\ell<b}\int_0^1\min\left(\frac{x}{D}+1,\|\xi\|^{-1}\right)$$
$$\times\sum_{D<m\le qD}\max_{r\ge 0}\Big|\sum_{k\le\frac{x}{D}}\mathrm{e}\left(\frac{\ell}{b}s_q(r+km)\right)\mathrm{e}(n\xi)\Big|d\xi+\mathcal{O}(D).$$

D'après le Théorème 2.3.5, avec $\rho_1 = \dfrac{\delta_1}{1-\delta_1}$ et $\rho_2 = \dfrac{\delta_2}{1-\delta_2}$ il existe $C = C(\eta) > 0$ tel que

$$\sum_{D<m\leq qD} \max_{r\geq 0} \left| \sum_{k\leq \frac{x}{D}} \mathrm{e}\left(\frac{\ell}{b} s_q(r+km)\right) \mathrm{e}(n\xi) \right| \leq CD\left(\frac{x}{D}\right)^{1-\eta},$$

avec $\eta = \eta(\rho_1, \rho_2)$ défini dans le Théorème 2.3.5. Il vient que

$$\sum_{D<m\leq qD} \max_{\substack{y,z \\ 0\leq y<z \\ z-y\leq x}} \max_{r\geq 0} \left| N_{y,z}(a,b;r,m) - \frac{z-y}{bm} \right| \leq$$

$$CD\left(\frac{x}{D}\right)^{1-\eta} \int_0^1 \min\left(\frac{x}{D}+1, \|\xi\|^{-1}\right) d\xi + \mathcal{O}(D).$$

Comme $D \leq x^{\delta_2} < x$, on a $x/D > 1$. De plus, l'inégalité

$$\int_0^1 \min\left(A, \|\xi\|^{-1}\right) d\xi \ll \log(A),$$

assure l'existence de $C_1 = C_1(\rho_1, \rho_2) > 0$ tel que

$$\sum_{D<m\leq qD} \max_{\substack{y,z \\ 0\leq y<z \\ z-y\leq x}} \max_{r\geq 0} \left| N_{y,z}(a,b;r,m) - \frac{z-y}{bm} \right| \leq C_1 D\left(\frac{x}{D}\right)^{1-\eta} \log\left(\frac{x}{D}\right) + \mathcal{O}(D). \quad (2.53)$$

De plus, par hypothèse, on a

$$x^{\delta_1} \leq D \leq x^{\delta_2}.$$

En injectant cela dans (2.53), on a pour tout $0 < \varepsilon_2 < 1$,

$$\begin{aligned}
\sum_{D<m\leq qD} \max_{\substack{y,z \\ 0\leq y<z \\ z-y\leq x}} \max_{r\geq 0} \left| N_{y,z}(a,b;r,m) - \frac{z-y}{bm} \right| &= C_1 D^{\eta} x^{1-\eta}(\log(x) - \log(D)) + \mathcal{O}(D) \\
&\leq C_1 x^{\delta_2\eta} x^{1-\eta}(1-\delta_1)\log(x) + \mathcal{O}(D) \\
&\leq C_2 x^{1-(1-\delta_2)\eta/(1+\varepsilon_2)} + \mathcal{O}(D) \\
&\leq C_3 x^{1-(1-\delta_2)\eta/(1+\varepsilon_2)},
\end{aligned}$$

étant donné que $D \leq x^{\delta_2}$ et $1-(1-\delta_2)\eta/(1+\varepsilon_2) \geq 1-(1-\delta_2) = \delta_2$, car δ_2 et $\eta/(1+\varepsilon_2)$ sont < 1.
Afin de conclure la preuve du Théorème 2.3.3, nous allons minorer l'expression $\frac{(1-\delta_2)\eta}{1+\varepsilon_2}$. Nous utilisons tout d'abord la valeur explicite de $\eta = \eta(\rho_1, \rho_2)$,

$$\begin{aligned}
\eta = &\frac{\rho_1 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{8^{1+\rho_2}(288\rho_2+300)(3\rho_2+2)\left(\log((3\rho_2+4)q) + b\log(q)(3\rho_2+5)\right)} \\
&\times \exp\left(-(3\rho_2+5)\left(\log((3\rho_2+4)q) + (3\rho_2+5)b\log(q)\right)\right).
\end{aligned}$$

Rappelons que $\rho_1 = \dfrac{\delta_1}{1-\delta_1}$ et $\rho_2 = \dfrac{\delta_2}{1-\delta_2}$. On a

$$\begin{aligned}
\frac{(1-\delta_2)\eta}{1+\varepsilon_2} = &\frac{\delta_1(1-\delta_2)^2 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{(1-\delta_1)8^{(1-\delta_2)^{-1}}(300-12\delta_2)(2+\delta_2)(1+\varepsilon_2)} \\
&\times \frac{\exp\left(-\dfrac{5-2\delta_2}{1-\delta_2}\left(\log(q(4-\delta_2)(1-\delta_2)^{-1}) + \dfrac{5-2\delta_2}{1-\delta_2} b\log(q)\right)\right)}{\log((4-\delta_2)q/(1-\delta_2)) + b\log(q)(5-2\delta_2)/(1-\delta_2)}.
\end{aligned}$$

Remarquons que $1-\delta_1 \leq 1$, $300-12\delta_2 \leq 300$, $2+\delta_2 \leq 3$, $4-\delta_2 \leq 4$, $5-2\delta_2 \leq 5$ et $1+\varepsilon_2 \leq 2$. Afin de simplifier l'expression, nous supprimons également la dépendance en δ_2 au numérateur des fractions apparaissant dans l'exponentielle, au prix d'une minoration légèrement moins précise :

$$\begin{aligned}\frac{(1-\delta_2)\eta}{1+\varepsilon_2} &\geq \frac{\delta_1(1-\delta_2)^2 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{1800\times 8^{(1-\delta_2)^{-1}}\left(\log(4q/(1-\delta_2))+5b\log(q)/(1-\delta_2)\right)} \\ &\quad\times \exp\left(-\frac{5}{1-\delta_2}\left(\log(4q(1-\delta_2)^{-1})+\frac{5b\log(q)}{1-\delta_2}\right)\right) \\ &=: \eta(\delta_1,\delta_2),\end{aligned}$$

comme annoncé. Ceci termine la preuve du Théorème 2.3.3.

2.7. Preuve du Théorème 2.3.1

Soit $0<\varepsilon<1$. Posons $\delta_2 = 1-\varepsilon$ et $\delta_1 = \dfrac{\varepsilon}{2}$ (notons que la condition $\delta_1 \leq \delta_2$ implique $\varepsilon \leq 2/3$). Pour $m \in [1, x^{1-\varepsilon}] \cap \mathbb{N}$, on pose

$$E(m) = \max_{\substack{y,z \\ 0\leq y<z \\ z-y\leq x}} \max_{r\geq 0} \left| N_{y,z}(a,b;r,m) - \frac{z-y}{bm}\right|.$$

Rappelons le théorème de Gelfond.

Théorème 2.7.1 (Gelfond, 1967/68)**.** *Soient $b,m,q \geq 2$ des entiers tels que $(b,q-1)=1$. Alors, pour tout $a \in \{0,\dots,b-1\}$ et pour tout $r \in \{0,\dots,m-1\}$, on a*

$$|\{n<N \,:\, s_q(n)\equiv a \pmod b,\ n\equiv r \pmod m\}| = \frac{N}{bm} + \mathcal{O}(N^\lambda),$$

avec

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

La constante implicite dans le $\mathcal{O}$ est indépendante de a,b,m,r.

On sépare en deux sommes selon la position de m par rapport à x^{δ_1}

$$\sum_{1\leq m\leq x^{1-\varepsilon}} E(m) = \sum_{1\leq m<x^{\delta_1}} E(m) + \sum_{x^{\delta_1}\leq m\leq x^{\delta_2}} E(m).$$

D'après le Théorème 2.7.1 on a pour y,z tels que $0\leq y<z$ et $z-y\leq x$,

$$\begin{aligned}N_{y,z}(a,b;r,m) &:= \left|\left\{y\leq n<z \,:\, n\equiv r \pmod m,\quad s_q(n)\equiv a \pmod b\right\}\right| \\ &= \frac{z-y}{bm} + \mathcal{O}\left((z-y)^\lambda\right).\end{aligned}$$

Comme $z-y\leq x$, on a

$$N_{y,z}(a,b;r,m) - \frac{z-y}{bm} = \mathcal{O}\left(x^\lambda\right),$$

où la constante implicite ne dépend pas de m. On en déduit que

$$\sum_{1\leq m<x^{\delta_1}} E(m) = \mathcal{O}(x^{\delta_1+\lambda}).$$

Concernant la seconde somme, on effectue un découpage q-adique

$$[x^{\delta_1}, x^{\delta_2}] \subset \biguplus_{\alpha=A_1}^{A_2} [q^\alpha, q^{\alpha+1}],$$

où

$$A_1 = \left\lfloor \frac{\delta_1 \log(x)}{\log(q)} \right\rfloor, \qquad A_2 = \left\lfloor \frac{\delta_2 \log(x)}{\log(q)} \right\rfloor - 1.$$

Donc

$$\sum_{x^{\delta_1} \le m \le x^{\delta_2}} E(m) \le \sum_{\alpha=A_1}^{A_2} \sum_{q^\alpha \le m \le q^{\alpha+1}} E(m).$$

De plus, pour $\alpha \in \{A_1, \dots, A_2\}$, et pour x suffisament grand, on a

$$x^{\delta_1/2} \le q^\alpha \le x^{\delta_2}.$$

Le Théorème 2.3.3 est appliquable pour $D = q^\alpha$, avec $\delta_1/2$ et δ_2 à la place de δ_1 et δ_2,

$$\sum_{1 \le m \le x^{1-\varepsilon}} E(m) = \sum_{1 \le m < x^{\delta_1}} E(m) + \sum_{x^{\delta_1} \le m \le x^{\delta_2}} E(m) \le \mathcal{O}\left(x^{\delta_1+\lambda}\right) + C x^{1-\frac{\eta}{1+\varepsilon_3}}, \quad (2.54)$$

pour tout $0 < \varepsilon_3 < 1$ et pour $\eta = \eta(\delta_1, \delta_2)$ définis dans le Théorème 2.3.3. Rappelons $\delta_2 = 1 - \varepsilon$ que $\delta_1 = \varepsilon/2$. On a, avec (2.4),

$$\begin{aligned} \frac{\eta}{1+\varepsilon_3} &:= \frac{(\delta_1/2)(1-\delta_2)^2 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{1800 \times 8^{(1-\delta_2)^{-1}} \left(\log(4q/(1-\delta_2)) + 5b\log(q)/(1-\delta_2)\right)(1+\varepsilon_3)} \\ &\quad \times \exp\left(-\frac{5}{1-\delta_2}\left(\log(4q(1-\delta_2)^{-1}) + \frac{5b\log(q)}{1-\delta_2}\right)\right) \\ &= \frac{\varepsilon^3 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{3600 \times 8^{1/\varepsilon}\left(\log(4q/\varepsilon) + 5b\log(q)/\varepsilon\right)(1+\varepsilon_3)} \\ &\quad \times \exp\left(-\frac{5}{\varepsilon}\left(\log(4q/\varepsilon) + \frac{5b\log(q)}{\varepsilon}\right)\right). \end{aligned} \quad (2.55)$$

En particulier, $\dfrac{\eta}{1+\varepsilon_3} \le \varepsilon$. En effet, comme $0 < \varepsilon < 1$, on a $\log(4q/\varepsilon) > 0$ et $5b\log(q)/\varepsilon > 5b\log(q) > 1$. Ainsi,

$$3600 \times 8^{1/\varepsilon}(\log(4q/\varepsilon) + 5b\log(q)/\varepsilon) > 1$$

et $\varepsilon^3 < \varepsilon$. De ce fait,

$$\frac{\eta}{1+\varepsilon_3} \le \varepsilon.$$

Désormais, concentrons-nous sur les deux exposants qui appraissent dans (2.54). On écrit

$$\delta_1 + \lambda - \left(1 - \frac{\eta}{1+\varepsilon_3}\right) \le \frac{\varepsilon}{2} + \lambda - 1 + \varepsilon.$$

Pour $\varepsilon < \dfrac{2}{3}(1-\lambda)$, la dernière quantité est négative. Il existe donc $C' > 0$ tel que

$$\sum_{1 \le m \le x^{1-\varepsilon}} E(m) \le C' x^{1-\frac{\eta}{1+\varepsilon_3}}.$$

Pour obtenir la valeur de η annoncée dans le Théorème 2.3.1, nous utilisons l'équation (2.55) ainsi que le fait que $1+\varepsilon_3 \leq 2$.
Finalement

$$\frac{\eta}{1+\varepsilon_3} \geq \frac{\varepsilon^3 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{7200 \times 8^{1/\varepsilon}\left(\log(4q/\varepsilon)+5b\log(q)/\varepsilon\right)} \times \exp\left(-\frac{5}{\varepsilon}\left(\log(4q/\varepsilon)+\frac{5b\log(q)}{\varepsilon}\right)\right)$$

et nous pouvons donc prendre

$$\eta(\varepsilon) = \frac{\varepsilon^3 \min\left(1/4, 3\log_q\left(P^-(q)\right)\right)}{7200 \times 8^{1/\varepsilon}\left(\log(4q/\varepsilon)+5b\log(q)/\varepsilon\right)} \times \exp\left(-\frac{5}{\varepsilon}\left(\log(4q/\varepsilon)+\frac{5b\log(q)}{\varepsilon}\right)\right)$$

comme annoncé. Ceci clôture la preuve du Théorème 2.3.1.

Remarque 2.7.2. Un raisonnement alternatif afin de traiter la première somme de (2.54) serait d'utiliser un résultat en moyenne dans l'esprit du Théorème 2.2.1. Cependant, cela nécessite une généralisation du Théorème 2.2.1 à toute base q. Cela nous donnerait une autre condition sur ε, mais la valeur explicite de η ne serait pas modifiée.

2.8. Choix des paramètres

Commençons par dresser un inventaire de tous les paramètres utilisés tout au long de ce chapitre, ainsi que de leurs rôles et contraintes.

▶ Paramètres introduits au cours des itérations de l'inégalité de van der Corput

- ▷ $k \geq 3$ le nombre d'itérations de l'inégalité de van der Corput (Lemme 2.5.6),
- ▷ $H_0 \leq q^{k\mu}$ apparaissant dans la première itération de l'inégalité de van der Corput (Lemme 2.5.3). La majoration est donnée en (2.40),
- ▷ $\lambda > \nu + 1$ utilisé pour appliquer le lemme de propagation de retenues (2.6),
- ▷ $H_1 = \cdots = H_{k-1} = q^{\rho}$ apparaissant dans Sous-section 1 (voir (2.35)) ; nous discuterons de la taille des E_i et de (2.18) plus tard (voir (2.66)).

▶ Paramètres utilisés pour les décalages $K_1, \ldots, K_{k-1}$

- ▷ $\mu > 0$ tel que $\nu + 1 \geq k\mu$ (voir (2.42)),
- ▷ $\rho + 1 < \sigma < \mu$ (voir (2.31) et (2.8)).

▶ Paramètres introduits durant les nombreux décalages

- ▷ $\rho = \lambda - k\mu$ (voir (2.16)),
- ▷ $T \geq 2$ défini dans le Lemme 2.5.9,
- ▷ $0 < \gamma \leq \rho$ utilisé pour définir l'ensemble B (voir (2.36)).

Afin de définir μ, rappelons que, par hypothèse (voir le début de la Section 5), nous avons

$$N^{\rho_1} < q^{\nu} \leq qN^{\rho_2}. \tag{2.56}$$

On pose $k = 3(\lfloor \rho_2 \rfloor + 1) \geq 3$ et on pose

$$\mu = \left\lfloor \frac{\nu - 1}{k + 1/8} \right\rfloor.$$

Observons que $\mu \leq \nu/k$ (ainsi, ce choix respecte (2.42)). De plus, on pose

$$\sigma = \left\lfloor \frac{\mu}{4} \right\rfloor, \qquad \tilde{\rho} = \nu - k\mu. \tag{2.57}$$

De la définition de $\tilde{\rho}$, on pose

$$\gamma = \left\lfloor \frac{\eta_0 \tilde{\rho}}{12(k-1)} \right\rfloor. \tag{2.58}$$

Ainsi, on définit T à partir de γ par

$$T = q^{\gamma}, \qquad H_0 = \lfloor q^{\gamma/4} \rfloor.$$

De plus, on pose

$$\lambda = \nu + \left\lfloor \frac{\gamma}{2} \right\rfloor. \tag{2.59}$$

La condition (2.6) est satisfaite, étant donné que $\gamma \to +\infty$. On rappelle que

$$\rho = \lambda - k\mu. \tag{2.60}$$

Nous donnons d'abord quelques équivalents asymptotiques de nos paramètres, qui seront importants pour prouver que notre choix de paramètres est admissible. Puisque $\nu \to +\infty$, ces équivalents seront utiles pour déterminer le taux de convergence de chaque terme dans (2.43). Cela suffira pour conclure.

Lemme 2.8.1. *Pour $\mu \to +\infty$, nous avons les équivalents suivants :*

(1)

$$\tilde{\rho} \sim \frac{\mu}{8}, \tag{2.61}$$

(2)

$$\gamma \sim \frac{\eta_0 \mu}{96(k-1)}, \tag{2.62}$$

(3)

$$\rho \sim \frac{\mu}{8} + \frac{\eta_0 \mu}{192(k-1)}. \tag{2.63}$$

Démonstration. Pour (2.61), comme k est constant, on a

$$\tilde{\rho} = \nu - k\left\lfloor \frac{\nu - 1}{k + 1/8} \right\rfloor \sim \nu - k\frac{\nu - 1}{k + 1/8} \sim \frac{1}{8}\left(\frac{\nu - 1 + 1 + 8k}{k + 1/8}\right) \sim \frac{\mu}{8}.$$

Concernant (2.62), d'après la définition γ et (2.61) on a

$$\gamma \sim \frac{\eta_0 \tilde{\rho}}{12(k-1)} \sim \frac{\eta_0 \mu}{96(k-1)}.$$

Comme pour (2.63), nous utilisons (2.61), (2.62) ainsi que la définition (2.59) de λ, pour obtenir

$$\rho = \lambda - k\mu = \tilde{\rho} + \left\lfloor \frac{\gamma}{2} \right\rfloor \sim \frac{\mu}{8} + \frac{\eta_0 \mu}{192(k-1)}.$$

□

Comme $k \geq 3$ et $0 < \eta_0 < 1$, on a les inégalités :

Corollaire 2.8.2. *Pour μ suffisamment grand,*

$$\gamma \leq \mu/192 \quad \textit{et} \qquad \rho \leq \mu/8 + \mu/384.$$

On remarque tout d'abord que la condition (2.37) est satisfaite. En effet, d'après (2.57) et (2.58), nous avons

$$3\gamma \leq \frac{\tilde{\rho}}{8} < \frac{\nu}{8} < \nu + 1.$$

De plus, la condition (2.40) est satisfaite pour H_0 dès que μ est suffisamment grand. Afin de poursuivre la démonstration du Théorème 2.3.5, nous avons besoin de minorer N en fonction de q^μ.

Lemme 2.8.3. *On a les majorations suivantes pour N et q^μ :*

(1)

$$N \geq q^{3\mu}, \tag{2.64}$$

(2)

$$q^\mu \gg N^{\frac{\rho_1}{k+1/8}}, \tag{2.65}$$

avec une constante implicite ne dépendant que de k et q.

Démonstration. D'après (2.56) on a

$$N \geq q^{\frac{\nu-1}{\rho_2}} \geq q^{\frac{\nu-1}{\lfloor \rho_2 \rfloor + 1}} = q^{3\frac{\nu-1}{k}} \geq q^{3\mu},$$

ce qui prouve (2.64). En utilisant encore une fois (2.56), on a $N^{\rho_1} < q^\nu$ et

$$\frac{1}{q^{(k+1/8)^{-1}}} N^{\frac{\rho_1}{k+1/8}} < q^{\frac{\nu-1}{k+1/8}} < q^{\lfloor \frac{\nu-1}{k+1/8} \rfloor + 1} = q^{\mu+1}.$$

On conclut que

$$q^\mu > C N^{\frac{\rho_1}{k+1/8}},$$

avec $C = 1/(q^{(k+1/8)^{-1}+1})$. □

Après ce travail préliminaire, nous nous concentrons désormais sur la majoration de chacun des termes intervenants dans (2.43).

► Majoration de $\dfrac{1}{H_0}$.

Pour commencer, remarquons que

$$H_0 = \lfloor q^{\frac{\gamma}{4}} \rfloor \leq q^{\mu/768} \leq q^{3\mu} \leq N,$$

une condition imposée sur H_0 dans le Lemme 2.5.3. Désormais, on utilise (2.62) et (2.65),

$$\frac{1}{H_0} = \frac{1}{\lfloor q^{\gamma/4} \rfloor} \sim q^{-\gamma/4} \ll q^{-\frac{\eta_0 \mu}{384(k-1)}} \ll N^{\frac{-\rho_1 \eta_0}{(384k+48)(k-1)}}.$$

▶ Majoration de $\dfrac{H_0}{q^{\lambda-\nu}}$.

$$\frac{H_0}{q^{\lambda-\nu}} = \frac{\lfloor q^{\gamma/4} \rfloor}{q^{\lfloor \gamma/2 \rfloor}} \ll q^{-\gamma/4}.$$

On remarque que $\dfrac{1}{H_0}$ et $\dfrac{H_0}{q^{\lambda-\nu}}$ ont la même vitesse de convergence.

▶ Majoration de $\dfrac{H_0}{N}$.

Remarquons que $\dfrac{H_0}{N} < \dfrac{1}{H_0}$. En effet, d'après (2.64) on a

$$\frac{H_0}{N} \leq \frac{q^{\gamma/4}}{q^{3\mu}}.$$

En utilisant le fait que $\mu \geq 192\gamma$ (voir le Corollaire 2.8.2), on a

$$\frac{H_0}{N} \leq q^{\frac{-2303}{4}\gamma}.$$

Les estimations ci-dessus montrent que E_0, défini dans le Lemme 2.5.6, est inférieur à 1 pour ν suffisamment grand.

▶ Majoration de $\dfrac{q^{\rho+2\mu+3\sigma}}{N}$.

En utilisant (2.64) on a

$$\frac{q^{\rho+2\mu+3\sigma}}{N} \leq q^{\rho-\mu+3\sigma}.$$

De plus, d'après le Corollaire 2.8.2, on obtient, pour μ suffisamment grand

$$\rho - \mu + 3\sigma \leq \frac{-335\mu}{384} + 3\sigma.$$

Comme $\mu \geq 4\sigma$ (voir (2.57)), on trouve

$$\rho - \mu + 3\sigma \leq \frac{-47}{384}\mu.$$

L'inégalité (2.65) donne donc

$$\frac{q^{\rho+2\mu+3\sigma}}{N} \leq q^{-\frac{47}{384}\mu} \ll N^{-\frac{47\rho_1}{384k+48}}. \tag{2.66}$$

Cette estimation garantit également que $E_1, \ldots, E_{k-1}$ définis dans le Lemme 2.5.6 satisfont la condition (2.18) pour ν suffisamment grand.

▶ Majoration de $\dfrac{1}{T}$.

Comme précédemment, on utilise (2.62) et (2.65), et obtenons

$$\frac{1}{T}=\frac{1}{q^{\gamma}}\ll q^{-\frac{\eta_0}{96(k-1)}\mu}\ll N^{-\frac{\eta_0\rho_1}{96(k-1)(k+1/8)}}=N^{-\frac{\eta_0\rho_1}{(96k+12)(k-1)}}.$$

► Majoration de $q^{-3\gamma\log_q P^-(q)}$.

Une fois n'est pas coutume, on utilise (2.62) et (2.65) et on obtient

$$q^{-3\gamma\log_q P^-(q)}\ll q^{-\frac{3\eta_0\log_q P^-(q)}{96(k-1)}\mu}\ll N^{-\frac{3\eta_0\log_q P^-(q)}{(96k+12)(k-1)}\rho_1}.$$

► Majoration de $q^{3\gamma(k-1)-\eta_0/2\rho}$.

Majorons dans un premier temps l'exposant. Comme $\lambda>\nu$, on remarque que $\tilde{\rho}\leq\rho$ (see (2.57) et (2.60)). D'après la définition de γ on a

$$3\gamma(k-1)-\eta_0\rho/2\leq 3(k-1)\frac{\eta_0\rho}{12(k-1)}-\eta_0\rho/2=-\frac{\eta_0\rho}{4}.$$

On utilise (2.63) avec (2.65) afin d'obtenir

$$q^{3\gamma(k-1)-\eta_0\rho/2}\leq q^{-\frac{\eta_0\rho}{4}}\ll N^{-\frac{\eta_0}{4}\left(\frac{1}{8}+\frac{\eta_0}{192(k-1)}\right)\frac{\rho_1}{k+1/8}}\ll N^{-\frac{\eta_0\rho_1}{32(k+1/8)}}.$$

► Majoration de $Tq^{\lambda-\nu-1+\rho}(\log^+ N)^2\left(\frac{1}{N}+\frac{1}{q^{2\mu}}\right)$.

Puisque, d'après (2.64), on a $N\geq q^{2\mu}$, il nous suffit désormais d'estimer le terme

$$Tq^{\lambda-\nu-1+\rho-2\mu}(\log^+ N)^2.$$

Comme $T=q^{\gamma}$ on a

$$Tq^{\lambda-\nu-1+\rho-2\mu}(\log^+ N)^2\leq q^{\lambda-\nu+\rho+\gamma-2\mu}(\log^+ N)^2.$$

D'après le Corollaire (2.8.2) on a, pour μ suffisamment grand,

$$\begin{aligned}\lambda-\nu+\rho+\gamma-2\mu&=\left\lfloor\frac{\gamma}{2}\right\rfloor+\rho+\gamma-2\mu\\&\leq\frac{\mu}{384}+\frac{\mu}{8}+\frac{\mu}{384}+\frac{\mu}{192}-2\mu\\&\leq\frac{-179}{96}\mu.\end{aligned}$$

Ainsi

$$Tq^{\lambda-\nu-1+\rho-2\mu}(\log^+ N)^2\leq\frac{(\log N)^2}{q^{(179/96)\mu}}.$$

D'après l'inégalité (2.65) et comme $\log(N)\leq N^{1/4}$, on obtient

$$\begin{aligned}Tq^{\lambda-\nu-1+\rho-2\mu}(\log^+ N)^2&\ll(\log N)^2N^{-\frac{179\rho_1}{96k+12}}\\&\ll N^{-\frac{179\rho_1}{192k+24}}.\end{aligned}$$

► Majoration de $\frac{1}{q^{\sigma-\rho}}$.

On utilise $\sigma=\left\lfloor\frac{\mu}{4}\right\rfloor$ et le Corollaire (2.8.2). Cela conduit à

$$\frac{1}{q^{\sigma-\rho}}\leq\frac{1}{q^{\lfloor\mu/4\rfloor-\mu/8-\mu/384}}\ll q^{-(47/384)\mu}\ll N^{-\frac{47\rho_1}{384k+48}},$$

qui est la même majoration que (2.66).

Finalement, on collecte toutes nos majorations et revenons à (2.43). On a

$$\left|\frac{S_0(N,q^\nu,\xi)}{q^{\nu+1}N}\right|^{2^k} \ll N^{-\frac{\rho_1\eta_0}{(384k+48)(k-1)}} + N^{-\frac{47\rho_1}{384k+48}} + N^{-\frac{\rho_1\eta_0}{(96k+12)(k-1)}} + N^{-\frac{3\eta_0\log_q P^-(q)}{(96k+12)(k-1)}\rho_1} + N^{-\frac{\rho_1\eta_0}{32k+4}} + N^{-\frac{179\rho_1}{192k+24}}.$$

Par comparaison des différents termes, on a

$$\left|\frac{S_0(N,q^\nu,\xi)}{q^{\nu+1}N}\right|^{2^k} \ll N^{\frac{-\rho_1\eta_0}{(384k+48)(k-1)}} + N^{-\frac{3\eta_0\log_q P^-(q)}{(k-1)(96k+12)}\rho_1}.$$

Cette dernière inégalité est l'inégalité (2.48), comme annoncée.

2.9. Graphe de la fonction $\varepsilon \mapsto \log\eta(\varepsilon)$

Un programme simple écrit en Python permet de tracer le graphe de la quantité définie en (2.3), considérée comme une fonction de ε.

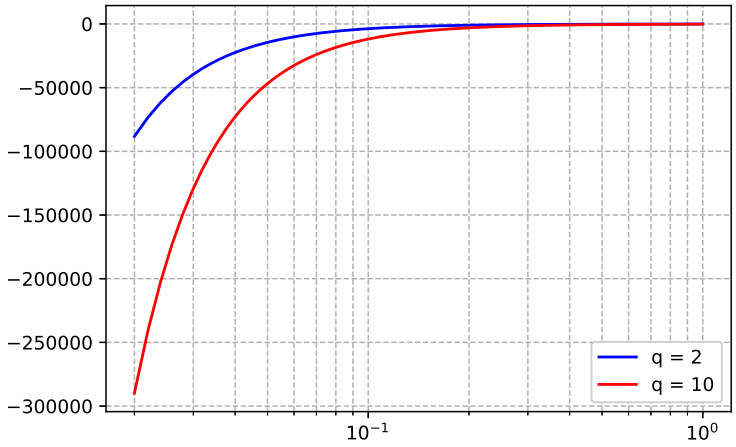


FIGURE 2.2 – Graphe de la fonction $\varepsilon \mapsto \log\eta(\varepsilon)$ dans $]0.02, 1[$ pour $b = q = 2$ en bleu et $b = 2$, $q = 10$ en rouge.

On remarque que $\eta(\varepsilon)$ devient extrêmement petit lorsque ε tend vers 0. De plus, on observe qu'il est assez difficile de calculer les valeurs de $\log\eta(\varepsilon)$ pour des très petites valeurs de ε. Cette complexité découle directement du comportement de η au voisinage de 0 (voir la Remarque 2.3.2).

Chapitre 3

Valeurs polynomiales sous contraintes digitales

1 Historique **83**
1 Facteurs premiers des valeurs polynomiales 83
2 Le cas général 85
3 Résultats principaux 87
2 Résultats auxiliaires **88**
3 Le plus grand facteur premier de n^2+1 sous contraintes digitales . . **90**
1 Définitions et notations spécifiques 91
2 Preuve du Théorème **3.1.13** 91
4 Valeurs polynomiales avec peu de facteurs premiers **99**
1 Définitions et premières propriétés 99
2 Preuve du Théorème **3.1.15** 100
5 Valeurs friables de F **103**
1 Cadre d'étude 103
2 Preuve du Théorème **3.1.16** 104

Ce chapitre s'intéresse à la répartition des valeurs polynomiales sous contraintes digitales. Ce travail fait l'objet de l'article **[Tou26+]** (soumis) dont l'introduction (pages 83 à 88) est légèrement modifiée afin d'ancrer ce chapitre dans la continuité de la thèse.

3.1. Historique

3.1.1. Facteurs premiers des valeurs polynomiales

Dirichlet prouva en 1838 que, pour deux entiers a, b premiers entre eux, il existe une infinité de nombres premiers de la forme $an+b$. Son élégante preuve utilise essentiellement les fonctions L de Dirichlet et on peut la retrouver dans le livre **[Ser78,** Chapter VI**]**. On sait donc que pour un polynôme $P = aX + b$ donné (avec a et b premiers entre eux), il existe une infinité de $n \in \mathbb{N}$ tels que $P(n) \in \mathbb{P}$, avec $\mathbb{P}$

désignant l'ensemble des nombres premiers.

Concernant les polynômes de degré 2

Qu'en est-il pour le polynôme $P = aX^2 + bX + c$, avec $a, b, c \in \mathbb{Z}$? Ce problème semble très ardu. En réalité, l'étude des valeurs premières du polynôme $P = X^2 + 1$ résiste encore aujourd'hui aux mathématiciens et mathématiciennes. En effet, on a la

Conjecture 3.1.1 (Landau, 1912)**.** Il existe une infinité de nombres premiers de la forme $n^2 + 1$.

Une première approche initiée par Tchebychev au XIXème siècle est de considérer le logarithme du produit

$$P(x) := \prod_{x \leq n \leq 2x} (n^2 + 1)$$

et de l'évaluer de deux manières distinctes (lorsque x tend vers $+\infty$). Tchebychev parvint à prouver le théorème suivant.

Théorème 3.1.2. *Soit $x > 0$. Notons $P^+\left(\prod_{n \leq x} (n^2+1)\right)$ le plus grand facteur premier de $\prod_{n \leq x} (n^2 + 1)$. Alors*

$$\frac{P^+\left(\prod_{n \leq x} (n^2+1)\right)}{x} \xrightarrow[x \to +\infty]{} +\infty.$$

Hooley **[Hoo67]** affina ce résultat en 1967 et montra que

$$P^+\left(\prod_{n \leq x} (n^2+1)\right) \gg x^{11/10}.$$

Autrement dit, il existe une infinité d'entiers n tels que le plus grand facteur premier de n^2+1 est plus grand que $n^{11/10}$. Ce résultat ne garantit pas l'infinitude de nombres premiers de la forme $(n^2 + 1)$ mais il s'agit d'un grand bond en avant qui permettra à Deshouillers et Iwaniec **[DI82]** (1982) d'améliorer l'exposant, le faisant passer de 1.1 à 1.202468.... Des améliorations ont été apportées depuis (voir **[DLBD20]**, **[Mer23]**). Le cœur de ces résultats repose sur les méthodes de crible, comme le crible de Selberg que Hooley utilise dans **[Hoo67]**. De nouvelles amélioriations ont été apportées en 2025. On peut citer les travaux de Pascadi **[Pas25]**, poussant la borne à 1.3 puis les travaux de Grimmelt et Merikoski **[GM25]** qui permettent d'atteindre la valeur 1.312. Contrairement aux travaux précédemment mentionnés dont les outils principaux sont les sommes de Kloosterman et les cribles, Grimmelt et Merikoski proposent une nouvelle approche via le calcul matriciel et les actions sur $SL_2(\mathbb{Z})$.

Concernant les polynômes de degré 3 **et** 4

Un des premiers résultats fondamentaux concernant le polynôme $F = X^3 + 2$ est celui de Hooley **[Hoo78]**. Ce résultat nécessite une hypothèse sur les sommes de Kloosterman courtes. Soient h, k, s des entiers, $s \neq 0$ et $\zeta_1, \zeta_2 \in \mathbb{R}$ tels que $0 \leq \zeta_2 - \zeta_1 \leq |r|$. Considérons l'hypothèse

$$\sum_{\substack{\zeta_1 \leq r \leq \zeta_2 \\ (s,r)=1}} \exp\left(\frac{2i\pi}{s}(h\bar{r} + kr)\right) \ll (1 - \zeta_2 - \zeta_1)^{1/2} s^{\varepsilon} (h, s)^{1/2}. \qquad (R^*)$$

Théorème 3.1.3 ([Hoo78]). *Supposons que R^* est vraie. Alors,*

$$P^+\left(\prod_{n\leq x}(n^3+2)\right) \gg x^{31/30}.$$

Heath-Brown [Hea01] obtint un premier résultat inconditionnel.

Théorème 3.1.4 ([Hea01], Theorem 1). *Soit $C = 10^{-303}$. Alors, pour x suffisamment grand, il existe une proportion positive d'entiers $n \in]x, 2x]$ tel que le plus grand facteur premier de n^3+2 soit supérieur à x^{1+C}.*

Améliorant une étape de [Hea01], Irving [Irv15] prouva que $P^+(n^3+2) > n^{1+10^{-52}}$ pour une infinité d'entiers n. Le douzième polynôme cyclotomique $\Phi_{12} := X^4 - X^2 + 1$ est un autre polynôme particulier, étudié dans un premier temps par Dartyge [Dar15].

Théorème 3.1.5 ([Dar15], Théorème 1.1, p.5). *Il existe $c > 0$ tel que pour X assez grand on ait la minoration :*

$$P^+\left(\prod_{X<n\leq 2X}\Phi_{12}(n)\right) \geq X^{1+c}.$$

La valeur $c = 10^{-26531}$ est admissible.

La Bretèche [Bre15] généralisa par la suite ce résultat, en montrant le théorème ci-après.

Théorème 3.1.6 ([Bre15], Théorème 1.2, p.1). *Soit F un polynôme à coefficients entiers, irréductible sur $\mathbb{Q}$, pair, unitaire de degré 4 dont le groupe de Galois associé est isomorphe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Il existe une constante $c_F > 0$ telle que, lorsque X tend vers l'infini, l'ensemble des entiers $n \leq X$ tels que*

$$P^+(F(n)) \geq X^{1+c_F}$$

est de densité strictement positive.

Concernant d'autres groupes de Galois, Dartyge et Maynard [DM25] prouvèrent le résultat suivant.

Théorème 3.1.7 ([DM25], Theorem 1.1, p.3). *Soit F un polynôme irréductible unitaire de degré 4 de groupe de Galois isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou isomorphe à $\mathbb{Z}/2\mathbb{Z}\ltimes\mathbb{Z}/4\mathbb{Z}$. Il existe $c = c_F > 0$ et $x_0 = x_0(F) > 0$ tel que pour tout $x > x_0$ on a*

$$|\{x \leq n \leq 2x \ : \ P^+(F(n)) \geq x^{1+c}\}| \gg x.$$

3.1.2. Le cas général

De nombreux résultats concernant le plus grand facteur premier de $F(n)$ (avec F un polynôme irréductible de degré $k \geq 2$) existent comme par exemple celui de Nagell [Nag21] en 1921.

Théorème 3.1.8 ([Nag21], p.344). *Soit F un polynôme irréductible de $\mathbb{Z}[X]$ de degré $k \geq 2$ sans diviseur fixe. Soit $\theta \in [0, 1[$. On a la minoration*

$$P^+\left(\prod_{n\leq x}F(n)\right) \gg_{F,\theta} x(\log x)^\theta.$$

Ce résultat fut amélioré en 1952 par Erdős **[Erd52]**. Il montra en effet que, sous les mêmes hypothèses, il existe $A > 0$ tel que

$$P^+\left(\prod_{n\leq x} F(n)\right) \gg_F x(\log x)^{A\log\log\log x}.$$

Le membre de droite sera amélioré en 1990 par Erdős et Schinzel **[Erd90]**, le faisant passer de $x(\log x)^{A\log\log\log x}$ à $x\exp\exp(c(\log\log x)^{2/3})$, où $c > 0$ est une constante absolue. La même année, Tenenbaum **[Ten90]** prouva le résultat suivant, qui est encore aujourd'hui le meilleur résultat général connu à ce jour.

Théorème 3.1.9 (**[Ten90]**, Théorème 2, p.216)**.** *Soit* $0 < \alpha < 2 - \log 4 < 0.61370$. *Pour chaque polynôme* F *de degré* $k > 1$, *irréductible dans* $\mathbb{Z}[X]$, *on a l'inégalité asymptotique*

$$P^+\left(\prod_{n\leq x} F(n)\right) > x\exp\left((\log x)^{\alpha}\right).$$

L'objectif de ce chapitre est de s'intéresser à la proportion des valeurs presque premières ($F(n)$, avec $n \in \mathbb{N}$) d'un polynôme F irréductible de degré k à coefficients entiers en y incorporant une condition de congruence sur la somme des chiffres des entiers n (écrits en base q). Afin de pouvoir étudier ce problème, une information capitale est celle concernant la répartition de la fonction somme des chiffres le long des progressions arithmétiques. Nous rappelons le résultat principal établi dans le Chapitre 2.

Théorème 2.3.1. *Soient* $0 < \varepsilon < 1$ *et* $b, q \geq 2$ *deux entiers tels que* $(b, q-1) = 1$. *Il existe une constante* $C = C(\varepsilon, b, q) > 0$ *et un exposant* $\eta = \eta(\varepsilon)$, *tels que*

$$\sum_{1\leq m\leq x^{1-\varepsilon}} \max_{\substack{y,z\\ 0\leq y<z\\ z-y\leq x}} \max_{r\geq 0} \left| \sum_{\substack{y\leq m<z\\ s_q(n)\equiv a \pmod b\\ m\equiv r \pmod m}} 1 - \frac{z-y}{bm}\right| \leq Cx^{1-\eta}.$$

Tout au long du chapitre, le Théorème 2.3.1 constituera un pivot dans l'adaptation de différents résultats concernant la proportion de valeurs polynomiales presque premières.
Les lignes suivantes établissent les théorèmes dont l'énoncé est adapté dans la sous-section 3.
Pour un polynôme F irréductible de $\mathbb{Z}[X]$ de degré $k \geq 2$ sans diviseur fixe, Richert **[Ric69]** montra en 1969 qu'il existe une infinité d'entiers de la forme $F(n)$ ayant au plus $(k+1)$ facteurs premiers. Plus précisément, on a le résultat suivant.

Théorème 3.1.10 (**[HR13]**, Theorem 9.7, p.259)**.** *Il existe* $x_0 = x_0(F) \in \mathbb{R}$ *tel que pour tout* $x \geq x_0$ *on a*

$$|\{n \leq x \,:\, F(n) = P_{k+1}\}| \geq \frac{2}{3}\prod_p \frac{1-\varrho(p)/p}{1-1/p}\frac{x}{\log(x)},$$

où, pour $d \geq 1$, *on pose*

$$\varrho(d) = |\{m \in \{0,\dots,d-1\},\, F(m) \equiv 0 \pmod d\}|.$$

Une autre notion qui permet d'appréhender la (non) primalité d'un nombre est celle de *friabilité*. Pour $y \in \mathbb{R}_+^*$, un nombre naturel n est dit y-friable si $P^+(n) \leq y$. Dartyge, Martin et Tenenbaum **[DMT01]** se sont intéressés à l'obtention d'une estimation de la quantité

$$\Psi_F(x,y) := |\{1 \leq n \leq x \ : \ P^+(F(n)) \leq y\}|.$$

En effet, ils prouvèrent le résultat suivant.

Théorème 3.1.11 (**[DMT01]**, Theorem 1.1)**.** *Soit $F \in \mathbb{Z}[X]$. Notons g le plus grand degré présent dans la décomposition de F en produit de facteurs irréductibles. Notons k le nombre de composantes irréductibles de F de degré g. Alors, pour tout $\varepsilon > 0$, et pour tout $y \geq x^{g-1/k+\varepsilon}$, on a*

$$\Psi_F(x,y) \asymp x.$$

Mounier **[Mou24]** a établi une minoration explicite de $\Psi_F(x,y)$.

Théorème 3.1.12 (**[Mou24]**, Théorème 1.7)**.** *Reprenons les notations du Théorème 3.1.11. Supposons de plus que $g > 1$. Pour $x \to +\infty$ et pour $y > x^{g-1}$, on a, en posant $u = \log(x)/\log(y)$:*

$$\frac{\Psi_F(x,y)}{x} \geq (gu)^g(1/u - kg + 1 + o(1)).$$

3.1.3. Résultats principaux

Étant donné que le Théorème 2.3.1 nous fournit une hypothèse fondamentale afin de pouvoir appliquer des théorèmes de cribles, nous avons le premier résultat suivant, portant sur le plus grand facteur premier de certains entiers du type n^2+1, sous la condition $s_q(n) \equiv a \pmod b$.

Théorème 3.1.13 (**[Tou26+]**, 2026+)**.** *Soient $b, q \geq 2$ tels que $(b, q-1) = 1$. Pour tout $\varepsilon > 0$, il existe une infinité d'entiers $n \geq 1$ tels que $s_q(n) \equiv a \pmod b$ et tels que le plus grand facteur premier de n^2+1 est plus grand que $n^{\theta_b - \varepsilon}$, où $\theta_b > 1$ est solution de l'équation :*

$$1 - \theta_b - 2\log(2-\theta_b) = \frac{1}{4b}. \tag{3.1}$$

Remarque 3.1.14. La preuve présentée par **[DI82]** nous fournit un résultat un peu meilleur dans le cas $b = 2$ que le résultat classique de Hooley **[Hoo67]**. En effet, on a $\theta_2 = 1.11154...$ Cependant, l'exposant θ_b décroît très vite vers 1 à mesure que b devient grand. Par exemple, pour $b = 10$, on trouve $\theta_{10} = 1.02439....$ On peut dans un premier temps montrer que si θ_b est solution de (3.1), alors

$$\theta_b \xrightarrow[b\to+\infty]{} 1.$$

Ainsi, en écrivant $\theta_b = 1 + \varepsilon(b)$, l'équation (3.1) devient

$$-\varepsilon(b) - 2\log(1-\varepsilon(b)) = \frac{1}{4b}.$$

En effectuant un développement limité à l'ordre 2, on montre que

$$\varepsilon(b) = \frac{1}{4b} + \mathcal{O}\left(\frac{1}{b^2}\right).$$

Finalement, on obtient l'expression de θ_b au voisinage de 1

$$\theta_b = 1 + \frac{1}{4b} + \mathcal{O}\left(\frac{1}{b^2}\right).$$

Plus généralement, concernant le cas d'un polynôme F de degré $k \geq 2$ irréductible dans $\mathbb{Z}[X]$ et sans diviseurs fixes, on a les résultats suivants. Le premier s'obtient en appliquant le crible à poids de Richert **[HR13]**. On rappelle qu'un polynôme F est dit sans diviseur fixe si pour tout $p \in \mathbb{P}$, il existe $n \in \mathbb{N}$ tel que $p \nmid F(n)$. Par exemple, 2 est un diviseur fixe du polynôme $F = X(X+1)$.

Théorème 3.1.15 (**[Tou26+]**, 2026+)**.** *Soit F un polynôme irréductible dans $\mathbb{Z}[X]$ de degré $k \geq 2$ sans diviseur fixe. Il existe une infinité d'entiers n tels que $s_q(n) \equiv a \pmod b$ et tels que $F(n)$ a au plus $(k+1)$ facteurs premiers. Plus précisément, pour $x \to +\infty$ on a :*

$$|\{n \leq x \,:\, F(n) = P_{k+1},\, s_q(n) \equiv a \pmod b\}| \geq \frac{22k+1}{33bk} \left(\prod_p \frac{1-\varrho(p)/p}{1-1/p} \right) \frac{x}{\log x},$$

où, pour $d \geq 1$, on pose

$$\varrho(d) = |\{m \in \{0, \dots, d-1\},\, F(m) \equiv 0 \pmod d\}|.$$

La preuve de ce résultat suit directement celle donnée dans le livre de Halberstam et Richert **[HR13,** p.259**]**. L'énoncé du théorème utilisé est mentionné dans la Section 4.

Le Théorème 3.5.1 et le Théorème 2.3.1 nous permettent d'appréhender la proportion d'entiers friables parmi les entiers du type $F(n)$, avec $n \leq x$ et ayant une condition de congruence du type $s_q(n) \equiv a \pmod b$, avec $(b, q-1) = 1$. En effet, le troisième résultat de ce chapitre est le suivant.

Théorème 3.1.16 (**[Tou26+]**, 2026+)**.** *Soit $x > 0$. Soit F un polynôme irréductible de $\mathbb{Z}[X]$ de degré $k \geq 2$ et de discriminant $D \neq 0$. Soient $b, q \in \mathbb{Z}$ tels que $(b, q-1) = 1$. Soit $\varepsilon > 0$. Supposons que $y \geq 1$ est tel que $y > x^{k-1+2\varepsilon}$. Posons $u = \log x / \log y$. Alors, pour $x \to +\infty$, on a la minoration*

$$|\{n \leq x \;:\; P^+(F(n)) \leq y\,,\, s_q(n) \equiv a \pmod b\}| \geq (1 - (k-1+\varepsilon)u + o(1))\frac{x}{b}.$$

3.2. Résultats auxiliaires

Dans cette section sont regroupés tous les résultats servant dans la preuve des résultats principaux. Le premier résultat, prouvé par Nagell, nous permettra par la suite de vérifier aisément certaines hypothèses en vue d'appliquer le crible linéaire pondéré. On définit la fonction ϱ qui à $d \in \mathbb{N}^*$ associe

$$\varrho(d) := |\{m \in \{0, \dots, d-1\},\, F(m) \equiv 0 \pmod d\}|. \tag{3.2}$$

Remarquons d'emblée que ϱ est multiplicative.

Lemme 3.2.1 (**[Nag21]**, Theorem 9.3, p.352)**.** *Soit F un polynôme irréductible de $\mathbb{Z}[X]$ sans diviseur fixe. Alors pour $x \to +\infty$, on a*

$$\sum_{p<x} \frac{\varrho(p)\log p}{p} = \log x + \mathcal{O}_F(1),$$

où ϱ est défini par (3.2).

Le lemme suivant, fourni également par Nagell **[Nag51]** donne une majoration du nombre de racines d'un polynôme modulo une puissance d'un nombre premier, ce dont on aura besoin dans la Section 5.

Lemme 3.2.2 (**[Nag51]**, Theorem 54, p.90)**.** *Soit F un polynôme irréductible de $\mathbb{Z}[X]$ de degré k et de discriminant $D \neq 0$. Soit $\alpha > 0$. Alors l'équation*

$$F(n) \equiv 0 \pmod{p^\alpha}$$

admet au plus kD^2 solutions modulo p^α.

Au cours du chapitre, des preuves vont être très similaires. Afin d'éviter des redondances, nous fournissons le résultat suivant. C'est dans cette proposition que le Théorème 2.3.1 joue un rôle clé.

Proposition 3.2.3. *Soit $f : \mathbb{N} \to \mathbb{R}_+^*$ une fonction multiplicative telle que*

$$\exists M \geq 0,\ \forall p \in \mathbb{P},\ \forall r \in \mathbb{N}^*,\ f(p^r) \leq M. \tag{$\bigstar$}$$

Soit $\alpha \in]0,1[$. Il existe $\eta = \eta(\alpha, b, q) > 0$ tel que

$$\sum_{d \leq x^\alpha} f(d) \max_{0 \leq m \leq d-1} \Big| \sum_{\substack{n \leq x \\ s_q(n) \equiv a \pmod b \\ n \equiv m \pmod d}} 1 - \frac{x}{bd} \Big| \ll_{b,q,\alpha} x^{1-\eta/2} (\log x)^{M^2/2}.$$

Remarque 3.2.4. On aurait pu mettre $x^{1-\delta}$ (pour $\delta = \delta(\alpha, b, q) > 0$ à la place de $x^{1-\eta/2}(\log x)^{M^2/2}$ mais la constante implicite dépend alors de M. Nous avons donc choisi de conserver $(\log x)^{M^2/2}$ pour expliciter la dépendance en M.

Démonstration. Pour $1 \leq d \leq x^\alpha$, posons

$$H(d) := \max_{0 \leq m \leq d-1} \Big| \sum_{\substack{n \leq x \\ s_q(n) \equiv a \pmod b \\ n \equiv m \pmod d}} 1 - \frac{x}{bd} \Big|.$$

D'après l'inégalité de Cauchy–Schwarz, on a

$$\sum_{d \leq x^\alpha} f(d) H(d) \leq \left(\sum_{d \leq x^\alpha} f(d)^2 H(d) \right)^{1/2} \times \left(\sum_{d \leq x^\alpha} H(d) \right)^{1/2}. \tag{3.3}$$

D'après le Théorème 2.3.1, il existe $\eta > 0$ tel que

$$\left(\sum_{d \leq x^\alpha} H(d) \right)^{1/2} \ll_{b,q,\alpha} x^{1/2 - \eta/2}.$$

De plus, on a trivialement

$$H(d) \ll_b \frac{x}{d}.$$

Ainsi, en injectant ces deux inégalités dans (3.3), on a

$$\sum_{d \leq x^\alpha} f(d) H(d) \ll_{b,q,\alpha} x^{1-\eta/2} \left(\sum_{d \leq x^\alpha} \frac{f(d)^2}{d} \right)^{1/2}.$$

Enfin, comme la fonction $d \mapsto \dfrac{f(d)^2}{d}$ est multiplicative, on écrit en utilisant l'hypothèse (★),

$$\begin{aligned}\sum_{d\leq x^\alpha} \frac{f(d)^2}{d} &\leq \sum_{P^+(d)\leq x^\alpha} \frac{f(d)^2}{d}\\ &\leq \prod_{p\leq x^\alpha}\left(\sum_{r=0}^{+\infty}\frac{f(p^r)^2}{p^r}\right)\\ &\leq \prod_{p\leq x^\alpha}\left(1+M^2\sum_{r=1}^{+\infty}\frac{1}{p^r}\right)\\ &= \prod_{p\leq x^\alpha}\left(1+\frac{M^2}{p-1}\right)\\ &\ll (\log x)^{M^2}.\end{aligned}$$

□

Remarque 3.2.5. Cette proposition nous servira deux fois dans ce chapitre. Dans la Section 4, on l'utilise avec la fonction $f : d \mapsto \mu^2(d)3^{\nu(d)}\varrho(d)$: cette fonction est bien multiplicative. De plus, pour tout $p \in \mathbb{P}$ et pour tout $r > 0$ fixés, on a $\varrho(p^r) \leq \varrho(p) \leq k$. Donc

$$\mu^2(p^r)3^{\nu(p^r)}\varrho(p^r) \leq 3k.$$

Dans la Section 5, on l'utilise avec la fonction ϱ, qui est également multiplicative. De plus, d'après le Lemme 3.2.2 on a pour tout $p \in \mathbb{P}$ et pour tout $r > 0$ fixés,

$$\varrho(p^r) \leq kD^2.$$

On rappelle également le théorème de Gelfond **[Gel68]**, qui nous sera utile dans la Section 3 du chapitre.

Théorème 3.2.6 (**[Gel68]**, Théorème 1, p.262)**.** *Soient $b, m, q \geq 2$ des entiers tels que $(b, q-1) = 1$. Alors, pour tout $a \in \{0, \dots, b-1\}$ et pour tout $r \in \{0, \dots, m-1\}$, on a*

$$|\{n < N \,:\, s_q(n) \equiv a \pmod b,\ n \equiv r \pmod m\}| = \frac{N}{bm} + \mathcal{O}(N^\lambda),$$

avec

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

La constante implicite dans le $\mathcal{O}$ est indépendante de a, b, m, r.

3.3. Le plus grand facteur premier de n^2+1 sous contraintes digitales

Nous faisons un rapide inventaire des notations et définitions spécifiques à cette partie uniquement.

3.3.1. Définitions et notations spécifiques

On fixe $\varepsilon > 0$. Soit $x \geq 1$.

► On considère β une fonction positive de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et à support compact dans $[x, 2x]$. De plus, on suppose que pour tout entier $r \geq 0$ et pour tout $t \in [x, 2x]$, on ait :

$$\beta^{(r)}(t) \ll t^{-r}, \tag{3.4}$$

où la constante implicite ne dépend que de r.

► On définit X par

$$X := \int_x^{2x} \beta(t)dt. \tag{3.5}$$

► Pour $d \geq 1$ entier, on pose

$$|\mathcal{A}_{d,q}| := \sum_{\substack{n^2+1 \equiv 0 \pmod{d} \\ s_q(n) \equiv a \pmod{b}}} \beta(n). \tag{3.6}$$

On désigne par $|\mathcal{A}_d|$ la quantité

$$|\mathcal{A}_d| := \sum_{n^2+1 \equiv 0 \pmod{d}} \beta(n). \tag{3.7}$$

Remarque 3.3.1. Le lecteur pourra trouver un exemple de fonction β (vérifiant les hypothèses mentionnées ci-dessus) dans [**[Fou85]**, Lemme 2].

Remarque 3.3.2. La continuité de β sur $[x, 2x]$ ainsi que le fait qu'elle est à support compact dans $[x, 2x]$ entraîne que

$$X = -\int_x^{2x} t\beta'(t)dt. \tag{3.8}$$

3.3.2. Preuve du Théorème 3.1.13

La preuve suit celle présentée par Deshouillers et Iwaniec **[DI82]**. La condition sur la somme des chiffres nous oblige cependant à utiliser d'autres résultats (comme le Théorème 2.3.1). En effet, les théorèmes tels que la formule sommatoire de Poisson (voir [**[DI82]**, Lemma 1]) ne sont plus applicables en raison de la présence de la contrainte

$$s_q(n) \equiv a \pmod{b}.$$

La méthode de Tchebychev–Hooley **[Hoo67]** consiste dans un premier temps à avoir un comportement asymptotique de la quantité

$$S(x) := \sum_{x < p \leq P_x} |\mathcal{A}_p| \log p,$$

où

$$P_x := P^+ \left(\prod_{x \leq n \leq 2x} (n^2 + 1) \right).$$

Dans un second temps, on cherche une majoration de $S(x)$ qui nous permet d'obtenir une minoration de P_x grâce à la formule asymptotique précédemment établie.

Nous allons procéder en quatre étapes. L'Étape 1 correspond à l'obtention d'une estimation de la somme totale

$$T(x) := \sum_{p\in\mathbb{P}} |\mathcal{A}_{p,q}| \log p. \tag{3.9}$$

L'Étape 2 correspond à l'obtention d'une estimation de la somme partielle

$$T_0(x) := \sum_{p\leq x} |\mathcal{A}_{p,q}| \log p. \tag{3.10}$$

L'Étape 3 constituera la conclusion des deux étapes. La dernière étape, l'Étape 4, reprendra la méthodologie principale de l'article de Deshouillers et Iwaniec **[DI82]**.

Étape 1 : estimation de $T(x)$

Dans un premier temps, transformons l'expression de $T(x)$ afin d'avoir une somme portant sur tous les entiers naturels supérieurs à 2. C'est l'objet du prochain lemme.

Lemme 3.3.3. *On a la réécriture*

$$T(x) = \sum_{d\in\mathbb{N}^*} |\mathcal{A}_{d,q}|\Lambda(d) + \mathcal{O}(x).$$

Démonstration. Par définition de Λ, on a

$$T(x) = \sum_{d\in\mathbb{N}^*} |\mathcal{A}_{d,q}|\Lambda(d) - \sum_{p\in\mathbb{P}} \sum_{k=2}^{+\infty} |\mathcal{A}_{p^k,q}| \log p.$$

Traitons la deuxième somme. Fixons $p \in \mathbb{P}$ et $k \geq 2$. Supposons $|\mathcal{A}_{p^k,q}| > 0$. Alors il existe $x \leq n \leq 2x$ tel que $p^k \mid (n^2+1)$. On en déduit que

$$p^k \leq 4x^2 + 1.$$

Comme $k \geq 2$, on a

$$p \leq \sqrt{4x^2+1}.$$

On obtient également

$$k \leq \frac{\log(4x^2+1)}{\log p}.$$

De plus, en utilisant le fait que β est bornée et en supprimant la condition sur la somme des chiffres, on a

$$\begin{aligned}
|\mathcal{A}_{p^k,q}| &\ll \sum_{\substack{x\leq n\leq 2x \\ n^2+1\equiv 0 \pmod{p^k}}} 1 \\
&= \sum_{\substack{\nu=0 \\ \nu^2+1\equiv 0 \pmod{p^k}}}^{p^k-1} \sum_{\substack{x\leq n\leq 2x \\ n\equiv\nu \pmod{p^k}}} 1 \\
&= \sum_{\substack{\nu=0 \\ \nu^2+1\equiv 0 \pmod{p^k}}}^{p^k-1} \left(\frac{x}{p^k} + \mathcal{O}(1)\right) \\
&= \left(\frac{x}{p^k} + \mathcal{O}(1)\right) \sum_{\substack{\nu=0 \\ \nu^2+1\equiv 0 \pmod{p^k}}}^{p^k-1} 1 \\
&\leq \frac{2x}{p^k} + \mathcal{O}(1),
\end{aligned}$$

car l'équation

$$\nu^2 + 1 \equiv 0 \pmod{p^k}$$

possède au plus 2 solutions modulo p^k. Ainsi, en remarquant que la famille $\{\log p/p^k\}_{p\geq 2, k\geq 2}$ est sommable, on obtient

$$\sum_{p\in\mathbb{P}}\sum_{k=2}^{+\infty} |\mathcal{A}_{q,p^k}| \log p \ll 2x \sum_{p\geq 2}\sum_{k\geq 2} \frac{\log p}{p^k} + \mathcal{O}\left(\sum_{2\leq p\leq\sqrt{4x^2+1}} \sum_{2\leq k\leq \frac{\log(4x^2+1)}{\log p}} \log p\right).$$

Enfin, en utilisant le théorème des nombres premiers, on a

$$\begin{aligned}\sum_{2\leq p\leq\sqrt{4x^2+1}} \sum_{2\leq k\leq \frac{\log(4x^2+1)}{\log p}} \log p &\leq \log(4x^2+1) \sum_{2\leq p\leq\sqrt{4x^2+1}} 1 \\ &\ll x.\end{aligned}$$

Finalement, nous avons montré que

$$T(x) = \sum_{d\in\mathbb{N}^*} |\mathcal{A}_{d,q}|\Lambda(d) + \mathcal{O}(x).$$

□

En profitant de l'additivité du logarithme et en utilisant le Lemme 2.7.1 afin de contrôler la condition sur la somme des chiffres, on montre le résultat ci-après. Il s'agit du cœur de l'Étape 1.

Lemme 3.3.4. *On a le comportement asymptotique suivant :*

$$T(x) = \frac{2X}{b}\log x + \mathcal{O}(x).$$

Démonstration. D'après le Lemme 3.3.3, on a

$$\begin{aligned}T(x) &= \sum_{d\in\mathbb{N}^*} |\mathcal{A}_{d,q}|\Lambda(d) + \mathcal{O}(x) \\ &= \sum_{d\in\mathbb{N}^*} \Lambda(d) \sum_{\substack{n^2+1\equiv 0 \pmod d \\ s_q(n)\equiv a \pmod b}} \beta(n) + \mathcal{O}(x) \\ &= \sum_{\substack{x\leq n\leq 2x \\ s_q(n)\equiv a \pmod b}} \beta(n) \sum_{d\mid n^2+1} \Lambda(d) + \mathcal{O}(x) \\ &= \sum_{\substack{x\leq n\leq 2x \\ s_q(n)\equiv a \pmod b}} \beta(n)\log\left(n^2+1\right) + \mathcal{O}(x).\end{aligned}$$

Comme $n\in[x,2x]$, on a $\log(n^2+1) = 2\log x + \mathcal{O}(1)$. Ainsi,

$$T(x) = 2\log x \sum_{\substack{x\leq n\leq 2x \\ s_q(n)\equiv a \pmod b}} \beta(n) + \mathcal{O}\left(\sum_{\substack{x\leq n\leq 2x \\ s_q(n)\equiv a \pmod b}} \beta(n)\right) + \mathcal{O}(x).$$

En supprimant la condition sur la somme des chiffres et en utilisant le fait que β est bornée, on majore trivialement la somme dans le terme d'erreur et on obtient

$$T(x) = 2\log x \sum_{\substack{x\leq n\leq 2x\\ s_q(n)\equiv a \pmod b}} \beta(n) + \mathcal{O}(x). \tag{3.11}$$

Il ne nous reste plus qu'à traiter la somme présente dans (3.11). Pour ce faire, nous utilisons dans un premier temps une sommation d'Abel pour détacher la condition portant sur la somme des chiffres du reste. Dans un second temps, on utilise le Lemme 2.7.1 afin de contrôler les termes d'erreur. On écrit

$$\begin{aligned}\sum_{\substack{x\leq n\leq 2x\\ s_q(n)\equiv a \pmod b}} \beta(n) &= \sum_{x<n\leq 2x} \beta(n)\mathbb{1}_{\{x\leq m\leq 2x\,:\, s_q(m)\equiv a \pmod b\}}(n)\\ &= \beta(2x)\left|\{m\leq 2x \,:\, s_q(m)\equiv a \pmod b\}\right| - \beta(x)\left|\{m\leq x \,:\, s_q(m)\equiv a \pmod b\}\right|\\ &\quad - \int_x^{2x} \beta'(t)\left(\sum_{\substack{n\leq t\\ s_q(n)\equiv a \pmod b}} 1\right) dt.\end{aligned}$$

Comme $\beta(2x) = \beta(x) = 0$, on a

$$\sum_{\substack{x\leq n\leq 2x\\ s_q(n)\equiv a \pmod b}} \beta(n) = -\int_x^{2x} \beta'(t)\left(\sum_{\substack{n\leq t\\ s_q(n)\equiv a \pmod b}} 1\right) dt.$$

D'après le Lemme 2.7.1, on a

$$\begin{aligned}\sum_{\substack{x\leq n\leq 2x\\ s_q(n)\equiv a \pmod b}} \beta(n) &= -\int_x^{2x} \beta'(t)\left(\frac{t}{b} + \mathcal{O}\left(t^\lambda\right)\right) dt\\ &= -\frac{1}{b}\int_x^{2x} t\beta'(t)dt + \mathcal{O}\left(\int_x^{2x} \beta'(t)t^\lambda dt\right).\end{aligned}$$

D'après (3.8) et l'hypothèse (3.4), on a

$$\sum_{\substack{x\leq n\leq 2x\\ s_q(n)\equiv a \pmod b}} \beta(n) = \frac{X}{b} + \mathcal{O}\left(x^\lambda\right),$$

avec X défini par (3.5). En injectant cela dans l'équation (3.11), on obtient

$$T(x) = \frac{2X}{b}\log x + \mathcal{O}(x).$$

□

Étape 2 : estimation de $T_0(x)$

On rappelle que $T_0(x)$ est défini par (3.10). L'idée est similaire à l'Étape 1. Isolons dans un premier temps le terme principal à l'aide de l'identité d'Abel. On s'intéressera au terme d'erreur par la suite.

Lemme 3.3.5. *$T_0(x)$ vérifie le comportement asymptotique suivant :*

$$T_0(x) = \frac{X\log x}{b} - R(x) + \mathcal{O}(x),$$

où

$$R(y) := \sum_{p\leq y}\log p \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \int_x^{2x} \beta'(t)\left(\sum_{\substack{n\leq t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1 - \frac{t}{bp}\right) dt. \tag{3.12}$$

Démonstration. On écrit

$$\begin{aligned} T_0(x) &= \sum_{p\leq x} |\mathcal{A}_{p,q}|\log p \\ &= \sum_{p\leq x}\log p \left(\sum_{\substack{n^2+1\equiv 0 \pmod p\\ s_q(n)\equiv a \pmod b}} \beta(n)\right) \\ &= \sum_{p\leq x}\log p \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \sum_{\substack{n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} \beta(n). \end{aligned} \tag{3.13}$$

En utilisant encore une fois $\beta(x) = \beta(2x) = 0$ et par la suite (3.8), on obtient, à l'aide d'une sommation d'Abel

$$\begin{aligned} \sum_{\substack{n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} \beta(n) &= -\int_x^{2x} \beta'(t) \sum_{\substack{n\leq t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1\, dt \\ &= \frac{X}{bp} - \int_x^{2x} \beta'(t)\left(\sum_{\substack{n\leq t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1 - \frac{t}{bp}\right) dt. \end{aligned}$$

En injectant la dernière égalité dans (3.13) et en séparant en deux sommes, on a

$$\begin{aligned} T_0(x) &= \frac{X}{b}\sum_{p\leq x}\frac{\rho(p)\log p}{p} - \sum_{p\leq x}\log p \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \int_x^{2x} \beta'(t)\left(\sum_{\substack{n\leq t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1 - \frac{t}{bp}\right) dt. \\ &= \frac{X}{b}\sum_{p\leq x}\frac{\rho(p)\log p}{p} - R(x). \end{aligned}$$

D'après le Lemme 3.2.1 et comme $X \ll x$, on a

$$T_0(x) = \frac{X\log x}{b} - R(x) + \mathcal{O}(x). \tag{3.14}$$

□

Concentrons-nous désormais sur $R(x)$. Nous montrons que $R(x)$ est négligeable devant x. L'idée est de scinder $R(x)$ en deux sommes $R(x^{1-\varepsilon})+(R(x)-R(x^{1-\varepsilon}))$. Cela nous permet d'appliquer dans un premier temps le Théorème 2.3.1 pour dominer la somme $R(x^{1-\varepsilon})$. Pour dominer la somme $R(x)-R(x^{1-\varepsilon})$, on utilise des majorations élémentaires.

Lemme 3.3.6. *Soit $\varepsilon>0$. On considère*

$$R(x^{1-\varepsilon}) := \sum_{p\le x^{1-\varepsilon}} \log p \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \int_x^{2x} \beta'(t) \left(\sum_{\substack{n\le t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1-\frac{t}{bp}\right) dt.$$

Alors on a

$$R(x^{1-\varepsilon}) \ll x^{1-\eta},$$

avec $\eta=\eta(\varepsilon,b,q)$ défini dans le Théorème 2.3.1.

Démonstration. D'après l'inégalité triangulaire, on a

$$|R(x^{1-\varepsilon})| \le \sum_{p\le x^{1-\varepsilon}} \log p \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \int_x^{2x} |\beta'(t)| \Big| \sum_{\substack{n\le t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1-\frac{t}{bp}\Big| dt$$

$$\le \sum_{p\le x^{1-\varepsilon}} \log p \max_{\substack{y\in[x,2x]\\ \mu\ge 0}} \Big| \sum_{\substack{n\le y\\ n\equiv\mu \pmod p\\ s_q(n)\equiv a \pmod b}} 1-\frac{y}{bp}\Big| \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \int_x^{2x} |\beta'(t)| dt.$$

Comme pour tout $t\in[x,2x]$, $\beta'(t)\ll 1/t$, alors

$$R(x^{1-\varepsilon}) \ll \sum_{p\le x^{1-\varepsilon}} \varrho(p)\log p \max_{\substack{y\in[x,2x]\\ \mu\ge 0}} \Big| \sum_{\substack{n\le y\\ n\equiv\mu \pmod p\\ s_q(n)\equiv a \pmod b}} 1-\frac{y}{bp}\Big|.$$

D'après le Lemme 3.2.2 et en majorant $\log p\le \log x$, on a, d'après le Théorème 2.3.1,

$$R(x^{1-\varepsilon}) \ll x^{1-\eta}\log x.$$

□

Il ne nous reste plus qu'à nous intéresser à la somme $R(x)-R(x^{1-\varepsilon})$. C'est l'objet du lemme suivant.

Lemme 3.3.7. *On a la majoration suivante :*

$$R(x)-R(x^{1-\varepsilon}) = \sum_{x^{1-\varepsilon}<p\le x} \log p \sum_{\substack{\nu=0\\ \nu^2+1\equiv 0 \pmod p}}^{p-1} \int_x^{2x} \beta'(t) \left(\sum_{\substack{n\le t\\ n\equiv\nu \pmod p\\ s_q(n)\equiv a \pmod b}} 1-\frac{t}{bp}\right) dt$$

$$\ll \varepsilon X\log x.$$

Démonstration. On utilise à nouveau l'inégalité triviale

$$\max_{\substack{y\in[x,2x]\\ \mu\geq 0}}\Big|\sum_{\substack{n\leq y\\ n\equiv\mu \pmod p\\ s_q(n)\equiv a \pmod b}} 1-\frac{y}{bp}\Big| \ll x/p,$$

puis on utilise le fait que pour tout $t\in[x,2x]$ on a $\beta'(t)\ll 1/t$. Il vient que

$$R(x)-R(x^{1-\varepsilon}) \ll \sum_{x^{1-\varepsilon}<p\leq x}\frac{\varrho(p)\log p}{p}\int_x^{2x} t\beta'(t)\,dt.$$

En utilisant (3.8) et le Lemme 3.2.1, on obtient

$$\begin{aligned} R(x)-R(x^{1-\varepsilon}) &\ll X\left(\log x-\log(x^{1-\varepsilon})+\mathcal{O}(1)\right)\\ &\ll \varepsilon X\log x. \end{aligned}$$

□

Étape 3 : synthèse de l'Étape 1 et de l'Étape 2

En rassemblant les Lemme 3.3.5, Lemme 3.3.6 et Lemme 3.3.7 de l'Étape 2, on a le comportement asymptotique

$$\begin{aligned} T_0(x) &= \frac{X\log x}{b}-R(x)+\mathcal{O}(x)\\ &= \frac{X\log x}{b}-\left(R(x^{1-\varepsilon})+R(x)-R(x^{1-\varepsilon})\right)+\mathcal{O}(x)\\ &= \frac{X\log x}{b}+\mathcal{O}\left(x^{1-\eta}\log x\right)+\mathcal{O}\left(\varepsilon X\log x\right)+\mathcal{O}(x)\\ &= \frac{X\left(1+\mathcal{O}(\varepsilon)\right)\log x}{b}+\mathcal{O}(x). \end{aligned}$$

On retranche cela à $T(x)$ estimé dans le Lemme 3.3.4, lors de l'Étape 1. On définit $P_{x,q}$ comme

$$P_{x,q}:=P^+\left(\prod_{\substack{x\leq n\leq 2x\\ s_q(n)\equiv a \pmod b}}(n^2+1)\right)$$

et on trouve, de manière analogue à [[DI82], (3)], que :

$$\mathfrak{S}(x):=\sum_{x<p\leq P_{x,q}}|\mathcal{A}_{p,q}|\log p=\frac{X\left(1+\mathcal{O}(\varepsilon)\right)\log x}{b}+\mathcal{O}(x). \tag{3.15}$$

Étape 4 : obtenir une minoration de $P_{x,q}$

L'objectif est d'obtenir une « bonne » majoration de

$$\sum_{x<p\leq D}|\mathcal{A}_{p,q}|\log p,$$

où

$$D=x^{\theta_b}$$

est le plus grand possible, afin d'obtenir une minoration de $P_{x,q}$.
Dans un premier temps, on supprime la condition portant sur la somme des chiffres,

$$\sum_{x<p\leq D} |\mathcal{A}_{p,q}| \log p \leq \sum_{x<p\leq D} |\mathcal{A}_p| \log p. \tag{3.16}$$

Désormais, nous allons reprendre la preuve de **[DI82]** afin de majorer le membre de droite de **(3.16)**. On pose

$$S(x) := \sum_{x<p\leq D} |\mathcal{A}_p| \log p.$$

Procédons à un découpage dyadique de $S(x)$. On écrit

$$S(x) = \sum_{0\leq j\leq J} S(x, Q_j) + \mathcal{O}(x), \tag{3.17}$$

où pour tout $0 \leq j \leq J \leq 2\log x$, on a $Q_j = 2^j x$ et

$$S(x, Q_j) = \sum_{Q_j<p\leq 4Q_j} |\mathcal{A}_p| C_j(p) \log p,$$

et pour tout $0 \leq j \leq J$, C_j est une fonction positive, de classe $\mathcal{C}^\infty$ et telle que

$$\begin{cases} \operatorname{Supp} C_j \subset [Q_j, 4Q_j], \\ \forall r \geq 0,\ \forall t \in [Q_j, 4Q_j],\ C_j^{(r)}(t) \ll t^{-r}. \end{cases}$$

Les C_j vérifient également la condition

$$\sum_{0\leq j\leq J} C_j(\xi) = \begin{cases} 1 & \text{si } 2x < \xi \leq P_x, \\ \mathcal{O}(1) & \text{si } x < \xi \leq 2x \quad \text{ou} \quad P_x < \xi \leq 2P_x, \\ 0 & \text{sinon.} \end{cases}$$

Remarque 3.3.8. On trouvera une construction de telles fonction dans **[Fou85,** Lemme 2**]**.

On obtient une première majoration de $S(x, Q_j)$ du type

$$S(x, Q_j) \leq XV(x, Q_j) + R(x, Q_j), \tag{3.18}$$

où les quantités $V(x, Q_j)$ et $R(x, Q_j)$ sont définies dans [**[DI82]**, p.5]. Le terme principal sera ici $XV(x, Q_j)$. En effet, les auteurs de [**[DI82]**, **5.**] montrent que

$$R(x, Q_j) \ll x^{1-\varepsilon}.$$

Ainsi,

$$\sum_{1\leq j\leq J} R(x, Q_j) \ll x^{1-\varepsilon} \log x.$$

Concernant le terme principal, d'après [**[DI82]**, p.10], on a :

$$X \sum_{0\leq j\leq J} V(x, Q_j) = (1 + \mathcal{O}(\varepsilon)) f(\theta_b) X \log x, \tag{3.19}$$

où

$$f(x) = 4(1 - x - 2\log(2 - x)). \tag{3.20}$$

Finalement, d'après (3.19), (3.18), (3.17) et (3.16), on a

$$\begin{aligned}\sum_{x<p\leq D} |\mathcal{A}_{p,q}| \log p &\leq (1 + \mathcal{O}(\varepsilon)) f(\theta_b) X \log x + x^{1-\varepsilon} \log x + \mathcal{O}(x) \\ &= (1 + \mathcal{O}(\varepsilon)) b f(\theta_b) \frac{X \log x}{b} + x^{1-\varepsilon} \log x + \mathcal{O}(x).\end{aligned}$$

En choisissant $\theta_b > 0$ tel que $bf(\theta_b) < 1$, on obtient :

$$\sum_{x<p\leq D} |\mathcal{A}_{p,q}| \log p < (1 + \mathcal{O}(\varepsilon)) \frac{X \log x}{b} + x^{1-\varepsilon} \log x + \mathcal{O}(x). \tag{3.21}$$

Or, on rappelle que $\mathfrak{S}(x) = \sum_{x<p\leq P_{x,q}} |\mathcal{A}_{p,q}| \log p$ vérifie le comportement asymptotique (3.15), à savoir

$$\mathfrak{S}(x) = \frac{X\,(1 + \mathcal{O}(\varepsilon)) \log x}{b} + \mathcal{O}(x).$$

Nécessairement, on a $P_{x,q} \geq x^{\theta_b - \varepsilon}$.

3.4. Valeurs polynomiales avec peu de facteurs premiers

3.4.1. Définitions et premières propriétés

Soient b et q deux entiers naturels tels que $(b, q-1) = 1$. Soient $a \in \{0, \dots, b-1\}$ et $x > 0$ qui tend vers $+\infty$.
On considère F un polynôme irréductible dans $\mathbb{Z}[X]$ de degré $k \geq 2$ sans diviseur fixe. On rappelle de plus la fonction ϱ qui à $d \in \mathbb{N}^*$ associe

$$\varrho(d) := |\{m \in \{0, \dots, d-1\},\ F(m) \equiv 0 \pmod d\}|.$$

L'objectif de cette section est de prouver le Théorème 3.1.15. Nous utilisons le résultat présent dans [[HR13], Theorem 9.3, p.253], qui repose sur le crible linéaire pondéré. Il nous faut donc d'abord définir l'ensemble qu'on souhaite cribler. Il s'agit du multi-ensemble (avec donc d'éventuelles répétitions)

$$\mathcal{A} := \{F(n) \,:\, n \leq x,\ s_q(n) \equiv a \pmod b\}.$$

Pour d un entier sans facteur carré, on définit

$$\mathcal{A}_d := \{F(n) \,:\, n \leq x,\ s_q(n) \equiv a \pmod b,\ F(n) \equiv 0 \pmod d\}.$$

On remarque que

$$|\mathcal{A}_d| = X \frac{\omega(d)}{d} + r(\mathcal{A}, d),$$

avec

$$X = \frac{x}{b}, \qquad \omega(d) = \rho(d), \qquad r(\mathcal{A}, d) = \sum_{\substack{m=0 \\ d|F(m)}}^{d-1} \left(\sum_{\substack{n\leq x \\ s_q(n)\equiv a \pmod b \\ n \equiv m \pmod d}} 1 - \frac{x}{bd} \right). \tag{3.22}$$

Cette réécriture de $|\mathcal{A}_d|$ nous servira pour la suite.

3.4.2. Preuve du Théorème 3.1.15

Pour utiliser [**[HR13]**, Theorem 9.3, p.253], on rappelle les hypothèses que nous devons vérifier. Les hypothèses ci-dessous se trouvent respectivement aux pages 29, 252, 253 et 219 (avec $\kappa = 1$) de **[HR13]**.

$$\exists A_1 \geq 1,\ \forall p \in \mathbb{P},\ 0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1}. \tag{Ω_1}$$

$$\exists A_2 > 0,\ \forall\ 2 \leq v \leq w,\ -A_2 \log\log(3X) \leq \sum_{v \leq p < w} \frac{\omega(p)}{p} \log p - \log\left(\frac{w}{v}\right) \leq A_2. \tag{$\Omega_2^*(1)$}$$

$$\exists A_3 > 0,\ \forall\ 2 \leq z \leq y,\ \sum_{z \leq p < y} |\mathcal{A}_{p^2}| \leq A_3 \left(\frac{X \log x}{z} + y\right). \tag{Ω_3}$$

$$\exists A_4, A_5 \geq 1,\ \sum_{d < X^\alpha/(\log x)^{A_4}} \mu^2(d) 3^{\nu(d)} |r(\mathcal{A}, d)| \leq A_5 \frac{X}{\log^2 X}. \tag{$R(1,\alpha)$}$$

Le [**[HR13]**, Theorem 9.3, p.253] s'énonce comme suit.

Théorème 3.4.1 (**[HR13]**, p.253). *Supposons* (Ω_1), ($\Omega_2^*(1)$), (Ω_3) *et* ($R(1,\alpha)$) *pour un certain* α *avec* $0 < \alpha < 1$. *Pour* $r \geq 2$, *on pose*

$$\Lambda_r = r + 1 - \frac{\log\left(4/(1+3^{-r})\right)}{\log(3)}.$$

Soit $0 < \delta \leq \frac{2}{3}$. *Supposons que pour tout* $a \in \mathcal{A}$, *on ait*

$$|a| \leq X^{\alpha(\Lambda_r - \delta)}. \tag{3.23}$$

Alors, il existe $X_0 = X_0(\delta, r)$ *tel que, pour tout* $X \geq X_0$, *on a*

$$|\{P_r\ :\ P_r \in \mathcal{A}\}| \geq \frac{\delta}{\alpha} \prod_p \frac{1 - \omega(p)/p}{1 - 1/p} \frac{X}{\log x}.$$

Pour la preuve du Théorème **3.1.15**, nous allons vérifier les conditions (Ω_1), ($\Omega_2^*(1)$), (Ω_3) et ($R(1,\alpha)$) afin d'appliquer le Théorème **3.4.1**.

▶ **Vérification de** (Ω_1) :
Soit $p \in \mathbb{P}$. Rappelons que dans notre cas, F est de degré k. On distingue deux cas.
▷ Cas 1 : $p \leq k$.
Comme F est sans diviseur fixe, alors $0 \leq \varrho(p) < p$. En utilisant le fait que $\varrho(p) \in \mathbb{N}$, on a :

$$\frac{\varrho(p)}{p} \leq \frac{p-1}{p} = 1 - \frac{1}{p} \leq 1 - \frac{1}{k}.$$

▷ Cas 2 : $p > k$.
On a :

$$0 \leq \frac{\varrho(p)}{p} \leq \frac{k}{p} \leq \frac{k}{k+1} = 1 - \frac{1}{k+1}.$$

Par ailleurs, on a directement la minoration $\dfrac{\varrho(p)}{p} \geq 0$. Ainsi, il suffit de prendre $A_1 = k + 1$ et (Ω_1) est vérifiée.

▶ **Vérification de** $(\Omega_2^*(1))$: La vérification est faite dans **[HR13]**. Nous la refaisons cependant ici. Pour prouver l'encadrement $(\Omega_2^*(1))$, on utilise le Lemme **3.2.1**. Comme pour tout $p \in \mathbb{P}$ on a $\omega(p) = \varrho(p)$, alors on a directement pour tout $2 \leq v \leq w$:

$$\begin{aligned}\sum_{v\leq p<w} \frac{\omega(p)\log p}{p} &= \sum_{v\leq p<w} \frac{\varrho(p)\log p}{p} \\ &= \sum_{p<w} \frac{\omega(p)\log p}{p} - \sum_{p<v} \frac{\omega(p)\log p}{p} \\ &= \log w - \log v + O_F(1) \\ &= \log\left(\frac{w}{v}\right) + O_F(1).\end{aligned}$$

Ainsi, il existe $A_2 > 0$ tel que

$$\Big| \sum_{v\leq p<w} \frac{\varrho(p)\log p}{p} - \log\left(\frac{w}{v}\right) \Big| \leq A_2,$$

ce qui prouve la condition $(\Omega_2^*(1))$.

▶ **Vérification de** (Ω_3) **:**
Soient $2 \leq z < y$. On écrit :

$$\begin{aligned}\sum_{z\leq p<y} |\mathcal{A}_{p^2}| &= \sum_{z\leq p<y} |\{F(n) \ : \ n \leq x, \ F(n) \equiv 0 \ (\mathrm{mod}\ p^2), \ s_q(n) \equiv a \ (\mathrm{mod}\ b)\}| \\ &\leq \sum_{z\leq p<y} |\{F(n) \ : \ n \leq x, \ F(n) \equiv 0 \ (\mathrm{mod}\ p^2)\}| \\ &\leq \sum_{z\leq p<y} |\{n \leq x \ : \ F(n) \equiv 0 \ (\mathrm{mod}\ p^2)\}|.\end{aligned}$$

Or, pour tout $z \leq p < y$, on a, en découpant selon la classe de congruence de n $(\mathrm{mod}\ p^2)$

$$\begin{aligned}|\{n \leq x \ : \ F(n) \equiv 0 \ (\mathrm{mod}\ p^2)\}| &= \sum_{\nu=0}^{p^2-1} \sum_{\substack{n\leq x \\ F(n)\equiv 0 \ (\mathrm{mod}\ p^2) \\ n\equiv \nu \ (\mathrm{mod}\ p^2)}} 1 \\ &= \sum_{\substack{\nu=0 \\ p^2\mid F(\nu)}}^{p^2-1} \sum_{\substack{n\leq x \\ n\equiv \nu \ (\mathrm{mod}\ p^2)}} 1 \\ &\ll \left(\frac{x}{p^2} + \mathcal{O}(1)\right) \sum_{\substack{\nu=0 \\ p^2\mid F(\nu)}}^{p^2-1} 1 \\ &\ll \frac{x}{p^2} + 1,\end{aligned}$$

d'après le Lemme **3.2.2**. Ainsi,

$$\sum_{z\leq p<y} |\mathcal{A}_{p^2}| \ll \sum_{z\leq p<y} \left(\frac{x}{p^2} + 1\right) \ll \frac{x}{z} + y$$

et (Ω_3) est ainsi vérifiée.

▶ **Vérification de** $(R(1,\alpha))$ **:**
On rappelle la définition **(3.22)** de $r(\mathcal{A},d)$:

$$r(\mathcal{A},d) := \sum_{\substack{m=0\\ d|F(m)}}^{d-1} \left(\sum_{\substack{n\le x\\ s_q(n)\equiv a \pmod b\\ n\equiv m \pmod d}} 1 - \frac{x}{bd} \right).$$

Ainsi, pour $D \ge 1$, on obtient,

$$\begin{aligned}\sum_{d<D} \mu^2(d)3^{\nu(d)}|r(\mathcal{A},d)| &= \sum_{d<D} \mu^2(d)3^{\nu(d)} \left| \sum_{\substack{m=0\\ d|F(m)}}^{d-1} \left(\sum_{\substack{n\le x\\ s_q(n)\equiv a \pmod b\\ n\equiv m \pmod d}} 1 - \frac{x}{bd} \right) \right| \\ &\le \sum_{d<D} \mu^2(d)3^{\nu(d)}\varrho(d) \max_{0\le m\le d-1} \left| \sum_{\substack{n\le x\\ s_q(n)\equiv a \pmod b\\ n\equiv m \pmod d}} 1 - \frac{x}{bd} \right|.\end{aligned}$$

Écrivons $D = x^{1-\varepsilon}$ $(0 < \varepsilon < 1)$. D'après la Proposition **3.2.3** et la Remarque **3.2.5** on a

$$\sum_{d<D} \mu^2(d)3^{\nu(d)}\varrho(d) \max_{0\le m\le d-1} \left| \sum_{\substack{n\le x\\ s_q(n)\equiv a \pmod b\\ n\equiv m \pmod d}} 1 - \frac{x}{bd} \right| \ll x^{1-\eta/2}(\log x)^{9k^2/2}$$

et $(R(1,\alpha))$ est vérifiée.
Il nous reste à trouver α, r et δ tels que **(3.23)** soit vérifiée. Pour ce faire, on choisit

$$\varepsilon = 1/(22k+1), \quad \alpha = 1-\varepsilon, \quad r = k+1 \ge 2 \quad \text{et} \quad \delta = \frac{2}{3}. \tag{3.24}$$

Par définition de F et de $\mathcal{A}$, pour tout $a \in \mathcal{A}$ il existe $n \le x$ tel que

$$a = F(n) \ll_F n^k \le x^k. \tag{3.25}$$

De plus,

$$X^{\alpha(\Lambda_r-\delta)} := \left(\frac{x}{b}\right)^{\alpha(\Lambda_r-\delta)},$$

avec Λ_r défini dans le Théorème **3.4.1**. L'inégalité [**[HR13]**, (4.5), p.258)] (utilisable ici car $r \ge 2$) nous permet de minorer Λ_r par

$$\Lambda_r > r - \frac{2}{7}.$$

Donc,

$$\Lambda_r - \delta > k + 1 - \frac{2}{7} - \frac{2}{3} = k + \frac{1}{21}.$$

Ainsi,

$$\alpha(\Lambda_r - \delta) > \frac{k}{k+1/22}\left(k + \frac{1}{21}\right) = \gamma_k k, \tag{3.26}$$

avec

$$\gamma_k := \frac{k+1/21}{k+1/22} > 1.$$

En rassemblant (3.25) et (3.26), nous avons montré que

$$X^{\alpha(\Lambda_r-\delta)} > \left(\frac{x}{b}\right)^{\alpha(\Lambda_r-\delta)} > \frac{1}{b^{k\gamma_k}} x^{k\gamma_k}.$$

Ainsi, pour x suffisamment grand, on a

$$X^{\alpha(\Lambda_r-\delta)} > |a|$$

et **(3.23)** est donc vérifiée. Ainsi, le Théorème **3.4.1** s'applique. D'après les conditions posées en **(3.24)**, on a

$$\frac{\delta}{\alpha} = \frac{2}{3} \times \frac{22k+1}{22k} = \frac{22k+1}{33k},$$

ce qui termine la preuve du Théorème **3.1.15**.

3.5. Valeurs friables de F

3.5.1. Cadre d'étude

Les hypothèses $(\Omega_2^*(1))$ et $(R(1,\alpha))$ vont nous permettre, à l'aide de l'article de Mounier **[Mou24]**, d'établir un résultat analogue concernant les valeurs friables d'un polynôme F à coefficients entiers et irréductible de degré $k \geq 2$ sous contraintes digitales. Comme précédemment, on pose

$$\mathcal{A} = \{F(n) \,:\, n \leq x,\, s_q(n) \equiv a \pmod b\}.$$

On rappelle que $\mathcal{A}$ est un multi-ensemble. $\mathcal{A}$ contient donc des éventuelles répétitions. Le Théorème 1.1 de **[Mou24]** nous permet, à condition de vérifier ses hypothèses, de minorer la quantité $\Psi_{\mathcal{A}}(y)$ définie par

$$\Psi_{\mathcal{A}}(y) := |\{n \in \mathcal{A} \,:\, P^+(n) \leq y\}|.$$

On pose, de manière usuelle

$$u := \frac{\log x}{\log y}. \tag{3.27}$$

Comme on crible ici les éléments de la forme $F(n)$ avec $n \leq x$, on pose

$$x' := \sup \mathcal{A} \ll x^k$$

et

$$u' := \frac{\log x'}{\log y}.$$

Remarquons d'emblée que l'on a le comportement asymptotique

$$u' = ku + \mathcal{O}\left(\frac{1}{\log y}\right). \tag{3.28}$$

Cette estimation de u' nous servira par la suite, lors de certaines minorations et majorations.

Notons que l'on garde la même écriture que **(3.22)**. Les hypothèses à vérifier sont celles présentes dans [**[Mou24]**, p.2] qu'on rappelle ici.

$$\exists \kappa > 0,\ \forall z > 0\,,\ \sum_{p \le z} \frac{\log p}{p} \omega(p) = \kappa \log(z) + \mathcal{O}_F(1). \tag{A_κ}$$

$$\forall \alpha \ge 0,\ \omega(p^\alpha) = \mathcal{O}_F(1). \tag{B}$$

$$\exists \theta \in]1 - 1/u', 1[\,,\ \exists \delta > 0,\ \sum_{d \le y^{u'\theta}} |r(\mathcal{A}, d)| \ll_\theta \frac{X}{(\log y)^\delta}. \tag{C_θ}$$

Le théorème principal qu'on utilise pour prouver le Théorème 3.1.16 est le suivant.

Théorème 3.5.1 (**[Mou24]**, Théorème 1.1)**.** *Soient $u \ge 1$ et $\theta \in]0,1[$ tels que $(1-\theta)u' < 1$. Alors sous les conditions (A_κ), (B), (C_θ), on a, pour $x \to +\infty$*

$$\Psi_{\mathcal{A}}(y) \ge (\varrho_{\theta,\kappa}(u) + o(1))|\mathcal{A}|,$$

*où $\varrho_{\theta,\kappa} > 0$ est explicite (voir [**[Mou24]**, Proposition 1.4]).*

Remarque 3.5.2. Le nombre $\varrho_{\theta,\kappa}(u)$ est défini par morceaux (selon la valeur de θ). Par la suite, on choisira

$$0 < \theta = \frac{1-\varepsilon}{k} < \frac{1}{2}.$$

Par conséquent, $\varrho_{\theta,\kappa}$ vaut

$$\varrho_{\theta,\kappa}(u) = \kappa(1 - (1-\theta)u)u^{\kappa-1}.$$

3.5.2. Preuve du Théorème 3.1.16

On pose

$$\mathcal{A} = \{F(n) \,:\, n \le x,\ s_q(n) \equiv a \pmod b\}.$$

On vérifie chaque hypothèse du Théorème 3.5.1, à commencer par le choix de θ. Soit $0 < \varepsilon < 1$. On prend

$$\theta = \frac{1-\varepsilon}{k} < 1.$$

Montrons que

$$(1-\theta)u' < 1. \tag{3.29}$$

On écrit

$$\begin{aligned}(1-\theta)u' &= \frac{k-1+\varepsilon}{k}\left(ku + \mathcal{O}\left(\frac{1}{\log y}\right)\right)\\ &(k-1+\varepsilon)\left(u + \mathcal{O}\left(\frac{1}{\log y}\right)\right)\\ &< (k-1+\varepsilon)\left(\frac{1}{k-1+2\varepsilon} + \mathcal{O}\left(\frac{1}{\log y}\right)\right)\\ &< 1,\end{aligned}$$

pour x assez grand. La condition (3.29) est vérifiée.

▶ Vérification de (A_κ) :
C'est une conséquence du Lemme 3.2.1 ($\kappa = 1$).

▶ Vérification de (B) :
Pour vérifier (B), on utilise le Lemme 3.2.2. Comme $D \neq 0$, on a, pour tout $\alpha > 0$

$$\omega(p^\alpha) = \varrho(p^\alpha) = |\{m \in \{0, \dots, p^\alpha - 1\},\ F(m) \equiv 0 \pmod{p^\alpha}\}| = \mathcal{O}_F(1).$$

▶ **Vérification de** (C_θ) **:**
L'hypothèse (C_θ) étant proche de l'hypothèse $(R(1,\alpha))$ de la section précédente, nous allons procéder de la même manière.

En utilisant le fait que

$$u < \frac{1}{k-1+2\varepsilon} = \mathcal{O}(1),$$

on a, pour x suffisamment grand,

$$y^{u'\theta} = y^{\theta(ku+\mathcal{O}(1/\log x))} = x^{\theta k}\exp(\mathcal{O}\,(1/u)) \leq x^{\theta k}x^{\varepsilon/2} = x^{1-\varepsilon/2}.$$

Ainsi,

$$\begin{aligned}\sum_{d\leq y^{u'\theta}}|r(\mathcal{A},d)| &\leq \sum_{d<x^{1-\varepsilon/2}}\left|\sum_{\substack{m=0\\ d|F(m)}}^{d-1}\left(\sum_{\substack{n\leq x\\ s_q(n)\equiv a \pmod b\\ n\equiv m \pmod d}} 1-\frac{x}{bd}\right)\right| \\ &\leq \sum_{d\leq x^{1-\varepsilon/2}}\varrho(d)\max_{0\leq m\leq d-1}\left|\sum_{\substack{n\leq x\\ s_q(n)\equiv a \pmod b\\ n\equiv m \pmod d}} 1-\frac{x}{bd}\right|.\end{aligned}$$

D'après la Proposition **3.2.3** et la Remarque **3.2.5**, on a donc

$$\sum_{d\leq y^{u'\theta}}|r(\mathcal{A},d)| \ll x^{1-\eta/2}\,(\log x)^{k^2D^4/2},$$

ce qui suffit pour conclure que l'hypothèse (C_θ) est vérifiée et que donc le Théorème **3.5.1** s'applique. Comme $\theta = \dfrac{1-\varepsilon}{k} < 1/2$ et $\kappa = 1$, alors [**[Mou24]**, Proposition 1.4, p.3] fournit la constante de minoration

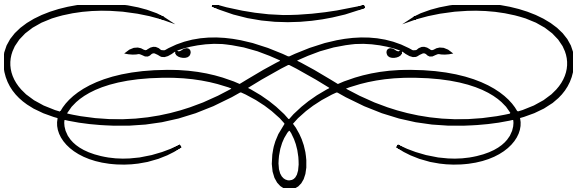
$$\varrho_{\theta,1}(u) := 1-(1-\theta)u'.$$

En utilisant **(3.28)**, on obtient

$$\begin{aligned}\varrho_{\theta,1}(u) &= 1-\left(\frac{k-1+\varepsilon}{k}\right)(ku+o(1)) \\ &= 1-(k-1+\varepsilon)u+o(1),\end{aligned}$$

ce qui achève la preuve du Théorème **3.1.16**.

Annexe A : Fractions de Farey



Les résultats suivants sont standard et se trouvent également (par exemple) dans le livre **[HW75]**. Les fractions de Farey interviennent dans la preuve de la généralisation de Spiegelhofer **[Spi20]**, présente dans le Chapitre 2.

Définition A.0.3 (Suite de Farey)**.** Soit $n \geq 1$ un entier. On appelle suite de Farey d'ordre n, notée $\mathcal{F}_n$, la suite formée des fractions irréductibles $0 \leq \frac{a}{b} \leq 1$ avec $b \leq n$. Deux fractions sont dites *voisines* dans la séquence $\mathcal{F}_n$ si elles sont consécutives dans $\mathcal{F}_n$.

Exemple A.0.4.

$$\begin{aligned}
\mathcal{F}_1 &= \left(\frac{0}{1}; \frac{1}{1}\right), \\
\mathcal{F}_2 &= \left(\frac{0}{1}; \mathbf{\frac{1}{2}}; \frac{1}{1}\right), \\
\mathcal{F}_3 &= \left(\frac{0}{1}; \mathbf{\frac{1}{3}}; \frac{1}{2}; \mathbf{\frac{2}{3}}; \frac{1}{1}\right), \\
\mathcal{F}_4 &= \left(\frac{0}{1}; \mathbf{\frac{1}{4}}; \frac{1}{3}; \frac{1}{2}; \frac{2}{3}; \mathbf{\frac{3}{4}}; \frac{1}{1}\right).
\end{aligned}$$

Remarque A.0.5. Par translation, on définit la suite de Farey d'ordre n sur $\mathbb{R}$, qu'on continuera de noter $\mathcal{F}_n$ par la suite.

Lemme A.0.6 (Point médian)**.** *Soient $\frac{a}{b} < \frac{c}{d}$ deux fractions irréductibles de dénominateurs positifs. Alors*

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}.$$

La fraction $\frac{a+c}{b+d}$ est appelée point médian des fractions $\frac{a}{b}$ et $\frac{c}{d}$.

Démonstration. La preuve se fait par équivalence. Montrons la première inégalité. La seconde se traite de la même manière.

$$\begin{aligned}
\frac{a}{b} < \frac{a+c}{b+d} &\iff a(b+d) < (a+c)b \\
&\iff ad < bc \\
&\iff \frac{a}{b} < \frac{c}{d},
\end{aligned}$$

ce qui est vrai par hypothèse. □

Proposition A.0.7 (Critère de Farey)**.** *Soient $\frac{a}{b} < \frac{c}{d}$ deux fractions de Farey voisines de $\mathcal{F}_n$. Alors,*

$$bc - ad = 1 \quad et \quad b + d > n.$$

De plus,

$$\frac{a+c}{b+d} - \frac{a}{b} < \frac{1}{bn}$$

et

$$\frac{c}{d} - \frac{a+c}{b+d} < \frac{1}{dn}.$$

Définition A.0.8. Soit $\alpha \in \mathbb{R}$ et soient $\frac{a}{b}, \frac{c}{d} \in \mathcal{F}_n$ deux fractions de Farey voisines. Supposons que

$$\frac{a}{b} \leq \alpha < \frac{c}{d}.$$

Si $\alpha \leq \frac{a+c}{b+d}$, alors on définit

$$\frac{P_n(\alpha)}{Q_n(\alpha)} = \frac{a}{b}.$$

Sinon, on définit

$$\frac{P_n(\alpha)}{Q_n(\alpha)} = \frac{c}{d}.$$

Proposition A.0.9 (Approximation des fractions de Farey)**.** *Pour $\alpha \in \mathbb{R}$ et pour $n \in \mathbb{N}$, on a*

$$|Q_n(\alpha)\alpha - P_n(\alpha)| < \frac{1}{n}.$$

Démonstration. Soit $\alpha \in \mathbb{R}$ et soient $\frac{a}{b}, \frac{c}{d} \in \mathcal{F}_n$ deux fractions voisines telles que :

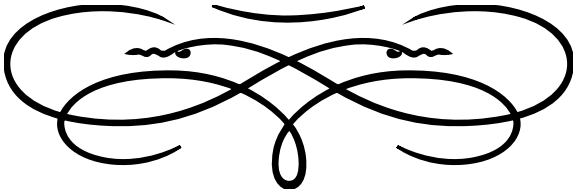
$$\frac{a}{b} \leq \alpha < \frac{c}{d}.$$

Supposons par exemple que $\alpha < \frac{a+c}{b+d}$, le cas $\alpha \geq \frac{a+c}{b+d}$ se traitant de la même manière. Alors $P_n(\alpha) = a$ et $Q_n(\alpha) = b$. De plus,

$$\begin{aligned} |Q_n(\alpha)\alpha - P_n(\alpha)| &= |b\alpha - a| \\ &= b\alpha - a \\ &< b\Big(\frac{a+c}{b+d}\Big) - a \\ &< b \times \Big(\frac{a+c}{b+d} - \frac{a}{b}\Big) \\ &< b \times \frac{1}{bn} = \frac{1}{n}. \end{aligned}$$

□

Annexe B : Discrépance d'un nombre réel



Définition B.0.10. Soient $\alpha \in \mathbb{R}$ et $N \geq 1$ un entier. La N-discrépance de α, notée $D_N(\alpha)$, est la quantité définie par

$$D_N(\alpha) = \sup_{\substack{0 \leq x \leq 1 \\ y \in \mathbb{R}}} \left| \frac{1}{N} \sum_{0 \leq n < N} \mathbb{1}_{[0,x[+y+\mathbb{Z}}(n\alpha) - x \right|.$$

La notion de N-discrépance apparaît naturellement dans le résultat suivant, utilisé par Müllner et Spiegelhofer **[MS17,** Lemma 3.3**]**.

Proposition B.0.11. *Soit J un intervalle de $\mathbb{R}$ contenant N entiers. Soit $\alpha, \beta \in \mathbb{R}$. Soient t, T, ℓ, L des entiers tels que be $0 \leq t < T$ et $0 \leq \ell < L$. Alors*

$$\left| \{ n \in J \ : \frac{t}{T} \leq \{n\alpha + \beta\} < \frac{t+1}{T}, \ \lfloor n\alpha + \beta \rfloor \equiv \ell \pmod{L} \} \right| = \frac{N}{LT} + \mathcal{O}\left(N D_N\left(\frac{\alpha}{L}\right)\right)$$

avec une constante implicite absolue.

Le lemme suivant fournit une majoration du nombre de $n < N$ tels que $\|n\alpha + \beta\|$ soit proche d'un entier. Il s'agit de l'analogue en base q des arguments donnés par Spiegelhofer **[Spi20,** p. 2575**]**. Ce lemme nous est utile lors de la phase de décalage des chiffres.

Lemme B.0.12. *Soient $N > 1$ un entier, $\sigma > 1$, $H \in \mathbb{N}$ tels ques $H < q^{\sigma-1}$. De plus, soient $\alpha, \beta \in \mathbb{R}$. On a*

$$|\{n \in \{0, \dots, N-1\} \ : \ \|n\alpha + \beta\| < H/q^\sigma\}| \leq N D_N(\alpha) + \frac{2HN}{q^\sigma}.$$

Démonstration. Ceci découle de translations élémentaires d'intervalles et de la défi-

nition de la discrépance, i.e

$$\begin{aligned}
&\left|\left\{n \in \{0,\dots,N-1\} \ : \ \|n\alpha+\beta\| < H/q^\sigma\right\}\right| \\
&\qquad = \left|\left\{n \in \{0,\dots,N-1\} \ : \ n\alpha+\beta \in (\mathbb{Z}+[-H/q^\sigma, H/q^\sigma])\right\}\right|, \\
&\qquad = \left|\left\{n \in \{0,\dots,N-1\} \ : \ n\alpha \in (\mathbb{Z}+[0,2H/q^\sigma]-\beta-H/q^\sigma)\right\}\right| \\
&\qquad \leq \frac{2HN}{q^\sigma} + ND_N(\alpha).
\end{aligned}$$

□

Comme chaque décalage de chiffre introduit un terme d'erreur faisant intervenir la discrépance, et que nous effecturons $(k-1)$ tels décalages dans CHAPITRE 2, le lemme suivant sera utilisé pour estimer l'erreur globale engendrée par ces décalages successifs. La démonstration se trouve dans l'article de Müllner et Spiegelhofer **[MS17,** Lemma 3.4, p.704**]** pour $q=2$, mais elle reste valable pour tout $q \geq 2$ (avec les modifications évidentes à apporter à la preuve).

Proposition B.0.13. *Soit $q \geq 2$. Il existe une constante absolue $C>0$ telle que pour tout $m, n, N \in \mathbb{N}$ on a*

$$\sum_{0 \leq d < q^m} D_N\left(\frac{d}{q^m}\right) \leq C\,\frac{N+q^m}{N}(\log^+ N)^2.$$

Annexe C : Propriétés de la fonction partie entière

Cette annexe met en lumière certaines propriétés de la fonction partie entière. Ces dernières, très pratiques, sont présentées dans [**[Spi20]**, Lemma 4.1].

Proposition C.0.14. *On a les propriétés suivantes :*

(1) Soit $0 < \varepsilon \leq \frac{1}{2}$. *On suppose que* $a, b \in \mathbb{R}$ *vérifient* $\|a\| < \varepsilon$ *et* $\|b\| \geq \varepsilon$. *Alors,*

$$\lfloor a+b \rfloor = \left\lfloor a + \frac{1}{2} \right\rfloor + \lfloor b \rfloor. \tag{C.30}$$

(2) Pour tout $a \in \mathbb{R}$ *et* $n \in \mathbb{N}$, *on a :*

$$\|na\| \leq n\|a\|. \tag{C.31}$$

(3) Soient $a \in \mathbb{R}$, $\varepsilon > 0$ *et* $n \in \mathbb{N}$ *tels que* $\|a\| < \varepsilon$ *et* $2n\varepsilon < 1$. *Alors :*

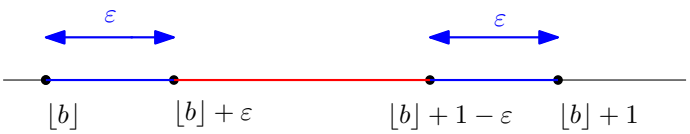
$$\langle na \rangle = n\langle a \rangle. \tag{C.32}$$

Démonstration. Montrons chaque point.

▶ Preuve de (C.30)

D'une part, la condition $\|b\| \geq \varepsilon$ se traduit par :

$$\lfloor b \rfloor + \varepsilon \leq b \leq \lfloor b \rfloor + 1 - \varepsilon.$$



On traduit ensuite la condition $\|a\| < \varepsilon$.
Deux cas se présentent.

▷ Cas 1 : $\lfloor a \rfloor \leq a < \lfloor a \rfloor + \varepsilon$.
Dans ce cas,

$$\left\lfloor a + \frac{1}{2} \right\rfloor = \lfloor a \rfloor.$$

Ainsi,

$$\lfloor a \rfloor + \lfloor b \rfloor + \varepsilon \leq a + b < \lfloor a \rfloor + \varepsilon + \lfloor b \rfloor + 1 - \varepsilon.$$

Donc,

$$\lfloor a \rfloor + \lfloor b \rfloor \leq a + b < \lfloor a \rfloor + \lfloor b \rfloor + 1,$$

d'où l'égalité souhaitée.

▷ Cas 2 : $\lfloor a \rfloor + 1 - \varepsilon < a < \lfloor a \rfloor + 1$.
Dans ce cas,

$$\left\lfloor a + \frac{1}{2} \right\rfloor = \lfloor a \rfloor + 1.$$

D'autre part,

$$\lfloor a \rfloor + 1 + \lfloor b \rfloor < a + b < \lfloor a \rfloor + 1 + \lfloor b \rfloor + 1 - \varepsilon.$$

Donc :

$$\lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor + 1,$$

d'où l'égalité souhaitée.

► Preuve de (C.31)

Soit $m \in \mathbb{Z}$. On a :

$$n|a - m| = |na - nm| \geq \min_{x \in \mathbb{Z}} |na - x|.$$

Il suffit de passer au min à gauche de l'inégalité.

► Preuve de (C.32)

On traduit à nouveau la condition $\|a\| < \varepsilon$.

▷ Cas 1 : $\lfloor a \rfloor \leq a < \lfloor a \rfloor + \varepsilon$.
En multipliant chaque membre de cette inégalité par n et en ajoutant à chaque membre $\frac{1}{2}$, il vient que :

$$n\lfloor a \rfloor + \frac{1}{2} \leq na + \frac{1}{2} < n\lfloor a \rfloor + \underbrace{\underbrace{n\varepsilon}_{<\frac{1}{2}} + \frac{1}{2}}_{<1}.$$

Ainsi,

$$< na >= \left\lfloor na + \frac{1}{2} \right\rfloor = n \underbrace{\lfloor a \rfloor}_{=<a>}.$$

▷ Cas 2 : $\lfloor a \rfloor + 1 - \varepsilon \leq a < \lfloor a \rfloor + 1$.
En multipliant chaque membre de cette inégalité par n et en ajoutant à chaque membre $\frac{1}{2}$, il vient que :

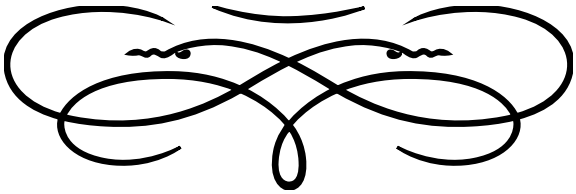
$$n\lfloor a \rfloor + n \underbrace{-n\varepsilon + \frac{1}{2}}_{>0} \leq na + \frac{1}{2} < n\lfloor a \rfloor + n + \frac{1}{2}.$$

Ainsi,

$$< na >= \lfloor na + \frac{1}{2} \rfloor = n(\underbrace{\lfloor a \rfloor + 1}_{=<a>}).$$

□

Bibliographie



[AS99] J.-P. Allouche, J. O. Shallit. The ubiquitous Prouhet–Thue–Morse sequence. In : *Sequences and their Applications (Singapore,1998)*, Springer Ser. Discrete Math. Theor. Comput. Sci. (1999), 1–16. doi:10.1007/978-1-4471-0551-01

[BS48] R. Bellman, H. N. Shapiro. On a problem in additive number theory. *Ann. of Math. 49* (1948), 333–340. doi:10.2307/1969281

[Bes71] J. Bésineau. Indépendance statistique d'ensembles liés à la fonction « Somme des chiffres ». *Séminaire de théorie des nombres* (**19**) (1971), no. 19, 1–20. https://www.numdam.org/item/STNB1970-1971A190/

[Bom65] E. Bombieri. On the large sieve. *Mathematika, Lond.* (**12**) (1965), no.201–225. doi:10.1112/S0025579300005313

[Bre15] R. de la Bretèche. Greatest first prime factor of values of entire polynomials (with an appendix written with Jean-François Mestre). (Plus grand facteur premier de valeurs de polynômes aux entiers.) *Acta Arith.* **169** (2015), no.3, 221–250. http://eudml.org/doc/279316

[DLBD20] R. de la Bretèche, S. Drappeau. Level of distribution of quadratic polynomials and an upper bound sieve for friable integers. (Niveau de répartition des polynômes quadratiques et crible majorant pour les entiers friables.) *J. Eur. Math. Soc. (JEMS)* **22** (2020), no.5, 1577–1624. doi:10.4171/JEMS/951

[BKM23] J. Byszewski, J. Konieczny, C. Müllner. Gowers norms for automatic sequences. *Discrete Anal.* **62** (2023), no.4. doi:10.19086/da.75201

[Coq79] J. Coquet. Corrélation de suites arithmétiques. Séminaire Delange-Pisot-Poitou. Théorie des nombres **20** (1978-1979), no.1, Exposé no.1. https://www.numdam.org/item/SDPP1978-1979201A110/

[Dar15] C. Dartyge. Le problème de Tchébychev pour le douzième polynôme cyclotomique. *Proc. Lond. Math. Soc. (3)* **111** (2015), no.1, 1–62. doi:10.1112/plms/pdv001

[DMT01] C. Dartyge, G. Martin, G. Tenenbaum. Polynomial values free of large prime factors. *Period. Math. Hung.* **43** (2001), no.1–2, 117–119. doi:10.1023/A:1015237700066

[DM25] C. Dartyge, J. Maynard. On the largest prime factor of quartic polynomial values : the cyclic and dihedral cases. *J. Eur. Math. Soc.* (2025), publié en ligne. doi:10.4171/JEMS/1586

[DT06] C. Dartyge, G. Tenenbaum. Congruences de sommes de chiffres de valeurs polynomiales. *Bull. Lond. Math. Soc.* **38** (2006), no.1, 61–69. doi:10.1112/S0024609305017789

[DT05] C. Dartyge, G. Tenenbaum. Sums of digits of multiples of integers. (Sommes des chiffres de multiples d'entiers.). *Ann. Inst. Fourier* **55** (2005), no.7, 2423–2474. doi:10.5802/aif.2166

[DDMSS22] J.-M. Deshouillers, M. Drmota, C. Müllner, A. Shubin, L. Spiegelhofer. Synchronizing automatic sequences along Piatetski-Shapiro sequences. *Isr. J. Math.* **269** (2025), no.1, 103–141. doi:10.1007/s11856-025-2755-9

[DI82] J.-M. Deshouillers, H. Iwaniec. On the greatest prime factor of n^2+1. *Ann. Inst. Fourier* **32** (1982), no.4, 1–11. doi:10.5802/aif.891

[DMR11] M. Drmota, C. Mauduit, J. Rivat. The sum-of-digits function of polynomial sequences. *J. Lond. Math. Soc., II. Ser.* **84** (2011), no.1, 81–102. doi:10.1112/jlms/jdr003

[DR05] M. Drmota, J. Rivat. The sum-of-digits function of squares. *J. Lond. Math. Soc., II. Ser.* **72** (2005), no.3, 273–292. doi: 10.1112/S0024610705006769

[Erd52] P. Erdős. On the greatest prime factor of $\prod_{k=1}^{n} f(k)$. *J. Lond. Math. Soc.* **27** (1952), 379–384. doi:10.1112/jlms/s1-27.3.379

[Erd90] P. Erdős, A. Schinzel. On the greatest prime factor of $\prod_{k=1}^{n} f(k)$. *Acta Arith.* **55** (1990), no.2, 191–200. doi:10.4064/aa-55-2-191-200

[Fou85] E. Fouvry. Sur le problème des diviseurs de Titchmarsh. *J. Reine Angew. Math.* **352** (1985), 51–76. doi:10.1515/crll.1985.357.51

[FM96a] E. Fouvry, C. Mauduit. Sums of digits and almost primes. *Math. Ann.* **305** (1996), no. 3, 571–599. doi:10.1007/BF01444238

[FM96b] E. Fouvry, C. Mauduit. Méthodes de crible et fonctions sommes des chiffres. *Acta Arith.* **77** (1996), no.4, 339–351. doi:10.4064/aa-77-4-339-351

[Gel68] A. Gelfond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arith.* **13** (1968), no.3, 259–265. doi:10.4064/aa-13-3-259-265

[Gow01] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.* **11** (2001), no. 3, 465–588. doi:10.1007/s00039-001-0332-9

[GK91] S. W. Graham, G. Kolesnik. Van der Corput's Method of Exponential Sums. *Cambridge University Press*, 1991. isbn:0-521-33927-8

[GM25] L. Grimmelt, J. Merikoski. On the greatest prime factor and uniform equidistribution of quadratic polynomials. *prépublication*, (2025). arXiv:2505.00493

[HR13] H. Halberstam, H.-E. Richert. Sieve methods. *Dover Publications* (2013). isbn:9780486320809

[HW75] G. H. Hardy, E. M. Wright. An Introduction to the Theory of Numbers. *Oxford, fourth edition* (1975). doi:10.1017/S0013091500002820

[Hea01] D. R. Heath-Brown. The largest prime factor of x^3+2. *Proc. London Math. Soc.* **82** (2001), no.3, 554–596. doi:10.1515/crll.1998.053

[Hoo67] C. Hooley. On the greatest prime factor of a quadratic polynomial. *Acta Math.* **117** (1967), 281–299. doi:10.1112/plms/82.3.554

[Hoo78] C. Hooley. On the greatest prime factor of a cubic polynomial. *J. Reine Angew. Math.* **303**/**304** (1978), 21–50. doi:10.1515/crll.1978.303-304.21

[Irv15] A. J. Irving. The largest prime factor of x^3+2. *Acta Arith.* **171** (2015), no.1, 67–80. doi:10.4064/aa171-1-5

[Jel25] P. Jelinek. Gowers norms for linearly recurrent numeration systems. *prépublication* (2025). arXiv:2510.16947

[Kim99] D. Kim. On the Joint Distribution of q-Additive Functions in Residue Classes. *Journal of Number Theory*, **74** (1999), no.2, 307–336. doi:10.1006/jnth.1998.2327

[Kon19] J. Konieczny. Gowers norms for the Thue–Morse and Rudin–Shapiro sequences. *Ann. Inst. Fourier*, **69** (2019), no.4, 1897–1913. doi:10.5802/aif.3285

[KI04] E. Kowalski, H. Iwaniec. Analytic Number Theory. *American Mathematical Society* **53** (2004). pp–615.

[Mar95] A. A. Markov. Über die Primteiler des Zahlen von der Form $1+4x^2$. *Bull. Acad. Sci. St. Petersburg* **3** (1895), 55–59.

[MMR14] B. Martin, C. Mauduit, J. Rivat. Théorème des nombres premiers pour les fonctions digitales. *Acta Arith.* **165** (2014), no.1, 11–45. doi:10.4064/AA165-1-2

[MR95] C. Mauduit, J. Rivat. Répartition des fonctions q-multiplicatives dans la suite $([n^c])_{n\in\mathbb{N}}$, $c > 1$. *Acta Arith.* **71** (1995), no.2, 171–179. doi:10.4064/AA100-2-2

[MR10] C. Mauduit, J. Rivat. Sur un problème de Gelfond : la somme des chiffres des nombres premiers. *Ann. Math. (2)* **171** (2010), no.3, 1591–1646. doi:10.4007/annals.2010.171.1591

[MR09] C. Mauduit, J. Rivat. The sum of digits of squares. *Acta Math.* **203** (2009), no.1, 107–148. doi:10.1007/s11511-009-0040-0

[Mer23] J. Merikoski. On the largest prime factor of n^2+1. *J. Eur. Math. Soc (JEMS)* **25** (2023), no.4, 1253–1284. doi:10.4171/JEMS/1216

[Mou24] A. Mounier. Un crible minorant effectif pour les entiers friables. *Acta Arith.* **220** (2025), 121–159. doi:10.4064/aa240514-8-4

[MS17] C. Müllner and L. Spiegelhofer. Normality of the Thue–Morse sequence along Piatetski–Shapiro sequences. II. *Israel J. Math.* **220** (2017), no.2, 691–738. doi:10.1007/s11856-017-1531-x

[Nag21] T. Nagel. Généralisation d'un théorème de Tchebycheff. *Journ. de Math.*, **8** (1921), no.4, 343–356. issn:0021-7874

[Nag51] T. Nagel. Introduction to Number Theory. *Uppsala : Almquist & Wiksell Boktryckeri* (1951). isbn:0821828339

[Pas25] A. Pascadi. Large sieve inequalities for exceptional Maass forms and the greatest prime factor of $n^2 + 1$. *Forum Math. Pi*, publié en ligne. doi:10.1017/fmp.2026.10025

[Que79] M. Queffélec. Mesures spectrales associées à certaines suites arithmétiques. *Bull. Soc. Math. France* **107** (1979), 385–421. doi:10.1017/fmp.2026.10025

[Ric69] H.-E. Richert. Selberg's sieve with weights. *Mathematika*, **16** (1969), no.1, 1–22. doi:10.24033/bsmf.1903

[Rot53] K. F. Roth. On certain sets of integers. *J. Lond. Math. Soc.* **28** (1953), 104–109. doi:10.1112/jlms/s1-28.1.104

[Ser78] J.-P. Serre. A course in arithmetic. *Graduate Texts in mathematics* **7**, Springer-Verlag. (1978). doi:10.1007/978-1-4684-9884-4

[Sha23] A. Shubin. Möbius orthogonality of Thue-Morse sequence along Piatetski-Shapiro numbers, *Stud. Math.* **273** (2023), no.3, 201–238. doi:10.4064/sm220818-3-8

[Spi20] L. Spiegelhofer. The level of distribution of the Thue–Morse sequence. *Compositio Math.* **156** (2020), no.12, 2560–2587. doi:10.1112/S0010437X20007563

[Spi23] L. Spiegelhofer. Thue–Morse along the sequence of cubes, *prépublication* (2023+) arXiv: 2308.09498

[Sto11] T. Stoll. The sum of digits of polynomial values in arithmetic progressions. *Funct. Approx. Comment. Math.* **47** (2011), no.2, 233–239. doi:10.7169/facm/2012.47.2.7

[Sze75] E. Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* **27** (1975), 299–345. doi:10.4064/aa-27-1-199-245

[Tao12] T. Tao. Higher order Fourier analysis. *Graduate Studies in Mathematics* **142** (2012). isbn:978-0-8218-8986-2/hbk

[Ten90] G. Tenenbaum. Sur une question d'Erdős et Schinzel II. *Invent. Math.* **99** (1990), no.1, 215–224. doi:10.1007/BF01234418

[Tou25] N. Toumi. The level of distribution of the sum-of-digits function in arithmetic progressions. *Int. J. Number Theory* **21** (2025), no.10, 2359–2426. doi:10.1142/S1793042125501155

[Tou26+] N. Toumi. Valeurs polynomiales sous contraintes digitales. *soumis le 15/12/2025* (2026+) hal-05558269.

[Vin65] A. I. Vinogradov, The density hypothesis for Dirichet L-series. *Izv. Akad. Nauk SSSR, Ser. Mat.* **29** (1965), no.4, 903–934. doi:10.1142/97898127766000019.

[Wal35] A. Walfisz. Zur additiven Zahlentheorie. II. (German). *Math. Z* **40** (1935), 592–607. doi:10.1007/BF01218882