Propriétés multiplicatives d'entiers soumis à des conditions digitales

Sylvain Col

UFR S.T.M.I.A.
École Doctorale IAE + M
Université Henri Poincaré - Nancy I
D.F.D. Mathématiques

Thèse

présentée pour l'obtention du titre de

Docteur de l'Université Henri Poincaré, Nancy-I

en Mathématiques

par

Sylvain Col

Propriétés multiplicatives d'entiers soumis à des conditions digitales

Soutenue publiquement le 22 Juin 2006

Membres du jury :		
M. Gérald Tenenbaum	Professeur à l'université Henri Poincaré	Nancy
M. Joël Rivat	Professeur à l'université de la Méditerranée	Marseille
M^{me} Cécile Dartyge	Maître de conférence à l'université Henri Poincaré	Nancy
Rapporteurs :		
M. Jean-Paul Allouche	Directeur de recherches à l'université Paris-Sud	Orsay
M. François Hennecart	Professeur à l'université Jean Monnet	Saint-Étienne
M. Christian Mauduit	Professeur à l'université de la Méditerranée	Marseille

Institut Élie Cartan Nancy, Laboratoire de Mathématiques, B.P. 239, 54506 Vandœuvre-lès-Nancy Cedex

Ta main capture mes paroles intactes,
Nos discussions gouvernent mes actes,
Tes soirées embrasent mes matinées,
Offrant à mes rêves leur destinée.

À Marie-Amélie

Moment traditionnel par excellence, remercier ceux ayant participé à l'élaboration d'une œuvre, les mains de l'ombre ayant porté le travail en pleine lumière et aujourd'hui entre vos mains, reste néanmoins une épreuve, peut-être par peur d'oublier quelqu'un, ou de se tromper sur ce qu'il faut conserver de quatre années, ou de ne plus être le même une fois la dernière pierre de l'œuvre posée. Si chaque instant passé à l'Institut Élie Cartan ne fut pas nécessairement merveilleux, le souvenir global reste inoubliable : tant de rencontres, de discussions et d'échanges avec des personnes de tout horizon, tant d'amitiés, d'unités et de groupes créés sur des thèmes tous différents, tant de joie, de bonheur et de plaisirs même dans les instants les plus inattendus, garnissent l'intégralité de ma mémoire qu'il me semble impossible de me souvenir du reste.

Quelle ne fut pas ma surprise la première fois où je découvris mon sujet : ésotérique certainement, intéressant encore plus, inquiétant peut-être. Dans le bureau de Joël Rivat, Cécile Dartyge m'emmena pour la première fois aux portes d'un monde inconnu, rempli de nombres étranges, de nombres rares, de nombres cachés, et pourtant de nombres si simples que les seuls chiffres 0 et 1 nous suffisent pour tous les énumérer ! Les lumières de ces nombres *ellipséphiques* envahirent rapidement la pièce, nous enveloppant et nous liant tel un pacte sur lequel je déposais mon sceau, franchissant les portes jusqu'alors totalement verrouillées.

Est-ce de la numérologie ? Que nenni ! Combien de temps je partageai leurs mystères et leurs magies grâce à vous, Cécile Dartyge, trop certainement, mais uniquement car le temps passe trop vite lorsqu'on est bien occupé. Merci de m'avoir accompagné sur cette piste : par vos conseils et votre disponibilité, n'hésitant pas à reprendre le baton de guide si je m'égarais trop, je réussis à pénétrer et étudier ce lieu, à éviter d'inutiles détours et embûches et à avancer tout au long du chemin. Mais si je vous remercie aujourd'hui, c'est surtout pour ce jour où, à Marseille, vous m'avez parlé d'un autre monde, encore presque vierge, celui des palindromes. Cette suggestion d'étudier une autre piste, cette confiance dans mes capacités à construire seul mon chemin, m'incitèrent à travailler jour et nuit pour percer le voile. Et je suis fier d'avoir été votre élève dans cette quête.

Ce travail existe aussi grâce à vous, Joël Rivat. Vos remarques ont construit cette thèse et imprègnent les fondations de toute la partie analytique. Il en est de même du travail de rédaction, tâche m'ayant presque fait baisser les bras. Si ces travaux ont pu enfin naître un jour, c'est bien grâce à votre main. Certes il me fallut plus de temps pour vous connaître, mais si je vous remercie aujourd'hui, c'est surtout pour deux autres

raisons : déjà de m'avoir permis de voyager, notamment au CIRM de Luminy, me permettant ainsi de me promener régulièrement dans un des plus beaux paysages de France : si les randonnées en montagne sont devenues une de mes passions, c'est un peu de votre faute ! Et aussi de rencontrer les plus grands mathématiciens, voire même de les inviter au restaurant, bref des moments merveilleux où j'ai vécu dans la communauté mathématique.

Rechercher au sein de l'Institut, secondé par un personnel toujours disponible, fut un honneur et dire que je suis reconnaissant pour la bonne ambiance et les conditions de travail optimales est une litote. Je remercie ceux avec qui j'ai partagé le lieu, notamment Gérald Tenenbaum et Jie Wu pour nos discussions tant mathématiques, philosophiques que littéraires.

Je remercie tout autant l'équipe de l'Institut de Mathématiques de Luminy qui m'a accueilli si souvent lors de mes déplacements à Marseille toujours chaleureusement et tout particulièrement vous, Christian Mauduit, pour vos encouragements, votre confiance dans mes idées et votre présence à ma thèse comme rapporteur.

J'exprime également toute ma reconnaissance à Jean-Paul Allouche et François Hennecart d'avoir été les deux autres rapporteurs de cette thèse. Pour votre gentillesse, vos conseils et le suivi régulier de l'avancement de mes recherches, merci à Andras Sárközy.

Comment surtout oublier le groupe si soudé des doctorants qui s'est forgé à Nancy ? Je ne citerais pas tout le monde, mais je ne peux oublier Sergio Bezerra dont j'ai partagé durant trois années le bureau 225, même si nous nous voyions plus souvent au dehors qu'au dedans ; Pierre Le Gall : ta passion si communicative dans des sujets qui m'auraient laissé de marbre, m'a permis d'oublier bien des mauvais moments ; Hermann Woehrel : discuter avec toi est toujours un plaisir et si *dispute* possède toujours son sens originel, tu n'y es pas totalement étranger ; Marie-Amélie Lawn : ta disponibilité, ta bonne humeur et le voile de mystère dont tu te pares t'ont fait vivre dans nombre de mes rêves. Si cette thèse a finalement été déposée, c'est par l'entremise de ta main : une promesse est une promesse et j'ai eu la joie de la tenir.

Pour les sorties si conviviales que nous avons organisées en lieu et place de formations souvent monotones, j'adresse une pensée toute particulière à l'équipe de l'association d'Alma-Mater dont la charge du journal, *Le Pont de l'Alma*, m'échut durant quatre années, et notamment à Nathalie Grova la présidente, Bruno Martin un ami de longue date et Sandra Monteiro, très chère à mon cœur.

Indéfectible, même au cours des plus difficiles périodes, ma famille m'a toujours aidé et je vous en remercie du plus profond de mon cœur. J'y joins aussi Benoît Madrid : même si nous ne nous sommes rencontrés physiquement qu'une fois, de tous mes amis, tu es le seul à me connaître entièrement et à connaître aussi bien Elligain que moi.

En résumé, ce périple dans le monde des nombres ellipséphiques et palindromiques s'est réduit, par votre présence à toutes et à tous, en une promenade… bien trop courte !

Table des matières

Chapitre 1

Introduction

1.1 Généralités

L'étude des propriétés arithmétiques des entiers se retrouve déjà chez les mésopotamiens. À l'origine, les recherches portaient sur les propriétés de certains entiers remarquables. De nombreux mythes, croyances et même religions gardent encore aujourd'hui des traces de ces nombres remarquables. Par exemple, un entier est dit *parfait* s'il est égal à la somme de ses parts aliquotes (*i.e.* de ses diviseurs propres). Ainsi, les entiers parfaits inférieurs à 10 000 sont 6, 28, 496 et 8 128 et dans la religion chrétienne, Dieu créa le monde en six jours. Ce choix du nombre 6 peut sembler anecdotique, mais il est intimement lié au nombre parfait 6 : le monde doit être parfait puisque 6 est parfait ([Rib04, p. 72])... Autre exemple, on attribue à Pythagore la maxime : *un ami est celui qui est l'autre comme sont 220 et 284* (chacun de ces nombres est la somme des parts aliquotes de l'autre) et ces deux nombres sont un signe d'amour dans des horoscopes. Plus tard, des auteurs sont même allés jusqu'à affirmer pouvoir comprendre le monde en comprenant simplement les propriétés arithmétiques des entiers ! Certains mythes associés aux nombres ont laissé des traces qui perdurent encore aujourd'hui : le vocabulaire concernant les nombres comprend les épithètes *parfaits*, *amicaux*, *aimables*, *et cetera*, pour désigner certaines propriétés des entiers.

Certains entiers, les nombres premiers, peuvent être considérés comme étant à l'origine des autres entiers et leur connaissance représente le *Graal* pour les théoriciens des nombres. Un entier est dit premier s'il possède exactement deux diviseurs (lui-même et 1). Une de leurs particularités fondamentales est que tout entier se décompose de manière essentiellement unique en un produit de facteurs premiers. Malheureusement, la recherche des nombres premiers est une quête ardue (trop ?) et même si les grecs savaient depuis Euclide prouver qu'il en existe une infinité et possédaient depuis Érathostène un algorithme particulièrement performant pour les découvrir, algorithme encore utilisé deux mille ans plus tard par Fermat puis Gauß dans leur temps libre pour étendre la table des nombres premiers connus, les moindres progrès sont rarissimes et toujours très douloureux.

Plusieurs mathématiciens ont cherché à comprendre les propriétés arithmétiques parfois surprenantes des entiers possédant une écriture particulière et le lien de ces entiers avec d'autres concepts, en particulier la géométrie. Ainsi, Fermat s'est intéressé aux nombres de la forme $2^{2^n}+1$ (pour $n \geqslant 1$) et a émis l'hypothèse que chacun de ces nombres est un nombre premier. Nous savons depuis Euler que cela n'est pas vrai puisque

$$2^{2^5} + 1 = 641 \cdot 6\,700\,417$$

et nous pensons même qu'il n'existe qu'un nombre fini d'entiers de Fermat qui sont premiers. Les nombres de Fermat sont liés à la possibilité de construire à la règle et au compas les polygones réguliers (résultat obtenu grâce à la théorie de Galois). Un autre exemple est Mersenne qui s'est intéressé aux nombres premiers dont l'écriture en base 2 n'utilise que le chiffre 1 *i.e.* les nombres de la forme $M_n := 2^n - 1$. Il est aisé de remarquer que n doit être premier pour que M_n le soit. Euclide avait déjà prouvé que si M_p est premier, alors l'entier $2^{p-1}M_p$ est un nombre parfait pair puis Euler a montré réciproquement que tout entier parfait pair se décompose sous la forme $2^{p-1}M_p$ où M_p est un nombre de Fermat premier *i.e.* leur écriture en base 2 comporte p chiffres 1 suivis de $p-1$ chiffres 0 :

$$6 = \overline{110}, \quad 28 = \overline{11100}, \quad 496 = \overline{111110000}, \quad 8128 = \overline{1111111000000}, \ldots$$

La connaissance des nombres premiers de Mersenne est donc rigoureusement équivalente à celle des entiers parfaits pairs. Comme nous pensons aujourd'hui qu'il existe une infinité de nombres premiers de Mersenne, il existerait une infinité de nombres parfaits.

La difficulté de la recherche de nombres premiers dans des suites du type précédent provient de l'extrême dispersion de leurs éléments. Par exemple seuls $O(\log x)$ nombres jusque x sont de Mersenne. D'autres types de contraintes donnent naissance à des suites plus denses dans lesquelles nous aurons plus de chances de trouver des nombres premiers. Ainsi, Dirichlet a montré l'existence d'une infinité de nombres premiers en progression arithmétique ($p \equiv a \mod q$). Ce résultat, précisé ultérieurement par un théorème de Siegel et Walfisz (voir par exemple [Ten95, paragraphe III.2.3]) dont il sera abondamment question dans la suite, concerne une suite de densité positive, possédant $\frac{x}{q} + O(1)$ éléments jusqu'à x. Pour étudier le cas d'une suite de densité nulle, Piatetski-Shapiro [Pia53] a montré l'existence d'une infinité de nombres premiers de la forme $p = \lfloor n^\alpha \rfloor$ avec $\alpha < \alpha_0 = 1 + \frac{1}{11}$. Cette suite possède $O(x^{1/\alpha})$ éléments jusqu'à x. La borne α_0 a ensuite été augmentée plusieurs fois, notamment par Kolesnik [Kol67], Heath-Brown [HB83], et Rivat-Sargos [RS01]. Pour obtenir des nombres premiers dans une suite encore plus rare, Fouvry et Iwaniec [FI97], s'inspirant d'un résultat de Fermat qui a caractérisé les nombres premiers qui sont somme de deux carrés, ont montré l'existence d'une infinité de nombres premiers de la forme $m^2 + n^2$ avec n premier. Friedlander et Iwaniec [FI98b, FI98a] ont ensuite montré l'existence d'une infinité de nombres premiers de la forme $m^2 + n^4$ et Heath-Brown [HB01] de la forme $m^3 + 2n^3$. Cette dernière suite comporte seulement $O(x^{2/3})$ éléments jusqu'à x.

La rareté de la suite considérée n'est pas le seul critère de difficulté. Ainsi, pour le problème des nombres premiers jumeaux, qui consiste à rechercher des nombres premiers dans la suite $p+2$ où p est premier, aucun progrès n'a été réalisé, bien que cette suite comporte asymptotiquement $O(\frac{x}{\log x})$ éléments jusqu'à x. La difficulté de trouver des nombres premiers est si grande que l'on a été amené à introduire les nombres *presque premiers i.e.* les nombres possédant au plus k facteurs premiers, k étant un paramètre à choisir le plus petit possible. Ainsi Chen a réussi à établir qu'il existe une infinité de nombres premiers p tels que $p+2$ possède au plus deux facteurs premiers. Dans le même esprit, dans le cadre des suites polynomiales, Iwaniec (1978) a montré l'existence d'une infinité de nombres de la forme n^2+1 avec au plus deux facteurs premiers.

Étant donné un paramètre y, nous pouvons toujours décomposer de façon unique un entier n sous la forme $n = ab$ où a regroupe tous les facteurs premiers de n inférieurs à y et b ceux supérieurs à y. La stratégie pour chercher des entiers presque premiers consiste souvent à imposer $a = 1$ dans la décomposition précédente. Il est naturel de regarder le problème symétrique consistant à imposer $b = 1$. Les entiers de cette forme ne possèdent pas de grands facteurs premiers et ils sont appelés *friables*. Cette notion a permis à H. Daboussi de donner une nouvelle démonstration élémentaire du théorème des nombres premiers ([MFT97]). Les entiers friables interviennent aussi en cryptographie car le système de codage R.S.A., souvent utilisé aujourd'hui, pourrait être cassé si la clé utilisée était le successeur d'un entier friable. Ces dernières années, à la suite de travaux de R. de la Bretèche, A. Hildebrand et G. Tenenbaum notamment, leur étude systématique est devenue une part importante de la théorie analytique des nombres. Ces entiers peuvent en effet être utilisés par exemple pour limiter le phénomène de Gibbs lors de l'approximation d'une fonction périodique par sa série de Fourier ou plus généralement, pour approcher une série par la « série partielle » restreinte aux entiers friables en offrant une approximation de meilleure qualité que l'approximation usuelle par la somme partielle.

Étant donnée une suite *éparse*, nous pouvons résumer les questions que l'on peut se poser habituellement de la manière suivante :

1. Cette suite comporte-t-elle une infinité de nombres premiers ou au moins une infinité de nombres presque premiers ? Dans l'affirmative, en quelle proportion ?
2. Dans cette suite, existe-t-il des entiers friables, c'est-à-dire des entiers sans grand facteur premier ? Dans l'affirmative, en quelle proportion ?
3. Ces suites d'entiers sont-elles bien réparties dans les progressions arithmétiques et pour quelles tailles du module ?

Dans les résultats cité ci-dessus, les suites étaient plus ou moins éparses, mais la contrainte sur les nombres premiers ou presque premiers recherchés était de nature essentiellement polynômiale (hormis le cas des nombres premiers jumeaux). Des suites définies par d'autres types de contraintes ont également été étudiées, notamment des contraintes de nature digitale. La première étude de ce type est due à N. J. Fine

puis à A. O. Gelfond qui ont prouvé que la suite des entiers dont la somme des chiffres appartient à une classe de congruence fixée est équirépartie dans les progressions arithmétiques. Puis C. Mauduit et A. Sárközy ont étudié la répartition des entiers dont la somme des chiffres est fixée. Une des différences fondamentales entre ces deux suites est la rareté de la suite considérée : dans le premier cas, la suite a une densité positive alors que dans le second elle est de densité nulle. Ensuite, P. Erdös, C. Mauduit et A. Sárközy ont étudié les entiers dont l'écriture dans la base fixée n'utilise que les chiffres d'une famille donnée, comme exemple d'une suite d'entiers encore plus rare équidistribuée dans les progressions arithmétiques. C. Mauduit les a baptisés entiers *ellipséphiques* en référence à la superposition des deux mots grecs, ελλιπτικος (littéralement *elliptique*) et ψνηον (littéralement *petit caillou poli par l'eau* ; ces cailloux étaient notamment utilisés pour voter et réaliser les calculs) et signifie *qui a des chiffres manquants*. Parmi les entiers ellipséphiques remarquables, mentionnons les entiers de Mersenne écrits en base 2 qui sont exactement la famille de tous les entiers ellipséphiques utilisant seulement le chiffre 1.

Les entiers ellipséphiques ne forment pas seulement une suite éparse mais présentent aussi la difficulté d'avoir une structure particulièrement chaotique. Par exemple les entiers ellipséphiques en base 3 associés à la famille de chiffres $\{0, 2\}$ possèdent une répartition totalement irrégulière calquée sur celle de l'ensemble de Cantor (une fois l'échelle réduite). Leur étude reste cependant possible car leur fonction génératrice se factorise complètement, ce qui permet d'isoler les irrégularités. Plusieurs études ont été menées sur les entiers ellipséphiques, notamment par W. D. Banks, J. Coquet, C. Dartyge, P. Erdös, M. Filaseta, S. Konyagin, C. Mauduit, A. Sárközy et I. E. Sparinski ([EMS98, EMS99, DM00, KMS00, DM01, Kon01, BS04]). En particulier, nous savons maintenant qu'il existe des nombres ellipséphiques presque premiers et qu'ils sont bien répartis dans les progressions arithmétiques.

Un autre type de suite éparse définie par une contrainte digitale est donnée par les palindromes. Ce sont les entiers dont l'écriture dans une base fixée est symétrique. Les entiers de Mersenne et ceux de Fermat sont des exemples de palindromes en base 2. Comme les entiers ellipséphiques, les palindromes se répartissent de façon plutôt chaotique, mais même si la fonction génératrice se factorise, cette opération seule ne permet pas de contrôler les irrégularités comme avec les entiers ellipséphiques. Par contre, en couplant astucieusement des exponentielles complexes, nous parviendrons à rompre la symétrie caractéristique des palindromes et nous pourrons alors généraliser les techniques développées pour étudier les entiers ellipséphiques.

Les contraintes de nature digitale définissant les entiers ellipséphiques et les palindromes semblent *a priori* indépendantes de leur structure multiplicative. Il est donc naturel de penser que ces suites se comportent comme des suites d'entiers tirés au hasard. Notre objectif dans cette thèse est de déterminer dans quelle mesure ces suites ont des propriétés multiplicatives comparables à celles des entiers naturels en essayant de répondre aux trois questions que nous avons formulées ci-dessus et à d'autres

questions connexes sur la structure des diviseurs. Nous présentons dans la suite de cette introduction un aperçu des résultats de cette thèse. Des énoncés plus précis se trouvent dans les parties correspondantes.

1.2 Diviseurs des entiers ellipséphiques

Nous fixons une base r et un ensemble de chiffres $\mathscr{D} \subset \{0, ..., r-1\}$ de cardinal t. Les entiers ellipséphiques en base r relativement à $\mathscr{D}$ sont les entiers dont l'écriture en base r n'utilise que des chiffres de $\mathscr{D}$. Nous notons $W_{\mathscr{D}}$ l'ensemble de ces entiers. Dans toute cette thèse, nous supposons $2 \leqslant t \leqslant r-1$, c'est-à-dire que $\mathscr{D}$ exclu au moins un chiffre et en garde au moins deux. Ainsi,

$$\rho \ := \ \frac{\log t}{\log r} \in]0,1[. \tag{1.1}$$

Ce paramètre ρ donne une estimation de la taille de $W_{\mathscr{D}}$,

$$\#W_{\mathscr{D}}(x) \ \asymp \ x^{\rho}, \tag{1.2}$$

où nous avons noté traditionnellement

$$W_{\mathscr{D}}(x) \ := \ \{n \in W_{\mathscr{D}}, \ n < x\}.$$

En effet, comme $\#W_{\mathscr{D}}(r^N) = t^N$, l'estimation est obtenue en écrivant $r^{N-1} \leqslant x < r^N$.

En particulier, $W_{\mathscr{D}}$ est une famille de densité nulle puisque $\rho < 1$. L'étude des entiers ellipséphiques a pris un grand essor ces dix dernières années à la suite des articles de P. Erdös, C. Mauduit et A. Sárközy [EMS98] et [EMS99]. Dans ces travaux, les auteurs montrent notamment la bonne répartition des entiers ellipséphiques dans les progressions arithmétiques lorsque le module q est suffisamment petit. En notant

$$W_{\mathscr{D}}(x, a, q) \ := \ \{n \in W_{\mathscr{D}}, \ n < x, \ n \equiv a \mod q\},$$

pour une certaine constante $c > 0$ ne dépendant au plus que de la base r, si q est assez petit par rapport à x, nous avons

$$\#W_{\mathscr{D}}(x, a, q) \ = \ \frac{\#W_{\mathscr{D}}(x)}{q}\Big(1 + O_r\big(\mathrm{e}^{-c\frac{\log x}{\log q}}\big)\Big).$$

Ce résultat a ensuite été amélioré par S. Konyagin [Kon01]. Dans leurs deux articles [EMS98, EMS99], P. Erdös, C. Mauduit et A. Sárközy proposent une série de questions ouvertes qui ont été à l'origine de nombreux travaux sur le sujet.

P. Erdös, C. Mauduit et A. Sárközy ont prouvé que lorsque $t > r^{\frac{1}{2}}$, il existe une infinité d'entiers ellipséphiques sans facteur carré. Plus généralement, si $k > \frac{1}{\rho}$, alors une infinité d'entiers ellipséphiques ne sont pas divisibles par une puissance $k^{\text{ème}}$ et leur résultat fournit un développement asymptotique du cardinal de ces nombres. Le cas $\mathscr{D} = \{0, 1\}$ et $r \leqslant 5$ a été résolu par M. Filaseta et S. Konyagin [FK96]. Une question

duale consiste à déterminer s'il existe une infinité d'entiers ellipséphiques multiples d'une grande puissance d'un grand nombre premier. P. Erdös, C. Mauduit et A. Sárközy ont également résolu ce problème lorsque $k < \frac{1}{2(1-\rho)}$, mais sans être en mesure pour autant de déterminer l'ordre de grandeur du nombre des entiers ellipséphiques de cette forme.

Dans la première partie de cette thèse, nous apportons une réponse complète à ce problème si 0 appartient à $\mathscr{D}$. Nous montrerons sous forme explicite le

Théorème 1.1. *Soient $k \geqslant 2$, $r \geqslant 3$ et $\mathscr{D}$ fixés. Si $0 \in \mathscr{D}$, il existe une constante $c = c_{k,r} > 0$ et une infinité d'entiers ellipséphiques n possédant un facteur de la forme p^k avec p premier vérifiant $p \asymp n^c$.*

Une valeur explicite de la constante c sera donnée dans l'énoncé du Théorème 2.4 qui fournit en outre une minoration du bon ordre de grandeur du nombre d'entiers ellipséphiques vérifiant le Théorème 1.1. Autrement dit, en nous restreignant aux entiers ellipséphiques, nous conservons une proportion comparable d'entiers ayant un grand facteur du type p^k. Par exemple, en base 10 avec $\mathscr{D} = \{0, 1\}$, il existe une infinité d'entiers ellipséphiques n ayant un facteur carré supérieur à $n^{1/80}$. Un résultat similaire avait déjà été obtenu par S. Konyagin dans [Kon01, corollaire 6]. Nous améliorons son théorème en montrant que le nombre de tels diviseurs dans un petit intervalle est de l'ordre de grandeur attendu.

Pour aborder ce problème, nous utilisons des estimations de moyennes sur le cercle unité de la série génératrice associée aux entiers ellipséphiques

$$G_{\mathscr{D},N}(u) \ := \sum_{n \in W_{\mathscr{D}}(r^N)} \mathrm{e}(nu). \tag{1.3}$$

Il est important de remarquer que cette fonction se factorise complètement sous la forme

$$G_{\mathscr{D},N}(u) \ := \prod_{k<N} \sum_{d \in \mathscr{D}} \mathrm{e}(udr^k). \tag{1.4}$$

Notre contribution essentielle consiste à évaluer les moments d'ordre m de $G_{\mathscr{D},N}$ lorsque m est un entier arbitrairement grand. Deux méthodes différentes seront utilisées :

- le traitement du cas particulier $\mathscr{D} = \{0, 1\}$ est de nature combinatoire : nous comptons les solutions d'un système d'équations ;
- le traitement du cas général repose sur un procédé d'approximations successives et n'utilise que des arguments d'analyse. Pour $\mathscr{D} = \{0, 1\}$, cette deuxième approche conduit à un résultat moins précis que celui obtenu par la première méthode.

En définissant pour tout réel $m \geqslant 1$, la constante K_m par

$$K_m \ := \ \limsup_{N \to \infty} \left\| |G_{\mathscr{D},N}|^m \right\|_1^{\frac{1}{N}},$$

nous obtiendrons des encadrements précis lorsque m est grand :

Théorème 1.2. *Si $\mathscr{D} = \{0, 1\}$ et si $m = 2l$ est un entier pair, alors nous avons*

$$\frac{1}{r} \ \leqslant \ K_m \ < \ \frac{1}{r} + \sqrt{\frac{2}{\pi m}}. \tag{1.5}$$

Si $\operatorname{pgcd}\mathscr{D} = 1$, *si* $0 \in \mathscr{D}$ *et si* $m \geqslant 1$, *alors nous avons*

$$\frac{1}{r} \leqslant K_m < \frac{1}{r} + (r+1)\sqrt{\frac{\pi}{32m}}. \tag{1.6}$$

1.3 Entiers ellipséphiques friables

Un entier est dit y friable lorsque tous ses facteurs premiers sont inférieurs à y. P. Erdös, C. Mauduit et A Sárközy [EMS99] ont montré que, pour chaque $\epsilon > 0$, une infinité d'entiers n n'utilisant que le chiffre 1, c'est-à-dire $n = r^{N-1}+\cdots+r+1$, sont n^ϵ friables. Plus précisément, ils ont trouvé une constante $c > 0$ ne dépendant que de la base r telle qu'une infinité d'entiers n vérifient

$$P^+(n) \leqslant \exp\Big(c\frac{\log n}{\log_2 n}\Big).$$

Pour préciser le résultat précédent, S. Konyagin, C. Mauduit et A. Sárközy [KMS00] ont demandé si pour tous $\epsilon > 0$, r et $\mathscr{D}$ fixés, il existe une proportion positive d'entiers ellipséphiques n qui sont n^ϵ friables ? À notre connaissance, aucune avancée n'a été réalisée sur cette question. À défaut d'y répondre complètement, nous apportons quelques éléments qui vont dans le sens d'une réponse positive :

Théorème 1.3. *Pour chaque* r *et* $\mathscr{D}$ *fixés, il existe* $\alpha < 1$ *tel qu'une proportion positive d'entiers ellipséphiques* n *sont* n^α *friables.*

Des valeurs explicites de l'exposant de friabilité α seront précisées dans les Théorèmes 5.1 et 5.2. Pour des choix de r et $\mathscr{D}$ convenables, nous montrerons qu'il pourra être rendu extrêmement petit :

Théorème 1.4. *Pour chaque* $\epsilon > 0$ *fixé, il existe des bases* r *et des ensembles de chiffres* $\mathscr{D}$ *tels qu'une proportion positive d'entiers ellipséphiques* n *(relativement à cette base* r *et cette famille de chiffres* $\mathscr{D}$*) sont* n^ϵ *friables.*

La recherche d'entiers friables dans des suites rares a fait l'objet de divers travaux ces dernières années comme ceux de J. B. Friedlander [Fri89] et de C. Dartyge, G. Martin et G. Tenenbaum [DMT01]. Pour adapter leur approche, nous développons des techniques de crible (Théorème 7.1) pour écarter les modules q possédant un nombre de diviseurs anormalement grand dans les estimations en moyenne des restes de

$$\#W_{\mathscr{D}}(x,a,q) - \frac{1}{q}\#W_{\mathscr{D}}(x) \tag{1.7}$$

en modifiant les poids du crible de Rosser-Iwaniec par l'adjonction d'une condition supplémentaire de type Brun.

1.4 Palindromes

Nous fixons une base que nous notons maintenant $g \geqslant 2$. Les palindromes (en base g) sont les entiers dont l'écriture dans cette base g est symétrique, c'est-à-dire les nombres s'écrivant identiquement de gauche à droite et de droite à gauche. Il est à noter que le chiffre du milieu des palindromes possédant un nombre impair de chiffres ont le chiffre du milieu n'est soumis à aucune condition spécifique, contrairement aux palindromes avec un nombre pair de chiffres. Ces derniers sont toujours divisibles par $g+1$ et ne peuvent donc certainement pas être premiers (sauf éventuellement $g+1$ lui-même, cas de la base décimale). La parité du nombre de chiffres possède donc un lien avec les propriétés multiplicatives des palindromes.

La série génératrice associée aux palindromes s'écrit sous la forme d'un produit. En notant, $\mathscr{R}_N$ les palindromes ayant exactement N chiffres, nous avons l'identité

$$\sum_{n\in\mathscr{R}_N} \mathrm{e}(nu) \;:=\; h_N(u) \prod_{1\leqslant k<\frac{N}{2}} \sum_{0\leqslant d<g} \mathrm{e}\left(d(g^{N-1-k}+g^k)\right), \tag{1.8}$$

$h_N(u)$ étant une fonction bornée par g^2 qui tient compte des irrégularités des chiffres du *bord* et du *milieu*.

Le premier article sur les propriétés multiplicatives des palindromes est à notre connaissance celui W. Banks, N. Hart et M. Sakata [BHS04]. Ils ont montré que les palindromes sont bien répartis dans les progressions arithmétiques de module q suffisamment petit. Leur approche ne donne cependant des résultats que pour des valeurs de q relativement petites malgré l'utilisation d'outils sophistiqués tels des sommes de Kloostermann et des travaux de F. Pappalardi sur la taille de l'ordre de g dans $(\mathbb{Z}/q\mathbb{Z})^*$. Ils en déduisent notamment une majoration du nombre de palindromes premiers, mais cette majoration n'est pas de l'ordre de grandeur attendu.

Nous adopterons une démarche totalement différente, essentiellement élémentaire. L'idée consiste à coupler des exponentielles complexes afin de rompre la symétrie caractéristique des palindromes. Une généralisation d'un argument combinatoire de S. Konyagin, qu'il a utilisé pour les entiers ellipséphiques, nous permettra d'étudier la fonction génératrice des palindromes.

Nous montrons sous forme explicite (Théorème 9.1) un résultat du type Siegel-Walfisz sur l'équirépartition des palindromes dans les progressions arithmétiques pour une famille de valeurs de q beaucoup plus large :

Théorème 1.5. *Pour toute base g fixée, il existe une constante $c>0$ telle que les palindromes inférieurs à x sont bien répartis dans les progressions arithmétiques de module q uniformément pour q ne possédant pas de facteurs communs avec g^3-g et vérifiant*

$$q \;\leqslant\; \exp\Big(\frac{c\log x}{\log_2 x}\Big).$$

À défaut de pouvoir montrer l'équirépartition des palindromes dans les progressions arithmétiques pour de plus grandes valeurs du module, nous pouvons montrer un théo-

rème d'évaluation en moyenne des erreurs, du type du théorème de Bombieri-Vinogradov sur la répartition des nombres premiers dans les progressions arithmétiques. Une version effective sera donnée par le Théorème 9.2 :

Théorème 1.6. *Pour toute base g fixée, il existe un exposant $\beta > 0$ tel qu'en moyenne sur les modules inférieurs à x^β et ne possédant pas de facteurs communs avec $g^3 - g$, les palindromes sont bien répartis les progressions arithmétiques.*

Par exemple, en base 10, nous pouvons choisir $\beta = \frac{1}{186}$. Un tel théorème permet d'estimer les termes d'erreurs issus des techniques de crible. Nous en déduirons une série de corollaires sur les propriétés arithmétiques des palindromes.

Nous sommes en mesure de fournir (Corollaire 9.1) une majoration du bon ordre de grandeur du nombre de palindromes premiers :

Théorème 1.7. *Pour toute base g fixée, nous avons la majoration*

$$\#\{p \leqslant x,\ p \text{ premier et palindrome}\} \ll_g \frac{1}{\log x}\#\{n \leqslant x,\ n \text{ palindrome}\}. \tag{1.9}$$

Montrer la minoration correspondante, à savoir l'existence d'une infinité de palindromes premiers, semble être actuellement un objectif hors de portée, le nombre de palindromes jusqu'à x n'excèdant pas $O(x^{1/2})$. Aussi, nous nous sommes intéressé aux palindromes presque premiers (Corollaire 9.2) :

Théorème 1.8. *Pour toute base g fixée, il existe un entier k_g tel que le nombre de palindromes ayant au plus k_g facteurs premiers (avec multiplicité) est de l'ordre de grandeur attendu à des puissances de $\log_2 x$ près :*

$$\#\{n \leqslant x,\ n \text{ palindrome},\ \Omega(n) \leqslant k_g\} \gg_g \frac{1}{\log x}\#\{n \leqslant x,\ n \text{ palindrome}\}. \tag{1.10}$$

Par exemple, il existe une infinité de palindromes en base 2 ayant moins de 60 facteurs premiers (comptés avec leurs multiplicités). En base 10, il en existe une infinité avec au plus 372 facteurs premiers.

Nous avons également abordé la question des palindromes friables, pour laquelle nous apportons une première réponse sous forme explicite dans le Théorème 12.1 :

Théorème 1.9. *Pour toute base g fixée, il existe $\alpha < 1$ tels qu'une proportion positive de palindromes n sont n^α friables.*

Première partie

Les diviseurs des nombres ellipséphiques

Chapitre 2

Énoncé des résultats

Soient $r \geqslant 3$ un entier et $\mathscr{D}$ un sous-ensemble strict de $\{0, \dots, r-1\}$ dont nous notons $t := \#\mathscr{D}$ le cardinal. Nous supposons

$$2 \leqslant t \leqslant r-1 \tag{2.1}$$

et nous posons

$$\rho := \frac{\log t}{\log r} \in]0,1[. \tag{2.2}$$

Nous désignons par $W_{\mathscr{D}}$ l'ensemble des nombres ellipséphiques :

$$W_{\mathscr{D}} := \left\{ \sum d_j r^j \ / \ \forall j,\ d_j \in \mathscr{D} \right\} \tag{2.3}$$

où toutes les sommes sur j sont finies. Nous noterons aussi

$$W_{\mathscr{D}}(x) := \{n \in W_{\mathscr{D}},\ n < x\}, \tag{2.4}$$

$$W_{\mathscr{D}}(x,a,q) := \{n \in W_{\mathscr{D}},\ n < x,\ n \equiv a \mod q\}. \tag{2.5}$$

Différentes propriétés multiplicatives de ces entiers ont déjà été étudiées par P. Erdős, C. Mauduit et A. Sárközy [EMS98, EMS99], C. Dartyge et C. Mauduit [DM00, DM01], S. Konyagin [Kon01] et W. D. Banks et I. E. Shparlinkski [BS04]. En particulier, dans [DM00], C. Dartyge et C. Mauduit montrent que l'étude de certains problèmes multiplicatifs se ramène à une majoration suffisamment fine de la norme L^1 sur le cercle unité de la fonction génératrice des entiers ellipséphiques. Nous notons comme eux

$$G_{\mathscr{D},N}(z) := \frac{1}{t^N} \sum_{n \in W_{\mathscr{D}}(r^N)} \mathrm{e}(nz) = \prod_{0 \leqslant k < N} \mathscr{U}_{\mathscr{D}}(r^k z), \tag{2.6}$$

où $\mathrm{e}(z) := e^{2i\pi z}$, et

$$\mathscr{U}_{\mathscr{D}}(z) := \frac{1}{t} \sum_{d \in \mathscr{D}} \mathrm{e}(dz). \tag{2.7}$$

Grâce à [EMS98, théorème 4], nous savons que, si k est un entier assez grand, il existe beaucoup d'entiers ellipséphiques non divisibles par la puissance k d'un nombre premier vérifiant $(p, r(r-1)) = 1$:

Théorème A. *Si $k > 1/\rho$, il existe une constante $c > 0$ (ne dépendant que de r et de k) telle que*

$$\#\{n \in W_{\mathscr{D}}(x) \ / \ (p, r(r-1)) = 1 \Rightarrow p^k \nmid n\} \\ = \#W_{\mathscr{D}}(x) \prod_{p \nmid r(r-1)} (1-p^{-k}) \Big(1 + O\Big(\exp\Big\{-c\Big(\rho - \tfrac{1}{k}\Big)\log^{1/2} x\Big\}\Big)\Big).$$

Un résultat similaire avait déjà été montré par M. Filaseta et S. Konyagin dans [FK96].

Inversement, en autorisant suffisamment de chiffres pour que $\rho > \frac{3}{4}$ (en base 10, nous devons prendre au moins 6 chiffres), [EMS98, Théorème 5] montre également l'existence d'entiers ellipséphiques possédant un grand facteur carré :

Théorème B. *Si $k < 1/(2(1-\rho))$, alors il existe des entiers n dans $W_{\mathscr{D}}(r^N)$ divisibles par la puissance k d'un nombre premier p avec*

$$p \gg_{k,r} \Big(\frac{N^{\rho/2}}{\log N}\Big)^{\frac{1}{(2k-1)}}.$$

Pour tout réel $m \geqslant 1$, nous définissons K_m par

$$K_m \ := \ \limsup_{N\to\infty} \big\| |G_{\mathscr{D},N}|^m \big\|_1^{\frac{1}{N}}. \tag{2.8}$$

Majorer les réels K_m est fondamental pour de nombreux problèmes concernant les entiers ellipséphiques. Par exemple, le Théorème 1 de [DM00] fournit un analogue du théorème de Bombieri-Vinogradov si nous pouvons trouver un m tel que $K_m < r^{-\frac{1}{2}}$.

Dans un premier temps nous traitons le cas $\mathscr{D} = \{0, 1\}$ qui est réputé le plus difficile, et peut-être le plus intéressant. En effet, moins $\mathscr{D}$ comporte de chiffre, plus la famille $W_{\mathscr{D}}$ est rare.

Théorème 2.1. *Si $\mathscr{D} = \{0, 1\}$ et $m = 2l$ est un entier pair, on a*

$$\frac{1}{r} \ \leqslant \ K_{2l} \ \leqslant \ \frac{1}{r} + 2^{-2l}\binom{2l}{l} \ < \ \frac{1}{r} + \frac{1}{\sqrt{\pi l}}. \tag{2.9}$$

La démonstration du Théorème 2.1 est essentiellement combinatoire. Dans le cas général, nous devrons mettre à profit un effet de périodicité sur les fonctions $G_{\mathscr{D},N}$ définies par (2.6) pour majorer K_m :

Théorème 2.2. *Supposons que* $\operatorname{pgcd} \mathscr{D} = 1$ *et* $0 \in \mathscr{D}$ *et qu'il existe une constante $A > 0$ telle que, pour tout x réel, il existe d_1 et $d_2 \in \mathscr{D}$ vérifiant*

$$\|(d_1 - d_2)x\| \geqslant A\|x\|. \tag{2.10}$$

Alors, pour tout réel $m \geqslant 1$, nous avons

$$\frac{1}{r} \ \leqslant \ K_m \ < \ \frac{1}{r} + \frac{\sqrt{\pi}}{2\sqrt{2}} \frac{\sqrt{t}}{A\sqrt{m}}. \tag{2.11}$$

Remarque 2.1. Si $\mathscr{D} = \{0,1\}$, la constante $A := 1$ est clairement admissible. La majoration (2.11) fournit $K_m < \frac{1}{r} + \sqrt{\frac{\pi}{4m}}$. Le second terme de (2.9), résultat d'une étude approfondie du cas particulier $\mathscr{D} = \{0,1\}$, est donc plus précis que celui de (2.11) d'un facteur $\frac{\pi}{\sqrt{8}}$.

Remarque 2.2. Les résultats des Théorèmes 2.1 et 2.2 sont intéressants lorsque m est très grand : nous pouvons alors choisir K_m aussi proche de $\frac{1}{r}$ que l'on désire.

Le Théorème 2.2 nécessite la détermination d'une constante A adéquate. Le Lemme 1 de [EMS98] fournit la valeur admissible $A := \frac{1}{2(r-1)^2}$. En reprenant la démonstration de [EMS98] et en procédant à quelques optimisations, nous améliorons ce résultat :

Théorème 2.3. *Soit $\mathscr{D}$ tel que* $\operatorname{pgcd}\mathscr{D} = 1$. *Notons δ (resp. Δ) le plus petit (resp. grand) élément strictement positif de $\mathscr{D} - \mathscr{D}$. Dans le Théorème 2.2, nous pouvons choisir*

$$A \;:=\; \frac{2}{\delta + \Delta} \;>\; \frac{1}{r-1}. \tag{2.12}$$

*Sous les hypothèses du théorème 2.2 (*i.e. $\operatorname{pgcd}\mathscr{D} = 1$ *et* $0 \in \mathscr{D}$*), nous avons*

$$\frac{1}{r} \;\leqslant\; K_m \;<\; \frac{1}{r} + \frac{1}{8}\sqrt{\frac{\pi(r+1)^3}{m}}. \tag{2.13}$$

Dans [EMS98, Problème 2, p. 104] les auteurs demandent pour $\mathscr{D} = \{0,1\}$ de trouver des nombres ellipséphiques divisibles par le carré de grands nombres premiers : est-il vrai que si $r \geqslant 3$, il existe une constante $c = c_r > 0$ telle qu'une infinité d'entiers n dont tous les chiffres sont 0 ou 1 en base r possèdent au moins un facteur premier p vérifiant $p > n^c$ et $p^2 \mid n$?

M.Filaseta et S. Konyagin dans [FK96] ont répondu positivement à cette question si $r \leqslant 5$. C. Dartyge et C. Mauduit dans [DM00] ont étendu le domaine de validité à $r \leqslant 8$. S. Konyagin dans [Kon01, corollaire 6] fournit une réponse sans condition sur r, mais sa méthode ne permet pas d'obtenir une estimation du nombre d'entiers ellipséphiques possédant un facteur premier de ce type. Le Théorème 2.4 ci-dessous répond positivement à cette question pour tout $r \geqslant 3$ et l'étend à tout ensemble $\mathscr{D}$ contenant 0. En outre, le Théorème 2.4 montre que la proportion de ces entiers est de l'ordre de grandeur attendu.

Théorème 2.4. *On suppose que $0 \in \mathscr{D}$, $r \geqslant 3$ et $k \geqslant 2$. Il existe une constante $c = c_{k,r} > 0$ telle que, uniformément pour $2 \leqslant y \leqslant x^c$,*

$$\#\{n \in W_{\mathscr{D}}(x) \;/\; \exists p \in [y, 2y[,\; p^k \mid n\} \;\geqslant\; \frac{k}{2^k}\frac{\#W_{\mathscr{D}}(x)}{y^{k-1}\log x}\{1 + O_k(\frac{1}{\log y})\}.$$

Une valeur admissible de la constante $c_{k,r}$ est donnée par la formule

$$c_{k,r} \;=\; \frac{32}{\pi}\frac{(r^{1/2k}-1)^2}{k(r+1)^5}. \tag{2.14}$$

Si $\mathscr{D} = \{0,1\}$ et $k = 2$, nous pouvons prendre

$$c = \frac{\pi}{8} r^{-\frac{3}{2}}\left(1 - 2r^{-\frac{1}{4}}\right). \tag{2.15}$$

La démonstration du Théorème 2.4 repose de manière cruciale sur la majoration (2.9) dans le cas $\mathscr{D} = \{0,1\}$, et sur la majoration (2.11) combinée avec (2.12) dans le cas général.

Chapitre 3

Moyenne de la fonction $G_{\mathscr{D},N}$

3.1 Définition de la constante K_m

Dans toute la suite nous étendons la définition de la fonction $G_{\mathscr{D},N}$ en posant pour tout réel $\mu \geqslant 0$, $G_{\mathscr{D},\mu} = G_{\mathscr{D},\lfloor\mu\rfloor}$. Ce prolongement permet d'exprimer K_m de la manière suivante

Lemme 3.1. *On a*

$$K_m \;=\; \limsup_{\mu\to\infty} \left\| |G_{\mathscr{D},\mu}|^m \right\|_1^{\frac{1}{\mu}}. \tag{3.1}$$

Démonstration. Nous écrivons pour $\mu \geqslant 1$,

$$\left\| |G_{\mathscr{D},\mu}|^m \right\|_1^{\frac{1}{\mu}} \;=\; \left(\left\| |G_{\mathscr{D},\lfloor\mu\rfloor}|^m \right\|_1^{\frac{1}{\lfloor\mu\rfloor}} \right)^{\lfloor\mu\rfloor/\mu},$$

et en passant à la limite supérieure dans les deux membres, nous obtenons le résultat en vertu de la définition (2.8). □

Avant de nous concentrer sur la majoration de K_m, étape clef de notre étude, nous allons, pour illustrer la qualité des estimations que nous obtiendrons, donner une minoration simple et utile de K_m :

Lemme 3.2. *Pour tout réel $m \geqslant 1$, nous avons*

$$K_m \;\geqslant\; \frac{1}{r}.$$

Démonstration. Nous écrivons

$$\mathscr{U}_{\mathscr{D}}(x) - 1 = \frac{1}{t} \sum_{d\in\mathscr{D}} (\mathrm{e}(dx) - 1).$$

En utilisant l'inégalité $|\mathrm{e}(x) - 1| \leqslant 2\pi\,|x|$ nous obtenons

$$|\mathscr{U}_{\mathscr{D}}(x) - 1| \;\leqslant\; \frac{1}{t} \sum_{d\in\mathscr{D}} 2\pi d\,|x| \;\leqslant\; 2\pi r\,|x|\,.$$

Ainsi pour $|x| \leqslant \frac{1}{N}$,

$$\left|\mathscr{U}_{\mathscr{D}}(x)\right| \;\geqslant\; 1 - \frac{2\pi r}{N}.$$

Si $0 < x < \frac{1}{N} r^{-N}$, alors $0 < r^k x < \frac{1}{N}$ pour $0 \leqslant k < N$, donc

$$|G_{\mathscr{D},N}(x)| \;=\; \prod_{0 \leqslant k < N} \left|\mathscr{U}_{\mathscr{D}}(r^k x)\right| \;\geqslant\; (1 - \frac{2\pi r}{N})^N.$$

Nous en déduisons la minoration

$$\begin{aligned}\Big(\int_0^1 |G_{\mathscr{D},N}(x)|^m \mathrm{d}x\Big)^{\frac{1}{N}} \;&\geqslant\; \Big(\int_0^{r^{-N}/N} |G_{\mathscr{D},N}(x)|^m \mathrm{d}x\Big)^{\frac{1}{N}} \\ &\geqslant\; \Big(\frac{r^{-N}}{N}(1 - \frac{2\pi r}{N})^{mN}\Big)^{\frac{1}{N}} \\ &\geqslant\; \frac{1}{r}(1 - \frac{2\pi r}{N})^m \Big(\frac{1}{N}\Big)^{\frac{1}{N}}\end{aligned}$$

et par passage à la limite supérieure nous avons finalement

$$K_m \;=\; \limsup_{N \to +\infty} \Big(\int_0^1 |G_{\mathscr{D},N}(x)|^m \mathrm{d}x\Big)^{\frac{1}{N}} \;\geqslant\; \frac{1}{r}.$$

□

Le lemme suivant montre que si nous sommes capables de majorer la constante K_m pour un certain entier m, nous pourrons alors obtenir une majoration des moyennes de $G_{\mathscr{D},N}$. Commençons par rappeler qu'un ensemble $\mathfrak{R}$ est dit δ-bien espacé lorsque l'écart entre deux points distincts de $\mathfrak{R}$ est supérieur à δ.

Lemme 3.3. *Soit $\epsilon > 0$ fixé. Soient $\delta > 0$ et $\mathfrak{R}$ une famille δ-bien espacée de points dans $[\frac{\delta}{2}, 1 - \frac{\delta}{2}]$, globalement invariante modulo 1 par la multiplication par r. Pour tout entier m tel que*

$$1 \;\leqslant\; m \;\leqslant\; \frac{\log r}{\log \frac{1}{\delta}} N, \tag{3.2}$$

nous avons

$$\sum_{x \in \mathfrak{R}} |G_{\mathscr{D},N}(x)| \;\ll_{\epsilon,m,r}\; \Big(\frac{1}{\delta}\Big)^{1 + \frac{\log K_m}{\log r} + \epsilon}. \tag{3.3}$$

la constante implicite dépendant au plus de ϵ, m et r.

3.2 Moyenne de la dérivée de $(G_{\mathscr{D},N})^m$

La constante K_m permet aussi de majorer les moyennes de la dérivée de G_N. C'est l'objectif de ce lemme :

Lemme 3.4. *Soit $\epsilon > 0$ fixé. Uniformément sur μ, nous avons la majoration*

$$\big\|\big(G_{\mathscr{D},\mu}{}^m\big)'\big\|_1 \;\ll_{\epsilon,m,r}\; r^\mu (K_m + \epsilon)^\mu. \tag{3.4}$$

Démonstration. Nous calculons la dérivée de $(G_N)^m$ comme un produit :

$$\begin{aligned}\left|({G_{\mathscr{D},\mu}}^m)'(x)\right| &= m\left|(G_{\mathscr{D},\mu})'(x)\right|\left|{G_{\mathscr{D},\mu}}^{m-1}(x)\right| \\ &\leqslant m\sum_{k<\mu} r^k\left|\mathscr{U}_{\mathscr{D}}{}'(r^k x)\right|\Big|\prod_{\substack{j<\mu\\ j\neq k}}\mathscr{U}_{\mathscr{D}}(r^j x)\Big|\left|{G_{\mathscr{D},\mu}}^{m-1}(x)\right| \\ &\leqslant m\sum_{k<\mu} r^k\left|\mathscr{U}_{\mathscr{D}}{}'(r^k x)\right|\left|{G_{\mathscr{D},k}}^{m}(x)\right|\end{aligned}$$

puisque nous retirons des nombres de module inférieur à 1 du produit intérieur. Nous majorons trivialement la dérivée de $\mathscr{U}_{\mathscr{D}}$ par une constante ne dépendant que de $\mathscr{D}$:

$$\left|\mathscr{U}'_{\mathscr{D}}(y)\right| \leqslant 2\pi\Big|\sum_{d\in\mathscr{D}} d\,\mathrm{e}(dy)\Big| \leqslant 2\pi\sum_{d\in\mathscr{D}} d.$$

Donc

$$\left|({G_{\mathscr{D},\mu}}^m)'(x)\right| \ll_r m\sum_{k<\mu} r^k\left|{G_{\mathscr{D},k}}^m(x)\right|. \tag{3.5}$$

Nous utilisons cette majoration pour obtenir

$$\begin{aligned}\left\|({G_{\mathscr{D},\mu}}^m)'\right\|_1 &\ll_r m\sum_{k<\mu} r^k\left\|{G_{\mathscr{D},k}}^m\right\|_1 \\ &\ll_{r,m,\epsilon} \sum_{k<\mu} r^k\big(K_m+\epsilon\big)^k\end{aligned}$$

et comme, d'après le Lemme 3.2, $r(K_m+\epsilon)>1$, on en déduit

$$\left\|({G_{\mathscr{D},\mu}}^m)'\right\|_1 \ll_{r,m,\epsilon} \frac{r^{\lceil\mu\rceil}(K_m+\epsilon)^{\lceil\mu\rceil}}{r(K_m+\epsilon)-1} \ll_{r,m,\epsilon} r^\mu(K_m+\epsilon)^\mu,$$

ce qui termine la preuve. □

3.3 Preuve du lemme 3.3

Lemme 3.5. *Soit $\mathfrak{R}$ un ensemble de points qui est globalement invariant modulo 1 par la multiplication par r. Pour tout $m\geqslant 1$ entier,*

$$\sum_{x\in\mathfrak{R}}\left|G_{\mathscr{D},N}(x)\right| \leqslant \sum_{x\in\mathfrak{R}}\left|G_{\mathscr{D},N/m}(x)\right|^m.$$

Démonstration. Nous pouvons évidemment supposer que $m\geqslant 2$. Commençons par étudier le cas où $\frac{N}{m}$ est un entier. On écrit

$$\begin{aligned}\mathscr{R}(N) := \sum_{x\in\mathfrak{R}}\left|G_{\mathscr{D},N}(x)\right| &= \sum_{x\in\mathfrak{R}}\prod_{0\leqslant k<N}\left|\mathscr{U}_{\mathscr{D}}(r^k x)\right| \\ &\leqslant \sum_{x\in\mathfrak{R}}\prod_{0\leqslant j\leqslant m-1}\ \prod_{\frac{j}{m}N\leqslant k<\frac{j+1}{m}N}\left|\mathscr{U}_{\mathscr{D}}(r^k x)\right|.\end{aligned}$$

L'inégalité arithmético-géométrique

$$(a_0 \cdots a_{m-1})^{1/m} \leqslant \tfrac{1}{m}(a_0 + \cdots + a_{m-1}),$$

appliquée avec

$$a_j \;=\; \Big(\prod_{\frac{j}{m}N \leqslant k < \frac{j+1}{m}N} |\mathscr{U}_{\mathscr{D}}(r^k x)| \Big)^m,$$

permet d'obtenir

$$\mathscr{R}(N) \;\leqslant\; \sum_{x\in\mathfrak{R}} \frac{1}{m} \sum_{0\leqslant j\leqslant m-1} \Big(\prod_{\frac{j}{m}N \leqslant k < \frac{j+1}{m}N} |\mathscr{U}_{\mathscr{D}}(r^k x)| \Big)^m.$$

Ainsi

$$\mathscr{R}(N) \;\leqslant\; \frac{1}{m} \sum_{0\leqslant j\leqslant m-1} \sum_{x\in\mathfrak{R}} \Big(\prod_{\frac{j}{m}N \leqslant k < \frac{j+1}{m}N} |\mathscr{U}_{\mathscr{D}}(r^k x)| \Big)^m.$$

Comme l'ensemble $\mathfrak{R}$ est stable modulo 1 par la multiplication par r, nous avons donc la majoration cherchée :

$$\mathscr{R}(N) \;\leqslant\; \frac{1}{m} \sum_{j\leqslant m-1} \sum_{x\in\mathfrak{R}} \Big(\prod_{k < \frac{N}{m}} |\mathscr{U}_{\mathscr{D}}(x)| \Big)^m.$$

Pour le cas général,si $\tilde{N}$ désigne le plus grand multiple de m inférieur à N, alors $\lfloor N/m \rfloor = \tilde{N}/m$ et

$$\mathscr{R}(N) \;\leqslant\; \mathscr{R}(\tilde{N}) \;\leqslant\; \sum_{x\in\mathfrak{R}} |G_{\mathscr{D},\tilde{N}/m}(x)|^m \;=\; \sum_{x\in\mathfrak{R}} |G_{\mathscr{D},N/m}(x)|^m$$

ce qui termine la preuve du lemme. □

Démonstration du lemme 3.3. Comme $G_{\mathscr{D},N}(r)$ est le produit de fonctions de module inférieur à 1, l'application

$$\mu \mapsto |G_{\mathscr{D},\mu}(r)|$$

est pour chaque réel r décroissante. Si $\mu \leqslant \frac{N}{m}$, nous avons donc grâce au lemme 3.5

$$\sum_{r\in\mathfrak{R}} |G_{\mathscr{D},N}(r)| \;\leqslant\; \sum_{r\in\mathfrak{R}} |G_{\mathscr{D},N/m}(r)|^m \;\leqslant\; \sum_{r\in\mathfrak{R}} |G_{\mathscr{D},\mu}(r)|^m.$$

Nous majorons cette somme en utilisant le lemme A.1 de Sobolev-Gallagher énoncé dans l'annexe A de cette thèse,

$$\sum_{r\in\mathfrak{R}} |G_{\mathscr{D},N}(r)| \;\leqslant\; \frac{1}{\delta} \big\| {G_{\mathscr{D},\mu}}^m \big\|_1 + \big\| ({G_{\mathscr{D},\mu}}^m)' \big\|_1.$$

Le lemme 3.4 fournit donc pour tout $\mu \leqslant \frac{N}{m}$,

$$\begin{aligned} \sum_{r\in\mathfrak{R}} |G_{\mathscr{D},N}(r)| \;&\ll_{\epsilon,r}\; \frac{1}{\delta}(K_m+\epsilon)^\mu + m\big(r(K_m+\epsilon)\big)^\mu \\ &\ll_{\epsilon,r}\; m\big(\frac{1}{\delta} + r^\mu\big)(K_m+\epsilon)^\mu. \end{aligned}$$

Nous optimisons le paramètre μ en choisissant

$$\mu \ := \ -\frac{\log \delta}{\log r}.$$

L'hypothèse du lemme implique $\mu \ \leqslant \ \frac{N}{m}$, donc

$$\begin{aligned}\sum_{r\in\mathfrak{R}} |G_{\mathscr{D},N}(r)| \ &\ll_{\epsilon,m,r} \ \frac{1}{\delta}(K_m+\epsilon)^{\mu} \\ &\ll_{\epsilon,m,r} \ \Big(\frac{1}{\delta}\Big)^{1+\frac{\log(K_m+\epsilon)}{\log r}}.\end{aligned}$$

La majoration du lemme s'en déduit immédiatement puisque ce résultat est vrai pour tout $\epsilon > 0$. □

3.4 Cardinal de $W_{\mathscr{D}}(x)$ et de $W_{\mathscr{D}}(x, a, q)$

Nous commençons par énoncer un résultat qui permet de limiter notre étude au cas où x est une puissance de r, *i.e.* lorsqu'il existe N tel que $x = r^N$. Des versions similaires ont déjà été exploitées par exemple par [DM00]. L'étude de ce cas particulier est naturelle car la moyenne des exponentielles

$$\frac{1}{t^N} \sum_{n\in W_{\mathscr{D}}(r^N)} \mathrm{e}(nz) \ = \ G_{\mathscr{D},N}(z)$$

se factorise alors complètement.

Lemme 3.6. *Soit $x = \sum_{N<M} x_N r^N$ décomposé dans la base r. Notons*

$$K := \max\{N < M, \ x_N \notin \mathscr{D}\}$$

*en convenant que $K = 0$ si l'ensemble est vide (*i.e. *si x est ellipséphique). Alors*

$$\#W_{\mathscr{D}}(x) \ = \ \sum_{K\leqslant N<M} \mathscr{D}(x_N) t^N, \tag{3.6}$$

et pour tout ensemble d'entiers $\mathscr{Q}$,

$$\sum_{q\in\mathscr{Q}} \max_{a\in\mathbb{Z}} \Big|\#W_{\mathscr{D}}(x,a,q) - \frac{\#W_{\mathscr{D}}(x)}{q}\Big| \ \leqslant \ \sum_{K\leqslant N<M} \mathscr{D}(x_N) t^N \mathscr{R}_N(\mathscr{Q}) \tag{3.7}$$

avec les notations

$$\mathscr{D}(y) \ := \ \#\{d \in \mathscr{D}, \ d < y\}, \tag{3.8}$$

$$\mathscr{R}_N(\mathscr{Q}) \ := \ \sum_{q\in\mathscr{Q}} \frac{1}{q} \sum_{0<l<q} \Big|G_{\mathscr{D},N}\big(\frac{l}{q}\big)\Big|. \tag{3.9}$$

Démonstration. Nous pouvons séparer $W_{\mathscr{D}}(x)$ en deux classes : les entiers dont le premier chiffre est strictement inférieur à x_{M-1} et ceux dont le premier chiffre est égal à x_{M-1}. Si $x_{M-1} \notin \mathscr{D}$, alors

$$W_{\mathscr{D}}(x) = W_{\mathscr{D}}(x_{M-1} r^{M-1}).$$

Si $x_{M-1} \in \mathscr{D}$, alors nous avons l'union disjointe

$$W_{\mathscr{D}}(x) = W_{\mathscr{D}}(x_{M-1}r^{M-1}) \sqcup (x_{M-1}r^{M-1} + W_{\mathscr{D}}(x - x_{M-1}r^{M-1}))$$

et nous pouvons appliquer de nouveau ce découpage à $x - x_{M-1}r^{M-1}$ (qui est le nombre x "privé" de son premier chiffre). À l'étape $M-K$, en notant $X_N := \sum_{N<j<M} x_j r^j$, nous obtenons l'égalité

$$W_{\mathscr{D}}(x) \;=\; \bigsqcup_{K \leqslant N < M} (X_N + W_{\mathscr{D}}(x_N r^N)).$$

L'égalité (3.6) s'en déduit puisque la réunion est disjointe. Nous obtenons aussi pour tout $z \in \mathbb{C}$,

$$\sum_{n \in W_{\mathscr{D}}(x)} \mathrm{e}(zn) \;=\; \sum_{K \leqslant N < M} \mathrm{e}(zX_N) \sum_{n \in W_{\mathscr{D}}(x_N r^N)} \mathrm{e}(zn). \tag{3.10}$$

La première étape pour montrer (3.7) est de se ramener à des sommes trigonométriques grâce à l'égalité

$$\#W_{\mathscr{D}}(x,a,q) \;=\; \sum_{n \in W_{\mathscr{D}}(x)} \frac{1}{q} \sum_{0 \leqslant l < q} \mathrm{e}\Big(\frac{l(n-a)}{q}\Big)$$

En isolant le terme $l = 0$:

$$\#W_{\mathscr{D}}(x,a,q) \;=\; \frac{\#W_{\mathscr{D}}(x)}{q} + \frac{1}{q} \sum_{0<l<q} \mathrm{e}\Big(-\frac{la}{q}\Big) \sum_{n \in W_{\mathscr{D}}(x)} \mathrm{e}\Big(\frac{ln}{q}\Big).$$

Nous obtenons successivement, en utilisant (3.10) avec $z := \frac{l}{q}$ pour la seconde majoration,

$$\begin{aligned}
\Big|\#W_{\mathscr{D}}(x,a,q) - \frac{\#W_{\mathscr{D}}(x)}{q}\Big| \;&\leqslant\; \frac{1}{q} \sum_{0<l<q} \Big| \sum_{n \in W_{\mathscr{D}}(x)} \mathrm{e}\Big(\frac{ln}{q}\Big)\Big| \\
&\leqslant\; \frac{1}{q} \sum_{0<l<q} \sum_{K \leqslant N < M} \Big| \sum_{n \in W_{\mathscr{D}}(x_N r^N)} \mathrm{e}\Big(\frac{ln}{q}\Big)\Big| \\
&\leqslant\; \sum_{K \leqslant N < M} \frac{1}{q} \sum_{0<l<q} \Big| \sum_{\substack{n_0,\dots,n_N \in \mathscr{D} \\ n_N < x_N}} \prod_{j \leqslant N} \mathrm{e}\Big(\frac{ln_j r^j}{q}\Big)\Big|
\end{aligned}$$

où $n = \sum_j n_j r^j$ est la décomposition de n en base r. Ainsi,

$$\sum_{q \in \mathscr{Q}} \Big|\#W_{\mathscr{D}}(x,a,q) - \frac{\#W_{\mathscr{D}}(x)}{q}\Big| \;\leqslant\; \sum_{q \in \mathscr{Q}} \sum_{K \leqslant N < M} \frac{1}{q} \sum_{0<l<q} \Big| \prod_{j \leqslant N} \sum_{\substack{n_j \in \mathscr{D} \\ n_N < x_N}} \mathrm{e}\Big(\frac{ln_j r^j}{q}\Big)\Big|,$$

donc en isolant le terme $j = N$ que l'on majore trivialement par $\mathscr{D}(x_N)$,

$$\begin{aligned}
\sum_{q \in \mathscr{Q}} \Big|\#W_{\mathscr{D}}(x,a,q) - \frac{\#W_{\mathscr{D}}(x)}{q}\Big| \;&\leqslant\; \sum_{q \in \mathscr{Q}} \sum_{K \leqslant N < M} \mathscr{D}(x_N) t^N \frac{1}{q} \sum_{0<l<q} \Big|G_{\mathscr{D},N}\big(\frac{l}{q}\big)\Big| \\
&\leqslant\; \sum_{K \leqslant N < M} \mathscr{D}(x_N) t^N \mathscr{R}_N(\mathscr{Q}).
\end{aligned}$$

□

Remarque 3.1. En réunissant les informations de (3.6) et de (3.7), nous obtenons la majoration moins précise mais plus "explicite" : pour tout $\epsilon > 0$,

$$\sum_{q\in\mathscr{Q}} \max_{a\in\mathbb{Z}} \Big|\#W_{\mathscr{D}}(x,a,q) - \frac{\#W_{\mathscr{D}}(x)}{q}\Big| \leqslant \#W_{\mathscr{D}}(x)\left(\sup_{(1-\epsilon)M\leqslant N<M}(\mathscr{R}_N(\mathscr{Q})) + \frac{t^3}{t-1}\frac{\#\mathscr{Q}}{x^{\rho\epsilon}}\right). \tag{3.11}$$

Démonstration de (3.11). Majorons le membre de droite de (3.7) :

$$\begin{aligned}\sum_{K\leqslant N<M} &\mathscr{D}(x_N)t^N\mathscr{R}_N(\mathscr{Q}) \\ &\leqslant \sum_{\max\{K,(1-\epsilon)M\}\leqslant N<M} \mathscr{D}(x_N)t^N\mathscr{R}_N(\mathscr{Q}) + \sum_{N<(1-\epsilon)M} \mathscr{D}(x_N)t^N\mathscr{R}_N(\mathscr{Q}) \\ &\leqslant \#W_{\mathscr{D}}(x) \sup_{(1-\epsilon)M\leqslant N<M} \mathscr{R}_N(\mathscr{Q}) + \frac{t}{t-1}\#\mathscr{Q}\, t^{M-\epsilon M+1}\end{aligned}$$

en remplaçant $\mathscr{R}_N(\mathscr{Q})$ par sa borne supérieure dans le premier terme et par $\#\mathscr{Q}$ dans le second. Comme $r^{M-1} \leqslant x < r^M$, nous avons $t^{M-1} \leqslant \#W_{\mathscr{D}}(x)$ et $t^{-M\epsilon} < x^{-\rho\epsilon}$, ce qui permet de terminer la preuve de (3.11). □

3.5 Réduction de la preuve du Théorème 2.4

Nous montrons comment une bonne majoration de K_m et le lemme 3.3 permet de démontrer le Théorème 2.4.

Lemme 3.7. *Soient $r \geqslant 3$, $k \geqslant 2$ et m un entier pair tel que*

$$r^{2k-1}{K_m}^{2k} < 1. \tag{3.12}$$

Soit $c > 0$ un réel vérifiant

$$\begin{aligned} c &> \tfrac{2k-1}{\rho} && \text{si } tK_m{}^{\frac{1}{m}} \leqslant 1\ ; \\ c &> 2km - \frac{1}{\rho}\left(1-2k-2k\frac{\log K_m}{\log r}\right) && \text{sinon.}\end{aligned}$$

Alors uniformément pour $2 \leqslant y \leqslant x^{\frac{1}{c}}$, on a

$$\#\{n\in W_{\mathscr{D}}(x),\ \exists p^k \mid n,\ y\leqslant p<2y\} \geqslant \frac{k}{2^k}\frac{\#W_{\mathscr{D}}(x)}{y^{k-1}\log x}\Big(1+O(\frac{1}{\log y})\Big).$$

Démonstration. Soit $2 \leqslant y \leqslant x^{\frac{1}{c}}$. En notant $\nu_p(n)$ la valuation p-adique de n, on a pour tout entier n :

$$n \geqslant \prod_{\substack{p\mid n\\ p\geqslant y\\ \nu_p(n)\geqslant k}} p^{\nu_p(n)} \geqslant \prod_{\substack{p\mid n\\ p\geqslant y\\ \nu_p(n)\geqslant k}} y^k = \prod_{\substack{p^k\mid n\\ p\geqslant y}} y^k = y^{k\#\{p\geqslant y,\ p^k\mid n\}}.$$

Ainsi

$$\#\{p \geqslant y,\ p^k \mid n\} \ \leqslant\ \frac{\log n}{k \log y},$$

et donc

$$\begin{aligned}
&\#\{n \in W_{\mathscr{D}}(x) \ / \ \exists p^k \mid n,\ y \leqslant p < 2y\} \\
&\qquad \geqslant\ \frac{k \log y}{\log x} \sum_{n \in W_{\mathscr{D}}(x)} \sum_{\substack{y \leqslant p < 2y \\ p^k \mid n}} 1 \ =\ \frac{k \log y}{\log x} \sum_{y \leqslant p < 2y} \#W_{\mathscr{D}}(x, 0, p^k) \\
&\qquad \geqslant\ \frac{k \log y}{\log x} \sum_{y \leqslant p < 2y} \frac{\#W_{\mathscr{D}}(x)}{p^k} - \sum_{y \leqslant p < 2y} \Big| \frac{\#W_{\mathscr{D}}(x)}{p^k} - \#W_{\mathscr{D}}(x, 0, p^k) \Big| \\
&\qquad \geqslant\ \frac{k \log y}{\log x} \sum_{y \leqslant p < 2y} \frac{\#W_{\mathscr{D}}(x)}{p^k} - \sum_{K \leqslant N < M} \mathscr{D}(x_N) t^N \mathscr{R}_N(\mathscr{Q}_y) \qquad (3.13)
\end{aligned}$$

en appliquant le lemme 3.6 énoncé et prouvé dans le paragraphe précédant, avec le choix de $\mathscr{Q}_y := \{p^k,\ y \leqslant p < 2y\}$. En utilisant le théorème des nombres premiers, nous vérifions que le terme principal dans (3.13) est supérieur à

$$\frac{k}{2^k} \frac{\#W_{\mathscr{D}}(x)}{y^{k-1} \log x} \Big(1 + 0\big(\frac{1}{\log y}\big) \Big)$$

Une meilleure constante peut être obtenue en évaluant cette somme plus précisément. La preuve sera donc terminée dès que nous aurons montré

$$\sum_{K \leqslant N < M} \mathscr{D}(x_N) t^N \mathscr{R}_N(\mathscr{Q}_y) \ \ll\ \frac{\#W_{\mathscr{D}}(x)}{y^{k-1} \log^2 x}, \qquad (3.14)$$

la constante implicite pouvant dépendre des paramètres r, t, k, m ou c.

Nous appliquons le lemme 3.3 à l'ensemble y^{-2k} bien espacé

$$\mathfrak{R} \ :=\ \{\tfrac{l}{p^k},\ 0 < l < p^k,\ y \leqslant p < 2y\}. \qquad (3.15)$$

Si y est assez grand, par exemple $y > r$, tout nombre premier $p \in [y, 2y[$ est premier avec r donc le lemme de Gauß assure que $\mathfrak{R}$ est bien globalement invariant modulo 1 par la multiplication par r. Dès que

$$m \ \leqslant\ \frac{\log r}{2k \log y} N, \qquad (3.16)$$

nous avons d'après (3.3)

$$\begin{aligned}
\mathscr{R}_N(\mathscr{Q}_y) \ &\leqslant\ \frac{1}{y^k} \sum_{y \leqslant p < 2y} \sum_{0 < l < p^k} \Big| G_{\mathscr{D},N}\big(\frac{l}{p^k}\big) \Big| \\
&\ll_\epsilon\ y^{-k} m \big(y^{2k}\big)^{1 + \frac{\log(K_m + \varepsilon)}{\log r}} \\
&\ll_{\epsilon,m}\ \big(y^k\big)^{1 + 2\frac{\log(K_m + \varepsilon)}{\log r}}. \qquad (3.17)
\end{aligned}$$

Ainsi,

$$\begin{aligned}&\sum_{K\leqslant N<M} \mathscr{D}(x_N)t^N\mathscr{R}_N(\mathscr{Q}_y)\\ &\ll_{\epsilon,m} \sum_{K\leqslant N<M} \mathscr{D}(x_N)t^N y^{k(1+2\frac{\log(K_m+\varepsilon)}{\log r})} + \sum_{N<2km\frac{\log y}{\log r}} t^{N+1}y^k(K_m+\varepsilon)^{\frac{N}{m}},\end{aligned}$$

la seconde majoration étant obtenue en appliquant le lemme 3.3 avec le choix de

$$m \ := \ \frac{\log r}{2k\log y}N$$

pour que notre hypothèse sur m soit vérifiée.

La première somme s'évalue grâce à (3.6), tandis que la seconde se calcule comme somme d'une série géométrique de raison $t(K_m+\varepsilon)^{\frac{1}{m}}$. Traitons en détail le cas le plus compliqué où $tK_m{}^{\frac{1}{m}} > 1$:

$$\sum_{K\leqslant N<M} \mathscr{D}(x_N)t^N\mathscr{R}_N(\mathscr{Q}_y) \ \leqslant \ \Big(\#W_{\mathscr{D}}(x) + \frac{t^2(K_m+\varepsilon)^{\frac{1}{m}}}{t(K_m+\varepsilon)^{\frac{1}{m}}-1}y^{2km\rho}\Big)y^{k(1+2\frac{\log(K_m+\varepsilon)}{\log r})}.$$

Comme $y \leqslant x^{\frac{1}{c}}$, la condition (3.14) est vraie dès que (quitte à choisir ε assez petit) :

$$\begin{aligned}2km\rho + k(1+2\frac{\log K_m}{\log r}) \ &< \ c\rho + 1 - k,\\ k(1+2\frac{\log K_m}{\log r}) \ &< \ 1-k.\end{aligned}$$

Ces conditions sur c et sur K_m sont exactement celles imposées dans l'énoncé du Lemme 3.7. □

Remarque 3.2. Nous ne parviendrons pas à obtenir de majoration de K_m suffisamment précise pour être dans le cas $tK_m{}^{\frac{1}{m}} \leqslant 1$. Il est d'ailleurs probable que cette condition soit impossible. Si $tK_m{}^{\frac{1}{m}} > 1$, l'hypothèse (3.12) montre que le choix de $c = 2km$ est acceptable.

Remarque 3.3. Notre méthode permet aussi d'obtenir une majoration du nombre d'entiers ellipséphiques divisibles par une puissance d'un grand nombre premier en partant de la majoration

$$\#\{n\in W_{\mathscr{D}}(x),\ \exists p^k \mid n,\ y\leqslant p\leqslant 2y\} \ \leqslant \ \sum_{n\in W_{\mathscr{D}}(x)}\ \sum_{\substack{y\leqslant p\leqslant 2y\\ p^k\mid n}} 1.$$

3.6 Encadrement de K_m pour $\mathscr{D} = \{0,1\}$

Nous prouvons dans cette partie le Théorème 2.1 par une méthode essentiellement combinatoire : nous interprétons K_m comme le nombre de solutions d'une équation et nous dénombrons par récurrence ces solutions.

Lemme 3.8. *Pour $\beta \in \mathbb{Z}$, notons $X_N(\beta)$ le nombre de solutions dans $W_{\mathscr{D}}(r^N)$ de l'équation*

$$n_1 + \cdots + n_l \;=\; m_1 + \cdots + m_l + \beta r^N. \tag{3.18}$$

Pour $N = 0$, nous convenons que $X_0(\beta) = 1$ si $\beta = 0$ et 0 sinon. Alors

$$\|{G_{\mathscr{D},N}}^{2l}\|_1 \;=\; t^{-2lN} X_N(0) \tag{3.19}$$

et $X_N(\beta)$ se calcule grâce à la relation de récurrence

$$X_{N+1}(\beta) = \sum_{|j|<\frac{l}{r-1}} \binom{2l}{l+j-\beta r} X_N(j), \tag{3.20}$$

Démonstration. Pour prouver (3.19), il suffit de remarquer qu'en développant le produit, nous avons

$$\begin{aligned} t^{2lN}\|{G_{\mathscr{D},N}}^{2l}\|_1 \;&=\; \int_0^1 \Big(\sum_{n\in W_{\mathscr{D}}(r^N)} \mathrm{e}(nu)\Big)^l \Big(\sum_{m\in W_{\mathscr{D}}(r^N)} \mathrm{e}(-mu)\Big)^l \mathrm{d}u \\ &= \int_0^1 \sum_{\substack{n_1,\dots,n_l\in W_{\mathscr{D}}(r^N)\\ m_1,\dots,m_l\in W_{\mathscr{D}}(r^N)}} \mathrm{e}((n_1+\cdots+n_l-m_1-\cdots+m_l)u)\mathrm{d}u \\ &= \sum_{\substack{n_1,\dots,n_l\in W_{\mathscr{D}}(r^N)\\ m_1,\dots,m_l\in W_{\mathscr{D}}(r^N)}} \int_0^1 \mathrm{e}((n_1+\cdots+n_l-m_1-\cdots+m_l)u)\mathrm{d}u \end{aligned}$$

et l'intégrale vaut 1 ou 0 suivant que $n_1+\cdots+n_l = m_1+\cdots+m_l$ ou pas. Nous comptons donc exactement le nombre de solutions dans $W_{\mathscr{D}}(r^N)$ de l'équation

$$n_1 + \cdots + n_l \;=\; m_1 + \cdots + m_l,$$

ce qui est la définition de $X_N(0)$.

Pour prouver (3.20), décomposons les nombres ellipséphiques de $W_{\mathscr{D}}(r^{N+1})$ en isolant leur chiffre d'indice N :

$$\begin{aligned} n_k \;&=\; d_k r^N + \tilde{n}_k && \text{avec } d_k \in \mathscr{D} \text{ et } \tilde{n}_k \in W_{\mathscr{D}}(r^N)\ ; \\ m_k \;&=\; e_k r^N + \tilde{m}_k && \text{avec } e_k \in \mathscr{D} \text{ et } \tilde{m}_k \in W_{\mathscr{D}}(r^N). \end{aligned}$$

Alors $n_1 + \cdots + n_l = m_1 + \cdots + m_l + \beta r^{N+1}$ si et seulement si

$$\Big(\sum_k d_k\Big) r^N + \sum_k \tilde{n}_k \;=\; \Big(\sum_k e_k\Big) r^N + \sum_k \tilde{m}_k + \beta r^{N+1}$$

si et seulement s'il existe $j \in \mathbb{Z}$ tel que

$$\sum_k \tilde{n}_k \;= \sum_k \tilde{m}_k + j r^N \tag{3.21}$$

et

$$\sum_k d_k \;=\; \sum_k e_k + \beta r - j. \tag{3.22}$$

Pour chaque j, nous avons donc $X_N(j)$ choix possibles pour les $\tilde{n}_k$ et $\tilde{m}_j$ et nous avons $\binom{2l}{l+\beta r-j}$ choix pour les d_k et e_k. Comme $\mathscr{D} = \{0, 1\}$, le nombre de solutions de l'équation (3.22) est en effet

$$\sum_{i\in\mathbb{Z}} \binom{l}{i}\binom{l}{l+\beta r-j-i} \;=\; \binom{2l}{l+\beta r-j}.$$

Cette relation se démontre par exemple en identifiant les coefficients de $x^{l+\beta r-j}$ du polynôme $(1+x)^l(1+x)^l = (1+x)^{2l}$ développé par la formule du binôme de Newton.

Remarquons aussi que l'égalité (3.21) impose $|j| < \frac{l}{r-1}$ puisque nous avons les encadrements

$$0 \;\leqslant\; \sum_k \tilde{n}_k \leqslant l\frac{r^N-1}{r-1}, \quad 0 \;\leqslant\; \sum_k \tilde{m}_k \leqslant l\frac{r^N-1}{r-1}.$$

Ainsi,

$$X_{N+1}(\beta) \;=\; \sum_{|j|<\frac{l}{r-1}} \binom{2l}{l+j-\beta r} X_N(j), \tag{3.23}$$

ce qui termine la preuve du lemme. □

Lemme 3.9. *Pour tous nombres entiers $N \geqslant 0$, $l \geqslant 1$ et $r \geqslant 3$,*

$$K_{2l} \;\leqslant\; \frac{1}{r}\sum_{0\leqslant n<r} \cos^{2l}\left(\pi\frac{n}{r}\right) \;<\; \frac{1}{r} + 2^{-2l}\binom{2l}{l}. \tag{3.24}$$

Démonstration. Posons $k := \lceil \frac{l}{r-1} \rceil$. Notons

$$X_N := \begin{pmatrix} X_N(1-k) \\ \vdots \\ X_N(k-1) \end{pmatrix} \in \mathbb{R}^{2k-1}$$

et M la matrice définie par

$$M = \left[\binom{2l}{l-ir+j}\right]_{-k<i,j<k}$$

de sorte que $X_{N+1} = MX_N$.

Munissons $\mathbb{R}^{2k-1}$ de la norme 1 et $M_{2k-1}(\mathbb{R})$ de la norme qui lui est subordonnée,

$$\|M\| \;:=\; \max_{|j|<k}\Big\{\sum_{|i|<k}|m_{i,j}|\Big\}.$$

Ainsi

$$|X_N(0)| \;\leqslant\; \|X_N\| \;=\; \|M^N X_0\| \;\leqslant\; \|M\|^N\|X_0\| \;=\; \|M\|^N.$$

En utilisant l'équation (3.19), nous trouvons la première majoration

$$K_{2l} \;\leqslant\; 2^{-2l}\max_{|j|<\frac{l}{r-1}}\Big\{\sum_{|i|<\frac{l}{r-1}}\binom{2l}{l-ir}\Big\}. \tag{3.25}$$

Fixons maintenant j et notons $\xi := \mathrm{e}(\frac{1}{r})$. Alors

$$\begin{aligned}\sum_{k\equiv j[r]} \binom{2l}{l-k} &= \sum_k \frac{1}{r} \sum_{0\leqslant n<r} \xi^{(k-j)n} \binom{2l}{l-k} \\ &= \frac{1}{r} \sum_{0\leqslant n<r} \xi^{-n(j+l)} \left(1+\xi^n\right)^{2l} \\ &= \frac{1}{r} \sum_{0\leqslant n<r} \xi^{-nj} \left(\xi^{\frac{n}{2}}+\xi^{-\frac{n}{2}}\right)^{2l} \\ &\leqslant \frac{2^{2l}}{r} \sum_{0\leqslant n<r} \cos^{2l}\left(\pi\frac{n}{r}\right).\end{aligned}$$

En prenant le maximum sur j dans (3.25), nous avons démontré la première majoration du lemme. Nous majorons la somme par l'intégrale correspondante pour en déduire

$$\begin{aligned}K_{2l} &\leqslant \frac{1}{r} + \frac{1}{r} \sum_{0<n<r} \cos^{2l}\left(\pi\frac{n}{r}\right) \\ &< \frac{1}{r} + 2\int_0^{\frac{1}{2}} \cos^{2l}(\pi s)\,\mathrm{d}s\end{aligned}$$

ce qui prouve le lemme 3.9 après le calcul de l'intégrale de Wallis. □

3.7 Encadrement de K_m pour $\mathscr{D}$ quelconque

Le lemme 1 de [EMS98] énonce que si $\mathscr{D}$ est un sous-ensemble de $\{0,...,r-1\}$ de cardinal au moins 2 et tel que $\operatorname{pgcd}\mathscr{D} = 1$, alors pour tout $x \in \mathbb{R}$, il existe $d \in \mathscr{D}$ tel que

$$\|dx\| \geqslant \frac{1}{2(r-1)^2}\|x\|.$$

Cette minoration est ensuite utilisée pour majorer $\mathscr{U}_{\mathscr{D}}$ point par point :

$$|\mathscr{U}_{\mathscr{D}}(x)| \leqslant 1 - \frac{1}{(r-1)^5}\|x\|^2,$$

majoration qui peut être utilisée à son tour pour estimer K_m. Nous commençons en reprenant la preuve de la majoration de $\mathscr{U}_{\mathscr{D}}$ dans le but d'améliorer la constante obtenue : elle présentera l'avantage d'être du bon ordre de grandeur en r.

Lemme 3.10. *Soit $\mathscr{D}$ tel que* $\operatorname{pgcd}\mathscr{D} = 1$. *Notons δ le plus petit élément non nul de $\mathscr{D}$ et Δ le plus grand. Alors pour tout $x \in \mathbb{R}$, il existe $d \in \mathscr{D}$ tel que*

$$\|dx\| \geqslant \frac{2}{\delta+\Delta}\|x\|. \tag{3.26}$$

Démonstration. Notons $K := \frac{2}{\delta+\Delta}$ et considérons $x \in \mathbb{R}$ tel que

$$\|\delta x\| < K\|x\|. \tag{3.27}$$

Nous allons montrer l'existence d'un $d \in \mathscr{D}$ vérifiant (3.26).

Écrivons $\delta x = m + \theta$ avec $m \in \mathbb{Z}$, et $|\theta| = \|\delta x\| \leqslant \frac{1}{2}$.

Supposons que $\delta \mid md$ pour tout $d \in \mathscr{D}$. On aurait alors

$$\delta \mid \operatorname{pgcd}(m\mathscr{D}) \;=\; m \operatorname{pgcd} \mathscr{D} \;=\; m.$$

Donc $\frac{m}{\delta}$ est un entier et l'hypothèse (3.27) permet de calculer

$$\|x\| \;=\; \Big\|\frac{m}{\delta} + \frac{\theta}{\delta}\Big\| \;=\; \frac{|\theta|}{\delta} = \frac{\|\delta x\|}{\delta} \;<\; \frac{K}{\delta}\|x\|.$$

Comme $K \leqslant 1$ et $\delta \geqslant 1$, nous aboutissons à une absurdité. Par conséquent, il existe un $d \in \mathscr{D}$ tel que $\delta \nmid md$. Pour un tel $d \in \mathscr{D}$, montrons que $\|dx\| \geqslant K\|x\|$.

On écrit $dx = d\frac{m}{\delta} + d\frac{\theta}{\delta}$, donc

$$\|dx\| \;\geqslant\; \Big\|\frac{dm}{\delta}\Big\| - \frac{d}{\delta}|\theta|.$$

Or

$$\Big\|\frac{dm}{\delta}\Big\| \;\geqslant\; \frac{1}{\delta} \;\geqslant\; \frac{2\|x\|}{\delta}$$

et, à l'aide de l'hypothèse (3.27),

$$\frac{d}{\delta}|\theta| \;=\; \frac{d}{\delta}\|\delta x\| \;\leqslant\; \frac{d}{\delta}K\|x\| \;\leqslant\; \frac{\Delta}{\delta}K\|x\|$$

puisque Δ est le plus grand élément de $\mathscr{D}$. Ainsi

$$\|dx\| \;\geqslant\; \frac{2}{\delta}\|x\| - \frac{\Delta}{\delta}K\|x\|.$$

ce qui termine la preuve puisque $2/\delta - K\Delta/\delta = K$. □

Remarque 3.4. Montrons que la constante de (3.26) est du bon ordre de grandeur :

Si $\mathscr{D} = \{0, 1\}$, nous trouvons que $K = 1$, et nous ne pouvons évidemment pas faire mieux.

Si $\mathscr{D} = \{0, d_1, d_2\}$ avec $d_2 \geqslant 3$ impair et $d_1 := d_2 - 2$. Notons aussi $k := \frac{d_2-1}{2}$ et $l := d_1$ qui sont des entiers tels que

$$k(d_1 + d_2) \;=\; ld_2 + 1.$$

Pour le choix de $x := \frac{l}{d_1+d_2}$, nous avons donc

$$\begin{aligned}
\|d_1 x\| \;&=\; \Big\|\frac{d_1}{d_2}\frac{d_2 l}{d_1 + d_2}\Big\| \;=\; \Big\|l - k + \frac{1}{d_2} - \frac{d_1}{d_2}\frac{1}{d_1 + d_2}\Big\| \\
&=\; \Big\|\frac{1}{d_1 + d_2}\Big\| \;=\; \frac{1}{d_1 + d_2}, \\
\|d_2 x\| \;&=\; \Big\|\frac{d_2 l}{d_1 + d_2}\Big\| \;=\; \Big\|k - \frac{1}{d_1 + d_2}\Big\| \;=\; \frac{1}{d_1 + d_2}.
\end{aligned}$$

Comme $\dfrac{1}{d_1 + d_2} = \dfrac{\|x\|}{d_1}$, nous avons pour tout d de $\mathscr{D}$, $\|dx\| = \dfrac{1}{d_1}\|x\|$. En choisissant $d_1 = r - 3$ ou $r - 4$ suivant la parité de r, nous avons bien trouvé un ensemble $\mathscr{D}$ pour laquelle la constante de (3.26) est presque optimale (du bon ordre de grandeur en r).

Lemme 3.11. *Pour tout réel y, nous avons la majoration*

$$|1+\mathrm{e}(y)| \leqslant 2(1-4\|y\|^2). \tag{3.28}$$

Démonstration. Sans perte de généralité, nous pouvons supposer que $0 \leqslant y \leqslant \frac{1}{2}$ en utilisant la parité et la périodicité de la fonction étudiée. Alors

$$|1+\mathrm{e}(y)| = 2\cos(\pi y) = 2-4\sin^2(\pi y/2).$$

La concavité de $z \mapsto \sin(\pi z/2)$ entre 0 et $\frac{1}{2}$ permet de la minorer cette fonction par sa corde, donc

$$\sin(\pi y/2) \geqslant \sqrt{2}\, y$$

d'où l'on déduit la majoration du lemme. □

Lemme 3.12. *Soit $\mathscr{D}$ une sous-ensemble de $\{0,...,r-1\}$ de cardinal $t \geqslant 2$. Soit $A>0$ tel que pour tout $x \in \mathbb{R}$, il existe d_1 et $d_2 \in \mathscr{D}$ avec $\|(d_1-d_2)x\| \geqslant A\|x\|$. Pour tout $x \in \mathbb{R}$, nous avons*

$$|\mathscr{U}_{\mathscr{D}}(x)| \leqslant 1-\frac{8A^2}{t}\|x\|^2. \tag{3.29}$$

Démonstration. Soit $x \in \mathbb{R}$. Par hypothèse, il existe deux éléments d_1 et $d_2 \in \mathscr{D}$ tels que

$$\|(d_1-d_2)x\| \geqslant A\|x\|. \tag{3.30}$$

Ainsi,

$$\begin{aligned} |\mathscr{U}_{\mathscr{D}}(x)| &= \frac{1}{t}\Big|\sum_{d\in\mathscr{D}} \mathrm{e}(dx)\Big| \\ &\leqslant \frac{1}{t}\,|\mathrm{e}(d_1x)+\mathrm{e}(d_2x)| + \frac{t-2}{t} \\ &\leqslant 1-\frac{2}{t}+\frac{1}{t}\,|1+\mathrm{e}\left((d_1-d_2)x\right)| \end{aligned}$$

en isolant les éléments de $\mathscr{D}$ correspondant à d_1 et d_2. La majoration (3.28) donne

$$\begin{aligned} |\mathscr{U}_{\mathscr{D}}(x)| &\leqslant 1-\frac{2}{t}+\frac{2}{t}\Big(1-4\big\|(d_1-d_2)x\big\|^2\Big) \\ &\leqslant 1-\frac{8A^2}{t}\|x\|^2 \end{aligned}$$

en utilisant (3.30). □

Corollaire 3.1. *Soit $\mathscr{D}$ un sous-ensemble strict de $\{0,...,r-1\}$, de cardinal $t \geqslant 2$, contenant 0 et tel que* $\operatorname{pgcd}\mathscr{D}=1$. *Alors pour tout x réel,*

$$|\mathscr{U}_{\mathscr{D}}(x)| \leqslant 1-\frac{64}{(r+1)^3}\|x\|^2. \tag{3.31}$$

Démonstration. Notons $\mathscr{D}' := (\mathscr{D} - \mathscr{D}) \cap [1, +\infty[$ et δ (respectivement Δ) le plus petit (respectivement grand) élément de$\mathscr{D}'$.

Si $\delta = 1$, cela signifie qu'il existe deux éléments d_1 et d_2 dans $\mathscr{D}$ avec $d_2 = d_1 + 1$. L'hypothèse du lemme 3.12 est donc vérifiée pour le choix de $A := 1$, ce qui implique

$$\left|\mathscr{U}_{\mathscr{D}}(x)\right| \;\leqslant\; 1 - \frac{8}{t}\|x\|^2.$$

Comme $r \geqslant 3$, $r^2+3r-5 \geqslant 0$, donc $r^3+3r^2-5r+7 \geqslant 0$ ce qui se réécrit $(r+1)^3 \geqslant 8(r-1)$. Donc

$$\frac{8}{t} \;\geqslant\; \frac{8}{r-1} \;\geqslant\; \frac{64}{(r+1)^3},$$

ce qui termine la preuve de la majoration du lemme lorsque $\delta = 1$.

Si $t = 2$, comme $\mathscr{D}$ contient 0 et comme $\operatorname{pgcd}\mathscr{D} = 1$, c'est que $\mathscr{D} = \{0, 1\}$ et la majoration (3.31) est vraie.

Nous pouvons donc supposer que $\delta \geqslant 2$ et que $t \geqslant 3$. Comme $0 \in \mathscr{D}$, $\mathscr{D}\backslash\{0\}$ est un sous ensemble de $\mathscr{D}'$, donc $\operatorname{pgcd}\mathscr{D}' = 1$. Nous pouvons donc utiliser le lemme 3.10 avec $\mathscr{D}'$, ce qui permet d'appliquer la majoration du lemme 3.12 et d'obtenir

$$\left|\mathscr{U}_{\mathscr{D}}(x)\right| \;\leqslant\; 1 - \frac{32}{t(\delta+\Delta)^2}\|x\|^2. \tag{3.32}$$

L'hypothèse $0 \in \mathscr{D}$ implique aussi que

- l'ensemble $\mathscr{D}$ est δ bien espacé
- δ est inférieur au plus petit élément non nul de $\mathscr{D}$
- Δ est aussi le plus grand élément de $\mathscr{D}$.

Donc $\delta + (t-2)\delta$ est inférieur à $\Delta \leqslant r - 1$, ce qui donne

$$\delta \;\leqslant\; \frac{r-1}{t-1}. \tag{3.33}$$

Donc

$$t(\delta+\Delta)^2 \;\leqslant\; t\Big(\frac{r-1}{t-1} + r - 1\Big)^2 \;=\; (r-1)^2\frac{t^3}{(t-1)^2} \;=: P(t).$$

Nous avons

$$P'(t) \;=\; (r-1)^2\frac{t^2(t-3)}{(t-1)^3} \;\geqslant\; 0,$$

donc P est croissante. La majoration (3.33) et notre hypothèse $\delta \geqslant 2$ fournit $t \leqslant \frac{r+1}{2}$, donc

$$t(\delta+\Delta)^2 \;\leqslant\; P\Big(\frac{r+1}{2}\Big) \;=\; \frac{(r+1)^3}{2}.$$

La démonstration du lemme est achevée en reportant cette estimation dans (3.32). □

Lemme 3.13. *Définissons M_m par*

$$M_m \;=\; \max_{u\in[0,1]} \frac{1}{r} \sum_{0\leqslant h<r} \Big|\mathscr{U}_{\mathscr{D}}\Big(\frac{u+h}{r}\Big)\Big|^m.$$

Alors $K_m \leqslant M_m$ pour tout $m \geqslant 1$.

Démonstration. Prenons $N \geqslant 1$ et calculons l'intégrale de ${G_{\mathscr{D},N}}^{2l}$ en découpant le segment $[0,1]$ en r sous-segments de longueur $\frac{1}{r}$:

$$\begin{aligned}
\left\|{G_{\mathscr{D},N}}^m\right\|_1 &= \sum_{0\leqslant h<r} \int_{\frac{h}{r}}^{\frac{h+1}{r}} \prod_{k<N} \left|\mathscr{U}_{\mathscr{D}}(r^k s)\right|^m \mathrm{d}s \\
&= \sum_{0\leqslant h<r} \int_{\frac{h}{r}}^{\frac{h+1}{r}} \left|\mathscr{U}_{\mathscr{D}}(s)\right|^m \prod_{k<N-1} \left|\mathscr{U}_{\mathscr{D}}(r^k r s)\right|^m \mathrm{d}s \\
&= \sum_{0\leqslant h<r} \int_0^1 \left|\mathscr{U}_{\mathscr{D}}(\frac{u+h}{r})\right|^m \prod_{k<N-1} \left|\mathscr{U}_{\mathscr{D}}(r^k(u+h))\right|^m \mathrm{d}u \\
&= \sum_{0\leqslant h<r} \int_0^1 \left|\mathscr{U}_{\mathscr{D}}(\frac{u+h}{r})\right|^m \left|G_{\mathscr{D},N-1}\right|^m \mathrm{d}u
\end{aligned}$$

puisque $G_{\mathscr{D},N-1}$ est de période 1. La définition de M_m implique donc

$$\left\|{G_{\mathscr{D},N}}^m\right\|_1 \leqslant M_m \left\|{G_{\mathscr{D},N-1}}^m\right\|_1 \leqslant \ldots \leqslant {M_m}^N$$

qui est un résultat plus précis que celui annoncé dans le lemme. □

Lemme 3.14. *Soit $B > 0$ tel que, pour tout $x \in \mathbb{R}$,*

$$|\mathscr{U}_{\mathscr{D}}(x)| \leqslant 1 - B\|x\|^2. \tag{3.34}$$

Pour tout $m \geqslant 1$,

$$M_m < \frac{1}{r} + \sqrt{\frac{\pi}{mB}}.$$

Démonstration. Utilisons notre hypothèse (3.34) pour majorer directement $\mathscr{U}_{\mathscr{D}}$ dans la définition de M_m. Ainsi,

$$M_m \leqslant \max_{u\in[0,1]} \frac{1}{r} \sum_{0\leqslant h<r} \Big(1 - B\Big\|\frac{u+h}{r}\Big\|^2\Big)^m.$$

Mais si $u \in [0,1]$,

$$\frac{1}{r} \sum_{0\leqslant h<r} \Big(1 - B\Big\|\frac{u+h}{r}\Big\|^2\Big)^m \leqslant \frac{1}{r} \sum_{-\frac{r}{2}\leqslant h\leqslant\frac{r}{2}} \Big(1 - B\frac{(u+h)^2}{r^2}\Big)^m$$

puisque $\|\frac{u+h}{r}\| = \|\frac{u+h-r}{r}\|$.

Dans le membre de droite, chaque terme de la somme est une fonction concave de u. Cette somme est donc aussi une fonction concave de u. La symétrie sur h impliquant celle en u, la dérivée de cette fonction majorante s'annule donc pour $u = 0$. Le maximum du membre de droite est donc atteint pour $u = 0$. Ainsi,

$$\begin{aligned}
M_m &\leqslant \frac{1}{r} \sum_{-\frac{r}{2}\leqslant h\leqslant\frac{r}{2}} \Big(1 - \frac{B}{r^2}h^2\Big)^m \qquad (3.35)\\
&\leqslant \frac{1}{r} + \frac{2}{r} \sum_{1\leqslant h\leqslant\frac{r}{2}} \exp\Big(-\frac{mB}{r^2}h^2\Big) \\
&\leqslant \frac{1}{r} + \frac{2}{r} \int_0^{\frac{r}{2}} \exp\,(-\frac{mB}{r^2}s^2)\mathrm{d}s \\
&< \frac{1}{r} + \frac{2}{\sqrt{mB}} \int_0^{\infty} \exp\,(-u^2)\mathrm{d}u
\end{aligned}$$

qui est bien le résultat du lemme 3.14. □

Chapitre 4

Preuve des Théorèmes 2.1 à 2.4

4.1 Preuve du Théorème 2.1

Les lemmes 3.9 et 3.2 donnent les inégalités (2.9).

4.2 Preuve des Théorèmes 2.2 et 2.3

Les lemmes 3.12 3.13 et 3.14 donnent la majoration, le lemme 3.2 la minoration des inégalités (2.11).

Le lemme 3.10 fournit la preuve de (2.12). La majoration de (2.13) s'obtient en utilisant le corollaire 3.1 et les lemmes 3.13 et 3.14.

4.3 Preuve du Théorème 2.4

Si m est assez grand, on a $K_m = \frac{1}{r} + O_r(\frac{1}{\sqrt{m}})$. Donc l'hypothèse (3.12) du Lemme 3.7 est vérifiée pour m assez grand (pouvant dépendre de r). Le Théorème 2.4 est donc vrai pour le cas général.

Il reste à montrer que les valeurs annoncées sont possibles : numériquement, en utilisant le Théorème 2.3, il suffit de trouver un entier pair m avec

$$m \ > \ \frac{\pi}{64} \frac{(r+1)^3 r^2}{(r^{1/2k}-1)^2}.$$

Nous pouvons donc trouver un entier pair m vérifiant l'hypothèse (3.12) avec

$$m \ < \ \frac{\pi}{64} \frac{(r+1)^5}{(r^{1/2k}-1)^2}.$$

Finalement, nous pouvons prendre

$$c \ = \ \frac{1}{2km} \ > \ \frac{32}{\pi} \frac{(r^{1/2k}-1)^2}{k(r+1)^5},$$

ce qui termine la démonstration de (2.14).

Dans le cas où $\mathscr{D} = \{0, 1\}$ et $k = 2$, le Théorème 2.4 annonce une meilleure constante c. Pour l'obtenir, nous avons intérêt de choisir l le plus petit possible pour que l'inégalité (3.12) reste vraie. Le choix de

$$l := \left\lceil \frac{r^{1.5}}{\pi} + \frac{1}{8} \right\rceil$$

vérifie l'hypothèse (3.12) et permet de prendre

$$c \;=\; \frac{1}{8l} \;>\; \frac{\pi}{8} r^{-\frac{3}{2}} (1 - 2r^{-\frac{1}{4}})$$

dans (2.15).

Deuxième partie

Nombres ellipséphiques friables

Chapitre 5

Énoncé des résultats

Soient $r \geqslant 3$ un entier et $\mathscr{D}$ un sous-ensemble strict de $\{0, \dots, r-1\}$ dont nous notons $t := \#\mathscr{D}$ le cardinal. Nous supposons $t \geqslant 2$ et nous posons

$$\rho \ := \ \frac{\log t}{\log r} \in]0,1[. \tag{5.1}$$

Nous désignons par $W_{\mathscr{D}}$ l'ensemble des entiers ellipséphiques :

$$W_{\mathscr{D}} \ := \ \Big\{ \sum_j d_j r^j \ / \ \forall j, \ d_j \in \mathscr{D} \Big\},$$

où toutes les sommes sur j sont finies. Nous notons aussi

$$\begin{aligned} W_{\mathscr{D}}(x) \ &:= \ \{n \in W_{\mathscr{D}}, \ n < x\}, \\ W_{\mathscr{D}}(x,a,q) \ &:= \ \{n \in W_{\mathscr{D}}, \ n < x, \ n \equiv a \mod q\}. \end{aligned}$$

C. Dartyge et C. Mauduit [DM00], et indépendamment S. Konyagin [Kon01] ont prouvé l'existence d'un nombre $\theta > 0$ tel qu'en moyenne sur les diviseurs $q < x^\theta$, le défaut moyen de répartition dans les progressions arithmétiques des nombres ellipséphiques est "petit" :

Théorème A. *Il existe un exposant $\beta > 0$ tel que pour tout $\epsilon > 0$ et $A > 0$, nous avons la majoration*

$$\sum_{\substack{q < x^{\beta-\epsilon} \\ (q, r(r+1))=1}} \Big| \#W_{\mathscr{D}}(x,0,q) - \frac{\#W_{\mathscr{D}}(x)}{q} \Big| \ \ll_{A,\epsilon} \ \frac{\#W_{\mathscr{D}}(x)}{\log^A x}. \tag{5.2}$$

Comme par exemple E. Fouvry et C. Mauduit [FM96], nous appellerons *exposant de répartition* pour $W_{\mathscr{D}}$ tout nombre β vérifiant cette inégalité (5.2).

Dans l'étude des propriétés multiplicatives des nombres ellipséphiques, une question naturelle est de savoir s'il existe des nombres *friables*, c'est-à-dire ne possédant que des petits facteurs premiers. Étant donné un entier n, désignons par $P^+(n)$ et $P^-(n)$ son plus grand et plus petit facteur premier avec les conventions traditionnelles $P^+(1) = 1$ et $P^-(1) = \infty$. S. Konyagin, C. Mauduit et A. Sárközy dans [KMS00] ont posé la question

Problème 5.1. *Est-il vrai que pour tous $\epsilon > 0$ et r, $\mathscr{D}$ fixés, nous avons uniformément pour x assez grand,*

$$\#\{n \in W_{\mathscr{D}}(x),\ P^+(n) < n^\epsilon\} \gg_{r,\epsilon} \#W_{\mathscr{D}}(x) \ ? \tag{5.3}$$

Un premier pas a été franchi pour le cas des nombres s'écrivant avec un unique chiffre, $n = d\frac{r^k-1}{r-1}$:

Théorème B (A. Sárközy, P. Erdös, C. Mauduit [EMS99, théorème 4])**.** *Soient $r \geqslant 2$ et un chiffre $d \in \{1, .., r-1\}$. Il existe une constante $c_r > 0$ et une infinité de nombres $n \in W_{\{d\}}$ pour lesquels*

$$P^+(n) \ < \ \exp\Big(c_r \frac{\log n}{\log_2 n}\Big).$$

où nous avons utilisé la notation $\log_2(x) := \log\log(x)$.

Remarquons que ce cas particulier garantit l'existence d'une infinité (mais en proportion nulle) de nombre ellipséphiques répondant à la question posée. Aucun autre résultat sur les entiers ellipséphiques friables n'existe dans la littérature à notre connaissance aujourd'hui. Les théorèmes 5.1 et5.2 ci-dessous nous permettent de répondre partiellement au problème 5.1 : nous montrons que pour tous r et $\mathscr{D}$ fixés, il existe un nombre $0 < \alpha < 1$ tel qu'une proportion positive d'entiers ellipséphiques sont x^α friables. De plus, le corollaire 5.5 fournit pour chaque $\epsilon > 0$, des exemples de familles $\mathscr{D}$ et d'entiers r pour lesquels la minoration (5.3) est vraie.

La recherche d'une évaluation quantitative des nombres ellipséphiques friables nous amène à introduire

$$\Psi_{\mathscr{D}}(x, y) \ := \ \#\Big\{n \in W_{\mathscr{D}}(x) \,/\, P^+(n) \leqslant y\Big\}.$$

L'équation (5.3) s'écrit alors de façon équivalente

$$\Psi_{\mathscr{D}}(x, x^\epsilon) \ \gg_{r,\epsilon} \ \#W_{\mathscr{D}}(x). \tag{5.4}$$

Remarque 5.1. Le cas exclu $\mathscr{D} = \{0, ..., r-1\}$ correspond à $W_{\mathscr{D}} = \mathbb{N}$ et donne la fonction $\Psi(x, y)$, étudiée par exemple par K. Alladi, N. G. De Bruijn, A. Hildebrand et G. Tenenbaum [All82, dB51, HT93]. Toute fonction puissance convient alors pour y : pour tout $\alpha > 0$, nous avons $\Psi(x, x^\alpha) \gg_\alpha x$ (la formule de Hildebrand [Hil86, Théorème 1] fournit un équivalent dans une bien plus vaste région).

Pour estimer le nombre d'éléments friables d'une suite donnée, nous aurons recours à des méthodes de crible voisines à celles utilisées par J. B. Friedlander [Fri89] dans l'étude des entiers $(p_n - a)_n$ friables, où p_1,...,p_n,... désigne la suite des nombres premiers, ou par C. Dartyge, G. Martin et G. Tenenbaum [DMT01] pour celle des entiers $(F(n))_n$ friables, F étant un polynôme à coefficients entiers. Nous montrons alors le théorème :

Théorème 5.1. *Soit $0 < \beta \leqslant \frac{1}{2}$ un exposant de répartition pour $W_{\mathscr{D}}$. Pour tout $\alpha > 1 - \beta$, nous avons :*

$$\Psi_{\mathscr{D}}(x, x^\alpha) \ \gg_{r,\alpha} \ \#W_{\mathscr{D}}(x).$$

Lorsque l'exposant de répartition est supérieur à $\frac{1}{2}$, le résultat du théorème 5.1 reste valable, mais la démonstration est légèrement plus technique. En utilisant une méthode plus sophistiquée, nous pourrons même obtenir un plus petit exposant α, mais les termes d'erreurs

$$\mathscr{R}_q(x) \ := \ \#W_{\mathscr{D}}(x,0,q) - \frac{1}{q}\#W_{\mathscr{D}}(x) \tag{5.5}$$

que nous savons estimer en moyenne grâce à (5.2) apparaissent alors naturellement pondérés par $\tau(q)$, le nombre de diviseurs de q. La suite $W_{\mathscr{D}}$ étant trop rare, la technique utilisée par J. B. Friedlander [Fri89] ou par G. Tenenbaum et E. Fouvry [FT96, paragraphe 7] dans une situation voisine est insuffisante pour nous ramener sans perte à la simple recherche d'un exposant de répartition. Au paragraphe 7, nous énonçons le théorème 7.1 qui permet d'éviter cette difficulté : en modifiant les poids du crible de Rosser-Iwaniec, nous gardons un contrôle sur le nombre de diviseurs de q et nous pouvons ainsi écarter les entiers possédant un nombre anormalement grand de diviseurs. Ce théorème 7.1 permet d'obtenir le théorème

Théorème 5.2. *Notons $\Phi(W,Y)$ la fonction définie par*

$$\Phi(W,Y) \ := \ 1+\rho\Big(\frac{W}{Y}\Big) - \frac{1-W}{Y}, \tag{5.6}$$

où ρ désigne la fonction de Dickman, définie (par exemple dans [Ten95, paragraphe 5.4 p. 375]) comme la solution de l'équation différentielle avec retard

$$u\rho'(u)+\rho(u-1) \ = \ 0 \qquad \text{et} \qquad \rho(u) \ = \ 1 \quad \text{pour } u \leqslant 1.$$

Pour tout $0<W<1$, l'équation

$$\Phi(W,Y)=0 \tag{5.7}$$

possède une unique solution $Y=\alpha_W$. Pour $\frac{1}{3}<W<1$, la fonction $W\mapsto\alpha_W$ est strictement décroissante, concave et $\alpha_W<1-W$.

Soit $\beta>\frac{1}{2}$ un exposant de répartition pour $W_{\mathscr{D}}$. Pour tout $\alpha>\alpha_\beta$, nous avons :

$$\Psi_{\mathscr{D}}(x,x^\alpha) \ \gg_{r,\alpha} \ \#W_{\mathscr{D}}(x).$$

L'essentiel de cette partie est consacrée à la preuve du théorème 5.2. La démonstration du théorème 5.1 est bien plus courte.

Remarque 5.2. La fonction $W\mapsto\alpha_W$ est tracée à la figure 8.1, paragraphe 8.6. Ce graphe résume les résultats des deux théorèmes. Si le théorème 5.2 apporte toujours un meilleur exposant que $1-\beta$, qui correspond au prolongement du résultat du théorème 5.1, ce gain n'est significatif que lorsque l'exposant de répartition β est compris entre 0.5 et 0.75.

En utilisant les exposants de répartition obtenus par C. Dartyge et C. Mauduit [DM00], nous obtiendrons alors

Corollaire 5.1. *Soient $\mathscr{D}=\{0,1\}$ et $r\geqslant 3$ fixé. Notons*

$$\alpha \ := \ 1-\frac{\pi}{4r}\Big(1-\frac{3\pi}{4r}\Big).$$

Uniformément pour $x \geqslant 2$,

$$\Psi_{\mathscr{D}}(x, x^{\alpha}) \gg_r \#W_{\mathscr{D}}(x).$$

Pour les petites valeurs de r, de meilleurs exposants sont obtenus par les mêmes auteurs dans [DM01] :

Corollaire 5.2. *Soient* $\mathscr{D} = \{0, 1\}$ *et* $r \geqslant 3$ *fixés. Prenons* α *comme suit*

r	3	4	5	6	7	8	9	10
α	0.658	0.751	0.848	0.864	0.875	0.907	0.912	0.916

Uniformément pour $x \geqslant 2$,

$$\Psi_{\mathscr{D}}(x, x^{\alpha}) \gg_r \#W_{\mathscr{D}}(x).$$

Si $\mathscr{D}$ est quelconque, l'équation (2.3) du Théorème 2.3 de cette thèse et le Théorème 1 de [DM00] impliquent qu'il existe un nombre α,

$$\alpha > \frac{16}{\pi r^3}\Big(1 - \frac{2}{\sqrt{r}}\Big),$$

qui est un exposant de distribution. Nous en déduisons immédiatement le

Corollaire 5.3. *Supposons toujours que* $0 \in \mathscr{D}$ *et* $t = \#\mathscr{D} \geqslant 2$. *Choisissons*

$$\alpha := 1 - \frac{16}{\pi r^3}\Big(1 - \frac{2}{\sqrt{r}}\Big).$$

Alors

$$\Psi_{\mathscr{D}}(x, x^{\alpha}) \gg_r \#W_{\mathscr{D}}(x).$$

Les résultats de C. Dartyge et C. Mauduit [DM01] permettent aussi de trouver des familles $\mathscr{D}$ pour lesquelles l'exposant de répartition est très important et donc pour lesquelles le théorème 5.2 apporte un gain :

Corollaire 5.4. *Soient* r *assez grand et* t *un entier soumis à la condition*

$$t \geqslant r^{1/2}\log r + r^{1/2}.$$

Si $\mathscr{D}$ *est la famille* $\{0, 1, \ldots, t-1\}$, *nous avons uniformément pour* $x \geqslant 2$,

$$\Psi_{\mathscr{D}}(x, x^{\alpha}) \gg_r \#W_{\mathscr{D}}(x) \qquad \textit{avec} \qquad \alpha := 0.32111.$$

Corollaire 5.5. *Soit* $\epsilon > 0$ *assez petit fixé. Il existe* r *et* $\mathscr{D}$ *tels que*

$$\Psi_{\mathscr{D}}(x, x^{\epsilon}) \gg_r \#W_{\mathscr{D}}(x).$$

Par exemple, il suffit que $\mathscr{D} = \{0, 1, ..., t-1\}$ *et que* r *et* t *vérifient*

$$r \geqslant \frac{1+\epsilon}{\epsilon}\log\frac{1}{\epsilon} \qquad \textit{et} \qquad t \geqslant \mathrm{e}^{-\frac{1}{2}}\, r^{1-\epsilon}\log r.$$

Chapitre 6

Exposant de friabilité pour $\beta \leqslant \frac{1}{2}$: preuve du Théorème 5.1

Remarque 6.1. Ce théorème pourrait aussi être démontré comme un corollaire aux lemmes nécessaires à la démonstration du théorème 5.2. Nous le traitons tout de même séparément car sa preuve est nettement moins technique et met en œuvre très peu de crible.

Soit $0 < \beta \leqslant \frac{1}{2}$ un exposant de répartition (défini dans le théorème A). Soit $\alpha > 1-\beta$ et notons $y = x^\alpha$. Introduisons trois paramètres supplémentaires v, w et z tels que

$$0 \ < \ z \ \leqslant \ v \ \leqslant \ w \ < \ x. \tag{6.1}$$

Pour évaluer $P^+(n)$, observons que si $d \mid n$, tout facteur premier p de n est un diviseur de d ou de $\frac{n}{d}$ donc vérifie $p \leqslant \max\{d, \frac{n}{d}\}$. En particulier, pour tout diviseur d de n, $P^+(n) \leqslant \max\{d, \frac{n}{d}\}$. Imposons

$$y \ \geqslant \ \max\{w, x/v\}. \tag{6.2}$$

En comptant seulement les entiers ellipséphiques possédant un diviseur ni trop grand ni trop petit, nous avons

$$\Psi_{\mathscr{D}}(x,y) \ \geqslant \ \#\left\{n \in W_{\mathscr{D}}(x) \ / \ \exists\, k|n,\, v < k \leqslant w\right\}$$

puisque si n est compté dans le membre de droite ci-dessus, alors

$$P^+(n) \ \leqslant \ \max\left\{k, \tfrac{n}{k}\right\} \ \leqslant \ \max\left\{w, \tfrac{x}{v}\right\} \ \leqslant \ y.$$

Pour avoir un meilleur contrôle, nous comptons seulement les diviseurs k sans petit facteur premier :

$$\Psi_{\mathscr{D}}(x,y) \ \geqslant \ \#\left\{n \in W_{\mathscr{D}}(x) \ / \ \exists\, k|n,\, v < k \leqslant w,\, P^-(k) \geqslant z\right\}. \tag{6.3}$$

Pour alléger les notations, nous utilisons la fonction multiplicative $u_z(\cdot)$ définie par

$$u_z(k) \ := \ \begin{cases} 1 & \text{si } P^-(k) \geqslant z, \\ 0 & \text{sinon} \end{cases} \tag{6.4}$$

et $U_z(x)$ sa fonction sommatoire :

$$U_z(x) \ := \ \sum_{k<x} u_z(k).$$

Cette fonction est très souvent appelée $\Phi(x,z)$. Comme u_z est une fonction multiplicative, la convolée $u_z * \mathbb{1}$ l'est aussi. Nous avons donc l'estimation

$$\sum_{k|n} u_z(k) \ = \ u_z * \mathbb{1}(n) \ = \ \prod_{\substack{p^\nu \| n \\ p \geqslant z}} (\nu+1).$$

En majorant $\nu+1$ par 2^ν dans chaque terme du produit (majoration précise au moins lorsque n ne possède pas de grandes puissances), nous avons donc

$$\sum_{k|n} u_z(k) \ \leqslant \ 2^{\frac{\log n}{\log z}}. \tag{6.5}$$

Cette majoration (6.5) explique l'introduction du paramètre z : le membre de droite est en effet borné dès que z est une puissance de x. Nous reportons l'estimation (6.5) dans (6.3) pour obtenir

$$\begin{aligned}\Psi_{\mathscr{D}}(x,y) \ &\geqslant \ \sum_{n\in W_{\mathscr{D}}(x)} 2^{-\frac{\log n}{\log z}} \sum_{\substack{v<k\leqslant w \\ k|n}} u_z(k) \\ &\geqslant \ 2^{-\frac{\log x}{\log z}} \sum_{v<k\leqslant w} u_z(k) \sum_{n\in W_{\mathscr{D}}(x,0,k)} 1.\end{aligned}$$

La définition (5.5) du reste $\mathscr{R}_k(x)$ fournit donc,

$$\Psi_{\mathscr{D}}(x,y) \ \geqslant \ 2^{-\frac{\log x}{\log z}} \sum_{v<k\leqslant w} u_z(k)\Big(\frac{\#W_{\mathscr{D}}(x)}{k} - |\mathscr{R}_k(x)|\Big), \tag{6.6}$$

Nous avons l'estimation classique du nombre d'entiers criblés (voir par exemple [Ten95, théorème 3, paragraphe III.6.2, p. 406]) :

Lemme 6.1. *Uniformément pour $2 \leqslant z \leqslant x$, nous avons*

$$\frac{U_z(x)}{x} \ = \ \frac{1}{\log z}\omega\Big(\frac{\log x}{\log z}\Big) - \frac{z}{x\log z} + O\Big(\frac{1}{\log^2 z}\Big),$$

ω étant la fonction de Buchstab (voir par exemple [Ten95]) : c'est la solution de l'équation différentielle avec retard

$$(u\omega(u))' \ = \ \omega(u-1) \qquad \text{et} \qquad u\omega(u) \ = \ 1 \quad \text{pour } 1 \leqslant u \leqslant 2.$$

Elle est minorée par $\frac{1}{2}$ et majorée par 1 telle que $\omega(u) = \mathrm{e}^{-\gamma} + O(u^{-\frac{u}{2}})$ où γ désigne traditionnellement la constante d'Euler.

Corollaire 6.1. *Uniformément pour $2 \leqslant z\log z \leqslant v \leqslant w$,*

$$\sum_{v\leqslant n<w} \frac{u_z(n)}{n} \ \geqslant \ \frac{1}{2}\frac{\log\frac{w}{v}}{\log z}\Big(1 + O\Big(\frac{1}{\log z} + \frac{1}{\log\frac{w}{v}}\Big)\Big). \tag{6.7}$$

$$\sum_{v\leqslant n<w} \frac{u_z(n)}{n} \ = \ \mathrm{e}^{-\gamma}\frac{\log\frac{w}{v}}{\log z}\Big(1 + O\Big(\frac{1}{\log z} + \frac{\log z}{\log\frac{w}{v}}\Big)\Big). \tag{6.8}$$

Démonstration. Une intégration par parties et le lemme 6.1 donnent

$$\begin{aligned}\sum_{v\leqslant n<w}\frac{u_z(n)}{n} &= \int_v^w \frac{1}{u}\,\mathrm{d}U_z(u)\\ &= O\Big(\frac{1}{\log z}\Big)+\int_v^w \omega\Big(\frac{\log u}{\log z}\Big)\frac{\mathrm{d}u}{u\log z}\Big(1+O\Big(\frac{1}{\log z}\Big)\Big)\\ &= O\Big(\frac{1}{\log z}\Big)+\int_{\frac{\log v}{\log z}}^{\frac{\log w}{\log z}} \omega(s)\mathrm{d}s\Big(1+O\Big(\frac{1}{\log z}\Big)\Big).\end{aligned}$$

L'estimation asymptotique $\omega(s)=\mathrm{e}^{-\gamma}+O\big(\mathrm{e}^{-s}\big)$ fournit donc

$$\sum_{v\leqslant n<w}\frac{u_z(n)}{n} = O(1)+\mathrm{e}^{-\gamma}\frac{\log\frac{w}{v}}{\log z}\Big(1+O\Big(\frac{1}{\log z}\Big)\Big)$$

ce qui démontre l'estimation (6.8). La minoration $\omega(s)\geqslant\frac12$ fournit aussi

$$\sum_{v\leqslant n<w}\frac{u_z(n)}{n} = O\Big(\frac{1}{\log z}\Big)+\frac12\frac{\log\frac{w}{v}}{\log z}\Big(1+O\Big(\frac{1}{\log z}\Big)\Big)$$

ce qui démontre la minoration (6.7). □

Si z est assez grand (dès que $z>\tilde r:=r(r+1)$ par exemple), nous obtenons la minoration

$$\Psi_{\mathscr{D}}(x,y)\ \geqslant\ 2^{-\frac{\log x}{\log z}}\Big\{\frac12\frac{\log\frac{w}{v}}{\log z}\#W_{\mathscr{D}}(x)\Big(1+O\big(\frac{1}{\log z}+\frac{1}{\log\frac{w}{v}}\big)\Big)-\sum_{\substack{k\leqslant w\\(k,\tilde r)=1}}|\mathscr{R}_k(x)|\Big\}$$

en reportant l'équation (6.7) dans (6.6). La définition de l'exposant de répartition fournit donc le résultat du théorème 5.1 dès qu'il existe une constante $\epsilon>0$ avec

$$z\ \geqslant\ x^{\epsilon},\qquad v\ \geqslant\ z\log z,\qquad \frac{w}{v}\ \geqslant\ x^{\epsilon}\qquad\text{et}\qquad w\ \leqslant\ x^{\beta-\epsilon}.$$

Ces choix sont possibles en prenant $\epsilon>0$ assez petit et

$$w\ :=\ x^{\beta-\epsilon},\qquad v\ :=\ x^{\beta-2\epsilon}\qquad\text{et}\qquad z\ :=\ x^{\epsilon}.$$

Comme $\beta\leqslant\frac12$, en prenant $\alpha:=1-\beta+2\epsilon$, l'hypothèse (6.2) est bien validée :

$$x^{\alpha}\ \geqslant\ \frac{x}{v}\qquad\text{et}\qquad x^{\alpha}\ \geqslant\ w,$$

ce qui termine la preuve du théorème en choisissant ϵ assez petit.

Chapitre 7

Crible de Rosser-Iwaniec modifié

La principale motivation de cette partie est de modifier le crible de Rosser-Iwaniec en y ajoutant une condition de type Brun portant sur le nombre de facteurs premiers : nous ne conservons dans le système de poids que les entiers possédant au plus R facteurs premiers, R étant une constante arbitraire. Ceci nous permettra de ramener l'étude d'une somme du type de

$$\sum_{q<Q} \tau(q)|\mathscr{R}_q|$$

obtenue comme terme d'erreur de l'utilisation du crible à la recherche d'un exposant de répartition, ce qui nous est donné par le Théorème A.

7.1 Notations et résultats.

Rappelons les notations classiques du crible linéaire, utilisées par exemple par S. Halberstam et H. E. Richert dans [HR74] ou H. Iwaniec dans [Iwa80] :
- $\mathscr{P}$ est un ensemble de nombres premiers. Nous notons alors

$$\mathscr{R}(z) \ := \ \#\{p \in \mathscr{R},\ p < z\} \qquad \text{et} \qquad P(z) \ := \prod_{p \in \mathscr{R}(z)} p.$$

- $\mathscr{A}$ est une suite d'entiers et pour tout d, $\mathscr{A}_d$ est l'ensemble des éléments de $\mathscr{A}$ multiples de d *i.e.* $\mathscr{A}_d := \{a \in \mathscr{A},\ d \mid a\}$.
- $X > 0$ est une approximation de $\#\mathscr{A}$.
- On suppose qu'il existe une fonction multiplicative ρ vérifiant pour tout $p \in \mathscr{P}$,

$$0 \leqslant \rho(p) < p$$

et telle que pour tout les d sans facteur carré, les quantités

$$\mathscr{R}_d \ := \ \#\mathscr{A}_d - \frac{\rho(d)}{d} X, \tag{7.1}$$

sont des terme d'erreur suffisamment petits au moins en moyenne.
- Nous imposons les conditions sur $\mathscr{R}$ et ρ au travers de la fonction

$$V(z) := \prod_{p\in\mathscr{R}(z)} \Big(1-\frac{\rho(p)}{p}\Big),$$

à savoir qu'il existe une constante $L \geqslant 1$ telle que, pour tout $2 \leqslant w < z$,

$$\frac{V(w)}{V(z)} \leqslant \Big(1+\frac{L}{\log w}\Big)\frac{\log z}{\log w}, \tag{7.2}$$

condition d'application du crible linéaire.
- Nous noterons $f(s)$ et $F(s)$ les fonctions de minoration et de majoration du crible linéaire (voir [Iwa80] pour une définition précise) : ce sont des fonctions monotones qui vérifient

$$\begin{aligned} 0 < f(s) < 1 < F(s) \qquad & \text{pour } s > 2, \\ F(s) = 1 + O(\mathrm{e}^{-s}) \qquad & \text{lorsque } s \to \infty, \\ f(s) = 1 + O(\mathrm{e}^{-s})) \qquad & \text{lorsque } s \to \infty. \end{aligned}$$

- Pour tout $D \geqslant z \geqslant 2$, nous définissons enfin s par la relation $D = z^s$.

Dans ce chapitre nous montrons la variante suivante du résultat d'Iwaniec [Iwa80]

Théorème 7.1. *Uniformément pour tous $\mathscr{P}$, ρ et $L \geqslant 1$, $\mathscr{A}$ une partie finie de $\mathbb{N}^*$, $D \geqslant z \geqslant 2$, $X > 0$ et $R \geqslant 3$ vérifiant l'hypothèse du crible linéaire (7.2),*

$$\begin{aligned} \sum_{\substack{a\in\mathscr{A}\\(a,P(z))=1}} 1 &\geqslant XV(z)(f(s)+O(\mathscr{E})) - \sum_{\substack{d<D\\d\mid P(z)\\\omega(d)\leqslant R}} |\mathscr{R}_d| \\ \sum_{\substack{a\in\mathscr{A}\\(a,P(z))=1}} 1 &\leqslant XV(z)(F(s)+O(\mathscr{E})) + \sum_{\substack{d<D\\d\mid P(z)\\\omega(d)\leqslant R}} |\mathscr{R}_d| \end{aligned}$$

en ayant noté $\mathscr{E} := \mathrm{e}^{\sqrt{L}}\, s^{-\frac{s}{2}} \log^{-\frac{1}{3}} D + \log z \Big(\dfrac{\mathrm{e}\log(L\log z)+4}{R-2}\Big)^{R-2}$.

En imposant à R d'être suffisamment grand (par rapport à s et à z), nous pouvons garder le même terme d'erreur que celui de [Iwa80, théorème 1] :

Corollaire 7.1. *Soit η tel que $\eta \log \frac{\eta}{e} \geqslant \frac{4}{3}$. Par exemple tout $\eta \geqslant 3.845$ convient. Si*

$$R \geqslant \eta \log(L\log z) + \frac{1}{\log\eta - 1}(s+\frac{1}{3})\log s + O(1), \tag{7.3}$$

$$(s+\frac{1}{3})\log s \ll \log(L\log z), \tag{7.4}$$

alors dans le Théorème 7.1 précédant $\mathscr{E} \ll e^{\sqrt{L}} s^{-s} \log^{-\frac{1}{3}} D$, la constante implicite dépendant au plus de celles de (7.3) et (7.4).

Démonstration. Notre hypothèse (7.4) permet d'utiliser la majoration (1.7) de [Iwa80] à la place de (1.6) pour le premier terme de $\mathscr{E}$. Nous reportons la majoration de R dans le second terme de $\mathscr{E}$ du Théorème 7.1 qui est décroissant avec R et le corollaire est démontré. □

Remarque 7.1. Une adaption de cette méthode est également possible dans le cas du crible non linéaire *i.e.* dans le cas où la condition (7.2) est remplacée par : il existe un $\kappa > 0$ tel que, pour tout $2 \leqslant w < z$,

$$\frac{V(w)}{V(z)} \ \leqslant \ \Big(1 + \frac{L}{\log w}\Big)\Big(\frac{\log z}{\log w}\Big)^{\kappa}. \tag{7.5}$$

7.2 Preuve du Théorème 7.1

Supposons pour commencer que R est un entier impair. Définissons la fonction de Möbius tronquée λ^- par $\lambda_d^- := \mu(d)$ si

$$\begin{aligned} &(i) \quad r \leqslant R \\ &(ii) \quad \text{pour tout } l \leqslant \frac{r}{2}, \text{ nous avons } p_1 \cdots p_{l-1} \cdot {p_l}^3 < D \end{aligned}$$

en ayant décomposé $d = p_1 \cdots p_r$ en facteurs premiers avec $p_1 \geqslant ... \geqslant p_r$. Dans le cas contraire, définissons $\lambda_d^- := 0$.

Remarque 7.2. Si nous supprimons la condition *(i)* (c'est-à-dire si R est suffisamment grand), nous retrouvons les poids de Rosser définis dans l'article d'H. Iwaniec [Iwa81, p. 207].

Nous allons maintenant prouver que (λ_d^-) vérifie

$$\lambda^- * 1(n) \ \leqslant \ \mu * 1(n) \ = \ \delta(n), \tag{7.6}$$

en ayant noté 1 la suite identiquement égale à 1 et δ l'unité de la convolution (nous rappelons que $\delta(n) = 0$ pour $n \geqslant 2$ et $\delta(1) = 1$). Remarquons que nous pouvons supposer n sans facteur carré, car $\lambda^- * 1(n) = \lambda^- * 1(k_n)$, où $k_n := \prod_{p|n} p$ est le plus grand diviseur de n sans facteur carré. Enfin, remarquons que l'inégalité est une égalité lorsque n=1.

Fixons donc $n \neq 1$ sans facteur carré et notons $p := P^-(n)$ son plus petit facteur premier. L'inégalité (7.6) est équivalente à $\#L_n^+ \leqslant \#L_n^-$ en posant

$$L_n^- := \{d | n, \ \lambda_d^- = -1\} \qquad \text{et} \qquad L_n^+ := \{d | n, \ \lambda_d^- = 1\}.$$

Pour réaliser cette majoration, construisons une injection de L_n^+ dans L_n^- :

$$\begin{aligned} j := \ \{d, \ d \mid n\} \ &\longrightarrow \ \{d, \ d \mid n\} \\ d \ &\longmapsto \ j_d \ = \begin{cases} d/p & \text{si } p \text{ divise } d, \\ dp & \text{sinon.} \end{cases} \end{aligned}$$

n étant sans facteur carré, j est bien définie et injective. Il reste à voir que $j(L_n^+) \subset L_n^-$. Soit donc $d \in L_n^+$, décomposé en facteurs premiers $d = p_1 \cdots p_r$ avec $p_1 > ... > p_r$. Notons que r est un entier pair puisque $(-1)^r = \mu(d) = 1$. Distinguons deux cas :

Si p divise d. Comme p est le plus petit facteur premier de n, c'est aussi celui de d. Ainsi $j_d = p_1 \cdots p_{r-1}$. Les conditions *(i)* et *(ii)* étant vérifiées pour d, elles le sont *a fortiori* pour j_d. D'où

$$\lambda^-(j_d) \;=\; \mu(j_d) \;=\; (-1)^{r-1} \;=\; -1.$$

Sinon, p ne divise pas d. Dans ce cas $j_d = p_1 \cdots p_{r+1}$ avec $p_{r+1} = p$ puisque p est le plus petit facteur premier de n. Comme r est pair et que nous avons supposé R impair, $r+1 \leqslant R$ ce qui est la condition *(i)* pour j_d. Enfin, la condition *(ii)* est également vraie car $l \leqslant \frac{r+1}{2}$ si et seulement si $l \leqslant \frac{r}{2}$. De nouveau, nous trouvons aussi que

$$\lambda^-(j_d) \;=\; \mu(j_d) \;=\; (-1)^{r+1} \;=\; -1.$$

Dans tous les cas, nous avons bien $j_d \in L_n^-$, d'où $j(L_n^+) \subset L_n^-$, ce qui termine la preuve de (7.6).

Ces considérations permettent d'effectuer les manipulations habituelles du crible :

$$\begin{aligned}\sum_{\substack{a\in\mathscr{A}\\(a,P(z))=1}} 1 \;&=\; \sum_{a\in\mathscr{A}} \delta((a,P(z))) \;\geqslant\; \sum_{a\in\mathscr{A}} \sum_{\substack{d\mid a\\ d\mid P(z)}} \lambda_d^- \\ &\geqslant \sum_{d\mid P(z)} \lambda_d^- \sum_{\substack{a\in\mathscr{A}\\ d\mid a}} 1 \;=\; \sum_{d\mid P(z)} \lambda_d^- \Big(X\frac{\rho(d)}{d} + \mathscr{R}_d \Big) \\ &\geqslant X \sum_{d\mid P(z)} \lambda_d^- \frac{\rho(d)}{d} - \sum_{\substack{d\mid P(z)\\ \lambda_d^-\neq 0}} |\mathscr{R}_d|\end{aligned} \tag{7.7}$$

puisque $|\lambda^-(d)| \leqslant 1$. Pour évaluer le premier terme, utilisons le théorème [1] 1 de H. Iwaniec [Iwa80] : définissons $\tilde{\lambda}^-$ par

$$\tilde{\lambda}_d^- \;:=\; \begin{cases} \mu(d) & \text{si d vérifie la condition } \textit{(ii)}, \\ 0 & \text{sinon.} \end{cases}$$

Alors

Lemme 7.1 (Iwaniec [Iwa80])**.** *Uniformément pour s, L, D,*

$$\sum_{d\mid P(z)} \tilde{\lambda}_d^- \frac{\rho(d)}{d} \;=\; V(z)\Big(f(s) + O(\mathrm{e}^{\sqrt{L}}\, s^{-s} \log^{-\frac{1}{3}} D) \Big).$$

1. en fait, les équations (3.5), (4.2), (9.1) et (9.2) qui sont utilisées pour prouver le théorème 1.

Il nous suffit donc de majorer

$$\Big|\sum_{d|P(z)}\tilde{\lambda}_d^-\frac{\rho(d)}{d}-\sum_{d|P(z)}\lambda_d^-\frac{\rho(d)}{d}\Big| \;=\; \sum_{\substack{d|P(z)\\ \tilde{\lambda}_d^-\neq\lambda_d^-}}\frac{\rho(d)}{d} \;\leqslant\; \sum_{\substack{d|P(z)\\ \omega(d)>R}}\frac{\rho(d)}{d},$$

ce qui peut être fait par la méthode de Rankin : pour tout $y\geqslant 1$,

$$\begin{aligned}\sum_{\substack{d|P(z)\\ \omega(d)>R}}\frac{\rho(d)}{d} &\leqslant \sum_{d|P(z)}\frac{\rho(d)}{d}y^{\omega(d)-R}\\ &\leqslant y^{-R}\prod_{p<z}\Big(1+y\frac{\rho(p)}{p}\Big)\\ &\leqslant y^{-R}\Big(\prod_{p<z}(1-\frac{\rho(p)}{p})\Big)^{-y}.\end{aligned}$$

Majorons le produit grâce à l'hypothèse (7.2). Si $K:=(1+L/\log 2)/\log 2$,

$$\sum_{\substack{d|P(z)\\ \omega(d)>R}}\frac{\rho(d)}{d} \;\leqslant\; y^{-R}\Big(K\log(z)\Big)^{y} \;\leqslant\; \Big(\frac{\mathrm{e}\log(K\log z)}{R}\Big)^{R},$$

pour le choix optimal de $y=R/\log(K\log z)$, ce qui termine la minoration du lemme lorsque R est un entier impair. Le cas général s'en déduit en remplaçant R par le plus grand entier impair qui lui est inférieur.

La majoration se traite de façon similaire en définissant, lorsque R un entier pair, le nouveau système de poids λ^+ par $\lambda_d^+:=\mu(d)$ si

$$\begin{aligned}&(i)\quad r\leqslant R\\ &(ii)\quad \text{pour tout } l\leqslant\frac{r-1}{2},\ \text{nous avons } p_1\cdots p_{l-1}\cdot {p_l}^3<D\end{aligned}$$

en ayant de nouveau décomposé $d=p_1\cdots p_r$ en facteurs premiers avec $p_1\geqslant ...\geqslant p_r$. Dans le cas contraire, définissons $\lambda_d^+:=0$. Nous avons alors

$$\lambda^+*1(n) \;\geqslant\; \mu*1(n) \;=\; \delta(n), \tag{7.8}$$

inégalité remplaçant (7.6) pour l'inégalité (7.7).

Chapitre 8

Exposant de friabilité pour $\beta > \frac{1}{2}$: preuve du Théorème 5.2

Comme $\max\{d, \frac{n}{d}\} \geqslant \sqrt{n}$ pour tout diviseur d de n, la méthode utilisée pour démontrer le théorème 5.1 ne permet pas d'obtenir mieux que $y = x^\alpha$ avec $\alpha = \frac{1}{2}$. Une généralisation de l'adaptation utilisée par Friedlander [Fri89] permet de supprimer cette limite.

Dans toute cette section, pour simplifier les notations, nous définissons implicitement les nombres V, W, Y et Z de $]0,1[$ par les relations

$$v = x^V, \qquad w = x^W, \qquad y = x^Y \qquad \text{et} \qquad z = x^Z.$$

Nous notons aussi

$$\begin{aligned} \tilde{W_{\mathscr{D}}}(x) &:= \{n \in W_{\mathscr{D}},\ \tfrac{x}{2} \leqslant n < x\}, \\ \tilde{W_{\mathscr{D}}}(x,a,q) &:= \{n \in W_{\mathscr{D}},\ \tfrac{x}{2} \leqslant n < x,\ n \equiv a \mod q\}. \end{aligned}$$

8.1 Preuve du Théorème 5.2 - Décomposition $S_1 - S_2$.

Lemme 8.1. *Soit $\mathscr{N}$ un ensemble d'entiers. Soient $2 \leqslant z \leqslant y \leqslant x$. Alors*

$$\Psi_{\mathscr{D}}(x,y) \geqslant 2^{-\frac{\log x}{\log z}} (S_1 - S_2)$$

avec (nous rappelons que la fonction u_z est définie dans (6.4))

$$\begin{aligned} S_1 &:= \sum_{\substack{l \in \mathscr{N} \\ P^+(l) \leqslant y}} \sum_{n \in \tilde{W_{\mathscr{D}}}(x,0,l)} u_z(\tfrac{n}{l}), \\ S_2 &:= \sum_{\substack{l \in \mathscr{N} \\ P^+(l) \leqslant y}} \sum_{\substack{n \in \tilde{W_{\mathscr{D}}}(x,0,l) \\ P^+(\frac{n}{l}) > y}} u_z(\tfrac{n}{l}). \end{aligned}$$

Démonstration. Nous utilisons de nouveau de la majoration (6.5)

$$\sum_{l|n} u_z(\tfrac{n}{l}) \ \leqslant \ 2^{\frac{\log n}{\log z}},$$

ce qui assure (en ne conservant que les $n \geqslant \frac{x}{2}$ pour une raison technique)

$$\begin{aligned}\Psi_{\mathscr{D}}(x,y) \ &\geqslant \sum_{\substack{n\in\tilde{W}_{\mathscr{D}}(x)\\ P^+(n)\leqslant y}} 2^{-\frac{\log n}{\log z}} \sum_{l|n} u_z(\tfrac{n}{l}) \\ &\geqslant 2^{-\frac{\log x}{\log z}} \sum_{\substack{n\in\tilde{W}_{\mathscr{D}}(x)\\ P^+(n)\leqslant y}} \sum_{\substack{l\in\mathscr{N}\\ l|n}} u_z(\tfrac{n}{l}).\end{aligned}$$

Mais si n se décompose sous la forme du produit $n = kl$, alors $P^+(n) \leqslant y$ si et seulement si $P^+(l) \leqslant y$ et $P^+(k) \leqslant y$. Ainsi,

$$\begin{aligned}\Psi_{\mathscr{D}}(x,y) \ &\geqslant \ 2^{-\frac{\log x}{\log z}} \sum_{n\in\tilde{W}_{\mathscr{D}}(x)} \Bigg(\sum_{\substack{l\in\mathscr{N}\\ l|n\\ P^+(l)\leqslant y}} u_z(\tfrac{n}{l}) - \sum_{\substack{l\in\mathscr{N}\\ l|n\\ P^+(l)\leqslant y\\ P^+(\frac{n}{l})>y}} u_z(\tfrac{n}{l}) \Bigg) \\ &\geqslant \ 2^{-\frac{\log x}{\log z}} \Bigg(\sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y}} \sum_{n\in\tilde{W}_{\mathscr{D}}(x,0,l)} u_z(\tfrac{n}{l}) - \sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y}} \sum_{\substack{n\in\tilde{W}_{\mathscr{D}}(x,0,l)\\ P^+(\frac{n}{l})>y}} u_z(\tfrac{n}{l}) \Bigg).\end{aligned}$$

en intervertissant l'ordre de sommation. □

Dans la suite, nous définissons $\mathscr{N}$ comme l'ensemble des entiers d'un petit intervalle, ces entiers étant premiers à $\tilde{r} := r(r+1)$ et ne possédant pas trop de facteurs premiers :

$$\mathscr{N} \ := \ \{v \leqslant l < w, \ (l,\tilde{r}) = 1, \ \omega(l) \leqslant R\}, \tag{8.1}$$

R étant un paramètre à notre disposition que nous choisirons dans (8.3).

8.2 Preuve du Théorème 5.2 - Minoration de S_1

Lemme 8.2. *Uniformément pour $0 < Z < Y < V < W < 1$, $s > 2$ et x assez grand, nous avons*

$$\begin{aligned}S_1 \ \geqslant \ \#\tilde{W}_{\mathscr{D}}(x)\,\mathrm{e}^{-\gamma}\,\frac{W-V}{Z} f(s)\rho\Big(\frac{W}{Y}\Big)\Big(1 + O_{Z,r,s}\Big(\frac{1}{\log_2 x}\Big) + O\Big(\frac{W-V}{Y}\Big)\Big) \\ + O_{Z,r,s}\Bigg(\log^6 x \sum_{\substack{q<x^{W+sZ}\\ (q,\tilde{r})=1}} |\mathscr{R}_q(x)|\Bigg),\end{aligned}$$

la seconde constante implicite étant absolue.

Démonstration. Pour chaque entier l, utilisons le corollaire 7.1 avec

$$\mathscr{R} := \{p \nmid \tilde{r}\}, \qquad \text{et} \qquad \rho(p) := 1.$$

Nous notons que pour $z > \tilde{r}$,

$$V(z) \;=\; \prod_{\substack{p<z\\(p,\tilde{r})=1}} \Big(1-\frac{1}{p}\Big) \;=\; \frac{\tilde{r}}{\phi(\tilde{r})}\,\frac{\mathrm{e}^{-\gamma}}{\log z}\Big(1+O_r\big(\frac{1}{\log z}\big)\Big) \tag{8.2}$$

est une fonction indépendante de l. Si nous choisissons

$$R \;:=\; 4\log_2 z + C \tag{8.3}$$

pour une suffisamment grande constante C pouvant dépendre de r et de s,

$$\sum_{n\in\tilde{W}_{\mathscr{D}}(x,0,l)} u_z\big(\tfrac{n}{l}\big) \;\geqslant\; \frac{\#\tilde{W}_{\mathscr{D}}(x)}{l}V(z)\big(f(s)+O_r(\log^{-\frac{1}{3}} z)\big) - \sum_{\substack{d\leqslant z^{\epsilon}\\ \mu^2(d)=1\\ \omega(d)\leqslant R\\ (d,\tilde{r})=1}} |\mathscr{R}_{dl}(x)|,$$

la constante implicite dépendant au plus de r. Ainsi,

$$\begin{aligned}\sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y\\ (l,\tilde{r})=1}} \sum_{n\in\tilde{W}_{\mathscr{D}}(x,0,l)} u_z\big(\tfrac{n}{l}\big) \;\geqslant\; \#\tilde{W}_{\mathscr{D}}(x)\big(f(s)+O_r(\log^{-\frac{1}{3}} z)\big)V(z) \sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y\\ (l,\tilde{r})=1}} \frac{1}{l}\\ - \sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y\\ (l,\tilde{r})=1}} \sum_{\substack{d\leqslant z^{s}\\ \mu^2(d)=1\\ \omega(d)\leqslant R\\ (d,\tilde{r})=1}} |\mathscr{R}_{dl}(x)|.\end{aligned} \tag{8.4}$$

Nous estimons le nombre des entiers friables grâce à la formule de Hildebrand telle qu'énoncée dans [FT91, Théorème 1 et équation (1.10)]). En réalité, nous utilisons seulement un cas très particulier de ce Théorème, celui où $\frac{\log x}{\log y}$ est borné et q est fixé.

Lemme 8.3. *Soient $\epsilon > 0$ et r un entier. Uniformément pour $x^{\epsilon} \leqslant y \leqslant x$,*

$$\frac{1}{x}\sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y\\ (n,\tilde{r})=1}} 1 \;=\; \frac{\phi(\tilde{r})}{\tilde{r}}\rho\Big(\frac{\log x}{\log y}\Big)\Big(1+O_{r,\epsilon}\Big(\frac{1}{\log y}\Big)\Big).$$

Le théorème de Hardy-Ramanujan sur l'ordre normal de $\omega(n)$ (voir par exemple [Ten95, théorème 4, paragraphe III.3.4, p. 308]) implique

Lemme 8.4. *Soient $\epsilon > 0$, r un entier et C' une constante fixés. Uniformément pour $x^{\epsilon} \leqslant y \leqslant x$, nous avons*

$$\frac{1}{x}\sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y\\ (n,\tilde{r})=1\\ \omega(n)\leqslant R'}} 1 \;=\; \frac{\phi(\tilde{r})}{\tilde{r}}\rho\Big(\frac{\log x}{\log y}\Big)\Big(1+O_{r,\epsilon,C'}\Big(\frac{1}{\log_2 x}\Big)\Big), \tag{8.5}$$

avec $R' := 4\log_2 x + C'$.

Démonstration. Comme $\frac{R'-\log_2 x}{\sqrt{\log_2 x}} \asymp \sqrt{\log_2 x}$ tend bien avec l'infini avec x, nous avons grâce, au théorème de Hardy-Ramanujan

$$\sum_{\substack{l\leqslant x\\ \omega(l)>R'}} 1 \ll \frac{x\log_2 x}{(R'-\log_2 x)^2} \ll_{C'} \frac{x}{\log_2 x}.$$

En reportant cette estimation dans le lemme 8.3, nous obtenons le résultat cherché puisque la quantité $\rho(\frac{\log x}{\log y})$ est bornée en fonction de ϵ. □

Sous les hypothèses du lemme 8.2, nous en déduisons finalement l'estimation

$$\begin{aligned}\sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y\\ (l,\tilde{r})=1}} \frac{1}{l} &= \int_v^w \frac{1}{u}\mathrm{d}\Big(\sum_{\substack{l<u\\ P+(n)\leqslant y\\ \omega(l)\leqslant R\\ (l,\tilde{r})=1}} 1\Big)\\ &= \frac{\phi(\tilde{r})}{\tilde{r}}\Big\{1+O_{r,Z,s}\Big(\frac{1}{\log_2 v}\Big)\Big\}\Big\{\rho\Big(\frac{\log w}{\log y}\Big)-\rho\Big(\frac{\log v}{\log y}\Big)\\ &\qquad\qquad +\int_v^w \rho\Big(\frac{\log u}{\log y}\Big)\frac{\mathrm{d}u}{u}\Big\}\\ &= \frac{\phi(\tilde{r})}{\tilde{r}}\log\frac{w}{v}\Big\{1+O_{r,Z,s}\Big(\frac{1}{\log_2 x}\Big)\Big\}\Big\{\rho\Big(\frac{W}{Y}\Big)\\ &\qquad\qquad +O\Big(\rho'\Big(\frac{W}{Y}\Big)\frac{W-V}{Y}\Big)\Big\}\end{aligned}$$

La décroissance de la fonction de Dickman implique que pour tout $u>1$,

$$|\rho'(u)| = \frac{1}{u}\rho(u-1) \leqslant \frac{1}{u}\int_{u-1}^u \rho(t)\mathrm{d}t = \rho(u). \tag{8.6}$$

Donc

$$\sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y\\ (l,\tilde{r})=1}} \frac{1}{l} = \frac{\phi(\tilde{r})}{\tilde{r}}\rho\Big(\frac{W}{Y}\Big)\log\frac{w}{v}\Big\{1+O_{r,Z,s}\Big(\frac{1}{\log_2 x}\Big)+O\Big(\frac{W-V}{Y}\Big)\Big\}. \tag{8.7}$$

Il existe au plus 2^{2R} décompositions d'un entier q sous la forme $q=ld$ avec $\omega(l)<R$ et $\omega(d)<R$, $\mu^2(d)=1$. Donc

$$\begin{aligned}\sum_{\substack{l\in\mathscr{N}\\ P^+(l)\leqslant y\\ (l,\tilde{r})=1}}\sum_{\substack{d\leqslant z^s\\ \mu^2(d)=1\\ \omega(d)\leqslant R\\ (d,\tilde{r})=1}} |\mathscr{R}_{dl}(x)| &\leqslant \sum_{\substack{q<wz^s\\ (q,\tilde{r})=1}} 2^{2R}|\mathscr{R}_q(x)|\\ &\ll_{r,s} \log^{8\log 2} z \sum_{\substack{q<wz^s\\ (q,\tilde{r})=1}} |\mathscr{R}_q(x)|,\end{aligned} \tag{8.8}$$

par notre choix de $R=4\log_2 z+C$. La preuve du lemme est terminée en reportant les estimations (8.2), (8.7) et (8.8) dans la minoration (8.4). □

8.3 Preuve du Théorème 5.2 - Majoration de S_2

Lemme 8.5. *Uniformément pour $0 < Z < Y < V < W < 1$, $Y < 1 - V - 2Z - \sqrt{Z}$ et x assez grand, nous avons*

$$S_2 \leqslant \#\tilde{W}_{\mathscr{D}}(x)\,\mathrm{e}^{-\gamma}\,\frac{(W-V)}{Y}\,\frac{(1-V-Y-2Z)}{Z}\Big(1+O\Big(\sqrt{Z}+\frac{1}{\log z}\Big)\Big) + \sum_{\substack{q<x^{1-V}\\(q,\tilde{r})=1}} |\mathscr{R}_q(x)|.$$

Démonstration. Nous commençons par oublier que nous sommons sur des entiers l friables, puis nous faisons le changement de variable $q = \frac{n}{l}$. Donc

$$S_2 \leqslant \sum_{\substack{v<l\leqslant w\\ P^+(l)\leqslant y}} \sum_{\substack{n\in\tilde{W}_{\mathscr{D}}(x,0,l)\\ P^+(\frac{n}{l})>y}} u_z\big(\tfrac{n}{l}\big) \leqslant \sum_{v<l\leqslant w} \sum_{\substack{n\in\tilde{W}_{\mathscr{D}}(x,0,l)\\ P^+(\frac{n}{l})>y}} u_z\big(\tfrac{n}{l}\big) \leqslant \sum_{\substack{\frac{x}{2w}\leqslant q<\frac{x}{v}\\ P^+(q)>y}} u_z(q) \sum_{n\in\tilde{W}_{\mathscr{D}}(x,0,q)} 1.$$

L'estimation directe de la somme intérieure à l'aide de la définition (5.5) de $\mathscr{R}_q(x)$, donne pour $z > \tilde{r}$:

$$S_2 \leqslant \#\tilde{W}_{\mathscr{D}}(x) \sum_{\substack{\frac{x}{2w}\leqslant q<\frac{x}{v}\\ P^+(q)>y}} \frac{u_z(q)}{q} + \sum_{\substack{q<\frac{x}{v}\\(q,\tilde{r})=1}} |\mathscr{R}_q(x)|. \tag{8.9}$$

Mais en isolant le plus grand facteur premier de q,

$$\begin{aligned}\sum_{\substack{\frac{x}{2w}\leqslant q<\frac{x}{v}\\ P^+(q)>y}} \frac{u_z(q)}{q} &= \sum_{p>y} \sum_{\substack{\frac{x}{2w}\leqslant pq<\frac{x}{v}\\ P^+(q)>y}} \frac{u_z(q)}{pq} \leqslant \sum_{p>y} \sum_{\frac{x}{2w}\leqslant pq<\frac{x}{v}} \frac{u_z(q)}{pq}\\ &\leqslant \sum_{\frac{x}{2wy}\leqslant q<\frac{x}{vy}} \frac{u_z(q)}{q} \sum_{y<p\leqslant\frac{x}{vq}} \frac{1}{p} + \sum_{q<\frac{x}{2wy}} \frac{u_z(q)}{q} \sum_{\frac{x}{2wq}<p\leqslant\frac{x}{vq}} \frac{1}{p}\\ &\leqslant S_2^+ + S_2^- \qquad \text{disons.}\end{aligned} \tag{8.10}$$

Pour évaluer S_2^- et S_2^+, nous commençons par estimer les sommes intérieures à l'aide du théorème de Mertens :

$$\begin{aligned}S_2^- &= \sum_{q<\frac{x}{2wy}} \frac{u_z(q)}{q}\Big\{\log\Big(1+\frac{\log\frac{2w}{v}}{\log\frac{x}{2wq}}\Big)+O\Big(\frac{1}{\log y}\Big)\Big\}\\ &\leqslant \sum_{q<\frac{x}{2wy}} \frac{u_z(q)}{q}\,\frac{\log\frac{2w}{v}+O(1)}{\log y}\end{aligned}$$

car $\log\frac{x}{2wq} \geqslant y$. De même,

$$\begin{aligned}S_2^+ &= \sum_{\frac{x}{2wy}\leqslant q<\frac{x}{vy}} \frac{u_z(q)}{q}\Big\{\log\frac{\log\frac{x}{vq}}{\log y}+O\Big(\frac{1}{\log y}\Big)\Big\}\\ &\leqslant \sum_{\frac{x}{2wy}\leqslant q<\frac{x}{vy}} \frac{u_z(q)}{q}\,\frac{\log\frac{2w}{v}+O(1)}{\log y}\end{aligned}$$

car $\frac{x}{vq} \leqslant \frac{2w}{v}$. Donc

$$S_2^+ + S_2^- \ \leqslant \ \frac{\log \frac{2w}{v} + O(1)}{\log y} \sum_{q<\frac{x}{vy}} \frac{u_z(q)}{q}. \tag{8.11}$$

Si q est un entier inférieur à z^2 tel que $P^-(q) \geqslant z$, alors q est un nombre premier. Donc

$$\sum_{q<z^2} \frac{u_z(q)}{q} \ = \ \sum_{z\leqslant p<z^2} \frac{1}{p} \ \ll \ 1,$$

ce qui, combiné avec l'estimation (6.8), fournit

$$\begin{aligned} \sum_{q<\frac{x}{vy}} \frac{u_z(q)}{q} \ &= \ \sum_{z^2\leqslant q<\frac{x}{vy}} \frac{u_z(q)}{q} + \sum_{q\leqslant z^2} \frac{u_z(q)}{q} \\ &= \ \mathrm{e}^{-\gamma} \frac{\log \frac{x}{vyz^2}}{\log z} \Big(1 + O\Big(\frac{1}{\log z} + \frac{\log z}{\log \frac{x}{vyz^2}}\Big)\Big). \end{aligned} \tag{8.12}$$

En regroupant (8.10), (8.11) et (8.12), nous obtenons

$$\sum_{\substack{\frac{x}{2w}\leqslant q<\frac{x}{v}\\ P^+(q)>y}} \frac{u_z(q)}{q} \ \leqslant \ \mathrm{e}^{-\gamma} \frac{\log \frac{2w}{v}}{\log y} \frac{\log \frac{x}{vyz^2}}{\log z} \Big(1 + O\Big(\frac{1}{\log z} + \frac{\log z}{\log \frac{x}{vyz^2}} + \frac{1}{\log y}\Big)\Big)$$

L'hypothèse $Y \leqslant 1 - V - 2Z - \sqrt{Z}$ implique $\frac{Z}{1-V-Y-2Z} \leqslant \sqrt{Z}$. Donc

$$\sum_{\substack{\frac{x}{2w}\leqslant q<\frac{x}{v}\\ P^+(q)>y}} \frac{u_z(q)}{q} \ \leqslant \ \mathrm{e}^{-\gamma} \frac{W-V}{Y} \frac{1-V-Y-2Z}{Z} \Big(1 + O\Big(\frac{1}{\log z} + \sqrt{Z}\Big)\Big). \tag{8.13}$$

Le lemme est démontré en reportant l'estimation (8.13) dans (8.9). □

8.4 Preuve du Théorème 5.2 - Choix des paramètres.

Nous résumons les résultats obtenus dans les lemmes 8.1, 8.2 et 8.5 dans le lemme suivant

Lemme 8.6. *Soit $\epsilon > 0$ assez petit fixé. Uniformément pour $x \geqslant x_0(\epsilon)$ assez grand et*

$$\epsilon \ < \ Y \ < \ 1 - W - \epsilon, \qquad Y \ < \ W - \epsilon$$

tels que

$$1 + f\Big(\frac{1}{\epsilon}\Big)\rho\Big(\frac{W}{Y}\Big) - \frac{1-W}{Y} - \frac{\epsilon}{Y} \ \gg_\epsilon \ 1, \tag{8.14}$$

en notant $\delta := \max\{1 - W + \epsilon,\ W + \epsilon\}$, nous avons

$$\Psi_{\mathscr{D}}(x,y) \ \gg_{\epsilon,r} \ \#W_{\mathscr{D}}(x) + O_{\epsilon,r}\Big(\log^6 x \sum_{\substack{q<x^\delta\\ (q,\tilde{r})=1}} |\mathscr{R}_q(x)|\Big).$$

Démonstration. Nous utilisons les lemmes 8.1, 8.2 et 8.5 avec les choix suivants

$$Z := \tfrac{1}{4}\epsilon^2, \qquad V := W - \tfrac{1}{2}\epsilon \qquad \text{et} \qquad s = \epsilon^{-1}.$$

Les hypothèses des lemmes 8.2 et 8.5 sont vérifiées si ϵ est assez petit puisque

$$Y < 1 - W - \epsilon = 1 - V - 2Z - \sqrt{Z} + \tfrac{1}{2}\epsilon^2 - \epsilon.$$

Le lemme 8.1 donne donc

$$\Psi_{\mathscr{D}}(x,y) \geqslant 2^{-\frac{1}{Z}}\,\mathrm{e}^{-\gamma}\,\frac{W-V}{Z}\#\tilde{W}_{\mathscr{D}}(x)\Big(f\Big(\frac{1}{\epsilon}\Big)\rho\Big(\frac{W}{Y}\Big) - \frac{1-V-Y-2Z}{Y}\Big)$$
$$\Big(1 + O(\epsilon) + O_{\epsilon,r}\Big(\frac{1}{\log_2 x}\Big)\Big) + O_{\epsilon,r}\Big(\log^6 x \sum_{\substack{q<wz^s+\frac{x}{v}\\(q,\tilde{r})=1}} |\mathscr{R}_q(x)|\Big).$$

Grâce à notre hypothèse (8.14), nous avons donc

$$\Psi_{\mathscr{D}}(x,y) \gg_{\epsilon,r} \#\tilde{W}_{\mathscr{D}}(x)\Big(1 + O(\epsilon)\Big) + O_{\epsilon,r}\Big(\log^6 x \sum_{\substack{q<wz^s+\frac{x}{v}\\(q,\tilde{r})=1}} |\mathscr{R}_q(x)|\Big).$$

Mais si ϵ est assez petit, nous avons $1 + O(\epsilon) > 0$ et la preuve du lemme est achevée. □

Il reste maintenant à choisir dans le lemme 8.6 le paramètre W de façon optimale permettant de prendre Y le plus petit possible. Dans le lemme 8.7, nous commençons par démontrer diverses propriétés de la fonction α_W, notamment celles énoncées dans le théorème 5.2, propriétés qui seront utiles pour choisir W.

Lemme 8.7. *Rappelons la définition de* $\Phi(W,Y)$,

$$\Phi(W,Y) := 1 + \rho\Big(\frac{W}{Y}\Big) - \frac{1-W}{Y}.$$

et pour $0 < W < 1$ *de* α_W, *la solution de l'équation* $\Phi(W,\alpha_W) = 0$. *Alors*

1. *Pour tout* $0 < W < 1$, *le nombre* α_W *est bien défini et* $\alpha_W < 1 - W$.
2. *Pour* $\frac{1}{3} < W < 1$, α_W *est une fonction de* W *continûment dérivable, strictement décroissante et concave.*
3. *Une équation paramétrique du graphe de* α_W *(pour* $W \in]0,1[$*) est*

$$\Big(W = \frac{k}{k+1+\rho(k)},\ \alpha_W = \frac{1}{k+1+\rho(k)}\Big),\ k \in]0,\infty[.$$

4. *Pour* $\frac{1}{3} < W < 1$, *nous avons* $\alpha_W > \frac{1-W}{2}$.

Démonstration. Pour le premier point, nous montrons que la fonction $\Phi(W,\cdot)$ est strictement croissante. Comme elle est continue, que

$$\Phi(W,0) = -\infty \qquad \text{et que} \qquad \Phi(W,1-W) = \rho\Big(\frac{W}{1-W}\Big) > 0,$$

nous aurons bien l'existence et l'unicité de α_W et $\alpha_W < 1 - W$. Comme

$$\frac{\partial \Phi}{\partial Y}(W,Y) \;=\; -\frac{1}{Y^2}\rho'\Big(\frac{W}{Y}\Big) + \frac{1-W}{Y^2} \;>\; 0 \tag{8.15}$$

puisque ρ est décroissante et $W < 1$, nous en déduisons la croissance $\Phi(W,\cdot)$.

Pour le deuxième point, nous commençons par montrer que $\alpha_W < W$. En effet, $\Phi(W,W) = 3 - \frac{1}{W} > 0$ et nous savons que $\Phi(W,\cdot)$ est une fonction croissante par le premier point. En particulier, $\Phi(W,Y)$ est une fonction continûment dérivable au voisinage de (W,α_W). Le théorème des fonctions implicites assure donc que α_W est aussi continûment dérivable. Nous pouvons maintenant dériver la relation $\alpha_W \Phi(W,\alpha_W) = 0$ par rapport à W en utilisant la formule des fonctions composées. Ainsi,

$$\alpha'_W\Big\{1 + \rho\Big(\frac{W}{\alpha_W}\Big) - \frac{W}{\alpha_W}\rho'\Big(\frac{W}{\alpha_W}\Big)\Big\} + 1 + \rho'\Big(\frac{W}{\alpha_W}\Big) \;=\; 0.$$

En utilisant l'équation fonctionnelle de la fonction de Dickman ρ, nous trouvons finalement

$$\alpha'_W \underbrace{\Big\{\frac{1-W}{\alpha_W} + \rho\Big(\frac{W}{\alpha_W} - 1\Big)\Big\}}_{>0} + \underbrace{1 + \rho'\Big(\frac{W}{\alpha_W}\Big)}_{>0} \;=\; 0. \tag{8.16}$$

La relation (8.16) montre que $\alpha'_W < 0$. Donc α_W est strictement décroissante.

Nous avons $\Phi(W, \frac{1}{2}W) = 4 - \log 2 - \frac{2}{W}$. En particulier, pour $W \neq \frac{2}{4-\log 2}$, nous avons $\alpha_W \neq \frac{W}{2}$. La relation (8.16) montre que α'_W est une fonction continûment dérivable, sauf au point d'abscisse $W = \frac{2}{4-\log 2}$. Nous pouvons donc dériver de nouveau la relation (8.16) par rapport à W. Ainsi,

$$\alpha''_W\Big\{\overbrace{\frac{1-W}{\alpha_W} + \rho\Big(\frac{W}{\alpha_W} - 1\Big)}^{>0}\Big\} + \overbrace{\frac{\alpha_W - W\alpha'_W}{\alpha_W^2}}^{>0}\overbrace{\rho''\Big(\frac{W}{\alpha_W}\Big)}^{>0}$$
$$+ \underbrace{\alpha'_W}_{<0}\Big\{\underbrace{-\frac{1}{\alpha_W} - \frac{(1-W)\alpha'_W}{\alpha_W^2} + \frac{\alpha_W - W\alpha'_W}{\alpha_W^2}\rho'\Big(\frac{W}{\alpha_W} - 1\Big)}_{<0}\Big\} \;=\; 0.$$

En particulier,

$$\alpha''_W\Big\{\frac{1-W}{\alpha_W} + \rho\Big(\frac{W}{\alpha_W} - 1\Big)\Big\} \;<\; 0.$$

ce qui implique bien que $\alpha''_W < 0$ et donc la concavité de la fonction.

Pour le troisième point, il suffit de remarquer que

$$\Phi\Big(\frac{k}{k+1+\rho(k)}, \frac{1}{k+1+\rho(k)}\Big) \;=\; 0,$$

ce qui est clair en écrivant la définition de Φ.

Pour le quatrième point, le point 3 de ce lemme avec $k = 1$, implique que $\alpha_{\frac{1}{3}} = \frac{1}{3}$. La concavité de α_W assure que la courbe est au dessus de sa corde entre les points d'abscisse $\frac{1}{3}$ et 1, donc que $\alpha_W > \frac{1}{2}(1-W)$. □

8.5 Preuve du Théorème 5.2

Soit $\frac{1}{2} < \beta < 1$ un exposant de répartition fixé. Pour chaque $\epsilon > 0$ assez petit (en terme de β), nous allons construire des paramètres W et Y vérifiant les hypothèses du lemme 8.6 avec $\delta < \beta$, ces paramètres ne dépendant que de ϵ et de β. En outre, lorsque ϵ tend vers 0, le paramètre Y pourra être choisi arbitrairement proche de α_β. Ce lemme 8.6 et la définition d'un exposant de répartition donnée par (5.2) avec $A := 7$ terminera la preuve du théorème 5.2.

Si $\epsilon > 0$ assez petit en terme de β, alors

$$1 - \beta + 4\epsilon \;<\; \beta \qquad \text{et} \qquad \epsilon^{\frac{1}{2}} \;<\; \frac{1-\beta}{2}, \tag{8.17}$$

$$\alpha_{\beta - 2\epsilon - \tilde{\epsilon}} \;<\; 1 - \beta, \tag{8.18}$$

$$-\alpha'_\beta \frac{\partial \Phi}{\partial Y}(\beta, \alpha_\beta) + O_\beta(\tilde{\epsilon}) \;>\; 0, \tag{8.19}$$

où nous avons noté $\tilde{\epsilon} := \epsilon^{\frac{1}{4}}$ pour simplifier les notations. Comme $\frac{1}{2} < \beta < 1$, la condition (8.17) est vraie. Comme $W \mapsto \alpha_W$ est continue et que le point 1 du lemme 8.7 assure $\alpha_\beta < 1 - \beta$, la condition (8.18) est également vraie. Pour la condition (8.19), il suffit juste de se souvenir que dans la démonstration du point 1 du lemme 8.7, nous avons prouvé que $\Phi(\beta, \cdot)$ est strictement croissante et que le point 2 de ce même lemme 8.7 implique $\alpha'_\beta < 0$.

Si $\epsilon > 0$ est assez petit pour vérifier simultanément les trois conditions (8.17), (8.18) et (8.19), nous choisissons alors

$$W \;:=\; \beta - 2\epsilon \qquad \text{et} \qquad Y \;:=\; \alpha_{W - \tilde{\epsilon}}. \tag{8.20}$$

La condition (8.17) implique

$$1 - W - \epsilon \;<\; W - \epsilon \qquad \text{et} \qquad \delta \;=\; W + \epsilon \;<\; \beta.$$

La condition (8.18) implique

$$Y \;<\; 1 - W - \epsilon.$$

La condition (8.17) et le point 4 du lemme 8.7 permettent de majorer

$$\epsilon \;<\; \epsilon^{\frac{1}{2}} \;<\; \frac{1-\beta}{2} \;<\; \frac{1-W}{2} \;<\; \alpha_W \;<\; Y. \tag{8.21}$$

Le théorème 5.2 sera donc prouvé dès que nous aurons vérifié la condition (8.14). Mais

$$1 + f\Big(\frac{1}{\epsilon}\Big)\rho\Big(\frac{W}{Y}\Big) - \frac{1 - W + \epsilon}{Y} - \Phi(W, Y)$$
$$= \Big(f\Big(\frac{1}{\epsilon}\Big) - 1\Big)\Big(\rho\Big(\frac{W}{Y}\Big) - \frac{1-W}{Y}\Big) + \frac{\epsilon}{Y} \;\ll\; \frac{\epsilon}{Y} \;\ll\; \tilde{\epsilon}^2,$$

puisque nous venons de prouver dans (8.21) que $Y > \epsilon^{\frac{1}{2}}$. Donc

$$\begin{aligned} 1 + f\Big(\frac{1}{\epsilon}\Big)\rho\Big(\frac{W}{Y}\Big) - \frac{1-W+\epsilon}{Y} &= \Phi(W, \alpha_Y) + O(\tilde{\epsilon}^2) \\ &= \tilde{\epsilon}\,\frac{\partial}{\partial\tilde{\epsilon}}\Big(\Phi(W, \alpha_Y)\Big) + O_\beta(\tilde{\epsilon}^2) \\ &= \tilde{\epsilon}\,\frac{\partial W}{\partial\tilde{\epsilon}}\,\frac{\partial\Phi}{\partial W}(\beta, \alpha_\beta) + \tilde{\epsilon}\,\frac{\partial\alpha_Y}{\partial\tilde{\epsilon}}\,\frac{\partial\Phi}{\partial Y}(\beta, \alpha_\beta) + O_\beta(\tilde{\epsilon}^2) \\ &= -\tilde{\epsilon}\,\alpha'_\beta\,\frac{\partial\Phi}{\partial Y}(\beta, \alpha_\beta) + O_\beta(\tilde{\epsilon}^2) \;>\; 0 \end{aligned}$$

grâce à la condition (8.19).

Remarque 8.1. Les choix de V et W sont optimaux de part le point 2 du lemme 8.7.

8.6 Tracé de $W \mapsto \alpha_W$.

Le point 3 du lemme 8.7 permet de tracer paramétriquement la fonction $W \mapsto \alpha_W$:

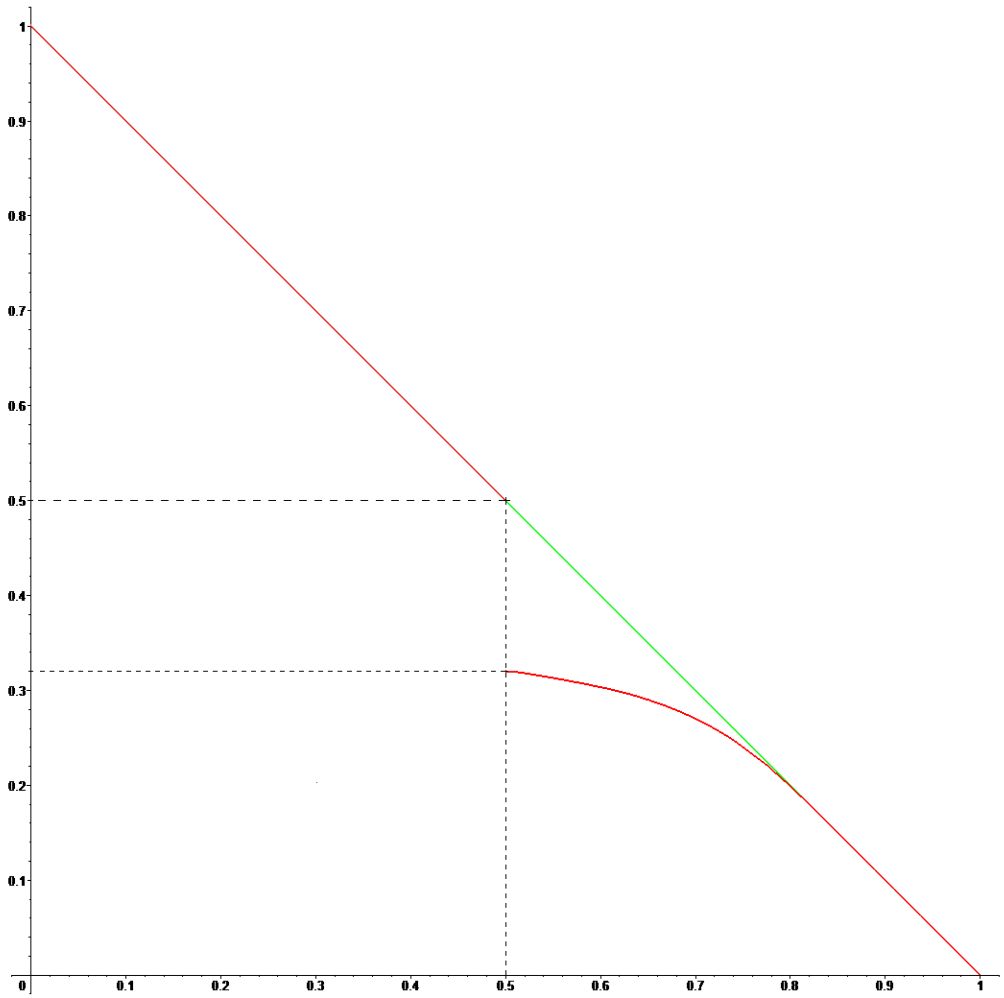

FIGURE 8.1 – Graphe de $W \mapsto 1 - W$ et de $W \mapsto \alpha_W$.

Troisième partie

Palindromes

La recherche sur les palindromes a commencé il y a plus de vingt siècles : les auteurs grecs et latins se divertissaient déjà en composant des phrases palindromiques. Le plus célèbre exemple est très certainement :

νιψον ανομηματα μη μοναν οψιν
(lave tes péchés et non seulement ton visage),

maxime qui orne les fonts baptismaux grecs ainsi que de nombreuses églises de Cambridge jusqu'à Constantinople. Dans toutes les langues et tous les alphabets des auteurs ont joué avec cette contrainte. En anglais, le palindrome

A man, a plan, a canal : Panama.

est tout aussi connu. Des auteurs comme G. Perec ont composé des textes et poèmes palindromiques. Le lecteur intéressé trouvera plusieurs exemples sur internet comme sur le site *http ://www.fatrazie.com*. Et maintenant,

Engage le jeu, que je le gagne !

Chapitre 9

Énoncé des résultats

Dans toute cette partie, $g \geqslant 2$ est un entier fixé : c'est la base utilisée pour écrire les nombres. Nous notons $\|x\|$ la distance de x aux entiers. Si $\mathscr{A}$ est un ensemble de nombres, nous notons $\mathscr{A}^* := \mathscr{A}\backslash\{0\}$ les éléments non nuls de $\mathscr{A}$. Sauf mention explicite du contraire, toutes les constantes c_1, c_2,... et les constantes implicites de Vinogradov peuvent dépendre de g. Nous désignons par $\log_k x$ la $k^{\text{ème}}$ composée du logarithme :

$$\log_k x \ := \ \log(\log_{k-1} x) \qquad \text{et} \qquad \log_1 x \ := \ \log x.$$

Nous appelons écriture de n dans la base g l'unique suite presque nulle $(n_j)_j$ d'entiers $0 \leqslant n_j \leqslant g-1$ telle que n s'écrit

$$n \ = \ \sum_j n_j g^j.$$

Nous disons que n possède N chiffres en base g si $N-1$ est le plus grand indice j pour lequel $n_j \neq 0$. Nous notons $\mathscr{R}_N$ les palindromes ayant exactement N chiffres en base g : ce sont les entiers de N chiffres dont l'écriture en base g possède la symétrie par rapport à $\frac{N-1}{2}$ *i.e.*

$$n \in \mathscr{R}_N \qquad \Longleftrightarrow \qquad n = \sum_{j<N} n_j g^j, \quad n_{N-1} \neq 0 \quad \text{et} \quad n_j = n_{N-1-j}.$$

Nous désignons respectivement par $\mathscr{R}^0$ et $\mathscr{R}^1$ les palindromes ayant un nombre respectivement pair et impair de chiffres et par $\mathscr{R}$ l'ensemble de tous les palindromes, de sorte que

$$\mathscr{R} \ = \ \mathscr{R}^0 \sqcup \mathscr{R}^1 \qquad \text{avec} \qquad \mathscr{R}^\delta \ = \ \bigsqcup_{M \geqslant 0} \mathscr{R}_{2M+\delta}, \tag{9.1}$$

toutes ces unions étant disjointes (nous avons convenu que 0 est l'unique palindrome de 0 chiffre).

Pour des raisons techniques, il est souvent plus simple de ne pas avoir la condition $n_{N-1} \neq 0$. Nous dirons alors que l'entier n est un pseudopalindrome de taille N si n

possède au plus N chiffres et si son écriture en base g possède la symétrie par rapport à $\frac{N-1}{2}$. Nous notons $\mathscr{Q}_N$ l'ensemble des pseudopalindromes de taille N *i.e.*

$$n \in \mathscr{Q}_N \qquad \Longleftrightarrow \qquad n = \sum_{j<N} n_j g^j, \quad n_j = n_{N-1-j}.$$

Comme pour les palindromes, nous notons respectivement $\mathscr{Q}$, $\mathscr{Q}^0$ et $\mathscr{Q}^1$ la famille des pseudopalindromes de toute taille, de taille paire et de taille impaire. Remarquons que 0 est un pseudopalindrome de toute taille (car son écriture possède toutes les symétries) et qu'un palindrome différent de 0 est exactement un pseudopalindrome ne se terminant pas par 0 :

$$\mathscr{Q}^* \;=\; \bigsqcup_{N\geqslant 0} g^N \mathscr{R}^* \qquad \text{et} \qquad \mathscr{R}^* \;=\; \mathscr{Q}\backslash g\mathscr{Q}.$$

Il est donc aisé d'obtenir des résultats sur les palindromes à partir de résultats sur les pseudopalindromes et réciproquement.

Nous notons

$$\Phi_N(k) \;:=\; g^{N-k} + g^k \tag{9.2}$$

ce qui permet d'écrire

$$\begin{aligned} n \in \mathscr{Q}_{2M} \qquad &\Longleftrightarrow \qquad n = \sum_{j<M} n_j \Phi_{2M-1}(j), && 0 \leqslant n_j < g, \\ n \in \mathscr{Q}_{2M+1} \qquad &\Longleftrightarrow \qquad n = \sum_{j<M} n_j \Phi_{2M}(j) + n_M g^M, && 0 \leqslant n_j < g. \end{aligned}$$

Enfin, pour tout ensemble d'entiers $\mathscr{A}$, nous posons

$$\begin{aligned} \mathscr{A}(x) \;&:=\; \{n \in \mathscr{A},\ n < x\}, \\ \mathscr{A}(x,a,q) \;&:=\; \{n \in \mathscr{A}(x),\ n \equiv a \mod q\}. \end{aligned}$$

Le but de cet article est d'évaluer le cardinal de $\mathscr{R}(x,a,q)$. Nous l'estimons uniformément dans le théorème 9.1 et en moyenne dans le théorème 9.2 par rapport à q. À notre connaissance, il existe actuellement un seul résultat de ce type dans la littérature : le corollaire 4.5 de W. D. Banks, D. N. Hart et M. Sakata [BHS04] donne la majoration :

Théorème A (BHS)**.** *Il existe une constante $c > 0$ ne dépendant que de g telle qu'uniformément pour les entiers q premiers avec $g^3 - g$ et $x > 0$, nous avons la majoration*

$$\max_{a\in\mathbb{Z}} \Big| \#\mathscr{R}(x,a,q) - \frac{\#\mathscr{R}(x)}{q} \Big| \;\ll_g\; \#\mathscr{R}(x) q \exp\Big(-\frac{c\log x}{q^2}\Big).$$

Si $(q, g^3-g) = 1$ et si q n'est pas trop grand *i.e.* essentiellement pour

$$q \;<\; \Big(\frac{c\log x}{\log_2 x}\Big)^{\frac{1}{2}} \qquad \text{et} \qquad (q\,,\, g^3-g) = 1, \tag{9.3}$$

le théorème A fournit un équivalent du cardinal de $\mathscr{R}(x,a,q)$. Sous la condition (9.3), les palindromes inférieurs à x sont uniformément distribués dans les progressions arithmétiques de module q. Le théorème A impose cependant de choisir q beaucoup trop petit pour avoir des applications arithmétiques de bonne qualité. Dans le théorème suivant, nous prolongeons le domaine de validité de q :

Théorème 9.1. *Il existe des constantes c, $\tilde{c} > 0$ ne dépendant que de g telles qu'uniformément pour les entiers q vérifiant*

$$q \leqslant \exp\Big(\frac{c\log x}{\log_2 x}\Big) \qquad et \qquad (q\,,\, g^3-g)=1, \tag{9.4}$$

nous avons la majoration

$$\max_{a\in\mathbb{Z}} \Big|\#\mathscr{R}(x,a,q) - \frac{\#\mathscr{R}(x)}{q}\Big| \ll_g \frac{\#\mathscr{R}(x)}{q}\exp\Big(-\frac{\tilde{c}\log x}{\log q}\Big).$$

Il faut remarquer que notre démonstration ne reprend pas les idées de [BHS04] : leur démonstration utilise des outils plus élaborés puisqu'elle repose sur des majorations de sommes de Kloosterman. La notre présente l'avantage d'être élémentaire : les seules propriétés des pseudopalindromes que nous utiliserons réellement sont deux identités très simples :

$$g\Phi_{N-1}(k) = \Phi_{N+1}(k+1) \tag{9.5}$$

$$g\Phi_N(k+1) - \Phi_N(k) = (g^2-1)g^k \tag{9.6}$$

L'identité (9.5) nous servira pour exprimer les moyennes de palindromes comme un produit et l'identité (9.6) pour supprimer la symétrie qui caractérise les palindromes : le membre de gauche de (9.6) représente une combinaison linéaire de pseudopalindromes où le paramètre N est important, alors que le membre de droite représente simplement un entier divisible par g^2-1 où le paramètre N n'intervient plus ! Nous démontrerons dans le paragraphe 12.7 que cette identité (9.6) est optimale dans la mesure où toute autre identité permettant une telle simplification fait aussi intervenir un facteur g^2-1.

La technique développée ici s'adapte à l'étude de toute famille d'entiers définie par des propriétés simples de géométrie sur les chiffres en utilisant des identités analogues à (9.5) et (9.6). Par exemple, toute famille d'entiers obtenue par translation ou symétrie centrale ou symétrie axiale ou... de blocs de chiffres et concaténation de telles applications. De plus, la technique que nous mettons en œuvre est totalement compatible avec celle utilisée pour l'étude des nombres ellipséphiques (*i.e.* les entiers dont l'écriture n'utilise que certains chiffres). À ces familles d'entiers, nous pouvons donc imposer l'absence de certains chiffres dans leur écriture.

Le théorème 9.1 est l'analogue du théorème de Siegel-Walfisz concernant la répartition des nombre premiers dans les progressions arithmétiques. Il reste cependant insuffisant pour de nombreuses applications car il ne permet pas de choisir q de la taille d'une puissance de x. Nous démontrons alors l'analogue du théorème de Bombieri-Vinogradov pour la famille des palindromes : en moyenne, les palindromes restent bien distribués dans les progressions arithmétiques pour des diviseurs de l'ordre d'une certaine puissance de x.

Théorème 9.2. *Il existe $\beta > 0$ ne dépendant au plus que de g tel que pour tout A et*

$\epsilon > 0$, nous avons la majoration

$$\sum_{\substack{q<x^{\beta-\epsilon}\\(q,g^3-g)=1}} \sup_{y\leqslant x}\max_{a\in\mathbb{Z}} \Big|\#\mathscr{R}(y,a,q) - \frac{\#\mathscr{R}(y)}{q}\Big| \ll_{g,A,\epsilon} \frac{\#\mathscr{R}(x)}{\log^A x}. \tag{9.7}$$

Nous pouvons choisir l'exposant $\beta-\epsilon=\beta_g$ avec $\epsilon>0$ et

g	2	3	4	5	6	7	8	9	10
β_g	$\frac{1}{30}$	$\frac{1}{94}$	$\frac{1}{74}$	$\frac{1}{122}$	$\frac{1}{114}$	$\frac{1}{158}$	$\frac{1}{150}$	$\frac{1}{194}$	$\frac{1}{186}$

Si g est assez grand, nous pouvons prendre

$$\beta \sim \frac{1}{6\pi g}.$$

Un nombre $\beta>0$ vérifiant la propriété (9.7) pour tous les A et $\epsilon>0$ est appelé un exposant de répartition pour la famille des palindromes.

Remarque 9.1. Les sommes d'exponentielles de pseudopalindromes sont des fonctions extrêmement oscillantes puisque

$$\Phi_N(j) = g^{N-j}+g^j$$

réunit ensemble les indices de très bas et de très haut degré. Pour éviter que les dérivées de ces fonctions ne soient trop importantes, nous sommes obligés d'utiliser une voie détournée : plutôt que d'étudier directement les moyennes d'exponentielles de pseudopalindromes, nous montrons dans le lemme 10.2 que nous pouvons supprimer le caractère symétrique en combinant astucieusement un indice avec son successeur à l'aide de l'identité (9.6). Cette simplification a évidemment un coût et c'est la raison pour laquelle les exposants β_g obtenus dans le théorème 9.2 sont petits par rapport à $\frac{1}{2}$.

En utilisant des techniques de crible, nous déduirons du théorème 9.2 le

Théorème 9.3. *Soient $\beta>0$ un exposant de distribution pour les palindromes et $\epsilon>0$. Uniformément pour tout x et z assez grands, si $z<x^{\frac{1}{2}\beta-\epsilon}$, nous avons l'estimation*

$$\#\{n\in\mathscr{R}(x),\ P^-(n)\geqslant z\} \asymp_{g,\epsilon} \frac{\#\mathscr{R}(x)}{\log z}. \tag{9.8}$$

Remarque 9.2. Il peut paraître décevant d'obtenir un ordre de grandeur et non pas un équivalent du membre de gauche de (9.8), comme nous pourrions nous y attendre. Un équivalent du type du membre de droite est impossible, car tout palindrome possédant un nombre pair de chiffres est divisible par $g+1$. Ainsi, entre g^{2N-1} et g^{2N}, tous les palindromes ont un nombre pair de chiffre donc ne peuvent pas être premier. Mais

$$\frac{\#\mathscr{R}(g^{2N-1})}{\log g^{2N-1}} = \frac{g^{N-1}(g-1)}{(2N-1)\log g} \not\asymp \frac{g^N(g-1)}{2N\log g} = \frac{\#\mathscr{R}(g^{2N})}{\log g^{2N}}.$$

Nous pourrions tout de même espérer une estimation ressemblant à

$$\#\{n\in\mathscr{R}(x),\ P^-(n)\geqslant z\} \sim c_g\Big(\frac{\log x}{\log z}\Big)\frac{\#\mathscr{R}^1(x)}{\log z},$$

mais cela est encore impossible à cause des facteurs premiers de g. En particulier, la formule conjecturée par [BHS04] sur le nombre de palindromes premiers, à savoir l'existence d'une constante $c_g > 0$ telle que

$$\#\{n \in \mathscr{R}(x),\ n \text{ premier}\} \ \sim\ c_g \frac{\#\mathscr{R}(x)}{\log x}$$

est clairement fausse (sauf si g est un nombre premier en remplaçant $\mathscr{R}$ par $\mathscr{R}^1$ dans le membre de droite).

Nous déduirons du Théorème 9.3 trois applications. La première est une majoration du bon ordre de grandeur du nombre de palindrome premiers :

Corollaire 9.1. *Uniformément pour tout x, nous avons*

$$\#\{n \in \mathscr{R}(x),\ n \textit{ premier}\} \ \ll_g\ \frac{\#\mathscr{R}(x)}{\log x}.$$

La seconde est une minoration du bon ordre de grandeur à des puissances de $\log\log x$ près, du nombre de palindromes presque premiers :

Corollaire 9.2. *Il existe une constante $k_g > 0$ ne dépendant que de g telle que*

$$\#\{n \in \mathscr{R}(x),\ \Omega(n) \leqslant k_g\} \ \gg_g\ \frac{\#\mathscr{R}(x)}{\log x}.$$

Par exemple, nous pouvons choisir $k_2 = 60$, $k_{10} = 372$ et si g est assez grand, $k_g \sim 24\pi g$.

La dernière porte sur les palindromes friables :

Corollaire 9.3. *Il existe $\alpha > 0$ ne dépendant que de g tel qu'il existe une proportion positive de palindromes n qui sont n^α friables.*

Chapitre 10

Majoration d'une moyenne de pseudopalindromes

Nous posons

$$U(x) \ := \ \frac{1}{g}\sum_{d<g} \mathrm{e}(dx) \qquad \text{et} \qquad G_N(x) \ := \ \frac{1}{\#\mathscr{Q}_N}\sum_{n\in\mathscr{Q}_N} \mathrm{e}(nx). \tag{10.1}$$

où nous avons noté traditionnellement $\mathrm{e}(z) := e^{2i\pi z}$. Remarquons que $U(x)$ s'exprime aisément à l'aide de G_N puisque $U(x) = G_1(x)$. Le lemme suivant montre que $G_N(x)$ s'exprime également à partir de U.

Lemme 10.1. *Soient N un entier et $\delta = 0$ ou 1 de même parité que N. Pour tout x réel, nous avons*

$$G_N(x) \ = \ G_\delta(g^{\frac{N-1}{2}}x) \prod_{k<\frac{N+1}{2}} U(\Phi_{N-1}(k)x), \tag{10.2}$$

où $G_0(y) = 1$ et $G_1(y) = U(y)$ sont des fonctions bornées par 1.

Démonstration. Écrivons $N = 2M+\delta$ et montrons par récurrence sur M la factorisation

$$G_N(x) \ = \ G_\delta(g^M x) \prod_{k<M+1} U(\Phi_{N-1}(k)x), \tag{10.2'}$$

qui est équivalente à (10.2). Si $M = 0$, alors $G_N(x) = G_\delta(x) = G_\delta(g^M x)$ et le résultat est vrai. Supposons donc la factorisation vraie pour $M \geqslant 0$ et prouvons la pour $M+1$. En isolant le premier chiffre, nous avons la partition

$$\mathscr{Q}_{N+2} \ = \ \bigsqcup_{n_0<g} \Big(n_0\Phi_{N+1}(0) + g\mathscr{Q}_N\Big).$$

Donc

$$\begin{aligned} G_{N+2}(x) \ &= \ \frac{1}{\#\mathscr{Q}_{N+2}}\sum_{n\in\mathscr{Q}_{N+2}} \mathrm{e}(nx) \\ &= \ \frac{1}{g\#\mathscr{Q}_N}\sum_{n_0<g}\sum_{n\in\mathscr{Q}_N} \mathrm{e}\left((n_0\Phi_{N+1}(0)+gn)x\right), \end{aligned}$$

ce qui s'écrit en utilisant la définition de U,

$$G_{N+2}(x) \;=\; U(\Phi_{N+1}(0)x)G_N(gx). \tag{10.3}$$

Si nous utilisons l'hypothèse de récurrence pour évaluer le membre de droite de (10.3), nous en déduisons

$$G_{N+2}(x) \;=\; U(\Phi_{N+1}(0)x)G_\delta(g^{M+1}x)\prod_{k<M+1}U(g\Phi_{N-1}(k)x).$$

En utilisant l'identité (9.5), nous trouvons finalement

$$G_{N+2}(x) \;=\; U(\Phi_{N+1}(0)x)G_\delta(g^{M+1}x)\prod_{0<k<M+2}U(\Phi_{N+1}(k)x),$$

ce qui est exactement la factorisation (10.2') pour $M+1$. □

Le lemme 10.1 exprime la moyenne $G_N(x)$ sous la forme d'un produit de fonctions bornées par 1. Si nous montrons que chacune de ces fonctions s'approche rarement de 1, nous en déduirons une bonne majoration pour $|G_N(x)|$. C'est l'objectif du lemme 10.2 : exprimer sous une forme plus simple les facteurs du produit.

Soit $0 < c_3 < 4$ une constante (pouvant dépendre de g). Nous définissons pour tous réels $\mu > 0$ et x,

$$\mathcal{U}(x) \;:=\; 1 - c_3\|x\|^2 \qquad \text{et} \qquad \mathcal{G}_\mu(x) \;:=\; \prod_{k<\mu}\mathcal{U}(g^k x). \tag{10.4}$$

Nous n'indiquons pas la dépendance de ces fonctions par rapport à c_3 car cette constante est fixée dans toute la suite avec le lemme suivant.

Lemme 10.2. *Notons*

$$c_3 \;:=\; \begin{cases} 1 & \text{si } g \text{ est pair,} \\ 1 - \frac{1}{g} - \frac{1}{g^2} + \frac{1}{g^3} & \text{si } g \text{ est impair.} \end{cases} \tag{10.5}$$

Pour tous k et x, nous avons alors

$$\left|U(\Phi_N(k)x)U^2(\Phi_N(k+1)x)\right| \;\leqslant\; \mathcal{U}((g^2-1)g^k x). \tag{10.6}$$

En particulier, nous avons

$$|G_N(r)| \;\leqslant\; |\mathcal{G}_{\frac{N-1}{2}}((g^2-1)r)|^{\frac{1}{3}}. \tag{10.7}$$

Démonstration. Traitons en détail le cas g pair. En développant avec le binôme de Newton, nous avons

$$U(x)^2 \;=\; \frac{1}{g^2}\sum_{d<2g-1}a_h\,\mathrm{e}(hx) \qquad \text{où} \qquad a_h \;:=\; \min\{h+1, 2g-1-h\}.$$

Nous marions les exponentielles dont les exposants h sont de même reste modulo g :

$$\left|U(x)^2\right| \;\leqslant\; \frac{1}{g^2}\sum_{d<g}\left|(d+1)\,\mathrm{e}\left(dx\right) + (g-d-1)\,\mathrm{e}\left((d+g)x\right)\right|$$

Nous avons ainsi fait apparaître des termes $|1+\mathrm{e}(gx)|$. Nous allons les dénombrer :

$$\begin{aligned}\big|(d+1)\,\mathrm{e}\,(dx)+(g-d-1)\,\mathrm{e}\,((d+g)x)\big| \;&\leqslant\; \min\big(d+1,g-d-1\big)|1+\mathrm{e}(gx)|\\ &\quad+\max\big(d+1,g-d-1\big)-\min\big(d+1,g-d-1\big)\end{aligned}$$

En distinguant suivant la taille de $d+1$ et de $g-d-1$, nous obtenons

$$\begin{aligned}&\big|(d+1)\,\mathrm{e}\,(dx)+(g-d-1)\,\mathrm{e}\,((d+g)x)\big|\\ &\qquad\leqslant\;\begin{cases}(d+1)|1+\mathrm{e}(gx)|+g-2(d+1) & \text{si } d<\frac{g}{2}-1,\\ \frac{g}{2}|1+\mathrm{e}(gx)| & \text{si } d=\frac{g}{2}-1,\\ (g-d-1)|1+\mathrm{e}(gx)|+2(d+1)-g & \text{si } d>\frac{g}{2}-1,\end{cases}\end{aligned}$$

et finalement

$$\begin{aligned}|U(x)^2| \;&\leqslant\; \frac{2}{g^2}\sum_{d<\frac{g}{2}-1}(d+1)|1+\mathrm{e}\,(gx)|+\frac{1}{2g}|1+\mathrm{e}(gx)|+A\\ &\leqslant\; \Big(\frac{2}{g^2}\frac{\frac{g}{2}\big(\frac{g}{2}-1\big)}{2}+\frac{1}{2g}\Big)|1+\mathrm{e}(gx)|+A\end{aligned}$$

où A correspond aux termes majorés trivialement :

$$A \;=\; \frac{1}{g^2}\Big(g^2-4\sum_{d<\frac{g}{2}-1}(d+1)-g\Big).$$

Ainsi,

$$|U(x)^2| \;\leqslant\; \frac{1}{4}|1+\mathrm{e}(gx)|+\frac{1}{2}. \tag{10.8}$$

La base g étant paire, nous pouvons regrouper chaque élément pair de $\{0,\dots,g-2\}$ avec son successeur. Ainsi,

$$|U(x)| \;\leqslant\; \frac{1}{g}\frac{g}{2}|1+\mathrm{e}\,(x)| \;=\; \frac{1}{2}|1+\mathrm{e}\,(x)| \tag{10.9}$$

et en ne conservant du produit que la moitié des exponentielles (celles qui ont le même exposant), nous en déduisons l'estimation

$$\begin{aligned}&|\overline{U(\Phi_N(k)x)}U^2(\Phi_N(k+1)x)|\\ &\qquad\leqslant\; \frac{1}{8}|1+\mathrm{e}\,(-\Phi_N(k)x)||1+\mathrm{e}\,(g\Phi_N(k+1)x)|+\frac{1}{2}\\ &\qquad\leqslant\; \frac{1}{8}|1+\mathrm{e}\,(-\Phi_N(k)x+g\Phi_N(k+1))|+\frac{3}{4}\\ &\qquad\leqslant\; \frac{1}{8}|1+\mathrm{e}\,((g^2-1)g^kx)|+\frac{3}{4}\end{aligned}$$

en utilisant l'identité (9.6). D'où la majoration, en utilisant (3.28),

$$\begin{aligned}|U(\Phi_N(k)x)U^2(\Phi_N(k+1)x)| \;&\leqslant\; \frac{1}{8}|1+\mathrm{e}\,((g^2-1)g^kx)|+\frac{3}{4}\\ &\leqslant\; \frac{1}{4}(1-4\|(g^2-1)g^kx\|^2)+\frac{3}{4}\\ &\leqslant\; 1-\|(g^2-1)g^kx\|^2\end{aligned}$$

ce qui termine la preuve de la première majoration lorsque g est pair.

Si g est impair, la démarche est identique : quelques points de détail seulement changent (principalement le fait qu'il reste un terme célibataire que nous majorons donc par 1). Nous indiquons les deux résultats intermédiaires :

$$|U(x)^2| \leqslant \frac{1-\frac{1}{g^2}}{4}|1+\mathrm{e}(gx)|+1-\frac{1-\frac{1}{g^2}}{4} \tag{10.8'}$$

$$|U(x)| \leqslant \frac{1-\frac{1}{g}}{2}|1+\mathrm{e}(x)|+1-\frac{1-\frac{1}{g}}{2} \tag{10.9'}$$

d'où nous déduisons la majoration du lemme de la même façon que précédemment.

En regroupant $U(\Phi_N(k)r)$ avec $U(\Phi_N(k+1)r)^2$ dans l'expression de G_N donnée par le lemme 10.1, nous obtenons

$$|G_N(r)| \leqslant \prod_{k<\frac{N-1}{2}} |U(\Phi_N(k)r)U(\Phi_N(k+1)r)^2|^{\frac{1}{3}} \leqslant |\mathcal{G}_{\frac{N-1}{2}}(r)|^{\frac{1}{3}},$$

ce qui finit la preuve du lemme. □

Lemme 10.3. *Pour tout ensemble sans répétition $\mathfrak{R}$ de points de $]0,1[$ globalement invariant modulo 1 par les multiplications par g et par g^2-1 :*

$$g\mathfrak{R} = \mathfrak{R} \mod 1 \qquad et \qquad (g^2-1)\mathfrak{R} = \mathfrak{R} \mod 1,$$

pour tout entier $m \geqslant 1$ et pour tout N, nous avons

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \leqslant \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^\alpha, \tag{10.10}$$

où nous avons posé $\mu := \frac{N-1}{2m}$, $\alpha := \frac{m}{3}$ et où c_3 est la constante du lemme 10.2.

Démonstration. Soit r un réel fixé. Le lemme 10.2 et l'inégalité arithmético-géométrique donnent la majoration

$$\begin{aligned} |G_N(r)| &\leqslant |\mathcal{G}_{\frac{N-1}{2}}((g^2-1)r)|^{\frac{1}{3}} \\ &\leqslant \frac{1}{m}\sum_{h<m} \prod_{\frac{h(N-1)}{2m} \leqslant k < \frac{(h+1)(N-1)}{2m}} |\mathcal{U}(g^k(g^2-1)r)|^{\frac{m}{3}} \end{aligned}$$

En sommant sur les $r \in \mathfrak{R}$, nous avons donc

$$\begin{aligned} \sum_{r\in\mathfrak{R}} |G_N(r)| &\leqslant \frac{1}{m}\sum_{h<m}\sum_{r\in\mathfrak{R}} \prod_{\frac{h(N-1)}{2m}\leqslant k<\frac{h(N-1)}{2m}+\mu} |\mathcal{U}(g^k(g^2-1)r)|^\alpha \\ &\leqslant \frac{1}{m}\sum_{h<m}\sum_{r\in\mathfrak{R}}\prod_{j<\mu} |\mathcal{U}(g^j(g^2-1)r)|^\alpha \end{aligned}$$

puisque la multiplication par une puissance de g laisse $\mathfrak{R}$ invariant modulo 1. Par définition de $\mathcal{G}_\mu$, nous avons donc

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \leqslant \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu((g^2-1)r)|^\alpha, \tag{10.11}$$

ce qui implique immédiatement la majoration (10.10) puisque $\mathfrak{R}$ est invariant modulo 1 par la multiplication par g^2-1. □

Les deux prochains chapitres de cette partie sont consacrés à l'obtention de majorations pour

$$\sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^\alpha, \tag{10.12}$$

suivant la taille de μ, α et de propriétés spécifiques de $\mathfrak{R}$.

Chapitre 11

Théorèmes 9.1 et 9.2 dans le cas des pseudopalindromes de taille N

Pour démontrer le théorème 9.1, nous allons choisir α très grand dans (10.12) puisque ce paramètre va tendre vers l'infini avec μ. Il nous faut donc une majoration de (10.12) uniforme en α. Il existe à notre connaissance deux techniques permettant d'obtenir ce type de résultat : celle développée par C. Mauduit et A. Sarközy dans [MS97] pour l'étude des entiers dont la somme des chiffres est fixée et celle développée par S. Konyagin dans [Kon01] pour l'étude des entiers ellipséphiques. Nous utilisons ici cette seconde méthode qui permet d'obtenir une bonne majoration pour les très grands diviseurs.

11.1 Lemme de S. Konyagin

Soit $\delta > 0$. Un ensemble $\mathfrak{R}$ est dit δ bien espacé si pour tous choix de $r \neq r'$ dans $\mathfrak{R}$, nous avons $|r - r'| \geqslant \delta$. nous énonçons sous une forme générale un résultat obtenu par S. Konyagin lors d'une étape de la démonstration du théorème 1 de [Kon01] sur l'estimation du cardinal de $W_{\mathscr{D}}(x, a, q)$: il a étudié le cas particulier où $\mathfrak{R} = \{\frac{a}{q},\ 1 \leqslant a \leqslant q-1\}$, pour q fixé.

Lemme 11.1 (Konyagin)**.** *Soit $\mathfrak{R}$ un ensemble δ bien espacé de points de $[\frac{\delta}{2}, 1 - \frac{\delta}{2}]$ tel que si une fraction est dans $\mathfrak{R}$, son dénominateur irréductible est premier avec $2g$. Soit M un entier tel que $\delta g^M > 1$. Il existe alors une application injective*

$$\begin{array}{ccc} \mathfrak{R} & \longrightarrow & (\mathbb{Z} \cap]-\frac{g+1}{2}, \frac{g+1}{2}[)^M \\ r & \longmapsto & (\Delta_j)_{j<M} \end{array}$$

telle que $\|g^j r\| \leqslant \frac{1}{2g}$ si et seulement si $\Delta_j = 0$. De plus, si $r \in \mathfrak{R}$, alors (Δ_j) n'est pas identiquement nulle.

Démonstration. Notons

$$\mathfrak{N} \ := \ \{(n_0, \dots, n_M) \in \mathbb{Z}^{M+1},\ 0 \leqslant n_j \leqslant g^j\ \forall j,\ 0 < n_M < g^M\}.$$

Montrons que les deux applications suivantes sont bien définies et injectives :

$$\begin{array}{ccccc} \mathfrak{R} & \longrightarrow & \mathfrak{N} & \longrightarrow & \mathbb{Z}^M\backslash\{0\} \\ r & \longmapsto & (n_j)_{j<M+1} & \longmapsto & (\Delta_j)_{j<M} \end{array}$$

où $\Delta_j := n_{j+1} - gn_j$ et n_j est le plus proche entier de $g^j r$.

L'hypothèse faite sur $\mathfrak{R}$ assure que le nombre $g^j r$ n'est jamais un demi-entier si $r \in \mathfrak{R}$. La suite (n_j) est donc bien définie. Montrons qu'elle appartient à $\mathfrak{N}$: nous avons $0 < g^j r < g^j$ puisque $0 < r < 1$ et donc $0 \leqslant n_j \leqslant g^j$ pour tout j. Comme nous avons l'encadrement plus précis

$$\tfrac{\delta}{2} \;\leqslant\; r \;\leqslant\; 1 - \tfrac{\delta}{2} \qquad \text{et} \qquad \delta g^M \;>\; 1,$$

nous en déduisons $\frac{1}{2} < g^M r < g^M - \frac{1}{2}$. En utilisant maintenant que n_M est un entier, nous avons $1 \leqslant n_j \leqslant g^M - 1$, ce qui démontre que $(n_j) \in \mathfrak{N}$.

Soient $r \neq r'$ deux points différents de $\mathfrak{R}$. Alors

$$1 \;<\; g^M \delta \;\leqslant\; \left| g^M r - g^M r' \right|,$$

ce qui assure que $n_M \neq n'_M$. La première application est bien injective.

Clairement la suite (Δ_j) est bien définie. La seule propriété à prouver est qu'elle n'est pas identiquement nulle. Raisonnons par l'absurde et supposons que $\Delta_j = 0$ pour tout j. Alors $0 = \Delta_j = n_{j+1} - n_j$ pour tout j, ce qui implique que $n_M = g^M n_0$. Mais $n_0 = 0$ ou 1 par définition de $\mathfrak{N}$. Donc $n_M = 0$ ou g^M ce qui est incompatible avec la définition de $\mathfrak{N}$.

Pour montrer l'injectivité de la seconde application, il suffit de montrer que n_0 se détermine de façon unique à partir de (Δ_j). La suite (n_j) sera alors complètement déterminée puisque $n_{j+1} = gn_j + \Delta_j$. Notons Δ_i le premier terme non nul de la suite (Δ_j) dont nous venons de prouver l'existence. Comme précédemment, nous avons

$$n_{i+1} \;=\; g^{i+1} n_0 + \Delta_i \tag{11.1}$$

puisque (n_j) est une suite géométrique de raison g tant que $j \leqslant i$. Mais par définition de $\mathfrak{N}$, nous savons que $0 \leqslant n_i \leqslant g^i$. L'équation (11.1) impose donc $n_0 = 0$ si $\Delta_i > 0$ et $n_0 = 1$ si $\Delta_i < 0$. La valeur de n_0 est donc bien déterminée par la suite (Δ_j), ce qui prouve l'injectivité.

Pour terminer la preuve du lemme, il reste à prouver que si $r \in \mathfrak{R}$, alors

1. $|\Delta_j| < \frac{g+1}{2}$ pour tout j,
2. $\|g^j r\| \leqslant \frac{1}{2g}$ si et seulement si $\Delta_j = 0$.

Pour cela, notons $\epsilon_j := g^j r - n_j$ l'erreur commise en remplaçant $g^j r$ par son approximation entière n_j. L'entier Δ_j admet une nouvelle expression :

$$\Delta_j \;=\; -\epsilon_{j+1} + g\epsilon_j.$$

La majoration du premier point se déduit immédiatement de cette nouvelle expression de Δ_j puisque $g^j r$ n'est jamais un demi-entier. L'équivalence du second point est tout aussi simple puisque $\|g^j r\| = |\epsilon_j| = \frac{1}{g}|\Delta_j + \epsilon_{g+1}|$ et Δ_j est un entier. □

Corollaire 11.1 (Konyagin). *Il existe une constante $c_2 > 0$ ne dépendant que de g telle que pour tout $\mathfrak{R}$ ensemble δ bien espacé de points de $[\frac{\delta}{2}, 1-\frac{\delta}{2}]$ vérifiant l'hypothèse du lemme 11.1, pour tout réel $\alpha > 0$ et tout entier $M \geqslant 1$ tel que $\frac{1}{\delta} < g^M$, nous avons*

$$\sum_{r\in\mathfrak{R}} |\mathcal{G}_M(r)|^\alpha \leqslant \Big(1 + c_2(1-\tfrac{c_3}{4g^2})^\alpha\Big)^M - 1.$$

Par exemple, nous pouvons choisir $c_2 := g$. Dans le cas où g est impair, nous pouvons choisir $c_2 := g-1$.

Démonstration. Le lemme 11.1 permet de réaliser une partition de $\mathfrak{R}$ suivant le nombre de fois où $\|g^j r\|$ est "petit" : pour tout entier k, nous notons $\mathfrak{R}(k)$ l'ensemble des points $r \in \mathfrak{R}$ pour lesquels

$$\#\{j < M,\ \|g^j r\| > \tfrac{1}{2g}\} = k,$$

de sorte que

$$\begin{aligned}\sum_{r\in\mathfrak{R}} |\mathcal{G}_M(r)|^\alpha &= \sum_{r\in\mathfrak{R}} \prod_{j<M} \Big(1 - c_3\|g^j r\|^2\Big)^\alpha \\ &\leqslant \sum_{k\geqslant 0} \#\mathfrak{R}(k)\Big(1-\frac{c_3}{4g^2}\Big)^{\alpha k}.\end{aligned}$$

Mais $\#\mathfrak{R}(0) = 0$, puisque le lemme 11.1 assure que la suite (Δ_j) n'est pas identiquement nulle. L'application injective du lemme 11.1 permet de majorer $\#\mathfrak{R}(k)$ par le nombre de M-uplets à valeurs dans $\{-\frac{c_2}{2}, \dots, \frac{c_2}{2}\}$ avec exactement $M-k$ composantes nulles : il y a $\binom{M}{M-k}$ choix pour les $M-k$ zéros de la suite et c_2 choix pour chacun des k autres nombres. Donc

$$\begin{aligned}\sum_{r\in\mathfrak{R}} |\mathcal{G}_M(r)|^\alpha &\leqslant \sum_{k\geqslant 1} \binom{M}{M-k} {c_2}^k \Big(1-\frac{c_3}{4g^2}\Big)^{\alpha k} \\ &\leqslant \Big(1 + c_2\Big(1-\frac{c_3}{4g^2}\Big)^\alpha\Big)^M - 1\end{aligned}$$

ce qui termine la preuve. □

11.2 Preuve du théorème 9.1 pour $\mathscr{Q}_N$

Soit $\mathfrak{R}$ un ensemble de fractions de $]0,1[$. Nous disons que $\mathfrak{R}$ vérifie l'hypothèse (H_δ) si $\mathfrak{R}$ est δ bien espacé, si $\mathfrak{R}$ est invariant modulo 1 par les multiplications par g et par g^2-1 et si les dénominateurs irréductibles de $\mathfrak{R}$ sont tous premiers avec $2g$:

$$\left\{\begin{array}{ccccc} r \neq r' \in \mathfrak{R} & & \Longrightarrow & & |r-r'| \geqslant \delta \\ g\mathfrak{R} = \mathfrak{R} \mod 1 & & \text{et} & & (g^2-1)\mathfrak{R} = \mathfrak{R} \mod 1 \\ \frac{l}{q} \in \mathfrak{R} & \text{et} & (l,q)=1 & \Longrightarrow & (q,2g)=1 \end{array}\right\} \qquad (\mathrm{H}_\delta)$$

Lemme 11.2. *Il existe une constante $c_4 > 0$ ne dépendant que de g telle qu'uniformément pour tout $\delta > 0$, tout ensemble $\mathfrak{R}$ de fractions de $[\frac{\delta}{2}, 1 - \frac{\delta}{2}]$ vérifiant l'hypothèse (H_δ) et tout entier N assez grand pour que*

$$\frac{N-1}{4} \geqslant \frac{\log \frac{1}{\delta}}{\log g} \qquad et \qquad c_4 N \geqslant \log\left(\tfrac{1}{\delta}\right) \log_2\left(\tfrac{1}{\delta}\right), \tag{11.2}$$

nous avons la majoration

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \ll_g \log\left(\frac{g}{\delta}\right) \mathrm{e}^{-\frac{c_4 N}{\log \frac{1}{\delta}}}.$$

Par exemple, si c_3 est une constante admissible pour le lemme 10.2, nous pouvons choisir $c_4 := \frac{\log g}{24 g^2} c_3$.

Remarque 11.1. Dès que $\frac{1}{\delta}$ est assez grand par rapport à g, ce qui est toujours le cas en pratique, la seconde condition de (11.2) implique la première.

Démonstration. Nous choisissons l'entier m tel que

$$\frac{N-1}{2}\frac{\log g}{\log \frac{1}{\delta}} - 1 \leqslant m < \frac{N-1}{2}\frac{\log g}{\log \frac{1}{\delta}},$$

Nous avons bien $m \geqslant 1$ grâce à la première condition de notre hypothèse (11.2). Le lemme 10.3 permet alors d'écrire, en notant $\mu := \frac{N-1}{2m}$,

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \leqslant \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^{\frac{m}{3}}. \tag{11.3}$$

Remarquons que le majorant de la définition de m implique

$$g^\mu = g^{\frac{N-1}{2m}} > g^{\frac{\log \frac{1}{\delta}}{\log g}} = \frac{1}{\delta}.$$

Si nous notons $M := \lceil \mu \rceil$, nous aurons donc $\frac{1}{\delta} < g^M$ et nous pouvons utiliser le corollaire 11.1 pour majorer le membre de droite de (11.3). Ainsi,

$$\begin{aligned}
\sum_{r\in\mathfrak{R}} |G_N(r)| &\leqslant \left(1 + c_2\left(1 - \tfrac{c_3}{4g^2}\right)^{\frac{m}{3}}\right)^M - 1 \\
&\leqslant \left(1 + c_2\, \mathrm{e}^{-\frac{c_3}{4g^2}\frac{m}{3}}\right)^M - 1 \\
&\leqslant \exp\left(c_2(\mu+1) e^{-\frac{c_3}{12g^2} m}\right) - 1.
\end{aligned}$$

Donc

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \leqslant \exp\left(c_2\left(\frac{N-1}{2m} + 1\right) \mathrm{e}^{-\frac{c_3}{12g^2} m}\right) - 1. \tag{11.4}$$

Le minorant de la définition de m donne

$$\frac{\log g}{\log \frac{1}{\delta}} \frac{N-1}{2m} \leqslant 1 + \frac{1}{m} \leqslant 2.$$

Donc

$$\frac{N-1}{2m}+1 \ll_g \log\frac{1}{\delta}.$$

Le membre de droite de (11.4) étant décroissant avec m, nous avons pour deux constantes $c_4>0$ et $c_5>0$ ne dépendant que de g,

$$\begin{aligned}\sum_{r\in\mathfrak{R}}|G_N(r)| &\leqslant \exp\Big(c_5\log\big(\tfrac{1}{\delta}\big)\,\mathrm{e}^{-\frac{c_4N}{\log\frac{1}{\delta}}}\Big)-1\\ &\leqslant \mathrm{e}^{c_5\log\left(\frac{1}{\delta}\right)\mathrm{e}^{-\frac{c_4N}{\log\frac{1}{\delta}}}},\end{aligned}$$

puisque la convexité de l'exponentielle assure lorsque $x\in[0,1]$ que $\mathrm{e}^{ax}-1\leqslant(\mathrm{e}^a-1)x$. La seconde condition de notre hypothèse (11.2) garantit que nous sommes effectivement dans l'intervalle $[0,1]$. □

Lemme 11.3. *Il existe des constantes c et $\tilde{c}>0$ ne dépendant que de g telles qu'uniformément pour N assez grand (en terme de g) et q un entier vérifiant*

$$q \leqslant \exp\Big(\frac{cN}{\log N}\Big) \qquad et \qquad (q,g^3-g) = 1,$$

nous avons la majoration

$$\max_{a\in\mathbb{Z}}\Big|\#\mathscr{Q}_N(g^N,a,q)-\frac{\#\mathscr{Q}_N}{q}\Big| \ll_g \frac{\#\mathscr{Q}_N}{q}\exp\Big(-\frac{\tilde{c}N}{\log q}\Big).$$

Si c_4 désigne une constante admissible pour le lemme 11.2, nous pouvons prendre tous les c et $\tilde{c}>0$ tels que

$$c+\tilde{c} \leqslant c_4.$$

Démonstration. Pour estimer le nombre de pseudopalindromes divisibles par q, nous introduisons des somme d'exponentielles :

$$\begin{aligned}\#\mathscr{Q}_N(g^N,a,q) &= \sum_{n\in\mathscr{Q}_N}\frac{1}{q}\sum_{l<q}\mathrm{e}\Big(l\frac{n-a}{q}\Big)\\ &= \frac{1}{q}\sum_{l<q}\mathrm{e}\Big(-\frac{al}{q}\Big)\sum_{n\in\mathscr{Q}_N}\mathrm{e}\Big(\frac{nl}{q}\Big)\\ &= \frac{\#\mathscr{Q}_N}{q}\sum_{l<q}\mathrm{e}\Big(-\frac{al}{q}\Big)G_N\Big(\frac{l}{q}\Big).\end{aligned}$$

Nous isolons le terme $l=0$ qui fournit la partie principale :

$$\#\mathscr{Q}_N(g^N,a,q) = \frac{\#\mathscr{Q}_N}{q}+\frac{\#\mathscr{Q}_N}{q}\sum_{0<l<q}\mathrm{e}\Big(-\frac{al}{q}\Big)G_N\Big(\frac{l}{q}\Big).$$

Avec une inégalité triangulaire, nous obtenons donc

$$\Big|\#\mathscr{Q}_N(g^N,a,q)-\frac{\#\mathscr{Q}_N}{q}\Big| \leqslant \frac{\#\mathscr{Q}_N}{q}\sum_{0<l<q}\Big|G_N\Big(\frac{l}{q}\Big)\Big|. \tag{11.5}$$

Notons $\mathfrak{R} := \{\frac{l}{q},\ 0 < l < q\}$. Comme nous avons fait l'hypothèse que $(q, g^3 - g) = 1$, nous avons $(q, g) = 1$ et $(q, g^2 - 1) = 1$, donc les multiplications par g et par $g^2 - 1$ sont des bijections dans $(\mathbb{Z}/q\mathbb{Z})\backslash\{0\}$. Ainsi $\mathfrak{R}$ est un ensemble de fractions de $[\frac{\delta}{2}, 1 - \frac{\delta}{2}]$ vérifiant l'hypothèse (H_δ) avec $\delta := \frac{1}{q}$. De plus

$$\begin{aligned}\log\Big(\frac{1}{\delta}\Big)\log_2\Big(\frac{1}{\delta}\Big) &= \log q \log_2 q \\ &\leqslant \frac{cN}{\log N}\Big(\log\frac{cN}{\log N}\Big) \\ &\leqslant cN(1 + o(1)).\end{aligned}$$

Comme $c < c_4$, les hypothèses du lemme 11.2 sont donc vérifiées lorsque N est assez grand par rapport à g, ce qui permet de majorer :

$$\Big|\#\mathscr{Q}_N(g^N, a, q) - \frac{\#\mathscr{Q}_N}{q}\Big| \ll_g \frac{\#\mathscr{Q}_N}{q}\log(q)\exp\Big(-\frac{c_4 N}{\log q}\Big).$$

Mais

$$\log(q)\exp\Big(-\frac{cN}{\log q}\Big) \leqslant \frac{cN}{\log N}\exp\big(-\log N\big) = \frac{c}{\log N} \ll_g 1,$$

et puisque nous avons imposé $c + \tilde{c} \leqslant c_4$, nous avons donc

$$\log(q)\exp\Big(-\frac{c_4 N}{\log q}\Big) \ll_g \exp\Big(-\frac{\tilde{c}N}{\log q}\Big),$$

ce qui termine la preuve du lemme. □

11.3 Lemmes préliminaires à la démonstration du théorème 9.2

Pour un réel $\alpha \geqslant 1$, nous définissons $\mathcal{K}_\alpha$ par

$$\mathcal{K}_\alpha := \limsup_{\mu\to\infty} \big\||\mathcal{G}_\mu|^\alpha\big\|_1^{\frac{1}{\mu}}. \tag{11.6}$$

Lemme 11.4. *Définissons $\mathcal{M}_\alpha$ par*

$$\mathcal{M}_\alpha := \max_{u\in[0,1]} \frac{1}{g}\sum_{0\leqslant h<g}\Big|\mathcal{U}\Big(\frac{u+h}{g}\Big)\Big|^\alpha. \tag{11.7}$$

Alors $\mathcal{K}_\alpha \leqslant \mathcal{M}_\alpha$ pour tout $\alpha \geqslant 1$.

Démonstration. Prenons un entier $N \geqslant 1$ et calculons l'intégrale de ${\mathcal{G}_N}^{2l}$ en découpant

le segment $[0,1]$ en g sous-segments de longueur $\frac{1}{g}$:

$$\begin{aligned}
\left\| |\mathcal{G}_N|^\alpha \right\|_1 &= \sum_{0\leqslant h<g} \int_{\frac{h}{g}}^{\frac{h+1}{g}} \prod_{k<N} |\mathcal{U}(g^k s)|^\alpha \mathrm{d}s \\
&= \sum_{0\leqslant h<g} \int_{\frac{h}{g}}^{\frac{h+1}{g}} |\mathcal{U}(s)|^\alpha \prod_{k<N-1} |\mathcal{U}(g^k g s)|^\alpha \mathrm{d}s \\
&= \frac{1}{g} \sum_{0\leqslant h<g} \int_0^1 |\mathcal{U}(\tfrac{u+h}{g})|^\alpha \prod_{k<N-1} |\mathcal{U}(g^k(u+h))|^\alpha \mathrm{d}u \\
&= \frac{1}{g} \sum_{0\leqslant h<g} \int_0^1 |\mathcal{U}(\tfrac{u+h}{g})|^\alpha |\mathcal{G}_{N-1}(u)|^\alpha \mathrm{d}u \qquad (11.8)
\end{aligned}$$

puisque $\mathcal{G}_{N-1}$ est une fonction 1 périodique. La définition de $\mathcal{M}_\alpha$ implique

$$\left\| {\mathcal{G}_N}^\alpha \right\|_1 \leqslant \mathcal{M}_\alpha \left\| {\mathcal{G}_{N-1}}^\alpha \right\|_1 \leqslant \ldots \leqslant {\mathcal{M}_\alpha}^N.$$

Ainsi, $\limsup_{N\to\infty} \left\| |\mathcal{G}_N|^\alpha \right\|_1^{\frac{1}{N}} \leqslant \mathcal{M}_\alpha$. Comme

$$\left\| |\mathcal{G}_\mu|^\alpha \right\|_1^{\frac{1}{\mu}} = \left(\left\| |\mathcal{G}_{\lceil\mu\rceil}|^\alpha \right\|_1^{\frac{1}{\lceil\mu\rceil}} \right)^{\frac{\lceil\mu\rceil}{\mu}},$$

nous obtenons $\mathcal{K}_\alpha \leqslant \mathcal{M}_\alpha$ en prenant la limite supérieure à gauche et à droite de cette égalité. □

Nous redonnons le lemme 3.14 avec les notations propres à cette partie :

Lemme 11.5. *Pour tout réel $\alpha \geqslant 1$,*

$$\mathcal{M}_\alpha < \frac{1}{g} + \sqrt{\frac{\pi}{\alpha c_3}}. \qquad (11.9)$$

Plus g est grand, plus la majoration $\mathcal{K}_\alpha \leqslant \mathcal{M}_\alpha$ donnée par le lemme 11.4 est précise. Lorsque g est très petit, nous obtiendrons une majoration plus fine en effectuant plus d'itérations dans le processus de moyenne. Définissons par récurrence sur k les fonctions

$$P_0(u) := 1 \qquad \text{et} \qquad P_{k+1}(u) := \frac{1}{g} \sum_{0\leqslant h<g} |\mathcal{U}(\tfrac{u+h}{g})|^\alpha P_k(\tfrac{u+h}{g}). \qquad (11.10)$$

Des fonctions P_k de ce type ont déjà été introduites et étudiées par [FM96] et [DM01].

Lemme 11.6. *Pour tout réel $\alpha \geqslant 1$ et tout entier k, nous avons*

$$\mathcal{K}_\alpha \leqslant \mathcal{M}_\alpha^k \qquad \text{où} \qquad \mathcal{M}_\alpha^k := \left(\max_{u\in[0,1]} \tilde{P}_k(u) \right)^{\frac{1}{k}}. \qquad (11.11)$$

Démonstration. Nous repartons de la majoration (11.8) :

$$\left\| |\mathcal{G}_N|^\alpha \right\|_1 = \int_0^1 \frac{1}{g} \sum_{0\leqslant h<g} |\mathcal{U}(\tfrac{u+h}{g})|^\alpha |\mathcal{G}_{N-1}(u)|^\alpha \mathrm{d}u.$$

La définition de $P_1(u)$ donne donc

$$\left\| |\mathcal{G}_N|^\alpha \right\|_1 = \int_0^1 P_1(u) |\mathcal{G}_{N-1}(u)|^\alpha \mathrm{d}u.$$

En utilisant le même argument de découpage de l'intégrale puis de changement de variable, nous avons pour tout entier $k \leqslant N$,

$$\left\| |\mathcal{G}_N|^\alpha \right\|_1 = \int_0^1 P_k(u) |\mathcal{G}_{N-k}(u)|^\alpha \mathrm{d}u,$$

ce qui implique immédiatement la majoration $\mathcal{K}_\alpha \leqslant \mathcal{M}_\alpha^k$. □

Lemme 11.7. *Si $c_3 < 4$ et $\alpha \geqslant 1$, alors uniformément pour N assez grand, nous avons*

$$\left\| \left({\mathcal{G}_N}^\alpha\right)' \right\|_1 \leqslant \frac{4c_3\alpha}{4-c_3} \frac{g^N-1}{g-1} \left\| {\mathcal{G}_N}^\alpha \right\|_1 \ll_{g,\alpha,c_3} g^N \left\| {\mathcal{G}_N}^\alpha \right\|_1.$$

Démonstration. Supposons $\alpha > 1$. Nous écrivons alors l'égalité vérifiée presque partout

$$\left({\mathcal{G}_N}^\alpha\right)' = \alpha {\mathcal{G}_\alpha}' {\mathcal{G}_N}^{\alpha-1}$$

et nous appliquons l'inégalité de Hölder avec les exposants α et $\frac{\alpha}{\alpha-1}$. Ainsi,

$$\left\| \left({\mathcal{G}_N}^\alpha\right)' \right\|_1 \leqslant \alpha \left\| {\mathcal{G}_N}^\alpha \right\|_1^{1-\frac{1}{\alpha}} \left\| {\mathcal{G}_N}' \right\|_\alpha. \tag{11.12}$$

Mais si $g^k x$ n'est pas un demi-entier (donc pour presque tout x),

$$|{\mathcal{G}_N}'(x)| \leqslant |\mathcal{G}_N(x)| \sum_{k<N} 2c_3 g^k \frac{\|g^k x\|}{1 - c_3 \|g^k x\|^2},$$

ce qui implique que pour presque tout x,

$$|{\mathcal{G}_N}'(x)| \leqslant \frac{c_3}{1-\frac{c_3}{4}} \frac{g^N-1}{g-1} |\mathcal{G}_N(x)|. \tag{11.13}$$

Nous reportons cette majoration dans (11.12) et le lemme est démontré. Si $\alpha = 1$, le lemme se déduit directement de la majoration (11.13). □

11.4 Lemme de C. Mauduit et A. Sárközy

C. Mauduit et A. Sárközy dans [MS97, lemme 2] ont prouvé le lemme suivant. Nous donnons ici une preuve simplifiée et légèrement améliorée de leur résultat, preuve obtenue en choisissant de façon optimale les différents paramètres à notre disposition au cours de la démonstration.

Lemme 11.8 (MS)**.** *Soient $r = \frac{l}{q}$ une fraction irréductible et $\mu > 0$. S'il existe un nombre premier p tel que $p \mid q$ et $p \nmid g$, alors*

$$\sum_{k<\mu} \|g^k r\|^2 > \frac{\log g}{(g+1)^2} \frac{\mu}{\log(gq)} - \frac{1}{(g+1)^2}. \tag{11.14}$$

En particulier, si q est premier avec $g(g-1)$, pour tout $\beta \in \mathbb{R}$, nous avons

$$\sum_{k<\mu} \|\beta + g^k r\|^2 > \frac{\log g}{4(g+1)^2} \frac{\mu}{\log(gq)} - \frac{1}{2(g+1)^2}. \tag{11.14'}$$

Remarque 11.2. La condition restante sur l'existence d'un p divisant m mais pas g est évidemment nécessaire, sans quoi le membre de gauche est une fonction bornée de μ alors que le membre de droite tend vers l'infini.

Démonstration. Notons $d := \left\lceil \frac{\log q}{\log g} \right\rceil$ et réalisons la division euclidienne de μ par d. Il existe un entier $n \geqslant 0$ tel que

$$nd \ \leqslant \ \mu \ < \ (n+1)d.$$

Alors

$$\sum_{k<\mu} \|g^k r\|^2 \ \geqslant \ \sum_{k<n} \sum_{j<d} \|g^{j+kd} r\|^2. \tag{11.15}$$

Fixons l'entier k et montrons que nous pouvons toujours trouver un indice $j = j_k < d$ pour lequel

$$\|g^{j+kd} r\| \ \geqslant \ \frac{1}{g+1}.$$

Notre hypothèse sur l'existence d'un nombre premier p divisant q mais pas g implique que $q \nmid g^{kd}$ donc que $g^{kd} r \notin \mathbb{Z}$. Comme $\frac{g}{g+1} > \frac{1}{2}$, il existe un entier t tel que

$$0 \ < \ R \ := \ |g^{kd} r - t| \ < \ \frac{g}{g+1}.$$

Choisissons alors l'entier $j = j_k$ tel que

$$g^j R \ < \ \frac{g}{g+1} \ \leqslant \ g^{j+1} R. \tag{11.16}$$

Donc

$$\frac{1}{g+1} \ = \ \frac{1}{g} \frac{g}{g+1} \ \leqslant \ \frac{1}{g} g^{j+1} R \ = \ g^j R \ < \ \frac{g}{g+1} \ = \ 1 - \frac{1}{g+1},$$

ce qui nous assure que pour ce choix de j_k

$$\|g^{j_k+kd} r\| \ = \ \|g^{j_k} R\| \ \geqslant \ \frac{1}{g+1}. \tag{11.17}$$

Mais $\frac{1}{R} \leqslant q$ puisque R est une fraction non triviale de dénominateur au plus q. La minoration de (11.16) assure donc

$$j_k \ < \ \frac{\log \frac{gq}{g+1}}{\log g} \ < \ \frac{\log q}{\log g} \ \leqslant \ d.$$

En reportant la minoration (11.17) dans (11.15), nous trouvons que

$$\sum_{k<\mu} \|g^k r\|^2 \ \geqslant \ \sum_{k<n} \|g^{j_k} g^{kd} r\|^2 \ \geqslant \ \frac{n}{(g+1)^2}.$$

Mais par définition de n et de d, nous avons

$$n \ > \ \frac{\mu}{d} - 1 \ \geqslant \ \frac{\mu \log g}{\log(gq)} - 1,$$

ce qui implique la minoration (11.14).

Pour en déduire (11.14'), nous regroupons chaque terme de la somme avec son successeur :

$$\begin{aligned}\sum_{k<\mu}\|\beta+g^k r\|^2 &\geqslant \frac{1}{2}\sum_{k<\mu-1}\Big(\|\beta+g^k r\|^2+\|\beta+g^{k+1}r\|^2\Big)\\ &\geqslant \frac{1}{4}\sum_{k<\mu-1}\|g^k(g-1)r\|^2\end{aligned}$$

en utilisant la minoration $\|x\|^2+\|y\|^2\geqslant\frac{1}{2}\|x-y\|^2$ valable pour tous réels x et y. Comme nous avons supposé q premier avec $g(g-1)$, nous pouvons appliquer (11.14) à la fraction $(g-1)r$. Ainsi,

$$\sum_{k<\mu}\|\beta+g^k r\|^2 \;>\; \frac{\log g}{4(g+1)^2}\frac{\mu-1}{\log gq}-\frac{1}{4(g+1)^2},$$

ce qui implique immédiatement (11.14'). □

Corollaire 11.2. *Il existe une constante $c_6>0$ ne dépendant que de g telle que pour toute fraction r de dénominateur irréductible q premier avec g et tout $\mu>0$, nous avons*

$$|\mathcal{G}_\mu(r)| \;<\; 2\exp\Big(-\frac{c_6\mu}{\log gq}\Big). \tag{11.18}$$

Par exemple, $c_6:=\frac{\log g}{(g+1)^2}c_3$ convient.

Démonstration. Nous reportons directement la majoration du lemme 11.8 dans la définition de $\mathcal{G}_\mu$:

$$\begin{aligned}|\mathcal{G}_\mu(r)| &= \exp\Big(\sum_{k<\mu}\log\big(1-c_3\|g^k r\|^2\big)\Big)\\ &\leqslant \exp\Big(\sum_{k<\mu}-c_3\|g^k r\|^2\Big)\\ &\leqslant \exp\Big(-\frac{c_6\mu}{\log gq}+\frac{1}{(g+1)^2}\Big),\end{aligned}$$

ce qui termine la preuve puisque $\exp\big((g+1)^{-2}\big)\leqslant\exp\big(\frac{1}{9}\big)<2$. □

11.5 Preuve du théorème 9.2 pour $\mathscr{Q}_N$

A l'inverse de la démonstration du théorème 9.1 où nous avions choisi α très grand dans (10.12) puisque α tendait vers l'infini avec μ, nous essayons ici de trouver le plus petit α possible, car l'exposant de distribution que nous obtiendrons sera décroissant avec α. En particulier, α doit absolument rester borné quand μ est grand et nos majorations peuvent donc dépendre du paramètre α.

Nous posons pour tous réels $\mu>0$ et $\alpha\geqslant 1$,

$$\mathscr{S}_\mu^\alpha(Q) \;:=\; \sum_{\substack{q<Q\\(q,g)=1}}\sum_{(l,q)=1}|\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha. \tag{11.19}$$

En utilisant une méthode similaire à celle de la démonstration du lemme 2 de l'article de S. Konyagin [Kon01], nous pourrions montrer que pour un choix convenable des paramètres c, $\tilde{c} > 0$ et $\alpha \geqslant 1$ ne dépendant que de g, nous avons

$$\mathscr{S}_\mu^\alpha(Q) \ll_g Q\exp(-\tfrac{\tilde{c}}{2}\sqrt{\mu}) \qquad \text{dès que} \qquad \exp(\tilde{c}\sqrt{\mu}) < Q < g^{c\mu},$$

qui est le type de majoration nécessaire pour démontrer le théorème 9.2. Nous allons utiliser une autre méthode pour majorer $\mathscr{S}_\mu^\alpha(Q)$, similaire à celle que nous avons utilisée dans la première partie de cette thèse, qui fournira une majoration du même type mais valable pour une constante c nettement plus grande.

Lemme 11.9. *Soient $\alpha \geqslant 1$ et $c_7 > 0$ fixés. Uniformément pour $Q \leqslant \frac{1}{g}\exp(c_7\sqrt{\mu})$ et $\mu > 0$, nous avons*

$$\mathscr{S}_\mu^\alpha(Q) \ll_{g,\alpha} \exp\Big(-(\frac{\alpha c_6}{c_7} - 2c_7)\sqrt{\mu}\Big), \tag{11.20}$$

où c_6 désigne une constante admissible pour le corollaire 11.2.

Démonstration. Puisque nous sommons sur des entiers premiers avec g, nous pouvons utiliser la majoration du corollaire 11.2 qui fournit

$$\begin{aligned}\mathscr{S}_\mu^\alpha(Q) &\leqslant \sum_{q<Q}\sum_{(l,q)=1} 2^\alpha \exp\Big(-\frac{\alpha c_6\mu}{\log gq}\Big)\\ &\leqslant \sum_{q<Q}\sum_{(l,q)=1} 2^\alpha \exp\Big(-\frac{\alpha c_6\mu}{\log gQ}\Big)\\ &\leqslant 2^\alpha\sum_{q<Q}\varphi(q)\exp\Big(-\frac{\alpha c_6\mu}{\log gQ}\Big)\end{aligned}$$

où $\varphi(q)$ désigne la fonction d'Euler. Comme $\varphi(q) \leqslant q-1$, nous avons

$$\begin{aligned}\mathscr{S}_\mu^\alpha(Q) &\leqslant 2^{\alpha-1}Q^2\exp\Big(-\frac{\alpha c_6\mu}{\log gQ}\Big)\\ &\leqslant \frac{2^{\alpha-1}}{g^2}\exp\Big((2c_7 - \frac{\alpha c_6}{c_7})\sqrt{\mu}\Big),\end{aligned}$$

ce qui termine la preuve de cette majoration. □

Lemme 11.10. *Soient $\alpha \geqslant 1$ et $\epsilon > 0$ fixés. Uniformément pour $\mu > 0$ et Q assez grands, nous avons*

$$\mathscr{S}_\mu^\alpha(Q) \ll_{g,\alpha,\epsilon} Q^2(\mathcal{K}_\alpha+\epsilon)^\mu + Q^{2+2\frac{\log(\mathcal{K}_\alpha+\epsilon)}{\log g}}. \tag{11.21}$$

Démonstration. Comme $\mathcal{G}_\mu$ est un produit de fonctions bornées par 1, on observe que l'application $\nu \mapsto \mathscr{S}_\nu^\alpha(Q)$ est décroissante. Pour tout $\nu \leqslant \mu$, nous avons donc

$$\mathscr{S}_\mu^\alpha(Q) \leqslant \mathscr{S}_\nu^\alpha(Q) = \sum_{r\in\mathfrak{R}}|\mathcal{G}_\nu(r)|^\alpha,$$

avec $\mathfrak{R} := \{\frac{l}{q},\ (l,q)=1,\ q<Q,\ (q,g)=1\}$ qui est une famille $\delta = Q^{-2}$ bien espacée de points de $[\frac{\delta}{2}, 1-\frac{\delta}{2}]$. Le lemme A.1 de Sobolev-Gallagher énoncé dans l'annexe A permet d'écrire

$$\begin{aligned}\mathscr{S}_\mu^\alpha &\leqslant Q^2\|{\mathcal{G}_\nu}^\alpha\|_1 + \|({\mathcal{G}_\nu}^\alpha)'\|_1\\ &\ll_{\alpha,g} (Q^2+g^\nu)\|{\mathcal{G}_\nu}^\alpha\|_1\end{aligned}$$

en utilisant le lemme 11.7 pour majorer la dérivée. Si ν est assez grand, la définition de $\mathcal{K}_\alpha$ implique que

$$\mathscr{S}_\mu^\alpha(Q) \ll_{g,\alpha,\epsilon} (Q^2+g^\nu)(\mathcal{K}_\alpha+\epsilon)^\nu.$$

Nous optimisons notre paramètre $\nu \leqslant \mu$ en choisissant

$$\nu := \min\Big\{\mu,\ 2\frac{\log Q}{\log g}\Big\} \tag{11.22}$$

qui est effectivement assez grand par rapport à g, α et ϵ dès que Q et μ le sont, ce qui est une hypothèse du lemme. Nous obtenons ainsi

$$\mathscr{S}_\mu^\alpha \ll_{g,\alpha,\epsilon} Q^2(\mathcal{K}_\alpha+\epsilon)^\mu + Q^2(\mathcal{K}_\alpha+\epsilon)^{2\frac{\log Q}{\log g}},$$

ce qui termine la preuve du lemme. □

Lemme 11.11. *Soit $\alpha \geqslant 1$ vérifiant*

$$\mathcal{K}_\alpha < g^{-\frac{1}{2}}. \tag{11.23}$$

Pour tout $\epsilon > 0$, il existe une constante $c_8 > 0$ ne dépendant que de g, de α et de ϵ telle qu'uniformément pour $\mu > 0$ et Q assez grands, nous avons

$$\sum_{\substack{q<Q\\(q,g)=1}}\sum_{0<l<q} |\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha \ll_{g,\alpha,\epsilon} Qe^{-c_8\sqrt{\mu}} + Q^2(\mathcal{K}_\alpha+\epsilon)^\mu. \tag{11.24}$$

Démonstration. Remarquons que pour tout $\epsilon > 0$ assez petit, nous avons

$$2 + 2\frac{\log(\mathcal{K}_\alpha+\epsilon)}{\log g} \leqslant 1-\epsilon. \tag{11.25}$$

En effet, la condition (11.25) varie continûment avec ϵ et notre hypothèse (11.23) assure que c'est une inégalité stricte lorsque $\epsilon = 0$. Sans perte de généralité, nous pouvons supposer que $\epsilon > 0$ réalise la condition (11.25).

Dans la somme du lemme, nous rendons les fractions irréductibles en isolant leur plus grand facteur commun d. Donc

$$\begin{aligned}\sum_{\substack{q<Q\\(q,g)=1}}\sum_{0<l<q} |\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha &\leqslant \sum_{d<Q}\sum_{\substack{q<\frac{Q}{d}\\(q,g)=1}}\sum_{(l,q)=1} \big|\mathcal{G}_\mu(\tfrac{l}{q})\big|^\alpha\\ &\leqslant \Big(\sum_{d<D} + \sum_{D\leqslant d<Q}\Big)\mathscr{S}_\mu^\alpha(\tfrac{Q}{d}),\end{aligned}$$

où D est un paramètre à notre disposition.

Soit c_6 une constante admissible pour le corollaire 11.2. Nous choisissons

$$c_7 \ := \ \sqrt{\frac{\alpha c_6}{2+\epsilon}} \qquad \text{et} \qquad c_8 \ := \ \epsilon c_7 \tag{11.26}$$

qui ne dépendent donc que de g, de α et de ϵ. Nous prenons enfin

$$D \ := \ gQ \exp\big(-c_7\sqrt{\mu}\big). \tag{11.27}$$

Lorsque $d \geqslant D$, alors $\frac{Q}{d}$ est *petit* et nous utilisons le lemme 11.9 pour estimer $\mathscr{S}_\mu^\alpha(\frac{Q}{d})$. Lorsque $d < D$, alors $\frac{Q}{d}$ est *grand* et nous estimons $\mathscr{S}_\mu^\alpha(\frac{Q}{d})$ à l'aide du lemme 11.10. Ainsi,

$$\begin{aligned}\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha \ &\ll_{g,\alpha} \ \sum_{d<D} \Big(\frac{Q}{d}\Big)^{2+2\frac{\log(\mathcal{K}_\alpha+\epsilon)}{\log g}} \\ &\qquad + \sum_{d<D} \Big(\frac{Q}{d}\Big)^2 (\mathcal{K}_\alpha+\epsilon)^\mu + \sum_{D\leqslant d<Q} e^{-(\frac{\alpha c_6}{c_7}-2c_7)\sqrt{\mu}}.\end{aligned}$$

Notre condition (11.25) sur le choix de $\epsilon > 0$ fournit donc

$$\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha \ \ll_{g,\alpha} \ \sum_{d<D} \Big(\frac{Q}{d}\Big)^{1-\epsilon} + \sum_{d\geqslant 1} \Big(\frac{Q}{d}\Big)^2 (\mathcal{K}_\alpha+\epsilon)^\mu + \sum_{d<Q} \mathrm{e}^{-(\frac{\alpha c_6}{c_7}-2c_7)\sqrt{\mu}}$$

et en calculant la somme de ces séries, nous obtenons

$$\begin{aligned}\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha \ &\ll_{g,\alpha} \ Q\Big(\frac{Q}{D}\Big)^{-\epsilon} + Q^2(\mathcal{K}_\alpha+\epsilon)^\mu + Q\,\mathrm{e}^{-(\frac{\alpha c_6}{c_7}-2c_7)\sqrt{\mu}} \\ &\ll_{g,\alpha} \ Qe^{-\epsilon c_7\sqrt{\mu}} + Q^2(\mathcal{K}_\alpha+\epsilon)^\mu + Q\,\mathrm{e}^{-(\frac{\alpha c_6}{c_7}-2c_7)\sqrt{\mu}},\end{aligned}$$

ce qui démontre le lemme puisque $c_8 := \epsilon c_7 = \frac{\alpha c_6}{c_7} - 2c_7$ grâce à notre choix du paramètre c_7. □

Lemme 11.12. *Soit $m \geqslant 3$ un entier tel que*

$$\mathcal{K}_{m/3} \ < \ g^{-\frac{1}{2}}. \tag{11.28}$$

Notons β l'exposant défini par

$$\beta \ := \ -\frac{\log \mathcal{K}_{m/3}}{2m\log g} \ > \ \frac{1}{4m}. \tag{11.29}$$

Pour tout $\epsilon > 0$, il existe une constante $c_9 > 0$ ne dépendant que de g, de m et de ϵ telle qu'uniformément pour N et $Q \leqslant g^{(\beta-\epsilon)N}$ assez grands, nous avons

$$\sum_{\substack{\frac{1}{2}Q\leqslant q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}} \Big|\#\mathscr{Q}_N(g^N,a,q) - \frac{\#\mathscr{Q}_N}{q}\Big| \ \ll_{g,m,\epsilon} \ \#\mathscr{Q}_N\,\mathrm{e}^{-c_9\sqrt{N}}.$$

Démonstration. L'équation (11.5) que nous avons déjà utilisée pour démontrer le lemme 11.3 permet d'écrire

$$\sum_{\substack{\frac{1}{2}Q\leqslant q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}}\Big|\#\mathscr{Q}_N(g^N,a,q)-\frac{\#\mathscr{Q}_N}{q}\Big| \;\leqslant\; \#\mathscr{Q}_N \sum_{\substack{\frac{1}{2}Q\leqslant q<Q\\(q,g^3-g)=1}} \frac{1}{q}\sum_{0<l<q}|G_N(\tfrac{l}{q})|$$
$$\leqslant\; \frac{2\#\mathscr{Q}_N}{Q} \sum_{\substack{q<Q\\(q,g^3-g)=1}}\sum_{0<l<q}|G_N(\tfrac{l}{q})|.$$

Pour chaque q, nous utilisons le lemme 10.3 avec l'ensemble

$$\mathfrak{R} := \{\frac{l}{q},\ 0<l<q\}$$

qui est invariant modulo 1 par les multiplications par g et par g^2-1 puisque q est premier avec $g^3-g=g(g^2-1)$. Donc

$$\sum_{\substack{\frac{1}{2}Q\leqslant q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}}\Big|\#\mathscr{Q}_N(g^N,a,q)-\frac{\#\mathscr{Q}_N}{q}\Big| \;\leqslant\; \frac{2\#\mathscr{Q}_N}{Q} \sum_{\substack{q<Q\\(q,g^3-g)=1}}\sum_{0<l<q}|\mathcal{G}_\mu(\tfrac{l}{q})|^\alpha$$

en ayant noté $\alpha := \frac{m}{3}$ et $\mu := \frac{N-1}{2m}$. Nous avons $\alpha \geqslant 1$ puisque $m \geqslant 2$ et notre hypothèse (11.28) permet donc d'appliquer la majoration du lemme 11.11.

Si $\epsilon > 0$ est assez petit, la définition de β permet d'écrire

$$\beta - \epsilon + \frac{\log(\mathcal{K}_{m/3}+\epsilon^2)}{2m\log g} \;=\; -\epsilon + O_{g,m}(\epsilon^2) \;<\; 0. \tag{11.30}$$

Sans perte de généralité, nous pouvons supposer que $\epsilon > 0$ est assez petit pour vérifier (11.30).

Le lemme 11.11 permet donc de trouver une constante $c_8 > 0$ telle que

$$\sum_{\substack{\frac{1}{2}Q\leqslant q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}}\Big|\#\mathscr{Q}_N(g^N,a,q)-\frac{\#\mathscr{Q}_N}{q}\Big| \;\ll_{g,m,\epsilon}\; \#\mathscr{Q}_N\Big(e^{-c_8\sqrt{\mu}}+Q(\mathcal{K}_\alpha+\epsilon^2)^\mu\Big),$$

ce qui démontre la majoration du lemme avec

$$c_9 \;:=\; c_8 m^{-\frac{1}{2}} \tag{11.31}$$

puisque

$$Q(\mathcal{K}_\alpha+\epsilon^2)^\mu \;\ll_g\; g^{\left(\beta-\epsilon+\frac{\log(\mathcal{K}_\alpha+\epsilon^2)}{2m\log g}\right)N}$$

et l'exposant est strictement négatif grâce à notre hypothèse (11.30). □

Corollaire 11.3. *Soient c_3 une constante admissible pour le lemme 10.2 et*

$$\alpha \;:=\; \frac{\pi g}{c_3(1-g^{-\frac{1}{2}})^2}. \tag{11.32}$$

Alors tout entier m supérieur à 3α vérifie l'hypothèse (11.28). En particulier, lorsque g tend vers l'infini, un exposant de distribution admissible pour le théorème 9.2 est

$$\beta \;=\; \frac{1+o(1)}{12\pi g}.$$

Démonstration. L'application $\alpha \mapsto \mathcal{K}_\alpha$ étant clairement décroissante, il suffit de montrer que le réel α défini par (11.32) vérifie l'hypothèse (11.23) pour en déduire que tout entier $m \geqslant 2\alpha$ vérifie (11.28) (comme $c_3 < 4$ et $g \geqslant 2$, nous avons bien $\alpha \geqslant 1$). Ceci est immédiat en utilisant les lemmes 11.4 et 11.5 et le corollaire est donc démontré. □

Dans le chapitre 13, nous améliorerons les résultats obtenus de ce chapitre.

Chapitre 12

Preuve des Théorèmes

12.1 Cardinal de $\mathscr{Q}_N(x)$ et de $\mathscr{Q}_N(x,a,q)$

Lemme 12.1. *Soit N un entier. Pour tout pseudopalindrome x de taille N s'écrivant*

$$x \;=\; \sum_{k<N} x_k g^k \qquad \textit{avec} \qquad x_{N-1-k} = x_k,$$

nous avons

$$\#\mathscr{Q}_N(x) \;=\; \sum_{k<\frac{N+1}{2}} x_k \#\mathscr{Q}_{N-2k} \tag{12.1}$$

et pour tout entier q premier avec g nous avons la majoration

$$\max_{a\in\mathbb{Z}} \Big|\#\mathscr{Q}_N(x,a,q) - \frac{\#\mathscr{Q}_N(x)}{q}\Big| \;\leqslant\; \sum_{k<\frac{N+1}{2}} x_k \#\mathscr{Q}_{N-2k}\mathscr{R}_{N-2k}(q) \tag{12.2}$$

en ayant noté

$$\mathscr{R}_N(q) \;:=\; \frac{1}{q}\sum_{0<l<q} \Big|G_N\Big(\frac{l}{q}\Big)\Big|.$$

Démonstration. Décomposons $N = 2M+\delta$ avec $\delta = 0$ ou 1 de même parité que N et traitons en détail le cas légèrement plus technique correspondant à $\delta = 1$. Pour tout $0 \leqslant k \leqslant M$, nous notons

$$X_k \;:=\; \sum_{j<k} x_j \Phi_{N-1}(j)$$
$$\tilde{X}_k \;:=\; x_M g^{M-k} + \sum_{k\leqslant j<M} x_j \Phi_{N-1-2k}(j-k)$$

de sorte que $x = X_k + g^k \tilde{X}_k$ pour tout k : X_k est le *bord* du pseudopalindrome x obtenu en remplaçant par des 0 les chiffres centraux ; $\tilde{X}_k$ est le *milieu* du pseudopalindrome x). Avec ces notations, montrons la partition

$$\mathscr{Q}_N(x) \;=\; \bigsqcup_{k<M+\delta} \Big(X_k + g^k \mathscr{Q}_{N-2k}(x_k g^{N-1-2k})\Big), \tag{12.3}$$

l'union étant disjointe.

Soit n un pseudopalindrome de N chiffres que nous décomposons en

$$n \ := \ n_{N-1}\Phi_{N-1}(0) + g\tilde{n},$$

$\tilde{n}$ étant un pseudopalindrome à $N-2$ chiffres. Alors n est inférieur à x si et seulement si

$$\text{ou} \begin{cases} n_{N-1} < x_0 \text{ et } \tilde{n} \text{ est quelconque} \\ n_0 = x_0 \text{ et } \tilde{n} \text{ est inférieur à } \frac{1}{g}(x - X_0) \end{cases}$$

si et seulement si

$$\text{ou} \begin{cases} n \in X_0 + g^0 \mathscr{Q}_N(x_0 g^{N-1}) \\ n_0 = x_0 \text{ et } \tilde{n} \text{ est inférieur au pseudopalindrome } \tilde{X}_1. \end{cases}$$

Par récurrence décroissante, nous obtenons exactement la formule (12.3) à la $M + \delta^{\text{ème}}$ étape. Nous en déduisons en particulier la formule (12.1) en calculant le cardinal de l'égalité (12.3).

Pour évaluer le nombre de pseudopalindromes divisibles par q, nous introduisons des somme d'exponentielles, exactement comme nous l'avons déjà fait dans les démonstrations des lemmes 11.3 et 11.12 :

$$\begin{aligned} \#\mathscr{Q}_N(x,a,q) \ &= \ \sum_{n\in\mathscr{Q}_N(x)} \frac{1}{q}\sum_{l<q} \mathrm{e}\Big(l\frac{n-a}{q}\Big) \\ &= \ \frac{1}{q}\sum_{l<q} \mathrm{e}\Big(-\frac{al}{q}\Big) \sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\Big(\frac{nl}{q}\Big). \end{aligned} \tag{12.4}$$

Nous isolons le terme $l = 0$ qui fournit la partie principale :

$$\#\mathscr{Q}_N(x,a,q) \ = \ \frac{\#\mathscr{Q}_N(x)}{q} + \frac{1}{q}\sum_{0<l<q} \mathrm{e}\Big(-\frac{al}{q}\Big) \sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\Big(\frac{nl}{q}\Big).$$

La décomposition (12.3) permet donc d'écrire pour tout entier a

$$\begin{aligned} \Big|\#\mathscr{Q}_N(x,a,q) - \frac{\#\mathscr{Q}_N(x)}{q}\Big| & \\ &\leqslant \ \frac{1}{q}\sum_{0<l<q}\sum_{k<M+\delta} \Big|\sum_{n\in\mathscr{Q}_N(x_k g^{N-1-2k})} \mathrm{e}\Big((X_k + g^k n)\frac{l}{q}\Big)\Big| \\ &\leqslant \ \frac{1}{q}\sum_{0<l<q}\sum_{k<M+\delta} x_k\Big|\sum_{n\in\mathscr{Q}_{N-2k}} \mathrm{e}\Big(g^k n\frac{l}{q}\Big)\Big| \\ &\leqslant \ \sum_{k<M+\delta}\frac{1}{q}\sum_{0<l<q} x_k \#\mathscr{Q}_{N-2k}\Big|G_{N-2k}\Big(\frac{g^k l}{q}\Big)\Big| \end{aligned} \tag{12.5}$$

par définition de G_{N-2k}. Par hypothèse, q est premier avec g, donc la multiplication par g^k est une bijection de $(\mathbb{Z}/q\mathbb{Z})\backslash\{0\}$. Le changement de variable $\tilde{l} = g^k l$ fournit donc

$$\Big|\#\mathscr{Q}_N(x,a,q) - \frac{\#\mathscr{Q}_N(x)}{q}\Big| \ \leqslant \ \sum_{k<M+\delta} x_k \#\mathscr{Q}_{N-2k}\frac{1}{q}\sum_{0<\tilde{l}<q}\Big|G_{N-2k}\Big(\frac{\tilde{l}}{q}\Big)\Big|$$

ce qui termine la preuve du lemme. □

Corollaire 12.1. *Soit N un entier. Pour tout nombre réel x, pour tout $\tilde{N} \leqslant \frac{1}{2}N$ et pour tout ensemble d'entiers $\mathcal{Q}$ dont chaque élément est premier avec g, nous avons*

$$\sum_{q\in\mathcal{Q}} \sup_{y\leqslant x} \max_{a\in\mathbb{Z}} \Big|\#\mathscr{Q}_N(y,a,q) - \frac{\#\mathscr{Q}_N(y)}{q}\Big| \\ \ll_g \ \#\mathscr{Q}_N(x) g^{-\tilde{N}} \#\mathcal{Q} + \#\mathscr{Q}_N(x) \sup_{\substack{N-2\tilde{N}\leqslant M\leqslant N \\ M\equiv N \mod 2}} \{\mathscr{R}_M(\mathcal{Q})\} \tag{12.6}$$

en ayant noté

$$\mathscr{R}_N(\mathcal{Q}) \ := \ \sum_{q\in\mathscr{Q}} \frac{1}{q} \sum_{0<l<q} \Big|G_N\Big(\frac{l}{q}\Big)\Big|.$$

Démonstration. Soit $y \leqslant x$. Quitte à remplacer y par le plus petit pseudopalindrome supérieur à y, nous pouvons supposer que y est un pseudopalindrome. Distinguons la méthode utilisée suivant la taille de y.

Si $y \geqslant g^N$, alors $\mathscr{Q}_N(y,a,q) = \mathscr{Q}_N(g^N,a,q)$ puisque g^N-1 est le plus grand pseudopalindrome de N chiffres.

Si $y < g^N$, nous notons k l'entier minimal tel que y possède au moins $N-2k$ chiffres. Alors $\mathscr{Q}_N(y) = g^k \mathscr{Q}_{N-2k}(y/g^{2k})$. Les éléments de $\mathcal{Q}$ étant premiers avec g, nous avons

$$\#\mathscr{Q}_N(y,a,q) \ = \ \#\mathscr{Q}_{N-2k}(y/g^{2k},a',q),$$

a' étant défini par $g^k a' \equiv a \mod q$. Le résultat se déduit donc de l'estimation obtenue pour $N-2k$.

Pour chaque entier $q \in \mathcal{Q}$, nous pouvons donc utiliser la majoration du lemme 12.1. D'où, pour tout $y \leqslant x$,

$$\max_{a\in\mathbb{Z}} \Big|\#\mathscr{Q}_N(y,a,q) - \frac{\#\mathscr{Q}_N(y)}{q}\Big| \ \ll_g \ \sum_{k<\frac{N+1}{2}} \#\mathscr{Q}_N g^{-k} \mathscr{R}_{N-2k}(q).$$

En sommant sur les entiers q de $\mathcal{Q}$, nous obtenons

$$\sum_{q\in\mathcal{Q}} \sup_{y\leqslant x} \max_{a\in\mathbb{Z}} \Big|\#\mathscr{Q}_N(y,a,q) - \frac{\#\mathscr{Q}_N(y)}{q}\Big| \ \ll_g \ \sum_{k<\frac{N+1}{2}} \#\mathscr{Q}_N g^{-k} \mathscr{R}_{N-2k}(\mathcal{Q}).$$

Lorsque $k \geqslant \tilde{N}$, nous utilisons la majoration triviale $|\mathscr{R}_{N-2k}| \leqslant \#\mathcal{Q}$. Ainsi,

$$\sum_{q\in\mathscr{Q}} \sup_{y\leqslant x} \max_{a\in\mathbb{Z}} \Big|\#\mathscr{Q}_N(x,a,q) - \frac{\#\mathscr{Q}_N(x)}{q}\Big| \\ \ll_g \ \#\mathscr{Q}_N \sum_{k>\tilde{N}} g^{-k} \#\mathcal{Q} + \#\mathscr{Q}_N \sum_{k\leqslant\tilde{N}} g^{-k} \sup_{\substack{N-2\tilde{N}\leqslant M\leqslant N \\ M\equiv N \mod 2}} \{\mathscr{R}_M(\mathcal{Q})\}.$$

Mais x possède N chiffres par hypothèse, ce qui implique $\#\mathscr{Q}_N \leqslant g\#\mathscr{Q}_N(x)$ et termine la démonstration. □

12.2 Termes d'erreurs de $\mathscr{R}(x,a,q)$ et $\mathscr{Q}(x,a,q)$

Lemme 12.2. *Si q est un entier premier avec g, alors pour tout x nous avons la majoration*

$$\sup_{y\leqslant x}\max_{a\in\mathbb{Z}}\Big|\#\mathscr{R}(y,a,q)-\frac{\#\mathscr{R}(y)}{q}\Big| \;\leqslant\; 2\sup_{y\leqslant x}\max_{a\in\mathbb{Z}}\Big|\#\mathscr{Q}(y,a,q)-\frac{\#\mathscr{Q}(y)}{q}\Big|.$$

Démonstration. Un palindrome étant un pseudopalindrome ne se finissant pas par 0, nous avons

$$\mathscr{R} \;=\; \mathscr{Q}\backslash g\mathscr{Q}. \tag{12.7}$$

Donc

$$\#\mathscr{R}(y) \;=\; \#\mathscr{Q}(y)-\#\mathscr{Q}(y/g)$$

et en notant a' un entier tel que $ga'\equiv a \mod q$,

$$\#\mathscr{R}(y,a,q) \;=\; \#\mathscr{Q}(y,a,q)-\#\mathscr{Q}(y/g,a',q).$$

Si $y\leqslant x$, nous avons donc

$$\begin{aligned}\Big|\#\mathscr{R}(y,a,q)-\frac{\#\mathscr{R}(y)}{q}\Big| &\\ &\leqslant \Big|\#\mathscr{Q}(y,a,q)-\frac{\#\mathscr{Q}(y)}{q}\Big|+\Big|\#\mathscr{Q}(y/g,a',q)-\frac{\#\mathscr{Q}(y/g)}{q}\Big|\\ &\leqslant 2\sup_{z\leqslant x}\max_{b\in\mathbb{Z}}\Big|\#\mathscr{Q}(z,b,q)-\frac{\#\mathscr{Q}(z)}{q}\Big|.\end{aligned}$$

En prenant la borne supérieure en a puis en y, nous trouvons exactement la majoration du lemme. □

12.3 Preuve du Théorème 9.1

Il suffit de réunir les résultats du corollaire 12.1 et du lemme 11.3 puisque

$$\mathscr{Q}(x) \;=\; \bigsqcup_{M\leqslant N}\mathscr{Q}_M(x) \qquad \text{où} \qquad N \;>\; \frac{\log x}{\log g}.$$

Cela démontre donc le Théorème 9.1 pour $\mathscr{Q}$. Le lemme 12.2 finit la démonstration.

12.4 Preuve du Théorème 9.2

Il suffit de réunir les résultats du corollaire 12.1 et du lemme 11.12 puisque

$$\mathscr{Q}(x) \;=\; \bigsqcup_{M\leqslant N}\mathscr{Q}_M(x) \qquad \text{où} \qquad N \;>\; \frac{\log x}{\log g}.$$

Cela démontre donc la première partie du Théorème 9.2 pour $\mathscr{Q}$. Le lemme 12.2 finit la démonstration de (9.7), c'est-à-dire l'existence d'un exposant β. En utilisant les lemmes 11.4 et 11.5, nous vérifions que l'entier $m := \frac{1}{4\beta_g}$ vérifie l'hypothèse (11.28) du lemme 11.12 où β_g est donné par

g	2	3	4	5	6	7	8	9	10
β_g	$\frac{1}{68}$	$\frac{1}{180}$	$\frac{1}{144}$	$\frac{1}{236}$	$\frac{1}{220}$	$\frac{1}{308}$	$\frac{1}{288}$	$\frac{1}{380}$	$\frac{1}{368}$

Donc β_g est un exposant de distribution. L'exposant $\beta \sim \frac{1}{6\pi g}$ et les autres exposants β_g du Théorème 9.2 seront obtenu dans le corollaire 13.1.

Pour prouver que la fraction β_g donnée par le tableau convient, il suffit donc juste de vérifier que si nous posons $m := \frac{1}{4\beta_g}$, alors $m \geqslant 3$ est un entier qui réalise la condition (11.28). Faisons le par exemple en détail pour $g = 10$. Pour cela, nous utilisons le lemme 11.4 et l'équation (3.35) plus précise que le lemme 11.5 pour majorer $\mathcal{K}_{\frac{m}{3}}$. Ainsi,

$$\mathcal{K}_{\frac{m}{3}} \leqslant \mathcal{M}_{\frac{m}{3}} \leqslant \frac{1}{g} \sum_{-\frac{g}{2} \leqslant h \leqslant \frac{g}{2}} \left(1 - \frac{h^2}{g^2}\right)^{\frac{m}{3}} < 0.31622 < 10^{-\frac{1}{2}}.$$

Nous pouvons donc choisir

$$\beta := -\frac{\log \mathcal{K}_{m/3}}{2m \log g} > -\frac{\log 0.31622}{2 \cdot 46 \log 10} > 0.0027174,$$

ce qui démontre le corollaire pour $g = 10$.

Si g est quelconque, nous utilisons directement la majoration du lemme 11.5 pour majorer $\mathcal{K}_{\frac{m}{3}}$. Nous devons donc trouver un entier $m \geqslant 3$ tel que

$$\frac{1}{g} + \sqrt{\frac{3\pi}{mc_3}} \leqslant \sqrt{\frac{1}{g}} \qquad i.e. \qquad m \geqslant \frac{3\pi g}{c_3}(1 - g^{-\frac{1}{2}})^{-2}$$

et nous pouvons alors choisir l'exposant $\beta = \frac{1}{4m}$. Le choix du plus petit entier supérieur à $\frac{3\pi g}{c_3}(1 - g^{-\frac{1}{2}})^{-2}$ pour m termine donc la preuve.

12.5 Préparation au crible

Nous établissons dans ce paragraphe une variante du Théorème 9.2 plus adaptée aux méthodes de cribles : le lemme 12.6. Nous avons besoin d'étudier la répartition des palindromes ayant des facteurs en commun avec

$$g^3 - g = (g-1)g(g+1).$$

Comme nous le verrons, les diviseurs impairs de $g^2 - 1$ ne sont pas un vrai problème (quitte à distinguer l'étude de $\mathscr{R}^0$ et celle de $\mathscr{R}^1$), mais il en va tout autrement des diviseurs de $2g$: par exemple, si $q_g \mid g$, quand le premier chiffre x_0 de x n'est pas un multiple de q_g, il n'y a aucun pseudopalindrome divisible par q_g ayant x_0 pour premier chiffre.

Plutôt que d'étudier de nombreux cas différents, nous simplifions le résultat en remplaçant l'étude des palindromes par celle de $\tilde{\mathscr{R}}$, défini dans le lemme 12.4.

Lemme 12.3. *Supposons g impair. Tout élément de $\mathscr{R}^0$ est pair. Tout élément de $\mathscr{R}^1$ est de même parité que son chiffre médian.*

Démonstration. Montrons que $\Phi_N(j)$ est pair pour tout $j \leqslant N$:

$$\Phi_N(j) \ \equiv \ 1^j + 1^{N-j} \ \equiv \ 0 \mod 2.$$

Le lemme s'en déduit immédiatement. □

Lemme 12.4. *Posons*

$$\begin{aligned} \tilde{\mathscr{R}}^0 \ &:= \ \{n \in \mathscr{R}^0, \ (n,g)=1\}, \\ \tilde{\mathscr{R}}^1 \ &:= \ \{n \in \mathscr{R}^1, \ (n,2g)=1\}, \\ \tilde{\mathscr{R}} \ &:= \ \mathscr{R}^0 \cup \mathscr{R}^1. \end{aligned}$$

Alors

$$\#\tilde{\mathscr{R}}^0(x) \ \gg_g \ \#\mathscr{R}(x) \qquad et \qquad \#\tilde{\mathscr{R}}^1(x) \ \gg_g \ \#\mathscr{R}(x).$$

Démonstration. En utilisant la décomposition (9.1), il suffit de prouver qu'uniformément sur N, nous avons

$$\#\tilde{\mathscr{R}}_N \ \gg_g \frac{\phi(g)}{g}\#\mathscr{R}_N, \tag{12.8}$$

en ayant noté $\tilde{\mathscr{R}}_N$ les éléments de $\tilde{\mathscr{R}}$ dont l'écriture dans la base g possède exactement N chiffres.

Supposons N pair. Soit $n \in \mathscr{R}_N$ que nous décomposons en

$$n \ = \ n_0\Phi_{N-1}(0) + g\tilde{n}, \qquad \text{avec } \tilde{n} \in \mathscr{Q}_{N-2}.$$

Alors

$$(n,g)=1 \qquad \Longleftrightarrow \qquad (n_0,g)=1.$$

Il existe donc exactement $\phi(g)$ choix possibles pour n_0 et les autres chiffres de n peuvent être choisis arbitrairement, ce qui prouve (12.8).

Supposons N impair et notons $M := \frac{N-1}{2}$. Soit $n \in \mathscr{R}_N$ que nous décomposons en

$$n \ = \ n_0\Phi_{N-1}(0) + g\tilde{n} + n_M g^M,$$

où $\tilde{n}$ est un élément de $\mathscr{Q}_{N-2}$ dont le chiffre médian est 0. En utilisant le lemme 12.3, nous avons alors

$$(n,2g)=1 \qquad \Longleftrightarrow \qquad (n_0,g)=1 \text{ et } (n_M,2)=1.$$

Il existe donc exactement $\phi(g)$ choix possibles pour n_0, $\left\lceil \frac{g-1}{2} \right\rceil$ choix pour n_M et les autres chiffres de n peuvent être choisis arbitrairement, ce qui prouve (12.8). □

Lemme 12.5. *Soit $r = \frac{l}{q}$ une fraction irréductible telle que q possède un facteur commun $q_1 \geqslant 3$ avec $g-1$. Pour tout entier $j \leqslant N$,*

$$\|\Phi_N(j)r\| \ \geqslant \ \frac{1}{q}.$$

Soit $r = \frac{l}{q}$ une fraction irréductible telle que q possède un facteur commun $q_1 \geqslant 3$ avec $g+1$. Si N est pair, pour tout entier $j \leqslant N$,

$$\|\phi_N^+(j)r\| \ \geqslant \ \frac{1}{q}.$$

Démonstration. Pour la première minoration, réduisons $\phi_N^+(j)$ modulo $g-1$:

$$\Phi_N(j) \ \equiv \ 1^j + 1^{N-j} \ \equiv 2 \mod g-1.$$

Comme $q_1 \mid g-1$, nous avons donc

$$\Phi_N(j) \ \equiv \ 2 \mod q_1.$$

L'hypothèse $q_1 \geqslant 3$ assure donc $\Phi_N(j) \neq 0 \mod q_1$. Mais $q_1 \mid q$, donc $\Phi_N(j)r \notin \mathbb{Z}$ puisque $r = \frac{l}{q}$ est irréductible. La fraction $\Phi_N(j)r \notin \mathbb{Z}$ étant de dénominateur au plus q, nous avons bien $\|\Phi_N(j)r\| \geqslant \frac{1}{q}$.

Pour la seconde minoration, nous procédons exactement de la même façon après avoir remarqué que

$$\begin{aligned} \Phi_N(j) &\equiv (-1)^j + (-1)^{N-j} && \mod g+1 \\ &\equiv (-1)^j(1+(-1)^N) && \mod g+1 \\ &\equiv (-1)^j 2 && \mod g+1 \end{aligned}$$

puisque N est pair. □

Lemme 12.6. *Il existe deux fonctions multiplicatives ρ_0 et ρ_1 telles que*

$$\rho_0(p) \ = \ \begin{cases} 1 & si\ (p, g(g+1)) = 1 \\ 0 & si\ p \mid g \\ p & si\ p \mid g+1 \end{cases} \qquad et \qquad \rho_1(p) \ = \ \begin{cases} 1 & si\ (p,2g) = 1 \\ 0 & si\ p \mid 2g \end{cases}$$

et si β est l'exposant obtenu dans la preuve du Théorème 9.2, alors

$$\sum_{\substack{q<x^{\beta-\epsilon} \\ \mu^2(q)=1}} \left| \#\tilde{\mathscr{R}}^k(x,0,q) - \frac{\rho_k(q)}{q} \#\tilde{\mathscr{R}}^k(x) \right| \ \ll_{g,\beta,\epsilon,A} \ \frac{\#\tilde{\mathscr{R}}^k(x)}{\log^A x}. \tag{12.9}$$

Démonstration. Traitons le cas particulier légèrement plus technique où g est impair (si g est pair, la module 2 est exclu directement puisque nous avons remplacé l'étude de $\mathscr{R}$ par celle de $\tilde{\mathscr{R}}$) et où $k=0$ (si $k=1$, nous traitons les diviseurs de $g+1$ exactement

comme nous traitons ici ceux de $g-1$). Si q est un entier premier avec g et sans facteur carré, nous définissons q_0 et q' par

$$\begin{aligned} q &:= q_0 q', \\ q_0 \mid g^2-1, &\qquad (g^2-1, q') = 1, \end{aligned} \tag{12.10}$$

ces conditions déterminant q_0 et q' de façon unique. Nous décomposons ensuite q_0 en

$$\begin{aligned} q_0 &:= q_{g-1} q_{g+1}, \\ q_{g-1} \mid g-1, \qquad q_{g+1} \mid g+1, &\qquad (q_{g-1}, 2) = 1, \end{aligned} \tag{12.11}$$

ces conditions déterminant q_{g-1} et q_{g+1} de façon unique.

Tout d'abord, nous montrons que nous pouvons nous restreindre à l'étude des pseudopalindromes en adaptant la preuve du lemme 12.2. Comme

$$\tilde{\mathscr{R}}_N = \bigsqcup_{(d,g)=1} (d\Phi_{N-1}(0) + g\mathscr{Q}_{N-2}),$$

pour tout $y \in \tilde{\mathscr{R}}_N$ que nous décomposons en $y = y_0\Phi_{N-1}(0) + g\tilde{y}$ avec $\tilde{y} \in \mathscr{Q}_{N-2}$,

$$\#\tilde{\mathscr{R}}_N(y) = \sum_{\substack{(d,g)=1 \\ d<y_0}} \#\mathscr{Q}_{N-2} + \#\mathscr{Q}_{N-2}(\tilde{y})$$

et, en notant g' un inverse de g modulo q,

$$\begin{aligned} \#\tilde{\mathscr{R}}_N(y,a,q) = \sum_{\substack{(d,g)=1 \\ d<y_0}} &\#\mathscr{Q}_{N-2}(\infty, a - d\Phi_{N-1}(0)g', q) \\ &+ \#\mathscr{Q}_{N-2}(\tilde{y}, a - y_0\Phi_{N-1}(0)g', q). \end{aligned}$$

Comme dans la preuve du lemme 12.2, nous en déduisons

$$\begin{aligned} &\sup_{y\leqslant x} \max_{a\in\mathbb{Z}} \Big|\#\tilde{\mathscr{R}}_N(y,a,q) - \frac{\rho_0(q)}{q}\#\tilde{\mathscr{R}}_N(y)\Big| \\ &\qquad \leqslant \phi(g) \sup_{z\leqslant x} \max_{b\in\mathbb{Z}} \Big|\#\mathscr{Q}_{N-2}(z,b,q) - \frac{\rho_0(q)}{q}\#\mathscr{Q}_{N-2}(z)\Big|. \end{aligned} \tag{12.12}$$

Nous adaptons la preuve du lemme 12.1 en intégrant dans le terme général tous les diviseurs de $g+1$ puisque les lemmes 12.5 et 12.3 nous assurent qu'ils sont tous divisibles par q_{g+1} : le théorème chinois permet de remplacer l'équation (12.4) par

$$\begin{aligned} \#\mathscr{Q}_N(x,0,q) &= \frac{1}{q} \sum_{l_{g+1}<q_{g+1}} \sum_{l<q_{g-1}q'} \sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\Big(\frac{nl_{g+1}}{q_{g+1}} + \frac{nl}{q_{g-1}q'}\Big) \\ &= \frac{q_{g+1}}{q} \sum_{l<q_{g-1}q'} \sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\Big(\frac{nl}{q_{g-1}q'}\Big). \end{aligned}$$

En reprenant la démonstration du lemme 12.1, nous obtenons alors

$$\Big|\#\mathscr{Q}_N(x,0,q) - \frac{\rho_0(q)}{q}\#\mathscr{Q}_N(x)\Big| \leqslant \sum_{j<\frac{N+1}{2}} x_j \#\mathscr{Q}_{N-2j}\mathscr{R}_{N-2j}(q_{g-1}q') \tag{12.13}$$

avec les même notations que dans le lemme 12.1 :

$$\mathscr{R}_N(d) \ := \ \frac{1}{d}\sum_{0<l<d}\Big|G_N\Big(\frac{l}{d}\Big)\Big|.$$

Il nous suffit donc de montrer que les majorations obtenues pour $\mathscr{R}_N(q)$ lorsque q est un entier premier avec g^3-g, restent valables lorsque nous supposons seulement que q est premier avec g^2+g et sans facteur carré. Comme $(q_{g-1},q')=1$, le théorème chinois permet d'écrire

$$\begin{aligned}\mathscr{R}_N(q) \ &:= \ \frac{1}{q}\sum_{0<l_{g-1}<q_{g-1}}\Big|G_N\Big(\frac{l_{g-1}}{q_{g-1}}\Big)\Big|+\frac{1}{q}\sum_{l_{g-1}<q_{g-1}}\sum_{0<l'<q'}\Big|G_N\Big(\frac{l_{g-1}}{q_{g-1}}+\frac{l'}{q'}\Big)\Big|\\ &=: \ \mathscr{S}_{g-1}+\mathscr{S}',\end{aligned}$$

disons.

Commençons par majorer $\mathscr{S}'$, le terme correspondant à $l'\neq 0$. Nous utilisons le lemme 10.2 ce qui permet de faire disparaître la fraction $\frac{l_{g-1}}{q_{g-1}}$ puisque $q_0 \mid g^2-1$:

$$\Big|G_N\Big(\frac{l_{g-1}}{q_{g-1}}+\frac{l'}{q'}\Big)\Big| \ \leqslant \ \Big|\mathcal{G}_{\frac{N-1}{2}}\Big((g^2-1)(\frac{l_{g-1}}{q_{g-1}}+\frac{l'}{q'})\Big)\Big|^{\frac{1}{3}} \ = \ \Big|\mathcal{G}_{\frac{N-1}{2}}\Big((g^2-1)\frac{l'}{q'}\Big)\Big|^{\frac{1}{3}}.$$

Le changement de variable $l=(g^2-1)l'$ laisse invariant modulo q' l'ensemble $\{0<l'<q'\}$ puisque $(g^2-1,q')=1$. Donc

$$\mathscr{S}' \ \leqslant \ \frac{q_{g-1}}{q}\sum_{0<l'<q'}\Big|\mathcal{G}_{\frac{N-1}{2}}\Big((g^2-1)\frac{l'}{q'}\Big)\Big|^{\frac{1}{3}} \ = \ \frac{1}{q'}\sum_{0<l'<q'}\Big|\mathcal{G}_{\frac{N-1}{2}}\Big(\frac{l'}{q'}\Big)\Big|^{\frac{1}{3}}.$$

Nous pouvons utiliser maintenant les majorations du lemme 11.11 et terminer la majoration de $\mathscr{S}'$ comme nous avons prouvé le Théorème 9.2.

Comme q_{g-1} est impair, nous pouvons utiliser le lemme 12.5 pour évaluer $\mathscr{S}_{g-1}$. La factorisation (10.2) fournit pour $0<l_{g-1}<q_{g-1}$

$$\Big|G_N\Big(\frac{l_{g-1}}{q_{g-1}}\Big)\Big| \ \ll_g \ \Big(1-\frac{1}{q_{g-1}}\Big)^N,$$

ce qui est suffisant pour terminer la preuve du lemme. □

12.6 Preuve du Théorème 9.3

Démonstration du théorème 9.3. Commençons par nous souvenir que tout élément de $\mathscr{R}^0$ est divisible par $g+1$ donc n'aura aucune chance de vérifier le résultat du Théorème. Nous allons donc travailler uniquement avec les éléments de $\mathscr{R}^1$ et en réalité seulement avec ceux de $\tilde{\mathscr{R}}^1$ puisque les éléments de $\mathscr{R}^1\backslash\tilde{\mathscr{R}}^1$ sont exactement ceux possédant un facteur commun avec $2g$, donc en particulier, un petit facteur premier.

Soit $\epsilon>0$ fixé. Si z est assez grand (par exemple dès que $z>g+1$), alors

$$\begin{aligned}\#\{n\in\mathscr{R}(x),\ P^-(n)\geqslant z\} \ &= \ \#\{n\in\mathscr{R}^1(x),\ P^-(n)\geqslant z\}\\ &= \ \#\{n\in\tilde{\mathscr{R}}^1(x),\ P^-(n)\geqslant z\}.\end{aligned}$$

Nous appliquons le crible linéaire tel qu'énoncé dans le corollaire 7.1 avec la famille $\mathscr{A} := \tilde{\mathscr{R}}^1$, $X := \#\tilde{\mathscr{R}}^1$, $s := 2+\epsilon$, R assez grand, par exemple $R := 4\log_2(z)$. Ainsi, si z est assez grand,

$$\#\{n \in \mathscr{R}^1(x),\ P^-(n) \geqslant z\} \ \geqslant\ \#\tilde{\mathscr{R}}^1 \prod_{p<z}\Big(1-\frac{\rho_1(p)}{p}\Big) f(2+\epsilon)\Big(1+O\big(\log^{-\frac{1}{3}} z\big)\Big) \\ - \sum_{\substack{q<z^{2+\epsilon}\\ \mu^2(q)=1}} \Big|\#\tilde{\mathscr{R}}^1(x,0,q) - \frac{\rho_1(q)}{q}\#\tilde{\mathscr{R}}^1(x)\Big|$$

Le lemme 12.4 permet de remplacer dans le membre de gauche le facteur $\#\tilde{\mathscr{R}}^1(x)$ par $\#\mathscr{R}^1(x)$, la formule de Mertens permet de minorer le produit restant par $O_g\big(\log^{-1} z\big)$ et le lemme 12.6 de montrer que le terme d'erreur est négligeable puisque que

$$z^{2+\epsilon} \ <\ x^{(2+\epsilon)(\frac{1}{2}\beta-\epsilon)} \ <\ x^{\beta-\epsilon},$$

ce qui montre que

$$\#\{n \in \mathscr{R}(x),\ P^-(n) \geqslant z\} \ \asymp\ \frac{\#\mathscr{R}^1(x)}{\log z} \ \asymp\ \frac{\#\mathscr{R}(x)}{\log z}. \tag{12.14}$$

Le théorème 9.3 est donc prouvé. □

12.7 Optimalité de l'identité (9.6)

Nous pouvons nous demander s'il ne serait pas possible d'utiliser une autre identité que (9.6) dans laquelle les facteurs de $g-1$ ne sont pas artificiellement exclus. Nous allons démontrer que c'est effectivement impossible.

Soit $(P_j)_{j\leqslant J}$ une famille de polynômes telle qu'il existe un polynôme P vérifiant l'identité

$$\sum_{j\leqslant J} P_j(g)\Phi_N(k+j) \ =\ P(g)g^k.$$

En identifiant à gauche et à droite de l'égalité les coefficients dépendant de N et ceux n'en dépendant pas, nous devons donc avoir

$$\sum_{j\leqslant J} g^{J-j}P_j(g) \ =\ 0 \qquad \text{et} \qquad \sum_{j\leqslant J} g^j P_j(g) \ =\ P(g).$$

En calculant $P_J(g)$ à l'aide de la relation linéaire, nous avons

$$g^J P_J(g) \ =\ -\sum_{j<J} g^{2J-j}P_j(g).$$

En reportant cette estimation dans la seconde égalité, nous trouvons

$$\sum_{j<J}(g^j - g^{2J-j})P_j(g) \ =\ P(g). \tag{12.15}$$

Le membre de gauche de (12.15) s'annulant pour $g=1$ et $g=-1$, le polynôme $P(g)$ est divisible par g^2-1. La relation (9.6) est donc optimale.

12.8 Palindromes premiers et presque premiers : preuve des corollaires 9.1 et 9.2

Pour le corollaire 9.1, nous utilisons le théorème 9.3 avec (par exemple)

$$z \ := \ x^{\frac{\beta}{3}}.$$

Si $n < x$ est un nombre premier, alors n vérifie l'une des deux propriétés

$$n \ < \ z \qquad \text{ou} \qquad P^-(n) \ \geqslant \ z.$$

Nous donc avons la majoration

$$\begin{aligned} \#\{n \in \mathscr{R}(x),\ n \text{ premier}\} \ &\leqslant \ z + \#\{n \in \mathscr{R}(x),\ P^-(n) \geqslant z\} \\ &\ll_g \ z + \frac{\#\mathscr{R}(x)}{\log z}. \end{aligned}$$

z est absorbé par le second terme puisque $\frac{\beta}{3} < \frac{1}{2}$, donc

$$\#\{n \in \mathscr{R}(x),\ n \text{ premier}\} \ \ll_g \ \frac{\#\mathscr{R}(x)}{\log x},$$

ce qui termine la preuve du corollaire 9.1.

Pour le corollaire 9.2, il suffit de remarquer que les conditions $n < x$ et $P^-(n) \geqslant z$ impliquent la majoration $\Omega(n) < \frac{\log x}{\log z}$.

12.9 Palindromes friables : preuve du corollaire 9.3

Nous allons montrer un théorème plus précis que le corollaire 9.3 :

Théorème 12.1. *Soit $\beta \leqslant \frac{1}{2}$ un exposant de répartition pour les palindromes. Pour tout $\alpha > 1 - \beta$, il existe une proportion positive de palindromes x^α friables.*

Démonstration. Nous reprenons la même démonstration que celle faite pour la recherche d'entiers ellipséphiques friables. Soit $0 < \beta \leqslant \frac{1}{2}$ un exposant de répartition. Soit $\epsilon > 0$ assez petit et choisissons

$$\alpha \ := \ 1 - \beta + 2\epsilon \qquad \text{et} \qquad y \ := \ x^\alpha$$

Introduisons trois paramètres supplémentaires v, w et z définis par

$$w \ := \ x^{\beta-\epsilon}, \qquad v \ := \ x^{\beta-2\epsilon} \qquad \text{et} \qquad z \ := \ x^\epsilon.$$

Si $\epsilon > 0$ est assez petit, nous avons alors

$$z \ \geqslant \ x^\epsilon, \qquad v \ \geqslant \ z \log z, \qquad \frac{w}{v} \ \geqslant \ x^\epsilon, \qquad w \ \leqslant \ x^{\beta-\epsilon}$$

et comme $\beta \leqslant \frac{1}{2}$, nous avons aussi

$$y \ \geqslant \ w \qquad \text{et} \qquad y \ \geqslant \ \frac{x}{v}.$$

Nous avons alors

$$\Psi(x,y) \ \geqslant \ \#\left\{n \in \mathscr{R}(x) \ / \ \exists\, k|n,\, v < k \leqslant w,\, P^-(k) \geqslant z\right\}.$$

Nous utilisons de nouveau la fonction multiplicative $u_z(\cdot)$ définie par

$$u_z(k) \ := \ \begin{cases} 1 & \text{si } P^-(k) \geqslant z, \\ 0 & \text{sinon} \end{cases} \tag{12.16}$$

et $U_z(x)$ sa fonction sommatoire, comme dans (6.4) :

$$U_z(x) \ := \ \sum_{k<x} u_z(k).$$

Nous utilisons de nouveau la majoration (6.5) pour obtenir

$$\begin{aligned}
\Psi(x,y) \ &\geqslant \ \sum_{n\in\mathscr{R}(x)} 2^{-\frac{\log n}{\log z}} \sum_{\substack{v<k\leqslant w \\ k|n}} u_z(k) \\
&\geqslant \ 2^{-\frac{\log x}{\log z}} \sum_{v<k\leqslant w} u_z(k) \sum_{n\in\mathscr{R}(x,0,k)} 1 \\
&\geqslant \ 2^{-\frac{\log x}{\log z}} \sum_{v<k\leqslant w} \frac{u_z(k)}{k} \#\mathscr{R}(x) - 2^{-\frac{\log x}{\log z}} \sum_{v<k\leqslant w} u_z(k) \Big| \#\mathscr{R}(x,0,k) - \frac{\#\mathscr{R}(x)}{k} \Big|.
\end{aligned}$$

Si z est assez grand (dès que $z > \tilde{r} := r^3 - r$ par exemple), l'équation (6.7) fournit la minoration

$$\begin{aligned}
\Psi(x,y) \ \geqslant \ 2^{-\frac{\log x}{\log z}} \frac{1}{2} \frac{\log \frac{w}{v}}{\log z} \#W_{\mathscr{D}}(x) \Big(1 + O\big(\frac{1}{\log z} + \frac{1}{\log \frac{w}{v}}\big)\Big) \\
- 2^{-\frac{\log x}{\log z}} \sum_{\substack{k\leqslant w \\ (k,\tilde{r})=1}} \Big| \#\mathscr{R}(x,0,k) - \frac{\#\mathscr{R}(x)}{k} \Big|.
\end{aligned}$$

Comme $w \leqslant x^{\beta-\epsilon}$, la somme est évaluable à l'aide du théorème 9.2. Donc

$$\Psi(x,y) \ \gg_\epsilon \ \#\mathscr{R}(x),$$

ce qui termine la preuve. □

Chapitre 13

Amélioration de l'exposant de distribution : moyennes quadratiques de pseudopalindromes

Dans ce chapitre, nous améliorons l'exposant β trouvé au chapitre 12.4 en remarquant que le milieu d'un palindrome reste un palindrome. Nous introduisons un paramètre $0 < \eta < 1$ et nous posons alors $B(x)$ le produit des facteurs du bord de $G_N(x)$

$$B(x) \ := \prod_{k<(1-\eta)N} U(\Phi_{N-1}(k)x) \tag{13.1}$$

et $C(x)$ le produit des facteurs centraux de $G_N(x)$

$$C(x) \ := \prod_{(1-\eta)N\leqslant k\leqslant \frac{N}{2}} U(\Phi_{N-1}(k)x). \tag{13.2}$$

Lemme 13.1. *Soit c_3 une constante admissible pour le lemme 10.2. Pour tout entier m et tout réel $\eta \in [0,1]$, il existe un entier K tel que pour tout réel x,*

$$|G_N(x)| \ \leqslant \ |G_{\eta N}(g^K x)| \cdot |\mathcal{G}_{\frac{(1-\eta)N-1}{2}}((g^2-1)x)|^{\frac{1}{3}}$$

En particulier, si $\mathfrak{R}$ est un ensemble de points de $[0,1[$ sans répétition et stable par les multiplications par g^2-1 et g, alors

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \ \leqslant \ \Big(\sum_{r\in\mathfrak{R}} |G_{\eta N}(r)|^2 \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^{\frac{2m}{3}}\Big)^{\frac{1}{2}},$$

avec $\mu := \frac{(1-\eta)N-1}{2m}$.

Démonstration. Nous utilisons la factorisation (10.2) pour obtenir

$$|G_N(x)| \ \leqslant \ |C(x)|\,|B(x)|\,.$$

Nous majorons le terme du bord $B(x)$ de la même façon que dans le lemme 10.2. Ainsi

$$|B(x)| \leqslant \left|\mathcal{G}_{\frac{(1-\eta)N-1}{2}}\left((g^2-1)x\right)\right|^{\frac{1}{3}}.$$

Pour le facteurs $C(x)$, nous pouvons suivre la démarche inverse de la démonstration du lemme 10.1 et nous reconnaissons donc que

$$C(x) = G_{\eta N}(g^K x),$$

K étant le plus grand entier inférieur à $\frac{(1-\eta)N}{2}$, ce qui termine la démonstration de la majoration de G_N.

Pour prouver le second point, nous commençons par utiliser l'inéglité de Cauchy-Schwarz

$$\sum_{r\in\mathfrak{R}}|G_N(r)| \leqslant \Big(\sum_{r\in\mathfrak{R}}|G_{\eta N}(g^K r)|^2 \sum_{r\in\mathfrak{R}}|\mathcal{G}_{\frac{(1-\eta)N-1}{2}}\left((g^2-1)r\right)|^{\frac{2}{3}}\Big)^{\frac{1}{2}}.$$

Dans la première somme, nous effectuons le changement de variable $r' = g^K r$. Nous majorons la seconde somme en suivant exactement la même démarche que dans la preuve du lemme 10.3. □

Lemme 13.2. *Soit α un entier pair. Uniformément pour tout μ assez grand et pour tout ensemble $\mathfrak{R}$ de points de $[\frac{\delta}{2}, 1-\frac{\delta}{2}]$ qui est δ bien espacé et stable modulo 1 par la multiplication par g, nous avons*

$$\sum_{r\in\mathfrak{R}}|G_\mu(r)|^\alpha \ll_{g,\alpha,\epsilon} \delta^{-1}(K_\alpha+\epsilon)^\mu + \delta^{-1-\frac{\log(K_\alpha+\epsilon)}{\log g}}.$$

Pour $\alpha = 2$, nous avons la majoration

$$\sum_{r\in\mathfrak{R}}|G_\mu(r)|^2 \ll_g \delta^{-1}g^{-\frac{\mu}{2}} + \delta^{-\frac{1}{2}}.$$

Démonstration. Soit $\nu \leqslant \mu$ tel que $\lceil\nu\rceil$ et $\lceil\mu\rceil$ sont de même parité. Pour $K = \left\lfloor\frac{\mu-\nu}{2}\right\rfloor$ et pour tout réel x, nous avons

$$|G_\mu(x)| \leqslant \prod_{k<\frac{\mu}{2}} U(\Phi_{\mu-1}(k)x) \leqslant \prod_{K\leqslant k<\frac{\mu}{2}} U(\Phi_{\mu-1}(k)x) \leqslant |G_\nu(g^K x)|.$$

La multiplication par g laissant $\mathfrak{R}$ invariant, nous en déduisons la majoration

$$\sum_{r\in\mathfrak{R}}|G_\mu(r)|^\alpha \leqslant \sum_{r\in\mathfrak{R}}|G_\nu(r)|^\alpha. \tag{13.3}$$

Nous majorons cette somme exactement comme nous l'avons fait dans le lemme 11.10. Le lemme A.1 de Sobolev-Gallagher fournit donc la majoration

$$\sum_{r\in\mathfrak{R}}|G_\mu(r)|^\alpha \leqslant \delta^{-1}\|{G_\nu}^\alpha\|_1 + \|({G_\nu}^\alpha)'\|_1.$$

La même technique que celle déjà développée dans la preuve du lemme 11.10 donne alors

$$\sum_{r\in\mathfrak{R}} \big|G_\mu(r)\big|^\alpha \ \ll_{g,\alpha,\epsilon}\ \big(\delta^{-1}+g^\nu\big)(K_\alpha+\epsilon)^\nu,$$

par définition de K_α (la dérivée se majorant bien ainsi car α est un entier pair). Nous optimisons notre paramètre ν en choisissant

$$\nu \ := \ \min\Big\{\mu, -\frac{\log\delta}{\log g}\Big\} \qquad \text{ou} \qquad \min\Big\{\mu, -\frac{\log\delta}{\log g}\Big\}-1$$

pour avoir $\lceil\nu\rceil$ et $\lceil\mu\rceil$ de même parité. Ainsi,

$$\sum_{r\in\mathfrak{R}} \big|G_\mu(r)\big|^\alpha \ \ll_{g,\alpha,\epsilon}\ \delta^{-1}(K_\alpha+\epsilon)^\mu+\delta^{-1}(K_\alpha+\epsilon)^{-\frac{\log\delta}{\log g}},$$

ce qui termine la preuve de la première majoration. Le cas $\alpha=2$ s'en déduit immédiatement puisqu'il est clair que

$$\big\|{G_\mu}^2\big\|_1 \ \ll_g\ g^{-\frac{\mu}{2}} \qquad \text{et} \qquad \big\|({G_\mu}^2)'\big\|_1 \ \ll_g\ g^{\frac{\mu}{2}}.$$

La majoration est donc vraie pour $\epsilon=0$ avec $K_2=g^{-\frac{1}{2}}$. □

Lemme 13.3. *Soient $m\geqslant 2$ un entier et $\epsilon>0$. Uniformément pour tout N assez grand et pour tout ensemble $\mathfrak{R}$ de points de $\big[\frac{\delta}{2},1-\frac{\delta}{2}\big]$ vérifiant l'hypothèse (H_δ), nous avons la majoration*

$$\sum_{r\in\mathfrak{R}} \big|G_N(r)\big| \ \ll_{g,m,\epsilon}\ \big(\delta^{-\frac{1}{2}}g^{-\frac{N}{8m+4}}+\delta^{-\frac{1}{4}}\big)\delta^{-\frac{1}{2}}\big(\mathcal{K}_\alpha+\epsilon\big)^{\frac{N}{4m+2}}, \tag{13.4}$$

en ayant noté $\alpha:=\frac{2m}{3}$.

Démonstration. En réunissant les majorations des lemmes 13.1 et 13.2, nous obtenons pour tout choix de $\eta\in[0,1]$ et tout entier $m\geqslant 2$,

$$\sum_{r\in\mathfrak{R}} \big|G_N(r)\big| \ \ll_{g,m,\epsilon}\ \Big(\delta^{-\frac{1}{2}}g^{-\frac{\eta N}{4}}+\delta^{-\frac{1}{4}}\Big)\Big(\delta^{-\frac{1}{2}}\big(\mathcal{K}_\alpha+\epsilon\big)^{\frac{\mu}{2}}+\delta^{-\frac{1}{2}-\frac{\log(\mathcal{K}_\alpha+\epsilon)}{2\log g}}\Big)$$

en ayant noté

$$\alpha \ := \ \tfrac{2m}{3} \qquad \text{et} \qquad \mu:=\tfrac{1-\eta}{2m}N. \tag{13.5}$$

Comme $m\geqslant 2$, nous avons bien $\alpha\geqslant 1$ et la majoration est donc licite. Nous optimisons notre paramètre η en choisissant

$$\eta \ := \ \frac{1}{2m+1} \qquad \text{de sorte que} \qquad \mu \ = \ \eta N. \tag{13.6}$$

Donc

$$\sum_{r\in\mathfrak{R}} \big|G_N(r)\big| \ \ll_{g,m,\epsilon}\ \Big(\delta^{-\frac{1}{2}}g^{-\frac{\eta N}{4}}+\delta^{-\frac{1}{4}}\Big)\delta^{-\frac{1}{2}}\big(\mathcal{K}_\alpha+\epsilon\big)^{\frac{\mu}{2}},$$

ce qui démontre la majoration annoncée. □

Lemme 13.4. *Soient $m \geqslant 2$ un entier et $\epsilon > 0$. Il existe une constante $c_8 > 0$ telle qu'uniformément pour Q et N assez grand, nous avons la majoration*

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(\tfrac{l}{q})| \ll_{g,m,\epsilon} Q^2 g^{-\frac{N}{8m+4}} (\mathcal{K}_\alpha + \epsilon)^{\frac{N}{4m+2}} + Q^{\frac{3}{2}} (\mathcal{K}_\alpha + \epsilon)^{\frac{N}{4m+2}} + Q e^{-c_8\sqrt{N}}, \quad (13.7)$$

en ayant noté $\alpha := \frac{2m}{3}$.

Démonstration. Nous suivons la même démonstration que celle du lemme 11.11. Nous commençons par rendre les fractions irréductibles en isolant leur facteur commun d. Ainsi, pour le même choix du paramètre

$$D := gQ \exp\big(-c_7\sqrt{N}\big)$$

que dans le lemme 11.11, nous avons la majoration

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(\tfrac{l}{q})| \leqslant \sum_{d<D} \sum_{r\in\mathfrak{R}} |G_N(r)| + \sum_{D\leqslant d<Q} \sum_{r\in\mathfrak{R}} |G_N(r)|$$

pour l'ensemble

$$\mathfrak{R} := \{\tfrac{l}{q},\ q < \tfrac{Q}{q},\ (l,q) = 1,\ (q, g^3 - g) = 1\}$$

qui vérifie l'hypothèse (H_δ) pour $\delta = (\frac{Q}{d})^{-2}$. Lorsque $d \geqslant D$, nous utilisons la même majoration que dans le lemme 11.11. Lorsque $d < D$, nous utilisons la majoration du lemme 13.3. Ainsi,

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(\tfrac{l}{q})| \ll_{g,m,\epsilon} \sum_{d<D} (\tfrac{Q}{d})^2 g^{-\frac{N}{8m+4}} (\mathcal{K}_\alpha + \epsilon)^{\frac{N}{4m+2}} + \sum_{d<D} (\tfrac{Q}{d})^{\frac{3}{2}} (\mathcal{K}_\alpha + \epsilon)^{\frac{N}{4m+2}} + \sum_{D\leqslant d<Q} e^{-c_8\sqrt{N}}.$$

En évaluant ces séries, nous avons donc

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(\tfrac{l}{q})| \ll_{g,m,\epsilon} Q^2 g^{-\frac{N}{8m+4}} (\mathcal{K}_\alpha + \epsilon)^{\frac{N}{4m+2}} + Q^{\frac{3}{2}} (\mathcal{K}_\alpha + \epsilon)^{\frac{N}{4m+2}} + Q e^{-c_8\sqrt{N}}.$$

ce qui termine la preuve. □

Corollaire 13.1. *Si $m \geqslant 2$ est un entier tel que*

$$\mathcal{K}_{\frac{2m}{3}} < g^{-\frac{1}{2}}. \quad (13.8)$$

Alors

$$\beta \;:=\; \Big(\frac{1}{2} - \frac{\log \mathcal{K}_{2m/3}}{\log g}\Big)\frac{1}{4m+2} \;>\; \frac{1}{4m+2}.$$

est un exposant de distribution admissible pour $\mathscr{R}$. Pour toute base g, il existe donc un exposant de distribution admissible $\beta > \beta_g$, où β_g est donné par le tableau

g	2	3	4	5	6	7	8	9	10
β_g	$\frac{1}{38}$	$\frac{1}{98}$	$\frac{1}{74}$	$\frac{1}{122}$	$\frac{1}{114}$	$\frac{1}{158}$	$\frac{1}{150}$	$\frac{1}{194}$	$\frac{1}{186}$

et lorsque g est assez grand,

$$\beta \;=\; \frac{1+o(1)}{6\pi g}.$$

Démonstration. L'exposant β se déduit du lemme 13.4 exactement comme nous avons trouvé le premier exposant de distribution. □

Corollaire 13.2. *Pour $g = 2$, il existe un exposant de distribution*

$$\beta \;>\; 0.03356 \;>\; \frac{1}{30}.$$

Pour $g = 3$, il existe un exposant de distribution

$$\beta \;>\; 0.01065 \;>\; \frac{1}{94}.$$

Démonstration. Pour $g = 2$, nous choisissons $m = 7$ dans le corollaire 13.1 puis nous majorons $\mathcal{K}_\alpha$ grâce au lemme 11.6. Pour $g = 3$, nous choisissons $m = 23$. En notant $\alpha := \frac{2m}{3}$, nous avons,

$$\begin{aligned}
\text{pour } g = 2 \quad &: \quad \mathcal{K}_\alpha \;\leqslant\; \mathcal{M}_\alpha^5 \;<\; 0.703763 \;<\; 2^{-\frac{1}{2}},\\
\text{pour } g = 3 \quad &: \quad \mathcal{K}_\alpha \;\leqslant\; \mathcal{M}_\alpha^2 \;<\; 0.576562 \;<\; 3^{-\frac{1}{2}}.
\end{aligned}$$

l'hypothèse du corollaire 13.1 est vérifiée, ce qui termine la preuve. □

Remarque 13.1. Pour $g = 2$, nous avons choisi $k = 5$ pour la majoration $\mathcal{K}_\alpha \leqslant \mathcal{M}_\alpha^k$ du lemme 11.6, car c'est le plus petit entier permettant de choisir $m = 7$ dans le corollaire 13.1. Le nombre de termes à sommer dans la définition de $\mathcal{M}_\alpha^k$ étant proportionnel à g^k, les calculs dépassent très vite les capacités des machines actuelles, même s'ils sont réalisables en valeur exacte ($\mathcal{M}_\alpha^k$ ne fait intervenir que des nombres algébriques de degré au plus k). Il est à noter qu'il est impossible d'utiliser la valeur $m = 6$ dans le corollaire 13.1 même pour des entiers k beaucoup plus grand.

Annexe A

Le lemme de Sobolev-Gallagher

Lemme A.1. *Soient $\delta > 0$, $\mathfrak{R}$ un ensemble δ-bien espacé de points de $[\frac{\delta}{2}, 1-\frac{\delta}{2}]$ et f une fonction admettant une dérivée continue sur $[0,1]$. Alors*

$$\sum_{x\in\mathfrak{R}} |f(x)| \ \leqslant\ \delta^{-1}\|f\|_1 + \frac{1}{2}\|f'\|_1.$$

Démonstration. Soit $\phi : [0,1] \to \mathbb{C}$, une fonction possédant une dérivée continue sur $]0,1[$. En évaluant chaque intégrale à l'aide d'une intégration par parties, nous avons l'identité

$$\begin{aligned}\int_{\frac{1}{2}}^1 (t-1)\phi'(t)\mathrm{d}t + \int_0^{\frac{1}{2}} t\phi'(t)\mathrm{d}t \ &= \ \Big[(t-1)\phi(t)\Big]_{\frac{1}{2}}^1 + \Big[t\phi(t)\Big]_0^{\frac{1}{2}} - \int_0^1 \phi(t)\mathrm{d}t \\ &= \phi(\frac{1}{2}) - \int_0^1 \phi(t)\mathrm{d}t.\end{aligned}$$

Donc

$$\left|\phi(\frac{1}{2})\right| \ \leqslant\ \int_0^1 |\phi(t)|\,\mathrm{d}t + \frac{1}{2}\int_0^1 |\phi'(t)|\,\mathrm{d}t. \tag{A.1}$$

Pour chaque point x de $\mathfrak{R}$, nous appliquons pour la fonction $\phi(t) := f(x + t\delta - \frac{\delta}{2})$ cette inégalité. Nous obtenons les majorations

$$\begin{aligned}|f(x)| \ &\leqslant\ \int_0^1 \left|f(x + t\frac{\delta}{2} - \frac{\delta}{2})\right|\mathrm{d}t + \frac{1}{2}\int_0^1 \frac{\delta}{2}\left|f'(x + t\frac{\delta}{2} - \frac{\delta}{2})\right|\mathrm{d}t \\ &\leqslant\ \delta^{-1}\int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f(t)|\,\mathrm{d}t + \frac{1}{2}\int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f'(t)|\,\mathrm{d}t.\end{aligned}$$

Donc, en sommant sur les points x de $\mathfrak{R}$,

$$\sum_{x\in\mathfrak{R}} |f(x)| \ \leqslant\ \delta^{-1}\sum_{x\in\mathfrak{R}}\int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f(t)|\,\mathrm{d}t + \frac{1}{2}\sum_{x\in\mathfrak{R}}\int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f'(t)|\,\mathrm{d}t.$$

L'ensemble $\mathfrak{R}$ étant δ-bien espacé dans $[\frac{\delta}{2}, 1-\frac{\delta}{2}]$, les plages de sommation des différentes intégrales sont disjointes et contenues dans $[0,1]$. Le lemme s'en déduit donc immédiatement. □

Bibliographie

[All82] Krishnaswami Alladi. The turán–kubilius inequality for integers without large prime factors. *Journal für die Reine und Angewandte Mathematik*, pages 180–196, 1982.

[BHS04] William D. Banks, Derrick N. Hart, and Mayumi Sakata. Almost all palindromes are composite. *Mathematical Research Letters*, pages 853–868, 2004.

[BS04] William D. Banks and Igor E. Shparlinski. Arithmetic properties of numbers with restricted digits. *Acta Arithmetica*, pages 313–332, 2004.

[dB51] N. G. de Bruijn. On the number of positive integers $\leqslant x$ and free of prime factors $> y$. *Nederl. Akad. Wetensch. Proc.*, pages 50–60, 1951.

[DM00] Cécile Dartyge and Christian Mauduit. Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres". *Journal of Number Theory*, pages 270–291, 2000.

[DM01] Cécile Dartyge and Christian Mauduit. Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers. *Journal of Number Theory*, pages 230–255, 2001.

[DMT01] Cécile Dartyge, Greg Martin, and Gérald Tenenbaum. Polynomial values free of large prime factors. *Periodica Mathematica Hungarica. Journal of the János Bolyai Mathematical Society*, pages 111–119, 2001.

[EMS98] Paul Erdös, Christian Mauduit, and András Sárközy. On the arithmetic properties of integers with missing digits i : Distribution in residue classes. *Journal of Number Theory*, pages 99–120, 1998.

[EMS99] Paul Erdös, Christian Mauduit, and András Sárközy. On the arithmetic properties of integers with missing digits ii : Prime factors. *Discrete Mathematics*, pages 149–164, 1999.

[FI97] Étienne Fouvry and Henryk Iwaniec. Gaussian primes. *Acta Arithmetica*, pages 249–287, 1997.

[FI98a] J. Friedlander and Henryk Iwaniec. Asymptotic sieve for primes. *Annals of Mathematics. Second Series*, pages 1041–1065, 1998.

[FI98b] J. Friedlander and Henryk Iwaniec. The polynomial X^2+Y^4 captures its primes. *Ann. of Math. (2)*, pages 945–1040, 1998.

[FK96] Michael Filaseta and Sergei Konyagin. Squarefree values of polynomials all of whose coefficients are 0 and 1. *Acta Aritmetica*, pages 191–205, 1996.

[FM96] Étienne Fouvry and Christian Mauduit. Méthodes de cribles et fonctions sommes des chiffres. *Acta Arithmetica*, pages 339–351, 1996.

[Fri89] John B. Friedlander. Shifted primes without large prime factors. In *Number theory and applications (Banff, AB, 1988)*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., pages 393–401. Kluwer Acad. Publ., Dordrecht, 1989.

[FT91] Étienne Fouvry and Gérald Tenenbaum. Integers without large prime factors in arithmetic progressions. *Proceedings of the London Mathematical Society*, pages 449–494, 1991.

[FT96] Étienne Fouvry and Gérald Tenenbaum. Répartition statistique des entiers sans grand facteur premier dans les progressions arithmétiques. *Proceedings of the London Mathematical Society*, pages 481–514, 1996.

[HB83] D. Roger" Heath-Brown. The piatetski-shapiro prime number theorem. *Journal of Number Theory*, pages 242–266, 1983.

[HB01] D. Roger Heath-Brown. Primes represented by $x^3 + 2y^3$. *Acta Mathematica*, pages 1–84, 2001.

[Hil86] Adolf Hildebrand. On the number of positive integers $\leqslant x$ and free of prime factors $> y$. *Journal of Number Theory*, pages 289–307, 1986.

[HR74] Heini Halberstam and H.-E. Richert. *Sieve methods*. Academic Press, London–New-York, 1974. London Mathematical Society Monographs.

[HT93] Adolf Hildebrand and Gérald Tenenbaum. Integers without large prime factors. *Journal de Théorie des Nombres de Bordeaux*, pages 411–484, 1993.

[Iwa80] Henryk Iwaniec. Rosser's sieve. *Acta Arithmetica*, pages 171–202, 1980.

[Iwa81] Henryk Iwaniec. Rosser's sieve–bilinear forms of the remainder terms–some applications. *Academic Press*, pages 203–230, 1981.

[KMS00] Sergei Konyagin, Christian Mauduit, and András Sárközy. On the number of prime factors of integers characterized by digit properties. *Periodica Mathematica Hungarica*, pages 37–52, 2000.

[Kol67] G. A. Kolesnik. The distribution of primes in sequences of the form $[n^c]$. *Akademiya Nauk SSR. Mathematicheskie Zametki*, pages 117–128, 1967.

[Kon01] Sergei Konyagin. Arithmetic properties of integers with missing digit : distribution in residue classes. *Periodica Mathematica Hungarica*, pages 145–162, 2001.

[MFT97] Michel Mendès France and Gérald Tenenbaum. *Les nombres premiers*. Que sais-je ? [what Do I Know]. Presses Universitaires de France, 1997.

[MS97] Christian Mauduit and Aandrás Sárközy. On the arithmetic structure of the integers whose sum of digits is fixed. *Acta Arithmetica*, pages 145–173, 1997.

[Pia53] Ilya I. Piatetskǐ-Šhapiro. On the distribution of prime numbers in sequences of the form $[f(n)]$. *Mat. Sbornik N.S.*, pages 559–566, 1953.

[Rib04] Paulo Ribenboim. *The little book of bigger primes.* Springer-Verlag, second edition, 2004.

[RS01] Joël Rivat and Patrick Sargos. Nombres premiers de la forme $\lfloor n^c \rfloor$. *Canadian Journal of Mathematics*, pages 414–433, 2001.

[Ten95] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres.* Cours Spécialisés. Société Mathématique de France, second edition, 1995.

Monsieur **COL Sylvain**

DOCTORAT DE L'UNIVERSITE HENRI POINCARE, NANCY 1

en MATHEMATIQUES

VU, APPROUVÉ ET PERMIS D'IMPRIMER N° 1204

Nancy, le 3 juillet 2006

Le Président de l'Université

UNIVERSITÉ HENRI POINCARÉ, NANCY
LE PRÉSIDENT
J.P. FINANCE

Université Henri Poincaré, Nancy I
24-30 rue Lionnois - B.P. 3069 - 54013 NANCY Cédex
Tél. : 03 83 68 20 00 - Fax : 03 83 68 21 00

Résumé

Pour une base fixée, les entiers ellipséphiques (c'est-à-dire les entiers dont l'écriture n'utilise que certains chiffres) et les palindromes forment des sous ensembles éparses des entiers, ensembles définis par des conditions digitales. Nous étudions si ces ensembles ont des propriétés multiplicatives similaires à celles des entiers.

Nous évaluons d'abord les grands moments de la série génératrice des entiers ellipséphiques. Comme application, nous en déduisons l'existence d'un $0 < c < 1$ tel que pour tout entier k, une infinité d'entiers ellipséphiques n possédant un diviseur p^k de l'ordre de n^c, p désignant un nombre premier. De plus, le nombre de tels entiers est de l'ordre de grandeur attendu.

Nous établissons ensuite un résultat de crible où les modules possédant un nombre anormalement grand de diviseurs sont écartés du terme d'erreur. Nous en déduisons l'existence d'une proportion positive d'entiers ellipséphiques friables c'est-à-dire possédant tous leurs facteurs premiers majorés par n^c, pour une constante $c < 1$ fixée.

Nous montrons enfin à l'aide de techniques élémentaires comment réduire l'étude de la série génératrice des palindromes à une série proche de celle des entiers ellipséphiques ce qui permet d'étudier la répartition des palindromes dans les progressions arithmétiques et ainsi d'obtenir une majoration de l'ordre de grandeur attendu du nombre de palindromes premiers. Nous en déduisons en particulier l'existence d'une infinité de palindromes possédant en base 10 au plus 372 facteurs premiers (comptés avec multiplicité).

Mots-Clefs

conditions digitales, nombres ellipséphiques, palindromes, nombres (presque) premiers, entiers friables, méthodes de crible, exposant de répartition, somme d'exponentielles, série génératrice, inégalité de Sobolev-Gallagher.

Summary

Numbers with missing digits and palindromic numbers (with respect to a fixed basis) are subset of the integers. This subsets are defined by digital conditions and are scattered. We study if this sets have multiplicative properties similar to those of the integers.

Firstly, we evaluate the high moments of the generating series of numbers with missing digits. As a application, we show that there is a $0 < c < 1$ such that for all integer k, the integers n with missing digits which have a factor p^k with $p^k \sim n^c$ and p a prime, are innumerable. Moreover the number of such integers has the expected size.

Secondly, we establish a result of sieve where the modules with an abnormally large number of divisors are expelled of the error term. We deduce consequently the existence of a positive proportion of numbers with missing digits which have no large prime factors.

Thirdly, using elementary methods, we show how to reduce the study of the generating series of the palindromes to a series close to that of the numbers with missing digits. This makes possible to study their repartition in the arithmetical progressions and thus to obtain an upper bound for the palindromic primes. We deduce in particular that the palindromes with at most 372 prime factors in basis 10 are endless.

Keywords

number with missing digits, palindrome, (nearly) primes, numbers with small prime factors, sieves, exponent of distribution, exponentials sum, generating series, Sobolev-Gallagher's inequality.