Sur deux questions de crible

David Feutrie

UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Sur deux questions de crible

THÈSE

présentée et soutenue publiquement le 13 décembre 2019

pour l'obtention du

Doctorat de l'Université de Lorraine

(mention mathématiques)

par

David Feutrie

Composition du jury

Examinateurs :	Youness LAMZOURI	Professeur, Université de Lorraine
	Joël RIVAT	Professeur, Université d'Aix-Marseille
Rapporteurs :	Michel BALAZARD	Chargé de recherche CNRS, Université Aix-Marseille
	Bruno MARTIN	Professeur, Université du Littoral Côte d'Opale
Encadrants :	Cécile DARTYGE	Maître de conférences, Université de Lorraine
	Gérald TENENBAUM	Professeur, Université de Lorraine

Institut ÉLIE CARTAN

Élie Cartan de Lorraine
Laboratoire de mathématiques — UMR 7502
54506 VANDOEUVRE-LÈS-NANCY

Remerciements

Je commencerai bien évidemment par remercier mes directeurs de thèse Cécile Dartyge et Gérald Tenenbaum pour les quatre années qu'ils ont passées à diriger mon travail, pour les nombreux aiguillages et conseils qu'ils m'ont donnés, en particulier dans les périodes plus dures de la recherche.

Je remercie mes rapporteurs de thèse Michel Balazard et Bruno Martin pour le temps qu'ils ont pris à se consacrer à la relecture de mes recherches.

Je remercie également Youness Lamzouri et Joël Rivat pour avoir accepté de faire aussi partie de mon jury de thèse.

Je remercie également les autres membres de théorie analytique des nombres au sein de l'IECL, en particulier Thomas Stoll, ainsi qu'Anne de Roton, qui m'a été d'un grand soutien à certains moments plus difficiles.

Je tiens à remercier l'ensemble des doctorants qui m'ont accompagné durant toutes ces années, entre ceux qui sont déjà partis et ceux qui sont arrivés après. Je commencerai par Simon Jacques, avec qui j'ai pu créer au sein du travail une grande et belle amitié. Ma pensée vient ensuite à Zhiwei Wang, mon voisin de bureau durant 3 ans, ce qui nous a permis d'avoir de nombreuses échanges, en particulier sur le bon usage des mots français. Je pense ensuite à Jérémy Haut qui, avec Simon, a été mon collègue de bureau durant la dernière année de ma thèse et qui m'a été aussi d'un grand soutien. Je remercie également Pierre-Adrien, Johann, Armand, Gautier, Florian, Robin, Youssef et Renan qui ont été mes collègues en théorie analytique des nombres, et qui m'ont aidé dans la finalisation de la présentation de la thèse. Je ne peux m'empêcher de d'avoir une pensée également pour les autres doctorants ou jeunes docteurs du laboratoire, en particulier Tom, Clémence, Lizao, Rihab, Yann, Dimitri, etc. Je termine par une petite pensée pour les jeunes docteurs de théorie des nombres que j'ai croisés à l'extérieur de l'IECL, en particulier Lucile, Kevin, Cathy et Elie.

Je remercie les chercheurs du laboratoire avec qui, grâce aux enseignements que nous avons eus en commun, ont permis de nouer une certaine complicité. Je pense en particulier à Aurélie Gueudin-Muller, Nicole Bardy-Panse, Irène Marcovici et Bruno Duchesne, ainsi que tous ceux qui avec qui j'ai pu avoir quelque discussion lors d'un repas le midi ou lors d'une pause à la salle de détente (pas de café pour moi, qui n'ai toujours pas su m'y mettre).

Je ne peux pas passer par cette phase sans penser aux nombreux amis qui m'ont été d'une aide dont ils ne pourront jamais s'imaginer à quel point elle me fut profitable. Je les remercie particulièrement pour tous ces moments que nous avons fait ensemble et qui resteront gravés dans ma mémoire. Une pensée d'abord pour certains week-ends à Nolay où j'ai pu ressentir ce que voulait dire "Il n'y a rien sur cette terre de plus précieux qu'une véritable amitié". Je repense également aux soirées bowling, aux soirées bar (même si je ne me suis toujours pas mis à l'alcool), aux marches vers Sion ou Saint-Nicolas-de-Port, aux sorties cinés, aux balades à vélo, aux matchs de foot, etc.

Je ne pourrai citer l'ensemble des amis à Nancy qui me furent d'une grande aide. J'adresse d'abord un merci particulier au père Jean-Michaël dont les conseils avisés

furent décisifs dans les choix de mon travail. Je pense aussi à Raïssa, Capucine, Hugo, Lorella, Amédée, Hortense et Jean-Laurent, Mélanie, Coline, Margot, Guillaume, Paul-Emmanuel, Julie, Benoit, François, Olivier, Pierre, Camille, Patrick et Astrid, Gauthier, Kayle, Sophie, ainsi qu'à tous ceux dont le manque de place m'empêche de continuer la liste. Une pensée aussi à mes colocataires de NDL (Emmanuel, Pierre-Emmanuel, Louis-Marie etc.) ainsi que pour les amis de plus longue date, comme Benoit, dont nos chemins se sont croisés de nouveau à Nancy, Bénédicte et Grégoire, Étienne, Isabelle, Stéphanie, etc.

Je terminerai ces remerciements par les membres de ma famille qui ont toujours été derrière moi durant mes thèses et bien évidemment lors de ces quatre années. Mes pensées vont d'abord à ceux qui nous ont quitté, en particulier ma mère qui n'a pas pu connaître sur terre le début de ma thèse, et mes grands-parents qui sont partis au cours de mon travail de doctorat, et à qui je dois beaucoup. Je pense bien sûr à mon père qui est d'un soutien indéfectible et à mon frère dont la complicité s'est intensifié malgré la distance.

Table des matières

Introduction

Soient $(a,q)=1$: existe-t-il une infinité de nombres premiers p vérifiant $p\equiv a \pmod q$? Cette question fut l'un des problèmes les plus célèbres de la théorie des nombres. Elle fut résolue par Dirichlet en 1837 [9], généralisant ainsi le théorème d'Euclide.

Par la suite, Hadamard [22] et La Vallée-Poussin [32], en s'intéressant plus précisément au problème de l'équirépartition de tels entiers, ont prouvé que

$$\pi(x;a,q):=\#\big|\{p\leqslant x:\ p\equiv a\ (\mathrm{mod}\ q)\}\big|\sim\frac{x}{\varphi(q)\log x}\qquad(x\to\infty). \tag{0.0.1}$$

La notion de progression arithmétique a pris une importance considérable dans la théorie des nombres au fil des derniers siècles, plus spécifiquement pour les nombres premiers appartenant à une progression arithmétique. Ainsi, la démonstration faite par Dirichlet pour prouver le théorème de la progression arithmétique lui a fait introduire plusieurs familles de fonctions telles que les caractères de Dirichlet et leur fonction L associée. Depuis, ces fonctions sont devenues des outils indispensables en théorie analytique des nombres. Elles interviennent par exemple dans la formulation de l'hypothèse de Riemann généralisée, qui demeure depuis l'une des conjectures les plus célèbres, ou bien pour démontrer le théorème de Bombieri-Vinogradov prouvé en 1965, et qui reste depuis lors un outil majeur de la théorie analytique des nombres.

L'objet de cette thèse est d'étudier deux ensembles précis dont les caractéristiques font intervenir une progression arithmétique $a\,(\mathrm{mod}\ q)$:

- les entiers sans diviseur dans une progression arithmétique fixée ;
- les entiers sans grande puissance de facteur premier qui sont premiers à un entier q, puis la partie de ces entiers qui sont dans une progression arithmétique $a\,(\mathrm{mod}\ q)$.

1. Entiers sans diviseur dans une progression arithmétique

1.1. Diviseur

La notion de diviseur est une notion fondamentale dans la théorie des nombres.

Commençons par évoquer la quantité

$$\tau(n):=\sum_{d\,|\,n}1\quad(n\geqslant 1).$$

Cette fonction est multiplicative et vérifie

$$\tau(n) = \prod_{p^\nu \| n} (\nu + 1) \qquad (n \geqslant 1).$$

De plus (voir [57]), elle possède également les propriétés [1]

$$\tau(n) = O(n^\varepsilon) \quad (\varepsilon > 0), \qquad \limsup_{n\to\infty} \frac{\log \tau(n) \log_2 n}{\log n} = \log 2$$

et, afin de préciser son comportement moyen, on a

$$\sum_{n\leqslant x} \tau(n) = x(\log x + 2\gamma - 1) + O(\sqrt{x})$$

où γ désigne la constante d'Euler.

Une autre fonction dont la définition nécessite l'utilisation des diviseurs d'un entier est la fonction

$$\sigma(n) := \sum_{d\,|\,n} d \quad (n \geqslant 1),$$

qui est aussi multiplicative et qui intervient dans différents ensembles d'entiers étudiés dans l'histoire des mathématiques.

Par exemple, nous pouvons citer l'ensemble des nombres amicaux, qui sont des paires d'entiers (m, n) vérifiant $\sigma(n) = \sigma(m) = m+n$. La première paire de nombres amicaux connue est $(220, 284)$, à laquelle certains penseurs de l'Antiquité, en particulier à l'école des pythagoriciens, avaient attribué des pouvoirs magiques et des qualités sociales. Depuis, d'autres paires ont été découvertes par plusieurs mathématiciens, notamment Euler et Fermat. À ce jour, s'il est impossible de savoir s'il existe une infinité de telles paires, Pomerance [42] a montré que, si l'on note $A(x)$ le nombre de paires d'entiers amicaux dont le premier élément est inférieur à x, il existe une constante $c > 0$ tel que

$$A(x) = O\big(x \exp(-c\sqrt{\log_3 x \log_4 x})\big),$$

et Erdös [14] a conjecturé que pour tout $\varepsilon > 0$ et k, il existe $x_0(\varepsilon, k)$ tel que

$$x^{1-\varepsilon} < A(x) < \frac{x}{(\log x)^k} \qquad \big(x > x_0(\varepsilon, k)\big).$$

Un autre ensemble célèbre faisant intervenir la fonction σ est celui des nombres parfaits, qui sont les entiers n vérifiant $\sigma(n) = 2n$, dont 6 et 28 font partie. La recherche des nombres parfaits est liée à celle des nombres premiers de Mersenne, qui sont les nombres premiers de la forme $2^n - 1$. Un résultat connu sur le sujet et démontré par Euler est le fait que tout nombre parfait pair s'écrit sous la forme $2^{p-1}(2^p - 1)$. Toutefois, même si ces nombres sont rares parmi l'ensemble des entiers, il est actuellement impossible de savoir s'il en existe un nombre fini, ni même si des nombres parfaits impairs existent. Néanmoins Pomerance, en 2003, par une approche heuristique, a conjecturé que la deuxième affirmation était fausse.

1. Ici et dans la suite, la fonction log désigne le logarithme népérien. De plus, on note $\log_1 := \log$ et $\log_k := \log(\log_{k-1})$ pour $k \geqslant 2$.

Les nombres pratiques, qui sont les entiers n dont tous les entiers inférieurs à n peuvent s'écrire comme somme de diviseurs distincts de n, forment un autre ensemble de nombres sur lequel il est intéressant de se pencher. Par exemple, les nombres parfaits ou les puissances de 2 sont des nombres pratiques. L'une des particularités de ces entiers concerne les nombreuses propriétés qu'ils partagent avec les nombres premiers. Ainsi, notant $P(x)$ le nombre d'entiers pratiques inférieurs à x, Margenstern [37] a conjecturé qu'il existe une constante $c > 0$ telle que

$$P(x) \sim \frac{cx}{\log x} \qquad (x \geqslant 3).$$

Tenenbaum [55, 56] puis Saias [47] ont apporté une contribution importante à cette conjecture avant que Weingartner [61] ne finisse par la démontrer.

1.2. Quelques exemples d'ensembles d'entiers liés par leurs diviseurs

La notion de diviseur intervient dans de nombreux problèmes de théorie des nombres, ces problèmes ayant des applications dans d'autres domaines des mathématiques.

Nous pouvons d'abord évoquer les entiers qui admettent un diviseur dans un intervalle défini. Ainsi, Tenenbaum [53] puis Ford [15] se sont intéressés à la quantité

$$H(x, y, z) := \#\big\{n \leqslant x : \exists d \mid n,\ d \in]y, z]\big\},$$

et en ont obtenu plusieurs estimations selon les valeurs de x, y et z. Ces travaux ont donné différentes applications, par exemple l'obtention d'un ordre de grandeur pour l'ensemble des permutations d'ordre n ayant le même nombre de points fixes [11], des estimations pour les hyperboles modulaires [50], qui sont les solutions $(x, y) \in \mathbb{N}^2$ de l'équation $xy \equiv a \pmod m$ lorsque $(a, m) = 1$, ou encore une étude de l'écart entre un entier et son inverse dans $\mathbb{Z}/n\mathbb{Z}$ [16].

Un autre sujet important et utilisant les diviseurs concerne les entiers à diviseurs z-denses où $z > 1$, c'est-à-dire les entiers n qui, si l'on note $1 = d_1(n) < d_2(n) < \ldots < d_{\tau(n)} = n$ la suite croissante des diviseurs de n, vérifient

$$\max_{1 \leqslant i < \tau(n)} \frac{d_{i+1}(n)}{d_i(n)} \leqslant z.$$

La fonction de comptage $D(x, z)$ de cet ensemble a été notamment étudiée par Tenenbaum [55, 56], par Saias [47], puis par Weingartner [61] qui a montré que

$$D(x, z) = xd\Big(\frac{\log x}{\log z}\Big)\Big\{1 + O\Big(\frac{1}{\log z}\Big)\Big\} \cdot \Big\{1 + O\Big(\frac{1}{\log(2x)}\Big)\Big\} \quad (x \geqslant 1, z \geqslant 2)$$

avec

$$d(v) := 1 - \int_0^{(v-1)/2} \frac{d(u)}{u+1} \omega\Big(\frac{v-u}{u+1}\Big) \mathrm{d}u \quad (v \geqslant 0)$$

où ω désigne la fonction de Buchstab et $d(v) = 0$ lorsque $v < 0$. Comme évoqué par Tenenbaum, ces entiers ont également une application importante sur le "petit crible" d'Erdös et Ruzsa défini dans [13], c'est-à-dire sur l'estimation de la quantité

$H(x) := \min F(x,A)$ où A est un ensemble d'entiers, $F(x,A)$ désigne le nombre d'entiers $\leqslant x$ qui n'ont aucun diviseur dans A, et le minimum est porté sur les ensembles A vérifiant $\sum_{a\in A} 1/a \leqslant 1$ et $1 \notin A$. En appliquant son résultat, Saias [48] a démontré qu'il existe deux constantes $c_1, c_2 > 0$ telles que

$$c_1 \frac{x}{\log x} \leqslant H(x) \leqslant c_2 \frac{x}{\log x} \quad (x \geqslant 2).$$

Évoquons enfin la fonction Δ de Hooley, qui est définie comme suit :

$$\Delta(n) := \max_{u\in\mathbb{R}} \#\big\{d :\ d \mid n, u < \log d \leqslant u+1\big\}.$$

Introduite et étudiée initialement par Hooley [29], elle a ensuite été développée par Hall & Tenenbaum [23] et Maier & Tenenbaum [35, 36], qui ont montré que

$$(\log_2 n)^{\gamma+o(1)} < \Delta(n) < (\log_2 n)^{\log 2+o(1)} \qquad \text{p.p.},$$

lorsque $\gamma := -\log 2/\log\big(\frac{1-1/\log 27}{1-1/\log 3}\big) \approx 0,33827\ldots$. Cette quantité a de nombreuses applications telles que l'obtention d'une majoration de

$$\big|\big\{p :\ p+a \leqslant x,\ \exists d \mid p+a,\, d \in]y,z]\big\}\big| \qquad \big(y \geqslant 2,\ 2y \leqslant z \leqslant \min\{y^{3/2}, \sqrt{x}\}\big)$$

(cf. [30]) ou une généralisation d'un résultat de Shiu grâce à la majoration de sommes de la forme $\sum_{n\leqslant x} \Delta(|Q(n)|)^t$ où $t > 0$ et Q est un polynôme bien choisi (cf. [39]). On pourra trouver une excellente présentation de la fonction Δ de Hooley dans la synthèse de Tenenbaum [54].

1.3. Cribler par une progression arithmétique

Nous consacrons la première partie de cette thèse à l'étude des entiers sans diviseur dans une progression arithmétique fixée. De tels entiers interviennent en théorie algébrique et algorithmique des nombres ; par exemple, les entiers impairs sans facteur carré et qui s'écrivent comme somme de deux carrés n'ont aucun diviseur dans la progression arithmétique $3 \pmod 4$.

1.3.1. Historique

En 1953, Landau [33] a montré que, si on fixe un entier $q \geqslant 2$ et a vérifiant $1 < a < q$ et $(a,q) = 1$, alors presque tout entier $n \in \mathbb{N}^*$ admet un diviseur d vérifiant $d \equiv a \pmod q$. Ce résultat peut être réécrit, en notant

$$\tau(n;a,q) := \#\big\{d \mid n,\ d > 1,\ d \equiv a \pmod q\big\},$$

par l'expression

$$\#\{n \leqslant x : \tau(n;a,q) \geqslant 1\} = x + o(x).$$

Erdös [12] a généralisé ce résultat à $q \leqslant (\log x)^{\log 2-\varepsilon}$ avec $\varepsilon > 0$, l'exposant $\log 2$ étant optimal.

Ainsi qu'il a été relevé dans [40], la preuve de Landau implique directement le fait que pour $q \geqslant 3$ fixé, le nombre des entiers inférieurs à x dont les facteurs premiers, et donc les diviseurs, sont tous congrus à 1 modulo q est asymptotiquement égal à

$$\big\{C_q + o(1)\big\}\frac{x}{(\log x)^{1-1/\varphi(q)}} \tag{0.0.2}$$

où l'on a posé

$$C_q := \frac{q}{\Gamma(1/\varphi(q))\varphi(q)}\prod_p\Big(1-\frac{1}{p}\Big)^{1/\varphi(q)}\Big(1-\frac{\vartheta(p)}{p}\Big)^{-1} > 0,$$

avec

$$\vartheta(p) := \begin{cases} 1 & \text{si } p \equiv 1 \pmod q, \\ 0 & \text{dans le cas contraire.} \end{cases}$$

L'objet de la première partie de ce travail est de s'intéresser à l'ensemble

$$\mathcal{N}_{a,q} := \big\{n \in \mathbb{N}^* : \tau(n;a,q) = 0\big\},$$

et en particulier de trouver une estimation asymptotique de sa fonction de comptage.

Cet ensemble a déjà été étudié dans deux articles. D'abord, Banks, Friedlander et Luca fournissent en 2008 [1] une estimation de la fonction de comptage de $\mathcal{N}_{a,q}$ dans le cas particulier où q est un nombre premier fixé. Trois ans plus tard, Narkiewicz et Radziejewski [40] généralisent le résultat à q quelconque. Ils observent d'abord que les cas particuliers $a = 2$, $q = 1$ et $a = 0$, q quelconque sont triviaux et que lorsque $(a,q) > 1$, on peut se ramener au cas $(a,q) = 1$, ce qui implique qu'il suffit de s'intéresser au cas $q \geqslant 3$ et $(a,q) = 1$. Sous ces conditions, ils obtiennent alors l'estimation [2]

$$\mathcal{N}_{a,q}(x) = \big\{C(a,q) + o(1)\big\}\frac{x(\log_2 x)^{\alpha(a,q)}}{(\log x)^{1-\beta(a,q)}}$$

où $C(a,q) > 0$, $\alpha(a,q) > 0$ et $0 \leqslant \beta(a,q) < 1$. Ces trois constantes dépendent des propriétés de $G_q := (\mathbb{Z}/q\mathbb{Z})^*$ en tant que groupe multiplicatif.

Le cas $a = 1$ est particulier : dans cette circonstance, les constantes sont plus faciles à expliciter. En effet, nous avons $\alpha(1,q) = D_q - 2$ où D_q désigne la constante de Davenport de G_q, qui est définie comme le plus petit entier r tel que, de toute suite de $t \geqslant r$ éléments de G_q, on peut extraire une sous-suite dont le produit des éléments est égal à 1. De plus, $\beta(1,q) = 0$. Enfin, en posant

$$\mathfrak{S}(\boldsymbol{\nu}) := \sum_{j\in G_q}\nu_j \quad \big(\boldsymbol{\nu} \in \mathbb{N}^{G_q}\big),$$

$$E_q(a) := \Big\{\boldsymbol{\nu} \in \mathbb{N}^{G_q} : \boldsymbol{\mu} \in \mathbb{N}^{G_q},\, \boldsymbol{\mu} \preccurlyeq \boldsymbol{\nu}, \mathfrak{S}(\boldsymbol{\mu}) > 0 \Rightarrow \textstyle\prod_{j\in G_q} j^{\mu_j} \not\equiv a \pmod q\Big\},$$

où $\boldsymbol{\mu} \preccurlyeq \boldsymbol{\nu}$ signifie $\mu_j \leqslant \nu_j$ $(j \in G_q)$, nous avons

$$C(1,q) = \frac{q(D_q+1)}{\varphi(q)^{D_q}} \sum_{\substack{\boldsymbol{\nu}\in E_q(1)\\ \mathfrak{S}(\boldsymbol{\nu})=D_q-1}} \frac{1}{\prod_{j\in G_q}\nu_j!}.$$

2. Pour $x \geqslant 2$, nous notons $E(x) := |E \cap [1;x]|$ la fonction de comptage d'un ensemble d'entiers E.

Dans le cas $a \neq 1$, nous avons $\beta(a,q) = B(a,q)/\varphi(q)$, où $B(a,q)$ est le cardinal du plus grand sous-groupe de G_q ne contenant pas $a \pmod q$ $(0 < \beta(a,q) < 1)$, $\alpha(a,q)$ est une constante qui dépend aussi de ce sous-groupe, et $C(a,q)$ est défini par une formule explicite reposant également sur la théorie des groupes et faisant intervenir l'ensemble $E_q(a)$.

L'outil principal utilisé par [40] est la méthode de Delange développée par ce dernier en 1956 dans [7]. Le cas $a = 1$ se distingue des autres cas à cause de la finitude de l'ensemble $E_q(1)$, ce qui permet d'appliquer directement cette méthode pour obtenir le résultat. L'idée de départ pour les autres cas consiste, en notant $\mathfrak{H}(a)$ l'ensemble des sous-groupes de G_q ne contenant pas $a \pmod q$ et

$$\Omega_j(n) := \sum_{\substack{p^\nu \parallel n \\ p \equiv j \pmod q}} \nu \qquad (j \in G_q),$$

à subdiviser $\mathcal{N}$ en sous-ensembles

$$\mathcal{N}_H(\boldsymbol{\nu}) := \big\{n : \ \Omega_j(n) = \nu_j \ (j \notin H)\big\}$$

avec $H \in \mathfrak{H}(a)$ et $\boldsymbol{\nu} = (\nu_j)_{j \in G_q} \in E_q(a)$ tel que $\nu_j = 0$ si $j \in H$. On utilise ensuite la méthode de Delange pour chacun de ces sous-ensembles. Le terme principal de l'estimation de $\mathcal{N}(x)$ provient des sous-groupes H dont le cardinal est le plus grand possible. La démonstration se conclut grâce à l'utilisation de notions de théorie des groupes, en particulier avec les p-groupes. Cependant, les dernières lignes du paragraphe 6 de l'article de [40] sont très peu détaillées. La fin de la démonstration est peu convaincante. En outre, l'expression de $C(a,q)$ se révèle particulièrement absconse.

1.3.2. Les nouveaux résultats

Dans la première partie de cette thèse, nous faisons une étude plus approfondie de l'estimation de $\mathcal{N}_{a,q}(x)$. De plus, nous obtenons également une formulation simplifiée de $C(a,q)$, ne reposant plus sur la théorie des groupes, ainsi qu'un terme d'erreur dans (1.1.2) qui est plus explicite car proposant un développement asymptotique selon les puissances négatives de $\log_2 x$. Ceci dévoile un terme d'erreur plus précis que celui de [40]. Enfin, nous fournissons une preuve complète de l'estimation de $\mathcal{N}_{a,q}(x)$.

Pour cela, nous utilisons certaines notations semblables à celles de Narkiewicz et Radziejewski en recourant aux outils de l'analyse complexe plutôt qu'à ceux de la théorie des groupes. Ainsi, nous posons

$$\begin{aligned} H_q &:= [\![0;\varphi(q)]\!]^{G_q} = \big\{\boldsymbol{\nu} = (\nu_j)_{j\in G_q} : 0 \leqslant \nu_j \leqslant \varphi(q) \ (j \in G_q)\big\}, \\ H_q^* &:= H_q \smallsetminus \{\mathbf{0}\}, \\ \mathcal{E}_q(a) &:= H_q^* \cap E_q(a). \end{aligned}$$

L'ensemble $\mathcal{E}_q(a)$, qui est par définition un sous-ensemble fini de $E_q(a)$, joue dans notre démonstration un rôle similaire à ce dernier pour [40].

De plus, lorsque $\boldsymbol{\nu} \in \mathcal{E}_q(a)$, on dit qu'un élément j de G_q est une classe $\boldsymbol{\nu}$-complète si $\nu_j = \varphi(q)$; on note

$$I_q(\boldsymbol{\nu}) := \big\{j \in G_q : \nu_j = \varphi(q)\big\}$$

l'ensemble des classes $\boldsymbol{\nu}$-complètes, $J_q(\boldsymbol{\nu})$ son complémentaire dans G_q, et

$$\mathsf{s}(\boldsymbol{\nu}) := \sum_{j \in J_q(\boldsymbol{\nu})} \nu_j.$$

Fixons d'abord a et q, et notons simplement $\mathcal{N}$ au lieu de $\mathcal{N}_{a,q}$. La première étape de la démonstration repose sur la propriété

$$n \in \mathcal{N} \Leftrightarrow \Big(\min\big\{\Omega_j(n), \varphi(q)\big\}\Big)_{j \in G_q} \in \mathcal{E}_q(a).$$

On en déduit une partition de $\mathcal{N}$ en une union finie de sous-ensembles $\mathcal{N}_{\boldsymbol{\nu}}$ où, pour $\boldsymbol{\nu} \in \mathcal{E}_q(a)$,

$$\mathcal{N}_{\boldsymbol{\nu}} := \Big\{n \geqslant 2 : \Omega_j(n) = \nu_j \text{ si } \nu_j < \varphi(q);\ \Omega_j(n) \geqslant \varphi(q) \text{ si } \nu_j = \varphi(q)\Big\}.$$

Une utilisation de la formule de Cauchy nous donne, pour $\boldsymbol{R} \in (\mathbb{R}^{+*})^{G_q}$ tel que $R_j > 1$ si $j \in I_q(\boldsymbol{\nu})$, l'expression

$$\mathcal{N}_{\boldsymbol{\nu}}(x) = \frac{1}{(2i\pi)^{\varphi(q)}} \oint_{\mathcal{C}(\mathbf{0};\boldsymbol{R})} T(x;\boldsymbol{z}) \frac{\mathrm{d}\boldsymbol{z}}{\wp(\boldsymbol{z},\boldsymbol{\nu})}$$

en posant, pour $\boldsymbol{z} \in \mathbb{C}^{G_q}$, $\mathrm{d}\boldsymbol{z} := \prod_{j \in G_q} z_j$, $\mathcal{C}(\mathbf{0},\boldsymbol{R}) := \prod_{j \in G_q} \big\{z_j \in \mathbb{C} : |z_j| = R_j\big\}$, $\wp(\boldsymbol{z},\boldsymbol{\nu}) := \prod_{j \in J_q(\boldsymbol{\nu})} z_j^{\nu_j+1} \prod_{j \in I_q(\boldsymbol{\nu})} \big\{z_j^{\varphi(q)}(z_j - 1)\big\}$, et

$$T(x;\boldsymbol{z}) := \sum_{n \leqslant x} \prod_{j \in G_q} z_j^{\Omega_j(n)}.$$

En étudiant $\mathcal{N}(x)$, les auteurs de [40] ont utilisé la méthode de Selberg-Delange décrite dans [7] en 1956. Pour obtenir une estimation de $T(x,\boldsymbol{z})$, nous utilisons ici la même méthode dans une version améliorée, due à Tenenbaum [57, chapitre II.5], qui fournit

$$T(x;\boldsymbol{z}) = x(\log x)^{\sum_{j \in G_q} z_j/\varphi(q)-1} \Big\{ \sum_{0 \leqslant m \leqslant N} \frac{\lambda_m(\boldsymbol{z})}{(\log x)^m} + O\Big(\frac{1}{(\log x)^{N+1}}\Big)\Big\}.$$

où λ_m est une fonction indépendante de x et de N.

Nous pouvons alors nous intéresser à l'estimation des quantités

$$\mathcal{N}_{\boldsymbol{\nu}}^{(m)}(x) := \frac{x}{(2i\pi)^{\varphi(q)}(\log x)^{1+m}} \oint_{\mathcal{C}(\mathbf{0},\boldsymbol{R})} (\log x)^{\sum_{j \in G_q} z_j/\varphi(q)} \lambda_m(\boldsymbol{z}) \frac{\mathrm{d}\boldsymbol{z}}{\wp(\boldsymbol{z},\boldsymbol{\nu})} \quad \big(m \in \mathbb{N}\big).$$

Lorsque $m = 0$, l'apport du contour de Hankel [57, théorème II.0.17] dans cette estimation permet de simplifier certains calculs. Toutefois, l'application de ce contour diffère selon que $I_q(\boldsymbol{\nu})$ soit vide ou non. Enfin, une utilisation adéquate des formules

de Cauchy et de Leibniz permettent d'obtenir une estimation très précise de $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$. L'utilisation des mêmes propriétés lorsque $m > 0$ permettent également d'obtenir une estimation de $\mathcal{N}_{\boldsymbol{\nu}}^{(m)}(x)$ dans ce cas, mais avec moins de précisions. Nous pouvons alors obtenir un développement asymptotique convenable de $\mathcal{N}_{\boldsymbol{\nu}}(x)$, et donc de $\mathcal{N}(x)$ après avoir réordonné les termes, et en gardant en terme principal les $\mathcal{N}_{\boldsymbol{\nu}}(x)$ tels que $I_q(\boldsymbol{\nu})$ soit maximal.

Ainsi, en posant

$$\begin{aligned}
&\mathfrak{I}(a) := \max\big\{|I_q(\boldsymbol{\nu})| : \boldsymbol{\nu} \in \mathcal{E}_q(a)\big\},\\
&\mathfrak{s}(a,k) := \max\big\{\mathfrak{s}(\boldsymbol{\nu}) : |I_q(\boldsymbol{\nu})| = k\big\} \quad (0 \leqslant k \leqslant \mathfrak{I}(a)),\\
&\mathfrak{K}_a := \mathfrak{s}(a, \mathfrak{I}(a)),\\
&d_k(a) := \max_{0\leqslant\ell\leqslant k}\big\{\mathfrak{s}(a,\mathfrak{I}(a)-\ell) + (\varphi(q)-1)(k-\ell)\big\},
\end{aligned}$$

et en introduisant les quantités

$$\Xi(a) := \frac{1}{\Gamma\big(\mathfrak{I}(a)/\varphi(q)\big)\varphi(q)^{\mathfrak{K}_a}} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(a)\\ |I_q(\boldsymbol{\nu})|=\mathfrak{I}(a)\\ \mathfrak{s}(\boldsymbol{\nu})=\mathfrak{K}_a}} \frac{C_q(\boldsymbol{\nu})}{\boldsymbol{\nu}!} \qquad \big(1 < a \leqslant q,\, (a,q)=1\big),$$

avec

$$C_q(\boldsymbol{\nu}) := \Big(\frac{q}{\varphi(q)}\Big)^{|J_q(\boldsymbol{\nu})|/\varphi(q)} \prod_{j\in I_q(\boldsymbol{\nu})} \prod_{\chi\neq\chi_0} \mathscr{L}(\chi)^{\overline{\chi(j)}/\varphi(q)}$$

où

$$\mathscr{L}(\chi) := \prod_p \Big(1-\frac{1}{p}\Big)^{-\chi(p)},$$

et

$$\Xi(1) := \frac{q\mathfrak{K}_1}{\varphi(q)^{\mathfrak{K}_1+1}} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(1)\\ \mathfrak{s}(\boldsymbol{\nu})=\mathfrak{K}_1}} \frac{1}{\boldsymbol{\nu}!},$$

nous pouvons énoncer le résultat principal de notre première partie.

Théorème 0.0.1. *Soient $q \geqslant 3$, $a \geqslant 1$, $(a,q) = 1$, $N \in \mathbb{N}$. Il existe un entier $M = M_q$ tel que l'on ait, pour $x \geqslant 3$,*

(0.0.3)
$$\mathcal{N}_{a,q}(x) = \frac{x}{(\log x)^{1-\mathfrak{I}(a)/\varphi(q)}}\bigg\{\sum_{0\leqslant m\leqslant N}\sum_{0\leqslant k\leqslant\mathfrak{I}(a)} \frac{\mathfrak{P}_{m,k}(\log_2 x)}{(\log x)^{m+k/\varphi(q)}} + O\bigg(\frac{(\log_2 x)^M}{(\log x)^{N+1}}\bigg)\bigg\}.$$

où $\mathfrak{P}_{m,k}$ est un polynôme de degré au plus égal à $d_k(a)$ lorsque $a > 1$ et à $d_0(1) - 1$ lorsque $a = 1$, avec égalité dans les deux cas si $m = k = 0$.

En particulier :

(i) *Si $1 < a < q$, alors $\mathfrak{I}(a) > 0$, et le terme principal de* (0.0.3) *vaut*

$$\frac{\Xi(a)x(\log_2 x)^{\mathfrak{K}_a}}{\boldsymbol{\nu}!(\log x)^{1-\mathfrak{I}(a)/\varphi(q)}},$$

(ii) *Si* $a = 1$, *alors* $\mathfrak{I}(1) = 0$, $\mathfrak{K}_1 > 0$, *et le terme principal de* (0.0.3) *vaut*

$$\frac{\Xi(1)x(\log_2 x)^{\mathfrak{K}_a-1}}{\boldsymbol{\nu}!\log x}\cdot$$

Prenons un exemple avec le cas $q = 10$. Nous avons alors $G_q = \{1, 3, -3, -1\}$, et le Théorème 1.4.1 nous donne

$$\begin{aligned}\mathcal{N}_{3,10}(x) &= \mathcal{N}_{-3,10}(x) \sim c_1\frac{x}{\sqrt{\log x}},\\ \mathcal{N}_{-1,10}(x) &\sim c_2\frac{x(\log_2 x)^2}{(\log x)^{3/4}},\\ \mathcal{N}_{1,10}(x) &\sim c_3\frac{x(\log_2 x)^2}{\log x}\cdot\end{aligned}$$

avec $c_1 \approx 0,78439$, $c_2 \approx 0,03045$ et $c_3 \approx 3,91463$.

1.4. Conséquences

En étudiant quelques cas particuliers où q est petit, une question s'est vite posée : les éléments a dont l'estimation $\mathcal{N}_{a,q}(x)$ est la plus grande vérifient-ils une propriété commune ?

La réponse s'est rapidement orientée vers les non résidus quadratiques modulo q, c'est-à-dire vers les entiers a tels qu'il n'existe aucun x vérifiant $x^2 \equiv a \pmod q$.

Le corollaire suivant, qui se déduit du Théorème 1.4.1 grâce à des notions élémentaires de théorie des groupes, donne un ordre de grandeur de $\mathcal{N}_{a,q}(x)$ lorsque a vérifie cette propriété.

Corollaire 0.0.2. *Un entier* a *est non résidu quadratique modulo* q *si, et seulement si,* $\mathfrak{I}(a) = \varphi(q)/2$. *Dans ce cas, nous avons* $\mathfrak{K}_a = 0$ *et, pour* x *assez grand,*

$$\mathcal{N}_{a,q}(x) \asymp \frac{x}{\sqrt{\log x}}\cdot$$

De plus, dans le cas où G_q *est cyclique et si* a *et* b *sont deux non résidus quadratiques modulo* q, *nous avons*

$$\mathcal{N}_{a,q}(x) \sim \mathcal{N}_{b,q}(x) \qquad (x \to \infty).$$

Le corollaire se vérifie pour l'exemple $q = 10$ vu précédemment puisque 3 et -3 sont les seuls non résidus quadratiques modulo 10.

Dans un autre registre, une relecture de la démonstration du Théorème 1.4.1 permet d'observer que remplacer l'entier a de G_q par un ensemble d'éléments de G_q dans cette démonstration demandait très peu de modifications ; aussi un second résultat peut rapidement se déduire de cette démonstration modifiée, et permet d'étendre le Théorème 1.4.1 aux entiers sans diviseur dans un ensemble fini $\boldsymbol{a} = \{a_1, \dots, a_k\}$ d'éléments de G_q. L'énoncé obtenu dans ce cas est identique à celui d'une seule classe, si ce n'est en faisant quelques adaptations dans les notations, notamment en y remplaçant la valeur a par l'ensemble $\boldsymbol{a}$, et en distinguant ici les cas $1 \in \boldsymbol{a}$ et $1 \notin \boldsymbol{a}$. Ce nouveau résultat implique alors une estimation de la fonction de comptage de l'ensemble des entiers dont tous les diviseurs sont des résidus quadratiques modulo q.

Le cas particulier $\boldsymbol{a} = G_q\backslash\{1\}$ permet de retrouver le résultat (0.0.2).

2. Ultrafriables en progression arithmétique

Dans la seconde partie de cette thèse, nous nous penchons sur l'étude de l'ensemble de deux quantités liées aux entiers y-ultrafriables, qui sont les éléments de l'ensemble

$$U(y) := \{n : \ p^k \mid n \Rightarrow p^k \leqslant y\} \qquad (y > 0). \tag{0.0.4}$$

Ces éléments forment un sous-ensemble des entiers y-friables, ces derniers constituant l'ensemble

$$S(y) := \{n : \ p \mid n \Rightarrow p \leqslant y\} \qquad (x > 0,\, y > 0), \tag{0.0.5}$$

qui ont déjà fait l'objet d'une abondante littérature.

2.1. Théorèmes de Siegel-Walfisz et Bombieri-Vinogradov et zéro de Siegel

Le problème de l'équirépartition des entiers dans une progression arithmétique donnée a été résolue avec la formule (0.0.1), qui utilisait la quantité $\pi(x; a, q)$. Cependant, dans les problèmes de théorie des nombres impliquant les progressions arithmétiques, les mathématiciens privilégient en général, à la place de $\pi(x; a, q)$, la fonction

$$\psi(x; a, q) := \sum_{\substack{n \leqslant x \\ n \equiv a \,(\mathrm{mod}\ q)}} \Lambda(n),$$

où la quantité $\Lambda(n)$ vaut $\log p$ lorsque n est une puissance d'un nombre premier p et 0 sinon. En effet, la fonction $\psi(x; a, q)$ est plus simple à exploiter que $\pi(x; a, q)$. La formule (0.0.1) est par ailleurs équivalente à l'expression

$$\psi(x; a, q) \sim \frac{x}{\varphi(q)} \quad (x \to \infty). \tag{0.0.6}$$

Deux résultats célèbres en théorie analytique des nombres concernent l'estimation de la quantité $\psi(x; a, q)$. Nous utiliserons ici les formules énoncées dans [57].

Le premier de ces résultats, démontré en 1936 par Walfisz [60] d'après un résultat de Siegel [51], donne une majoration du terme d'erreur de (0.0.6).

Théorème (Siegel-Walfisz)**.** *Pour toute constante $A > 0$ et uniformément pour $x \geqslant 3$, $1 \leqslant q \leqslant (\log x)^A$ et $(a, q) = 1$, il existe $c = c(A) > 0$ telle qu'on a*

$$\psi(x; a, q) = \frac{x}{\varphi(q)} + O\big(x\mathrm{e}^{-c\sqrt{\log x}}\big). \tag{0.0.7}$$

La difficulté de la question de l'uniformité en q dans l'énoncé précédent provient principalement de l'existence ou non d'un éventuel "zéro de Siegel". Cet élément est défini par la propriété suivante, démontrée par Landau en 1918 [34].

Théorème. *Il existe une constante absolue $c > 0$ telle que la région $\{s \in \mathbb{C} : \ \sigma > 1 - c/\log(q(|\tau| + 2))\}$ contienne au plus un zéro de $\prod_{\chi \,(\mathrm{mod}\ q)} L(s, \chi)$. Dans ce cas, l'éventuel zéro exceptionnel, appelé zéro de Siegel, est réel, simple, et correspond à un caractère réel.*

Le second résultat, basé sur les travaux de Bombieri [2] et Vinogradov [59], donne une estimation de (0.0.7) en moyenne.

Théorème (Bombieri-Vinogradov)**.** *Pour toute constante $A > 0$, on a uniformément pour $Q \geqslant 1$, $x \geqslant 1$,*

$$\sum_{q\leqslant Q} \max_{\substack{y\leqslant x\\(a,q)=1}} \Big|\psi(y;a,q) - \frac{y}{\varphi(q)}\Big| \ll \frac{x}{(\log x)^A} + \sqrt{x}Q\big(\log(Qx)\big)^4\big).$$

2.2. Entiers friables

Étant donné deux réels strictement positifs x et y, rappelons la notation $S(y)$ définie en (0.0.5). Nous notons alors $\Psi(x,y)$ la fonction de comptage de cet ensemble. Ces entiers jouent un rôle important en théorie algorithmique des nombres et en cryptographie, en particulier dans l'algorithme de factorisation $p-1$ de Pollard ou dans le problème du logarithme discret. On pourra se référer à l'exposé de Pomerance [43] à ce sujet.

Dickman [8], en étudiant $\Psi(x,y)$, obtient comme premier résultat $\Psi(x,y) \sim \rho(u)x$ où $u := \log x/\log y$ et ρ, nommée fonction de Dickman, est définie comme étant la solution du système

$$\begin{cases} \rho(u) = 1 & \text{si } 0 \leqslant u \leqslant 1,\\ u\rho'(u) + \rho(u-1) = 0 & \text{si } u > 1. \end{cases}$$

Ce résultat est ensuite amélioré par Hildebrand [26], qui obtient que, pour tout $\varepsilon > 0$, on a

$$\Psi(x,y) = x\rho(u)\Big\{1 + O_\varepsilon\Big(\frac{\log(u+1)}{\log y}\Big)\Big\} \quad \big(\exp\{(\log_2 x)^{5/3+\varepsilon}\} \leqslant y \leqslant x\big).$$

Saias [46], en précisant un résultat formulé par de Bruijn [4] et en reprenant sa définition de la quantité

$$\Lambda(x,y) := \begin{cases} x\displaystyle\int_0^{+\infty} \rho(u-v)\mathrm{d}\Big(\frac{\lfloor y^v\rfloor}{y^v}\Big) & \text{si } x \notin \mathbb{N},\\ \displaystyle\lim_{\substack{t\to x\\ t>x}} \Lambda(t,y) & \text{sinon,} \end{cases}$$

obtient la formule

$$\Psi(x,y) = \Lambda(x,y)\Big\{1 + O_\varepsilon\big(\exp\big\{-(\log y)^{3/5-\varepsilon}\big\}\big)\Big\}$$

dans le même domaine que Hildebrand.

Une autre estimation de $\Psi(x,y)$ a été formulée par Hildebrand et Tenenbaum [27] dans un domaine plus général pour x et y. L'outil principal utilisé pour la démonstration de cette estimation est la méthode du col, qui joue également un rôle fondamental dans les résultats que nous avons obtenus. Pour cela, nous pouvons noter $\zeta(s,y)$ la série de Dirichlet associée à $\Psi(x,y)$:

$$\zeta(s,y) := \sum_{P^+(n)\leqslant y} \frac{1}{n^s} = \prod_{p\leqslant y} \Big(1 - \frac{1}{p^s}\Big)^{-1} \qquad (\Re e\ s > 0).$$

La formule de Perron (cf. [57], chapitre II.2.) permet de représenter $\Psi(x,y)$ sous la forme

$$\Psi(x,y)=\frac{1}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\zeta(s,y)x^s\frac{\mathrm{d}s}{s}\qquad(\alpha>0,x\notin\mathbb{N}).$$

À cet effet, le choix optimal de α correspond au point-selle $\alpha=\alpha(x,y)$, qui est défini comme étant l'unique solution de l'équation

$$\sum_{p\leqslant y}\frac{\log p}{p^\alpha-1}=\log x,$$

en remarquant que

$$-\frac{\zeta'(\alpha,y)}{\zeta(\alpha,y)}=\sum_{p\leqslant y}\frac{\log p}{p^\alpha-1}\cdot$$

L'expression de α peut être formulée par une estimation explicite : pour $u\geqslant 1$, si on définit $\xi=\xi(u)$ comme étant l'unique solution de l'équation $\mathrm{e}^\xi=1+u\xi$ et $\xi(1):=0$, les études faites sur α [27] fournissent, pour tout $\varepsilon>0$,
(0.0.8)

$$\alpha(x,y)=\begin{cases}1-\dfrac{\xi(u)}{\log y}+O\Big(\mathrm{e}^{-(\log y)^{3/5-\varepsilon}}+\dfrac{1}{u(\log y)^2}\Big) & \big((\log x)^{1+\varepsilon}\leqslant y\leqslant x\big),\\[2ex] \dfrac{\log(1+y/\log x)}{\log y}\Big\{1+O\Big(\dfrac{1}{\log y}\Big)\Big\} & \big(2\leqslant y\leqslant(\log x)^3\big).\end{cases}$$

De plus, nous posons

$$\phi_2(s,y):=\sum_{p\leqslant y}\frac{p^s(\log p)^2}{(p^s-1)^2}\qquad(\Re e\ s>0).$$

La fonction $s\mapsto\phi_2(s,y)$ est la dérivée seconde de $s\mapsto\log(\zeta(s,y))$. Hildebrand et Tenenbaum obtiennent la formule

$$\Psi(x,y)=\frac{x^\alpha\zeta(\alpha,y)}{\alpha\sqrt{2\pi\phi_2(\alpha,y)}}\Big\{1+O\Big(\frac{1}{u}+\frac{\log y}{y}\Big)\Big\}\qquad(x\geqslant y\geqslant 2).$$

On pourra trouver une présentation plus complète de l'étude de $\Psi(x,y)$ dans les synthèses de Hildebrand & Tenenbaum [28], Granville [21] ou Dartyge [3].

2.3. Entiers friables en progressions arithmétiques

Étant donné un entier $q\geqslant 2$, on pose $\Psi_q(x,y)$ la fonction de comptage des éléments de $S(y)$ qui sont premiers à q et $\Psi(x,y;a,q)$ celle des éléments de $S(y)$ qui sont congrus à a modulo q.

La quantité $\Psi_q(x,y)$ a été étudiée principalement par La Bretèche et Tenenbaum [6], qui ont utilisé également la méthode du col avec le même point-col α que pour $\Psi(x,y)$. Ils ont aussi fait une étude de la fonction $f_q(s):=\prod_{p|q}(1-p^{-s})$ définie sur $\Re e\ s>0$ pour obtenir

$$\Psi_q(x,y)=f_q(\alpha)\Psi(x,y)\{1+O(E)\}\qquad(x\geqslant y\geqslant 2,\ P^+(q)\leqslant y,\ \omega(q)\ll\sqrt{y})$$

où $E = E(x,y)$ dépend de conditions précises sur q.

Quand à la quantité $\Psi(x,y;a,q)$, elle a d'abord été étudiée par Fouvry-Tenenbaum [17] lorsque y est suffisamment grand afin d'obtenir un résultat de type Siegel-Walfisz pour les friables, et cela en étudiant d'abord la quantité

$$\Psi(x,y;\chi) := \sum_{n\in S(x,y)} \chi(n)$$

lorsque χ est un caractère modulo q non principal. En notant

$$Y := \mathrm{e}^{\sqrt{\log y}}, \quad H(u) := \exp\Big(\frac{u}{\log^2(u+1)}\Big)$$

et en fixant $A > 0$, ils obtiennent qu'il existe $c_0, c_1, \dots$ des constantes strictement positives dépendant au plus de A telles que, sous la condition

$$\exp\big(c_0(\log_2 x)^2\big) \leqslant y \leqslant x, \tag{0.0.9}$$

on ait les majorations

$$\Psi(x,y;\chi) \ll Y^{-c_1}$$

lorsque $1 < q \leqslant (\log x)^A$, et

$$\Psi(x,y;\chi) \ll \Psi(x,y)\Big\{Y^{-c_2} + y^{-c_3/\log q} + \vartheta(\chi)\frac{\log q}{\log y}H(u)^{-c_3}\Big\}$$

lorsque $(\log x)^A < q \leqslant y^{c_4/\log_2 x}$, où $\vartheta(\chi)$ vaut 1 pour un caractère exceptionnel et 0 pour les $\varphi(q)-2$ autres caractères. La propriété d'orthogonalité des caractères fournit alors, sous la même condition (0.0.9),

$$\frac{\Psi(x,y;a,q)}{\Psi_q(x,y)/\varphi(q)} - 1 \ll \begin{cases} Y^{-c_4} & \big(1 < q \leqslant (\log x)^A\big), \\ Y^{-c_4} + \dfrac{q\log q}{\varphi(q)\log y}H(u)^{-c_3} & \big((\log x)^A < q \leqslant Y^{c_4}\big) \end{cases}$$

La différence de l'estimation du terme d'erreur selon les valeurs de q provient de l'existence de l'éventuel zéro de Siegel.

Soundararajan [52] puis Harper [25] ont obtenu que l'estimation $\Psi(x,y;a,q) \sim \Psi_q(x,y)/\varphi(q)$ a lieu pour y et q assez grands, plus précisément pour $\varepsilon > 0$, $q \leqslant y^{4\sqrt{e}-\varepsilon}$ et $\exp(y^{1-\varepsilon}) \geqslant x \geqslant y^{(\log_2 y)^4}$.

Un résultat de type Bombieri-Vinogradov pour $S(y)$ a été obtenu par Fouvry et Tenenbaum [17, 18], puis amélioré par Drappeau [10] puis Harper [24]. Ce dernier a montré que, pour $c > 0$ et $K > 0$, nous avons, lorsque $(\log x)^K \leqslant y \leqslant x$ est suffisamment grand et $1 \leqslant Q \leqslant \sqrt{\Psi(x,y)}$,

$$\sum_{q\leqslant Q}\max_{(a,q)=1}\Big|\Psi(x,y;a,q) - \frac{\Psi_q(x,y)}{\varphi(q)}\Big| \ll \Psi(x,y)\Big(\mathrm{e}^{-cu/(\log(u+1))^2} + y^{-c}\Big) + \sqrt{\Psi(x,y)}Q(\log x)^{7/2},$$

où la constante implicite est absolue.

2.4. Entiers ultrafriables

À présent, pour $x > 0$ et $y > 0$, nous rappelons la notation $U(y)$ définie en (0.0.4) et notons $\Upsilon(x, y)$ sa fonction de comptage.

Ces entiers trouvent une application en théorie des graphes, comme le montre le récent article de Sander [49].

La quantité $\Upsilon(x, y)$ a été étudiée en 2015 par Tenenbaum [58] en utilisant la méthode du col. Pour cela, si on définit $\nu_p := \lfloor \log y/\log p \rfloor$ pour tout nombre premier $p \leqslant y$ et $\psi(y) := \psi(y; 1, 1) = \sum_{p\leqslant y} \nu_p \log p$ la fonction de Tchebychev, on peut restreindre le domaine d'étude à $\psi(y) > 2\log x$. Après avoir défini $s \mapsto Z(s, y)$ comme étant la fonction de Dirichlet associée à la fonction de comptage de $\Upsilon(x, y)$, c'est-à-dire

$$Z(s, y) := \prod_{p\leqslant y} \frac{1 - p^{-(\nu_p+1)s}}{1 - p^{-s}} \qquad (\Re e\ s > 0),$$

on peut alors définir le point-col $\beta = \beta(x, y)$ comme étant l'unique solution de l'équation $\varphi_1(\beta, y) = 0$, où

$$\varphi_1(s, y) := -\frac{Z'(s, y)}{Z(s, y)} = \sum_{p\leqslant y} \Big\{ \frac{\log p}{p^s - 1} - \frac{(\nu_p + 1)\log p}{p^{(\nu_p+1)s} - 1} \Big\} \qquad (\Re e\ s > 0,\ y \geqslant 2).$$

Comme pour α, le réel β peut être formulé par une estimation simple. D'abord, d'après [58], lorsque $(\log x)^{1+\varepsilon} \leqslant y \leqslant x$, l'estimation de β est la même que celle de α formulée dans (0.0.8), et lorsque $2\log x < \psi(y) \ll (\log x)^3$, la valeur de β se différencie de celle de α puisque dans ce domaine,

$$\beta = \frac{1 + O\big(1/\log y\big)}{\log y} \log\Big(\frac{\psi(y)}{\log x} - 1\Big).$$

Sous la condition $x \geqslant y \geqslant (\log x)^{2+\varepsilon}$ avec $\varepsilon > 0$, il y a très peu de variations entre $\Upsilon(x, y)$ et $\Psi(x, y)$ puisque, sous cette condition,

$$\Upsilon(x, y) = \Psi(x, y)\Big\{1 + O\Big(\frac{u\log(2u)}{\sqrt{y}\log y}\Big)\Big\}.$$

En posant, pour $y \geqslant 2$, $\sigma := \Re e\ s > 0$ et $z \in \mathbb{R}$,

$$\varphi_2(s, y) := -\frac{\mathrm{d}\varphi_1}{\mathrm{d}\sigma}(s, y), \quad \sigma_2 := \varphi_2(\beta, y), \quad G(z) := \frac{\mathrm{e}^{z^2/2}}{\sqrt{2\pi}} \int_z^\infty \mathrm{e}^{-t^2/2}\mathrm{d}t,$$

Tenenbaum obtient, grâce à la méthode du col, l'estimation

$$\Upsilon(x, y) = x^\beta Z(\beta, y) G(\beta\sqrt{\sigma_2})\Big\{1 + O\Big(\frac{1}{u}\Big)\Big\} \quad \big(2\log x < \psi(y) \ll (\log x)^3\big). \tag{0.0.10}$$

ainsi que les équivalences

$$\Upsilon(x, y) \sim \Psi(x, y) \Leftrightarrow y/(\log x)^2 \to \infty,$$
$$\Upsilon(x, y) = o\big(\Psi(x, y)\big) \Leftrightarrow y/(\log x)^2 \to 0.$$

2.5. Ultrafriables en progression arithmétique

Il apparait alors naturel de s'intéresser au comportement asymptotique des quantités

$$\Upsilon_q(x,y) := \sum_{\substack{n\in U(x,y)\\(n,q)=1}} 1, \qquad \Upsilon(x,y;a,q) := \sum_{\substack{n\in U(x,y)\\ n\equiv a \pmod q}} 1,$$

ce dont nous traitons dans le second chapitre de cette thèse.

Comme pour $\Upsilon(x,y)$, nous pouvons remarquer que l'estimation de $\Upsilon_q(x,y)$ est triviale lorsque $\psi(y) \leqslant \log x$, et dans le cas $\log x < \psi(y) \leqslant 2\log x$, cette estimation peut se déduire du domaine

$$\psi(y) > 2\log x. \tag{0.0.11}$$

Nous pouvons alors restreindre le domaine d'étude à (0.0.11), et un calcul simple permet également de montrer qu'il suffit de s'intéresser au cas $(a,q)=1$.

Le premier résultat obtenu dans cette étude nous donne une estimation de $\Upsilon_q(x,y)$ lorsque, pour $\varepsilon > 0$, nous avons

$$x \geqslant y \geqslant (\log x)^{2+\varepsilon}, \quad P^+(q) \leqslant y, \quad \omega(q) \ll \sqrt{y}. \tag{0.0.12}$$

La démonstration se base sur une majoration optimale de $\Psi_q(x,y) - \Upsilon_q(x,y)$, similaire à celle de la démonstration de (0.0.10). Plusieurs résultats de La Bretèche-Tenenbaum [6] y sont également utilisés.

Théorème 0.0.3. *Soit $\varepsilon > 0$. Sous les conditions* (0.0.12)*, nous avons*

$$\Upsilon_q(x,y) = \Psi_q(x,y)\biggl\{1 + O\Bigl(\frac{qu\log 2u}{\varphi(q)\sqrt{y}\log y}\Bigr)\biggr\}.$$

Notant p_k le k-ième nombre premier, de sorte que $p_k \asymp k\log 2k$ $(k \geqslant 1)$, et

$$z_q := p_{\omega(q)} \qquad (q \geqslant 1)$$

avec la convention $p_0 := 2$, nous posons ensuite

$$\eta = \eta(x,y) := \frac{\psi(y)}{\log x} - 2, \quad \vartheta_q = \vartheta_q(y) := \frac{\log z_q}{\log y} \asymp \frac{\log\{2+\omega(q)\}}{\log y} \quad (q \geqslant 1),$$

et introduisons les termes d'erreur $\Delta_q = \Delta_q(x,y)$ et $D_q = D_q(x,y)$ définis par

$$\Delta_q := \begin{cases} \dfrac{(\log x)^{\vartheta_q}}{\log y}\Bigl(1 + \dfrac{1}{\vartheta_q\log(1+\eta)}\Bigr) & \text{si } 2\log x < \psi(y) \ll (\log x)^2, \\[2ex] \dfrac{\vartheta_q\{u\log 2u\}^{\vartheta_q}}{1+\vartheta_q\log 2u} & \text{si } y > (\log x)^2, \end{cases}$$

et $D_q := \min\{\omega(q), \Delta_q\}$.

Posons également

$$g_q(s) := \prod_{p\,|\,q} \frac{1-p^{-s}}{1-p^{-(\nu_p+1)s}} \qquad (q \geqslant 1,\ s \in \mathbb{C}).$$

Afin d'obtenir une estimation de $\Upsilon_q(x,y)$ sur un domaine qui englobe $\psi(y) \leqslant (\log x)^3$ et avec des conditions optimales pour q, nous suivons un schéma similaire à celui qui permet de montrer le résultat principal de [58], en travaillant ici sur la série de Dirichlet associée à $\Upsilon_q(x,y)$, c'est-à-dire sur

$$Z_q(s,y) := \prod_{\substack{p\leqslant y\\ p\nmid q}} \frac{1-p^{-(\nu_p+1)s}}{1-p^{-s}} \quad (\Re e\ s>0),$$

tout en utilisant le même point col β que $\Upsilon(x,y)$.

Pour cela, nous avons d'abord recours à une application de la première formule de Perron effective (cf. [57], thm. II.2.3.) à $\Upsilon_q(x,y)$. Nous pouvons ensuite obtenir des majorations convenables des quantités $|Z_q(\beta+i\tau,y)/Z_q(\beta,y)|$ et $\Upsilon_q(x+x/z,y)-\Upsilon_q(x,y)$, en adaptant les conditions sur $|\tau|$ et z, et les appliquer à l'intégrale de Perron obtenue précédemment. L'estimation principale de $\Upsilon_q(x,y)$ donnée dans le résultat ci-dessous se déduit finalement d'une majoration convenable des termes d'erreur obtenus, ainsi que d'une adaptation aux entiers ultrafriables des lemmes 3.13 à 3.15 de [6].

Lorsque $\psi(y)$ est très proche de $2\log x$, un recours aux développements limités permet d'affiner les termes principaux de notre estimation.

Théorème 0.0.4. *Soit $\varepsilon>0$. Sous les conditions*

$$x\geqslant y\geqslant 2,\quad x>x_0,\quad 2\log x<\psi(y)\leqslant \exp\big((\log x)^{1/5}/(\log_2 x)^{(1+\varepsilon)/5}\big),$$
$$q\geqslant 1,\quad P^+(q)\leqslant y,\quad \omega(q)\ll y^{1/2-(1+\varepsilon)(\log_2 u)/\log u},$$

les assertions suivantes sont valides.

(i) *Nous avons*

$$\begin{aligned}\Upsilon_q(x,y)&=g_q(\beta)\Upsilon(x,y)\Big\{1+O\Big(\frac{1+D_q^2}{u}+\frac{D_q(1+\eta)}{\sqrt{u}+\eta u}\Big)\Big\}\\ &=x^\beta Z_q(\beta,y)G(\beta\sqrt{\sigma_2})\Big\{1+O\Big(\frac{1+D_q^2}{u}+\frac{D_q(1+\eta)}{\sqrt{u}+\eta u}\Big)\Big\},\end{aligned}$$

et donc, lorsque $\eta\gg 1$,

$$\Upsilon_q(x,y)=g_q(\beta)\Upsilon(x,y)\Big\{1+O\Big(\frac{1+\Delta_q^2}{u}\Big)\Big\}.$$

(ii) *Si de plus $\eta\leqslant\frac12$, alors*

$$\Upsilon_q(x,y)=g_q(\beta)\Upsilon(x,y)\Big\{1+R+O\Big(\frac{1+\omega(q)^2}{u}\Big)\Big\}$$

avec $R\asymp \omega(q)(1+\eta)/\big(\sqrt{u}+\eta u\big)$.

(iii) *Sous la condition supplémentaire $\eta=o\big(1/\sqrt{u}\big)$, nous avons*

$$\Upsilon_q(x,y)=g_q(\beta)\Upsilon(x,y)\Big\{1+\frac{\omega(q)}{\sqrt{\pi u}}+O\Big(\eta\omega(q)+\frac{\log q}{\sqrt{u}\log y}+\frac{\omega(q)^2}{u}\Big)\Big\}.$$

Les autres résultats portent sur l'estimation de $\Upsilon(x,y;a,q)$ dont le terme principal est $\Upsilon_q(x,y)/\varphi(q)$ pour obtenir un résultat de type Siegel-Walfisz. Il s'agit pour cela d'obtenir d'abord une majoration de la quantité

$$\Upsilon(x,y;\chi) := \sum_{n\in U(x,y)} \chi(n)$$

avec des conditions optimales sur y, pour χ un caractère modulo q distinct du caractère principal. Cette quantité est un outil fondamental de l'étude de $\Upsilon(x,y;a,q)$.

Une nouvelle utilisation de la première formule de Perron effective pour $\Upsilon(x,y;\chi)$ nécessite de travailler avec sa série de Dirichlet associée, c'est-à-dire avec

$$Z(s,\chi;y) := \prod_{p\leqslant y} \frac{1-\chi(p)^{\nu_p+1}p^{-(\nu_p+1)s}}{1-\chi(p)p^{-s}},$$

notamment en donnant une majoration de $|Z(s,\chi;y)/Z_q(\beta,y)|$. Cela nous ramène à trouver une minoration de la quantité

$$\mathbb{D}(y,\tau;\chi) := \sum_{p\leqslant y} \frac{(1-\Re e(\chi(p)p^{-i\tau}))\log p}{p^\beta}.$$

Cette minoration est possible grâce à l'utilisation du théorème d'Abel et à l'étude de

$$S(y,\tau;\chi) := \sum_{n\leqslant y} \frac{\chi(n)\Lambda(n)}{n^{\beta+i\tau}}$$

où Λ désigne la fonction de Van Mangoldt. L'étude de cette quantité se fait en utilisant à nouveau la première formule de Perron effective puis en appliquant le théorème des résidus grâce à un déplacement du segment d'intégration de l'intégrale de Perron, ce segment étant choisi en tenant compte des propriétés relatives à la région de Vinogradov-Korobov. La difficulté principale de l'estimation de $S(y,\tau;\chi)$ réside dans l'existence de l'éventuel zéro de Siegel. Notant

$$Y_\varepsilon = Y_\varepsilon(y) := \mathrm{e}^{(\log y)^{3/2-\varepsilon}} \quad (\varepsilon>0, y\geqslant 2),$$

nous obtenons finalement le résultat suivant.

Théorème 0.0.5. *Soit $A>0$. Pour $\varepsilon>0$, $c_1>0$, $c_2>0$ assez petits, sous les conditions*

$$x\geqslant 2, \quad 2\log x < \psi(y) \leqslant \mathrm{e}^{(\log x)^\varepsilon}, \tag{0.0.13}$$

$$2\leqslant q\leqslant y^{c_1/\log_2 y}, \tag{0.0.14}$$

et pour tout caractère de Dirichlet χ de module q non principal, nous avons

$$\Upsilon(x,y;\chi) \ll \Upsilon_q(x,y)\Big\{\mathrm{e}^{-c_2u/\{1+\vartheta(\chi)(\log u)^4\}} + Y_\varepsilon^{-1}\Big\}$$

où $\vartheta(\chi)$ vaut 0 ou 1 et n'est non nul que si $q>(\log y)^A$ et χ est égal à un unique caractère réel exceptionnel.

Le résultat suivant, qui fournit une estimation de $\Upsilon(x,y;a,q)$ sous les conditions mentionnées dans le Théorème 0.0.5, découle directement du résultat précédent grâce à l'orthogonalité des caractères.

Théorème 0.0.6. *Soit $\varepsilon>0$. Sous les hypothèses* (0.0.13), (0.0.14) *et $(a,q)=1$, nous avons*

$$\Upsilon(x,y;a,q)=\frac{\Upsilon_q(x,y)}{\varphi(q)}\Big\{1+O\Big(\mathrm{e}^{-c_2u/(\log u)^4}+Y_\varepsilon^{-1}\Big)\Big\}. \tag{0.0.15}$$

En l'absence de caractère de Siegel modulo q, on peut substituer u à $u/(\log u)^4$ dans le terme d'erreur de (0.0.15).

Enfin, nous pouvons également établir une estimation de $\Upsilon(x,y;a,q)$ sur un domaine qui contient $y\geqslant \mathrm{e}^{(\log x)^\varepsilon}$ lorsque $\varepsilon>0$. L'idée principale de la démonstration est d'adapter le résultat de Granville [20] aux entiers ultrafriables.

Théorème 0.0.7. *Soit $\varepsilon>0$. Sous les conditions $x\geqslant y\geqslant(\log x)^{2+\varepsilon}$, $q\leqslant\sqrt{y}$, et $(a,q)=1$, il existe une constante $c>0$ telle que*

$$\Upsilon(x,y;a,q)=\frac{\Upsilon_q(x,y)}{\varphi(q)}\Big\{1+O\Big(\frac{\log q}{u^c\log y}+\frac{1}{\log y}\Big)\Big\}.$$

Le fait que la fonction indicatrice des ultrafriables ne soit pas complètement multiplicative ne permet pas en revanche de reprendre la démonstration de Granville pour avoir une estimation de type Siegel-Walfisz pour les ultrafriables dans un domaine plus général en x et y.

Chapitre 1

Cribler par une progression arithmétique

Sommaire

1.1 Contexte

Un résultat de Landau datant de 1909 [33], et dont une démonstration simplifiée a été fournie par Raikov en 1938 [44], stipule que, pour tout entier $q \geqslant 2$ fixé et tout résidu $a \pmod q$ tel que $(a,q)=1$, presque tous les entiers n'excédant pas x possèdent un facteur premier (et donc un diviseur) congru à a modulo q. De plus, ainsi qu'il a été remarqué dans [40], le résultat de Landau implique directement que, pour $q \geqslant 3$ fixé, le nombre $T(x;1,q)$ des entiers n'excédant pas x et dont tous les facteurs premiers, et donc tous les diviseurs, sont congrus à 1 modulo q, vérifie

$$T(x;1,q) = \frac{\{C_q + o(1)\}x}{(\log x)^{1-1/\varphi(q)}} \qquad (x \to \infty),$$

où l'on a posé

$$\begin{aligned} C_q &:= \frac{1}{\Gamma\big(1/\varphi(q)\big)} \lim_{s\to 1^+} \prod_{p\equiv 1 \pmod q} \Big(1-\frac{1}{p^s}\Big)^{-1}\Big(1-\frac{1}{s}\Big)^{1/\varphi(q)} \\ &= \frac{q}{\Gamma(1/\varphi(q))\varphi(q)} \prod_p \Big(1-\frac{1}{p}\Big)^{1/\varphi(q)}\Big(1-\frac{\vartheta(p)}{p}\Big)^{-1} > 0, \end{aligned} \tag{1.1.1}$$

avec

$$\vartheta(p) := \begin{cases} 1 & \text{si } p \equiv 1 \pmod q, \\ 0 & \text{dans le cas contraire.} \end{cases}$$

Erdős [12] a ensuite montré que, pour tout $\delta > 0$, lorsque x tend vers l'infini et $1 \leqslant q \leqslant (\log x)^{\log 2 - \delta}$, tous les entiers $n \leqslant x$ sauf au plus $o(x)$ exceptions ont au moins un diviseur dans chaque classe de congruence modulo q. De plus, il établit que la limitation relative au paramètre q est optimale, dans le sens où l'assertion est en défaut si l'on chosit $\delta < 0$.

Par la suite, l'ensemble exceptionnel, formé des entiers n'ayant aucun diviseur > 1 dans une réunion finie de progressions arithmétiques, a fait l'objet d'évaluations quantitatives. Une telle condition structurelle apparaît dans les théories algébrique et algorithmique des nombres. Ainsi, les entiers impairs, sans facteur carré et représentables comme somme de deux carrés n'admettent aucun diviseur congru à 3 modulo 4.

En 2008, Banks, Friedlander et Luca [1] ont donné une évaluation asymptotique, lorsque $q \geqslant 3$ est un nombre premier fixé, pour la taille de l'ensemble résiduel dans le crible par une unique progression arithmétique de module q. [1]

Trois ans plus tard, Narkiewicz et Radziejewski [40] ont généralisé ce résultat au cas où $q \geqslant 3$ est un entier quelconque. Ils ont ainsi établi que le nombre $N(x;a,q)$ des entiers n'excédant pas x et n'ayant aucun diviseur > 1 dans la classe résiduelle $a \pmod q$ telle que $(a,q)=1$ vérifie [2]

$$N(x;a,q) = \big\{C(a,q) + o(1)\big\}\frac{x(\log_2 x)^{\alpha(a,q)}}{(\log x)^{1-\beta(a,q)}} \tag{1.1.2}$$

1. Ici et dans la suite les progressions arithmétiques considérées sont constituées d'entiers > 1.
2. Ici et dans la suite, nous notons $\log_k$ la k-ième itérée de la fonction logarithme.

où $C(a,q) > 0$, $\alpha(a,q) > 0$ et $0 \leqslant \beta(a,q) < 1$. Ces trois constantes dépendent des propriétés du groupe multiplicatif $G_q := (\mathbb{Z}/q\mathbb{Z})^*$.

Il est à noter que les constantes sont plus faciles à expliciter lorsque $a = 1$. En effet, nous avons $\alpha(1,q) = D_q - 2$ où D_q désigne la constante de Davenport de G_q, définie comme le plus petit entier r tel que toute suite de r éléments de G_q contienne une sous-suite dont le produit des éléments est égal à 1 — voir notamment [41] pour une étude exhaustive de cette constante. De plus, $\beta(1,q) = 0$. Enfin, posant

$$\mathfrak{S}(\boldsymbol{\nu}) := \sum_{j\in G_q} \nu_j \qquad \big(\boldsymbol{\nu} \in \mathbb{N}^{G_q}\big),$$
$$E_q(a) := \Big\{\boldsymbol{\nu} \in \mathbb{N}^{G_q} : \boldsymbol{\mu} \in \mathbb{N}^{G_q},\, \boldsymbol{\mu} \preccurlyeq \boldsymbol{\nu}, \mathfrak{S}(\boldsymbol{\mu}) > 0 \Rightarrow \textstyle\prod_{j\in G_q} j^{\mu_j} \not\equiv a \pmod q\Big\},$$

où $\boldsymbol{\mu} \preccurlyeq \boldsymbol{\nu}$ signifie $\mu_j \leqslant \nu_j$ $(j \in G_q)$, nous avons

$$C(1,q) = \frac{q(D_q+1)}{\varphi(q)^{D_q}} \sum_{\substack{\boldsymbol{\nu}\in E_q(1)\\ \mathfrak{S}(\boldsymbol{\nu})=D_q-1}} \frac{1}{\prod_{j\in G_q}\nu_j!}.$$

Lorsque $a \neq 1$, nous avons $\beta(a,q) = B(a,q)/\varphi(q) > 0$, où $B(a,q)$ est le cardinal du plus grand sous-groupe de G_q ne contenant pas $a \pmod q$, $\alpha(a,q)$ est une constante qui dépend également de ce sous-groupe, et $C(a,q)$ est défini par une formule explicite issue de la théorie des groupes et faisant intervenir l'ensemble $E_q(a)$.

L'objectif de notre travail est non seulement d'obtenir, pour tous a, q fixés, une estimation de la fonction de comptage de l'ensemble [3]

$$\mathcal{N} = \mathcal{N}_{a,q} := \Big\{n \geqslant 2 :\ \big(d \mid n,\ d > 1\big) \Rightarrow d \not\equiv a \pmod q\Big\}$$

sous la forme (1.1.2), avec une formulation simplifiée des constantes ne reposant plus sur la théorie des groupes, mais aussi d'expliciter le terme d'erreur de (1.1.2) en proposant un développement asymptotique selon les puissances négatives de $\log_2 x$.

À cette fin, nous introduisons d'abord un sous-ensemble fini $\mathcal{E}_q(a)$ de $E_q(a)$ afin de représenter l'ensemble $\mathcal{N}$ comme une union disjointe de sous-ensembles $\mathcal{N}_{\boldsymbol{\nu}}$ de $\mathcal{N}$ définis par (1.4.8) *infra* et plus simples à étudier. Pour obtenir un développement asymptotique de chacun des $\mathcal{N}_{\boldsymbol{\nu}}(x)$, nous utilisons un théorème de type Selberg-Delange, plus précis que celui qui est utilisé dans [40]. Le gain de précision relativement à (1.1.2) est également renforcé par l'emploi du théorème de Hankel, qui permet d'avoir une simplification des calculs.

Nous verrons que le cas $a = 1$ est particulier et doit être traité séparément. Cela provient du fait que la condition $n \in \mathcal{N}_{1,q}$ implique que $\Omega(n)$ est borné en fonction de q seul, [4] alors que, pour $1 < a \leqslant q$, $\Omega(n)$ peut être arbitrairement grand pour $n \in \mathcal{N}_{a,q}$.

À la fin de ce travail, nous montrons comment une légère altération de la définition $\mathcal{E}_q(a)$ permet de généraliser notre résultat à l'ensemble des entiers n'admettant aucun

3. Afin de simplifier la rédaction, nous avons choisi d'exclure systématiquement l'élément $n = 1$ de l'ensemble $\mathcal{N}_{a,q}$.

4. Ici et dans la suite, nous désignons par $\Omega(n)$ le nombre total des facteurs premiers, comptés avec multiplicité, d'un entier n.

diviseur > 1 dans un ensemble fini de classes résiduelles modulo q. Cette extension fournit de nouvelles propriétés des entiers dont tous les diviseurs sont des résidus quadratiques.

1.2 Cas particuliers

Pour $x \geqslant 1$, nous notons $E(x) := \big|E\cap[1;x]\big|$ la fonction de comptage d'un ensemble d'entiers E.

Commençons par rappeler les résultats relatifs à certains cas particuliers étudiés dans [1] et [40]. Nous avons pour ces différents cas une estimation simple de $\mathcal{N}_{a,q}(x)$; en effet,

- si $q = 2$ et $a = 1$, nous avons
$$\mathcal{N}_{1,2}(x) = \frac{\log x}{\log 2} + O(1)$$
puisque $\mathcal{N}_{1,2}$ est l'ensemble des puissances de 2 ;
- si $a = 0$, alors
$$\mathcal{N}_{0,q}(x) = \Big(1 - \frac{1}{q}\Big)x + O(1)$$
étant donné que $\mathcal{N}_{0,q}$ est l'ensemble des entiers non divisibles par q ;
- si $d := (a,q) > 1$ et $a \neq 0$, en posant $q = dr$ et $a = db$, nous avons
$$\mathcal{N}_{a,q}(x) \;=\; \Big(1 - \frac{1}{d}\Big)x + \mathcal{N}_{b,r}\Big(\frac{x}{d}\Big) + O(1),$$
puisque $\mathcal{N}_{a,q} = \{n \in \mathbb{N}^* : d \nmid n\} \cup \{dm : m \in \mathcal{N}_{b,r}\}$.

Nous pouvons donc, sans perte de généralité, restreindre l'étude au cas $(a,q) = 1$.

1.3 Définitions et notations principales

Compte tenu de ce qui précède, nous pouvons supposer dans la suite $q \geqslant 3$ et $(a,q) = 1$. Ces entiers sont fixés une fois pour toutes.

Pour tous entiers naturels k, ℓ, $k \leqslant \ell$, nous notons $[\![k;\ell]\!]$ l'ensemble des entiers compris largement entre k et ℓ.

Lorsque s désigne un nombre complexe, σ et τ sont définis implicitement comme respectivement les parties réelle et imaginaire de s.

La fonction Gamma d'Euler est notée Γ.

Pour tout caractère de Dirichlet χ modulo q distinct du caractère principal χ_0, nous posons

$$\mathscr{L}(\chi) := \prod_p \Big(1 - \frac{1}{p}\Big)^{-\chi(p)}. \tag{1.3.1}$$

Ce produit infini est bien convergent. En effet, $L(1,\chi)$ est classiquement développable en produit eulérien convergent et le rapport du terme général à celui de (1.3.1) vérifie

$$\Big(1 - \frac{\chi(p)}{p}\Big)^{-1}\Big(1 - \frac{1}{p}\Big)^{\chi(p)} = 1 + O\Big(\frac{1}{p^2}\Big)$$

Les définitions et notations suivantes sont systématiquement employées dans la suite. On rappelle que G_q désigne le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$. Nous posons

$$\begin{aligned} &H_q := [\![0;\varphi(q)]\!]^{G_q} = \big\{\boldsymbol{\nu} = (\nu_j)_{j\in G_q} : 0 \leqslant \nu_j \leqslant \varphi(q)\ (j \in G_q)\big\},\\ &H_q^* := H_q \smallsetminus \{\mathbf{0}\}. \end{aligned} \tag{1.3.2}$$

Pour $\boldsymbol{z} := (z_j)_{j\in G_q} \in \mathbb{C}^{G_q}$, nous posons $\|\boldsymbol{z}\| := \max_{j\in G_q}|z_j|$ et $|\boldsymbol{z}| := (|z_j|)_{j\in G_q}$. Nous écrirons indifféremment $\|\boldsymbol{z}\| \ll 1$ ou $\boldsymbol{z} \ll 1$ pour signifier que $\boldsymbol{z}$ est borné.

Notation 1.3.1. *Pour tous entiers j, n tels que $(j,q) = 1$ et $n \geqslant 2$, nous notons $\Omega_j(n)$ le nombre total des facteurs premiers de n, comptés avec multiplicité, qui sont congrus à j modulo q, soit*

$$\Omega_j(n) := \sum_{\substack{p^\nu \| n\\ p\equiv j\,(\mathrm{mod}\,q)}} \nu.$$

Les notions d'a-admissibilité et de classe complète, décrites dans les définitions suivantes, jouent un rôle fondamental dans notre démonstration.

Définition et notation 1.3.2. *Nous posons $\mathcal{E}_q(a) := H_q^* \cap E_q(a)$ et désignons les éléments de $\mathcal{E}_q(a)$ comme* a-admissibles.

Définition et notation 1.3.3. *Soient $\boldsymbol{\nu} \in H_q^*$ et $j \in G_q$. On dit que j est une* classe $\boldsymbol{\nu}$-complète *si $\nu_j = \varphi(q)$.*

Nous notons

$$I_q(\boldsymbol{\nu}) := \big\{j \in G_q : \nu_j = \varphi(q)\big\} \tag{1.3.3}$$

l'ensemble des classes $\boldsymbol{\nu}$-complètes de G_q, posons $J_q(\boldsymbol{\nu}) := G_q \smallsetminus I_q(\boldsymbol{\nu})$ et introduisons la constante

$$C_q(\boldsymbol{\nu}) := \Big(\frac{q}{\varphi(q)}\Big)^{|J_q(\boldsymbol{\nu})|/\varphi(q)} \prod_{j\in I_q(\boldsymbol{\nu})}\prod_{\chi\neq\chi_0} \mathscr{L}(\chi)^{\overline{\chi(j)}/\varphi(q)} \tag{1.3.4}$$

Remarque 1.3.4. *Il est immédiat que $J_q(\boldsymbol{\nu}) \neq \varnothing$ pour tout $\boldsymbol{\nu}$ de $\mathcal{E}_q(a)$ puisque $\nu_a = 0$. Nous verrons en* (1.4.7) infra *que l'on a en fait $|J_q(\boldsymbol{\nu})| \geqslant \frac{1}{2}\varphi(q)$.*

Notation 1.3.5. *Pour $K \subseteq G_q$ et p premier, nous écrivons $p \in K$ si $p \in \cup_{j\in K}(j + q\mathbb{Z})$.*

Définition 1.3.6. *Soient $K \subseteq G_q$ et $\boldsymbol{t} \in H_q$. Nous définissons la K-*taille $\mathsf{s}_K(\boldsymbol{t})$ *de $\boldsymbol{t}$ par la formule*

$$\mathsf{s}_K(\boldsymbol{t}) := \sum_{j\in K} t_j. \tag{1.3.5}$$

La définition précédente servira principalement lorsque $K = J_q(\boldsymbol{\nu})$ avec $\boldsymbol{\nu} \in \mathcal{E}_q(a)$. Pour simplifier les écritures, nous posons alors

$$\mathsf{s}(\boldsymbol{t},\boldsymbol{\nu}) := \mathsf{s}_{J_q(\boldsymbol{\nu})}(\boldsymbol{t}) = \sum_{j\in J_q(\boldsymbol{\nu})} t_j \quad (\boldsymbol{t} \in H_q), \qquad \mathsf{s}(\boldsymbol{\nu}) := \mathsf{s}(\boldsymbol{\nu},\boldsymbol{\nu}). \tag{1.3.6}$$

Les notations suivantes permettront de simplifier l'écriture de certaines expressions.

Notations 1.3.7. *Pour $\boldsymbol{\nu} \in \mathcal{E}_q(a)$, $K \subseteq G_q$, $\boldsymbol{t} \in H_q$, $\boldsymbol{w} \in H_q$ vérifiant $\boldsymbol{t} \preccurlyeq \boldsymbol{w}$ et $(\boldsymbol{u}_m)_{1\leqslant m\leqslant k} \in H_q^k$ vérifiant $\boldsymbol{u}_m \preccurlyeq \boldsymbol{w}$ $(1 \leqslant m \leqslant k)$, nous posons*

$$\binom{\boldsymbol{w}}{\boldsymbol{t}} := \prod_{j\in G_q} \binom{w_j}{t_j}, \qquad \boldsymbol{\nu}! := \prod_{j\in J_q(\boldsymbol{\nu})} \nu_j!, \tag{1.3.7}$$

$$\binom{\boldsymbol{w}}{\boldsymbol{u}_1, \cdots, \boldsymbol{u}_m} := \prod_{j\in G_q} \binom{w_j}{u_{j,1}, \cdots, u_{j,m}} \tag{1.3.8}$$

$$\mathfrak{M}_K(\boldsymbol{w}) := \big\{\boldsymbol{t} \in H_q : 0 \leqslant t_j \leqslant w_j \ (j \in K),\ t_j = 0 \ (j \in G_q \smallsetminus K)\big\}, \tag{1.3.9}$$

$$\mathfrak{M}(\boldsymbol{w}, \boldsymbol{\nu}) := \mathfrak{M}_{J_q(\boldsymbol{\nu})}(\boldsymbol{w}), \tag{1.3.10}$$

$$\begin{aligned}\mathfrak{M}(\boldsymbol{\nu}) &:= \mathfrak{M}(\boldsymbol{\nu}, \boldsymbol{\nu})\\ &= \big\{\boldsymbol{t} \in H_q : 0 \leqslant t_j \leqslant \nu_j \ (j \in J_q(\boldsymbol{\nu})),\ t_j = 0 \ (j \in I_q(\boldsymbol{\nu}))\big\},\end{aligned} \tag{1.3.11}$$

$$\mathfrak{N}_K(\boldsymbol{t}) := \Big\{(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) \in \mathfrak{M}_K(\boldsymbol{t})^4 : \sum_{2\leqslant m\leqslant 4} \boldsymbol{u}_m \in \mathfrak{M}_K(\boldsymbol{u}_1)\Big\}, \tag{1.3.12}$$

$$\mathfrak{N}(\boldsymbol{\nu}) := \Big\{(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4) \in \mathfrak{M}(\boldsymbol{\nu})^4 : \sum_{2\leqslant m\leqslant 4} \boldsymbol{u}_m = \boldsymbol{u}_1\Big\}. \tag{1.3.13}$$

Remarque 1.3.8. *Si $K \subseteq G_q$, $\boldsymbol{w} \in H_q$, $\boldsymbol{t}, \boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in \mathfrak{M}_K(\boldsymbol{w})$, alors*

$$\binom{\boldsymbol{w}}{\boldsymbol{t}} = \prod_{j\in K} \binom{w_j}{t_j}, \qquad \binom{\boldsymbol{w}}{\boldsymbol{u}_1, \cdots, \boldsymbol{u}_k} = \prod_{j\in K} \binom{w_j}{u_{j,1}, \cdots, u_{j,k}}.$$

1.4 Résultats

Le résultat principal de ce travail est le suivant. Nous posons

$$\begin{aligned}&\mathfrak{I}(a) := \max\big\{|I_q(\boldsymbol{\nu})| : \boldsymbol{\nu} \in \mathcal{E}_q(a)\big\},\\ &\mathfrak{s}(a,k) := \max\big\{\mathsf{s}(\boldsymbol{\nu}) : |I_q(\boldsymbol{\nu})| = k\big\} \quad (0 \leqslant k \leqslant \mathfrak{I}(a)),\\ &\mathfrak{K}_a := \mathfrak{s}(a, \mathfrak{I}(a)),\\ &d_k(a) := \max_{0\leqslant\ell\leqslant k} \big\{\mathfrak{s}(a, \mathfrak{I}(a) - \ell) + (\varphi(q) - 1)(k - \ell)\big\},\end{aligned} \tag{1.4.1}$$

et, en rappelant la notation (1.3.4), introduisons la quantité

$$\Xi(a) := \frac{1}{\Gamma\big(\mathfrak{I}(a)/\varphi(q)\big)\varphi(q)^{\mathfrak{K}_a}} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(a)\\ |I_q(\boldsymbol{\nu})|=\mathfrak{I}(a)\\ \mathsf{s}(\boldsymbol{\nu})=\mathfrak{K}_a}} \frac{C_q(\boldsymbol{\nu})}{\boldsymbol{\nu}!} \qquad \big(1 < a \leqslant q,\ (a,q) = 1\big), \tag{1.4.2}$$

et posons

$$\Xi(1) := \frac{q\mathfrak{K}_1}{\varphi(q)^{\mathfrak{K}_1+1}} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(1)\\ \mathsf{s}(\boldsymbol{\nu})=\mathfrak{K}_1}} \frac{1}{\boldsymbol{\nu}!}.$$

Théorème 1.4.1. *Soient $q \geqslant 3$, $1 \leqslant a \leqslant q$, $(a,q) = 1$, $N \in \mathbb{N}$. Il existe un entier*

$$M = M_q \leqslant (\varphi(q) - 1)^{\varphi(q)}$$

tel que l'on ait, pour $x \geqslant 3$,

(1.4.3)
$$\mathcal{N}_{a,q}(x) = \frac{x}{(\log x)^{1-\mathfrak{I}(a)/\varphi(q)}}\Big\{ \sum_{0\leqslant m\leqslant N}\sum_{0\leqslant k\leqslant \mathfrak{I}(a)} \frac{\mathfrak{P}_{m,k}(\log_2 x)}{(\log x)^{m+k/\varphi(q)}} + O\Big(\frac{(\log_2 x)^M}{(\log x)^{N+1}}\Big)\Big\}.$$

où $\mathfrak{P}_{m,k}$ *est un polynôme de degré au plus égal à* $d_k(a)$ *lorsque* $a > 1$ *et à* $d_0(a) - 1$ *lorsque* $a = 1$, *avec égalité dans les deux cas si* $m = k = 0$.

En particulier :

(i) *si* $1 < a < q$, *alors* $\mathfrak{I}(a) > 0$, *et le terme principal de* (1.4.3) *vaut*

$$\frac{\Xi(a)x(\log_2 x)^{\mathfrak{K}_a}}{(\log x)^{1-\mathfrak{I}(a)/\varphi(q)}}. \tag{1.4.4}$$

(ii) *si* $a = 1$, *alors* $\mathfrak{I}(1) = 0$, $\mathfrak{K}_1 > 0$, *et le terme principal de* (1.4.3) *vaut*

$$\frac{\Xi(1)x(\log_2 x)^{\mathfrak{K}_1-1}}{\log x}. \tag{1.4.5}$$

Remarques 1.4.2. (i) Notre méthode permet de déterminer explicitement les coefficients de $\mathfrak{P}_{0,k}$ $(0 \leqslant k \leqslant \mathfrak{I}(a))$.

(ii) On peut vérifier que la constante apparaissant entre parenthèses dans le terme principal de (1.4.4) est identique à celle du résultat principal de [40] lorsque $a \neq 1$. De même, dans le cas $a = 1$, la constante de (1.4.5) et celle de [40] coïncident.

(iii) La constante implicite du terme d'erreur, disons $\mathfrak{R}$, de (1.4.3) peut dépendre des entiers q et N. Toutefois, le théorème II.5.2 de [57] permet de préciser que, pour des constantes convenables $c_1 > 0$, $c_2 > 0$, dépendant au plus de q, et uniformément pour $x \geqslant 3$, $N \in \mathbb{N}$, nous avons

$$\mathfrak{R} \ll (\log_2 x)^M\Big(\mathrm{e}^{-c_1\sqrt{\log x}} + \Big(\frac{c_2N+1}{\log x}\Big)^{N+1}\Big),$$

où la constante implicite ne dépend plus à présent que de q.

(iv) Nous verrons au Corollaire 1.4.11 *infra* que, sous certaines conditions explicites relatives à la classe a, la constante $C_q(\boldsymbol{\nu})$ est exprimable en fonction des seuls caractères de G_q.

L'énoncé du Théorème 1.4.1 met en évidence la disparité des cas $1 < a < q$ et $a = 1$ relativement à l'estimation asymptotique de $\mathcal{N}_{a,q}(x)$. L'origine de cette dichotomie provient du fait que $\mathfrak{I}(a) = 0$ si, et seulement si, $a = 1$. En effet :

Si $a = 1$, alors $I_q(\boldsymbol{\nu}) = \varnothing$ pour tout $\boldsymbol{\nu} \in \mathcal{E}_q$, puisque $j^{\varphi(q)} \equiv 1 \pmod q$ pour tout $j \in G_q$, et donc $\nu_j < \varphi(q)$. Ainsi $\mathfrak{I}(1) = 0$.

Si $1 < a < q$, $\boldsymbol{\nu}_0 := (\varphi(q), 0, \dots, 0)$ est a-admissible et $I_q(\boldsymbol{\nu}_0) \neq \varnothing$. Donc $\mathfrak{I}(a) > 0$.

Pour comparer l'énoncé du Théorème 1.4.1 et celui du théorème 5 de [40], dont la preuve repose sur la théorie des groupes, considérons l'ensemble

$$\mathfrak{H}(a) := \big\{H : H \text{ sous-groupe de } G_q,\ H \not\ni a\big\} \tag{1.4.6}$$

et nous notons $\mathfrak{H}^+(a)$ le sous-ensemble des éléments d'ordre maximal de $\mathfrak{H}(a)$.

Remarques 1.4.3 (Correspondance avec la théorie des groupes)**.**

(i) Lorsque $a \neq 1$ et $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ vérifie $|I_q(\boldsymbol{\nu})| = \mathfrak{I}(a)$, alors $I_q(\boldsymbol{\nu})$ est un sous-groupe non vide de G_q, et donc $\mathfrak{I}(a) \mid \varphi(q)$. En effet, d'une part, ainsi qu'il a été établi plus haut, l'hypothèse $a \neq 1$ implique $\mathfrak{I}(a) > 0$. D'autre part, pour tous j_1, j_2 de $I_q(\boldsymbol{\nu})$, $h \in G_q$ vérifiant $h \equiv j_1 j_2 \,(\mathrm{mod}\ q)$, et tout exposant μ, $0 \leqslant \mu \leqslant \varphi(q)$, nous avons

$$h^\mu \,(\mathrm{mod}\ q) = j_1^\mu j_2^\mu \,(\mathrm{mod}\ q) \in \Big\{ \prod_{j \in G_q} j^{\mu_j} \,(\mathrm{mod}\ q) : \boldsymbol{\mu} \in H_q^*,\ \mathbf{0} \preccurlyeq \boldsymbol{\mu} \preccurlyeq \boldsymbol{\nu} \Big\}.$$

Comme $|I_q(\boldsymbol{\nu})|$ est maximal, il s'ensuit que $\nu_h = \varphi(q)$ et donc $h \in I_q(\boldsymbol{\nu})$. De même, $(j^{-1})^\mu \equiv j^{\varphi(q)-\mu} (\mathrm{mod}\ q)$, ce qui implique $j^{-1} \in I_q(\boldsymbol{\nu})$.

De plus, $a \notin I_q(\boldsymbol{\nu})$, donc $I_q(\boldsymbol{\nu}) \in \mathfrak{H}^+(a)$.

(ii) Puisque $\mathfrak{I}(a) < \varphi(q)$ pour tout $a \in G_q$, il résulte en particulier de ce qui précède que

$$\mathfrak{I}(a) \leqslant \tfrac{1}{2}\varphi(q) \qquad (a \in G_q). \tag{1.4.7}$$

(iii) En comparant les puissances de $\log x$ et de $\log_2 x$ de (1.4.4) avec celles du terme principal du théorème 5 (ii) de [40], on constate que, lorsque $a \neq 1$, $\mathfrak{I}(a)$ est le cardinal d'un élément de $\mathfrak{H}^+(a)$ et $\mathfrak{K}_a = \varphi(q)/\mathfrak{I}(a) - 2$.

Le théorème suivant, d'intérêt intrinsèque, fournit une estimation asymptotique du nombre des entiers $n \leqslant x$ dont les $\Omega_j(n)$ ont des valeurs prescrites $< \varphi(q)$ ou sont $\geqslant \varphi(q)$. Cette évaluation constitue une étape essentielle dans la démonstration du Théorème 1.4.1, le lien entre les deux résultats étant explicité au Lemme 2.4.2 *infra.*

Pour tous $q \geqslant 3$, $a \geqslant 1$, tels que $(a,q) = 1$, et $\boldsymbol{\nu} \in \mathcal{E}_q(a)$, nous posons

$$\mathcal{N}_{\boldsymbol{\nu}} := \Big\{ n \geqslant 2 : \Omega_j(n) = \nu_j \text{ si } \nu_j < \varphi(q);\ \Omega_j(n) \geqslant \varphi(q) \text{ si } \nu_j = \varphi(q) \Big\}; \tag{1.4.8}$$

$$d_{k,\boldsymbol{\nu}} := \mathsf{s}(\boldsymbol{\nu}) + (\varphi(q) - 1)k. \tag{1.4.9}$$

Théorème 1.4.4. *Soient $\boldsymbol{\nu} \in \mathcal{E}_q(a)$, $N \in \mathbb{N}$. Pour $x \geqslant 3$, nous avons*

$$\mathcal{N}_{\boldsymbol{\nu}}(x) = \frac{x}{(\log x)^{1-|I_q(\boldsymbol{\nu})|/\varphi(q)}} \Big\{ \sum_{\substack{0 \leqslant m \leqslant N \\ 0 \leqslant k \leqslant |I_q(\boldsymbol{\nu})|}} \frac{P_{m,k,\boldsymbol{\nu}}(\log_2 x)}{(\log x)^{m+k/\varphi(q)}} + O\Big(\mathcal{R}_q(x,\boldsymbol{\nu})\Big) \Big\} \tag{1.4.10}$$

où $\mathcal{R}_q(x,\boldsymbol{\nu}) \ll (\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})+|I_q(\boldsymbol{\nu})|}/(\log x)^{N+1}$ et $P_{m,k,\boldsymbol{\nu}}$ désigne un polynôme tel que $\deg P_{m,k,\boldsymbol{\nu}} \leqslant d_{k,\boldsymbol{\nu}}$ lorsque $I_q(\boldsymbol{\nu}) \neq \varnothing$ et $\deg P_{m,k,\boldsymbol{\nu}} \leqslant d_{0,\boldsymbol{\nu}} - 1$ lorsque $I_q(\boldsymbol{\nu}) = \varnothing$, avec égalité dans les deux cas si $m = k = 0$.

En particulier :

(i) *si $I_q(\boldsymbol{\nu}) \neq \varnothing$, alors le terme principal de $\mathcal{N}_{\boldsymbol{\nu}}(x)$ vaut*

$$\frac{C_q(\boldsymbol{\nu}) x (\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})}}{\Gamma\big(|I_q(\boldsymbol{\nu})|/\varphi(q)\big)\varphi(q)^{\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!(\log x)^{1-|I_q(\boldsymbol{\nu})|/\varphi(q)}}$$

où $C_q(\boldsymbol{\nu})$ est défini en (1.3.4)*;*

(ii) *si $I_q(\boldsymbol{\nu}) = \varnothing$, alors le terme principal de $\mathcal{N}_{\boldsymbol{\nu}}(x)$ vaut*

$$\frac{q\,\mathsf{s}(\boldsymbol{\nu}) x (\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})-1}}{\varphi(q)^{1+\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!\,\log x}.$$

Les résultats suivants, qui découlent directement du Théorème 1.4.1, généralisent les corollaires de [1]. Il aurait également été possible de les déduire du résultat principal de [40].

Commençons par donner un critère pour que $\mathcal{N}_{a,q}(x)$ et $\mathcal{N}_{b,q}(x)$ aient le même ordre de grandeur lorsque a et b sont des éléments quelconques de G_q. Comme il n'y a pas nécessairement unicité des sous-ensembles $I_q(\boldsymbol{\nu})$ de G_q tels que $|I_q(\boldsymbol{\nu})|$ est fixé, $\mathcal{N}_{a,q}(x)$ et $\mathcal{N}_{b,q}(x)$ peuvent avoir le même ordre de grandeur sans être asymptotiquement équivalents.

Corollaire 1.4.5. *Soient $a, b \in G_q$. On a alors*

$$\mathfrak{I}(a) = \mathfrak{I}(b) \Leftrightarrow \mathcal{N}_{a,q}(x) \asymp \mathcal{N}_{b,q}(x). \tag{1.4.11}$$

Dans la remarque suivante, nous explicitons une condition impliquant l'équivalence asymptotique dans (1.4.11) et nous fournissons un exemple où elle n'a pas lieu.

Remarques 1.4.6. (i) *L'expression* (1.3.4) *permet de constater qu'il y a équivalence asymptotique dans* (1.4.11) *si $\mathfrak{H}^+(a) = \mathfrak{H}^+(b)$. C'est notamment le cas lorsque G_q est cyclique.*

(ii) *Il existe des entiers q tels que, pour certaines classes a et b vérifiant $\mathfrak{I}(a) = \mathfrak{I}(b)$, on ait $\mathcal{N}_{a,q}(x) \not\sim \mathcal{N}_{b,q}(x)$. Pour $q = 8$, nous avons ainsi $\mathfrak{I}(3) = \mathfrak{I}(-3) = \mathfrak{I}(-1) = 2$ alors qu'un calcul approché programmé en langage Python fournit*

$$\mathcal{N}_{a,8}(x) \sim \frac{c_{a,8}\, x}{\sqrt{\log x}} \qquad \big(a \in \{3, -3, -1\}\big),$$

avec $c_{3,8} \approx 2,38655$, $c_{-3,8} \approx 2,68906$ et $c_{-1,8} \approx 2,849191$.

Le corollaire suivant est une autre conséquence immédiate du Théorème 1.4.1.

Corollaire 1.4.7. *Si $ab \equiv 1 \pmod q$, alors $\mathcal{N}_{a,q}(x) \sim \mathcal{N}_{b,q}(x)$.*

Démonstration. Notant $\overline{a}$ l'inverse de a dans G_q, nous avons

$$b \notin I_q(\boldsymbol{\nu}) \Leftrightarrow \overline{b} \notin I_q(\boldsymbol{\nu})$$

pour tout $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ vérifiant $|I_q(\boldsymbol{\nu})| = \mathfrak{I}(a)$. La structure de groupe de $I_q(\boldsymbol{\nu})$ permet alors d'obtenir l'égalité

$$\Big\{\boldsymbol{\nu} \in \mathcal{E}_q(a) : |I_q(\boldsymbol{\nu})| = \mathfrak{I}(a),\, \mathsf{s}(\boldsymbol{\nu}) = \mathfrak{K}_a\Big\} = \Big\{\boldsymbol{\nu} \in \mathcal{E}_q(\overline{a}) : |I_q(\boldsymbol{\nu})| = \mathfrak{I}(\overline{a}),\, \mathsf{s}(\boldsymbol{\nu}) = \mathfrak{K}_{\overline{a}}\Big\},$$

ce qui permet de conclure. □

L'énoncé du Théorème 1.4.1 induit une question naturelle : quels sont les éléments a de G_q pour lesquels $\mathcal{N}_{a,q}(x)$ possède l'ordre de grandeur maximal ? Et si plusieurs éléments de G_q sont impliqués, comment les caractériser ?

L'inégalité (1.4.7) fournit une première réponse : si un élément $a \in G_q$ vérifie $\mathfrak{I}(a) = \varphi(q)/2$, alors la puissance de $\log x$ apparaissant dans (1.4.3) est maximale. Il reste alors à décider de l'existence de tels entiers. Les énoncés de [1] incitent à considérer les non résidus quadratiques modulo q.

Le corollaire suivant, démontré au paragraphe 1.12, fournit l'ordre de grandeur de $\mathcal{N}_{a,q}(x)$ lorsque a est non résidu quadratique modulo q ainsi que, le cas échéant, une formule explicite pour la constante $C_q(\boldsymbol{\nu})$ définie en (1.3.4) lorsque G_q est cyclique.

Rappelons la notation $\mathscr{L}(\chi)$ définie en (1.3.1).

Corollaire 1.4.8. *Un entier a de G_q est non résidu quadratique modulo q si, et seulement si, $\mathfrak{I}(a) = \varphi(q)/2$. Dans ce cas, nous avons $\mathfrak{K}_a = 0$ et*

$$\mathcal{N}_{a,q}(x) \asymp \frac{x}{\sqrt{\log x}}. \tag{1.4.12}$$

De plus, dans le cas où G_q est cyclique, nous avons

$$\mathcal{N}_{a,q}(x) \sim \frac{C_q\, x}{\sqrt{\log x}} \qquad (x \to +\infty), \tag{1.4.13}$$

avec

$$C_q := \sqrt{\frac{q\mathscr{L}(\chi_1)}{\pi\varphi(q)}}$$

où χ_1 désigne l'unique caractère d'ordre 2 de G_q.

Remarque 1.4.9. *Lorsque q est premier (ce qui implique G_q cyclique), le caractère χ_1 du Corollaire 1.4.8 est égal au symbole de Legendre, $b \mapsto \big(b|q\big)$ $(b \in \mathbb{Z})$.*

Nous montrons au paragraphe 1.11 que G_q est cyclique si, et seulement si, chaque non résidu quadratique a de G_q est tel que $\mathcal{E}_q(a)$ contient un unique élément $\boldsymbol{\nu}$ vérifiant $|I_q(\boldsymbol{\nu})| = \varphi(q)/2$. Lorsqu'il en est ainsi, l'ensemble $I_q(\boldsymbol{\nu})$ est le sous-groupe des résidus quadratiques de G_q, et la constante $\Xi(a)$ de (1.4.2) ne dépend pas de a lorsque a est non résidu quadratique. En revanche, lorsque G_q n'est pas cyclique, il existe au moins deux sous-ensembles distincts de $\mathcal{E}_q(a)$ de cardinal maximal $\varphi(q)/2$, ce qui ouvre la possiblité que la somme en $\boldsymbol{\nu}$ apparaissant dans (1.4.2) ne soit pas indépendante de a : c'est effectivement le cas lorsque $q = 8$, ainsi qu'il est mentionné à la Remarque 1.4.6.

Le corollaire suivant permet de comparer l'ordre de grandeur de $\mathcal{N}_{a,q}(x)$ avec celui de $\mathcal{N}_{b,q}(x)$ lorsque $a \in G_q$ et b est non résidu quadratique modulo q.

Corollaire 1.4.10. *Soient $a, b \in G_q$ tels que b soit non résidu quadratique modulo q.*

(i) *Nous avons, pour x assez grand,*

$$\mathcal{N}_{a,q}(x) \ll \mathcal{N}_{b,q}(x). \tag{1.4.14}$$

(ii) *De plus, si a est un résidu quadratique, alors*

$$\mathcal{N}_{a,q}(x) = o\big(\mathcal{N}_{b,q}(x)\big) \qquad (x \to \infty).$$

Plus précisément, pour tout δ, $0 < \delta < 1/\varphi(q)$, nous avons, pour x assez grand,

$$\mathcal{N}_{a,q}(x) \ll \frac{\mathcal{N}_{b,q}(x)}{(\log x)^{\delta}}. \tag{1.4.15}$$

Démonstration. L'estimation (1.4.14) est une conséquence directe de l'inégalité (1.4.7) et du Corollaire 1.4.8. Lorsque a est résidu quadratique, le Corollaire 1.4.8 implique $\mathfrak{I}(a) < \mathfrak{I}(b)$, et, plus précisément, $\mathfrak{I}(b) = \mathfrak{I}(a) + k + 1$ avec $k \in \mathbb{N}$. La majoration (1.4.15) en découle lorsqu'on choisit δ tel que $0 < \delta < (k+1)/\varphi(q)$. □

Le Corollaire 1.4.8 fournit l'ordre de grandeur de $\mathcal{N}_{a,q}(x)$ lorsque a est non résidu quadratique modulo q. Le corollaire suivant, qui généralise le Corollaire 1.4.8, donne l'ordre de grandeur dès que a est différent de 1. Pour $m \in \mathbb{N}^*$, nous notons

$$G_q^m := \{y^m : \ y \in G_q\}$$

l'ensemble des puissances m-ièmes de G_q.

Corollaire 1.4.11. *Soit $a \in G_q$, $a \neq 1$ et soit m le plus petit diviseur de $\varphi(q)$ tel que $a \notin G_q^m$. Alors $\mathfrak{I}(a) = \varphi(q)/m$, $\mathfrak{K}_a = m-2$, et*

$$\mathcal{N}_{a,q}(x) \asymp \frac{x(\log_2 x)^{m-2}}{(\log x)^{1-1/m}}. \tag{1.4.16}$$

Dans le cas où G_q est cyclique, nous avons

$$\mathcal{N}_{a,q}(x) \sim \frac{C_q}{\Gamma(1/m)\varphi(q)^{m-2}} \Bigg(\sum_{\substack{\boldsymbol{\nu} \in \mathcal{E}_q(a) \\ |I_q(\boldsymbol{\nu})| = \varphi(q)/m \\ \mathsf{s}(\boldsymbol{\nu}) = m-2}} \frac{1}{\boldsymbol{\nu}!} \Bigg) \frac{x(\log_2 x)^{m-2}}{(\log x)^{1-1/m}} \qquad (x \to \infty)$$

avec

$$C_q := \Big(\frac{q}{\varphi(q)}\Big)^{1-1/m} \prod_{\substack{\chi \neq \chi_0 \\ \chi^m = \chi_0}} \mathscr{L}(\chi)^{1/m}.$$

Si a n'est pas un résidu quadratique modulo q, alors $m = 2$: l'estimation (1.4.16) coïncide donc avec (1.4.12). Si a est un carré mais n'est pas un cube de G_q, alors $m = 3$, et il suit

$$\mathcal{N}_{a,q}(x) \asymp \frac{x \log_2 x}{(\log x)^{2/3}}.$$

Il est à noter que, lorsque $3 \mid \varphi(q)$, G_q contient des résidus quadratiques qui ne sont pas des résidus cubiques. Par exemple, si tous les facteurs premiers de q sont congrus à 1 modulo 3, le théorème chinois permet alors d'établir facilement que G_q possède $\varphi(q)/2^{\omega(q)}$ résidus quadratiques et $\varphi(q)/3^{\omega(q)}$ résidus cubiques. On trouvera notamment dans l'article de Chun Gang Ji [31] des formules générales pour le nombre de puissances m-ièmes dans $\mathbb{Z}/q\mathbb{Z}$.

1.5 Exemple d'application, le cas $q = 18$

Pour illustrer le Théorème 1.4.1, nous considérons dans ce paragraphe le cas $q = 18$. Nous avons $\varphi(q) = 6$ et $G_{18} = \{1, 5, 7, -7, -5, -1\}$. Les éléments 5 et -7 sont des générateurs de G_{18}, 7 et -5 sont d'ordre 3 et -1 est d'ordre 2. Les caractères modulo 18 sont définis dans le tableau suivant.

	1	5	7	-7	-5	-1
χ_0	1	1	1	1	1	1
χ_1	1	$\mathrm{e}^{i\pi/3}$	$\mathrm{e}^{2i\pi/3}$	$\mathrm{e}^{-i\pi/3}$	$\mathrm{e}^{-2i\pi/3}$	-1
χ_2	1	$\mathrm{e}^{2i\pi/3}$	$\mathrm{e}^{-2i\pi/3}$	$\mathrm{e}^{-2i\pi/3}$	$\mathrm{e}^{2i\pi/3}$	1
χ_3	1	-1	1	-1	1	-1
χ_4	1	$\mathrm{e}^{-2i\pi/3}$	$\mathrm{e}^{2i\pi/3}$	$\mathrm{e}^{2i\pi/3}$	$\mathrm{e}^{-2i\pi/3}$	1
χ_5	1	$\mathrm{e}^{-i\pi/3}$	$\mathrm{e}^{-2i\pi/3}$	$\mathrm{e}^{i\pi/3}$	$\mathrm{e}^{2i\pi/3}$	-1

Écrivons les coordonnées de $\boldsymbol{\nu} := (\nu_j)_{j\in G_q} \in \mathcal{E}_q(a)$ dans l'ordre suivant : $\boldsymbol{\nu} = (\nu_1, \nu_5, \nu_7, \nu_{-7}, \nu_{-5}, \nu_{-1})$.

Pour $a = 7$, on a

$$\mathcal{E}_q(7) = \Big\{(a_1, c_1, 0, b_1, 0, 0), (a_1, c_1, 0, c_2, c_3, 0), (a_1, c_1, 0, 0, 0, a_2), (a_1, 0, 0, 0, c_1, a_2) : \\ (a_1, a_2, b_1, c_1, c_2, c_3) \in [\![0; 6]\!]^2 \times [\![0; 3]\!] \times [\![0; 1]\!]^3\Big\}.$$

Dans ce cas, nous avons $\mathfrak{I}(7) = 2$ et $\mathfrak{K}_7 = 1$, et les seuls éléments de $\mathcal{E}_q(7)$ vérifiant ces deux conditions sont $\boldsymbol{\nu}_0 := (6, 1, 0, 0, 0, 6)$ et $\boldsymbol{\nu}_1 := (6, 0, 0, 0, 1, 6)$. De plus,

$$I_{18}(\boldsymbol{\nu}_0) = I_{18}(\boldsymbol{\nu}_1) = \{1, -1\}$$

(1 et -1 sont alors dans ce cas les classes complètes), et le seul élément de $\mathcal{E}_q(7)$ vérifiant $|I_q(\boldsymbol{\nu})| = 2$ et $\mathfrak{s}(\boldsymbol{\nu}) = 0$ est $\boldsymbol{\nu}_2 := (6, 0, 0, 0, 0, 6)$. Le Théorème 1.4.1 et les formules explicites données au paragraphe 1.9 fournissent, après un calcul direct,

$$\mathcal{N}_{7,18}(x) = \left\{\mathfrak{a}_0 + \frac{\mathfrak{a}_1}{\log_2 x} + O\left(\frac{(\log_2 x)^5}{(\log x)^{1/6}}\right)\right\}\frac{x \log_2 x}{(\log x)^{2/3}}$$

où

$$\mathfrak{a}_0 := \frac{C}{3\Gamma\big(1/3\big)},$$

$$\mathfrak{a}_1 := \frac{C}{3\Gamma(1/3)}\left\{\frac{\Gamma'(1/3)}{\Gamma(1/3)} + \sum_p\left(\log\Big(1 - \frac{1}{p}\Big) + \frac{1}{p}\right) + \sum_{\chi\in\{\chi_2,\chi_4\}}\overline{\chi(5)}\sum_p\frac{\chi(p)}{p} + \frac{13}{6}\right\},$$

avec

$$C := C_{18}(\boldsymbol{\nu}_0) = C_{18}(\boldsymbol{\nu}_1) = C_{18}(\boldsymbol{\nu}_2) \\ = 3^{2/3}\prod_{\chi\in\{\chi_2,\chi_4\}}\mathscr{L}(\chi)^{1/3}.$$

Pour $a = -5$, le résultat obtenu est identique car, dans ce cas, nous avons à nouveau $\mathfrak{I}(-5) = 2$ et $\mathfrak{K}_{-5} = 1$ et les seuls éléments de $\mathcal{E}_q(-5)$ vérifiant ces deux conditions sont $\boldsymbol{\nu}_3 := (6, 0, 1, 0, 0, 6)$ et $\boldsymbol{\nu}_4 := (6, 0, 0, 1, 0, 6)$; de plus, $I_{18}(\boldsymbol{\nu}_3) = I_{18}(\boldsymbol{\nu}_4) = \{1, -1\}$, comme dans le cas $a = 7$. Pour $a = -1$, nous avons $\mathfrak{I}(-1) = 3$ et $\mathfrak{K}_{-1} = 0$, et $\boldsymbol{\nu}_5 := (6, 0, 6, 0, 6, 0)$ est le seul élément de $\mathcal{E}_q(-1)$ vérifiant ces deux conditions ; il en résulte que

$$\mathcal{N}_{-1,18}(x) = \left\{\frac{C_{18}(\boldsymbol{\nu}_5)}{\sqrt{\pi}} + O\left(\frac{(\log_2 x)^5}{(\log x)^{1/6}}\right)\right\}\frac{x}{\sqrt{\log x}},$$

avec

$$C_{18}(\boldsymbol{\nu}_5) = \sqrt{3\mathscr{L}(\chi_3)}.$$

Si $a = 5$ ou $a = -7$, le résultat obtenu est identique au cas $a = -1$ car nous avons également $\mathfrak{I}(a) = 3$, $\mathfrak{K}_a = 0$, et $\boldsymbol{\nu}_5$ est le seul élément vérifiant ces deux conditions. Pour $a = 1$, nous avons $\mathfrak{I}(1) = 0$ et $\mathfrak{K}_1 = 5$, et les seuls éléments de $\mathcal{E}_q(1)$ vérifiant ces deux conditions sont $(0, 5, 0, 0, 0, 0)$ et $(0, 0, 0, 5, 0, 0)$, et dans ce cas,

$$\mathcal{N}_{1,18}(x) = \left\{\mathfrak{b}_0 + \frac{\mathfrak{b}_1}{\log_2 x} + O\left(\frac{\log_2 x}{\log x}\right)\right\}\frac{x(\log_2 x)^4}{\log x},$$

avec

$$\mathfrak{b}_0 := \frac{1}{31104},$$
$$\mathfrak{b}_1 := \frac{1}{1296}\Big\{\sum_p\Big(\log\Big(1-\frac{1}{p}\Big)+\frac{1}{p}\Big)+\sum_{\chi\in\{\chi_2,\chi_4\}}\overline{\chi(5)}\sum_p\frac{\chi(p)}{p}+\gamma-\frac{5}{6}\Big\},$$

où γ est la constante d'Euler. Nous pouvons ainsi remarquer que, lorsque $a \in \{5,-7,-1\}$ (qui sont les non résidus quadratiques de G_{18}), les $\mathcal{N}_{a,q}(x)$ sont tous du même ordre de grandeur, strictement supérieur à celui de $\mathcal{N}_{a,q}(x)$ lorsque $a \in \{7,-5\}$ (qui sont des carrés modulo 18 mais pas des cubes modulo 18), lui-même strictement supérieur à celui de $\mathcal{N}_{1,q}(x)$.

1.6 Réductions

Rappelons que $\mathcal{E}_q(a)$ désigne l'ensemble des éléments a-admissibles de H_q^*.

Durant toute la démonstration, les entiers a et q sont fixés, et l'ensemble $\mathcal{N}_{a,q}$ est noté simplement $\mathcal{N}$. Commençons par réécrire $\mathcal{N}$ sous la forme d'une union disjointe de sous-ensembles plus simples. Cette réécriture est traitée dans les deux lemmes suivants.

Pour cela, nous allons d'abord établir une correspondance entre un élément n de $\mathcal{N}$ et un élément de $\mathcal{E}_q(a)$ dépendant de n : cela fait l'objet du Lemme 1.6.1, qui joue un rôle fondamental dans notre preuve. Il se démontre grâce aux caractéristiques de $\mathcal{N}$ et $\mathcal{E}_q(a)$ en utilisant quelques notions de théorie des groupes, notamment le théorème d'Euler.

Lemme 1.6.1. *Soit n un entier $\geqslant 2$. Alors*

$$n \in \mathcal{N} \Leftrightarrow \Big(\min\big\{\Omega_j(n),\varphi(q)\big\}\Big)_{j\in G_q} \in \mathcal{E}_q(a). \tag{1.6.1}$$

Démonstration. Tout d'abord, on remarque que tout entier d vérifiant $d \equiv a \pmod q$ est tel que $(d,q)=1$ puisque $(a,q)=1$. Nous avons donc, pour $n \geqslant 2$,

$$n \in \mathcal{N} \Leftrightarrow \Big(\big(d \mid n,\ d>1,\ (d,q)=1\big) \Rightarrow d \not\equiv a \pmod q\Big). \tag{1.6.2}$$

Soient $n \geqslant 2$ et $d \mid n$ tel que $(d,q)=1$ et $d>1$; on peut écrire n sous la forme $n = n_0\prod_{j\in G_q} n_j$, où

$$n_j := \prod_{\substack{p^\nu \| n \\ p\equiv j \pmod q}} p^\nu \quad (j\in G_q), \qquad n_0 := \prod_{\substack{p^\nu\|n \\ p\mid q}} p^\nu.$$

Décomposons d de la même manière. Alors $d_0=1$ et $d_j \mid n_j$ pour tout $j\in G_q$. De plus, il existe $j\in G_q$ tel que $d_j>1$. Pour tout $j\in G_q$, on a $\Omega(n_j)=\Omega_j(n)$ et $\Omega(d_j)=\Omega_j(d)$. Dans ce cas, nous avons

$$d \equiv \prod_{j\in G_q} j^{\Omega(d_j)} \equiv \prod_{j\in G_q} j^{\Omega_j(d)} \pmod q.$$

Il s'ensuit que

$$\exists \boldsymbol{\mu} \in \prod_{j\in G_q} [\![0;\Omega_j(n)]\!] \smallsetminus \{\mathbf{0}\} : d \equiv \prod_{j\in G_q} j^{\mu_j} \pmod q. \tag{1.6.3}$$

De plus, pour tout vecteur $\boldsymbol{\mu} \in \prod_{j\in G_q} [\![0;\Omega_j(n)]\!] \smallsetminus \{\mathbf{0}\}$, il existe $d \mid n$ vérifiant $d > 1$, $(d,q) = 1$, et tel que $\Omega_j(d) = \mu_j$ pour tout $j \in G_q$. On déduit de (1.6.2), (1.6.3) et de ces correspondances que

$$n \in \mathcal{N} \Leftrightarrow \Big(\Big(\boldsymbol{\mu} \in \prod_{j\in G_q} [\![0;\Omega_j(n)]\!] \smallsetminus \{\mathbf{0}\}\Big) \Rightarrow \prod_{j\in G_q} j^{\mu_j} \not\equiv a \pmod q\Big). \tag{1.6.4}$$

Grâce au théorème d'Euler, nous pouvons imposer en outre, dans le membre de droite de cette équivalence,

$$\max_{j\in G_q}\{\mu_j\} \leqslant \varphi(q). \tag{1.6.5}$$

Observons que, dans cette dernière majoration, l'inégalité large ne peut en général pas être remplacée par l'inégalité stricte. Lorsque, par exemple, $a = 1$ et G_q est cyclique, une inégalité stricte dans (1.6.5) ne permettrait pas d'écarter les n vérifiant $\Omega_j(n) = \varphi(q)$ pour un $j \pmod q$ générateur de G_q, et $\Omega_k(n) = 0$ si $k \neq j$, puisque dans ce cas, l'inégalité stricte impliquerait $\boldsymbol{\mu} = \mathbf{0}$.

Il résulte de (1.6.4) et (1.6.5) que

$$n \in \mathcal{N} \Leftrightarrow \Big(\Big(\boldsymbol{\mu} \in \prod_{j\in G_q} [\![0;\min\{\Omega_j(n),\varphi(q)\}]\!] \smallsetminus \{\mathbf{0}\}\Big) \Rightarrow \prod_{j\in G_q} j^{\mu_j} \not\equiv a \pmod q\Big).$$

La condition de droite de cette équivalence est identique à celle de (1.6.1). □

Nous pouvons déjà observer une différence majeure entre les cas $1 < a < q$ et $a = 1$, comme expliqué dans la remarque ci-dessous.

Remarque 1.6.2. *Lorsque $a = 1$, $n \in \mathcal{N}$ et $(n,q) = 1$, la quantité $\Omega(n)$ est bornée : en effet, pour tout $j \in G_q$, $\Omega_j(n) < \varphi(q)$ puisque $j^{\varphi(q)} \equiv 1 \pmod q$.*

Nous sommes à présent en mesure d'opérer la réduction annoncée sous la forme d'une partition de l'ensemble $\mathcal{N}$. Pour $\boldsymbol{\nu} \in \mathcal{E}_q(a)$, nous rappelons la notation (1.4.8) définissant les ensembles $\mathcal{N}_{\boldsymbol{\nu}}$.

Lemme 1.6.3. *Nous avons $\mathcal{N} = \bigsqcup_{\boldsymbol{\nu}\in\mathcal{E}_q(a)} \mathcal{N}_{\boldsymbol{\nu}}$.*

Démonstration. Par définition, les ensembles $\mathcal{N}_{\boldsymbol{\nu}}$ sont deux à deux disjoints. Il résulte de cette observation et du Lemme 1.6.1 que

$$n \in \mathcal{N} \Leftrightarrow \exists!\, \boldsymbol{\nu} \in \mathcal{E}_q(a) :\ n \in \mathcal{N}_{\boldsymbol{\nu}},$$

et l'on a en fait explicitement $\boldsymbol{\nu} := \big(\min\{\Omega_j(n),\varphi(q)\}\big)_{j\in G_q}$. □

Ainsi

$$\mathcal{N}(x) = \sum_{\boldsymbol{\nu}\in\mathcal{E}_q(a)} \mathcal{N}_{\boldsymbol{\nu}}(x). \tag{1.6.6}$$

À partir de maintenant, et jusqu'au paragraphe 1.8 inclus, nous fixons un élément $\boldsymbol{\nu}$ de $\mathcal{E}_q$. La notion de classe $\boldsymbol{\nu}$-complète permet de transformer l'écriture de $\mathcal{N}_{\boldsymbol{\nu}}(x)$. C'est l'objet du lemme suivant, qui donne une estimation de $\mathcal{N}_{\boldsymbol{\nu}}(x)$ sous la forme d'une intégrale curviligne grâce à la formule de Cauchy.

Rappelons (cf. Définition 1.3.3) que $I_q(\boldsymbol{\nu})$ désigne l'ensemble des classes $\boldsymbol{\nu}$-complètes de G_q.

Pour $\boldsymbol{R}\in(\mathbb{R}^{+*})^{G_q}$, nous notons $\mathcal{C}(\mathbf{0},\boldsymbol{R})$ le polycercle $\prod_{j\in G_q}\big\{z_j\in\mathbb{C} : |z_j| = R_j\big\}$.

Pour $\boldsymbol{z}\in\mathbb{C}^{G_q}$, nous posons

$$T(x;\boldsymbol{z}) := \sum_{n\leqslant x}\prod_{j\in G_q} z_j^{\Omega_j(n)}. \tag{1.6.7}$$

Lemme 1.6.4. *Soit $\boldsymbol{R}\in(\mathbb{R}_+^*)^{G_q}$ tel que $R_j>1$ dès que $j\in I_q(\boldsymbol{\nu})$. Pour $x\geqslant 1$, nous avons*

$$\mathcal{N}_{\boldsymbol{\nu}}(x) = \frac{1}{(2i\pi)^{\varphi(q)}}\oint_{\mathcal{C}(\mathbf{0};\boldsymbol{R})} T(x;\boldsymbol{z})\prod_{j\in J_q(\boldsymbol{\nu})}\frac{\mathrm{d}z_j}{z_j^{\nu_j+1}}\prod_{j\in I_q(\boldsymbol{\nu})}\frac{\mathrm{d}z_j}{z_j^{\varphi(q)}(z_j-1)}. \tag{1.6.8}$$

Démonstration. Notons, pour E un ensemble d'entiers, $\mathbb{1}_E$ la fonction indicatrice de E, c'est-à-dire la fonction vérifiant $\mathbb{1}_E(n) := 1$ si $n\in E$ et 0 sinon.

Si $j\in J_q(\boldsymbol{\nu})$, la formule de Cauchy permet d'écrire

$$\mathbb{1}_{\{n:\ \Omega_j(n)=\nu_j\}}(n) = \frac{1}{2i\pi}\oint_{|z|=R_j} z^{\Omega_j(n)}\frac{\mathrm{d}z}{z^{\nu_j+1}}. \tag{1.6.9}$$

De même, si $j\in I_q(\boldsymbol{\nu})$, nous avons, sous l'hypothèse supplémentaire $R_j>1$,

$$\begin{aligned}\mathbb{1}_{\{n:\ \Omega_j(n)\geqslant\varphi(q)\}}(n) &= \frac{1}{2i\pi}\oint_{|z|=R_j} z^{\Omega_j(n)-1}\Big(\sum_{\nu\geqslant\varphi(q)} z^{-\nu}\Big)\mathrm{d}z\\ &= \frac{1}{2i\pi}\oint_{|z|=R_j} z^{\Omega_j(n)}\frac{\mathrm{d}z}{z^{\varphi(q)}(z-1)}.\end{aligned} \tag{1.6.10}$$

La formule (1.6.8) découle immédiatement de l'égalité

$$\mathcal{N}_{\boldsymbol{\nu}}(x) = \sum_{n\leqslant x}\prod_{j\in J_q(\boldsymbol{\nu})}\mathbb{1}_{\{n:\ \Omega_j(n)=\nu_j\}}(n)\prod_{j\in I_q(\boldsymbol{\nu})}\mathbb{1}_{\{n:\ \Omega_j(n)\geqslant\varphi(q)\}}(n)$$

ainsi que de (1.6.9) et (1.6.10). □

1.7 Utilisation de la méthode de Selberg-Delange

Nous nous proposons ici d'évaluer l'expression $T(x;\boldsymbol{z})$ définie en (1.6.7) en employant le théorème II.5.2 de [57], de type Selberg-Delange. La première étape consiste à vérifier les hypothèses décrites aux pages 277-278 de [57].

1.7.1 Calculs préliminaires

Dans toute la suite nous considérons $\boldsymbol{z} = (z_j)_{j\in G_q} \in \mathbb{C}^{G_q}$ tel que

$$1 < |z_j| < 2 \quad (j \in I_q(\boldsymbol{\nu})), \qquad 0 < |z_j| < 2 \quad (j \in J_q(\boldsymbol{\nu})). \tag{1.7.1}$$

Nous conservons la notation

$$\mathfrak{S}(\boldsymbol{z}) := \sum_{j\in G_q} z_j.$$

Comme la fonction $n \mapsto \prod_{j\in G_q} z_j^{\Omega_j(n)}$ est complètement multiplicative, la série de Dirichlet associée admet, pour $\Re e\, s > 1$, la représentation eulérienne suivante

$$\begin{aligned}\mathcal{F}(s;\boldsymbol{z}) &:= \sum_n \frac{1}{n^s} \prod_{j\in G_q} z_j^{\Omega_j(n)} = \prod_p \Big(1 - \frac{1}{p^s} \prod_{j\in G_q} z_j^{\Omega_j(p)}\Big)^{-1} \\ &= \prod_{p\,|\,q} \Big(1-\frac{1}{p^s}\Big)^{-1} \cdot \prod_{j\in G_q} \prod_{p\equiv j \,(\mathrm{mod}\, q)} \Big(1-\frac{z_j}{p^s}\Big)^{-1} \\ &= \prod_{p\,|\,q} \Big(1-\frac{1}{p^s}\Big)^{-1} \cdot \prod_{j\in G_q} \prod_{p\equiv j \,(\mathrm{mod}\, q)} \frac{(1-1/p^s)^{z_j}}{1-z_j/p^s}\Big(1-\frac{1}{p^s}\Big)^{-z_j},\end{aligned} \tag{1.7.2}$$

où les facteurs $(1-1/p^s)^{\pm z_j}$ sont définis *via* la détermination principale du logarithme complexe. Nous notons alors

$$\begin{aligned}\mathcal{B}_j(s;z) &:= \prod_{p\equiv j \,(\mathrm{mod}\, q)} \frac{(1-1/p^s)^z}{1-z/p^s} \quad (z\in\mathbb{C},\, j\in G_q), \\ \mathcal{B}(s;\boldsymbol{z}) &:= \prod_{j\in G_q} \mathcal{B}_j(s;z_j) \quad (\boldsymbol{z}\in\mathbb{C}^{G_q}).\end{aligned} \tag{1.7.3}$$

De plus, l'orthogonalité des caractères implique

$$\begin{aligned}\prod_{j\in G_q} \prod_{p\equiv j \,(\mathrm{mod}\, q)} \Big(1-\frac{1}{p^s}\Big)^{-z_j} &= \prod_{j\in G_q} \prod_p \Big(1-\frac{1}{p^s}\Big)^{-z_j \sum_\chi \chi(p)\overline{\chi(j)}/\varphi(q)} \\ &= \prod_{p\nmid q} \Big(1-\frac{1}{p^s}\Big)^{-\mathfrak{S}(\boldsymbol{z})/\varphi(q)} \cdot \prod_p \Big(1-\frac{1}{p^s}\Big)^{-\sum_{j\in G_q} z_j \sum_{\chi\neq\chi_0} \chi(p)\overline{\chi(j)}/\varphi(q)} \\ &= \zeta(s)^{\mathfrak{S}(\boldsymbol{z})/\varphi(q)} \cdot \prod_{p\,|\,q} \Big(1-\frac{1}{p^s}\Big)^{\mathfrak{S}(\boldsymbol{z})/\varphi(q)} \cdot \prod_{\chi\neq\chi_0} \prod_p \Big(1-\frac{1}{p^s}\Big)^{-\chi(p)D(\boldsymbol{z},\chi)},\end{aligned} \tag{1.7.4}$$

où l'on a posé

$$D(\boldsymbol{z},\chi) := \sum_{j\in G_q} z_j \overline{\chi(j)}/\varphi(q).$$

Notons encore

$$\mathcal{H}(s;\boldsymbol{z}) := \prod_{p\,|\,q} \Big(1-\frac{1}{p^s}\Big)^{\mathfrak{S}(\boldsymbol{z})/\varphi(q)-1}, \quad \mathscr{T}(s,\chi) := \prod_p \frac{1-\chi(p)/p^s}{(1-1/p^s)^{\chi(p)}} \tag{1.7.5}$$

et observons que, avec la notation traditionnelle $L(s,\chi)$ pour la fonction L de Dirichlet associée au caractère χ, nous avons, pour $\sigma > 1$,

$$\prod_p \Big(1-\frac{1}{p^s}\Big)^{-\chi(p)} = \prod_p \frac{1-\chi(p)/p^s}{(1-1/p^s)^{\chi(p)}}\Big(1-\frac{\chi(p)}{p^s}\Big)^{-1} = \mathscr{T}(s,\chi)L(s,\chi). \tag{1.7.6}$$

Posant

$$\mathscr{U}(s;\boldsymbol{z}) := \prod_{\chi\neq\chi_0} \mathscr{T}(s,\chi)^{D(\boldsymbol{z},\chi)}, \tag{1.7.7}$$

$$\mathcal{V}(s;\boldsymbol{z}) := \prod_{\chi\neq\chi_0} L(s,\chi)^{D(\boldsymbol{z},\chi)}, \tag{1.7.8}$$

$$\mathscr{G}(s;\boldsymbol{z}) := \mathcal{H}(s;\boldsymbol{z})\mathcal{B}(s;\boldsymbol{z})\mathscr{U}(s;\boldsymbol{z})\mathcal{V}(s;\boldsymbol{z}), \tag{1.7.9}$$

nous déduisons de (1.7.3)–(1.7.9) que

$$\mathcal{F}(s;\boldsymbol{z}) = \mathscr{G}(s;\boldsymbol{z})\zeta(s)^{\mathfrak{S}(\boldsymbol{z})/\varphi(q)}. \tag{1.7.10}$$

Désignons par $\{\gamma_j\}_{j=0}^{\infty}$ la famille de fonctions entières, liées à la fonction zêta, apparaissant au théorème II.5.1 de [57]. Nous utiliserons seulement les propriétés $\gamma_0 \equiv 1$ et, pour tous $A > 0, \varepsilon > 0$, $\gamma_h(z) \ll_{\varepsilon,A} (1+\varepsilon)^h$ $(|z| \leqslant A)$. Posons alors [5]

$$\lambda_m(\boldsymbol{z}) := \frac{1}{\Gamma\big(\mathfrak{S}(\boldsymbol{z})/\varphi(q)-m\big)} \sum_{j+h=m} \frac{1}{j!h!}\mathscr{G}^{(j)}(1,\boldsymbol{z})\gamma_h(\mathfrak{S}(\boldsymbol{z})) \quad \big(\boldsymbol{z}\in\mathbb{C}^{G_q}\big), \tag{1.7.11}$$

et rappelons ici les définitions ainsi que l'énoncé de la méthode de Selberg-Delange décrits dans [57].

Lemme 1.7.1. *Soit $N \in \mathbb{N}$. Sous les conditions* (1.7.1)*, nous avons*

$$T(x;\boldsymbol{z}) = x(\log x)^{\mathfrak{S}(\boldsymbol{z})/\varphi(q)-1}\bigg\{\sum_{0\leqslant m\leqslant N}\frac{\lambda_m(\boldsymbol{z})}{(\log x)^m} + O\bigg(\frac{1}{(\log x)^{N+1}}\bigg)\bigg\}. \tag{1.7.12}$$

Définition 1.7.2. *Soient $c > 0$, $0 < \delta \leqslant 1$ et $M > 0$. On dit qu'une série de Dirichlet $F(s) := \sum_{n\geqslant 1} a_n/n^s$ possède la propriété $\mathcal{P}(c,\delta,M)$ s'il existe $w \in \mathbb{C}$ tel que l'on ait $F(s) = G(s)\zeta(s)^w$ pour $\sigma > 1$, et si $G(s)$ est prolongeable en une fonction holomorphe pour $\sigma \geqslant 1 - c/\log(|\tau|+2)$ satisfaisant dans ce domaine à la majoration*

$$G(s) \leqslant M(1+|\tau|)^{1-\delta}. \tag{1.7.13}$$

Définition 1.7.3. *Soient $F(s) := \sum_{n\geqslant 1} a_n/n^s$ une série de Dirichlet à coefficients complexes et $H(s) := \sum_{n\geqslant 1} b_n/n^s$ une série de Dirichlet à coefficients réels positifs. On dit que $H(s)$ est une série majorante de $F(s)$ si $|a_n| \leqslant b_n$ $(n \geqslant 1)$.*

Le paragraphe suivant est consacré à la preuve du Lemme 1.7.1. Compte tenu de (1.7.10), et puisque $\mathcal{F}(s;|\boldsymbol{z}|)$ est une série majorante de $\mathcal{F}(s;\boldsymbol{z})$, il suffit, en vertu du théorème II.5.2 de [57], de vérifier que, sous les conditions (1.7.1), la série $\mathscr{G}(s;\boldsymbol{z})$ vérifie une majoration du type (1.7.13) lorsque les paramètres $c > 0$, $0 < \delta \leqslant 1$, et $M > 0$ sont convenablement choisis.

5. Ici et dans la suite, si f est une fonction à une ou plusieurs variables, suffisamment dérivable par rapport à la première variable, et si $v \in \mathbb{N}$, alors $f^{(v)}$ désigne la dérivée v-ième de f par rapport à la première variable.

1.7.2 Validation des hypothèses

1.7.2.1 Pour $\mathcal{H}(s;\boldsymbol{z})$

La fonction $s \mapsto \mathcal{H}(s;\boldsymbol{z})$ est holomorphe sur le demi-plan $\sigma > 0$ comme produit fini de fonctions holomorphes sur ce même demi-plan. Pour tout $\alpha > 0$, nous avons

$$\mathcal{H}(s;\boldsymbol{z}) \ll_\alpha 1 \quad (\sigma \geqslant \alpha,\ \boldsymbol{z} \ll 1). \tag{1.7.14}$$

1.7.2.2 Pour $\mathcal{B}(s;\boldsymbol{z})$

Soit $j \in G_q$. Le développement de $\mathcal{B}_j(s;z)$ en série de Dirichlet s'écrit

$$\mathcal{B}_j(s;z) = \sum_{n\geqslant 1} \frac{b_{j,z}(n)}{n^s},$$

où $b_{j,z}$ est la fonction multiplicative de n définie par

$$b_{j,z}(p^\mu) = 0 \quad \big(p \not\equiv j \pmod q,\ \mu \in \mathbb{N}^*\big) \tag{1.7.15}$$

$$1 + \sum_{\mu\geqslant 1} b_{j,z}(p^\mu)\xi^\mu = \frac{(1-\xi)^z}{1-z\xi} \quad \big(p \equiv j \pmod q\big). \tag{1.7.16}$$

On a en particulier

$$b_{j,z}(p) = 0 \qquad \big(p \equiv j \pmod q\big). \tag{1.7.17}$$

De plus, le membre de droite de (1.7.16) est holomorphe en ξ dans le disque $|\xi| < \min\big\{1, 1/|z|\big\}$. Pour tout $0 < \delta_1 < 1/2$, la formule de Cauchy fournit, pour $|z| \leqslant 2 - 2\delta_1$,

$$|b_{j,z}(p^\mu)| \leqslant M(\delta_1)(2-\delta_1)^\mu \quad \big(\mu \geqslant 2, p \equiv j \pmod q\big) \tag{1.7.18}$$

avec

$$M(\delta_1) := \sup_{\substack{|z|\leqslant 2-2\delta_1 \\ |\xi|\leqslant 1/(2-\delta_1)}} \left|\frac{(1-\xi)^z}{1-z\xi}\right|.$$

Choisissons par exemple $\delta_1 := \frac{1}{3}$. Il résulte des relations (1.7.15), (1.7.17) et (1.7.18) que l'on a, pour $\sigma > \sigma_1 := 1 - (\ln\frac{6}{5})/\ln 2$,

$$\sum_{p\equiv j \pmod q} \sum_{\mu\geqslant 1} \left|\frac{b_{j,z}(p^\mu)}{p^{\mu s}}\right| \leqslant M(\delta_1) \sum_{p\equiv j \pmod q} \sum_{\mu\geqslant 2} \frac{(5/3)^\mu}{p^{\mu\sigma}} \ll_\sigma 1.$$

Cela implique l'absolue convergence de $s \mapsto \mathcal{B}_j(s;z)$ pour $\sigma > \sigma_1$, $j \in G_q$, et plus généralement, sur le même demi-plan, celle de $s \mapsto \mathcal{B}(s;\boldsymbol{z})$. Pour $\alpha > \sigma_1$, nous obtenons donc

$$\mathcal{B}(s;\boldsymbol{z}) \ll_\alpha 1 \quad \big(\sigma \geqslant \alpha,\ \sup_j |z_j| \leqslant \tfrac{4}{3}\big). \tag{1.7.19}$$

1.7.2.3 Pour $\mathscr{U}(s;\boldsymbol{z})$

Soit χ un caractère non principal modulo q. Pour $\sigma > \frac{1}{2}$, nous avons

$$\mathscr{T}(s,\chi) = \prod_p \frac{1-\chi(p)/p^s}{(1-1/p^s)^{\chi(p)}} = \mathrm{e}^{\vartheta(s,\chi)}$$

avec

$$\vartheta(s,\chi) := \sum_p \sum_{k\geqslant 2} \frac{\chi(p)-\chi(p)^k}{kp^{ks}}. \tag{1.7.20}$$

Pour tout $\alpha > \frac{1}{2}$, nous avons donc $\vartheta(s,\chi) \ll_\alpha 1$ sur le demi-plan $\sigma \geqslant \alpha$. Nous en déduisons que

$$\mathscr{U}(s;\boldsymbol{z}) \ll_\alpha 1 \quad \big(\sigma \geqslant \alpha,\ \boldsymbol{z} \ll 1\big). \tag{1.7.21}$$

1.7.2.4 Pour $\mathcal{V}(s;\boldsymbol{z})$

Il reste à estimer $\mathcal{V}(s;\boldsymbol{z})$. Le théorème de Landau-Page (c.f. par exemple [57], th. II.8.25) et le fait que q soit fixé impliquent l'existence d'une constante $c > 0$ tel que $\prod_{\chi\neq\chi_0} L(s,\chi)$ n'ait pas de zéro sur le domaine

$$\mathcal{D}_c := \big\{ s\in\mathbb{C} : \sigma > 1 - c/\log\big(q(|\tau|+2)\big)\big\}.$$

On en déduit classiquement (c.f., par exemple, [57], lemme II.8.26) via le lemme de la partie réelle, l'existence d'une constante $M_1 > 0$ telle que

$$\left|\frac{L'(s,\chi)}{L(s,\chi)}\right| \leqslant M_1 \log\big(q(|\tau|+2)\big) \qquad \big(s\in\mathcal{D}_c,\ \chi\neq\chi_0\big).$$

Posant $\eta_0 := \frac{1}{2}c/\log\big(q(|\tau|+2)\big)$ et $s_0 := \sigma_0 + i\tau$ où $\sigma_0 := 1+\eta_0$, nous obtenons, pour $1-2\eta_0 \leqslant \sigma < 1+\eta_0$,

$$\begin{aligned}\big|\log L(s,\chi)\big| &\leqslant \left|\int_{\sigma_0}^{\sigma} \frac{L'(u+i\tau,\chi)}{L(u+i\tau,\chi)}\mathrm{d}u\right| + \big|\log L(\sigma_0+i\tau,\chi)\big| \\ &\leqslant M_1 \log\big(q(|\tau|+2)\big)\eta_0 + \big|\log L(\sigma_0+i\tau,\chi)\big| \\ &\leqslant M_1 c + \big|\log L(\sigma_0+i\tau,\chi)\big|,\end{aligned}$$

et

$$\begin{aligned}\big|\log L(\sigma_0+i\tau,\chi)\big| &= \left|\sum_{n\geqslant 2}\frac{\Lambda(n)\chi(n)}{n^{s_0}\log n}\right| \leqslant \sum_{n\geqslant 2}\frac{\Lambda(n)}{n^{1+\eta_0}\log n} = \log\zeta(1+\eta_0) \\ &\leqslant \log\frac{1}{\eta_0} + O(1) = \log_2|\tau| + O(1).\end{aligned}$$

La même majoration est clairement valable pour $|\log L(s,\chi)|$ lorsque $\sigma \geqslant 1+\eta_0$. Il résulte de ces estimations que pour $\sigma \geqslant 1-2\eta_0$ et $\chi\neq\chi_0$, nous avons, pour $\boldsymbol{z}\ll 1$,

$$\big|L(s,\chi)^{D(\boldsymbol{z},\chi)}\big| \leqslant \exp\big\{|D(\boldsymbol{z},\chi)||\log L(s,\chi)|\big\} \ll \big(\log|\tau|\big)^{O(1)}, \tag{1.7.22}$$

et donc

$$\mathcal{V}(s;\boldsymbol{z}) = \prod_{\chi\neq\chi_0} L(s,\chi)^{D(\boldsymbol{z},\chi)} \ll \big(\log|\tau|\big)^{O(1)} \qquad \big(s\in\mathcal{D}_c,\ \boldsymbol{z}\ll 1\big). \tag{1.7.23}$$

1.7.2.5 Conclusion

Quitte à diminuer la valeur de c, nous pouvons supposer

$$\sigma_0 := 1 - \frac{c}{\log(2q)} > \max\{\sigma_1, \sigma_2\}$$

de sorte que $s \mapsto \mathscr{G}(s; \boldsymbol{z})$ est holomorphe sur $\mathcal{D}_c$. De plus, (1.7.9), (1.7.14), (1.7.19), (1.7.21) et (1.7.22) impliquent que, sur ce domaine, on peut trouver $M > 0$ et $K > 0$ tel que

$$\mathscr{G}(s; \boldsymbol{z}) \leqslant M\big\{ \log\big(q(|\tau| + 2)\big)\big\}^K.$$

Comme indiqué à la fin du §1.7.1, la formule asymptotique (1.7.12) en découle.

En reportant (1.7.12) dans (1.6.8) sous les conditions $1 < R_j < 2$ si $j \in I_q(\boldsymbol{\nu})$ et $0 < R_j < 2$ si $j \in J_q(\boldsymbol{\nu})$, nous obtenons, pour tout entier $N \geqslant 0$,

$$\mathcal{N}_{\boldsymbol{\nu}}(x) = \frac{x}{\log x} \sum_{0 \leqslant m \leqslant N} \frac{U_q^{(m)}(x; \boldsymbol{\nu})}{(\log x)^m} + \mathfrak{R}_q(x; \boldsymbol{\nu}) \tag{1.7.24}$$

avec, pour $0 \leqslant m \leqslant N$,

$$U_q^{(m)}(x; \boldsymbol{\nu}) := \frac{1}{(2i\pi)^{\varphi(q)}} \oint_{\mathcal{C}(\mathbf{0}, \boldsymbol{R})} (\log x)^{\mathfrak{S}(\boldsymbol{z})/\varphi(q)} \frac{\lambda_m(\boldsymbol{z})}{\wp(\boldsymbol{z}, \boldsymbol{\nu})} \, \mathrm{d}\boldsymbol{z} \tag{1.7.25}$$

où l'on a posé $\wp(\boldsymbol{z}, \boldsymbol{\nu}) := \prod_{j \in J_q(\boldsymbol{\nu})} z_j^{\nu_j + 1} \prod_{j \in I_q(\boldsymbol{\nu})} \big\{ z_j^{\varphi(q)}(z_j - 1)\big\}$, et

$$\mathfrak{R}_q(x; \boldsymbol{\nu}) \ll \frac{x}{(\log x)^{N+2}} \oint_{\mathcal{C}(\mathbf{0}, \boldsymbol{R})} (\log x)^{\Re\mathrm{e}(\mathfrak{S}(\boldsymbol{z}))/\varphi(q)} \frac{|\mathrm{d}\boldsymbol{z}|}{|\wp(\boldsymbol{z}, \boldsymbol{\nu})|}.$$

1.8 Étude de $\mathcal{N}_{\boldsymbol{\nu}}(x)$

Nous allons d'abord évaluer le terme principal dans l'expression (1.7.24), soit

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) := \frac{x}{\log x} U_q^{(0)}(x; \boldsymbol{\nu}), \tag{1.8.1}$$

où $U_q^{(0)}$ est défini en (1.7.25). D'après (1.7.11), le terme $\lambda_0(\boldsymbol{z})$ apparaissant dans l'intégrande s'écrit

$$\lambda_0(\boldsymbol{z}) = \frac{\mathscr{G}(1; \boldsymbol{z})}{\Gamma\big(\mathfrak{S}(\boldsymbol{z})/\varphi(q)\big)}.$$

La première étape consiste à utiliser la formule de Hankel (cf. par exemple le théorème II.0.17 de [57])

$$\frac{1}{\Gamma(z)} = \frac{1}{2i\pi} \int_{\mathcal{H}(r)} \xi^{-z} \mathrm{e}^{\xi} \mathrm{d}\xi \quad (z \in \mathbb{C}) \tag{1.8.2}$$

où r est un nombre réel strictement positif et $\mathcal{H}(r)$ est le contour de Hankel constitué du cercle $|\xi| = r$ privé du point $\xi = -r$, et de la demi-droite $]-\infty, -r]$ parcourue

deux fois, avec arguments respectifs $+\pi$ et $-\pi$. Ce contour est parcouru dans le sens direct. Nous avons

$$\mathscr{G}(1;\boldsymbol{z}) = \frac{q}{\varphi(q)} \prod_{j\in G_q} F_j(z_j)$$

avec

$$F_j(z) := \Big(\frac{\varphi(q)}{q}\Big)^{z/\varphi(q)} \mathcal{B}_j(1;z) \prod_{\chi\neq\chi_0} \mathscr{L}(\chi)^{z\overline{\chi(j)}/\varphi(q)}, \tag{1.8.3}$$

et $\mathscr{L}(\chi)$ est défini en (1.3.1). La fonction F_j est bornée pour tout $j \in G_q$.

1.8.1 Cas $I_q(\boldsymbol{\nu}) \neq \varnothing$

On suppose dans toute cette partie que $I_q(\boldsymbol{\nu}) \neq \varnothing$ (i.e. $|I_q(\boldsymbol{\nu})| \geqslant 1$). Tout d'abord, l'égalité (1.8.2) appliquée à $z = \mathfrak{S}(\boldsymbol{z})/\varphi(q)$ et $r > 0$ fournit

$$\frac{1}{\Gamma\big(\mathfrak{S}(\boldsymbol{z})/\varphi(q)\big)} = \frac{1}{2i\pi} \int_{\mathcal{H}(r)} \xi^{-\mathfrak{S}(\boldsymbol{z})/\varphi(q)} \mathrm{e}^{\xi} \mathrm{d}\xi.$$

En reportant cette égalité dans (1.8.1), nous obtenons

$$U_q^{(0)}(x,\boldsymbol{\nu}) = \frac{q}{(2i\pi)^{\varphi(q)+1}\varphi(q)} \oint_{\mathcal{C}(\mathbf{0},\boldsymbol{R})} \int_{\mathcal{H}(r)} \prod_{j\in G_q} V_j(z_j;\xi) \cdot \mathrm{e}^{\xi}\, \mathrm{d}\xi\, \mathrm{d}\boldsymbol{z}. \tag{1.8.4}$$

où nous avons posé

$$V_j(z;\xi) := \begin{cases} \Big(\dfrac{\log x}{\xi}\Big)^{z/\varphi(q)} \dfrac{F_j(z)}{z^{\varphi(q)}(z-1)} & \big(\text{si } j \in I_q(\boldsymbol{\nu})\big), \\ \Big(\dfrac{\log x}{\xi}\Big)^{z/\varphi(q)} \dfrac{F_j(z)}{z^{\nu_j+1}} & \big(\text{si } j \in J_q(\boldsymbol{\nu})\big). \end{cases} \tag{1.8.5}$$

1.8.1.1 Interversion des ordres d'intégration

Dans ce paragraphe, nous vérifions qu'on peut échanger les ordres d'intégration dans le membre de droite de (1.8.4), et parvenir ainsi au lemme suivant.

Rappelons la définition du contour de Hankel introduit en (1.8.2) et posons

$$H_j(\xi) := \frac{1}{2i\pi} \oint_{|z|=R_j} V_j(z;\xi)\, \mathrm{d}z \quad \big(\xi \in \mathcal{H}(r),\, j \in G_q\big). \tag{1.8.6}$$

où les fonctions V_j sont définies en (1.8.5).

Lemme 1.8.1. *Soit $\boldsymbol{R} \in (\mathbb{R}_+^*)^{G_q}$ tel que $R_j > 1$ dès que $j \in I_q(\boldsymbol{\nu})$. Pour x suffisamment grand, nous avons*

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) = \frac{qx}{2i\pi\varphi(q)\log x} \int_{\mathcal{H}(r)} \prod_{j\in G_q} H_j(\xi) \mathrm{e}^{\xi} \mathrm{d}\xi. \tag{1.8.7}$$

Démonstration. Il suffit de vérifier que les intégrales sur les parties rectilignes du contour de Hankel sont absolument convergentes, autrement dit que, pour chaque x fixé assez grand,

$$M_1 := \oint_{\mathcal{C}(\mathbf{0},\boldsymbol{R})} \int_r^\infty \prod_{j\in G_q} \Big|V_j(z_j;\sigma \mathrm{e}^{\pm i\pi})\Big| \cdot \Big|\mathrm{e}^{\sigma \mathrm{e}^{\pm i\pi}}\Big| \mathrm{d}\sigma \prod_{j\in G_q} |\mathrm{d}z_j| < \infty.$$

Or, pour $z \in \mathbb{C}$, $|z| = R_j$ et $\sigma \geqslant r$, nous avons

$$\Big|V_j(z;\sigma \mathrm{e}^{-i\pi})\Big| \ll_x \sigma^{-\Re \mathrm{e}(z)/\varphi(q)} \ll_x 1,$$

par définition des F_j et compte tenu des hypothèses sur les R_j, d'où

$$M_1 \ll_x \int_r^\infty \mathrm{e}^{-\sigma} \mathrm{d}\sigma \ll_x 1.$$

□

Passons maintenant à une étude plus approfondie des H_j définis par (1.8.6).

Les notations qui seront utilisées dans toute la suite du paragraphe 1.8 ont été définies au paragraphe 1.3.

1.8.1.2 Étude des H_j lorsque $j \in J_q(\boldsymbol{\nu})$

Notons traditionnellement par $\mathbb{P}$ l'ensemble de tous les nombres premiers. Pour $j \in G_q$, $\mathscr{P} \subset \mathbb{P}$, et $t \in \mathbb{N}$, nous posons

$$\mathcal{I}(t;\mathscr{P}) := \Big\{\boldsymbol{i} = (i_p)_{p\in\mathscr{P}} : \inf_p i_p \geqslant 0,\ \sum_{p\in\mathscr{P}} i_p = t\Big\}; \tag{1.8.8}$$

$$\mathscr{P}_j := \big\{p \in \mathbb{P} : p \equiv j \pmod q\big\}; \tag{1.8.9}$$

$$\mathcal{D}_j(t) := t! \sum_{\boldsymbol{i}\in\mathcal{I}(t;\mathscr{P}_j)} \prod_{p\in\mathscr{P}_j} \Big(\sum_{v+w=i_p} \frac{\big(\log(1-1/p)\big)^v}{v!p^w}\Big); \tag{1.8.10}$$

$$\ell_j(\xi) := \log\Big(\frac{\varphi(q)}{q}\Big) - \log\xi - \sum_{\chi\neq\chi_0} \overline{\chi(j)} \sum_p \chi(p) \log\Big(1-\frac{1}{p}\Big) \quad (\xi \in \mathcal{H}(r)), \tag{1.8.11}$$

où $\log\xi$ est déterminé grâce à la convention relative aux arguments sur le contour de Hankel définie au début du paragraphe 1.8.

L'objet du lemme suivant consiste à expliciter la quantité $\prod_{j\in J_q(\boldsymbol{\nu})} H_j(\xi)$.

Lemme 1.8.2. *Pour tout $\xi \in \mathcal{H}(r)$,*

$$\prod_{j\in J_q(\boldsymbol{\nu})} H_j(\xi) = \frac{(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})}}{\varphi(q)^{\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!} \sum_{\boldsymbol{t}\in\mathfrak{M}(\boldsymbol{\nu})} \binom{\boldsymbol{\nu}}{\boldsymbol{t}} \frac{\prod_{j\in J_q(\boldsymbol{\nu})} c_{t_j,j}(\xi)}{(\log_2 x)^{\mathsf{s}(\boldsymbol{t},\boldsymbol{\nu})}},$$

où $\mathfrak{M}(\boldsymbol{\nu})$ a été défini en (1.3.11) *et où l'on a posé, pour $j \in J_q(\boldsymbol{\nu})$, $0 \leqslant t \leqslant \nu_j$,*

$$c_{t,j}(\xi) := \sum_{0\leqslant v\leqslant t} \binom{t}{v} \varphi(q)^{t-v} \ell_j(\xi)^v \mathcal{D}_j(t-v). \tag{1.8.12}$$

Nous donnons d'abord une expression de $H_j(\xi)$ lorsque $j \in J_q(\boldsymbol{\nu})$.

Lemme 1.8.3. *Soit $j \in J_q(\boldsymbol{\nu})$. Alors pour tout $\xi \in \mathcal{H}(r)$,*

$$H_j(\xi) = \frac{1}{\nu_j!}\Big(\frac{\log_2 x}{\varphi(q)}\Big)^{\nu_j} \sum_{0\leqslant t\leqslant \nu_j} \binom{\nu_j}{t} \frac{c_{t,j}(\xi)}{(\log_2 x)^t}. \tag{1.8.13}$$

La déduction du Lemme 1.8.2 à partir du Lemme 1.8.3 est immédiate en calculant $\prod_{j\in J_q(\boldsymbol{\nu})} H_j(\xi)$ grâce à (1.8.13).

La démonstration du Lemme 1.8.3 repose sur le résultat suivant, établi par développement des fonctions en séries entières et récurrence sur l'ordre du développement. Nous notons $\rho_t(g)$ le coefficient d'indice t dans le développement de Taylor formel à l'origine d'une fonction holomorphe g.

Lemme 1.8.4. *Soient $\mathscr{P}$ un ensemble de nombres premiers (fini ou non), et*

$$\{f_p : p \in \mathscr{P}\}$$

une famille de fonctions holomorphes dans un ouvert contenant 0 telles que

$$f := \prod_{p\in\mathscr{P}} f_p.$$

Alors :

$$\rho_t(f) = \sum_{\boldsymbol{i}\in\mathcal{I}(t;\mathscr{P})} \Big(\prod_{p\in\mathscr{P}} \rho_{i_p}(f_p)\Big)$$

où $\mathcal{I}(t;\mathscr{P})$ est défini en (1.8.8).

Démonstration du Lemme 1.8.3. Pour $\xi \in \mathcal{H}(r)$, $z \in \mathbb{C}$ vérifiant $|z| < 2$, et $j \in J_q(\boldsymbol{\nu})$, nous posons $\mathcal{B}_j(z) := \mathcal{B}_j(1;z)$ tel que défini en (1.7.3) et

$$\mathcal{A}_{j,\xi}(z) := F_j(z)\Big(\frac{\log x}{\xi}\Big)^{z/\varphi(q)} = (\log x)^{z/\varphi(q)} \mathrm{e}^{z\ell_j(\xi)/\varphi(q)} \mathcal{B}_j(z).$$

La formule de Cauchy implique

$$H_j(\xi) = \frac{\mathcal{A}_{j,\xi}^{(\nu_j)}(0)}{\nu_j!}.$$

De plus, une double application de la formule de Leibniz fournit

$$\mathcal{A}_{j,\xi}^{(\nu_j)}(z) = \mathrm{e}^{z\ell_j(\xi)/\varphi(q)} \sum_{0\leqslant t\leqslant\nu_j} \binom{\nu_j}{t} \Big(\frac{\log_2 x}{\varphi(q)}\Big)^{\nu_j-t} \sum_{0\leqslant v\leqslant t} \binom{t}{v} \Big(\frac{\ell_j(\xi)}{\varphi(q)}\Big)^v \mathcal{B}_j{}^{(t-v)}(z).$$

Considérons le développement de Taylor

$$\mathscr{W}_p(z) := \Big(1-\frac{1}{p}\Big)^z \Big(1-\frac{z}{p}\Big)^{-1} = \sum_{t\geqslant 0} z^t \sum_{v+w=t} \frac{\big(\log(1-1/p)\big)^v}{v!\, p^w}.$$

Une application du Lemme 1.8.4, avec $\mathscr{P} := \mathscr{P}_j$, $f_p := \mathscr{W}_p$, et $f := \mathcal{B}_j$, fournit $\mathcal{B}_j^{(t)}(0) = \mathcal{D}_j(t)$, où $\mathcal{D}_j$ est défini en (1.8.9). Cela implique

$$\mathcal{A}_{j,\xi}^{(\nu_j)}(0) = \sum_{0\leqslant t\leqslant \nu_j} \binom{\nu_j}{t} \frac{(\log_2 x)^{\nu_j - t}}{\varphi(q)^{\nu_j}} c_{t,j}(\xi),$$

d'où (1.8.13). □

1.8.1.3 Étude des H_j lorsque $j \in I_q(\boldsymbol{\nu})$

Rappelons la définition des fonctions F_j en (1.8.3). Pour $j \in I_q(\boldsymbol{\nu})$, $0 \leqslant k \leqslant \mathfrak{I}(a)$, $\xi \in \mathcal{H}(r)$, $z \in \mathbb{C}$, $z \neq 1$, nous posons

$$\mathscr{D}_{j,\xi}(z;x) := \frac{F_j(z)}{z-1}\left(\frac{\log x}{\xi}\right)^{z/\varphi(q)}, \tag{1.8.14}$$

$$g_{k,\xi}(\log_2 x) := \frac{\xi^{(k-|I_q(\boldsymbol{\nu})|)/\varphi(q)}}{((\varphi(q)-1)!)^k} \sum_{\substack{K\subseteq I_q(\boldsymbol{\nu})\\ |K|=k}} \prod_{j\in I_q(\boldsymbol{\nu})\smallsetminus K} F_j(1) \cdot \prod_{j\in K} \mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(0;x). \tag{1.8.15}$$

La formule de Leibniz fournit

$$\mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(0;x) = \sum_{0\leqslant \ell\leqslant \varphi(q)-1} \binom{\varphi(q)-1}{\ell} \left(\frac{\log_2 x}{\varphi(q)}\right)^{\ell} \mathfrak{d}_{j,\xi}(\ell)$$

où $\mathfrak{d}_{j,\xi}(\ell)$ est indépendant de x. La quantité $\mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(0;x)$ est donc polynomiale en $\log_2 x$, et $g_{k,\xi}(\log_2 x)$ est un polynôme de degré au plus $\varphi(q)-1$ en $\log_2 x$.

Lemme 1.8.5. *Pour tout $\xi \in \mathcal{H}(r)$, nous avons*

$$\prod_{j\in I_q(\boldsymbol{\nu})} H_j(\xi) = (\log x)^{|I_q(\boldsymbol{\nu})|/\varphi(q)} \sum_{0\leqslant k\leqslant |I_q(\boldsymbol{\nu})|} \frac{g_{k,\xi}(\log_2 x)}{(\log x)^{k/\varphi(q)}}. \tag{1.8.16}$$

Démonstration. Soit $j \in I_q(\boldsymbol{\nu})$. L'hypothèse $R_j > 1$ et le théorème des résidus nous permettent d'écrire (1.8.6) sous la forme

$$H_j(\xi) = F_j(1)(\log x)^{1/\varphi(q)}\xi^{-1/\varphi(q)} + h_j(\xi)$$

où, pour tout $r_j \in]0,1[$,

$$h_j(\xi) := \frac{1}{2i\pi} \oint_{|z|=r_j} \left(\frac{\log x}{\xi}\right)^{z/\varphi(q)} \frac{F_j(z)\mathrm{d}z}{z^{\varphi(q)}(z-1)} \quad (\xi \in \mathcal{H}(r)).$$

Il suit

$$\prod_{j\in I_q(\boldsymbol{\nu})} H_j(\xi) = \sum_{K\subseteq I_q(\boldsymbol{\nu})} \prod_{j\in K} h_j(\xi) \prod_{j\in I_q(\boldsymbol{\nu})\smallsetminus K} \left(\frac{\log x}{\xi}\right)^{1/\varphi(q)} F_j(1).$$

De plus, le théorème de Cauchy implique

$$h_j(\xi) = \frac{\mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(0;x)}{(\varphi(q)-1)!}. \tag{1.8.17}$$

Nous obtenons bien le résultat annoncé en regroupant les sous-ensembles $K \subseteq G_q$ de même cardinal. □

Remarque 1.8.6. *On vérifie aisément, grâce à l'orthogonalité des caractères, que l'on a, pour $j \in I_q(\boldsymbol{\nu})$,*

$$F_j(1) = \Big(\frac{\varphi(q)}{q}\Big)^{1/\varphi(q)} \prod_{\chi\neq\chi_0} \mathscr{L}(\chi)^{\overline{\chi(j)}/\varphi(q)} = \prod_p \Big(1-\frac{1}{p}\Big)^{1/\varphi(q)-\delta_j(p)} \tag{1.8.18}$$

où l'on a posé $\delta_j(p) := \begin{cases} 1 & \text{si } p \equiv j \pmod q, \\ 0 & \text{dans le cas contraire.} \end{cases}$

1.8.1.4 Estimation asymptotique de $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$

Rappelons que, pour $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ et $k \in \mathbb{N}$, le nombre entier $d_{k,\boldsymbol{\nu}}$ est défini en (1.4.9).

Compte tenu des résultats des paragraphes précédents, il est possible d'obtenir une formulation explicite de la quantité $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$ lorsque $I_q(\boldsymbol{\nu}) \neq \varnothing$ grâce à l'utilisation de la formule du binôme, de la formule de Leibniz et des propriétés du contour de Hankel.

Lemme 1.8.7. *Pour tout $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ tel que $I_q(\boldsymbol{\nu}) \neq \varnothing$, nous avons*

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) = \frac{x}{(\log x)^{1-|I_q(\boldsymbol{\nu})|/\varphi(q)}} \sum_{0\leqslant k\leqslant |I_q(\boldsymbol{\nu})|} \frac{P_{0,k,\boldsymbol{\nu}}(\log_2 x)}{(\log x)^{k/\varphi(q)}},$$

où

$$P_{0,k,\boldsymbol{\nu}}(\xi) := \sum_{0\leqslant n\leqslant d_{k,\boldsymbol{\nu}}} \alpha_{\boldsymbol{\nu},k,n}\, \xi^{d_{k,\boldsymbol{\nu}}-n} \qquad (k\in\mathbb{N}) \tag{1.8.19}$$

est un polynôme en ξ de degré au plus $d_{k,\boldsymbol{\nu}}$, avec égalité si $k=0$.

Remarque 1.8.8. *L'expression exacte des coefficients $\alpha_{\boldsymbol{\nu},k,n}$ est donnée en* (1.8.27) infra.

Démonstration. Rappelons la définition des ensembles $\mathfrak{M}(\boldsymbol{\nu})$ et $\mathfrak{N}(\boldsymbol{\nu})$ respectivement en (1.3.11) et (1.3.13), et celle des fonctions ℓ_j en (1.8.11). Posant

$$\mathfrak{A}_{k,\xi,\boldsymbol{t}}(x) := \frac{g_{k,\xi}(\log_2 x)(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})-\mathsf{s}(\boldsymbol{t},\boldsymbol{\nu})}}{\varphi(q)^{\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!(\log x)^{(k-|I_q(\boldsymbol{\nu})|)/\varphi(q)}} \quad (k\in\mathbb{N},\, \xi\in\mathcal{H}(r),\, \boldsymbol{t}\in H_q),$$

il résulte des Lemmes 1.8.2 et 1.8.5 que

$$\prod_{j\in G_q} H_j(\xi) = \sum_{0\leqslant k\leqslant |I_q(\boldsymbol{\nu})|} \sum_{\boldsymbol{t}\in\mathfrak{M}(\boldsymbol{\nu})} \binom{\boldsymbol{\nu}}{\boldsymbol{t}} \mathfrak{A}_{k,\xi,\boldsymbol{t}}(x) \prod_{j\in J_q(\boldsymbol{\nu})} c_{t_j,j}(\xi), \tag{1.8.20}$$

Développant les termes $\ell_j(\xi)^v = \big(-\log\xi + L_j\big)^v$ par la formule du binôme en posant

$$L_j := \ell_j(1) = \log\Big(\frac{\varphi(q)}{q}\Big) - \sum_{\chi\neq\chi_0} \overline{\chi(j)} \sum_p \chi(p)\log\Big(1-\frac{1}{p}\Big) \quad (j\in J_q(\boldsymbol{\nu})),$$

nous déduisons de (1.8.12) que, pour tout $t\in\mathbb{N}$,

$$c_{t,j}(\xi) = \sum_{\substack{a+b+c=t\\ \min(a,b,c)\geqslant 0}} \binom{t}{a,b,c} (-\log\xi)^c \mathcal{D}_j(a)\varphi(q)^a L_j^b \tag{1.8.21}$$

où $\mathcal{D}_j$ est défini en (1.8.10).

De plus, en posant $\boldsymbol{u}_m := (u_{j,m})_{j\in G_q} \in \mathfrak{M}(\boldsymbol{\nu})$ $(m\in\mathbb{N})$, $\boldsymbol{u} := (\boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3,\boldsymbol{u}_4)$ et

$$\mathfrak{B}(\boldsymbol{u}) := \binom{\boldsymbol{\nu}}{\boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3,\boldsymbol{u}_4} \prod_{j\in J_q(\boldsymbol{\nu})} \frac{\varphi(q)^{u_{j,2}} L_j^{u_{j,3}} \mathcal{D}_j(u_{j,2})}{(\nu_j-u_{j,1})!}, \tag{1.8.22}$$

nous déduisons de (1.8.21) via une interversion somme-produit que

$$\binom{\boldsymbol{\nu}}{\boldsymbol{u}_1} \prod_{j\in J_q(\boldsymbol{\nu})} c_{u_{j,1},j}(\xi) = \sum_{\substack{\boldsymbol{u}_m\in\mathfrak{M}(\boldsymbol{u}_1,\boldsymbol{\nu})\\ (2\leqslant m\leqslant 4)\\ \sum_{2\leqslant m\leqslant 4}\boldsymbol{u}_m=\boldsymbol{u}_1}} \mathfrak{B}(\boldsymbol{u})(-\log\xi)^{\mathsf{s}(\boldsymbol{u}_4,\boldsymbol{\nu})}. \tag{1.8.23}$$

À présent, reprenons la définition de $\mathscr{D}_{j,\xi}(z;x)$ en (1.8.14). Rappelant que ℓ_j est défini par (1.8.11), nous pouvons réécrire

$$\mathscr{D}_{j,\xi}(z;x) = \big(\mathrm{e}^{\ell_j(\xi)}\log x\big)^{z/\varphi(q)} \frac{\mathcal{B}_j(1;z)}{z-1}$$

et, pour $(w_1,w_3,w_4)\in[\![0;\varphi(q)-1]\!]^3$,

$$\mathcal{X}(w_1,w_3,w_4) := -\binom{\varphi(q)-1}{\varphi(q)-1-w_1,w_3,w_4} \frac{\mathcal{D}_j(w_3)}{\varphi(q)^{\varphi(q)-1-w_1+w_4}}.$$

Une triple application de la formule de Leibniz fournit

$$\mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(z;x) = \big(\mathrm{e}^{\ell_j(\xi)}\log x\big)^{z/\varphi(q)} {\sum_w}' \frac{(\log_2 x)^{\varphi(q)-1-w_1}\mathcal{X}(w_1,w_3,w_4)\ell_j(\xi)^{w_4}}{(1-z)^{w_2+1}}$$

où la somme $\sum'$ est indicée sur l'ensemble des $w := (w_1,w_2,w_3,w_4)\in[\![0;\varphi(q)-1]\!]^4$ vérifiant $w_2+w_3+w_4=w_1$.

Si nous notons, pour $w\in[\![0;\varphi(q)-1]\!]^4$,

$$\mathcal{Y}(w) := \binom{w_3+w_4}{w_4} L_j^{w_3} \mathcal{X}(w_1,w_2,w_3+w_4),$$

il résulte de la formule du binôme que

$$\mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(0;x) = {\sum_w}'' (\log_2 x)^{\varphi(q)-1-w_1}\mathcal{Y}(w)(-\log\xi)^{w_4} \tag{1.8.24}$$

où la somme $\sum''$ est indicée sur l'ensemble des $w \in [\![0;\varphi(q)-1]\!]^4$ vérifiant $\sum_{2\leqslant m\leqslant 4} w_m \leqslant w_1$.

En posant $\boldsymbol{v}_0 := (\varphi(q)-1)_{j\in G_q}$ et, pour $K \subseteq I_q(\boldsymbol{\nu})$, $\boldsymbol{v} := (\boldsymbol{v}_1,\boldsymbol{v}_2,\boldsymbol{v}_3,\boldsymbol{v}_4) \in \mathfrak{M}_K(\boldsymbol{v}_0)^4$ vérifiant $\boldsymbol{v}_m := (v_{j,m})_{j\in G_q}$,

$$\mathcal{Z}(\boldsymbol{v}) := \prod_{j\in K} \mathcal{Y}((v_{j,1},v_{j,2},v_{j,3},v_{j,4})),$$

il suit de (1.8.24) que

$$\prod_{j\in K} \mathscr{D}_{j,\xi}^{(\varphi(q)-1)}(0;x) = (\log_2 x)^{(\varphi(q)-1)|K|} \sum_{\boldsymbol{v}\in\mathfrak{N}_K(\boldsymbol{v}_0)} \frac{\mathcal{Z}(\boldsymbol{v})(-\log\xi)^{\mathsf{s}_K(\boldsymbol{v}_4)}}{(\log_2 x)^{\mathsf{s}_K(\boldsymbol{v}_1)}}. \tag{1.8.25}$$

Les égalités (1.8.7), (1.8.15), (1.8.17), (1.8.20), (1.8.23), (1.8.25) ainsi que l'application de la propriété

$$\int_{\mathcal{H}(r)} \xi^{-z}(-\log\xi)^m \mathrm{e}^{\xi}\mathrm{d}\xi = 2i\pi\Big(\frac{1}{\Gamma}\Big)^{(m)}(z) \tag{1.8.26}$$

au cas $z := (|I_q(\boldsymbol{\nu})|-k)/\varphi(q)$ et $m := \mathsf{s}(\boldsymbol{u}_4,\boldsymbol{\nu})+\mathsf{s}_K(\boldsymbol{v}_4)$ où $\boldsymbol{u}_4,\boldsymbol{v}_4 \in \mathbb{N}^{G_q}$ et $K \subseteq I_q$ de cardinal k, impliquent alors, en réordonnant les termes, le résultat voulu, en posant

$$\alpha_{\boldsymbol{\nu},k,n} := \frac{q}{\varphi(q)^{1+\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!\big((\varphi(q)-1)!\big)^k}\alpha^{(1)}_{\boldsymbol{\nu},k,n} \quad (n\in\mathbb{N}), \tag{1.8.27}$$

avec

$$\alpha^{(1)}_{\boldsymbol{\nu},k,n} := \sum_{\substack{0\leqslant n_1\leqslant \mathsf{s}(\boldsymbol{\nu})\\ 0\leqslant n_2\leqslant(\varphi(q)-1)k\\ n_1+n_2=n}} \sum_{\substack{\boldsymbol{u}\in\mathfrak{N}(\boldsymbol{\nu})\\ \mathsf{s}(\boldsymbol{u}_1,\boldsymbol{\nu})=n_1}} \mathfrak{B}(\boldsymbol{u}) \sum_{\substack{K\subseteq I_q(\boldsymbol{\nu})\\ |K|=k}} \prod_{j\in I_q(\boldsymbol{\nu})\smallsetminus K} F_j(1)$$
$$\times \sum_{\substack{\boldsymbol{v}\in\mathfrak{N}_K(\boldsymbol{v}_0)\\ \mathsf{s}_K(\boldsymbol{v}_1)=n_2}} \mathcal{Z}(\boldsymbol{v})\Big(\frac{1}{\Gamma}\Big)^{(\mathsf{s}(\boldsymbol{u}_4,\boldsymbol{\nu})+\mathsf{s}_K(\boldsymbol{v}_4))}\Big(\frac{|I_q(\boldsymbol{\nu})|-k}{\varphi(q)}\Big).$$

De plus, nous obtenons bien $\alpha_{\boldsymbol{\nu},0,0} \neq 0$ — cf. Remarque 1.8.9 ci-dessous. □

Remarque 1.8.9. *Il découle des calculs précédents que le terme principal de* $\mathcal{N}^{(0)}_{\boldsymbol{\nu}}(x)$ *vaut*

$$\frac{\alpha_{\boldsymbol{\nu},0,0}\, x(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})}}{(\log x)^{1-|I_q(\boldsymbol{\nu})|/\varphi(q)}}$$

avec

$$\alpha_{\boldsymbol{\nu},0,0} = \frac{q\prod_{j\in I_q(\boldsymbol{\nu})} F_j(1)}{\Gamma\big(|I_q(\boldsymbol{\nu})|/\varphi(q)\big)\varphi(q)^{1+\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!} > 0,$$

puisqu'il résulte de (1.8.18) *que*

$$\frac{q}{\varphi(q)}\prod_{j\in I_q(\boldsymbol{\nu})} F_j(1) = C_q(\boldsymbol{\nu}).$$

1.8.2 Cas $I_q(\boldsymbol{\nu}) = \varnothing$

La difficulté principale qui contraint à différencier les cas où $I_q(\boldsymbol{\nu})$ est l'ensemble vide ou non vient de l'application de la formule (1.8.26) à $z := (|I_q(\boldsymbol{\nu})| - k)/\varphi(q)$ dans le calcul de l'estimation de $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$, puisque $z = 0$ lorsque $I_q(\boldsymbol{\nu}) = \varnothing$, et que la fonction $1/\Gamma$ admet un zéro en 0, ce qui implique $\alpha_{\boldsymbol{\nu},0,0} = 0$. Cependant, une utilisation adaptée à ce cas de la formule de Hankel permet de contourner cette difficulté. Elle fournit alors une estimation de $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$ lorsque $I_q(\boldsymbol{\nu}) = \varnothing$ avec une formulation explicite de son terme principal. Cette utilisation fait l'objet du Lemme 1.8.10.

Lemme 1.8.10. *Pour tout $\boldsymbol{\nu} \in \mathcal{E}_q$ tel que $I_q(\boldsymbol{\nu}) = \varnothing$, nous avons*

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) = \frac{x}{\log x} P_{0,0,\boldsymbol{\nu}}(\log_2 x) \tag{1.8.28}$$

où

$$P_{0,0,\boldsymbol{\nu}}(\xi) := \sum_{0 \leqslant n \leqslant \mathsf{s}(\boldsymbol{\nu})-1} \beta_{\boldsymbol{\nu},n} \xi^{\mathsf{s}(\boldsymbol{\nu})-1-n}, \tag{1.8.29}$$

est un polynôme en ξ de degré $\mathsf{s}(\boldsymbol{\nu}) - 1$.

Remarque 1.8.11. *L'expression exacte des coefficients $\beta_{\boldsymbol{\nu},n}$ sera donnée en* (1.8.33) infra.

Démonstration. Nous nous limitons à indiquer les grandes lignes de la démonstration de l'estimation de $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$ lorsque $I_q(\boldsymbol{\nu}) = \varnothing$, les calculs étant similaires à ceux du cas $I_q(\boldsymbol{\nu}) \neq \varnothing$.

Lorsque $I_q(\boldsymbol{\nu}) = \varnothing$, choisissons $r = 1$, $z = 1 + \mathfrak{S}(\boldsymbol{z})/\varphi(q)$ dans (1.8.2). Nous obtenons

$$\frac{1}{\Gamma\big(\mathfrak{S}(\boldsymbol{z})/\varphi(q)\big)} = \frac{\mathfrak{S}(\boldsymbol{z})}{2i\pi\varphi(q)} \int_{\mathcal{H}(1)} \xi^{-\mathfrak{S}(\boldsymbol{z})/\varphi(q)} \xi^{-1} \mathrm{e}^{\xi} \, \mathrm{d}\xi.$$

Rappelons la définition des fonctions H_j en (1.8.6) et posons

$$\widetilde{H_k}(\xi) := \frac{1}{2i\pi} \oint_{|z|=R_k} F_k(z) (\log x)^{z/\varphi(q)} \xi^{-z/\varphi(q)} \frac{\mathrm{d}z}{z^{\nu_k}} \quad \big(k \in G_q,\ \xi \in \mathcal{H}(1)\big).$$

En ouvrant la somme $\mathfrak{S}(\boldsymbol{z}) = \sum_{k \in G_q} z_k$, nous pouvons réécrire (1.8.1) sous la forme

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) = \frac{qx}{(2i\pi)^{\varphi(q)+1} \varphi(q)^2 \log x} \sum_{k \in G_q} \int_{\mathcal{H}(1)} \widetilde{H_k}(\xi) \prod_{\substack{j \in G_q \\ j \neq k}} H_j(\xi) \xi^{-1} \mathrm{e}^{\xi} \mathrm{d}\xi.$$

Le Lemme 1.8.3 fournit

$$\widetilde{H_k}(\xi) = \frac{1}{(\nu_k - 1)!} \left(\frac{\log_2 x}{\varphi(q)} \right)^{\nu_k - 1} \sum_{0 \leqslant t \leqslant \nu_k - 1} \binom{\nu_k - 1}{t} \frac{c_{t,k}(\xi)}{(\log_2 x)^t} \quad (\nu_k \geqslant 1),$$

et la formule de Cauchy implique

$$\widetilde{H_k}(\xi) = 0 \quad (\nu_k = 0).$$

Sous la condition $t \leqslant \nu_k$, les identités

$$\binom{\nu_k}{t}\frac{\nu_k - t}{\nu_k!} = \begin{cases} \dfrac{1}{(\nu_k-1)!}\dbinom{\nu_k - 1}{t} & \text{si } t \leqslant \nu_k - 1 \text{ et } \nu_k \neq 0; \\ 0 & \text{dans le cas contraire} \end{cases}$$

permettent d'écrire

$$\widetilde{H_k}(\xi) = \frac{(\log_2 x)^{\nu_k - 1}}{\nu_k!\varphi(q)^{\nu_k - 1}} \sum_{0 \leqslant t \leqslant \nu_k} \binom{\nu_k}{t} \frac{(\nu_k - t)c_{t,k}(\xi)}{(\log_2 x)^t}. \tag{1.8.30}$$

D'autre part, il résulte de (1.8.13) que

$$\prod_{\substack{j \in G_q \\ j \neq k}} H_j(\xi) = \frac{(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu}) - \nu_k}\nu_k!}{\varphi(q)^{\mathsf{s}(\boldsymbol{\nu}) - \nu_k}\boldsymbol{\nu}!} \sum_{\boldsymbol{t} \in \mathfrak{M}_{G_q \smallsetminus \{k\}}(\boldsymbol{\nu})} \binom{\boldsymbol{\nu}}{\boldsymbol{t}} \frac{\prod_{j \in G_q} c_{t_j,j}(\xi)}{(\log_2 x)^{\mathsf{s}(\boldsymbol{t},\boldsymbol{\nu})}}. \tag{1.8.31}$$

En rappelant la définition de $\mathfrak{B}$ en (1.8.22), les formules (1.8.23), (1.8.30) et (1.8.31) nous donnent

$$\widetilde{H_k}(\xi) \prod_{\substack{j \in G_q \\ j \neq k}} H_j(\xi) = \frac{(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})-1}}{\varphi(q)^{\mathsf{s}(\boldsymbol{\nu})-1}\boldsymbol{\nu}!} \sum_{\boldsymbol{u} \in \mathfrak{N}(\boldsymbol{\nu})} \frac{\mathfrak{B}(\boldsymbol{u})(\nu_k - u_{k,1})}{(\log_2 x)^{\mathsf{s}(\boldsymbol{u}_1,\boldsymbol{\nu})}}(-\log \xi)^{\mathsf{s}(\boldsymbol{u}_4,\boldsymbol{\nu})}.$$

Il résulte de cette expression et de l'application de l'égalité (1.8.26) au cas $z = 1$ et $m = \mathsf{s}(\boldsymbol{u}_4, \boldsymbol{\nu})$ que

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) = \frac{qx(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})-1}}{\varphi(q)^{1+\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}! \ln x} \sum_{\boldsymbol{u} \in \mathfrak{N}(\boldsymbol{\nu})} \mathfrak{B}(\boldsymbol{u}) \frac{\mathsf{s}(\boldsymbol{\nu}) - \mathsf{s}(\boldsymbol{u}_1, \boldsymbol{\nu})}{(\log_2 x)^{\mathsf{s}(\boldsymbol{u}_1,\boldsymbol{\nu})}} \Big(\frac{1}{\Gamma}\Big)^{(\mathsf{s}(\boldsymbol{u}_4,\boldsymbol{\nu}))}(1).$$

En réordonnant les termes, nous avons

$$\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x) \;=\; \frac{x(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})-1}}{\log x} \sum_{0 \leqslant n < \mathsf{s}(\boldsymbol{\nu})} \frac{\beta_{\boldsymbol{\nu},n}}{(\log_2 x)^n} \tag{1.8.32}$$

où l'on a posé

$$\beta_{\boldsymbol{\nu},n} := \frac{q(\mathsf{s}(\boldsymbol{\nu}) - n)}{\varphi(q)^{1+\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}!} \sum_{\substack{\boldsymbol{u} \in \mathfrak{N}(\boldsymbol{\nu}) \\ \mathsf{s}(\boldsymbol{u}_1,\boldsymbol{\nu}) = n}} \mathfrak{B}(\boldsymbol{u}) \Big(\frac{1}{\Gamma}\Big)^{(\mathsf{s}(\boldsymbol{u}_4,\boldsymbol{\nu}))}(1) \quad (0 \leqslant n < \mathsf{s}(\boldsymbol{\nu})). \tag{1.8.33}$$

Nous obtenons bien le résultat annoncé. □

Remarque 1.8.12. *Les formules précédentes impliquent que le terme principal de* $\mathcal{N}_{\boldsymbol{\nu}}^{(0)}(x)$ *vaut*

$$\frac{q\mathsf{s}(\boldsymbol{\nu})x(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})-1}}{\varphi(q)^{1+\mathsf{s}(\boldsymbol{\nu})}\boldsymbol{\nu}! \log x}.$$

1.8.3 Cas général

Rappelons la définition de $U_q^{(m)}(x;\boldsymbol{\nu})$ en (1.7.25). Dans ce paragraphe, nous décrivons brièvement comment l'on peut obtenir un développement asymptotique pour

$$\mathcal{N}_{\boldsymbol{\nu}}^{(m)}(x) := \frac{x\,U_q^{(m)}(x;\boldsymbol{\nu})}{(\log x)^{1+m}} \quad (m \in \mathbb{N}^*). \tag{1.8.34}$$

Pour cela, nous posons, pour $\boldsymbol{z}_K := (\widetilde{z}_j)_{j\in G_q}$ vérifiant $\widetilde{z}_j := z_j$ si $j \in J_q(\boldsymbol{\nu}) \cup K$ et $\widetilde{z}_j := 1$ dans le cas contraire,

$$\mathfrak{F}_m(\boldsymbol{z}_K) := \frac{\lambda_m(\boldsymbol{z}_K)(\log x)^{\mathfrak{S}(\boldsymbol{z}_K)/\varphi(q)}}{\prod_{j\in K}(z_j-1)},$$
$$W_K^{(m)}(x;\boldsymbol{\nu}) := \frac{1}{(2i\pi)^{k+|J_q(\boldsymbol{\nu})|}} \oint_{\substack{|z_j|=R_j\\ j\in J_q(\boldsymbol{\nu})}} \oint_{\substack{|z_j|=r_j\\ j\in K}} \mathfrak{F}_m(\boldsymbol{z}_K) \prod_{j\in J_q(\boldsymbol{\nu})} \frac{\mathrm{d}z_j}{z_j^{\nu_j+1}} \prod_{j\in K} \frac{\mathrm{d}z_j}{z_j^{\varphi(q)}}.$$

En appliquant le théorème des résidus de la même manière que dans le cas $m = 0$, il suit

$$U_q^{(m)}(x;\boldsymbol{\nu}) = \sum_{0\leqslant k\leqslant |I_q(\boldsymbol{\nu})|} (2i\pi)^{|I_q(\boldsymbol{\nu})|-k} (\log x)^{(|I_q(\boldsymbol{\nu})|-k)/\varphi(q)} \sum_{\substack{K\subseteq I_q(\boldsymbol{\nu})\\ |K|=k}} W_K^{(m)}(x;\boldsymbol{\nu}). \tag{1.8.35}$$

Lorsque $I_q(\boldsymbol{\nu}) \neq \varnothing$, il résulte du théorème de Cauchy que

$$W_K^{(m)}(x;\boldsymbol{\nu}) = \frac{1}{\boldsymbol{\nu}!((\varphi(q)-1)!)^{|K|}} \Big(\prod_{j\in J_q(\boldsymbol{\nu})} \frac{\partial^{\nu_j}}{\partial z_j^{\nu_j}} \prod_{j\in K} \frac{\partial^{\varphi(q)-1}}{\partial z_j^{\varphi(q)-1}} \mathfrak{F}_m \Big)(\mathbf{0}). \tag{1.8.36}$$

Lorsque $I_q(\boldsymbol{\nu}) = K = \varnothing$, nous avons $\boldsymbol{z}_K = \boldsymbol{z}$ et nous posons $\mathfrak{H}_m(\boldsymbol{z}) := \mathfrak{F}_m(\boldsymbol{z})/\mathfrak{S}(\boldsymbol{z})$. Nous obtenons alors grâce au théorème de Cauchy

$$W_\varnothing^{(m)}(x;\boldsymbol{\nu}) = \frac{1}{\boldsymbol{\nu}!} \sum_{\ell\in G_q} \nu_\ell \Big(\frac{\partial^{\nu_\ell-1}}{\partial z_\ell^{\nu_\ell-1}} \prod_{\substack{j\in G_q\\ j\neq\ell}} \frac{\partial^{\nu_j}}{\partial z_j^{\nu_j}} \mathfrak{H}_m \Big)(\mathbf{0}). \tag{1.8.37}$$

Dans les deux cas, la formule de Leibniz implique alors que l'expression

$$\sum_{\substack{K\subseteq G_q\\ |K|=k}} W_K^{(m)}(x;\boldsymbol{\nu})$$

est un polynôme en $\log_2 x$, noté $P_{m,k,\boldsymbol{\nu}}(\log_2 x)$. Les expressions (1.8.34) à (1.8.37) fournissent

$$\mathcal{N}_{\boldsymbol{\nu}}^{(m)}(x) = \frac{x}{(\log x)^{1-|I_q(\boldsymbol{\nu})|/\varphi(q)+m}} \sum_{0\leqslant k\leqslant |I_q(\boldsymbol{\nu})|} \frac{P_{m,k,\boldsymbol{\nu}}(\ln_2 x)}{(\log x)^{k/\varphi(q)}}.$$

Remarques 1.8.13. (i) *Lorsque $I_q(\boldsymbol{\nu}) \neq \varnothing$, l'application de la formule de Leibniz à* (1.8.36) *implique que* $\deg P_{m,k,\boldsymbol{\nu}} \leqslant d_{k,\boldsymbol{\nu}}$, *où $d_{k,\boldsymbol{\nu}}$ est défini en* (1.4.9).

(ii) *Lorsque $I_q(\boldsymbol{\nu}) = \varnothing$, on obtient semblablement, à partir de* (1.8.37), *que*

$$\deg P_{m,0,\boldsymbol{\nu}} \leqslant d_{0,\boldsymbol{\nu}} - 1.$$

1.8.4 Étude du terme d'erreur

Précisons le terme d'erreur de (1.7.24), c'est-à-dire

$$\mathfrak{R} := \frac{x}{(\log x)^{N+2}} \oint_{\mathcal{C}(\mathbf{0},\boldsymbol{R})} \prod_{j\in G_q} \big|V_j(z;1)\big| \prod_{j\in G_q} |\mathrm{d}z_j|.$$

où V_j a été défini par (1.8.5).

Rappelons que $0 < R_j < 2$ si $j \in J_q(\boldsymbol{\nu})$ et $1 < R_j < 2$ si $j \in I_q(\boldsymbol{\nu})$.

Soit $j \in I_q(\boldsymbol{\nu})$. Nous avons alors

$$\big|V_j(z;1)\big| \ll \frac{(\log x)^{\Re e(z)/\varphi(q)}}{R_j^{\varphi(q)}(R_j-1)}\cdot$$

Définissons $\boldsymbol{\delta} \in (\mathbb{R}_+^*)^{G_q}$ par $R_j = 1 + \delta_j\varphi(q)/\log_2 x$, de sorte que

$$(\log x)^{\Re e(z)/\varphi(q)} \ll (\log x)^{1/\varphi(q)} \qquad (|z| = R_j).$$

Il suit

$$\begin{aligned}\oint_{|z|=R_j} \big|V_j(z;1)\mathrm{d}z\big| &\ll (\log_2 x)(\log x)^{1/\varphi(q)} \oint_{|z|=R_j} |\mathrm{d}z| \\ &\ll (\log_2 x)(\log x)^{1/\varphi(q)}.\end{aligned} \tag{1.8.38}$$

On procède de la même manière pour $j \in J_q(\boldsymbol{\nu})$ en posant $R_j := \delta_j\varphi(q)/\log_2 x$, ce qui implique $(\log x)^{\Re e(z)/\varphi(q)} \ll 1$ si $|z| = R_j$, et en effectuant le changement de variables $w := z\log_2 x/\varphi(q)$. Il vient

$$\oint_{|z|=R_j} \big|V_j(z;1)\mathrm{d}z\big| \ll (\log_2 x)^{\nu_j} \oint_{|w|=\delta_j} |\mathrm{d}w| \ll (\log_2 x)^{\nu_j}. \tag{1.8.39}$$

Les estimations (1.8.38) et (1.8.39) impliquent ainsi

$$\mathfrak{R} \ll \frac{x(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})+|I_q(\boldsymbol{\nu})|}}{(\log x)^{N+2-|I_q(\boldsymbol{\nu})|/\varphi(q)}}.$$

Nous en déduisons que (1.7.24) peut se réécrire sous la forme (1.4.10) ; cette assertion ainsi que les Remarques 1.8.9 et 1.8.12 permettent d'achever la preuve du Théorème 1.4.4.

1.9 Complétion de la preuve du Théorème 1.4.1

Compte tenu du Théorème 1.4.4 et de l'égalité (1.6.6), il est possible d'estimer la quantité $\mathcal{N}(x)$.

Les égalités (1.4.10) et (1.6.6) nous permettent de remarquer que la contribution principale dans le développement asymptotique de $\mathcal{N}(x)$ s'effectue pour les $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ tels que $|I_q(\boldsymbol{\nu})|$ est maximal. Nous notons alors $\mathfrak{I}(a) := \{|I_q(\boldsymbol{\nu})| : \boldsymbol{\nu} \in \mathcal{E}_q(a)\}$. Ainsi,

$$\mathcal{N}(x) = \sum_{0\leqslant\ell\leqslant\mathfrak{I}(a)} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(a)\\ |I_q(\boldsymbol{\nu})|=\mathfrak{I}(a)-\ell}} \mathcal{N}_{\boldsymbol{\nu}}(x) = \frac{x\mathcal{T}(x)}{(\log x)^{1-\mathfrak{I}(a)/\varphi(q)}} \tag{1.9.1}$$

où l'on a posé

$$\mathcal{T}(x) := \sum_{\substack{0\leqslant m\leqslant N\\ 0\leqslant \ell\leqslant \mathfrak{I}(a)}} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(a)\\ |I_q(\boldsymbol{\nu})|=\mathfrak{I}(a)-\ell}} \sum_{0\leqslant k\leqslant \mathfrak{I}(a)-\ell} \frac{P_{m,k,\boldsymbol{\nu}}(\log_2 x)}{(\log x)^{m+(k+\ell)/\varphi(q)}} + O\Big(\frac{(\log_2 x)^M}{(\log x)^{N+1}}\Big)$$

pour un certain $M\in\mathbb{N}$ (que l'on peut choisir indépendant de N car majoré par $(\varphi(q)-1)^{\varphi(q)}$ pour tout N). Un changement d'indice fournit

$$\mathcal{T}(x) = \sum_{\substack{0\leqslant m\leqslant N\\ 0\leqslant k\leqslant \mathfrak{I}(a)}} \sum_{0\leqslant \ell\leqslant k} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(a)\\ |I_q(\boldsymbol{\nu})|=\mathfrak{I}(a)-\ell}} \frac{P_{m,k-\ell,\boldsymbol{\nu}}(\log_2 x)}{(\log x)^{m+k/\varphi(q)}} + O\Big(\frac{(\log_2 x)^M}{(\log x)^{N+1}}\Big). \tag{1.9.2}$$

En notant

$$\mathfrak{P}_{m,k}(\xi) := \sum_{0\leqslant \ell\leqslant k} \sum_{\substack{\boldsymbol{\nu}\in\mathcal{E}_q(a)\\ |I_q(\boldsymbol{\nu})|=\mathfrak{I}(a)-\ell}} P_{m,k-\ell,\boldsymbol{\nu}}(\xi), \tag{1.9.3}$$

nous obtenons grâce à (1.9.1) et (1.9.2)

$$\mathcal{N}(x) = \frac{x}{(\log x)^{1-\mathfrak{I}(a)/\varphi(q)}}\Big\{ \sum_{0\leqslant m\leqslant N} \frac{1}{(\log x)^m} \sum_{0\leqslant k\leqslant \mathfrak{I}(a)} \frac{\mathfrak{P}_{m,k}(\log_2 x)}{(\log x)^{k/\varphi(q)}} + O\Big(\frac{(\log_2 x)^M}{(\log x)^{N+1}}\Big)\Big\}.$$

Rappelons la définition de $\mathfrak{s}(a,k)$ et $d_k(a)$ en (1.4.1). Lorsque $1<a<q$, il résulte des Remarques 1.8.12 et 1.8.13 et de (1.9.1) que $\mathcal{N}(x)$ a pour terme principal (1.4.4) et que le degré de $\mathfrak{P}_{m,k}$ est majoré par $d_k(a)$. Lorsque $a=1$, les Remarques 1.8.9 et 1.8.13 ainsi que l'égalité (1.9.1) impliquent que $\mathcal{N}(x)$ a pour terme principal (1.4.5) et que le degré de $\mathfrak{P}_{m,k}$ est majoré par $d_0(1)-1$.

Cela achève la démonstration du Théorème 1.4.1.

Remarque 1.9.1. *Les égalités* (1.8.19), (1.8.27), (1.8.29), (2.3.3) *et* (1.9.3) *permettent d'obtenir une formule explicite des coefficients de* $\mathfrak{P}_{0,k}$ $(0\leqslant k\leqslant \mathfrak{I}(a))$.

1.10 Dépendance des conditions

Nous montrons dans ce paragraphe que, pour $\boldsymbol{\nu}\in\mathcal{E}_q(a)$, les conditions $\Omega_j(n)=\nu_j$ et $\Omega_j(n)\geqslant\varphi(q)$ dans la définition de $\mathcal{N}_{\boldsymbol{\nu}}$ ne sont pas indépendantes, sauf pour certaines petites valeurs de q.

L'étude de cette dépendance nécessite l'utilisation du résultat suivant.

Lemme 1.10.1. *Soient m un entier $\geqslant 2$ et k vérifiant $1\leqslant k\leqslant m$. Alors*

$$\Gamma\Big(1-\frac{1}{m}\Big)^{m-k} = \Gamma\Big(\frac{k}{m}\Big) \Leftrightarrow k\in\{m-1;m\}. \tag{1.10.1}$$

Démonstration. Nous fixons m un entier $\geqslant 3$, le cas $m=2$ étant trivial.

Pour démontrer (1.10.1), il suffit de prouver l'inégalité

$$\frac{\Gamma\big(1-1/m\big)^{m-t}}{\Gamma\big(t/m\big)} < 1 \qquad \big(1\leqslant t<m-1\big). \tag{1.10.2}$$

En effet, (1.10.2) implique que l'égalité du terme de gauche de (1.10.1) est fausse pour tout $k \in [\![1; m-2]\!]$. De plus, cette égalité est trivialement vraie pour $k \in \{m-1; m\}$, d'où (1.10.1).

Pour cela, nous notons $f_m(t) := \Big(\Gamma\big(t/m\big)\Gamma\big(1-1/m\big)^t\Big)^{-1}$ pour $t > 0$. En posant $g(u) := (\Gamma'/\Gamma)(u)$ pour $u > 0$, nous avons

$$f_m'(t) = -\Big\{\frac{1}{m}g\Big(\frac{t}{m}\Big) + \log\Big(\Gamma\Big(1-\frac{1}{m}\Big)\Big)\Big\}f_m(t). \tag{1.10.3}$$

La fonction g étant classiquement croissante, il s'ensuit que $g(u) \leqslant g(1-1/m)$ si $u \leqslant 1-1/m$, et ainsi, en posant, pour $0 \leqslant v < 1$, $h(v) := vg(1-v) + \log\big(\Gamma(1-v)\big)$, nous avons

$$\frac{1}{m}\frac{\Gamma'}{\Gamma}\Big(\frac{t}{m}\Big) + \log\Big(\Gamma\Big(1-\frac{1}{m}\Big)\Big) \leqslant h\Big(\frac{1}{m}\Big) \qquad \big(t \leqslant m-1\big). \tag{1.10.4}$$

L'étude de la dérivée de h et l'inégalité $\Gamma'(t)^2 < \Gamma(t)\Gamma''(t)$ lorsque $t > 0$, qui découle de l'inégalité de Cauchy-Schwarz et qui implique que $g'(t) > 0$ sur ce domaine, permettent de montrer que h est strictement décroissante sur $[0; 1[$. Nous obtenons alors $h(1/m) < 0$ puisque $h(0) = 0$. Il résulte de cette inégalité ainsi que de (1.10.3) et (1.10.4) que f_m est strictement croissante sur $[1; m-1]$. En particulier, $f_m(t) < f_m(m-1)$ pour $1 \leqslant t < m-1$, d'où (1.10.2). □

Pour $j \in G_q$ et $\nu \in [\![0; \varphi(q)-1]\!]$, posons

$$\mathcal{N}_{j,\nu} := \big\{n : \Omega_j(n) = \nu\big\},$$

et

$$\mathcal{N}_{j,\varphi(q)} := \big\{n : \Omega_j(n) \geqslant \varphi(q)\big\}.$$

Par des méthodes similaires à celles que nous avons utilisées pour la démonstration du Théorème 1.4.4, nous obtenons

$$\frac{\mathcal{N}_{j,\nu}(x)}{x} \sim \Big(\frac{q}{\varphi(q)}\Big)^{1/\varphi(q)} \frac{(\log_2 x)^\nu \prod_{\chi\neq\chi_0} \mathscr{L}(\chi)^{-\overline{\chi(j)}/\varphi(q)}}{(\log x)^{1/\varphi(q)}\nu!\varphi(q)^\nu\Gamma\big(1-1/\varphi(q)\big)};$$
$$\frac{\mathcal{N}_{j,\varphi(q)}(x)}{x} \sim \Big(\frac{q}{\varphi(q)}\Big)^{1/\varphi(q)} F_j(1) \prod_{\chi\neq\chi_0} \mathscr{L}(\chi)^{-\overline{\chi(j)}/\varphi(q)}.$$

Ainsi, pour $\boldsymbol{\nu} \in H_q$, nous avons

$$\prod_{j\in G_q} \frac{\mathcal{N}_{j,\nu_j}(x)}{x} \sim \frac{(\log_2 x)^{\mathsf{s}(\boldsymbol{\nu})} q \prod_{j\in I_q(\boldsymbol{\nu})} F_j(1)}{(\log x)^{1-|I_q(\boldsymbol{\nu})|/\varphi(q)}\boldsymbol{\nu}!\varphi(q)^{\mathsf{s}(\boldsymbol{\nu})}\Gamma\big(1-1/\varphi(q)\big)^{|J_q(\boldsymbol{\nu})|}}. \tag{1.10.5}$$

En vertu du Théorème 1.4.4, du Lemme 1.10.1 et de l'équivalence (1.10.5), il s'ensuit que, lorsque $I_q(\boldsymbol{\nu}) \neq \varnothing$,

$$\prod_{j\in G_q} \frac{\mathcal{N}_{j,\nu_j}(x)}{x} \sim \frac{\mathcal{N}_{\boldsymbol{\nu}}(x)}{x} \Leftrightarrow \Gamma\Big(1-\frac{1}{\varphi(q)}\Big)^{\varphi(q)-|I_q(\boldsymbol{\nu})|} = \Gamma\Big(\frac{|I_q(\boldsymbol{\nu})|}{\varphi(q)}\Big)$$
$$\Leftrightarrow |I_q(\boldsymbol{\nu})| \in \big\{\varphi(q)-1; \varphi(q)\big\}.$$

Le cas $|I_q(\boldsymbol{\nu})| = \varphi(q)$ est à éliminer car nous avons $J_q(\boldsymbol{\nu}) \neq \varnothing$; de plus, $|I_q(\boldsymbol{\nu})| \mid \varphi(q)$ puisque $I_q(\boldsymbol{\nu})$ est un sous-groupe de G_q, donc

$$|I_q(\boldsymbol{\nu})| = \varphi(q) - 1 \Leftrightarrow \varphi(q) = 2 \Leftrightarrow q \in \{3; 4; 6\}.$$

Dans ce cas, G_q n'admet que deux éléments, ces éléments étant $1 \pmod q$ et $-1 \pmod q$. Les hypothèses impliquent nécessairement $(\nu_1, \nu_{-1}) = (2, 0)$.

Lorsque $I_q(\boldsymbol{\nu}) = \varnothing$, nous avons

$$\prod_{j \in G_q} \frac{\mathcal{N}_{j,\nu_j}(x)}{x} \sim \frac{\mathcal{N}_{\boldsymbol{\nu}}(x)}{x} \Leftrightarrow \mathsf{s}(\boldsymbol{\nu}) \sim \frac{\log_2 x}{\Gamma\big(1 - 1/\varphi(q)\big)^{\varphi(q)}},$$

ce qui est absurde. Nous en déduisons qu'il y a indépendance des conditions sur les $\Omega_j(n)$ si, et seulement si, $q \in \{2; 3; 6\}$. Dans ce cas, nous avons $G_q = \{1; \varphi(q) - 1\}$ et $(\nu_1, \nu_{-1}) = (2, 0)$.

1.11 Preuve du Corollaire 1.4.8

Commençons par établir deux lemmes de caractérisation des résidus quadratiques. Rappelons la notation $\mathfrak{H}(a)$, définie en (1.4.6).

Lemme 1.11.1. *Soient $q \geqslant 3$ et $a \in G_q$. Les deux assertions suivantes sont équivalentes :*

(i) *L'ensemble $\mathfrak{H}(a)$ contient un sous-groupe d'ordre maximal $\frac{1}{2}\varphi(q)$;*

(ii) *a est non résidu quadratique modulo q.*

Démonstration. Pour établir la condition nécessaire, nous raisonnons par l'absurde en supposant que a est résidu quadratique modulo q et qu'il existe $H \in \mathfrak{H}(a)$ tel que $|H| = \varphi(q)/2$. On sait que $a \neq 1$ puisque $\mathfrak{H}(1) = \varnothing$. De plus, il existe $x \in G_q$ tel que $x^2 \equiv a \pmod q$. Par hypothèse, $a \notin H$, donc $x \notin H$. Comme H est d'indice 2, nous avons $G_q = H \cup xH$, cette réunion étant disjointe. Or $a \notin H$ donc $a \in xH$. On a alors $a = x^2 = xh$ où $h \in H$, donc $x = h \in H$, d'où la contradiction souhaitée.

Établissons à présent la condition suffisante. Notons que $H \in \mathfrak{H}(a) \Rightarrow |H| < \varphi(q)$ puisque $a \notin H$. En vertu du théorème chinois, nous avons

$$G_q \cong \prod_{p^{\nu_p} \| q} (\mathbb{Z}/p^{\nu_p}\mathbb{Z})^* \quad (\nu_p \geqslant 1).$$

Si $\nu \geqslant 1$ et $p > 2$, $(\mathbb{Z}/p^\nu\mathbb{Z})^*$ est isomorphe au groupe $\mathbb{Z}/\varphi(p^\nu)\mathbb{Z}$, qui est de cardinal $\varphi(p^\nu) = p^{\nu-1}(p-1)$, donc pair. Lorsque $p = 2$, trois cas se présentent classiquement : si $\nu = 1$, le groupe est trivial, si $\nu = 2$, il est cyclique d'ordre 2, et si $\nu \geqslant 3$, il est produit direct d'un groupe cyclique d'ordre 2 par un groupe cyclique d'ordre $2^{\nu-2}$. Ainsi, en toute circonstance, G_q est isomorphe à un groupe du type $A_{q_1,\dots,q_k} := \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$ où les entiers $q_1, \dots, q_k$ sont tous pairs. Notons $\psi : G_q \to A_{q_1,\dots,q_k}$ l'isomorphisme correspondant, et $\psi(a) = (a_1, \dots, a_k)$. Comme a n'est pas un carré de G_q, il existe $i \in [\![1; k]\!]$ tel que $2 \mid q_i$ et $2 \nmid a_i$. Quitte à changer l'ordre des q_j, on peut supposer que $i = 1$. Soit

$$B_1 := \big\{(2y_1, y_2, y_3, \dots, y_k),\ 0 \leqslant y_1 < q_1/2, 0 \leqslant y_i < q_i\ (2 \leqslant i \leqslant k)\big\}.$$

Alors $H_1 := \psi^{-1}(B_1)$ est un sous-groupe de G_q d'ordre $\varphi(q)/2$. De plus, $a \notin H_1$, puisque a_1 serait pair dans le cas contraire. Cela implique bien la propriété souhaitée. □

Remarque 1.11.2. *Nous verrons au paragraphe 1.12 que la démonstration du Lemme 1.12.1 constitue une généralisation de celle du Lemme 1.11.1. Cependant, nous avons préféré expliciter la démonstration pour le cas spécifique des non résidus quadratiques à cause de la place importante qu'occupent ces entiers dans notre travail.*

Nous pouvons établir également, par des arguments basiques, une équivalence entre le caractère cyclique de G_q et l'unicité de l'élément de $\mathfrak{H}(a)$ décrit dans le Lemme 1.11.1.

Lemme 1.11.3. *Soient $q \geqslant 3$ et $a \in G_q$, non résidu quadratique. Alors G_q est cyclique si, et seulement si, il y a unicité de l'élément H de $\mathfrak{H}(a)$ tel que $|H| = \varphi(q)/2$.*

Démonstration. Si G_q est cyclique, il existe pour chaque $d \mid \varphi(q) = |G_q|$ un unique sous-groupe de G_q d'ordre d. La condition est donc suffisante.

Pour établir la condition nécessaire, raisonnons par contraposition en supposant G_q non cyclique. Conservons les notations de la démonstration du Lemme 1.11.1. Nous avons $G_q \cong A_{q_1,\dots,q_k}$, avec $k \geqslant 2$, et où les q_i sont pairs. Quitte à réordonner les q_i, nous pouvons donc supposer $2 \nmid a_1$, $2 \mid q_1$ et $2 \mid q_2$.

Si $2 \nmid a_2$, alors $H_2 := \psi^{-1}(B_2)$ où

$$B_2 := \big\{(y_1, 2y_2, y_3, \dots, y_k),\ 0 \leqslant y_2 < q_2/2,\ 0 \leqslant y_i < q_i\ (i \neq 2)\big\}$$

est un deuxième sous-groupe de $\mathfrak{H}(a)$ de cardinal $\varphi(q)/2$ différent de H_1. En effet, d'une part B_2 est bien un sous-groupe de $A_{q_1,\dots,q_k}$ de cardinal $\varphi(q)/2$, $B_2 \neq B_1$, et, d'autre part, si $a \in H_2$, alors $\exists y_1, \dots, y_k$ tels que $\psi(a) = (y_1, 2y_2, y_3, \dots, y_k)$, donc $2y_2 \equiv a_2 \pmod{q_2}$, ce qui est impossible car $2 \mid q_2$; il en résulte que $a \notin H_2$.

Si $2 \mid a_2$, nous pouvons choisir $H_3 := \psi^{-1}(B_3)$ où

$$B_3 := \big\{(2y_1 + y_2, y_2, y_3, \dots, y_k), 0 \leqslant y_1 < q_1/2, 0 \leqslant y_i < q_i\ (2 \leqslant i \leqslant k)\big\}.$$

En effet, d'une part B_3 est un sous-groupe de $A_{q_1,\dots,q_k}$ de cardinal $\varphi(q)/2$ différent de B_1, et, d'autre part, si $a \in H_3$, alors $\exists y_1, \dots, y_k$ tels que $\psi(a) = (2y_1 + y_2, y_2, y_3, \dots, y_k)$, i.e. $a_1 = 2y_1 + y_2$ et $a_2 = y_2$. Comme $2 \mid q_1$ et $2 \mid q_2$, les conditions $2 \mid a_2$ et $2 \nmid a_1$ impliquent respectivement $2 \mid y_1$ et $2 \nmid y_1$, une contradiction. Il s'ensuit que $a \notin H_3$ et donc $H_3 \in \mathfrak{H}(a)$. □

Remarques 1.11.4. (i) *Il résulte du Lemme 1.11.3 le fait que G_q est cyclique si, et seulement si, il existe un unique élément $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ vérifiant $|I_q(\boldsymbol{\nu})| = \varphi(q)/2$.*

(ii) *On peut également montrer que G_q est cyclique si, et seulement si, le sous-groupe des résidus quadratiques est de cardinal $\varphi(q)/2$. Ainsi, si G_q est cyclique et a est non résidu quadratique, l'unique sous-groupe de $\mathfrak{H}(a)$ de cardinal $\varphi(q)/2$ est le sous-groupe des résidus quadratiques de G_q.*

Nous sommes à présent en mesure de démontrer le Corollaire 1.4.8 en donnant une expression simplifiée du terme principal de $\mathcal{N}_{a,q}(x)$ lorsque G_q est cyclique.

Preuve du Corollaire 1.4.8. La première partie du Corollaire 1.4.8 découle immédiatement du Théorème 1.4.1 et du Lemme 1.11.1. L'égalité $\mathfrak{K}_a = 0$ également, compte tenu de la propriété $\mathfrak{K}_a = \varphi(q)/\mathfrak{I}(a) - 2$.

Lorsque G_q est cyclique, le Lemme 1.11.3 et la propriété $\mathfrak{K}_a = 0$ impliquent qu'il y a unicité de l'élément $\boldsymbol{\nu} \in \mathcal{E}_q(a)$ vérifiant $|I_q(\boldsymbol{\nu})| = \varphi(q)/2$ et $\mathsf{s}(\boldsymbol{\nu}) = 0$. La somme sur les $\boldsymbol{\nu}$ dans l'expression (1.4.4) n'a donc qu'un seul élément. Nous notons alors simplement C_q la constante $C_q(\boldsymbol{\nu})$ définie en (1.3.4).

On obtient la forme simplifiée du terme principal de $\mathcal{N}_{a,q}(x)$ en insérant les égalités $\mathfrak{I}(a) = \varphi(q)/2$ et $\mathfrak{K}_a = 0$ (qui impliquent $\Gamma(\mathfrak{I}(a)/\varphi(q)) = \sqrt{\pi}$ et $\boldsymbol{\nu}! = 1$) dans (1.4.4). De plus, puisque $I_q(\boldsymbol{\nu})$ est le sous-groupe des résidus quadratiques modulo q lorsque G_q est cyclique, l'expression de C_q est obtenue en insérant la formule

$$\sum_{j \in I_q(\boldsymbol{\nu})} \chi(j) = \begin{cases} \varphi(q)/2 & \text{si } \chi^2 = \chi_0, \\ 0 & \text{sinon,} \end{cases}$$

dans la relation (1.3.4). Nous obtenons ainsi le résultat souhaité. □

1.12 Preuve du Corollaire 1.4.11

Soit G un groupe abélien fini. Pour $a \in G$, notons $\mathfrak{H}(a)$ l'ensemble des sous-groupes de G ne contenant pas a, ce qui coïncide avec (1.4.6) lorsque $G = G_q$. Le résultat suivant a pour objet une caractérisation des éléments de G qui ne sont pas des puissances m-ièmes de G lorsque $m \mid |G|$.

Lemme 1.12.1. *Soit $m \in [\![2; |G|/2]\!]$ tel que $m \mid |G|$. Les deux assertions suivantes sont équivalentes :*

(i) $\mathfrak{H}(a)$ contient au moins un sous-groupe de cardinal $|G|/m$;

(ii) L'équation $a = y^m$ n'a pas de solution $y \in G$.

Démonstration. Pour établir la condition nécessaire, nous raisonnons par l'absurde et supposons qu'il existe dans $\mathfrak{H}(a)$ un sous-groupe H d'indice m et qu'il existe un élément y de G tel que $y^m = a$. Comme G est abélien, G/H possède une structure de groupe. Notons alors $\overline{y}$ la classe de y dans G/H et $\mathrm{o}(\overline{y})$ son ordre. Nous avons alors $\mathrm{o}(\overline{y}) \mid |G/H| = m$. Ainsi, il existe $\ell \mid m$ tel que $y^\ell \in H$, d'où $a = (y^\ell)^{m/\ell} \in H$, ce qui contredit l'hypothèse $H \in \mathfrak{H}(a)$.

Établissons à présent la condition suffisante. Comme tout groupe abélien fini est classiquement isomorphe à un produit direct de groupes cycliques, il existe des diviseurs $q_1, \dots, q_k$ de $|G|$ tels que G soit isomorphe à $A_{q_1,\dots,q_k} := \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$. Notons $\psi : G \to A_{q_1,\dots,q_k}$ l'isomorphisme correspondant, et, pour $y \in G$, $\psi(y) := (y_1, \dots, y_k)$. Comme $a \notin \{y^m : \ y \in G\}$, l'équation $(a_1, \dots, a_k) = m(y_1, \dots, y_k)$ n'admet pas de solution $(y_1, \dots, y_k) \in A_{q_1,\dots,q_k}$. Quitte à changer l'ordre des q_i, on peut supposer que l'équation $a_1 = my_1$ n'a pas de solution dans $\mathbb{Z}/q_1\mathbb{Z}$. Soit $m_1 := (m, q_1)$. Puisque $\prod_{1 \leqslant i \leqslant k} q_i = |G|$ et $m \mid |G|$, il existe $m_2, \dots, m_k$ tels que $m = \prod_{1 \leqslant i \leqslant k} m_i$ et $m_i \mid q_i$ lorsque $2 \leqslant i \leqslant k$. Soit

$$B_1 := \big\{(m_1 y_1, \dots, m_k y_k),\ 0 \leqslant y_i < q_i/m_i \ (1 \leqslant i \leqslant k)\big\}.$$

Alors $H_1 := \psi^{-1}(B_1)$ est un sous-groupe de G de cardinal $|G|/m$. De plus, ce sous-groupe ne contient pas a, ce qui implique bien la propriété souhaitée. □

Le Corollaire 1.4.11 découle immédiatement du Lemme 1.12.1 et du Théorème 1.4.1, en choisissant $G = G_q$. Il en va de même de l'égalité $\mathfrak{K}_a = m - 2$, compte tenu de la propriété $\mathfrak{K}_a = \varphi(q)/\mathfrak{I}(a) - 2$. Comme, lorsque G_q est cyclique, $I_q(\boldsymbol{\nu})$ est le sous-groupe des puissances m-ièmes modulo q, l'expression de C_q résulte dans ce cas de l'égalité

$$\sum_{j\in I_q(\boldsymbol{\nu})} \chi(j) = \begin{cases} \varphi(q)/m & \text{si } \chi^m = \chi_0, \\ 0 & \text{sinon.} \end{cases}$$

Remarque 1.12.2. *On ne peut pas remplacer dans le Lemme 2.6.2 la condition H d'indice 2 par une condition plus générale comme H d'indice m où m serait un diviseur de $\varphi(q)$. En effet, par exemple, il y a unicité du sous-groupe de G_{35} de cardinal 8, alors que G_{35} n'est pas cyclique.*

1.13 Extension à plusieurs classes de résidus

Donnons ici un bref aperçu du développement asymptotique pour le nombre des entiers n'excédant pas x et n'admettant aucun diviseur > 1 dans un ensemble fini de classes de résidus modulo q, généralisant ainsi notre résultat. Pour cela, fixons à nouveau un entier $q \geqslant 3$, et pour $k \in [\![1; \varphi(q) - 1]\!]$, fixons encore un ensemble $\boldsymbol{a} = \{a_1, \dots, a_k\}$ de k éléments de G_q deux à deux distincts. Posons ici

$$\mathcal{N}_{\boldsymbol{a},q} := \Big\{ n \geqslant 2 : \ \big(d \mid n,\ d > 1\big) \Rightarrow d \not\equiv a_i \pmod q \quad (1 \leqslant i \leqslant k) \Big\}.$$

Étendons maintenant la notion d'admissibilité à un ensemble fini de classes résiduelles.

Définition 1.13.1. *Soit $\boldsymbol{\nu} \in H_q^*$. On dit que $\boldsymbol{\nu}$ est $\boldsymbol{a}$-admissible si*

$$\big(\boldsymbol{\mu} \in H_q^*,\, \boldsymbol{\mu} \preccurlyeq \boldsymbol{\nu}\big) \Rightarrow \prod_{j\in G_q} j^{\mu_j} \not\equiv a_i \pmod q \quad (1 \leqslant i \leqslant k).$$

Nous notons $\mathcal{E}_q(\boldsymbol{a})$ l'ensemble des vecteurs $\boldsymbol{a}$-admissibles de H_q^*.

Des calculs similaires à ceux de la démonstration du Lemme 1.6.1 nous permettent de montrer l'équivalence

$$n \in \mathcal{N}_{\boldsymbol{a},q} \Leftrightarrow \big(\min\{\Omega_j(n), \varphi(q)\}\big)_{j\in G_q} \in \mathcal{E}_q(\boldsymbol{a}) \qquad (n \geqslant 2).$$

Posons $I_q(\boldsymbol{\nu})$ avec la même définition que pour un seul résidu, en remplaçant simplement $\mathcal{E}_q(a)$ par $\mathcal{E}_q(\boldsymbol{a})$. La remarque suivante découle immédiatement.

Remarques 1.13.2. (i) Si $1 \in \boldsymbol{a}$, alors $\forall \boldsymbol{\nu} \in \mathcal{E}_q(\boldsymbol{a})$, $I_q(\boldsymbol{\nu}) = \varnothing$.

(ii) Si $1 \notin \boldsymbol{a}$, alors $\exists \boldsymbol{\nu} \in \mathcal{E}_q(\boldsymbol{a})$ tel que $I_q(\boldsymbol{\nu}) \neq \varnothing$.

Nous avons donc le résultat suivant pour l'extension à plusieurs classes de résidus. Nous posons

$$\begin{aligned}
&\mathfrak{I}(\boldsymbol{a}) := \max_{\boldsymbol{\nu}\in\mathcal{E}_q(\boldsymbol{a})} |I_q(\boldsymbol{\nu})|,\\
&\mathfrak{s}(\boldsymbol{a},\ell) := \max\{\mathsf{s}(\boldsymbol{\nu},\boldsymbol{\nu}) : |I_q(\boldsymbol{\nu})| = \ell\} \quad (0\leqslant \ell\leqslant \mathfrak{I}(\boldsymbol{a})),\\
&\mathfrak{K}_{\boldsymbol{a}} := \mathfrak{s}(\boldsymbol{a},\mathfrak{I}(\boldsymbol{a})),\\
&d_k(\boldsymbol{a}) := \max_{0\leqslant\ell\leqslant\mathfrak{I}(\boldsymbol{a})} \big\{\mathfrak{s}(\boldsymbol{a},\mathfrak{I}(\boldsymbol{a})-\ell) + (\varphi(q)-1)(k-\ell)\big\}.
\end{aligned}$$

Théorème 1.13.3. *Il existe un entier $M = M_q$ tel que, pour chaque $N\in\mathbb{N}$, nous ayons, uniformément pour $x\geqslant 3$,*

$$\mathcal{N}(x) = \frac{x}{(\log x)^{1-\mathfrak{I}(\boldsymbol{a})/\varphi(q)}}\bigg\{\sum_{0\leqslant m\leqslant N}\sum_{0\leqslant k\leqslant\mathfrak{I}(\boldsymbol{a})}\frac{\mathfrak{P}_{m,k}(\log_2 x)}{(\log x)^{m+k/\varphi(q)}} + O\bigg(\frac{(\log_2 x)^M}{(\log x)^{N+1}}\bigg)\bigg\},$$

où $\mathfrak{P}_{m,k}$ est un polynôme de degré au plus égal à $d_k(\boldsymbol{a})$ si $1\notin\boldsymbol{a}$ et à $d_k(\boldsymbol{a})-1$ si $1\in\boldsymbol{a}$ avec égalité dans les deux cas si $m=k=0$.

En particulier :

(i) *si $1\notin\boldsymbol{a}$, alors $\mathfrak{I}(\boldsymbol{a})>0$, et le terme principal de $\mathcal{N}(x)$ est donné par l'expression* (1.4.4),

(ii) *si $1\in\boldsymbol{a}$, alors $\mathfrak{I}(a)=0$, $\mathfrak{K}_{\boldsymbol{a}}>0$, et le terme principal de $\mathcal{N}(x)$ est donné par l'expression* (1.4.5).

En particulier, si l'on choisit $\boldsymbol{a} = G_q\smallsetminus\{1\}$, on a toujours $\mathfrak{I}(\boldsymbol{a})=1$, ce maximum étant atteint pour $\boldsymbol{\nu}=(\varphi(q),0,\dots,0)$. Il en résulte que

$$\mathcal{N}_{\boldsymbol{a},q}(x) = \bigg\{C(\boldsymbol{a},q) + O\bigg(\frac{(\log_2 x)^{\varphi(q)-1}}{(\log x)^{1/\varphi(q)}}\bigg)\bigg\}\frac{x}{(\log x)^{1-1/\varphi(q)}},$$

avec

$$C(\boldsymbol{a},q) := \frac{1}{\Gamma\big(1/\varphi(q)\big)}\Big(\frac{q}{\varphi(q)}\Big)^{1-1/\varphi(q)}\prod_{\chi\neq\chi_0}\mathscr{L}(\chi)^{1/\varphi(q)}.$$

Nous pouvons vérifier facilement que le terme principal de l'expression précédente est bien le même que (1.1.1).

Terminons à nouveau par quelques applications aux résidus quadratiques. On omet les détails des démonstrations. Notons H le sous-groupe des résidus quadratiques de G_q et h son ordre.

Remarque 1.13.4. *On a $h=\varphi(q)/2^{\omega(q)+\varepsilon(q)}$ où $\omega(q)$ désigne le nombre de facteurs premiers divisant q comptés sans multiplicité, et*

$$\varepsilon(q) := \begin{cases} 0 & \text{si } 2\nmid q \text{ ou } 4\parallel q;\\ 1 & \text{si } 8\mid q;\\ -1 & \text{si } 2\parallel q.\end{cases}$$

En particulier, si G_q est cyclique, alors $h=\varphi(q)/2$ alors que, si G_q n'est pas cyclique, nous avons $h\leqslant\varphi(q)/4$.

Chun Gang Ji [31] a obtenu une formule générale pour le nombre de résidus k-ièmes de $\mathbb{Z}/q\mathbb{Z}$ lorsque $k\geqslant 2$.

Le Corollaire 1.13.5 fournit une estimation de l'ensemble des entiers dont tous les diviseurs sont des résidus quadratiques modulo q. Cette estimation est établie à partir du Théorème 1.13.3 grâce à une égalité reliant cet ensemble et celui de $\mathcal{N}_{\boldsymbol{a},q}$ lorsque $\boldsymbol{a}$ est un ensemble d'entiers choisi convenablement.

Corollaire 1.13.5. *Soit $\mathcal{M}_q$ l'ensemble des entiers dont tous les diviseurs sont des résidus quadratiques modulo q. Alors $\mathcal{M}_q = \mathcal{N}_{\boldsymbol{a}}$ où $\boldsymbol{a}$ est l'ensemble des non résidus quadratiques modulo q, et*

$$\mathcal{M}_q(x) = \biggl\{C_q + O\biggl(\frac{(\log_2 x)^{(\varphi(q)-1)h}}{(\log x)^{1/\varphi(q)}}\biggr)\biggr\}\frac{x}{(\log x)^{1-h/\varphi(q)}},$$

où

$$C_q := \frac{1}{\Gamma\bigl(h/\varphi(q)\bigr)}\Bigl(\frac{q}{\varphi(q)}\Bigr)^{1-h/\varphi(q)}\prod_{\chi\neq\chi_0}\mathscr{L}(\chi)^{\sum_{j\in H}\overline{\chi(j)}/\varphi(q)}.$$

En vertu des Théorèmes 1.4.1 et 1.13.3, nous pouvons établir une estimation de $\mathcal{N}_{b,q}(x)$ lorsque b est un élément de G_q et une estimation de $\mathcal{N}_{\boldsymbol{a},q}(x)$ lorsque $\boldsymbol{a}$ est un ensemble d'éléments de G_q.

Une question qui se pose alors naturellement est de savoir s'il est possible d'établir des correspondances entre $\mathcal{N}_{\boldsymbol{a},q}(x)$ et $\mathcal{N}_{b,q}(x)$. Le Corollaire 1.13.6 fournit une réponse à cette question dans le cas particulier des non résidus quadratiques modulo q.

Corollaire 1.13.6. *Soient $\boldsymbol{a} = \{a_1,\dots,a_k\}$ un ensemble de non résidus quadratiques modulo q, b un résidu non quadratique de G_q, et $\mathcal{M}_q$ l'ensemble défini dans le Corollaire 1.13.5.*

(i) Si G_q est cyclique, alors

$$\mathcal{N}_{\boldsymbol{a},q}(x) \sim \mathcal{N}_{b,q}(x). \tag{1.13.1}$$

En particulier, $\mathcal{M}_q(x) \sim \mathcal{N}_{b,q}(x)$.

(ii) Si G_q n'est pas cyclique, alors il existe $h \leqslant m \leqslant \varphi(q)/2$ tel que

$$\mathcal{N}_{\boldsymbol{a},q}(x) \asymp \frac{x}{(\log x)^{1-m/\varphi(q)}}.$$

En particulier,

$$\mathcal{M}_q(x) \asymp \frac{\mathcal{N}_{b,q}(x)}{(\log x)^{1/2-h/\varphi(q)}}.$$

Grâce au Théorème 1.13.3, nous pouvons même établir une formule explicite du terme principal de $\mathcal{N}_{\boldsymbol{a},q}(x)$ lorsque G_q est cyclique et $\boldsymbol{a}$ un ensemble de non résidus quadratiques modulo q ; cette formule fait l'objet de la remarque suivante.

Remarque 1.13.7. *Si G_q est cyclique et si $\boldsymbol{a}$ est un ensemble de non résidus quadratiques modulo q, alors*

$$\mathcal{N}_{\boldsymbol{a},q}(x) = \biggl\{\sqrt{\frac{q}{\pi\varphi(q)}\mathscr{L}(\chi_1)} + O\biggl(\frac{(\log_2 x)^{(\varphi(q)-1)\varphi(q)/2}}{(\log x)^{1/\varphi(q)}}\biggr)\biggr\}\frac{x}{\sqrt{\log x}}$$

où χ_1 désigne le caractère d'ordre 2 de G_q.

Le terme principal dans la remarque précédente est le même que celui du Corollaire 1.4.8 lorsque G_q est cyclique, ce qui se justifie facilement grâce au Corollaire 1.13.6.

1.14 Perspectives

Certains points non étudiés dans ce chapitre pourraient être abordés ultérieurement.

1. Le résultat a été démontré dans le cas où q est un entier fixé ; on pourrait chercher à vérifier s'il reste vrai lorsque $q \to +\infty$, en particulier pour tout $q \leqslant (\log x)^{\log 2-\delta}$ où $\delta > 0$, étant donné qu'Erdös a démontré en 1965 [12] que $\mathcal{N}_{a,q}(x) = o(x)$ dans ce cas, alors que le résultat n'est pas possible si $q \geqslant (\log x)^{\log 2+\delta}$ car cette fois-ci, $\mathcal{N}_{a,q}(x) = x + o(x)$.

2. Les coefficients du développement asymptotique (1.4.3) sont explicites, mais leurs expressions ne permettent pas de déterminer les cas d'annulation en toute généralité. À cet égard, une simplification des formules serait très utile.

3. L'expression de ces coefficients nous a permis de montrer que chacun des $\mathfrak{P}_{m,k}$ est de degré inférieur ou égal à $d_k(a)$ si $k \neq \mathfrak{I}(a)$ lorsque $a > 1$ et de degré inférieur ou égal à $d_0(1) - 1$ lorsque $a = 1$, mais ne nous a pas permis de déterminer s'il y a égalité dans les deux cas. Il serait utile de prouver s'il y a effectivement égalité, notamment grâce à la simplification demandée dans le paragraphe précédent, et ainsi de déterminer s'il y a indépendance du degré de $\mathfrak{P}_{m,k}$ par rapport à m.

Chapitre 2

Entiers ultrafriables en progression arithmétique

Sommaire

2.1 Introduction

Un entier positif n est dit y-friable si son plus grand facteur premier, noté $P^+(n)$ (avec la convention $P^+(1)=1$), n'excède pas y. Pour $x>0$, $y>0$, nous désignons par $S(x,y)$ l'ensemble des entiers y-friables inférieurs ou égaux à x et par $\Psi(x,y)$ son cardinal. Étant donné un entier $q \geqslant 2$, nous notons $\Psi_q(x,y)$ le nombre des éléments de $S(x,y)$ qui sont premiers à q. Pour tout entier a vérifiant $(a,q)=1$, nous définissons $\Psi(x,y;a,q)$ comme le nombre des éléments de $S(x,y)$ congrus à a modulo q. Ces cardinaux font l'objet d'une abondante littérature : voir notamment Fouvry-Tenenbaum [17], Hildebrand-Tenenbaum [27], La Bretèche-Tenenbaum [6], Granville [19, 20], et plus récemment Soundararajan [52] et Harper [25].

Un entier naturel est dit *y-ultrafriable* s'il n'est divisible par aucune puissance de nombre premier excédant y. Pour $x > 0$, $y > 0$, nous désignons par $U(x, y)$ l'ensemble des entiers y-ultrafriables n'excédant pas x et par $\Upsilon(x, y)$ son cardinal. Cette quantité a été récemment étudiée par Tenenbaum [58]. La notion d'entier ultrafriable est utile dans plusieurs branches de l'arithmétique, en particulier la théorie des graphes, ainsi que l'atteste l'article récent de Sander [49].

Nous nous proposons ici d'étudier la répartition des entiers ultrafriables dans les progressions arithmétiques en évaluant le comportement asymptotique des quantités

$$\Upsilon_q(x, y) := \sum_{\substack{n\in U(x,y)\\(n,q)=1}} 1, \qquad \Upsilon(x, y; a, q) := \sum_{\substack{n\in U(x,y)\\n\equiv a \pmod q}} 1$$

dans des domaines adéquats des variables x, y et q.

Étant donné deux fonctions f et g, la notation de Vinogradov $f \ll g$ signifie qu'il existe une constante C telle que $|f| \leqslant C|g|$ pour toutes les valeurs de la ou des variables dans un domaine spécifié ; nous écrirons $f \asymp g$ pour indiquer que l'on a à la fois $f \ll g$ et $g \ll f$.

Pour tout nombre premier $p \leqslant y$, notons $\nu_p = \nu_p(y) := \lfloor \log y/\log p \rfloor$, de sorte que p^{ν_p} est la plus grande puissance de p n'excédant pas y. Posant

$$\psi_q(y) := \sum_{\substack{p\leqslant y\\p\nmid q}} \nu_p \log p, \qquad N_{q,y} := \mathrm{e}^{\psi_q(y)},$$

nous observons, comme dans [58], que $\Upsilon_q(x, y)$ est la fonction de comptage des diviseurs de $N_{q,y}$. Ainsi

$$\Upsilon_q(x, y) = \tau(N_{q,y}) = \prod_{\substack{p\leqslant y\\p\nmid q}} (1 + \nu_p) \qquad (x \geqslant N_{q,y})$$

où $\tau(n)$ désigne le nombre de diviseurs de n, et donc, notant classiquement $\pi(y)$ le nombre de nombres premiers n'excédant pas y et $\omega(q)$ le nombre des facteurs premiers de q comptés sans multiplicité,

$$\Upsilon_q(x, y) = 2^{\pi(y)+O(\sqrt{y}/\log y)} \qquad \big(x \geqslant N_{q,y},\ \omega(q) \ll \sqrt{y}/\log y\big),$$

La symétrie des diviseurs de $N_{q,y}$ autour de $\sqrt{N_{q,y}}$ implique de plus

$$\Upsilon_q(x, y) = \tau(N_{q,y}) - \Upsilon_q\Big(\Big\lfloor \frac{N_{q,y}}{x} \Big\rfloor, y\Big) \qquad \Big(\sqrt{N_{q,y}} \leqslant x \leqslant N_{q,y}\Big).$$

Nous pouvons donc restreindre l'étude de $\Upsilon_q(x, y)$ au cas

$$x < \sqrt{N_{q,y}}, \quad \text{i.e.} \quad \psi_q(y) > 2 \log x.$$

Pour simplifier l'exposition, nous considérerons en fait le domaine plus vaste

$$x \geqslant y \geqslant 2, \quad \psi(y) > 2 \log x \tag{2.1.1}$$

où $\psi(y) := \psi_1(y) = \sum_{p\leqslant y} \nu_p \log p$ désigne la fonction de Tchébychev.

Soit $d := (a,q)$, de sorte que $(a/d, q/d) = 1$. Si $d \notin U(x,y)$, alors $\Upsilon(x,y;a,q) = 0$. Dans le cas contraire, nous avons

$$\Upsilon(x,y;a,q) = \sum_{\substack{m\leqslant x/d\\ m\equiv a/d \pmod{q/d}\\ p^\nu\|m\Rightarrow\nu\leqslant\nu_p-v_p(d)}} 1,$$

où $v_p(d)$ désigne la valuation p-adique de d. Les techniques développées dans le présent travail peuvent être aisément adaptées pour évaluer cette quantité : il suffit essentiellement de remplacer la série de Dirichlet $Z_q(s,y)$ introduite en (2.2.4) *infra* par

$$Z_q(s,y)\prod_{\substack{p^\nu\|d\\ p\nmid q/d}} \frac{1-p^{-(\nu_p+1-\nu)s}}{1-p^{-s}}\cdot$$

Une estimation de $\Upsilon(x,y;a,q)$ pour une condition particulière sur d est donnée dans la Remarque 2.2.8 *infra*.

Par souci de concision, nous restreignons cependant l'étude au cas $(a,q) = 1$.

2.2 Résultats

2.2.1 Évaluation de $\Upsilon_q(x,y)$

Tenenbaum [58] a montré que, pour tout $\varepsilon > 0$,

$$\Upsilon(x,y) = \Psi(x,y)\Big\{1 + O\Big(\frac{u\log 2u}{\sqrt{y}\log y}\Big)\Big\} \qquad \big(x \geqslant y \geqslant (\log x)^{2+\varepsilon}\big), \tag{2.2.1}$$

où, ici et dans la suite, nous notons $u := \log x/\log y$ $(x \geqslant 2, y \geqslant 2)$. En suivant la même méthode, nous établissons la pertinence de l'approximation de $\Upsilon_q(x,y)$ par $\Psi_q(x,y)$ pour ces mêmes « grandes » valeurs de y, et un large domaine en q.

Théorème 2.2.1. *Soit $\varepsilon > 0$. Sous les conditions*

$$x \geqslant y \geqslant (\log x)^{2+\varepsilon}, \quad P^+(q) \leqslant y, \quad \omega(q) \ll \sqrt{y}, \tag{2.2.2}$$

nous avons

$$\Upsilon_q(x,y) = \Psi_q(x,y)\bigg\{1 + O\bigg(\frac{qu\log 2u}{\varphi(q)\sqrt{y}\log y}\bigg)\bigg\}. \tag{2.2.3}$$

La formulation de notre évaluation de $\Upsilon_q(x,y)$ pour les petites valeurs de y nécessite quelques notations supplémentaires.

Nous désignons par

$$Z_q(s,y) := \prod_{\substack{p\leqslant y\\ p\nmid q}} \frac{1-p^{-(\nu_p+1)s}}{1-p^{-s}} \quad (\Re e\ s > 0). \tag{2.2.4}$$

la série de Dirichlet associée à la fonction de comptage $\Upsilon_q(x,y)$, convenons de poser $Z(s,y) := Z_1(s,y)$, et notons

$$\varphi_1(s,y) := -\frac{Z'(s,y)}{Z(s,y)} = \sum_{p\leqslant y}\Big\{\frac{\log p}{p^s-1} - \frac{(\nu_p+1)\log p}{p^{(\nu_p+1)s}-1}\Big\} \qquad (\Re e\ s>0,\ y\geqslant 2).$$

Ainsi qu'il a été observé dans [58], l'équation

$$\varphi_1(\sigma,y) = \log x \qquad (\sigma>0) \tag{2.2.5}$$

possède, sous la condition (2.1.1), une unique solution $\beta = \beta(x,y)$, qui est donc le point-selle relatif à l'intégrale de Perron pour $\Upsilon(x,y)$.

Désignons par

$$\Phi(z) := \frac{1}{\sqrt{2\pi}}\int_z^\infty \mathrm{e}^{-t^2/2}\mathrm{d}t \qquad (z\in\mathbb{R}) \tag{2.2.6}$$

la fonction de répartition décroissante de la loi gaussienne, et posons

$$G(z) := \mathrm{e}^{z^2/2}\Phi(z) \qquad (z\in\mathbb{R}),$$

de sorte que

$$G(z) = \tfrac12 + O(z) \quad (z\to 0), \quad G(z) = \frac{1}{\sqrt{2\pi}z}\Big\{1-\frac{1}{z^2}+O\Big(\frac{1}{z^4}\Big)\Big\} \quad (z\to+\infty). \tag{2.2.7}$$

Tenenbaum a obtenu dans [58] l'estimation

$$\Upsilon(x,y) = x^\beta Z(\beta,y)G(\beta\sqrt{\sigma_2})\Big\{1+O\Big(\frac{1}{u}\Big)\Big\} \qquad \big(2\log x<\psi(y)\ll(\log x)^3\big). \tag{2.2.8}$$

Nous nous proposons d'évaluer $\Upsilon_q(x,y)/\Upsilon(x,y)$ en exploitant cette estimation, relevant du paramètre implicite β. La démarche est analogue à celle de La Bretèche et Tenenbaum [6], qui ont estimé le rapport $\Psi_q(x,y)/\Psi(x,y)$ en utilisant les approximations du numérateur et du dénominateur issues de la méthode du col — cf. [27] —, et donc fonctions du point-selle de l'intégrale de Perron pour $\Psi(x,y)$, défini comme l'unique solution positive $\alpha := \alpha(x,y)$ de l'équation

$$\sum_{p\leqslant y}\frac{\log p}{p^\alpha-1} = \log x.$$

Notant p_k le k-ième nombre premier, de sorte que $p_k \asymp k\log 2k$ $(k\geqslant 1)$, et

$$z_q := p_{\omega(q)} \qquad (q\geqslant 1) \tag{2.2.9}$$

avec la convention $p_0 := 2$, nous posons ensuite

$$\eta = \eta(x,y) := \frac{\psi(y)}{\log x} - 2, \quad \vartheta_q = \vartheta_q(y) := \frac{\log z_q}{\log y} \asymp \frac{\log\{2+\omega(q)\}}{\log y} \quad (q\geqslant 1), \tag{2.2.10}$$

et introduisons les termes d'erreur $\Delta_q = \Delta_q(x,y)$ et $D_q = D_q(x,y)$ définis par

$$\Delta_q := \begin{cases} \dfrac{(\log x)^{\vartheta_q}}{\log y}\Big(1 + \dfrac{1}{\vartheta_q \log(1+\eta)}\Big) & \text{si } 2\log x < \psi(y) \ll (\log x)^2, \\ \dfrac{\vartheta_q\{u\log 2u\}^{\vartheta_q}}{1+\vartheta_q\log 2u} & \text{si } y > (\log x)^2, \end{cases} \tag{2.2.11}$$

et $D_q := \min\{\omega(q), \Delta_q\}$.

Posant

$$g_q(s) := \prod_{p\,|\,q} \frac{1-p^{-s}}{1-p^{-(\nu_p+1)s}} \qquad (q \geqslant 1,\ s \in \mathbb{C}),$$

et notant, ici et dans la suite, $\log_k$ la k-ième itérée de la fonction logarithme ($k \geqslant 1$), nous obtenons le résultat suivant, où x_0 désigne une constante absolue assez grande.

Théorème 2.2.2. *Soit $\varepsilon > 0$. Sous les conditions*

$$x \geqslant y \geqslant 2, \quad x > x_0, \quad 2\log x < \psi(y) \leqslant \exp\big((\log x)^{1/5}/(\log_2 x)^{(1+\varepsilon)/5}\big), \tag{2.2.12}$$

$$q \geqslant 1, \quad P^+(q) \leqslant y, \quad \omega(q) \ll y^{1/2-(1+\varepsilon)(\log_2 u)/\log u}, \tag{2.2.13}$$

les assertions suivantes sont valides :

(i) *Nous avons*

$$\begin{aligned} \Upsilon_q(x,y) &= g_q(\beta)\Upsilon(x,y)\Big\{1 + O\Big(\frac{1+D_q^2}{u} + \frac{D_q(1+\eta)}{\sqrt{u}+\eta u}\Big)\Big\} \\ &= x^\beta Z_q(\beta,y)G(\beta\sqrt{\sigma_2})\Big\{1 + O\Big(\frac{1+D_q^2}{u} + \frac{D_q(1+\eta)}{\sqrt{u}+\eta u}\Big)\Big\}, \end{aligned} \tag{2.2.14}$$

et donc, lorsque $\eta \gg 1$,

$$\Upsilon_q(x,y) = g_q(\beta)\Upsilon(x,y)\Big\{1 + O\Big(\frac{1+\Delta_q^2}{u}\Big)\Big\}.$$

(ii) *Si de plus $\eta \leqslant \frac{1}{2}$, alors*

$$\Upsilon_q(x,y) = g_q(\beta)\Upsilon(x,y)\Big\{1 + R + O\Big(\frac{1+\omega(q)^2}{u}\Big)\Big\} \tag{2.2.15}$$

avec $R \asymp \omega(q)(1+\eta)/\big(\sqrt{u}+\eta u\big)$.

(iii) *Sous la condition supplémentaire $\eta = o\big(1/\sqrt{u}\big)$, nous avons*

$$\Upsilon_q(x,y) = g_q(\beta)\Upsilon(x,y)\Big\{1 + \frac{\omega(q)}{\sqrt{\pi u}} + O\Big(\eta\omega(q) + \frac{\log q}{\sqrt{u}\log y} + \frac{\omega(q)^2}{u}\Big)\Big\}. \tag{2.2.16}$$

Remarques 2.2.3. (a) *Sous la condition* (2.2.13)*, et si en outre $0 < \eta \leqslant 1$, on vérifie que $\Delta_q \asymp \{1+\omega(q)\}/\eta$ et donc $D_q \asymp \omega(q)$.*

(b) *Lorsque $y = (\log x)^{1+\lambda}$ avec $\lambda \asymp 1$, les deux expressions de Δ_q apparaissant dans* (2.2.11) *sont du même ordre de grandeur.*

(c) *Ainsi que l'attestent les formules* (2.3.2) *et* (2.3.3) infra*, les points-selles* α *et* β *sont proches lorsque* $y > (\log x)^{1+\varepsilon}$*. Cela se traduit ici par l'estimation* $\Delta_q \asymp E_q$*, où* E_q *est le terme d'erreur introduit dans [6]. Nous pourrons donc réutiliser certaines estimations établies dans [6], notamment*

$$\Delta_q(1+\Delta_q) \ll \vartheta_q \log(u+1) \ll 1 \quad \big(\omega(q) \ll y^{1/\log(u+2)}\big). \tag{2.2.17}$$

(d) *Compte tenu des conditions* (2.2.12), (2.2.13)*, et des estimations de la quantité* E_q *établies dans [6], les remarques précédentes permettent de constater que les termes d'erreur du Théorème 2.2.2 tendent vers 0.*

(e) *Sous les hypothèses* $y > (\log x)^{2+\varepsilon}$ *et* $\omega(q) \ll \sqrt{y}/\log y$*, nous avons, d'après [6, Cor. 2.2],* (2.2.3) *avec* $q = 1$*,* (2.2.8)*, et* (2.3.2), (2.3.3) *infra,*

$$\begin{aligned}\Psi_q(x,y) &= g_q(\alpha)\Psi(x,y)\Big\{1+O\Big(\frac{1}{u}\Big)\Big\} = g_q(\alpha)\Upsilon(x,y)\Big\{1+O\Big(\frac{1}{u}\Big)\Big\}\\ &= g_q(\alpha)x^\beta Z(\beta,y)G(\beta\sqrt{\sigma_2})\Big\{1+O\Big(\frac{1}{u}\Big)\Big\}\\ &= x^\beta Z_q(\beta,y)G(\beta\sqrt{\sigma_2})\Big\{1+O\Big(\frac{1}{u}\Big)\Big\}.\end{aligned}$$

En vertu de (2.2.3)*, il s'ensuit que, sous les mêmes hypothèses,*

$$\Upsilon_q(x,y) = x^\beta Z_q(\beta,y)G(\beta\sqrt{\sigma_2})\Big\{1+O\Big(\frac{qu\log 2u}{\varphi(q)\sqrt{y}\log y}\Big)\Big\}. \tag{2.2.18}$$

On voit ainsi que le terme principal de la seconde formule (2.2.14) *constitue une bonne approximation de* $\Upsilon_q(x,y)$ *dans la totalité du domaine* $x \geqslant y \geqslant 2$*,* $\psi(y) > 2\log x$*.*

(f) *Comme* $\Upsilon_q(x,y)$ *ne dépend que du noyau sans facteur carré de* q *et comme* $\log q \leqslant \omega(q)\log y$ *si* $\mu(q)^2 = 1$ *et* $P^+(q) \leqslant y$*, l'ordre de grandeur du second terme d'erreur de* (2.2.16) *ne dépasse pas celui du terme principal complémentaire* $\omega(q)/\sqrt{\pi u}$*.*

2.2.2 Évaluation de $\Upsilon(x,y;a,q)$

Notre approche combine, d'une part, une majoration des quantités

$$\Upsilon(x,y;\chi) := \sum_{n\in U(x,y)} \chi(n),$$

lorsque χ est un caractère de Dirichlet de module q distinct du caractère principal χ_0, et, d'autre part, l'évaluation de Granville [20]

$$\Psi(x,y;a,q) := \sum_{\substack{n\in S(x,y)\\ n\equiv a \,(\mathrm{mod}\ q)}} 1 = \frac{\Psi_q(x,y)}{\varphi(q)}\Big\{1+O\Big(\frac{\log q}{u^c\log y}+\frac{1}{\log y}\Big)\Big\}, \tag{2.2.19}$$

valable, pour tout $\varepsilon > 0$, sous les conditions $x \geqslant y \geqslant q^{1+\varepsilon}$, et avec $c = c(\varepsilon) > 0$.

Le résultat suivant rassemble nos résultats relatifs à la première voie. Nous posons

$$Y_\varepsilon := Y_\varepsilon(y) = \mathrm{e}^{(\log y)^{3/2-\varepsilon}} \qquad (\varepsilon > 0,\ y \geqslant 2) \tag{2.2.20}$$

et désignons dans tout ce travail par c_j $(j = 1, 2, \ldots)$ des constantes absolues positives convenablement choisies.

Théorème 2.2.4. *Soit $A > 0$. Pour $\varepsilon > 0$, $c_0 > 0$, $c_1 > 0$ assez petits, sous les conditions*

$$x \geqslant 2, \quad 2\log x < \psi(y) \leqslant \mathrm{e}^{(\log x)^{\varepsilon}}, \tag{2.2.21}$$

$$2 \leqslant q \leqslant y^{c_0/\log_2 y}, \tag{2.2.22}$$

et pour tout caractère de Dirichlet χ de module q non principal, nous avons

$$\Upsilon(x,y;\chi) \ll \Upsilon_q(x,y)\Big\{\mathrm{e}^{-c_1 u/\{1+\vartheta(\chi)(\log u)^4\}} + Y_{\varepsilon}^{-1}\Big\} \tag{2.2.23}$$

où $\vartheta(\chi)$ vaut 0 ou 1 et n'est non nul que si $q > (\log y)^A$ et χ est égal à un unique caractère réel exceptionnel.

Le terme principal attendu pour $\Upsilon(x,y;a,q)$ est $\Upsilon_q(x,y)/\varphi(q)$, où φ désigne la fonction indicatrice d'Euler. Nous déduisons du Théorème 2.2.4 l'évaluation suivante, valable pour les petites valeurs de y.

Théorème 2.2.5. *Soit $\varepsilon > 0$. Sous les hypothèses* (2.2.21), (2.2.22) *$(a,q) = 1$, nous avons*

$$\Upsilon(x,y;a,q) = \frac{\Upsilon_q(x,y)}{\varphi(q)}\Big\{1 + O\Big(\mathrm{e}^{-c_1 u/(\log u)^4} + Y_{\varepsilon}^{-1}\Big)\Big\}. \tag{2.2.24}$$

En l'absence de caractère de Siegel modulo q, on peut substituer u à $u/(\log u)^4$ dans le terme d'erreur de (2.2.24).

Le résultat suivant, dont la démonstration repose sur (2.2.19), fournit une évaluation de $\Upsilon(x,y;a,q)$ pour les grandes valeurs de y.

Théorème 2.2.6. *Pour une valeur convenable de $c_2 > 0$, tout $\varepsilon > 0$, et sous les conditions $x \geqslant y \geqslant (\log x)^{2+\varepsilon}$, $q \leqslant \sqrt{y}$, et $(a,q) = 1$, nous avons*

$$\Upsilon(x,y;a,q) = \frac{\Upsilon_q(x,y)}{\varphi(q)}\Big\{1 + O\Big(\frac{\log q}{u^{c_2}\log y} + \frac{1}{\log y}\Big)\Big\}. \tag{2.2.25}$$

Remarque 2.2.7. *Dans le domaine de validité commun à* (2.2.24) *et* (2.2.25), *le terme d'erreur de* (2.2.24) *est le plus précis des deux. La discontinuité qualitative de ce terme d'erreur lorsque l'on passe d'un domaine à l'autre reflète la disparité des méthodes employées.*

Remarque 2.2.8. *Comme cela a été évoqué à la fin de l'introduction, les démonstrations des Théorèmes 2.2.4 à 2.2.6 peuvent être adaptées pour traiter le cas où $(a,q) > 1$. Par exemple, en notant $d := (a,q)$, si d est sans facteur carré et vérifie $(q/d,d) = 1$, nous avons, pour $\varepsilon > 0$ et sous les conditions* (2.2.21) *et* (2.2.22),

$$\Upsilon(x,y;a,q) = \frac{h_d(\beta)\Upsilon_{q/d}\big(x/d,y\big)}{\varphi\big(q/d\big)}\Big\{1 + O\Big(\mathrm{e}^{-c_1 u/(\log u)^4} + Y_{\varepsilon}^{-1}\Big)\Big\}$$

où

$$h_d(s) := \prod_{p\,|\,d}\frac{1-p^{-\nu_p s}}{1-p^{-(\nu_p+1)s}} \quad (\Re e\ s > 0).$$

2.3 Cols

Pour $v > 1$, désignons par $\xi(v)$ l'unique solution de l'équation $\mathrm{e}^{\xi(v)} = 1 + v\xi(v)$, et convenons que $\xi(1) := 0$. Posons encore

$$L_\varepsilon(y) := \mathrm{e}^{(\log y)^{3/5-\varepsilon}} \qquad (\varepsilon > 0,\ y \geqslant 2). \tag{2.3.1}$$

Il est établi dans [27] que, pour tout $\varepsilon > 0$, nous avons

$$\alpha = 1 - \frac{\xi(u)}{\log y} + O\Big(\frac{1}{u(\log y)^2} + \frac{1}{L_\varepsilon(y)}\Big) \qquad \big((\log x)^{1+\varepsilon} < y \leqslant x\big). \tag{2.3.2}$$

Les estimations suivantes du col β ont été obtenues dans [58].

Lemme 2.3.1. *Soit $\varepsilon > 0$. Nous avons*

(2.3.3)
$$\beta(x,y) = \begin{cases} 1 - \dfrac{\xi(u)}{\log y} + O\Big(\dfrac{1}{u(\log y)^2} + \dfrac{1}{L_\varepsilon(y)}\Big) & \big((\log x)^{1+\varepsilon} < y \leqslant x\big), \\ \dfrac{1 + O\big(1/\log y\big)}{\log y}\log\big(1+\eta\big) & \big(2\log x < \psi(y) \ll (\log x)^3\big). \end{cases}$$

Remarque. *Il est établi dans [27] que*

$$\xi(u) \sim \log(u\log u) \qquad (u \to \infty). \tag{2.3.4}$$

En particulier, nous avons donc

$$1 - \beta \asymp \frac{\log(2u)}{\log y} \qquad (\psi(y) > 2\log x). \tag{2.3.5}$$

Lemme 2.3.2. *On a uniformément pour $\psi(y) > 2\log x$*

$$\frac{y^{1-\beta} - 1}{1-\beta} \asymp \log x. \tag{2.3.6}$$

Démonstration. Lorsque $y \geqslant (\log x)^2$, l'estimation annoncée résulte du lemme 3 de [27] et de la première estimation (2.3.3). Sous la condition $2\log x < \psi(y) \ll (\log x)^3$, elle découle de l'estimation (2.16) de [58] et de (2.3.5) sous la forme $(1-\beta) \asymp 1$. □

Remarque. *Les estimations* (2.3.5) *et* (2.3.6) *impliquent immédiatement*

$$y^{1-\beta} \asymp u\log 2u \qquad (x \geqslant y \geqslant 2,\ \psi(y) > 2\log x). \tag{2.3.7}$$

2.4 Lemmes

2.4.1 Termes d'erreur

Lemme 2.4.1. *Soit $\varepsilon > 0$. Sous la condition* (2.2.13)*, nous avons*

$$D_q \ll \frac{\sqrt{u}}{(\log 2u)^{1/2+\varepsilon}}. \tag{2.4.1}$$

Démonstration. Lorsque $\eta \leqslant 1$, nous avons $D_q \asymp \omega(q)$ en vertu de la Remarque 2.2.3(a). Comme nous avons alors $y \ll \log x$ et $\log y \asymp \log 2u$, il suit

$$D_q \asymp \omega(q) \ll (u \log y)^{1/2-(1+\varepsilon)(\log_2 2u)/\log 2u} \ll \frac{\sqrt{u}}{(\log 2u)^{1/2+\varepsilon}}.$$

Lorsque $\eta > 1$, la condition (2.2.13) équivaut à

$$\vartheta_q \leqslant \frac{1}{2} - (1+\varepsilon)\frac{\log_2(2u)}{\log 2u} + O\Big(\frac{1}{\log y}\Big),$$

d'où, en reportant dans (2.2.11),

$$\Delta_q \ll \frac{\sqrt{u}}{(\log 2u)^{1/2+\varepsilon}}. \tag{2.4.2}$$

□

2.4.2 Estimations relatives à la fonction $g_q(s)$

Posons

$$\gamma_q(s) := \log g_q(s) = \sum_{p\,|\,q} \big\{ \log\big(1-p^{-s}\big) - \log\big(1-p^{-(\nu_p+1)s}\big)\big\} \qquad (\Re e\, s > 0),$$

où, dans le membre de droite, les logarithmes complexes sont pris en détermination principale. Introduisons également la quantité

$$C_q := \min\{\omega(q), \Delta_q^2\} \tag{2.4.3}$$

et, dans toute la suite, convenons que u_0 désigne une constante absolue assez grande.

Lemme 2.4.2. *Sous les conditions* (2.2.13) *et*

$$\psi(y) > 2\log x, \quad u \geqslant u_0, \tag{2.4.4}$$

nous avons

$$\gamma_q'(\beta) \ll D_q \log y, \qquad -\gamma_q''(\beta) \ll C_q (\log y)^2. \tag{2.4.5}$$

De plus, sous la condition supplémentaire $\eta \ll 1$, nous avons

$$\begin{aligned} \gamma_q'(\beta) &= \tfrac{1}{2}\omega(q)\log y + O\big(\eta\omega(q)\log y + \log q\big), \\ \gamma_q''(\beta) &= \tfrac{1}{12}\omega(q)(\log y)^2 + O\big(\eta\omega(q)(\log y)^2 + (\log q)\log y\big). \end{aligned} \tag{2.4.6}$$

Démonstration. Ainsi qu'il a été observé au lemme 3.13 de [6], les fonctions γ_q' et $-\gamma_q''$ sont décroissantes et positives sur $]0,\infty[$. Nous avons

$$\begin{aligned} \gamma_q'(\sigma) &= \sum_{p\,|\,q} \Big\{ \frac{\log p}{p^\sigma - 1} - \frac{(\nu_p+1)\log p}{p^{(\nu_p+1)\sigma}-1} \Big\}, \\ -\gamma_q''(\sigma) &= \sum_{p\,|\,q} \Big\{ \frac{(\log p)^2 p^\sigma}{(p^\sigma-1)^2} - \frac{(\nu_p+1)^2(\log p)^2 p^{(\nu_p+1)\sigma}}{(p^{(\nu_p+1)\sigma}-1)^2} \Big\}. \end{aligned}$$

Un développement limité à l'ordre 3 en 0 fournit donc

$$\gamma_q'(0) = \tfrac{1}{2}\sum_{p\,|\,q}\nu_p\log p \ll \omega(q)\log y,$$
$$-\gamma_q''(0) = \tfrac{1}{12}\sum_{p\,|\,q}\nu_p(\nu_p+2)(\log p)^2 \ll \omega(q)(\log y)^2.$$

Pour achever la preuve de (2.4.5), il reste donc à montrer que

$$\gamma_q^{(j)}(\beta) \ll (\Delta_q\log y)^j \qquad (j=1,2). \tag{2.4.7}$$

À cette fin, nous pouvons supposer que $\eta > 1$, puisque, dans le cas contraire, nous avons $\Delta_q \gg 1+\omega(q)$, ainsi qu'il a été observé à la Remarque 2.2.3(a). Nous utiliserons les majorations

$$\gamma_q'(\sigma) \ll \frac{z_q^{1-\sigma}-1}{(1-z_q^{-\sigma})(1-\sigma)}, \quad -\gamma_q''(\sigma) \ll \frac{(z_q^{1-\sigma}-1)\log z_q}{(1-z_q^{-\sigma})^2(1-\sigma)}, \tag{2.4.8}$$

établies au lemme 3.13 de [6].

Considérons d'abord le cas $y \leqslant (\log x)^2$. Parallèlement à la preuve du lemme 3.15 de [6], nous observons que les relations (2.4.8), (2.3.3), (2.3.5) et (2.3.7) impliquent

$$\gamma_q'(\beta) \ll y^{(1-\beta)\vartheta_q}\Big(1+\frac{1}{\beta\log z_q}\Big) \ll (\log x)^{\vartheta_q}\Big(1+\frac{1}{\vartheta_q\log(1+\eta)}\Big) = \Delta_q\log y,$$
$$-\gamma_q''(\beta) \ll (\log x)^{\vartheta_q}\Big(1+\frac{1}{\beta\log z_q}\Big)^2\vartheta_q\log y = (\Delta_q\log y)^2\frac{\vartheta_q\log y}{(\log x)^{\vartheta_q}} \ll (\Delta_q\log y)^2,$$

ce qui fournit bien (2.4.7).

Lorsque $y > (\log x)^2$, compte tenu de la Remarque 2.2.3(c), l'estimation (2.4.7) est une conséquence directe du lemme 3.14 de [6] et de la majoration $\vartheta_q \ll \Delta_q$, qui découle de la formule (2.10) du même article. □

Posons

$$\varphi_{j,q}(s,y) := (-1)^j\frac{\mathrm{d}^{j-1}}{\mathrm{d}\sigma^{j-1}}\frac{Z_q'(s,y)}{Z_q(s,y)}, \qquad \sigma_{j,q} := \varphi_{j,q}(\beta,y) \qquad (j\geqslant 1, q\geqslant 1), \tag{2.4.9}$$

et convenons d'omettre le second indice lorsque $q=1$. Le lemme suivant est une adaptation relative aux quantités (2.4.9) du lemme 2.5 de [58], qui correspond au cas $q=1$.

Lemme 2.4.3. *Soit $j\in\mathbb{N}^*$. Sous les conditions* (2.2.13) *et* (2.4.4)*, nous avons*

$$\sigma_{j,q} \ll u(\log y)^j. \tag{2.4.10}$$

Lorsque $j=3$, on peut multiplier le membre de droite par $\min(1,\beta\log y)+1/\sqrt{u}$. De plus, dans les mêmes hypothèses,

$$\sigma_{2,q} = \sigma_2\Big\{1+O\Big(\frac{1}{\log u}\Big)\Big\}. \tag{2.4.11}$$

Sous les conditions supplémentaires $q=1$ et $\psi(y)\ll(\log x)^3$, nous avons

$$\sigma_2 = \Big\{1+O\Big(\frac{1}{\log y}\Big)\Big\}\frac{1+\eta}{2+\eta}u(\log y)^2. \tag{2.4.12}$$

Démonstration. Lorsque $y \ll (\log x)^3$, toutes les majorations découlent directement du lemme 2.5 de [58] et des inégalités $\sigma_{j,q} \leqslant \sigma_j$ $(j \geqslant 1)$. Dans le domaine $y > (\log x)^2$, la même approche fonctionne, *mutatis mutandis*, en utilisant (2.3.7). L'égalité (2.4.12) coïncide avec la formule (2.21) de [58].

Il reste à établir (2.4.11). Le Lemme 2.4.2 implique

$$\sigma_2 - \sigma_{2,q} \ll C_q(\log y)^2.$$

Comme la majoration (2.4.1) implique $\omega(q) \ll \sqrt{u}$ lorsque $\psi(y) \ll \log x$ et

$$\Delta_q^2 \ll u/\log u$$

dans le cas contraire, nous obtenons bien l'évaluation annoncée. □

2.4.3 Estimations impliquant les séries $Z_q(s,y)$

Rappelons la définition (2.2.20) de Y_ε $(\varepsilon > 0)$.

La démonstration du lemme suivant étend à $Z_q(s,y)$ celle du lemme 2.6 de [58].

Lemme 2.4.4. *Il existe une constante $c_3 > 0$ telle que, pour tout $\varepsilon > 0$, et sous les conditions* (2.2.13), (2.4.4), *nous ayons*

$$\left|\frac{Z_q(\beta+i\tau,y)}{Z_q(\beta,y)}\right| \leqslant \begin{cases} \mathrm{e}^{-c_3 u(\tau\log y)^4} & (|\tau| \leqslant 1/\log y), \\ \mathrm{e}^{-c_3 u\tau^4/(1+\tau^4)} & (1/\log y < |\tau| \leqslant Y_\varepsilon). \end{cases} \tag{2.4.13}$$

Démonstration. Posons $s = \beta + i\tau$ $(\tau \in \mathbb{R})$ et notons $\|z\|$ la distance du nombre réel z à l'ensemble des entiers. Les calculs des pages 342-343 de [58] fournissent, pour une constante convenable $\kappa > 0$,

$$\left|\frac{Z_q(s,y)}{Z_q(\beta,y)}\right| \leqslant \mathrm{e}^{-\kappa W_q}$$

avec

$$W_q := \sum_{\substack{p\leqslant y\\ p\nmid q}} \frac{\|(\tau/2\pi)\log p\|^4}{p^\beta}.$$

Lorsque $|\tau| \leqslant 1/\log y$, et puisque (2.2.13) implique $z_q \leqslant y^{3/4}$, nous avons, grâce à (2.3.7),

$$\begin{aligned} \sum_{p\,|\,q} \frac{\|(\tau/2\pi)\log p\|^4}{p^\beta} &\ll \tau^4(\log z_q)^3 \frac{z_q^{1-\beta}-1}{1-\beta} \\ &\ll \tau^4(\log y)^3 \frac{y^{3(1-\beta)/4}-1}{1-\beta} \ll \frac{(\tau\log y)^4 u^{3/4}}{(\log 2u)^{1/4}}. \end{aligned} \tag{2.4.14}$$

Comme la minoration (2.27) de [58] implique

$$W_1 \gg \frac{\tau^4(\log y)^3(y^{1-\beta}-1)}{1-\beta} \gg u(\tau\log y)^4, \tag{2.4.15}$$

et comme u peut être choisi assez grand en vertu de (2.4.4), il suit $W_q \gg u(\tau \log y)^4$, ce qui implique bien (2.4.13) dans ce cas.

Lorsque $1/\log y \leqslant |\tau| \leqslant \sqrt{y}$, l'argument employé dans la démonstration du lemme 5.12 de [45] fournit

$$\sum_{\substack{z/2<p\leqslant z\\ p\nmid q}} \|(\tau/2\pi)\log p\|^4 \gg \frac{\tau^4}{1+\tau^4} \sum_{\substack{z/2<p\leqslant z\\ p\nmid q}} 1 \qquad (y^{3/4} < z \leqslant y). \tag{2.4.16}$$

Or, l'hypothèse (2.2.23) implique $\omega(q) = o\big(z/\log z\big)$. Il suit

$$\sum_{\substack{z/2<p\leqslant z\\ p\nmid q}} 1 \gg \frac{z}{\log z}, \tag{2.4.17}$$

d'où $W_q \gg \tau^4 u/(1+\tau^4)$ par sommation d'Abel, compte tenu de (2.3.6) — cf. [58].

Lorsque $\sqrt{y} < |\tau| \leqslant Y_\varepsilon$, le terme de gauche de (2.4.16) est

$$\gg \sum_{\substack{z/2<p\leqslant z\\ p\nmid q}} \sin^4\big(\tfrac12\tau\log p\big) = \tfrac38 \sum_{\substack{z/2<p\leqslant z\\ p\nmid q}} 1 - \tfrac12 \sum_{\substack{z/2<p\leqslant z\\ p\nmid q}} \big\{\cos(\tau\log p) - \tfrac14\cos(2\tau\log p)\big\}.$$

Comme $\omega(q) = o\big(z/\log z\big)$, l'argument du lemme 2.6 de [58] (relatif au cas $q = 1$) implique que la dernière somme est $o\big(z/\log z\big)$. Compte tenu de (2.4.17), une sommation d'Abel permet de conclure. □

Lemme 2.4.5. *Il existe une constante $c_4 > 0$ telle que, pour tout $\varepsilon > 0$ et sous les conditions* (2.2.13), (2.4.4) *et $1 \leqslant z \leqslant \min\{Y_\varepsilon, \mathrm{e}^{c_4 u}\}$, nous ayons*

$$\Upsilon_q(x + x/z, y) - \Upsilon_q(x, y) \ll x^\beta Z_q(\beta, y)/z. \tag{2.4.18}$$

Démonstration. La preuve est identique à celle du lemme 2.7 de [58] en remplaçant Z par Z_q, et en faisant appel au Lemme 2.4.4. □

2.4.4 Estimations relatives aux séries $Z(s, \chi; y)$

Dans toute cette partie, nous supposons que $\psi(y) > 2\log x$. Pour tout caractère de Dirichlet χ non principal modulo q, posons

$$Z(s,\chi;y) := \prod_{p\leqslant y} \frac{1-\chi(p)^{\nu_p+1}p^{-(\nu_p+1)s}}{1-\chi(p)p^{-s}} \qquad (\Re e(s) > 0),$$

et, sous la condition supplémentaire $|\tau| \leqslant Y_\varepsilon$, définissons également

$$\mathcal{W}_q(y,\tau;\chi) := \sum_{\substack{p\leqslant y\\ p\nmid q}} \frac{(1-\Re e(\chi(p)p^{-i\tau}))^2}{p^\beta}, \tag{2.4.19}$$

et convenons d'omettre l'indice q lorsque $q = 1$.

Les lemmes suivants serviront aux démonstrations des Théorèmes 2.2.4 et 2.2.5.

La preuve du lemme suivant est analogue à celle du lemme 2.6 de [58].

Lemme 2.4.6. *Pour un choix convenable des constantes $c_0 > 0$, $c_5 > 0$, nous avons*

$$\left|\frac{Z(\beta+i\tau,\chi;y)}{Z_q(\beta,y)}\right| \leqslant \mathrm{e}^{-c_5\mathcal{W}_q(y,\tau;\chi)} \qquad \Big(\tau\in\mathbb{R},\ q\leqslant y^{c_0/\log_2 y}\Big).$$

Démonstration. Soit $s := \beta + i\tau$. Un calcul de routine fournit

$$\left|\frac{Z(s,\chi;y)}{Z_q(\beta,y)}\right|^2 = \prod_{\substack{p\leqslant y\\ p\nmid q}} \frac{1+4\sin^2\big(\frac12\alpha_p(\nu_p+1)\big)/\{p^{\beta(\nu_p+1)}(1-p^{-\beta(\nu_p+1)})^2\}}{1+4\sin^2(\frac12\alpha_p)/\{p^\beta(1-p^{-\beta})^2\}} \tag{2.4.20}$$

où $\alpha_p \in]-\pi,\pi]$ est l'argument du nombre complexe $\chi(p)/p^{i\tau}$.

Posons $\vartheta_p := \|\alpha_p/2\pi\|$ et $B_p := p^\beta(1-p^{-\beta})^2$. En raisonnant comme dans la preuve du lemme 2.6 de [58] on obtient que le terme général du produit de (2.4.20) n'excède pas

$$1 - \frac{8\vartheta_p^2\sin^2(\pi\vartheta_p)}{3B_p+12\sin^2(\pi\vartheta_p)}.$$

La minoration $|\sin\pi\vartheta_p| \geqslant 2\vartheta_p$ fournit donc, pour une constante convenable $\kappa_0 > 0$,

$$\left|\frac{Z(s,\chi;y)}{Z_q(\beta,y)}\right|^2 \leqslant \mathrm{e}^{-\kappa_0\mathcal{V}_q} \tag{2.4.21}$$

où l'on a posé

$$\mathcal{V}_q := \sum_{\substack{p\leqslant y\\ p\nmid q}} \frac{\vartheta_p^4}{B_p+4\vartheta_p^2} \gg \sum_{\substack{p\leqslant y\\ p\nmid q}} \frac{\sin^4(\pi\vartheta_p)}{p^\beta} = \sum_{\substack{p\leqslant y\\ p\nmid q}} \frac{(1-\cos(\alpha_p))^2}{4p^\beta}.$$

Cette minoration implique bien le résultat annoncé. □

Posons à présent

$$\mathcal{D}(y,\tau;\chi) := \sum_{p\leqslant y} \frac{\{1-\Re e(\chi(p)/p^{i\tau})\}\log p}{p^\beta}, \quad S(y,\tau;\chi) := \sum_{n\leqslant y}\frac{\chi(n)\Lambda(n)}{n^{\beta+i\tau}}. \tag{2.4.22}$$

Lemme 2.4.7. *Sous la condition* (2.1.1)*, nous avons*

$$\mathcal{D}(y,\tau;\chi) = \frac{y^{1-\beta}}{1-\beta} - \Re e\big(S(y,\tau;\chi)\big) + O\bigg(\frac{y^{1-\beta}}{1-\beta}\Big\{\mathrm{e}^{-\sqrt{\log y}}+\frac1u\Big\}\bigg). \tag{2.4.23}$$

Démonstration. Compte tenu de (2.3.5) et (2.3.7), une forme forte du théorème des nombres premiers fournit par sommation d'Abel — c.f. [6, Lemme 3.5] —

$$\sum_{p\leqslant y}\frac{\log p}{p^\beta} = \frac{y^{1-\beta}}{1-\beta}\bigg\{1+O\Big(\mathrm{e}^{-\sqrt{\log y}}+\frac{1}{u\log 2u}\Big)\bigg\}.$$

De plus,

$$\begin{aligned}\sum_{p\leqslant y}\frac{\chi(p)\log p}{p^{\beta+i\tau}} - S(y,\tau;\chi) &\ll \sum_{\substack{p^\nu\leqslant y\\ \nu\geqslant 2}}\frac{\log p}{p^{\nu\beta}} \ll \big(1+y^{1/2-\beta}\big)\log y\\ &\ll \frac{y^{1-\beta}}{1-\beta}\Big(\frac1u+\frac{\log u}{\sqrt{y}\log y}\Big).\end{aligned}$$

La formule annoncée découle de ces estimations. □

Le lemme suivant est consacré à l'étude de $S(y,\tau;\chi)$ par l'approche développée au lemme III.5.16 de [57]. Nous notons χ_1 l'éventuel caractère de Siegel de module $q>1$ et β_1 le zéro correspondant. Posons

$$\eta(T) := 1/\{(\log T)^{2/3}(\log_2 T)^{1/3}\}, \quad \eta_q(T) := \min(1/\log q, \eta(T)),$$

de sorte que le théorème de Vinogradov-Korobov (cf. par exemple, [38], ch. 9, p. 176) garantit que, pour une constante positive convenable $c_6>0$, le domaine

$$\{\sigma+i\tau : |\tau|\leqslant T, \sigma > 1-c_6\eta_q(T)\}$$

est une région sans zéro de $L(s,\chi)$ lorsque $\chi\neq\chi_1$. Pour c_7 assez grande, $c_0>0$ assez petite, et $q\leqslant y^{c_0/\log_2 y}$, il existe donc, dès que y est assez grand, au plus un zéro de $\prod_{\chi\neq\chi_0} L(s,\chi)$ dans la demi-bande horizontale $\sigma > 1-3c_7(\log_2 y)/\log y$, $|\tau|\leqslant Y_\varepsilon$. Nous posons

$$\vartheta(\chi) := \begin{cases} 1 & \text{si } \chi=\chi_1 \text{ et } \beta_1 > 1-c_7(\log_2 y)/\log y \\ 0 & \text{dans le cas contraire.}\end{cases} \tag{2.4.24}$$

Lemme 2.4.8. *Soit $\varepsilon>0$ assez petit. Lorsque q satisfait* (2.2.22) *et sous la condition*

$$\chi\neq\chi_0, \quad |\tau|\leqslant Y_\varepsilon, \quad 2\log x < \psi(y), \quad y\leqslant \mathrm{e}^{(\log x)^\varepsilon}, \tag{2.4.25}$$

nous avons

$$S(y,\tau;\chi) = -\vartheta(\chi)\frac{y^{\beta_1-\beta-i\tau}}{\beta_1-\beta-i\tau} + O\Big(\frac{y^{1-\beta}}{(\log y)^3}\Big). \tag{2.4.26}$$

Démonstration. Nous pouvons supposer x et donc y assez grands. Notons $w := \beta+i\tau$, $v := 1-\beta+1/\log y$. Il résulte de la formule de Perron effective (cf. [57], corollaire II.2.4) que, sous la condition $|\tau|\leqslant Y_\varepsilon$, nous avons

$$S(y,\tau;\chi) = \frac{-1}{2i\pi}\int_{v-iY_\varepsilon}^{v+iY_\varepsilon} \frac{L'(s+w,\chi)y^s}{L(s+w,\chi)s}\mathrm{d}s + O\Big(\frac{y^{1-\beta}(\log y)^3}{Y_\varepsilon}\Big). \tag{2.4.27}$$

Pour ε assez petit, l'hypothèse (2.4.25) implique

$$1-\beta > 3c_7(\log_2 y)/\log y,$$

en vertu de (2.3.5).

Déplaçons alors le segment d'intégration vers la gauche jusque

$$\delta := 1-\beta-c_7(\log_2 y)/\log y > 2c_7(\log_2 y)/\log y.$$

Lorsque $\chi\neq\chi_1$, la zone traversée ne contient aucun pôle de l'intégrande, alors qu'elle en contient exactement un, à savoir $s=\beta_1-w$ lorsque $\chi=\chi_1$. De plus, dans les deux cas, le segment translaté est à distance $\geqslant c_7(\log_2 y)/\log y$ d'un pôle de l'intégrande.

Le théorème des résidus implique alors que l'intégrale de (2.4.27) vaut

$$\frac{-1}{2i\pi}\int_{\mathfrak{W}} \frac{L'}{L}(s+w,\chi)\frac{y^s}{s}\mathrm{d}s - \vartheta(\chi)\frac{y^{\beta_1-w}}{\beta_1-w} \tag{2.4.28}$$

où $\mathfrak{W}$ désigne la ligne brisée $[v-iY_\varepsilon, \delta-iY_\varepsilon, \delta+iY_\varepsilon, v+iY_\varepsilon]$ parcourue dans le sens trigonométrique inverse.

Compte tenu du placement de $\mathfrak{W}$ par rapport aux pôles de l'intégrande, on peut établir classiquement, via la formule explicite en fonction des zéros (cf., par exemple, [57], pp. 380-381), que

$$\Big|\frac{L'}{L}(s+w,\chi)\Big| \ll (\log qY_\varepsilon)^2 \qquad (s\in\mathfrak{W}).$$

L'intégrale de (2.4.28) est donc

$$\ll (\log yY_\varepsilon)^3 y^\delta + \frac{y^{1-\beta}(\log y)^3}{Y_\varepsilon} \ll \frac{y^{1-\beta}}{(\log y)^3},$$

quitte à augmenter la valeur de c_7. Cela complète la démonstration. □

Lemme 2.4.9. *Sous les conditions* (2.2.22) *et* (2.4.25)*, nous avons*

$$\mathcal{D}(y,\tau;\chi) \gg \frac{y^{1-\beta}}{(1-\beta)\{1+\vartheta(\chi)(\log_2 x)^2\}}. \tag{2.4.29}$$

Démonstration. Conservons les notations de la démonstration du Lemme 2.4.8.

Par (2.4.23) et (2.4.26), nous pouvons écrire, sous les hypothèses effectuées,

$$\mathcal{D}(y,\tau;\chi) = \frac{y^{1-\beta}}{1-\beta} + \vartheta(\chi)\Re e\Big(\frac{y^{\beta_1-\beta-i\tau}}{\beta_1-\beta-i\tau}\Big) + O\bigg(\frac{y^{1-\beta}}{1-\beta}\Big\{\frac{1}{(\log y)^3}+\frac{1}{u}\Big\}\bigg).$$

Cela implique immédiatement (2.4.29) si $\vartheta(\chi)=0$. Dans le cas contraire, nous avons $\chi=\chi_1$, $\beta_1 > 1-c_7\log_2 y/\log y$ et $\beta_1-\beta \gg (\log_2 x)/\log y$.

Si $|\tau| \leqslant 1/\log y$, posant $\varphi := \tau\log y - \arctan\{\tau/(\beta_1-\beta)\}$ il suit

$$\Re e\Big(\frac{y^{\beta_1-\beta-i\tau}}{\beta_1-\beta-i\tau}\Big) = \frac{y^{\beta_1-\beta}\cos\varphi}{|\beta_1-\beta+i\tau|} \geqslant 0,$$

d'où (2.4.29).

Si $1/\log y < |\tau| \leqslant Y_\varepsilon$, nous avons, pour une constante convenable $c_3>0$,

$$\begin{aligned}\Big|\Re e\Big(\frac{y^{\beta_1-\beta-i\tau}}{\beta_1-\beta-i\tau}\Big)\Big| &\leqslant \Big|\frac{y^{\beta_1-\beta}}{\beta_1-\beta-i\tau}\Big| \leqslant \frac{y^{1-\beta}}{|1-\beta+i/\log y|}\\ &\leqslant \frac{y^{1-\beta}}{1-\beta}\Big\{1-\frac{c_3}{(\log_2 x)^2}\Big\}.\end{aligned} \tag{2.4.30}$$

□

2.5 Preuve du Théorème 2.2.1

Plaçons-nous dans les hypothèses (2.2.2) avec, disons, $\varepsilon\in]0,\frac13[$, et posons

$$f_q(s) := \prod_{p\,|\,q}\big(1-p^{-s}\big) \qquad (s\in\mathbb{C}). \tag{2.5.1}$$

Lorsque x est suffisamment grand, on a $\alpha > 1/2 + \varepsilon/5$ d'après (2.3.2). Il suit

$$0 \leqslant \Psi_q(x,y) - \Upsilon_q(x,y) \leqslant \sum_{\substack{p\leqslant y\\ p\nmid q}} \Psi_q\Big(\frac{x}{p^{\nu_p+1}}, y\Big). \tag{2.5.2}$$

Sous la condition supplémentaire $y \leqslant x^{1/3}$, les Théorèmes 2.4.(i) et 2.1 de [6] fournissent

$$\Psi_q\Big(\frac{x}{p^{\nu_p+1}}, y\Big) \ll \frac{f_q(\alpha)}{p^{(\nu_p+1)\alpha}}\Psi(x,y) \ll \frac{\Psi_q(x,y)}{p^{(\nu_p+1)\alpha}}\cdot \tag{2.5.3}$$

En vertu des inégalités (2.5.2) et (2.5.3), il suit

$$\Psi_q(x,y) - \Upsilon_q(x,y) \leqslant \Psi_q(x,y)S, \tag{2.5.4}$$

où l'on a posé

$$S := \sum_{\substack{p\leqslant y\\ p\nmid q}} \frac{1}{p^{(\nu_p+1)\alpha}} \ll \frac{y^{1/2-\alpha}}{\log y} \ll \frac{u\log 2u}{\sqrt{y}\log y}, \tag{2.5.5}$$

d'après [58, formule (31)]. Cela implique bien (2.2.3) dans le cas considéré.

Lorsque $x^{1/3} \leqslant y \leqslant x$, nous avons $u \leqslant 3$ et $\Psi_q(x,y) \ll f_q(\alpha)\Psi(x,y) \asymp f_q(\alpha)x$ en vertu de [6, th. 24.4(i)] et, par exemple, [8]. De plus, on déduit aisément de (2.3.2) que $f_q(\alpha) \asymp f_q(1) = \varphi(q)/q$. La majoration triviale $\Psi_q\big(x/p^{\nu_p+1}, y\big) \leqslant x/p^{\nu_p+1}$ fournit donc

$$\Psi_q(x,y) - \Upsilon_q(x,y) \leqslant \sum_{p\leqslant y} \frac{x}{p^{\nu_p+1}} \ll \frac{\Psi(x,y)}{\sqrt{y}\log y} \ll \frac{\Psi_q(x,y)}{f_q(\alpha)\sqrt{y}\log y} \ll \frac{q\Psi_q(x,y)}{\varphi(q)\sqrt{y}\log y}\cdot$$

Cela complète la preuve de (2.2.3).

2.6 Preuve du Théorème 2.2.2

Étant donné $\varepsilon > 0$, nous nous plaçons sous les hypothèses (2.2.12) et (2.2.13).

Le lemme suivant étend à $Z_q(s,y)$ la formule (3.4) de [58].

Lemme 2.6.1. *Soit c_4 la constante apparaissant au Lemme 2.4.5. Pour un choix convenable de $c_8 > 0$, et tout $\varepsilon > 0$, nous avons, sous l'hypothèse* (2.2.13)*,*

$$\Upsilon_q(x,y) = \frac{1}{2i\pi}\int_{\beta-iT}^{\beta+iT} \frac{Z_q(s,y)x^s}{s}\mathrm{d}s + O\Big(\frac{x^\beta Z_q(\beta,y)\log T}{T}\Big) \tag{2.6.1}$$

avec $T := \mathrm{e}^{2c_8(\log u)^{4/3}} \leqslant \min(Y_{1/20}, \mathrm{e}^{c_4 u})$.

Démonstration. Une version effective de la formule de Perron (cf. [57, thm. II.2.3]) permet de montrer que la différence entre le membre de gauche de (2.6.1) et l'intégrale du membre de droite est

$$\begin{aligned}
&\ll \frac{1}{T} \sum_{\substack{n\geqslant 1\\ n\in U(y)}} \frac{x^\beta}{n^\beta\{1+T|\log(x/n)|\}}\\
&\ll \frac{x^\beta Z_q(\beta,y)}{T} + \sum_{|h|\leqslant T} \frac{x^\beta}{1+|h|}\Big\{\Upsilon_q\big(x\mathrm{e}^{(h+1)/T},y\big)-\Upsilon_q\big(x\mathrm{e}^{h/T},y\big)\Big\}\\
&\ll \frac{x^\beta Z_q(\beta,y)}{T}\Big\{1+\sum_{|h|\leqslant T}\frac{1}{|h|+1}\Big\},
\end{aligned}$$

d'après le Lemme 2.4.5. Cela implique bien (2.6.1). □

Pour $1\leqslant U\leqslant V$, désignons par $I_q(U,V)$ la contribution du domaine $U\leqslant|\tau|\leqslant V$ à l'intégrale de (2.6.1). Nous posons $T_0:=(\log u)^{(1+\varepsilon)/2}/\{\sqrt{u}\log y\}$.

Lemme 2.6.2. *Pour un choix convenable de $c_9>0$ et tout $\varepsilon>0$, nous avons, sous l'hypothèse* (2.2.12)*,*

$$I_q(T_0,T)\ll x^\beta Z_q(\beta,y)\mathrm{e}^{-c_9(\log(2u))^{1+\varepsilon}}. \tag{2.6.2}$$

Démonstration. Posons $T_1:=u^{-1/3}/\log y$, $T_2:=u^{-1/5}/\log y$. D'après le Lemme 2.4.4, nous pouvons écrire

$$I_q(T_2,T)\ll x^\beta Z_q(\beta,y)\big\{I_{21}+I_{22}\big\},$$

avec

$$I_{21}:=\int_{T_2}^{1/\log y}\mathrm{e}^{-c_3u(\tau\log y)^4}\frac{\mathrm{d}\tau}{\beta+\tau}\ll \mathrm{e}^{-c_3u(T_2\log y)^4}\log u\ll \mathrm{e}^{-\frac12 c_3u^{1/5}}$$

et

$$I_{22}:=\int_{1/\log y}^{T}\mathrm{e}^{-c_3u\tau^4/(1+\tau^4)}\frac{\mathrm{d}\tau}{\tau}\ll x^{-\frac12 c_3u/(\log y)^4}\log_2 y+\mathrm{e}^{-\frac12 c_3u}(\log u)^{4/3}.$$

Il s'ensuit que

$$I_q(T_2,T)\ll x^\beta Z_q(\beta,y)\mathrm{e}^{-c_9(\log(2u))^{1+\varepsilon}}. \tag{2.6.3}$$

Lorsque $T_1<|\tau|\leqslant T_2$, nous avons $\tau^2\sigma_{2,q}\gg u^{1/3}$ et $\tau^4\sigma_{4,q}\ll u^{1/5}$, en vertu Lemme 2.4.3. Il résulte alors d'un développement limité que

$$\begin{aligned}
Z_q(s,y)x^s &= Z_q(\beta,y)x^\beta\mathrm{e}^{i\tau\gamma_q'(\beta)-\tau^2\sigma_{2,q}/2+i\tau^3\sigma_{3,q}/6+\sigma_{4,q}\tau^4/24+O(1)}\\
&\ll Z_q(\beta,y)x^\beta\mathrm{e}^{-c_{10}u^{1/3}},
\end{aligned} \tag{2.6.4}$$

ce qui implique

$$I_q(T_1,T_2)\ll x^\beta Z_q(\beta,y)\mathrm{e}^{-c_{11}u^{1/3}}. \tag{2.6.5}$$

Lorsque $T_0 < |\tau| \leqslant T_1$, nous avons $\tau^2\sigma_{2,q} \gg (\log(2u))^{1+\varepsilon}$ et $\tau^4\sigma_{4,q} \ll u^{-1/3}$ d'après le Lemme 2.4.3. Un développement limité fournit donc

(2.6.6)
$$x^s Z_q(s,y) \ll x^\beta Z_q(\beta,y)\mathrm{e}^{-\tau^2\sigma_{2,q}/2+\tau^4\sigma_{4,q}/4+O(1)} \ll x^\beta Z_q(\beta,y)\mathrm{e}^{-c_{12}(\log(2u))^{1+\varepsilon}}.$$

L'estimation (2.6.2) découle de (2.6.3), (2.6.5) et (2.6.6). □

Nous sommes à présent en mesure de terminer la preuve du Théorème 2.2.2. D'après (2.6.1) et (2.6.2), nous avons

$$\Upsilon_q(x,y) = I_q(0,T_0) + O\Big(x^\beta Z_q(\beta,y)\mathrm{e}^{-c_9(\log(2u))^{1+\varepsilon}}\Big). \tag{2.6.7}$$

Évaluons à présent le terme principal de (2.6.7).

Puisque $T_0^j\sigma_{j,q} \ll 1$ lorsque $j = 3,4$ et $\varphi_{4,q}(\beta+i\tau,y) \ll \sigma_4^* := u(\log y)^4$ pour $|\tau| \leqslant 1/\log y$ et $T_0\gamma_q'(\beta) \ll 1$ grâce à (2.4.1) et (2.4.5), nous pouvons écrire

$$\begin{aligned} I_q(0,T_0) &= \frac{x^\beta Z_q(\beta,y)}{2\pi}\int_{-T_0}^{T_0} \mathrm{e}^{i\tau\gamma_q'(\beta)-\tau^2\sigma_{2,q}/2+i\tau^3\sigma_{3,q}/6+O(\tau^4\sigma_4^*)}\frac{\mathrm{d}\tau}{\beta+i\tau} \\ &= \frac{x^\beta Z_q(\beta,y)}{2\pi}\Big\{J_0 + iJ_1 + \tfrac{1}{6}iJ_2 + O(K)\Big\} \end{aligned} \tag{2.6.8}$$

où

$$\begin{aligned} J_0 &:= \int_{-T_0}^{T_0} \mathrm{e}^{-\tau^2\sigma_{2,q}/2}\frac{\mathrm{d}\tau}{\beta+i\tau}, \quad J_1 := \gamma_q'(\beta)\int_{-T_0}^{T_0} \tau\mathrm{e}^{-\tau^2\sigma_{2,q}/2}\frac{\mathrm{d}\tau}{\beta+i\tau}, \\ J_2 &:= \sigma_{3,q}\int_{-T_0}^{T_0} \tau^3\mathrm{e}^{-\tau^2\sigma_{2,q}/2}\frac{\mathrm{d}\tau}{\beta+i\tau}, \\ K &:= \int_{-T_0}^{T_0} \mathrm{e}^{-\tau^2\sigma_{2,q}/2}\Big(\tau^6\sigma_{3,q}^2 + \tau^4\sigma_4^* + \tau^2\gamma_q'(\beta)^2\Big)\frac{\mathrm{d}\tau}{\beta+|\tau|}. \end{aligned}$$

Des calculs semblables à ceux de la fin de la proposition 2.13 de [5], utilisant le Lemme 2.4.3, fournissent

$$J_0 = 2\pi G\big(\beta\sqrt{\sigma_{2,q}}\big) + O(\mathrm{e}^{-c_9u^{1/3}}), \qquad J_2 \ll \frac{1}{u(1+\beta\sqrt{\sigma_{2,q}})}. \tag{2.6.9}$$

Par le changement de variables $v = \tau\sqrt{\sigma_{2,q}}$, nous pouvons écrire

$$\begin{aligned} K &= \int_{-T_0\sqrt{\sigma_{2,q}}}^{T_0\sqrt{\sigma_{2,q}}} \mathrm{e}^{-v^2/2}\Big(\frac{\sigma_{3,q}^2v^6}{\sigma_{2,q}^3} + \frac{\sigma_4^*v^4}{\sigma_{2,q}^2} + \frac{\gamma_q'(\beta)^2v^2}{\sigma_{2,q}}\Big)\frac{\mathrm{d}v}{\beta\sqrt{\sigma_{2,q}}+|v|} \\ &\ll \frac{1+D_q^2}{u(1+\beta\sqrt{\sigma_{2,q}})}, \end{aligned} \tag{2.6.10}$$

la dernière majoration découlant des Lemmes 2.4.2 et 2.4.3.

En tenant à nouveau compte du fait que l'intégrale d'une fonction impaire sur un intervalle symétrique par rapport à l'origine est nulle, le même changement de

variables fournit

$$J_1 = \frac{-i\gamma_q'(\beta)}{\sqrt{\sigma_{2,q}}} \int_{-T_0\sqrt{\sigma_{2,q}}}^{T_0\sqrt{\sigma_{2,q}}} \frac{v^2 \mathrm{e}^{-v^2/2}\,\mathrm{d}v}{\beta^2\sigma_{2,q}+v^2},$$
$$= \frac{-i\gamma_q'(\beta)}{\sqrt{\sigma_{2,q}}} \Bigg\{ \int_{-T_0\sqrt{\sigma_{2,q}}}^{T_0\sqrt{\sigma_{2,q}}} \mathrm{e}^{-v^2/2}\,\mathrm{d}v - \beta^2\sigma_{2,q} \int_{-T_0\sqrt{\sigma_{2,q}}}^{T_0\sqrt{\sigma_{2,q}}} \frac{\mathrm{e}^{-v^2/2}\,\mathrm{d}v}{\beta^2\sigma_{2,q}+v^2} \Bigg\}.$$

Nous avons

$$\frac{1}{\sqrt{2\pi}} \int_{-T_0\sqrt{\sigma_{2,q}}}^{T_0\sqrt{\sigma_{2,q}}} \mathrm{e}^{-v^2/2}\,\mathrm{d}v = 1 + O\Big(\mathrm{e}^{-(\log u)^{1+\varepsilon/2}}\Big),$$
$$\beta\sqrt{\sigma_{2,q}} \int_{-T_0\sqrt{\sigma_{2,q}}}^{T_0\sqrt{\sigma_{2,q}}} \frac{\mathrm{e}^{-v^2/2}\,\mathrm{d}v}{\beta^2\sigma_{2,q}+v^2} = J_0,$$

et donc

$$\frac{iJ_1}{2\pi} = \frac{\gamma_q'(\beta)}{\sqrt{2\pi\sigma_{2,q}}} \Big\{ 1 - \beta\sqrt{2\pi\sigma_{2,q}} G\big(\beta\sqrt{\sigma_{2,q}}\big) \Big\} + O\Big(\mathrm{e}^{-(\log u)^{1+\varepsilon/2}}\Big). \tag{2.6.11}$$

En reportant (2.6.9), (2.6.10) et (2.6.11) dans (2.6.8) puis (2.6.7), nous obtenons

$$\Upsilon_q(x,y) = x^\beta Z_q(\beta,y) G(\beta\sqrt{\sigma_{2,q}}) \Big\{ 1 + R_q(\beta) + O\Big(\frac{1+D_q^2}{u}\Big) \Big\} \tag{2.6.12}$$

avec

$$R_q(\beta) := \beta\gamma_q'(\beta) \Big(\frac{1}{\sqrt{2\pi\sigma_{2,q}}\beta G(\beta\sqrt{\sigma_{2,q}})} - 1 \Big).$$

Comme (2.2.7) implique

$$\frac{1}{\sqrt{2\pi}zG(z)} - 1 \asymp \frac{1}{z(z+1)} \qquad (z>0), \tag{2.6.13}$$

il vient, par (2.4.5) et (2.3.3),

$$R_q(\beta) \ll \frac{D_q}{\sqrt{u}(1+\beta\sqrt{\sigma_{2,q}})} \ll \frac{D_q(1+\eta)}{\sqrt{u}+\eta u}. \tag{2.6.14}$$

Pour obtenir (2.2.14), il suffit donc de montrer que l'on peut remplacer $\sigma_{2,q}$ par σ_2 dans (2.6.12) et (2.6.14) sans altérer le terme d'erreur.

C'est clair dans la majoration (2.6.14) au vu de (2.4.11). Pour traiter le cas de (2.6.12), observons que l'on a $\sigma_{2,q}-\sigma_2 \ll C_q(\log y)^2$ en vertu de la seconde majoration (2.4.5), et donc

$$\sqrt{\sigma_{2,q}} - \sqrt{\sigma_2} \ll C_q(\log y)^2/\sqrt{\sigma_2} \ll C_q(\log y)/\sqrt{u}.$$

Comme il résulte de (2.2.7) que

$$\frac{G'(z)}{G(z)} = z - \frac{1}{\sqrt{2\pi}G(z)} \asymp \frac{-1}{1+z} \qquad (z>0), \tag{2.6.15}$$

nous obtenons, par l'égalité des accroissements finis,

$$G(\beta\sqrt{\sigma_{2,q}}) = \Big\{1 + O\Big(\frac{C_q\beta\log y}{\sqrt{u}(1+\beta\sqrt{\sigma_2})}\Big)\Big\}G\big(\beta\sqrt{\sigma_2}\big). \tag{2.6.16}$$

Par (2.4.11) et la Remarque 2.2.3(a), le terme d'erreur de (2.6.16) est en toute circonstance

$$\ll \frac{C_q\beta\log y}{\sqrt{u}+u\beta\log y} \ll \frac{C_q\eta}{\sqrt{u}+\eta u} \ll \begin{cases} \dfrac{D_q\eta}{\sqrt{u}+\eta u} & \text{si } \eta \leqslant 1 \\ \dfrac{D_q^2}{u} & \text{si } \eta > 1. \end{cases}$$

Cela établit bien (2.2.14).

Pour montrer (2.2.15), précisons le terme d'erreur de (2.2.14) lorsque $\eta \leqslant \frac12$. Nous pouvons supposer η arbitrairement petit et $q \geqslant 2$ grâce à (2.2.8). D'après (2.3.3), nous avons $\beta\log y \leqslant 1$ dès que y est assez grand.

D'après (2.4.6), nous pouvons écrire

$$\gamma_q'(\beta) = \tfrac12\omega(q)\log y\big\{1 + O\big(\mathfrak{R}\big)\big\} \tag{2.6.17}$$

avec $\mathfrak{R} := \eta + \log q/\{\omega(q)\log y\}$. Nous pouvons donc remplacer le signe $\ll$ par $\asymp$ dans l'estimation (2.6.14).

De plus, la seconde estimation (2.4.6) permet également d'écrire

$$\sigma_2 - \sigma_{2,q} = \tfrac{1}{12}\omega(q)(\log y)^2\big\{1 + O(\mathfrak{R})\big\}. \tag{2.6.18}$$

Il suit

$$\sqrt{\sigma_2} - \sqrt{\sigma_{2,q}} \asymp \frac{\omega(q)\log y}{\sqrt{u}}, \tag{2.6.19}$$

d'où, par (2.6.15),

$$\frac{G(\beta\sqrt{\sigma_{2,q}})}{G(\beta\sqrt{\sigma_2})} - 1 \asymp \frac{\eta\omega(q)}{\sqrt{u}(1+\eta\sqrt{u})}. \tag{2.6.20}$$

La formule (2.2.15) résulte de ces observations en reportant dans (2.6.12).

Prouvons à présent l'estimation (2.2.16), relative au cas $\eta = o(1/\sqrt{u})$. Il résulte de (2.6.19) que

$$\sqrt{\sigma_{2,q}} = \sqrt{\sigma_2}\Big\{1 + O\Big(\frac{\omega(q)}{u}\Big)\Big\}$$

et de (2.4.12) que

$$\sqrt{\sigma_2} = \frac{\sqrt{u}\log y}{\sqrt{2}}\Big\{1 + O\Big(\eta + \frac{1}{\log y}\Big)\Big\}.$$

Grâce à (2.6.17), il suit

$$\frac{\gamma_q'(\beta)}{\sqrt{2\pi\sigma_{2,q}}} = \frac{\omega(q)}{2\sqrt{\pi u}}\big\{1 + O\big(\mathfrak{R}\big)\big\}.$$

Compte tenu de (2.2.7), (2.6.12) et (2.6.20), nous obtenons bien (2.2.16) lorsque

$$\beta\sqrt{\sigma_2} \asymp \eta\sqrt{u} = o(1).$$

2.7 Preuve du Théorème 2.2.4

Plaçons-nous dans les hypothèses (2.2.21) et (2.2.22).

Parallèlement à (2.6.1), nous pouvons écrire, pour $\chi \neq \chi_0$ et $T := Y_{2\varepsilon}$,

$$\Upsilon(x,y;\chi) = \frac{1}{2i\pi}\int_{\beta-iT}^{\beta+iT} Z(s,\chi;y)x^s\frac{\mathrm{d}s}{s} + O\Big(\frac{x^\beta Z_q(\beta,y)\log T}{T}\Big). \tag{2.7.1}$$

De plus, le Lemme 2.4.6 implique que, pour $s=\beta+i\tau$, $|\tau|\leqslant T$, et une constante convenable $\kappa>0$, nous avons

$$|Z(s,\chi;y)| \leqslant Z_q(\beta,y)\mathrm{e}^{-\kappa\mathcal{W}_q(y,\tau;\chi)}. \tag{2.7.2}$$

où $\mathcal{W}_q(y,\tau;\chi)$ a été défini par (2.4.19).

Nous avons aussi, par sommation d'Abel — c.f. [6, lemme 3.6] — sous la seule condition (2.1.1), grâce à (2.3.6),

$$\sum_{p\leqslant y}\frac{1}{p^\beta} \asymp u. \tag{2.7.3}$$

La quantité $\mathcal{D}(y,\tau;\chi)$ étant définie en (2.4.22), nous pouvons donc déduire de (2.3.5), (2.3.7), et (2.4.29), via l'inégalité de Cauchy-Schwarz, que

$$\mathcal{W}(y,\tau;\chi) \geqslant \frac{\mathcal{D}(y,\tau;\chi)^2}{(\log y)^2\sum_{p\leqslant y}p^{-\beta}} \gg \frac{u}{1+\vartheta(\chi)(\log u)^4}, \tag{2.7.4}$$

où $\vartheta(\chi)$ a été défini par (2.4.24).

Rappelons la notation (2.2.9) et observons que l'hypothèse (2.2.22) implique $z_q \ll \log y$, et donc, compte tenu de (2.3.5), pour tout $\varepsilon>0$,

$$\sum_{p\,|\,q}\frac{1}{p^\beta} \ll \frac{z_q^{1-\beta}-1}{(1-\beta)\log z_q} \ll_\varepsilon u^\varepsilon. \tag{2.7.5}$$

Compte tenu de (2.7.4), il vient, pour un choix convenable de $c_2>0$,

$$|Z(s,\chi;y)| \leqslant Z_q(\beta,y)\mathrm{e}^{-c_2u(\chi)} \qquad (|\tau|\leqslant Y_{2\varepsilon}), \tag{2.7.6}$$

où l'on a posé $u(\chi) := u/\{1+\vartheta(\chi)(\log u)^4\}$.

En reportant (2.7.6) dans (2.7.1), nous obtenons

$$\Upsilon(x,y;\chi) \ \ll \ x^\beta Z_q(\beta,y)\Big\{(\log y)^{3/2}\mathrm{e}^{-c_2u(\chi)} + Y_\varepsilon^{-1}\Big\},$$

et donc, compte tenu de (2.2.18),

$$\Upsilon(x,y;\chi) \ \ll \ \Upsilon_q(x,y)\sqrt{u}\log y\Big\{(\log y)^{3/2}\mathrm{e}^{-c_2u(\chi)} + Y_\varepsilon^{-1}\Big\}.$$

La condition supplémentaire (2.2.21) permet donc de conclure.

2.8 Preuve du Théorème 2.2.5

La relation d'orthogonalité des caractères permet d'écrire

$$\Upsilon(x,y;a,q)=\frac{1}{\varphi(q)}\Big\{\Upsilon_q(x,y)+\sum_{\chi\neq\chi_0}\overline{\chi(a)}\Upsilon(x,y;\chi)\Big\}.$$

L'estimation annoncée découle donc directement du Théorème 2.2.4.

2.9 Preuve du Théorème 2.2.6

Plaçons-nous dans les hypothèses de l'énoncé. Il résulte de (2.2.3) et de l'estimation $q/\varphi(q)\ll\log_2 q$ que

$$\Psi_q(x,y)-\Upsilon_q(x,y)\ll\frac{qu\log(2u)\Psi_q(x,y)}{\varphi(q)\sqrt{y}\log y}\ll\frac{\Psi_q(x,y)}{\log y}. \tag{2.9.1}$$

De plus

$$\begin{aligned}\Psi(x,y;a,q)-\Upsilon(x,y;a,q)&\leqslant\sum_{\substack{p\leqslant y\\ p\nmid q}}\Psi\Big(\frac{x}{p^{\nu_p+1}},y;a/p^{\nu_p+1},q\Big)\\&\leqslant\sum_{p\leqslant y}\sup_{(b,q)=1}\Psi\Big(\frac{x}{p^{\nu_p+1}},y;b,q\Big)\end{aligned} \tag{2.9.2}$$

où, dans la première inégalité, a/p^{ν_p+1} désigne la classe des entiers b tels que

$$p^{\nu_p+1}b\equiv a\,(\mathrm{mod}\,q).$$

D'après (2.2.19), (2.5.3), sous la condition supplémentaire $y\leqslant x^{1/3}$, chaque terme de la dernière somme est

$$\ll\Psi_q\Big(\frac{x}{p^{\nu_p+1}},y\Big)\ll\frac{f_q(\alpha)\Psi(x,y)}{p^{(\nu_p+1)\alpha}}\ll\frac{\Psi_q(x,y)}{p^{(\nu_p+1)\alpha}}\ll\frac{\Upsilon_q(x,y)}{p^{(\nu_p+1)\alpha}}.$$

Les estimations (2.5.5) et (2.2.19) impliquent alors (2.2.25). [1]

Lorsque $x^{1/3}<y\leqslant x$, nous déduisons simplement de (2.9.2) que

$$\Psi(x,y;a,q)-\Upsilon(x,y;a,q)\ll\sum_{p\leqslant y}\frac{x}{p^{\nu_p+1}}\ll\frac{\Psi(x,y)}{\sqrt{y}\log y}\ll\frac{\Psi_q(x,y)}{\varphi(q)\log y}.$$

Nous obtenons encore (2.2.25).

1. Il est à noter que dans ce cas, la condition sur q peut être relâchée en $q\leqslant y^{1-\varepsilon}$.

Bibliographie

[1] W. D. Banks, J. B. Friedlander, and F. Luca. Integers without divisors from a fixed arithmetic progression. *Forum Math.*, 20(6) :1005–1037, 2008.

[2] E. Bombieri. On the large sieve. *Mathematika*, 12 :201–225, 1965.

[3] C. Dartyge. Entiers friables : un tour d'horizon. *Gaz. Math.*, (156) :29–39, 2018.

[4] N. G. de Bruijn. On the number of positive integers $\leq x$ and free of prime factors $> y$. *Nederl. Acad. Wetensch. Proc. Ser. A.*, 54 :50–60, 1951.

[5] R. de la Bretèche and G. Tenenbaum. Sur les lois locales de la répartition du k-ième diviseur d'un entier. *Proc. London Math. Soc. (3)*, 84(2) :289–323, 2002.

[6] R. de la Bretèche and G. Tenenbaum. Propriétés statistiques des entiers friables. *Ramanujan J.*, 9(1-2) :139–202, 2005.

[7] H. Delange. Sur la distribution des entiers ayant certaines propriétés. *Ann. Sci. Ecole Norm. Sup. (3)*, 73 :15–74, 1956.

[8] K. Dickman. On the frequency of numbers containing prime factors of a certain relative magnitude. *Ark. Mat. Astr. Fys.*, 22 :1–14, 1930.

[9] G. L. Dirichlet. Beweis des Satzes, dassjede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhand. Ak. Wiss. Berlin*, 48 :45–81, 1837.

[10] S. Drappeau. Théorèmes de type Fouvry-Iwaniec pour les entiers friables. *Compos. Math.*, 151(5) :828–862, 2015.

[11] S. Eberhard, K. Ford, and B. Green. Permutations fixing a k-set. *Int. Math. Res. Not. IMRN*, (21) :6713–6731, 2016.

[12] P. Erdős. On the distribution of divisors of integers in the residue classes (mod d). *Bull. Soc. Math. Grèce (N.S.)*, 6 I(fasc., fasc. 1) :27–36, 1965.

[13] P. Erdős and I. Z. Ruzsa. On the small sieve. I. Sifting by primes. *J. Number Theory*, 12(3) :385–394, 1980.

[14] P. Erdös. On amicable numbers. *Publ. Math. Debrecen*, 4 :108–111, 1955.

[15] K. Ford. The distribution of integers with a divisor in a given interval. *Ann. of Math. (2)*, 168(2) :367–433, 2008.

[16] K. Ford, M. R. Khan, I. E. Shparlinski, and C. L. Yankov. On the maximal difference between an element and its inverse in residue rings. *Proc. Amer. Math. Soc.*, 133(12) :3463–3468, 2005.

[17] E. Fouvry and G. Tenenbaum. Entiers sans grand facteur premier en progressions arithmetiques. *Proc. London Math. Soc. (3)*, 63(3) :449–494, 1991.

[18] E. Fouvry and G. Tenenbaum. Répartition statistique des entiers sans grand facteur premier dans les progressions arithmétiques. *Proc. London Math. Soc. (3)*, 72(3) :481–514, 1996.

[19] A. Granville. Integers, without large prime factors, in arithmetic progressions. I. *Acta Math.*, 170(2) :255–273, 1993.

[20] A. Granville. Integers, without large prime factors, in arithmetic progressions. II. *Philos. Trans. Roy. Soc. London Ser. A*, 345(1676) :349–362, 1993.

[21] A. Granville. Smooth numbers : computational number theory and beyond. In *Algorithmic number theory : lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 267–323. Cambridge Univ. Press, Cambridge, 2008.

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

[23] R. R. Hall and G. Tenenbaum. On the average and normal orders of Hooley's Δ-function. *J. London Math. Soc. (2)*, 25(3) :392–406, 1982.

[24] A. Harper. Bombieri–Vinogradov and Barban-Davenport–Halberstam type theorems for smooth numbers. 2012. pré-publication.

[25] A. J. Harper. On a paper of K. Soundararajan on smooth numbers in arithmetic progressions. *J. Number Theory*, 132(1) :182–199, 2012.

[26] A. Hildebrand. On the number of positive integers $\leq x$ and free of prime factors $> y$. *J. Number Theory*, 22(3) :289–307, 1986.

[27] A. Hildebrand and G. Tenenbaum. On integers free of large prime factors. *Trans. Amer. Math. Soc.*, 296(1) :265–290, 1986.

[28] A. Hildebrand and G. Tenenbaum. Integers without large prime factors. *J. Théor. Nombres Bordeaux*, 5(2) :411–484, 1993.

[29] C. Hooley. On a new technique and its applications to the theory of numbers. *Proc. London Math. Soc. (3)*, 38(1) :115–151, 1979.

[30] K.-H. Indlekofer and N. M. Timofeev. Divisors of shifted primes. *Publ. Math. Debrecen*, 60(3-4) :307–345, 2002.

[31] C. G. Ji. The number of kth power residues modulo m. *J. Nanjing Norm. Univ. Nat. Sci. Ed.*, 24(1) :1–2, 2001.

[32] C. La Vallée Poussin. Recherches analytiques sur la théorie des nombres premiers, 1. *Ann. Soc. Scient. Bruxelles*, 20 :183–256, 1896.

[33] E. Landau. *Handbuch der Lehre von der Verteilung der Primzahlen.* Taubner, 1909. Reprint Chelsea (1953).

[34] E. Landau. Über die Klassenzahl imaginär-quadratischer Zahlkörper. *Gött. Nachr. 1918*, pages 285–295, 1918.

[35] H. Maier and G. Tenenbaum. On the set of divisors of an integer. *Invent. Math.*, 76(1) :121–128, 1984.

[36] H. Maier and G. Tenenbaum. On the normal concentration of divisors. II. *Math. Proc. Cambridge Philos. Soc.*, 147(3) :513–540, 2009.

[37] M. Margenstern. Les nombres pratiques : théorie, observations et conjectures. *J. Number Theory*, 37(1) :1–36, 1991.

[38] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC ; by the American Mathematical Society, Providence, RI, 1994.

[39] M. Nair and G. Tenenbaum. Short sums of certain arithmetic functions. *Acta Math.*, 180(1) :119–144, 1998.

[40] W. Narkiewicz and M. Radziejewski. Integers without divisors in a given progression. *Monatsh. Math.*, 164(1) :75–85, 2011.

[41] J. E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1 :8–10, 1969.

[42] C. Pomerance. On the distribution of amicable numbers. *J. Reine Angew. Math.*, 293(294) :217–222, 1977.

[43] C. Pomerance. The role of smooth numbers in number-theoretic algorithms. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 411–422. Birkhäuser, Basel, 1995.

[44] D. Raikov. О распределении чисел, простые делители которых принадлежат заданной арифметической прогрессии. *Mat. Sbornik*, 4 :563–570, 1938.

[45] O. Robert and G. Tenenbaum. Sur la répartition du noyau d'un entier. *Indag. Math. (N.S.)*, 24(4) :802–914, 2013.

[46] E. Saias. Sur le nombre des entiers sans grand facteur premier. *J. Number Theory*, 32(1) :78–99, 1989.

[47] E. Saias. Entiers à diviseurs denses. I. *J. Number Theory*, 62(1) :163–191, 1997.

[48] E. Saias. Applications des entiers à diviseurs denses. *Acta Arith.*, 83(3) :225–240, 1998.

[49] J. W. Sander. Integral circulant Ramanujan graphs via multiplicativity and ultrafriable integers. *Linear Algebra Appl.*, 477 :21–41, 2015.

[50] I. E. Shparlinski. Modular hyperbolas. *Jpn. J. Math.*, 7(2) :235–294, 2012.

[51] C. Siegel. Über die Classenzahl quadratischer Körper. *Acta Arith.*, 1 :83–86, 1936.

[52] K. Soundararajan. The distribution of smooth numbers in arithmetic progressions. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 115–128. Amer. Math. Soc., Providence, RI, 2008.

[53] G. Tenenbaum. Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné. *Compositio Math.*, 51(2) :243–263, 1984.

[54] G. Tenenbaum. Fonctions Δ de Hooley et applications. In *Séminaire de théorie des nombres, Paris 1984–85*, volume 63 of *Progr. Math.*, pages 225–239. Birkhäuser Boston, Boston, MA, 1986.

[55] G. Tenenbaum. Sur un problème de crible et ses applications. *Ann. Sci. École Norm. Sup. (4)*, 19(1) :1–30, 1986.

[56] G. Tenenbaum. Sur un problème de crible et ses applications. II. Corrigendum et étude du graphe divisoriel. *Ann. Sci. École Norm. Sup. (4)*, 28(2) :115–127, 1995.

[57] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. coll. Échelles, quatrième édition. Belin, Paris, 2015.

[58] G. Tenenbaum. On ultrafriable integers. *Q. J. Math.*, 66(1) :333–351, 2015.

[59] A. I. Vinogradov. Correction to the paper of A. I. Vinogradov "On the density hypothesis for the Dirichlet L-series". *Izv. Akad. Nauk SSSR Ser. Mat.*, 30 :719–720, 1966.

[60] A. Walfisz. Zur additiven Zahlentheorie. II. *Mathematische Zeitschrift*, 40(1) :592–607, 1936.

[61] A. Weingartner. Practical numbers and the distribution of divisors. *Q. J. Math.*, 66(2) :743–758, 2015.

UNIVERSITÉ DE LORRAINE

École doctorale IAEM

Abstract — This thesis is divided into two main parts.

In the first chapter, we consider the number of integers not exceeding x and admitting no divisor in an arithmetic progression $a(\mathrm{mod}\ q)$ where q is fixed. We improve here a result of Narkiewicz and Radziejewski published in 2011 by providing a different main term with a simpler expression, and we specify the term error. The main tools are the Selberg-Delange method and the Hankel contour. We also study in detail the particular case where a is a quadratic nonresidue modulo q. We also extend our result to the integers which admit no divisor in a finite set of residual classes modulo q.

In the second chapter, we study the ultrafriable integers in arithmetic progressions. An integer is said to be y-ultrafriable if no prime power which divide it exceeds y. We begin with the studying of the counting function of these integers when they are coprime to q. Then we give an asymptotic formula about the number of y-ultrafriable integers which don't exceed a number x and in an arithmetic progression a modulo q, where q is a y-friable modulus, which means that it is without a prime divisor exceeding y. Our results are valid when q, x, y are integers which verify $\log x \ll y < x$, $q < y^{c/\log\log y}$, where $c > 0$ is a suitably chosen constant.

Keywords — divisors, arithmetic progression, sieves, ultrafriable integers

---

Institut ÉLIE CARTAN

Institut Élie Cartan de Lorraine
Laboratoire de mathématiques — UMR 7503
54506 VANDOEUVRE-LES-NANCY

UNIVERSITÉ DE LORRAINE

École doctorale IAEM

Résumé — Cette thèse se divise en deux grandes parties.

Le premier chapitre porte sur l'étude du nombre des entiers n'excédant pas x et n'admettant aucun diviseur dans une progression arithmétique $a(\mathrm{mod}\ q)$ donnée. Nous améliorons ici un résultat de Narkiewicz et Radziejewski de 2011 en fournissant une expression différente et plus simple du terme principal et en précisant le terme d'erreur. Les outils principaux sont la méthode de Selberg-Delange et le contour de Hankel. Nous étudions plus en détail le cas particulier où a n'est pas un résidu quadratique modulo q. Nous étendons également notre résultat aux entiers n'admettant aucun diviseur dans un ensemble fini de classes résiduelles modulo q.

Le second chapitre est consacré aux entiers ultrafriables dans les progressions arithmétiques. Un entier y-ultrafriable est un entier dont toutes les puissances de nombres premiers qui le divisent sont inférieures à y. Nous commençons par étudier la fonction de comptage des ces entiers lorsqu'ils sont premiers à un entier q. Nous donnons ensuite des formules asymptotiques sur le nombre d'entiers y-ultrafriables inférieurs à un entier x et dans une progression arithmétique a modulo q, où q est un module y-friable, c'est-à-dire sans facteur premier supérieur à y. Nos résultats sont valables pour des entiers q, x, y tels que $\log x \ll y < x$, $q < y^{c/\log\log y}$, où $c > 0$ est une constante choisie convenablement.

Mots clés — diviseurs, progressions arithmétiques, crible, entiers ultrafriables

---

Institut Élie Cartan de Lorraine
Laboratoire de mathématiques — UMR 7503
54506 VANDOEUVRE-LES-NANCY