Conjecture d'Artin sur les racines primitives généralisées parmi les entiers avec peu de facteurs premiers

Paul Péringuey

Collegium sciences et technologies
Université de Lorraine
École doctorale IAEM
Commission de mathématiques

THÈSE

présentée pour l'obtention du grade de

Docteur de l'Université de Lorraine

Spécialité : Mathématiques pures

par

Paul Péringuey

Conjecture d'Artin sur les racines primitives généralisées parmi les entiers avec peu de facteurs premiers

Soutenue publiquement le 12 décembre 2022 devant le jury composé de

Régis de la Bretèche	*Examinateur*	Professeur, Université Paris Cité
Cécile Dartyge	*Directrice de thèse*	Maîtresse de conférences, Université de Lorraine
Chantal David	*Rapporteuse*	Professeure, Université Concordia, Montréal
Sary Drappeau	*Invité*	Maître de Conférences, Université d'Aix-Marseille
Youness Lamzouri	*Examinateur*	Professeur, Université de Lorraine
Bruno Martin	*Examinateur*	Professeur, Université du Littoral Côte d'Opale
Guillaume Ricotta	*Rapporteur*	Maître de Conférences, Université de Bordeaux
Anne de Roton	*Examinatrice*	Maîtresse de Conférences, Université de Lorraine
Thomas Stoll	*Président*	Professeur, Université de Lorraine

au vu des rapports de

Chantal David	Professeure, Université Concordia, Montréal
Guillaume Ricotta	Maître de Conférences, Université de Bordeaux

Institut Élie Cartan de Lorraine,
Laboratoire de mathématiques, UMR 7502,
54506 Vandœuvre-lès-Nancy

Remerciements

Je souhaite exprimer mon infinie gratitude envers ma directrice de thèse, Cécile Dartyge, auprès de qui j'ai tant appris. Ton enthousiasme et ta gentillesse ont permis la réalisation de ce projet dans les meilleures conditions, et j'espère un jour avoir de nouveau l'opportunité de collaborer avec toi.

Je tiens à remercier chaleureusement les rapporteurs de mon mémoire de thèse, Chantal David et Guillaume Ricotta, pour avoir accepté de donner leurs avis d'expert sur mon travail.

Je tiens également à remercier les examinateurs de mon jury, Régis de la Bretèche, Youness Lamzouri, Bruno Martin, Anne de Roton et Thomas Stoll, qui m'a fait l'honneur de présider mon jury, ainsi que Sary Drappeau pour avoir été jury invité. Je leur suis reconnaissant pour leurs nombreuses remarques et conseils.

J'aimerais exprimer toute ma reconnaissance et ma gratitude à l'ensemble des membres de l'Institut Élie Cartan. Les quatre années passées au sein de l'institut ont été des plus enrichissantes, notamment au travers des captivantes conversations que j'y ai eues, mathématiques ou non.

En particulier, je suis très reconnaissant à Anne de Roton, qui en acceptant de travailler avec moi en 2016, m'a mis sur la voie qui m'a mené à réaliser cette thèse et avec qui j'ai toujours le plaisir de travailler.

Je souhaite remercier l'ensemble des professeurs de mathématiques que j'ai rencontrés tout au long de mon parcours, et tout spécialement Catherine Jaulent, qui a su me communiquer son goût pour les belles mathématiques.

Enfin, mes plus profonds remerciements vont à mes amis et ma famille, en particulier mes parents et mon frère, pour leur indéfectible soutient.

Table des matières

Chapitre 0

Introduction

0.1 État de l'art

0.1.1 Racines primitives et conjecture d'Artin

Soit $n \geq 2$ un entier. Si n est égal à 2, 4, une puissance de nombre premier impair ou au double d'une puissance de nombre premier impair alors le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique. Dans ce cas les générateurs du groupe multiplicatif sont appelés des racines primitives modulo n.

Dans ses *Disquisitiones Arithmeticae* ([7], p 393) Gauss établit une méthode simple pour calculer l'expression en base 10 des fractions de la forme $\frac{m}{p^r}$ à partir de celle de $\frac{1}{p^r}$ où p^r est une puissance de nombre premier pour laquelle 10 est racine primitive. En effet, si $m \equiv 10^\nu \pmod{p^r}$, alors le développement de la partie fractionnaire de $\frac{m}{p^r}$ sera celui de $\frac{1}{p^r}$ décalé de ν chiffres vers la gauche. Dans ses tables, il fournit une liste des premiers entiers dont le groupe multiplicatif est cyclique pour lesquels 10 est racine primitive. Il s'agit de la première occurrence de la question de l'ensemble des entiers pour lesquels un nombre donné est une racine primitive.

En septembre 1927, Emil Artin [6] conjecture, dans ses correspondances avec Helmut Hasse, qu'un entier a différent de -1 et qui n'est pas un carré est une racine primitive pour une infinité de nombres premiers, plus précisément il conjecture que

$$\lim_{x\to\infty} \frac{\#\{p \leq x,\ a \text{ est une racine primitive modulo } p\}}{\#\{p \leq x\}},$$

existe et vaut $C_A := \prod_q \left(1 - \frac{1}{q(q-1)}\right) = 0.37395581\ldots$, la constante d'Artin, si a n'est pas une puissance parfaite. Si a est une h-ième puissance parfaite, un terme correctif doit être ajouté et la limite est alors $C_A \times \prod_{q|h} \left(\frac{q(q-2)}{q^2-q-1}\right)$.

L'heuristique dont découle cette conjecture est décrite dans la partie 1.2. Il est important de noter que dans cette première formulation de la conjecture d'Artin, la proportion de nombres premiers pour lesquels a est une racine primitive ne dépend que du fait que a soit une puissance parfaite ou non.

En 1957 Derrick et Emma Lehmer ont vérifié numériquement la conjecture d'Artin pour plusieurs valeurs de a, et ont envoyé des tables résumant leurs résultats à Artin. Dans ces résultats la proportion de nombres premiers pour lesquels a est une racine primitive ne correspondait pas à la conjecture d'Artin pour certaines valeurs de a, et plus particulièrement pour $a = 5$. S'en suivit alors une correspondance entre Artin et les Lehmer (dont une partie est reproduite dans [35]) au cours de laquelle Artin revient sur sa conjecture. Notons $a = a_1 a_2^2$, avec a_1 sans facteur carré. Alors si $a_1 \equiv 1 \pmod 4$, un autre terme correctif doit être ajouté, provenant du fait que dans ce cas $\mathbb{Q}(\sqrt{a})$ peut être une sous-extension d'une extension cyclotomique (voir proposition 2.14). La valeur de ce terme correctif est fournie dans le cas où a est un nombre premier congru à 1 modulo 4 par Hasse [11], puis une formule générale est décrite par Lang et Tate dans la préface de [6], cependant Hooley [14] attribue la bonne version du terme correctif à Heilbronn.

En 1967, Hooley [14] fournit une démonstration de la conjecture d'Artin reposant sur l'hypothèse de Riemann généralisée pour certains corps de nombre, qui lui permet d'utiliser une version forte du théorème de Chebotarev.

Theorème 0.1 (Hooley)**.** *Soit a un entier différent de -1 et qui n'est pas un carré. Posons h le plus grand entier tel que a soit une puissance h-ième et notons $a = a_1 a_2^2$ où a_1 est sans facteur carré.*

Notons $\mathcal{N}_a(x)$ le nombre de nombres premiers plus petits que x pour lesquels a est une racine primitive. En supposant l'hypothèse de Riemann généralisée pour les fonctions zêta de Dedekind associées aux extensions du type $\mathbb{Q}(\sqrt[k']{b}, \xi_k)$ où b est un entier strictement positif, ξ_k une racine primitive k-ième de l'unité, k sans facteur carré et $k'|k$ on a :

$$\mathcal{N}_a(x) = \prod_q \left(1 - \frac{1}{q(q-1)}\right) \prod_{q|h} \left(\frac{q(q-2)}{q^2-q-1}\right) C(a_1) \frac{x}{\log x} + \mathcal{O}\left(\frac{x \log\log x}{\log^2 x}\right),$$

où

$$C(a_1) := \begin{cases} 1 - \mu(|a_1|) \prod\limits_{\substack{q|h \\ q|a_1}} \left(\frac{1}{q-2}\right) \prod\limits_{\substack{q\nmid h \\ q|a_1}} \left(\frac{1}{q^2-q-1}\right) & \text{si } a_1 \equiv 1 \pmod 4, \\ 1 & \text{sinon.} \end{cases}$$

Aucune preuve inconditionnelle de la conjecture d'Artin n'est à ce jour connue, cependant des résultats partiels existent. En 1984 Gupta et Ram Murty [9] ont démontré qu'il existe une infinité d'entiers a qui sont des racines primitives pour une infinité de nombres premiers. Ils ont obtenu ce résultat en construisant à partir de n'importe quel triplet de nombres premiers un ensemble de 13 entiers, dont les seuls facteurs premiers sont dans le triplet, tel que au moins un élément de cet ensemble soit racine primitive pour au moins $\delta \frac{x}{(\log x)^2}$ nombre premiers plus petits que x, avec $\delta > 0$. Heath-Brown [12] a amélioré ce résultat en 1988 en montrant qu'il y a au plus deux nombres premiers qui ne sont des racines primitives que pour un nombre fini de nombres premiers. Plus précisément, il a démontré le théorème suivant :

Theorème 0.2 (Heath-Brown)**.** *Soient q, r, s trois entiers non-nuls qui sont multiplicativement indépendants. Soit $N(x)$ le nombre de nombres premiers plus petits que x pour lesquels au moins un entier parmi q, r et s est une racine primitive. Si aucun entier parmi $\{q, r, s, -3qr, -3qs, -3rs, qrs\}$ n'est un carré alors*

$$N(x) \gg \frac{x}{\log^2 x}.$$

Il est intéressant de noter qu'aucun de ces deux résultats ne fournit une démonstration constructive, ainsi bien qu'il existe une infinité d'entiers qui sont des racines primitives pour une infinité de nombres premiers, il n'a pas encore été montré qu'un entier en particulier est une racine primitive pour une infinité de nombres premiers.

0.1.2 Entiers avec un nombre fixé de facteurs premiers et entiers criblés

Soit ℓ un entier positif. Nous introduisons trois fonctions de comptage relatives à l'ensemble des entiers ayant exactement ℓ facteurs premiers. Dans la première (respectivement la deuxième) on compte les facteurs premiers avec (respectivement sans) multiplicité tandis que pour la troisième on ne considère que les entiers sans facteur carré. On définit ainsi :

$$\begin{aligned}\sigma(x,\ell) &:= \sum_{\substack{n\leq x\\ \Omega(n)=\ell}} 1,\\ \pi(x,\ell) &:= \sum_{\substack{n\leq x\\ \omega(n)=\ell}} 1,\\ \rho(x,\ell) &:= \sum_{\substack{n\leq x\\ \omega(n)=\ell}} \mu^2(n),\end{aligned}$$

où $\Omega(n)$ (respectivement $\omega(n)$) est le nombre de facteurs premiers de n comptés avec (respectivement sans) multiplicité et μ est la fonction de Möbius. En 1900, Landau [16] démontre par récurrence, et en utilisant le théorème des nombres premiers, une formule asymptotique pour ces fonctions de comptage. Pour ℓ fixé et x tendant vers l'infini :

$$\sigma(x,\ell) \sim \pi(x,\ell) \sim \rho(x,\ell) \sim \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}, \tag{1}$$

où le terme d'erreur est partout en $\mathcal{O}\left(\frac{x(\log\log x)^{\ell-2}}{\log x}\right)$. Pillai a démontré que (1) reste vrai pour $\ell = o(\log\log x)$.

En 1953 et 1954, Sathe publie une série d'articles ([29], [30], [31], [32]) où il établit des formules asymptotiques pour $\sigma(x,\ell)$, $\pi(x,\ell)$ et $\rho(x,\ell)$ en procédant par récurrence pour $\ell \sim B\log\log x$, avec $0 < B < 2$. En utilisant une méthode totalement différente, Selberg [33] simplifie grandement la preuve de Sathe, et fournit des formules asymptotiques pour $B \geq 2$. Cet article marque d'ailleurs les prémices de la méthode de Selberg-Delange ([37] ou [36] Chapitre II.5). Pour $(2+\varepsilon)\log\log x \leq \ell \leq \frac{\log x}{\log 2}$, Nicolas [28] démontre une formule asymptotique pour $\sigma(x,\ell)$. Quant à $\pi(x,\ell)$ et $\rho(x,\ell)$, les grandes valeurs de ℓ sont plus difficiles à aborder. Hildebrand et Tenenbaum [13] ont démontré une formule asymptotique de $\pi(x,\ell)$ pour $1 \ll \ell \ll \frac{\log x}{(\log\log x)^2}$ et Kerner [15] en fournit une évaluation asymptotique valable uniformément

pour x grand et pour ℓ dans un large domaine. Des résultats existent aussi pour les petits intervalles, notamment Goudout [8] étudie le comportement de $\pi(x+h,\ell)-\pi(x,\ell)$ pour presque tout x, $\frac{\ell}{\log\log x}$ non nul borné et h tendant vers l'infini.

Nous nous intéresserons aussi aux pendants criblés de ces fonctions sommatoires, c'est-à-dire, en notant $P^-(n)$ le plus petit facteur premier de n, aux fonctions

$$\sigma(x,y,\ell) := \sum_{\substack{n\leq x\\ P^-(n)>y\\ \Omega(n)=\ell}} 1,$$

$$\pi(x,y,\ell) := \sum_{\substack{n\leq x\\ P^-(n)>y\\ \omega(n)=\ell}} 1,$$

$$\rho(x,y,\ell) := \sum_{\substack{n\leq x\\ P^-(n)>y\\ \omega(n)=\ell}} \mu^2(n).$$

Posons $u := \frac{\log x}{\log y}$. En 1982 Alladi [1] donne des formules asymptotiques pour ces fonctions de comptage, qui sont effectives du moment que u tende vers l'infini. En 1990, Balazard [2] fournit une autre formule asymptotique pour $\pi(x,y,\ell)$, qui est plus précise pour les valeurs bornées de u (lemme 3.10), ce qui lui permet de démontrer l'unimodalité de $\pi(x,\ell)$ et $\rho(x,\ell)$.

0.1.3 Généralisations de la conjecture d'Artin

La conjecture d'Artin a donné lieu a de nombreuses généralisations. Dès 1937, Bilharz [3] démontre l'équivalent de la conjecture d'Artin pour les corps de fonctions en supposant l'hypothèse de Riemann pour les fonctions zêta associées à ces corps, hypothèse qui fut démontrée par Weil [39]. Lang et Trotter [18] ont proposé une généralisation pour les courbes elliptiques, démontrée en supposant l'hypothèse de Riemann Généralisée par Serre. De nombreuses généralisations peuvent être trouvées dans les différents articles de synthèse concernant la conjecture d'Artin, comme par exemple [25], [21] et [26].

La généralisation de la conjecture d'Artin qui nous intéressera dans cette thèse est celle formulée par Li [20]. Il ne peut y avoir de racine primitive modulo un entier n que si ce dernier est de la forme $n = 2,\ 4,\ p^r,\ 2p^r$, où p est un nombre premier impair. Cependant Carmichael [5] a étendu le concept de racine primitive modulo n'importe quel entier $n \geq 2$. On dit qu'un entier a est une racine primitive généralisée modulo n si l'ordre de a dans $(\mathbb{Z}/n\mathbb{Z})^*$ est maximal. Carmichael introduit alors la fonction λ telle que $\lambda(n)$ est l'exposant de $(\mathbb{Z}/n\mathbb{Z})^*$ (c'est-à-dire la taille maximale d'un sous-groupe cyclique), qui jouera un rôle similaire à celui de l'indicatrice d'Euler pour les racines primitives. On peut alors reformuler les problèmes sur les racines primitives en des problèmes similaires pour les racines primitives généralisées. Comme pour les racines primitives notons $\mathbf{N}_a(x)$ le nombre d'entiers plus petits que x pour lesquels a est une racine primitive généralisée. On pourrait alors s'attendre à ce que, pour des entiers a convenables, il existe une fonction $B(a)$ telle que $\mathbf{N}_a(x) \sim B(a)x$. Cependant ce n'est pas le cas, Li [20] montre, inconditionnellement, que pour tout entier a, $\liminf \frac{\mathbf{N}_a(x)}{x} = 0$. De plus, en notant $\mathcal{E}$ l'ensemble des entiers tels que $|a| = 1$ ou $|a|$ est une puissance non-triviale (c'est-à-dire qu'il existe $h \geq 2$ et $b \in \mathbb{N}$ tels que $a = b^h$) ou a est le double d'un carré, on a que pour tout $a \in \mathcal{E}$, $\mathbf{N}_a(x) = o(x)$. Quant à la limite supérieure, Li et Pomerance [22] obtiennent, en utilisant l'hypothèse de Riemann généralisée, que pour $a \notin \mathcal{E}$, $\limsup \frac{\mathbf{N}_a(x)}{x} > 0$, et ils conjecturent même que $\limsup \frac{\mathbf{N}_a(x)}{x} = \alpha \frac{\varphi(|a|)}{|a|}$, où φ est l'indicatrice d'Euler et $\alpha \simeq 0,326$ est indépendant de a. De plus, Li et Pomerance [23] ont montré une version de la conjecture d'Artin pour les racines primitives généralisées en moyenne, c'est-à-dire pour $y > \exp\left((2+\varepsilon)(\log x \log\log x)^{\frac{1}{2}}\right)$, $\frac{1}{y}\sum_{1\leq a\leq y} \mathbf{N}_a(x) \underset{x\to\infty}{\sim} \sum_{n\leq x} \frac{R(n)}{n}$, où $R(n)$ est le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre maximal (ce qui correspond à un résultat de Stephens [34] pour la conjecture d'Artin). D'autres problèmes ont déjà été considérés dans ce contexte, par exemple Martin [24] a étudié l'ordre de grandeur de la plus petite racine primitive généralisée modulo un entier.

Nous nous intéressons dans cette thèse à la proportion d'éléments de certains sous-ensembles des entiers pour lesquels un entier donné est une racine primitive généralisée. Plus précisément, les sous-ensembles considérés seront l'ensemble des entiers ℓ-presque premiers, c'est-à-dire les entiers ayant au plus ℓ facteurs premiers comptés avec multiplicité, et celui des entiers criblés.

0.2 Plan de thèse et présentation des résultats

Cette thèse comporte deux principales parties, la première traitant de la conjecture d'Artin généralisée parmi les entiers avec un nombre fixé de facteurs premiers et la seconde parmi les entiers criblés. Nous commençons par établir une caractérisation des racines primitives généralisées d'un entier en fonction de sa décomposition en facteurs premiers, qui est le point de départ des deux parties sus-mentionnées.

La première partie a pour objectif de démontrer les théorèmes 0.3, 0.4 et 0.5. La notation (GRH) indique que les résultats sont conditionnels à l'Hypothèse de Riemann Généralisée pour les fonctions zêta de Dedekind associées à certains corps de nombres.

Theorème 0.3 (GRH)**.** *Soient $\ell \geq 1$, $E = \{1, \dots, \ell\}$, a un entier qui n'est ni -1, ni un carré parfait et $\mathcal{N}_{a,\ell}(x)$ le nombre de ℓ-presque premiers plus petits que x pour lesquels a est une racine primitive généralisée. On a :*

$$\mathcal{N}_{a,\ell}(x) = \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x} C_\ell(a)\,(1+o(1))\,,$$

avec les notations suivantes :

1. $C_\ell(a) = \prod_p (1 - W_\ell(p))\,(1 + V_\ell(a_1))$,

2. $W_\ell(p) := \sum_{i=1}^{\ell} \binom{\ell}{i} \sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j p^{i+j} (h,p)^i}{p^{2i}(p-1)^j (p^{i+j}-1)}$, *est la contribution ne dépendant que de* $h := \{\max \nu \in \mathbb{N},\ \exists b \in \mathbb{Z},\ b^\nu = a\}$,

3. $V_\ell(a_1) := \mu(2\tilde{a_1}) \frac{H_2(\ell,a_1)}{1-W_\ell(2)} \prod_{\substack{p \\ p|a_1 \\ p\geq 3}} (1 - W_\ell(p))^{-1}$, *est la contribution spécifique dépendant de* a, *où* $\tilde{a_1} := \frac{a_1}{(2,a_1)}$, *et* a_1 *est la partie sans facteur carré de* a,

4. $$H_2(\ell, a_1) := \sum_{k=1}^{\ell} \binom{\ell}{k} 2^{-\ell-k} \delta_\ell(k) \mu(\tilde{a_1})^k \prod_{\substack{p|\tilde{a_1} \\ p\geq 3}} \left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell} \right) \sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j} = \tilde{a_1}} \prod_{\{i,j\}\in\mathcal{D}} G_{i,j}^k(a_{i,j})$$

   où

   $$\delta_\ell(k) = \sigma(a_1,k) + 2^{\ell-2k} \sum_{m=0}^{\ell-k} \binom{\ell-k}{m} 2^{-3m} \sum_{r=0}^{\ell-k-m} \binom{\ell-k-m}{r} \frac{(-1)^r 2^{-r}}{2^{k+m+r}-1},$$

avec $\sigma(a_1,k) := \begin{cases} 2^{-\ell+k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1 \equiv 1 \pmod 4, \\ (-1)^k 2^{-\ell+k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1 \equiv 3 \pmod 4, \\ (-1)^k 2^{-2\ell+k}5^{\ell-k} & \text{sinon.} \end{cases}$,
$\mathcal{D} = [0,k]\times[0,\ell-k]\backslash\{0,0\}$, *et pour* $(i,j)\in\mathcal{D}$, $G_{i,j}^k$ *est la fonction multiplicative définie pour les nombres premiers impairs par :*

$$G_{i,j}^k(p) = \binom{k}{i}\binom{\ell-k}{j}\left(\frac{(p-1)(h,p)}{p^2(p-2)}\right)^{i+j}(2-p)^i\left(1+R_p(k+j)\right),$$

avec $R_p(m) := \sum_{r=0}^{\ell-m}\binom{\ell-m}{r}\frac{(-1)^r(p-1)^{\ell-m-r}}{(p^{m+r}-1)(p-2)^{\ell-m}}$.

La complexité des termes impliqués dans les résultats ci-dessus provient, en grande partie, du fait qu'un entier peut être racine primitive généralisée modulo $p_1\cdots p_\ell$ sans pour autant être racine primitive modulo un des p_i. Nous montrons dans le premier chapitre que pour être racine primitive généralisée modulo $p_1\cdots p_\ell$ un entier doit vérifier des critères plus faibles que celui d'être racine primitive mais cela simultanément modulo chacun des p_i, et donc le résultat ne découle pas immédiatement du résultat de Hooley[14], dont on retrouve ci-dessus le terme principal en prenant $\ell = 1$. Cependant on peut facilement calculer numériquement des valeurs particulières des différents termes du théorème 0.3 (voir l'annexe A). On a par exemple, en rappelant que $C_\ell(a) = \lim_{x\to\infty}\mathcal{N}_{a,\ell}(x)/\frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}$:

ℓ	$\prod_p(1-W_\ell(p))$, $h=1$	$C_\ell(2)$	$C_\ell(3)$	$C_\ell(5)$	$C_\ell(10)$
1	$\simeq 0.3739$	$\simeq 0.3739$	$\simeq 0.3739$	$\simeq 0.3936$	$\simeq 0.3739$
2	$\simeq 0.3759$	$\simeq 0.3222$	$\simeq 0.3950$	$\simeq 0.3878$	$\simeq 0.3775$
5	$\simeq 0.3261$	$\simeq 0.1318$	$\simeq 0.3252$	$\simeq 0.3278$	$\simeq 0.3272$
10	$\simeq 0.3051$	$\simeq 0.0293$	$\simeq 0.3053$	$\simeq 0.3046$	$\simeq 0.3047$
20	$\simeq 0.2919$	$\simeq 0.0015$	$\simeq 0.2918$	$\simeq 0.2920$	$\simeq 0.2920$
50	$\simeq 0.2807$	$\simeq 2\times 10^{-7}$	$\simeq 0.2807$	$\simeq 0.2807$	$\simeq 0.2807$

Dans la preuve du théorème 0.3 on étudie un ensemble plus grand que celui des ℓ-presque premiers pour lesquels a est une racine primitive généralisée, l'hypothèse de Riemann généralisée n'est alors utilisée que pour majorer les éléments de cet ensemble pour lesquels a n'est pas une racine primitive généralisée (voir section 2.2). Ainsi inconditionnellement on a la majoration :

Theorème 0.4. *Avec les mêmes notations que pour le Théorème 0.3, on a :*

$$\mathcal{N}_{a,\ell}(x) \le \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}C_\ell(a)\left(1+o(1)\right).$$

De plus nous montrerons un cas particulier du théorème 0.3 pour $\ell = 2$ avec un meilleur terme d'erreur :

Theorème 0.5 (GRH)**.** *Avec les mêmes notations et hypothèses que pour le théorème 0.3,*

$$\mathcal{N}_{a,2}(x) = \frac{x \log\log x}{\log x} C_2(a) + \mathcal{O}\left(\frac{x \log\log x}{\log x \log\log\log x}\right),$$

avec dans ce cas :

$$\prod_p (1 - W_2(p)) = \prod_{p \nmid h} \left(1 - \frac{2p^3 - 2p^2 - p - 1}{p^5 - p^4 - p^3 + p^2}\right) \prod_{p|h} \left(1 - \frac{2p-3}{p^2 - 2p + 1}\right).$$

La seconde partie quant à elle concernera les pendants criblés des théorèmes 0.3 et 0.4 :

Theorème 0.6 (GRH)**.** *Soit $0 < \theta < \frac{1}{2}$, a un entier qui n'est ni -1 ni un carré. Soit $\mathcal{N}_a(x, x^\theta)$ le nombre d'entiers x^θ criblés plus petits que x pour lesquels a est une racine primitive généralisée, c'est à dire*

$$\mathcal{N}_a(x, x^\theta) := \#\{n \leq x,\ P^-(n) > x^\theta,\ a \text{ racine primitive généralisée } \pmod n\}.$$

Alors sous l'Hypothèse de Riemann Généralisée, et en reprenant les notations du théorème 0.3 :

$$\mathcal{N}_a(x, x^\theta) \sim \sum_{\ell=1}^{\lfloor \frac{1}{\theta} \rfloor} f_\ell\left(\frac{1}{\theta}\right) C_\ell(a) \frac{x}{\log x},$$

où les fonctions f_ℓ sont définies par récurrence telles que :

- $f_1(u) := 1$ *pour* $u \geq 1$,
- $f_{k+1}(u) := \int_k^{u-1} f_k(v) \frac{dv}{v}$ *pour* $u > k + 1$.

et $C_\ell(a) := \prod_p (1 - W_\ell(p))\,(1 + V_\ell(a_1))$

Les fonctions f_i utilisées ici sont les mêmes que celles définies par Balazard [2].

De la même manière que la preuve du théorème 0.3 donne la majoration inconditionnelle du théorème 0.4, on a une majoration inconditionnelle dans le cas des entiers criblés.

Theorème 0.7. *Avec les mêmes notations que pour le Théorème 0.6, on a :*

$$\mathcal{N}_a(x, x^\theta) \leq \left(\sum_{\ell=1}^{\lfloor \frac{1}{\theta} \rfloor} f_\ell\left(\frac{1}{\theta}\right) A_\ell(a) \frac{x}{\log x}\right)(1 + o(1)).$$

Le premier chapitre est consacré à la caractérisation des racines primitives généralisées. On y démontrera que le fait que a soit une racine primitive généralisée modulo un entier sans facteur carré m est équivalent au fait que a vérifie simultanément des conditions modulo chacun des facteurs premiers de m. On déduira de cette caractérisation que a est une racine primitive généralisée modulo m si m ne vérifie pas une certaine propriété pour tout nombre premier q.

Le second chapitre traite des racines primitives généralisées parmi les presque-premiers. Le but principal de ce chapitre est la preuve du théorème 0.3. En utilisant l'Hypothèse de Riemann Généralisée nous ramenons le problème à l'évaluation du nombre de ℓ-presque premiers ne vérifiant pas ces propriétés pour q petit. Puis nous montrons que les $p_1, \cdots, p_\ell$ ne vérifiant pas ces propriétés pour q petit sont tels que chaque p_i vérifie un certain ensemble de conditions. Par des résultats de théorie algébrique des nombre nous montrons que ces conditions sont équivalentes au fait que p_i se décompose comme produit d'idéaux premiers distincts dans un certain corps de nombres. En utilisant la méthode de Selberg-Delange nous évaluons le nombre de $p_1 \cdots p_\ell \leq x$ vérifiant ces propriétés simultanément. Enfin, après avoir contrôlé les termes d'erreur, nous utilisons des méthodes combinatoires pour obtenir l'expression du terme principal. De plus le chapitre se termine avec une preuve pour le cas $\ell = 2$ où l'on remplace l'utilisation de la méthode de Selberg-Delange par la méthode de l'hyperbole, ce qui permet un meilleur terme d'erreur. Cependant l'utilisation de la méthode de l'hyperbole n'est pas adaptée à de plus grandes valeurs de ℓ car les termes d'erreur sont alors bien plus difficiles à contrôler.

Enfin le dernier chapitre a pour objectif de démontrer les théorèmes 0.6 et 0.7. Une observation nous permettra de se ramener à chercher les entiers criblés avec un nombre fixé de facteurs premiers, ce qui permettra de réutiliser de nombreux résultats du chapitre 2, avec la notable différence qu'il n'est pas nécessaire d'utiliser entièrement la méthode de Selberg-Delange dans ce cas, car les fonctions zêta de Dedekind criblées sont très proches de la fonction zêta de Riemann criblée, ce qui simplifie énormément la preuve. De plus le calcul du terme principal se déduira de celui du terme principal du théorème 0.3.

0.3 Notations

Nous adoptons les notations standards :

Les lettres p et q désigneront toujours des nombres premiers.

(b, c) est le pgcd de b et c.

$[b, c]$ est le ppcm de b et c.

$b|c^\infty$ indique que tous les diviseurs premiers de b sont des diviseurs de c.

$\nu_p(b)$ est la valuation p-adique de b.

$\mathrm{ord}_c(b)$ est l'ordre de b dans $(\mathbb{Z}/c\mathbb{Z})^*$.

$P^+(b)$ est le plus grand facteur premier de b avec la convention $P^+(1) = 1$.

$P^-(b)$ est le plus petit facteur premier de b avec la convention $P^-(1) = \infty$.

$\omega(b)$ est le nombre de facteur premier de b comptés sans multiplicité.

$\Omega(b)$ est le nombre de facteur premier de b comptés avec multiplicité.

μ est la fonction de Möbius.

φ est l'indicatrice d'Euler.

λ est la fonction lambda de Carmichael. Pour $n \in \mathbb{N}$, $\lambda(n)$ est l'ordre maximal des éléments du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

Nous adoptons aussi les notations suivantes, particulières à cette thèse :

Pour $l \in \mathbb{N}$ et $n \in \mathbb{N}$ donnés, on notera $\mathfrak{R}(l, n)$ l'ensemble des entiers dont la classe $\pmod n$ est une puissance l-ième :

$$\mathfrak{R}(l, n) = \{c \in \mathbb{Z}, \exists b \in \mathbb{Z}, c \equiv b^l \pmod n\}. \tag{2}$$

La lettre a désignera un entier fixé, généralement différent de -1 et qui n'est

pas un carré. On écrira $a = a_1 a_2^2$, où a_1 est sans facteur carré et on définit h comme le plus grand entier tel que a soit une h-ième puissance :

$$h := \max\{\nu \in \mathbb{N},\ \exists b \in \mathbb{Z},\ b^\nu = a\}. \tag{3}$$

GRH désigne l'hypothèse de Riemann généralisée pour les fonctions zêta de Dedekind associées aux corps de la forme $\mathbb{Q}(\sqrt[k_1]{a}, \xi_k)$, où k est sans facteur carré et $k_1 | k$. Les lemmes, théorèmes, propositions, etc., avec un label GRH sont des résultats conditionnels à cette hypothèse de Riemann.

Chapitre 1

Caractérisation des racines primitives généralisées et approche heuristique

1.1 Caractérisation des racines primitives généralisées.

Nous donnons dans ce paragraphe un critère caractérisant les racines primitives généralisées. Ce critère est énoncé dans le lemme 1.3.
Nous commençons par introduire une notation qui nous servira tout au long du chapitre.
Pour $q, p_1, \ldots, p_\ell$ des nombres premiers, on notera $M_q(p_1, \ldots, p_\ell)$ l'ensemble des $p \in \{p_1, \ldots, p_\ell\}$ pour lesquels la valuation q-adique de $p-1$ est maximale parmi les $p_i - 1$:

$$M_q(p_1, \ldots, p_\ell) := \left\{ p \in \{p_1, \ldots, p_\ell\}, \nu_q(p-1) = \max_{1 \leq i \leq \ell} \nu_q(p_i - 1) \right\}. \quad (1.1)$$

On commence par donner un résultat classique sur les ordres des éléments dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Lemme 1.1. *Pour tous a, n_1, n_2 dans $\mathbb{N}$, $(a, n_1 n_2) = 1$:*

$$\mathrm{ord}_{[n_1,n_2]}(a) = [\mathrm{ord}_{n_1}(a), \mathrm{ord}_{n_2}(a)]$$

Démonstration. Commençons par montrer que $\mathrm{ord}_{n_1}(a) | \mathrm{ord}_{[n_1,n_2]}(a)$.
Écrivons $\mathrm{ord}_{[n_1,n_2]}(a) = k\mathrm{ord}_{n_1}(a) + r$ avec $k \in \mathbb{N}$ et $0 \leq r < \mathrm{ord}_{n_1}(a)$.

alors

$$\begin{aligned} a^{\mathrm{ord}_{[n_1,n_2]}(a)} \equiv 1(n_1) &\Leftrightarrow a^{k\mathrm{ord}_{n_1}(a)}a^r \equiv 1(n_1) \\ &\Leftrightarrow a^r \equiv 1(n_1) \end{aligned}$$

Or $r < \mathrm{ord}_{n_1}(a)$ ainsi $r = 0$. Ainsi $\mathrm{ord}_{n_1}(a)|\mathrm{ord}_{[n_1,n_2]}(a)$, de même $\mathrm{ord}_{n_2}(a)|\mathrm{ord}_{[n_1,n_2]}(a)$ et donc $[\mathrm{ord}_{n_1}(a), \mathrm{ord}_{n_2}(a)]|\mathrm{ord}_{[n_1,n_2]}(a)$.
Reste à montrer que $a^{[\mathrm{ord}_{n_1}(a),\mathrm{ord}_{n_2}(a)]} \equiv 1([n_1, n_2])$, ce qui est immédiat car $n_1|a^{[\mathrm{ord}_{n_1}(a),\mathrm{ord}_{n_2}(a)]}-1$ et $n_2|a^{[\mathrm{ord}_{n_1}(a),\mathrm{ord}_{n_2}(a)]}-1$ donc $[n_1, n_2]|a^{[\mathrm{ord}_{n_1}(a),\mathrm{ord}_{n_2}(a)]}-1$. □

Ainsi l'ordre d'un entier a modulo un entier n sans facteur carré va dépendre des ordres de a modulo chaque facteur premier de n. De plus, une rapide application du théorème chinois donne que l'ordre maximum atteint par un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ avec n sans facteur carré est le plus petit multiple commun des $p_i - 1$, où p_i est un facteur premier de n. Cette propriété se retrouve dans la fonction lambda de Carmichael [5].

Lemme 1.2. *La fonction lambda de Carmichael $\lambda : \mathbb{N} \to \mathbb{N}$ est telle que $\lambda(n)$ est le maximum des ordres des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$. De plus, λ vérifie les propriétés suivantes :*

1. $\lambda(p^r) = \begin{cases} \frac{1}{2}\varphi(p^r) & \text{si } p = 2 \text{ et } r \geq 3 \\ \varphi(p^r) & \text{sinon} \end{cases}$,

2. *Si $n = \prod_{i=1}^{k} p_i^{v_i}$ avec $p_i \neq p_j$, alors $\lambda(n) = [\lambda(p_1^{v_1}), \ldots, \lambda(p_k^{v_k})]$.*

On peut alors formuler une caractérisation des racines primitives généralisées modulo un entier sans facteur carré.

Lemme 1.3. *Soient $p_1, \ldots, p_\ell$, des nombres premiers distincts et a un entier tel que $(a, p_1 \cdots p_\ell) = 1$.*
a est une racine primitive généralisée modulo $p_1 \cdots p_\ell$ si et seulement si pour tout nombre premier q tel que $q|\lambda(p_1 \cdots p_\ell)$, il existe $p \in M_q(p_1, \ldots, p_\ell)$ tel que a ne soit pas le résidu d'une q-ième puissance modulo p.

Démonstration. Supposons qu'il existe $q|\lambda(p_1 \cdots p_\ell)$ premier tel que pour tout $p \in M_q(p_1, \ldots, p_\ell)$, a soit le résidu d'une q-ième puissance modulo p et donc $\mathrm{ord}_p(a)|\frac{p-1}{q}$, c'est-à-dire $\nu_q(\mathrm{ord}_p(a)) < \nu_q(p-1)$. De plus pour $p \notin M_q(p_1, \ldots, p_\ell)$ on a, par définition de $M_q(p_1, \ldots, p_\ell)$, que $\nu_q(\mathrm{ord}_p(a)) \leq \nu_q(p-1) < \max_{1 \leq i \leq \ell} \nu_q(p_i - 1)$.

Ainsi d'après le lemme 1.1,

$$\nu_q(\mathrm{ord}_{p_1\cdots p_\ell}(a)) = \max_{p\in\{p_1,\ldots,p_\ell\}} \nu_q(\mathrm{ord}_p(a)) < \max_{p\in\{p_1,\ldots,p_\ell\}} \nu_q(p-1) = \nu_q(\lambda(p_1\cdots p_\ell))$$

et donc a n'est pas une racine primitive généralisée modulo $p_1\cdots p_\ell$.

Réciproquement, supposons que a ne soit pas une racine primitive généralisée modulo $p_1\cdots p_\ell$. Alors il existe q premier tel que $q|\lambda(p_1\cdots p_\ell)$ et $a^{\frac{\lambda(p_1\cdots p_\ell)}{q}} \equiv 1(p_1\cdots p_\ell)$.
Soit $p \in M_q(p_1,\ldots,p_\ell)$, alors d'après le lemme 1.1, $\mathrm{ord}_p(a)|\frac{p-1}{q}$.
Soit γ une racine primitive modulo p, alors il existe α tel que $\gamma^\alpha \equiv a(p)$ et donc $\gamma^{\alpha\frac{p-1}{q}} \equiv 1 \pmod p$.
Alors $p-1|\alpha\frac{p-1}{q}$, i.e $q|\alpha$. Ainsi a est bien le résidu d'une q-ième puissance modulo p.

□

Nous allons maintenant définir un critère pour caractériser les entiers sans facteur carré pour lesquels a n'est pas une racine primitive généralisée.

Définition 1.4. *On dit que a vérifie $\mathcal{R}(q, p_1\cdots p_\ell)$ si $(a, p_1\cdots p_\ell) = 1$, $q|\lambda(p_1\cdots p_\ell)$ et a est le résidu d'une q-ième puissance modulo p pour tout $p \in M_q(p_1,\ldots,p_\ell)$.*

Ainsi a est racine primitive généralisée modulo $p_1\cdots p_\ell$ s'il ne vérifie pas $\mathcal{R}(q, p_1\cdots p_\ell)$ pour tout q. Pour $\ell = 1$ on retrouve la propriété $\mathcal{R}(q,p)$ introduite par Hooley [14, §3]. La section suivante étend une approche heuristique de la conjecture d'Artin à notre problème.

1.2 Approche heuristique expliquant le terme $W_\ell(p)$ des Théorèmes 0.3 et 0.6

Dans un premier temps nous rappelons l'approche heuristique de Heilbronn [21] pour la conjecture d'Artin, c'est-à-dire quand $\ell = 1$. Dans ce cas a est une racine primitive $\pmod p$ si et seulement si a ne vérifie pas $\mathcal{R}(q,p)$ pour tout q. Fixons q un nombre premier et examinons la probabilité qu'un nombre premier p soit tel que a ne vérifie pas $\mathcal{R}(q,p)$.

$$\mathbb{P}(\text{“}a \text{ ne vérifie pas } \mathcal{R}(q,p)\text{”}) = 1 - \mathbb{P}(p \equiv 1 \pmod q)\mathbb{P}(a \in \mathfrak{R}(q,p)).$$

Alors, d'après le Théorème de Dirichlet sur les nombres premiers en progression arithmétique on a $\mathbb{P}(p \equiv 1 \pmod q) = \frac{1}{q-1}$. Rappelons que h est l'entier défini par (3), c'est-à-dire le plus grand entier tel que a soit une h-ième puissance . Alors trivialement si $q|h$,

$$\mathbb{P}(\text{“}\exists b \text{ tel que } a \equiv b^q \pmod p\text{”}|\text{“}p \equiv 1 \pmod q\text{”}) = 1.$$

Si $q \nmid h$, alors

$$\begin{aligned}&\mathbb{P}(\text{“}\exists b \text{ tel que } a \equiv b^q \pmod p\text{”}|\text{“}p \equiv 1 \pmod q\text{”})\\ &= \mathbb{P}(\text{“}a^{\frac{p-1}{q}} \equiv 1 \pmod p\text{”}|\text{“}p \equiv 1 \pmod q\text{”}).\end{aligned}$$

D'après le petit théorème de Fermat, la classe de $a^{\frac{p-1}{q}}$ appartient à $\{\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*,\ \bar{x}^q = \bar{1}\}$. Or cet ensemble possède q éléments, on peut donc supposer que la probabilité que $a^{\frac{p-1}{q}} \equiv 1 \pmod p$ est $\frac{1}{q}$ (voir [25]).
Un argument plus rigoureux ([20] lemme 3.2) consiste à observer que $p \equiv 1 \pmod q$ et “a vérifie $\mathcal{R}(q,p)$” si et seulement si p est totalement décomposé dans le corps de Kummer $L := \mathbb{Q}\left(\xi_q, a^{\frac{1}{q}}\right)$, où ξ_q est une racine primitive q-ième de l'unité. Cela revient à dire que les éléments de Frobenius $\sigma_{\mathfrak{p}}$ pour $\mathfrak{p} \in \mathcal{O}_L$ au dessus de p, sont bien définis et sont dans la classe de conjugaison de l'identité dans $\mathrm{Gal}(L/\mathbb{Q})$ qui est réduite à un singleton.
D'après le théorème de Tchebotarev la proportion de tels p est $\frac{1}{[L:\mathbb{Q}]}$, qui vaut $\frac{1}{q(q-1)}$ sauf si a est un carré.
Ainsi $\mathbb{P}(\text{“}a \text{ ne vérifie pas } \mathcal{R}(q,p)\text{”}) = 1 - \frac{(h,q)}{q(q-1)}$. Alors en supposant l'indépendance selon les q des événements “a vérifie $\mathcal{R}(q,p)$” on obtient

$$\mathbb{P}(\text{“}a \text{ est racine primitive } \pmod p\text{”}) = \prod_q \left(1 - \frac{(h,q)}{q(q-1)}\right) =: C_a(h),$$

où $C_a(1)$ est la constante d'Artin. Cependant, cette hypothèse d'indépendance est bien trop forte, par exemple $\mathbb{Q}(\sqrt{5})$ est un sous-corps de $\mathbb{Q}(\xi_5, \sqrt[5]{5})$ (car $\sqrt{5} = -2(e^{4i\pi/5} + e^{-4i\pi/5}) - 1$), et donc la condition “5 vérifie $\mathcal{R}(5,p)$” implique “5 vérifie $\mathcal{R}(2,p)$”. Un terme correctif dépendant de a devra alors être ajouté pour tenir compte de ce genre d'éventualités (voir[35]).

Passons maintenant au problème pour les entiers sans facteur carré ayant exactement ℓ facteurs premiers, en utilisant l'heuristique “naïve”. Notons

$$W_\ell(q) := \mathbb{P}(\text{“}a \text{ vérifie } \mathcal{R}(q, p_1 \cdots p_\ell)\text{”}).$$

Découpons $W_\ell(q)$ suivant la valuation q-adique de $\lambda(p_1\cdots p_\ell)$, et suivant la taille de $M_q(p_1,\dots,p_\ell)$.

$$\begin{aligned} W_\ell(q) &= \sum_{m=1}^{\infty}\sum_{i=1}^{\ell}\mathbb{P}\left(\begin{array}{l} \text{“}a \text{ vérifie } \mathcal{R}(q,p_1\cdots p_\ell)\text{”} \\ \nu_q(\lambda(p_1\cdots p_\ell))=m \\ |M_q(p_1,\dots,p_\ell)|=i \end{array}\right) \\ &= \sum_{m=1}^{\infty}\sum_{i=1}^{\ell}\binom{\ell}{i}\mathbb{P}\left(\begin{array}{ll} \nu_q(p_j-1)<m & \forall i<j\le\ell \\ \nu_q(p_j-1)=m & \forall 1\le j\le i \\ \exists b \text{ tel que } a\equiv b^q \pmod{p_j} & \forall 1\le j\le i \end{array}\right). \end{aligned}$$

Les événements impliquant les p_j sont maintenant indépendants :

$$W_\ell(q)=\sum_{m=1}^{\infty}\sum_{i=1}^{\ell}\binom{\ell}{i}\mathbb{P}(\nu_q(p-1)<m)^{l-i}\mathbb{P}\left(\begin{array}{l}\nu_q(p-1)=m \\ \text{“}\exists b \text{ tel que } a\equiv b^q \pmod p\text{”}\end{array}\right)^i.$$

Alors d'après le Théorème de Dirichlet $\mathbb{P}(\nu_q(p-1)<m)=1-\frac{1}{\varphi(q^m)}$. Puis

$$\begin{aligned} \mathbb{P}(\nu_q(p-1)=m,\ a\in\mathfrak{R}(q,p)) &= \mathbb{P}(p\equiv 1 \pmod{q^m},\ a\in\mathfrak{R}(q,p)) \\ &\quad -\mathbb{P}(p\equiv 1 \pmod{q^{m+1}},\ a\in\mathfrak{R}(q,p)) \\ &= \frac{(h,q)}{q}\left(\frac{1}{\varphi(q^m)}-\frac{1}{\varphi(q^{m+1})}\right)=\frac{(h,q)(q-1)}{q^2\varphi(q^m)}. \end{aligned}$$

On reporte dans $W_\ell(q)$:

$$W_\ell(q)=\sum_{m=1}^{\infty}\sum_{i=1}^{\ell}\binom{\ell}{i}\left(1-\frac{1}{\varphi(q^m)}\right)^{\ell-i}\frac{(h,q)^i(q-1)^i}{q^{2i}\varphi(q^m)^i}.$$

On développe $\left(1-\frac{1}{\varphi(q^m)}\right)^{l-i}$ en utilisant la formule du binôme de Newton, puis on inverse les sommes finies et la somme infinie, on obtient alors,

$$W_\ell(q)=\sum_{i=1}^{\ell}\binom{\ell}{i}\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}\frac{(-1)^j q^{i+j}(h,p)^i}{q^{2i}(q-1)^j(q^{i+j}-1)}.$$

Alors, en supposant l'indépendance des $\mathcal{R}(q,p_1\cdots p_\ell)$, on a que

$$\mathbb{P}(a \text{ est racine primitive généralisée } \pmod{p_1\cdots p_\ell})=\prod_q(1-W_\ell(q)).$$

Cependant on verra par la suite qu'il n'y a pas indépendance, et donc qu'un coefficient correctif dépendant de a_1, h et ℓ devra être ajouté.

Chapitre 2

Racines primitives généralisées parmi les presque premiers

Nous cherchons à compter les nombres m ℓ-presque premiers pour lesquels un nombre a donné est racine primitive généralisée. Il est immédiat que si a est un carré ou $a = -1$ alors a ne peut être racine primitive généralisée que dans le groupe trivial $(\mathbb{Z}/2\mathbb{Z})^*$ ou dans $(\mathbb{Z}/3\mathbb{Z})^*$.
Nous allons montrer, sous l'hypothèse de Riemann généralisée, que quand a n'est pas un carré parfait et $a \neq -1$ cet ensemble est infini et admet une densité positive parmi tous les ℓ-presque premiers.
De plus on a trivialement :

$$\sum_{p_1 \cdots p_{\ell-1} \leq x} 1 \ll \frac{x}{\log x} (\log\log x)^{\ell-2} \quad \text{et} \quad \sum_{\substack{p_1 \cdots p_\ell \leq x \\ p_1 = p_2}} 1 \ll \frac{x}{\log x} (\log\log x)^{\ell-2}.$$

On a donc un analogue de la formule (1) (page 7) dans le cadre des racines primitives généralisées. On ne s'intéresse dans la suite qu'aux a qui ne sont pas des carrés et aux $m \leq x$ sans facteur carré ayant exactement ℓ facteurs premiers. Dit autrement, les théorèmes 0.3 et 0.4 restent valides si l'on considère l'ensemble des entiers ayant exactement ℓ facteurs premiers comptés avec ou sans multiplicité, ou sans facteur carré.

2.1 Le découpage de Hooley

Nous adaptons des notations similaires à celles du paragraphe 3 de [14] puis procédons à un découpage de la fonction de comptage des ℓ presque premiers pour lesquels a est une racine primitive généralisée.
On a vu dans la section 1.1 qu'un entier $p_1 \cdots p_\ell$ était compté dans $\mathcal{N}_{a,\ell}(x)$ s'il ne vérifie par $\mathcal{R}(q, p_1 \cdots p_\ell)$ pour tout q.

Pour $\eta,\ \eta_1,\ \eta_2 \in \mathbb{R}$, $\eta_1 < \eta_2$, et k un entier sans facteur carré on considère les cardinaux suivants :

$$\mathcal{N}_{a,\ell}(x,\eta) = \#\{p_1 \cdots p_\ell \leq x |\ a \text{ ne vérifie pas } \mathcal{R}(q, p_1 \dots p_\ell),\ \forall q \leq \eta\}, \quad (2.1)$$

$$\mathcal{P}_a(x,k) = \#\{p_1 \cdots p_\ell \leq x |\ a \text{ vérifie } \mathcal{R}(q, p_1 \dots p_\ell),\ \forall q | k\}. \quad (2.2)$$

Enfin nous introduisons, de manière analogue à Hooley [14], des fonctions $\mathcal{M}_a(x, \eta_1, \eta_2)$ qui comptent les ℓ presque premier qui passent le test $\mathcal{R}(q, p_1 \cdots p_\ell)$ pour un q dans un certain intervalle. Plus précisément, pour $\eta_1 < \eta_2$, $\mathcal{M}_a(x, \eta_1, \eta_2)$ est le nombre de $p_1 \cdots p_\ell \leq x$ pour lesquels a vérifie $\mathcal{R}(q, p_1 \dots p_\ell)$ pour au moins un q dans l'intervalle $]\eta_1, \eta_2]$.
On découpe $]0, x-1[$ en 4 parties suivant les bornes suivantes :

$$\begin{aligned} &\cdot\ C_1 \text{ une constante arbitrairement grande ;} \\ &\cdot\ C_2 = x^{\frac{1}{2}} \log^{-8} x ; \\ &\cdot\ C_3 = x^{\frac{1}{2}} \log x. \end{aligned} \quad (2.3)$$

Tout d'abord,

$$\mathcal{N}_{a,\ell}(x) \leq \mathcal{N}_{a,\ell}(x, C_1). \quad (2.4)$$

On minore $\mathcal{N}_{a,\ell}(x)$ à l'aide des quantités $\mathcal{M}_a(x, \eta_1, \eta_2)$,

$$\mathcal{N}_{a,\ell}(x) \geq \mathcal{N}_{a,\ell}(x, C_1) - \mathcal{M}_a(x, C_1, x-1).$$

On en déduit

$$\mathcal{N}_{a,\ell}(x) = \mathcal{N}_{a,\ell}(x, C_1) + \mathcal{O}(\mathcal{M}_a(x, C_1, x-1)).$$

On obtient alors l'équation fondamentale :

$$\mathcal{N}_{a,\ell}(x) = \mathcal{N}_{a,\ell}(x, C_1) + \mathcal{O}(\mathcal{M}_a(x, C_1, C_2)) + \mathcal{O}(\mathcal{M}_a(x, C_2, C_3)) + \mathcal{O}(\mathcal{M}_a(x, C_3, x-1)). \quad (2.5)$$

Dans la section suivante nous fournissons des majorations de $\mathcal{M}_a(x, C_2, C_3)$ et $\mathcal{M}_a(x, C_3, x-1)$. Le terme $\mathcal{M}_a(x, C_1, C_2)$ est ensuite majoré à l'aide de l'Hypothèse de Riemann Généralisée.

2.2 La contribution des $p_1 \cdots p_\ell$ tels que a vérifie $\mathcal{R}(q, p_1 \cdots p_\ell)$ pour q grand est négligeable

2.2.1 Majoration de $\mathcal{M}_a(x, C_2, C_3)$ et $\mathcal{M}_a(x, C_3, x-1)$

Proposition 2.1. *En reprenant les définitions de C_2 et C_3 de (2.3), on a :*

i)

$$\mathcal{M}_a(x, C_2, C_3) = \mathcal{O}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right)$$

ii)

$$\mathcal{M}_a(x, C_3, x-1) = \mathcal{O}\left(\frac{x}{\log^2 x}\right).$$

Démonstration. i) Nous majorons $\mathcal{M}_a(x, C_2, C_3)$ à l'aide des cardinaux $\mathcal{P}_a(x, k)$ définis par (2.2) :

$$\mathcal{M}_a(x, C_2, C_3) \leq \sum_{C_2 < q \leq C_3} \mathcal{P}_a(x, q).$$

En ne retenant que la condition $q|\lambda(p_1 \cdots p_\ell)$ dans $\mathcal{R}(q, p_1 \dots p_\ell)$, on obtient l'inégalité

$$\mathcal{P}_a(x, q) \leq \ell! \sum_{\substack{p_1 \cdots p_\ell \leq x \\ p_1 \equiv 1(q)}} 1.$$

Soit $\varepsilon > 0$, on découpe cette somme selon la taille de $p_2 \cdots p_\ell$,

$$\sum_{C_2 < q \leq C_3} \sum_{\substack{p_1 \cdots p_\ell \leq x \\ p_1 \equiv 1(q)}} 1 = S_1 + S_2 + S_3,$$

avec

$$S_1 = \sum_{C_2 < q \leq C_3} \sum_{p_2 \cdots p_\ell < \sqrt{x}^{1-\epsilon}} \sum_{\substack{p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ p_1 \equiv 1(q)}} 1,$$

$$S_2 = \sum_{C_2 < q \leq C_3} \sum_{\sqrt{x}^{1-\epsilon} \leq p_2 \cdots p_\ell \leq \sqrt{x}^{1+\epsilon}} \sum_{\substack{p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ p_1 \equiv 1(q)}} 1,$$

$$S_3 = \sum_{C_2 < q \leq C_3} \sum_{p_2 \cdots p_\ell \geq \sqrt{x}^{1+\epsilon}} \sum_{\substack{p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ p_1 \equiv 1(q)}} 1.$$

Dans S_1 la somme sur p_1 est longue, on utilise le Théorème de Brun–Titchmarsh ([37] ou [36], Théorème I.4.16), qui stipule que le nombre de nombres premiers plus petit que x appartenant à une même classe de congruence modulo c est $\leq \frac{2x}{\varphi(c)\log\left(\frac{x}{c}\right)}$.

$$\begin{aligned} S_1 &\ll \sum_{C_2<q\leq C_3} \sum_{p_2\cdots p_\ell<\sqrt{x}^{1-\epsilon}} \frac{2x}{p_2\cdots p_\ell q \log(\frac{x}{p_2\cdots p_\ell q})} \\ &\ll \frac{x}{\log^2 x}(\log\log x)^{\ell-1} \sum_{C_2<q\leq C_3} \frac{\log q}{q} \\ &\ll \frac{x(\log\log x)^\ell}{\log^2 x}. \end{aligned}$$

Pour S_2, on ne peut plus profiter de la congruence $p_1 \equiv 1 \pmod q$ car p_1 et q sont d'un ordre de grandeur proche :

$$\begin{aligned} S_2 &= \sum_{\sqrt{x}^{1-\epsilon}\leq p_2\cdots p_\ell\leq\sqrt{x}^{1+\epsilon}} \sum_{p_1\leq\frac{x}{p_2\cdots p_\ell}} \sum_{\substack{C_2<q\leq C_3 \\ q|p_1-1}} 1 \\ &\ll \sum_{\sqrt{x}^{1-\epsilon}\leq p_2\cdots p_\ell\leq\sqrt{x}^{1+\epsilon}} \sum_{p_1\leq\frac{x}{p_2\cdots p_\ell}} 1, \end{aligned}$$

puis en appliquant le Théorème des nombres premiers, on obtient :

$$S_2 \ll \sum_{\sqrt{x}^{1-\epsilon}\leq p_2\cdots p_\ell\leq\sqrt{x}^{1+\epsilon}} \frac{x}{p_2\cdots p_\ell \log(\frac{x}{p_2\cdots p_\ell})}.$$

Comme $p_2\cdots p_\ell \leq \sqrt{x}^{1+\varepsilon}$, $\log(\frac{x}{p_2\cdots p_\ell}) \gg \log x$:

$$S_2 \ll \frac{x}{\log x} \sum_{\sqrt{x}^{1-\epsilon}\leq p_2\cdots p_\ell\leq\sqrt{x}^{1+\epsilon}} \frac{1}{p_2\cdots p_\ell}.$$

Si $p_2\cdots p_\ell > \sqrt{x}^{1-\epsilon}$, alors $\max(p_2,\ldots,p_\ell) > \sqrt{x}^{\frac{1-\epsilon}{\ell-1}}$. Les rôles de $p_2,\ldots,p_\ell$ étant symétriques, on peut supposer que ce maximum est atteint par p_2 :

$$S_2 \ll \frac{x}{\log x} \sum_{p_3\cdots p_\ell\leq\sqrt{x}^{\ell+3\ell\varepsilon}} \frac{1}{p_3\cdots p_\ell} \sum_{\sqrt{x}^{\frac{1-\epsilon}{\ell-1}}<p_2\leq\sqrt{x}^{1+\varepsilon}} \frac{1}{p_2}.$$

La somme sur p_2 est un $\mathcal{O}(1)$ où la constante peut dépendre de ℓ. On en déduit que $S_2 \ll \frac{x}{\log x}(\log\log x)^{\ell-2}$. Et enfin, pour S_3, on a trivialement pour x assez grand,

$$S_3 = 0,$$

car pour x assez grand, comme $p_1 \leq \frac{x}{p_2\cdots p_\ell}$ et $\frac{x}{p_2\cdots p_\ell} < C_2$ et donc $\sum_{\substack{C_2<q\leq C_3\\ q|p_1-1}} 1 = 0$. Ainsi $\mathcal{M}_a(x, C_2, C_3) = \mathcal{O}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right)$.

ii) Montrons maintenant que $\mathcal{M}_a(x, C_3, x-1) = \mathcal{O}\left(\frac{x}{\log^2 x}\right)$. Nous procédons ici de la même façon que Hooley [14, p212]. Observons que, comme les rôles des p_i sont symétriques dans la condition $\mathcal{R}(q, p_1 \dots p_\ell)$ on peut supposer que $a^{\frac{p_1-1}{q}} \equiv 1(\pmod{p_1})$ et donc $a^{2\frac{p_1-1}{q}} \equiv 1 \pmod{p_1}$.
Comme $q > x^{\frac{1}{2}}\log x$, pour $p_2\cdots p_\ell \leq x$ fixés, les nombres p_1 tels que $p_1\cdots p_\ell$ soit compté dans $\mathcal{M}_a(x, C_3, x-1)$ doivent diviser le produit positif (éventuellement vide) :

$$\prod_{m<x^{\frac{1}{2}}\log^{-1}x\prod_{i=2}^{\ell}p_i^{-1}} (a^{2m}-1) \tag{2.6}$$

Posons $S_a(\eta_1, \eta_2) = \{p : \exists q \in]\eta_1, \eta_2] \text{ tel que } q|p-1,\ a \in \mathfrak{R}(q,p)\}$. Ainsi

$$\mathcal{M}_a(x, C_3, x-1) \leq 2\sum_{p_2\cdots p_\ell\leq x}\ \sum_{\substack{p_1\leq\frac{x}{p_2\cdots p_\ell}\\ p_1\in S_a(C_3,x-1)}} 1$$

Les éléments de $S_a(C_3, x-1)$ étant des nombres premiers, leur produit divise (2.6). En minorant dans (2.6) par 2 chaque $p \in S_a(C_3, x-1)$ on obtient :

$$2^{\#\{p_1\leq\frac{x}{p_2\cdots p_\ell}:\ p_1\in S_a(C_3,x-1)\}} < \prod_{m<x^{\frac{1}{2}}\log^{-1}x\prod_{i=2}^{\ell}p_i^{-1}} a^{2m}$$

Ainsi, en prenant le logarithme :

$$\#\Big\{p_1 \leq \frac{x}{p_2\cdots p_\ell} :\ p_1 \in S_a(C_3, x-1)\Big\} < \frac{2\log|a|}{\log 2}\sum_{m<x^{\frac{1}{2}}\log^{-1}x\prod_{i=2}^{\ell}p_i^{-1}} m$$
$$= \mathcal{O}\left(\frac{x}{\log^2 x\prod_{i=2}^{\ell}p_i^2}\right)$$

et donc $\mathcal{M}_a(x, C_3, x-1) \ll \sum_{p_2 \cdots p_\ell \leq x} \frac{x}{\log^2 x \prod_{i=2}^{\ell} p_i^2} \ll \frac{x}{\log^2 x}$.

□

2.2.2 Majoration de $\mathcal{M}_a(x, C_1, C_2)$ sous GRH.

Nous procédons à la majoration de $\mathcal{M}_a(x, C_1, C_2)$. Pour ce faire nous aurons besoin du résultat suivant de Hooley [14] conditionnel à l'hypothèse de Riemann généralisée pour certains corps de nombres.

Lemme 2.2 (Hooley, GRH)**.** *Soit q un nombre premier, on a alors*

$$\sum_{\substack{p \leq x \\ q | p-1 \\ a \in \mathfrak{R}(q,p)}} 1 = \frac{1}{q(q-1)} \operatorname{Li}(x) + \mathcal{O}\big(\sqrt{x} \log(qx)\big).$$

Hooley parvient à ce résultat en montrant que les nombres premiers que l'on comptent sont exactement ceux qui se décomposent complètement dans un certain corps de nombre K (ce dont nous établissons une généralisation avec les propositions 2.9, 2.11 et 2.12). L'étude de la fonction zêta de Dedekind associée à K, ainsi qu'une majoration du discriminant de K, fournissent une bonne estimation du nombre d'idéaux premiers de K de norme plus petite que x. Il reste alors à remarquer que les nombres premiers se décomposant complètement dans K se décomposent en un produit de $[K : \mathbb{Q}]$ idéaux premiers distincts de norme première, et donc que la quantité que l'on souhaite compter est, à peu près, le nombre d'idéaux premier de K de norme première plus petite que x divisé par $[K : \mathbb{Q}]$.
Nous sommes maintenant en mesure de fournir la majoration suivante pour $\mathcal{M}_a(x, C_1, C_2)$.

Proposition 2.3 (GRH)**.** *Sous l'hypothèse de Riemann généralisée, et avec C_1 et C_2 comme dans* (2.3)*, on a :*

$$\mathcal{M}_a(x, C_1, C_2) \ll \frac{x(\log\log x)^{\ell-1}}{C_1 \log x} + \frac{x(\log\log x)^{\ell-2}}{\log x} \log\log\log x.$$

Démonstration. Dans $\mathcal{M}_a$ la condition a vérifie $\mathcal{R}(q, p_1 \dots p_\ell)$ implique qu'il existe $p \in \{p_1, \dots, p_\ell\}$ tel que a vérifie $\mathcal{R}(q, p)$. Le rôle des p_i étant symétriques, on peut supposer que a vérifie $\mathcal{R}(q, p_1)$.
Écrivons

$$\begin{aligned} \mathcal{M}_a(x, C_1, C_2) &\leq \#\left\{p_1 \cdots p_\ell \leq x \ \exists q \in]C_1, C_2], \text{ tels que } a \text{ vérifie } \mathcal{R}(q, p_1)\right\} \\ &\leq S + \#\left\{p_1 \cdots p_\ell \leq x,\ p_1 \leq \log^{64} x\right\}, \end{aligned}$$

où S est le nombre de $p_1 \cdots p_\ell \le x$ tels que $p_2 \cdots p_\ell \le \frac{x}{\log^{64} x}$ et il existe $q \in]C_1, C_2]$ tel que a vérifie $\mathcal{R}(q, p_1)$.
La contribution de $p_1 \le (\log x)^{64}$ est négligeable :

$$\begin{aligned}\#\left\{p_1 \cdots p_\ell \le x,\ p_1 \le \log^{64} x\right\} &\ll \sum_{p_1 \le \log^{64} x} \frac{x}{p_1 \log x} (\log\log x)^{\ell-2} \\ &\ll \frac{x}{\log x} (\log\log x)^{\ell-2} \log\log\log x.\end{aligned}$$

Réécrivons maintenant S :

$$S \ll \sum_{C_1 < q \le C_2} \sum_{\substack{p_2 \cdots p_\ell \le \frac{x}{q} \\ p_2 \cdots p_\ell \le \frac{x}{\log^{64} x}}} \sum_{\substack{q \le p_1 \le \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1 \\ a \in \mathfrak{R}(q, p_1)}} 1.$$

On découpe la somme sur $p_2 \cdots p_\ell$ en trois parties suivant si $p_2 \cdots p_\ell$ est petit, grand ou de l'ordre de $\frac{x}{q^2}$. Nous procéderons alors dans les deux derniers cas comme pour les majorations de $\mathcal{M}_a(x, C_2, C_3)$ et $\mathcal{M}_a(x, C_3, x-1)$.

$$S_1 := \sum_{C_1 < q \le C_2} \sum_{\substack{p_2 \cdots p_\ell \le \frac{x}{q^2 \log^6 x} \\ p_2 \cdots p_\ell \le \frac{x}{\log^{64} x}}} \sum_{\substack{q \le p_1 \le \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1 \\ a \in \mathfrak{R}(q, p_1)}} 1,$$

$$S_2 := \sum_{C_1 < q \le C_2} \sum_{\substack{\frac{x}{q^2 \log^6 x} < p_2 \cdots p_\ell \le \frac{x}{q^2} \log^2 x \\ p_2 \cdots p_\ell \le \frac{x}{\log^{64} x}}} \sum_{\substack{q \le p_1 \le \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1}} 1,$$

$$S_3 := \sum_{C_1 < q \le C_2} \sum_{\substack{p_2 \cdots p_\ell \le \frac{x}{q} \\ \frac{x}{q^2} \log^2 x < p_2 \cdots p_\ell \le \frac{x}{\log^{64} x}}} \sum_{\substack{q \le p_1 \le \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1 \\ a \in \mathcal{R}(q, p_1)}} 1,$$

et on a donc $S \ll S_1 + S_2 + S_3$.
Pour majorer S_1 on utilise le lemme 2.2 dû à Hooley.

$$S_1 \ll \sum_{C_1 < q \le C_2} \sum_{\substack{p_2 \cdots p_\ell \le \frac{x}{q^2 \log^6 x} \\ p_2 \cdots p_\ell \le \frac{x}{\log^{64} x}}} \left(\mathrm{Li}\left(\frac{x}{p_2 \cdots p_\ell}\right) \frac{1}{q(q-1)} + \sqrt{\frac{x}{p_2 \cdots p_\ell}} \log x \right)$$

Nous allons utiliser le Théorème de Landau sur le nombre de presque premiers [16], qui stipule que $\sum_{\substack{n\leq x\\ \omega(n)=\alpha\\ |\mu(n)|=1}} 1 \sim \frac{x(\log\log x)^{\alpha-1}}{\alpha!\log x}$. Alors par sommation d'Abel, on vérifie que le terme de reste est assez petit :

$$\sum_{C_1<q\leq C_2}\sum_{\substack{p_2\cdots p_\ell\leq \frac{x}{q^2\log^6 x}\\ p_2\cdots p_\ell\leq \frac{x}{\log^{64} x}}}\sqrt{\frac{x}{p_2\cdots p_\ell}}\log x \ll \sum_{C_1<q\leq C_2}\frac{x}{q\log^2 x}\ll \frac{x}{\log^2 x}\log\log x.$$

Puis pour le terme principal, on ne peut que majorer trivialement les contributions de $p_1,\dots,p_\ell$:

$$\sum_{\substack{p_2\cdots p_\ell\leq \frac{x}{q^2\log^6 x}\\ p_2\cdots p_\ell\leq \frac{x}{\log^{64} x}}}\mathrm{Li}\left(\frac{x}{p_2\cdots p_\ell}\right)\ll \sum_{p_1\cdots p_\ell\leq x}1\ll \frac{x}{\log x}(\log\log x)^{\ell-1}.$$

Comme la somme sur q est un reste de série convergente on peut majorer S_1 :

$$S_1\ll \sum_{C_1<q\leq C_2}\frac{x(\log\log x)^{\ell-1}}{q^2\log x}+\frac{x}{\log^2 x}\log\log x\ll \frac{x(\log\log x)^{\ell-1}}{C_1\log x}+\frac{x}{\log^2 x}\log\log x.$$

Passons à la majoration de S_2.
Notons $E(x,n):=\left\{q,\ \sqrt{\frac{x}{n\log^6 x}}<q\leq\sqrt{\frac{x}{n}\log^2 x}\right\}$, en appliquant le Théorème de Brun-Titchmarsh on obtient :

$$\begin{aligned}S_2&\ll \sum_{p_2\cdots p_\ell\leq\frac{x}{\log^{64} x}}\ \sum_{q\in E(x,p_2\cdots p_\ell)}\ \sum_{\substack{q<p_1\leq\frac{x}{p_2\cdots p_\ell}\\ q|p_1-1}}1\\ &\ll \sum_{p_2\cdots p_\ell\leq\frac{x}{\log^{64} x}}\ \sum_{q\in E(x,p_2\cdots p_\ell)}\frac{x}{qp_2\cdots p_\ell\log\left(\frac{x}{qp_2\cdots p_\ell}\right)}.\end{aligned}$$

On a $\sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-1}x\leq\frac{x}{qp_2\cdots p_\ell}\leq\sqrt{\frac{x}{p_2\cdots p_\ell}}\log^3 x$ et donc $\log\left(\frac{x}{qp_2\cdots p_\ell}\right)\sim\frac{1}{2}\log\left(\frac{x}{p_2\cdots p_\ell}\right)$.

Alors en appliquant le Théorème de Mertens et des manipulations standard sur les logarithmes,

$$\begin{aligned}\sum_{q\in E(x,p_2\cdots p_\ell)}\frac{1}{q} &\leq \log\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\log x\right)-\log\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-3}x\right)\\ &\quad+\mathcal{O}\left(\log^{-1}\left(\frac{x}{p_2\cdots p_\ell}\right)\right)\\ &\leq 4\frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}+\mathcal{O}\left(\left(\frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}\right)^2\right),\\ &\ll \frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}.\end{aligned}$$

Ainsi,

$$S_2 \ll x\log\log x\sum_{p_2\cdots p_\ell\leq\frac{x}{\log^{64}x}}\frac{1}{p_2\cdots p_\ell\log^2\left(\frac{x}{p_2\cdots p_\ell}\right)}.$$

On évalue alors cette somme par sommation d'Abel et en utilisant le théorème de Landau sur les presque premiers :

$$\begin{aligned}\sum_{p_2\cdots p_\ell\leq\frac{x}{\log^{64}x}}\frac{1}{p_2\cdots p_\ell\log^2\left(\frac{x}{p_2\cdots p_\ell}\right)} &\ll \int_{\ell!}^{\frac{x}{\log^{64}x}}\frac{(\log\log t)^{\ell-2}}{t\log t\log^2\frac{x}{t}}dt\\ &\ll (\log\log x)^{\ell-2}\int_{\ell!}^{\frac{x}{\log^{64}x}}\frac{1}{t\log t\log^2\frac{x}{t}}dt.\end{aligned}$$

On utilise le changement de variable $u=\log t$ et on effectue une décomposition en éléments simples, on obtient :

$$S_2 \ll \frac{x}{\log x}(\log\log x)^{\ell-2}.$$

Passons à la majoration de S_3. On va procéder comme dans le *ii*) de la proposition 2.1

$$S_3 := \sum_{C_1<q\le C_2} \sum_{\substack{p_2\cdots p_\ell \le \frac{x}{q} \\ \frac{x}{q^2}\log^2 x < p_2\cdots p_\ell \le \frac{x}{\log^{64} x}}} \sum_{\substack{q\le p_1\le \frac{x}{p_2\cdots p_\ell} \\ q\mid p_1-1 \\ a\in\mathcal{R}(q,p_1)}} 1.$$

Comme $a^{\frac{p_1-1}{q}} \equiv 1(p_1), a^{2\frac{p_1-1}{q}} \equiv 1(p_1)$. De plus $\frac{p_1-1}{q} \le \frac{x}{qp_2\cdots p_\ell} \le \sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-1} x$. Ainsi il existe $m \le \sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-1} x$ tel que $p_1 | a^m - 1$. On minore chaque p_i par C_1 (au lieu de 2 contrairement à la preuve de la proposition 2.1)

$$C_1^{\#\{C_1\le p_1\le \frac{x}{p_2\cdots p_\ell}:\ \exists q\ge \sqrt{\frac{x}{p_2}}\log x,\ a\equiv b^q \pmod{p_1}\}} \le \prod_{m\le \sqrt{\frac{x}{p_2\cdots p_\ell}}\frac{1}{\log x}} a^{2m},$$

et donc en prenant de nouveau les logarithmes

$$\begin{aligned}\#\{C_1 \le p_1 \le \frac{x}{p_2\cdots p_\ell} :\ \exists q \ge \sqrt{\frac{x}{p_2\cdots p_\ell}}\log x,\ a\equiv b^q \pmod{p_1}\} &\le \frac{2\log a}{\log C_1} \sum_{m\le \sqrt{\frac{x}{p_2\cdots p_\ell}}\frac{1}{\log x}} m \\ &\ll \frac{x}{p_2\cdots p_\ell \log C_1 \log^2 x}\end{aligned}$$

On reporte dans S_3

$$\begin{aligned}S_3 &\ll \sum_{p_2\cdots p_\ell \le x} \frac{x}{p_2\cdots p_\ell \log C_1 \log^2 x} \\ &\ll \frac{x(\log\log x)^{\ell-1}}{\log C_1 \log^2 x}.\end{aligned}$$

Ainsi

$$\mathcal{M}_a(x, C_1, C_2) \ll \frac{x(\log\log x)^{\ell-1}}{C_1 \log x} + \frac{x(\log\log x)^{\ell-2}}{\log x}\log\log\log x.$$

□

2.2.3 Nouvelle équation fondamentale

Maintenant en reprenant (2.5) et la proposition précédente, on obtient la proposition suivante :

Proposition 2.4 (GRH)**.**

$$\mathcal{N}_{a,\ell}(x) = \mathcal{N}_{a,\ell}(x, C_1) + \mathcal{O}\left(\frac{x(\log\log x)^{\ell-1}}{C_1 \log x} + \frac{x(\log\log x)^{\ell-2}}{\log x}\log\log\log x\right).$$

Exprimons alors $\mathcal{N}_{a,\ell}(x, C_1)$ en termes de $\mathcal{P}_a(x, k)$. Déjà, par inclusion-exclusion, on a en notant $\mathbb{1}\big(\mathcal{R}(q, p_1 \cdots p_\ell)\big)$ la fonction valant 1 si a vérifie $\mathcal{R}(q, p_1 \cdots p_\ell)$:

$$\begin{aligned}\mathcal{N}_{a,\ell}(x, C_1) &= \sum_{p \le x} \prod_{q \le C_1} \big(1 - \mathbb{1}\big(\mathcal{R}(q, p_1 \cdots p_\ell)\big)\big) \\ &= \sum_{p \le x} \sum_{\substack{l' \\ P^+(l') \le C_1}} \mu(l') \prod_{q \mid l'} \mathbb{1}\big(\mathcal{R}(q, p_1 \cdots p_\ell)\big) \\ &= \sum_{P^+(l') \le C_1} \mu(l') \mathcal{P}_a(x, l').\end{aligned}$$

La section suivante a pour objectif de séparer le plus possible les conditions sur les p_i dans $\mathcal{P}_a(x, k)$.

2.3 Expression de $\mathcal{P}_a(x, k)$

Commençons par démontrer le lemme suivant :

Lemme 2.5. *Soient u et v deux entiers premiers entre eux, a un entier et p un nombre premier, alors a appartient à la fois à $\mathfrak{R}(u, p)$ et à $\mathfrak{R}(v, p)$ si et seulement si a appartient à $\mathfrak{R}(uv, p)$.*

Démonstration. Il est clair que si $a \in \mathfrak{R}(uv, p)$ alors $a \in \mathfrak{R}(u, p) \cap \mathfrak{R}(v, p)$.
Supposons alors $a \in \mathfrak{R}(u, p) \cap \mathfrak{R}(v, p)$. Soient ν_1 et ν_2 tels que $\nu_1^u \equiv a \pmod{p_i}$ et $\nu_2^v \equiv a \pmod{p_i}$.
Puis, comme $(u, v) = 1$, il existe d'après le Théorème de Bézout λ_1 et λ_2 tels que $\lambda_1 u + \lambda_2 v = 1$.
Alors on a

$$(\nu_1^{\lambda_2} \nu_2^{\lambda_1})^{uv} \equiv (\nu_1^u)^{\lambda_2 v} (\nu_2^v)^{\lambda_1 u} \equiv a^{\lambda_1 u + \lambda_2 v} \equiv a \pmod{p}.$$

□

Rappelons la notation $E = \{1, \ldots, \ell\}$, et soit $\mathcal{P}^*(E)$ l'ensemble des parties non vides de E.
On déduit du lemme précédent et des définitions de $\mathcal{P}_a(x, k)$ et h données par (2.2) et (3) les conditions suivantes pour les nombres $p_1 \cdots p_\ell$ contribuant à $\mathcal{P}_a(x, k)$.

Proposition 2.6. *Soit $(p_1 \dots, p_\ell)$ un ℓ-uplet de nombres premiers distincts tel que $p_1 \cdots p_\ell \leq x$. Alors $p_1 \cdots p_\ell$ est compté dans $\mathcal{P}_a(x,k)$ si et seulement si les conditions suivantes sont vérifiées :*

- $(a, p_1 \cdots p_\ell) = 1$,
- *Il existe une unique factorisation de k sous la forme $k = \prod_{L \in \mathcal{P}^*(E)} k_L$ telle que, en notant $k'_L := \frac{k_L}{(h,k_L)}$ pour tout $L \in \mathcal{P}^*(E)$:*
  - $\forall i \in E,\ a \in \mathfrak{R}\left(\prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} k'_L, p_i\right)$ *et* $p_i \equiv 1 \pmod{\prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} k_L}$;
  - $\forall j \in E,\ \forall L \subset E \backslash \{j\}$, *tels que* $\forall q | k_L,\ \nu_q(p_j - 1) < \nu_q(\lambda(p_1 \cdots p_\ell))$.

Démonstration. Tous les $p_1 \cdots p_\ell$ comptés dans $\mathcal{P}_a(x,k)$ vérifient les conditions suivantes :

i) $(a, p_1 \cdots p_\ell) = 1$,

ii) $k | \lambda(p_1 \cdots p_\ell))$,

iii) $\forall q | k,\ \forall p_i \in M_q(p_1, \dots, p_\ell),\ a \in \mathfrak{R}(q, p_i)$.

Définissons pour tout diviseur premier q de k l'ensemble des indices des éléments de l'ensemble M_q associé : $I_q := \{i \in E,\ p_i \in M_q(p_1, \dots, p_\ell)\}$.
A chaque $L \subset E$ non vide, on peut associer un diviseur k_L de k défini par $k_L := \prod_{\substack{q|k \\ L = I_q}} q$ et ainsi $\prod_{L \in \mathcal{P}^*(E)} k_L$, les k_L pouvant valoir 1.
La condition $k | \lambda(p_1 \cdots p_\ell)$ peut s'écrire sous la forme $\forall q | k,\ \max_{1 \leq i \leq \ell} \nu_q(p_i - 1) > 0$, ce qui revient à $p_i \equiv 1 \pmod{\prod_{i \in L} k_L}$.
La condition iii) est quant à elle équivalente au fait que pour tout $i \in E$, $a \in \mathfrak{R}(q, p_i)$ pour tout q tel que $p_i \in M_q(p_1, \dots, p_\ell)$. En appliquant plusieurs fois le lemme 2.5, cette condition sur p_i est équivalente à

$$a \in \mathfrak{R}\left(\prod_{\substack{q|k \\ i \in I_q}} q, p_i\right) = \mathfrak{R}\left(\prod_{i \in L} k_L, p_i\right).$$

On note $k_L = k'_L(k_L, h)$. Comme k est sans facteur carré, $\left(k'_L, (k_L, h)\right) = 1$. D'après le lemme 2.5, $a \in \mathfrak{R}(k_L, p_i)$ si et seulement si $a \in \mathfrak{R}(k'_L, p_i)$ et $a \in \mathfrak{R}((k_L, h), p_i)$.

Or par définition de h, on a toujours $a \in \mathfrak{R}((k_L, h), p_i)$, et donc $a \in \mathfrak{R}(k_L, p_i) \Leftrightarrow a \in \mathfrak{R}(k'_L, p_i)$.
Appliquons à nouveau le lemme 2.5

$$a \in \mathfrak{R}\left(\prod_{i\in L} k_L, p_i\right) \Leftrightarrow a \in \bigcap_{i\in L} \mathfrak{R}(k_L, p_i) \Leftrightarrow a \in \bigcap_{i\in L} \mathfrak{R}(k'_L, p_i) \Leftrightarrow a \in \mathfrak{R}\left(\prod_{i\in L} k'_L, p_i\right).$$

Ainsi notre factorisation de k convient. Soit $\prod \tilde{k}_L$ une décomposition de k qui convient, alors pour tout $q|\tilde{k}_L$, $M_q(p_1, \ldots, p_\ell) = L$ et donc $\tilde{k}_L = k_L$.

□

Grâce à la proposition 2.6, on peut exprimer $\mathcal{P}_a(x, k)$ comme suit :

$$\mathcal{P}_a(x,k) = \sum_{\substack{\prod_{L\in\mathcal{P}^*(E)} k_L = k \\ \forall i,\ a\in\mathfrak{R}\left(\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} k'_L, p_i\right)}} \sum_{\substack{p_1\cdots p_\ell \le x \\ (a, p_1\cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 \pmod{\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} k_L}}} 1, \tag{2.7}$$

où les k_L et k'_L dépendent des p_i comme explicité précédemment. Dans la proposition suivante nous obtenons un découpage de $\mathcal{P}_a(x, k)$ dans lequel les conditions sur les $p_1, \ldots, p_\ell$ sont indépendantes (mis à part la contrainte $p_1 \cdots p_\ell \le x$).

Proposition 2.7. *On a :*

$$\mathcal{P}_a(x,k) = \frac{1}{\ell!} \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\} \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\} \\ c_{iL} | \frac{g_L}{k_L}}} \sum_{\substack{\{p_i,\ i\in\{1,\ldots,\ell\}\} \\ p_1\cdots p_\ell \le x \\ (a, p_1\cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 \pmod{u_i} \\ \forall i,\ (\frac{p_i-1}{u_i}, k)=1 \\ \forall i,\ a\in\mathfrak{R}\left(k'_i, p_i\right)}} 1,$$

où pour tout $i \in \{1, \ldots, \ell\}$, $u_i := \prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} g_L \prod_{\substack{L\in\mathcal{P}^*(E)\\ i\notin L}} c_{iL}$ *et* $k'_i := \prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} k'_L$.

Démonstration. À k et $p_1, \ldots, p_\ell$ fixés, notons pour $L \in \mathcal{P}^*(E)$ et $i \in L$, $g_L := \prod_{q|k_L} q^{\nu_q(p_i-1)} = (k_L^\infty, p_i - 1)$ et pour $i \notin L$ notons $c_{iL} := (k_L^\infty, p_i - 1)$.

Notons que la définition de g_L ne dépend pas du $i \in L$ choisi et que $c_{iL} | \frac{g_L}{k_L}$. Puis posons pour tout $i \in E$, $k_i := \prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} k_L$ et $k'_i := \prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} k'_L$.
On va sommer sur toutes les décompositions de k en $\prod_{L \in \mathcal{P}^*(E)} k_L$ et les g_L et c_{iL} possibles. C'est-à-dire sommer sur ces décompositions de k et sur les $g_L | k_L^\infty$, $k_L | g_L$ et $c_{iL} | \frac{g_L}{k_L}$.
Ainsi à k, $\{k_L,\ L \in \mathcal{P}^*(E)\}$ tels que $\prod_{L \in \mathcal{P}^*(E)} k_L = k$, $\{g_L,\ L \in \mathcal{P}^*(E)\}$ et $\{c_{iL},\ L \in \mathcal{P}^*(E),\ i \notin L\}$ fixés, les $p_1 \cdots p_\ell$ qui contribuent à $\mathcal{P}_a(x,k)$ pour lesquels les k_L, g_L et c_{iL} correspondent sont tels que :

1. $(a, p_1 \cdots p_\ell) = 1$;
2. pour tout i, $p_i \equiv 1(k_i)$;
3. pour tout i, $a \in \mathfrak{R}(k'_i, p_i)$;
4. pour tous $L \in \mathcal{P}^*(E)$ et $i \in L$, $g_L | (p_i - 1)$ et $(\frac{p_i - 1}{g_L}, k_L) = 1$;
5. pour tous $L \in \mathcal{P}^*(E)$ et $i \notin L$, $c_{iL} | (p_i - 1)$ et $(\frac{p_i - 1}{c_{iL}}, k_L) = 1$.

Comme pour tout L, $k_L | g_L$ la condition $\forall L \in \mathcal{P}^*(E)$, $i \in L$, $g_L | (p_i - 1)$ et $(\frac{p_i - 1}{g_L}, k_L) = 1$ implique $p_i \equiv 1(k_i)$. Puis, comme k est sans facteur carré, les conditions :

1. pour tout $L \in \mathcal{P}^*(E)$, $i \in L$, $g_L | p_i - 1$ et $(\frac{p_i - 1}{g_L}, k_L) = 1$;
2. pour tout $L \in \mathcal{P}^*(E)$, $i \notin L$, $c_{iL} | p_i - 1$ et $(\frac{p_i - 1}{c_{iL}}, k_L) = 1$;

sont ensembles équivalentes au fait que pour tout $i \in \{1, \ldots, \ell\}$,

$$\Big(\prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} g_L \prod_{\substack{L \in \mathcal{P}^*(E) \\ i \notin L}} c_{iL} \Big) \Big| (p_i - 1) \text{ et } \left(\frac{p_i - 1}{\prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} g_L \prod_{\substack{L \in \mathcal{P}^*(E) \\ i \notin L}} c_{iL}}, k \right) = 1.$$

Notons alors pour tout i, $u_i := \prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} g_L \prod_{\substack{L \in \mathcal{P}^*(E) \\ i \notin L}} c_{iL}$ et disons, pour raccourcir les notations, que la condition $p_i \equiv 1 \pmod{u_i}$ est impliquée par $(\frac{p_i - 1}{u_i}, k) = 1$.

Les $p_1 \cdots p_\ell$ qui contribuent à $\mathcal{P}_a(x,k)$ pour lesquels les k_L, g_L et c_{iL} correspondent sont alors tels que :

1. $(a, p_1 \cdots p_\ell) = 1$;
2. pour tout i, $a \in \mathfrak{R}(k_i', p_i)$;
3. pour tout $i \in \{1, \ldots, \ell\}$, $(\frac{p_i - 1}{u_i}, k) = 1$.

On peut alors écrire $\mathcal{P}_a(x,k)$ comme suit :

$$\mathcal{P}_a(x,k) = \frac{1}{\ell!} \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\} \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\} \\ c_{iL} | \frac{g_L}{k_L}}} \sum_{\substack{\{p_i,\ i\in\{1,\ldots,\ell\}\} \\ p_1\cdots p_\ell \le x \\ (a, p_1\cdots p_\ell)=1 \\ \forall i,\ (\frac{p_i-1}{u_i},k)=1 \\ \forall i,\ a\in\mathfrak{R}\left(k_i', p_i\right)}} 1.$$

Le facteur $\frac{1}{\ell!}$ provenant du fait que un même nombre $p_1 \cdots p_\ell$ est compté $\ell!$ fois suivant l'ordre des facteurs premiers et comme $p_i \neq p_j$ pour $i \neq j$.

□

Afin de pouvoir calculer la dernière somme de $\mathcal{P}_a(x,k)$ nous aurons besoin de contrôler la taille des g_L, ce que nous faisons dans la proposition suivante.

Proposition 2.8. *Pour $k \le C_1$, C_5 une constante arbitrairement grande, $0 < t < 1$, on a :*

$$\mathcal{P}_a(x,k) = \mathcal{P}_a{}'(x,k) + \mathcal{O}\left(\frac{C_1 x}{C_5^t \log x} (\log\log x)^{\ell-1} \right),$$

où

$$\mathcal{P}_a{}'(x,k) := \frac{1}{\ell!} \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\} \\ g_L \le C_5 \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\} \\ c_{iL} | \frac{g_L}{k_L}}} \sum_{\substack{\{d_i,\ i\in\{1,\ldots,\ell\}\} \\ d_i | k}} \prod_{i\in\{1,\ldots,\ell\}} \mu(d_i) \sum_{\substack{\{p_i,\ i\in\{1,\ldots,\ell\}\} \\ p_1\cdots p_\ell \le x \\ (a, p_1\cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 (u_i d_i) \\ \forall i,\ a\in\mathfrak{R}\left(k_i', p_i\right)}} 1.$$

Démonstration. Il suffit de montrer que la contribution des g_L tels que $\max g_L > C_5$ est un $\mathcal{O}\left(\frac{x}{C_5^t \log x}(\log\log x)^{\ell-1}\right)$. Quitte à permuter l'ordre des p_i, il suffit de vérifier que la contribution d'un $g_{L_0} > C_5$, avec $L_0 \in \mathcal{P}^*(E)$ et $1 \in L_0$ est un $\mathcal{O}\left(\frac{x}{C_5^t \log x}(\log\log x)^{\ell-1}\right)$.
Un nombre presque premier donné ne pouvant être compté dans la somme sur tous les presque premiers plus petits que x que pour une valeur donnée des g_L et $c_{i,L}$, on a la majoration suivante :

$$\begin{aligned} S :=& \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\}\\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\setminus L_0\}\\ g_L \mid k_L^\infty \\ k_L \mid g_L}} \sum_{\substack{g_{L_0}\geq C_5\\ g_{L_0}\mid k_{L_0}^\infty \\ k_{L_0}\mid g_{L_0}}} \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\}\\ c_{iL}\mid \frac{g_L}{k_L}}} \sum_{\substack{\{p_i,\ i\in\{1,\dots,\ell\}\}\\ p_1\cdots p_\ell \leq x\\ \forall i,\ p_i\equiv 1 (u_i)}} 1 \\ \leq& \sum_{\substack{\prod_{L\in\mathcal{P}^*(E)} k_L = k\\ g_{L_0}\mid k_{L_0}^\infty \\ g_{L_0}>C_5}} \sum_{p_2\cdots p_\ell \leq x} \sum_{\substack{p_1\leq \frac{x}{p_2\cdots p_\ell}\\ p_1\equiv 1 \pmod{g_{L_0}}}} 1. \end{aligned}$$

On veut montrer que $S \ll \frac{x}{C_5^t \log x}(\log\log x)^{\ell-1}$.
On a vu précédemment que la contribution d'un $p_i \leq (\log x)^{64}$ était négligeable, donc

$$S \ll \sum_{\substack{\prod_{L\in\mathcal{P}^*(E)} k_L = k\\ g_{L_0}\mid k_{L_0}^\infty \\ g_{L_0}>C_5}} \sum_{p_2\cdots p_\ell \leq \frac{x}{(\log x)^{64}}} \sum_{\substack{p_1\leq \frac{x}{p_2\cdots p_\ell}\\ p_1\geq (\log x)^{64}\\ p_1\equiv 1 \pmod{g_{L_0}}}} 1,$$

p_1 étant premier, la condition $p_1 \equiv 1 \pmod{g_{L_0}}$ entraîne que $p_1 \geq g_{L_0}$.
On majore la somme sur p_1 en utilisant le théorème de Brun-Titchmarsh quand $g_{L_0} \leq (\log x)^{10}$ et par $\frac{x}{p_2\cdots p_\ell g_{L_0}}$ quand $g_{L_0} > (\log x)^{10}$. Ainsi $S \ll S_1 + S_2$, avec

$$S_1 := \sum_{\substack{\prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{g_{L_0}\mid k_{L_0}^\infty \\ C_5 < g_{L_0} \leq (\log x)^{10}}} \sum_{p_2\cdots p_\ell \leq \frac{x}{(\log x)^{64}}} \frac{x}{p_2\cdots p_\ell \varphi(g_{L_0}) \log\left(\frac{x}{p_2\cdots p_\ell g_{L_0}}\right)},$$

$$S_2 := \sum_{\substack{\prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{g_{L_0}\mid k_{L_0}^\infty \\ g_{L_0} > (\log x)^{10}}} \sum_{p_2\cdots p_\ell \leq \frac{x}{(\log x)^{64}}} \frac{x}{p_2\cdots p_\ell g_{L_0}}.$$

Pour la somme S_2 on utilise la méthode de Rankin pour majorer la somme sur g_{L_0} :

$$\sum_{\substack{g_{L_0}\mid k_{L_0}^\infty \\ g_{L_0} > (\log x)^{10}}} \frac{1}{g_{L_0}} \leq \frac{1}{(\log x)^5} \sum_{g_{L_0}\mid k_{L_0}^\infty} \frac{1}{g_{L_0}^{\frac{1}{2}}} \leq \frac{1}{(\log x)^5} \prod_{p\mid k_{L_0}} \left(\frac{p^{\frac{1}{2}}}{p^{\frac{1}{2}}-1}\right) \ll \frac{C_1}{(\log x)^5}.$$

En reportant dans la somme S_2 on obtient $S_2 \ll \frac{C_1 x}{(\log x)^5}(\log\log x)^{\ell-1}$.
Dans la somme S_1, $g_{L_0} \ll (\log x)^{10}$ tandis que $\frac{x}{p_2\cdots p_\ell} \geq (\log x)^{64}$ donc $\log\left(\frac{x}{p_2\cdots p_\ell g_{L_0}}\right) \gg \log\left(\frac{x}{p_2\cdots p_\ell}\right)$.
De plus $\frac{1}{\varphi(g_{L_0})} \leq \frac{1}{g_{L_0}}\frac{k_{L_0}}{\varphi(k_{L_0})} \ll \frac{\log\log C_1}{\varphi(g_{L_0})}$.
Nous appliquons de nouveau la méthode de Rankin avec un paramètre $t \in]0,1[$. On peut majorer la somme sur g_{L_0} par :

$$\sum_{\substack{g_{L_0}|k_{L_0}^{\infty} \\ C_5<g_{L_0}\leq(\log x)^{10}}} \frac{1}{\varphi(g_{L_0})} \ll \frac{C_1}{C_5^t}.$$

Ainsi $S_2 \ll \frac{C_1}{C_5^t}\frac{x}{\log x}(\log\log x)^{\ell-1}$. □

Dans les preuves des théorèmes 0.3 et 0.4, C_5 sera une constante fixée (arbitrairement grande). Cela est nécessaire pour pouvoir majorer certaines quantités relatives à des fonctions zêta de Dedekind associées aux corps $K_i := \mathbb{Q}(\xi_{u_i d_i}, a^{\frac{1}{k_i'}})$. Dans la preuve du théorème 0.5, correspondant au cas $\ell = 2$, les quantités C_1 et C_5 pourront tendre vers l'infini avec x. On prendra dans ce cas $C_1 = \log\log\log x$ et $C_5 = \log x$.
Afin de calculer les dernières sommes de $\mathcal{P}_a{}'(x,k)$ nous aurons besoin de plusieurs résultats de théorie algébrique des nombres, qui seront l'objet de la section suivante.

2.4 Correspondance entre les ℓ-presque premiers recherchés et les idéaux premiers de certains corps de nombres

Dans toute cette partie m est un entier naturel, m' un entier naturel sans facteur carré qui divise m, p un nombre premier et a un entier qui n'est ni -1 ni un carré et tel que $(a,p) = 1$. On suppose de plus que pour tout $q|m'$, q premier, a n'est pas une q-ième puissance. Commençons par la proposition suivante :

Proposition 2.9. *L'existence de solutions pour l'équation $\nu^{m'} \equiv a \pmod p$ et la condition $p \equiv 1 \pmod{m'}$ sont ensembles équivalentes au fait que l'équation $\nu^{m'} \equiv a \pmod p$ a exactement m' racines.*

Démonstration. Supposons qu'il existe ν tel que $\nu^{m'} \equiv a \pmod{p}$ et que $m'|(p-1)$. Alors $x^{m'} \equiv 1 \pmod{p}$ a m' solutions, que nous pouvons expliciter. Soit α une racine primitive modulo p, les racines m'-ième de 1 sont de la forme $x = \alpha^{\left(\frac{p-1}{m'}\right)\lambda}$, avec $0 \leq \lambda < m'$.
Alors pour chacune de ces racines, $(\nu x)^{m'} \equiv a \pmod{p}$ et ainsi le polynôme $X^{m'} - a$ a au moins m' racines dans $(\mathbb{Z}/p\mathbb{Z})^*$. Comme c'est un polynôme de degré m' on déduit que ce sont les seules.

Supposons maintenant que $\nu^{m'} \equiv a \pmod{p}$ a exactement m' racines. Alors le morphisme de groupe $\varphi : \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \to & (\mathbb{Z}/p\mathbb{Z})^* \\ \nu & \mapsto & \nu^{m'} \end{array}$ a un noyau $\mathrm{Ker}\varphi$ de cardinal m'.
Or $\mathrm{Card}(\mathrm{Ker}\varphi)|\mathrm{Card}((\mathbb{Z}/p\mathbb{Z})^*)$ et on a bien $m'|p-1$.

□

Nous allons exprimer cette propriété en utilisant le Théorème de Kummer ([27] Prop I.8.3), dont nous donnons une version faible.

Theorème 2.10 (Kummer)**.** *Soit $K = \mathbb{Q}[\theta]$ un corps de nombre et $P \in \mathbb{Z}[X]$ son polynôme minimal et O_K son anneau des entiers. Soit p un nombre premier tel que l'idéal (p) engendré par p dans O_K soit premier avec le conducteur de $Z[\theta]$. Soit*

$$\bar{P}(X) = \bar{P}_1(X)^{e_1} \cdots \bar{P}_r(X)^{e_r},$$

la factorisation de $\bar{P}(X) = P(X) \pmod{p}$ en un produit de polynômes irréductibles $\bar{P}_i(X) = P_i(X) \pmod{p}$ où les P_i sont des polynômes unitaires. Alors les

$$\mathfrak{P}_\mathfrak{i} = pO_k + P_i(\theta)O_k, \text{ pour } 1 \leq i \leq r,$$

sont les différents idéaux premiers de O_k au dessus de p. Le degré d'inertie de $\mathfrak{P}_\mathfrak{i}$ est le degré de $\bar{P}_i(X)$ et on a

$$(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Or le fait que l'équation $\nu^{m'} \equiv a \pmod{p}$ ait exactement m' racines correspond au fait que le polynôme $X^{m'} - a$ se factorise modulo p en un produit de m' polynômes unitaires distincts de degré 1. Ainsi cette propriété est équivalente au fait que $p \nmid m'$ et p se factorise dans $\mathbb{Q}(\sqrt[m']{a})$ comme produit de m' idéaux premiers distincts.

Montrons maintenant la proposition suivante qui est un résultat classique de théorie algébrique des nombres.

Proposition 2.11. *Les deux assertions suivantes sont équivalentes :*

- $p \equiv 1 \pmod{m}$,
- $p \nmid m$ *et* p *se factorise dans* $\mathbb{Q}(\xi_m)$ *en* $\varphi(m)$ *idéaux premiers distincts.*

Démonstration. Soit Φ_m le m-ième polynôme cyclotomique. Les racines de Φ_m modulo p sont des solutions de l'équation $x^m \equiv 1 \pmod{p}$.
Soit α une racine primitive modulo p. Alors pour $0 \leq r \leq p-1$, $(\alpha^r)^m \equiv 1(p)$ si et seulement si $rm \equiv 0 \pmod{p-1}$. Posons $d = (m, p-1)$. Alors

$$\begin{aligned} \alpha^{rm} \equiv 1(p) &\Leftrightarrow r\frac{m}{d} \equiv 0 \left(\frac{p-1}{d}\right) \\ &\Leftrightarrow \frac{p-1}{d} | r \end{aligned}$$

Ainsi les solutions de $x^m \equiv 1(p)$ sont les $\alpha^{\lambda \frac{p-1}{d}}$ avec $0 \leq \lambda < d$. Mais ce sont aussi les solutions de $x^d \equiv 1(p)$, ainsi les facteurs irréductibles de degré 1 de $\Phi_m \pmod{p}$ sont ceux de $\Phi_d \pmod{p}$.
Les $\alpha^{\lambda \frac{p-1}{d}}$ avec $\lambda < d$, $(\lambda, d) = 1$ sont des racines primitives d-ièmes de l'unité et donc $\Phi_d \pmod{p} = \prod_{\substack{(\lambda,d)=1 \\ 1 \leq \lambda < d}} (X - \alpha^{\lambda \frac{p-1}{d}})$. Ainsi $\deg(\Phi_d) = \varphi(d)$.
Alors d'après le Théorème de Kummer p se décompose en $\varphi(m)$ idéaux premiers distincts dans $\mathbb{Q}(\xi_m)$ si et seulement si $d = m$, i.e $m | p-1$. □

La proposition suivante, nous permettra de passer de conditions dans $\mathbb{Q}(\xi_m)$ et $\mathbb{Q}(\sqrt[m']{a})$ à des conditions dans $\mathbb{Q}(\sqrt[m']{a}, \xi_m)$.

Proposition 2.12. *Les trois conditions suivantes* $p \nmid m$, p *se décompose en* $\varphi(m)$ *idéaux premiers distincts dans* $\mathbb{Q}(\xi_m)$ *et* p *se décompose en* m' *idéaux premiers distincts dans* $\mathbb{Q}(\sqrt[m']{a})$ *ont lieu si et seulement si* $p \nmid m$ *et* p *se factorise dans* $K = \mathbb{Q}(\sqrt[m']{a}, \xi_m)$ *comme produit d'idéaux premiers distincts et de norme* p.

Démonstration. Supposons que $p \nmid m$, p se décompose en $\varphi(m)$ idéaux premiers distincts dans $\mathbb{Q}(\xi_m)$ et p se décompose en m' idéaux premiers distincts dans $\mathbb{Q}(\sqrt[m']{a})$.
La décomposition de (p) dans $\mathbb{Q}(\xi_m)$ est de la forme $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_{\varphi(m)}$ où pour tout $1 \leq i \leq \varphi(m)$, $\mathfrak{p}_i$ est un idéal premier de norme p, $\mathfrak{p}_i \neq \mathfrak{p}_j$.
Notons $\overline{\Phi_m} = \Phi_m \pmod{p}$, alors $\overline{\Phi_m}$ se factorise comme suit $\overline{\Phi_m}(X) = (X - u_1) \cdots (X - u_{\varphi(m)})$ et on a, quitte à modifier l'ordre des indices $\mathfrak{p}_i = (p, \xi_m - u_i)$.

De la même manière, en notant $B(X) = X^{m'} - a$, $\overline{B}(X) = B(X) \pmod p$, on a $\overline{B}(X) = (X - v_1) \cdots (X - v_{m'})$.
Comme $K = \mathbb{Q}(\xi_m)(\sqrt[m']{a})$, on peut noter P le polynôme minimal de $\sqrt[m']{a}$ sur $\mathbb{Q}(\xi_m)$ et $\overline{P} = P \pmod p$. Ainsi $\overline{P} | \overline{B}$ et donc $\overline{P}$ est scindé. Puis quitte à changer l'ordre des racines, $\overline{P}(X) = (X - v_1) \cdots (X - v_s)$, où $s \leq m'$.
A fortiori pour chaque $1 \leq i \leq \varphi(m)$, $P \pmod{\mathfrak{p}_i}$ est scindé et $P \equiv (X - v_1) \cdots (X - v_s) \pmod{\mathfrak{p}_i}$.
On applique le Théorème de Kummer à l'extension K de $\mathbb{Q}(\xi_m)$. Pour $1 \leq i \leq \varphi(m)$, $P \pmod{\mathfrak{p}_i}$ étant scindé, $\mathfrak{p}_i$ se décompose sur K en $\mathfrak{p}_i \mathcal{O}_K = \mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_{r_i}}$ avec $r_i = s$ et $N_{K/\mathbb{Q}}(\mathfrak{p}_{i_j}) = N_{\mathbb{Q}(\xi_m)/\mathbb{Q}}(\mathfrak{p}_i) = p$. Puis $p\mathcal{O}_K = \prod_{i=1}^{\varphi(m)} \mathfrak{p}_i \mathcal{O}_K = \prod_{\substack{1 \leq i \leq \varphi(m) \\ 1 \leq j \leq r_i}} \mathfrak{p}_{i_j}$ où $N_{K/\mathbb{Q}}(\mathfrak{p}_{i_j}) = p$.

Supposons maintenant que $p \nmid m$ et p se factorise dans $K = \mathbb{Q}(\sqrt[m']{a}, \xi_m)$ comme produit d'idéaux premiers distincts et de norme p.
Alors $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ où $s = [K : Q]$ et pour tout $1 \leq i \leq s$, $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p$.
Soit $L = \mathbb{Q}(\xi_m)$ et $p\mathcal{O}_L = Q_1 \cdots Q_r$ la décomposition de p en produit d'idéaux premiers dans L.
Soit f_i pour $1 \leq i \leq s$, tel que $N_{K/\mathbb{Q}}(Q_i) = p^{f_i}$. Alors f_i est le degré de l'extension $\mathcal{O}_L / Q_i \mathcal{O}_L$ par rapport à $\mathbb{F}_p$.
Or pour tout $i \in \{1, \ldots, r\}$, il existe au moins un $j \in \{1, \ldots, s\}$ tel que $\mathfrak{p}_j$ intervienne dans la décomposition de Q_i dans $\mathcal{O}_K$. Ainsi

$$[\mathcal{O}_K / \mathfrak{p}_j \mathcal{O}_K : \mathbb{F}_p] = [\mathcal{O}_K / \mathfrak{p}_j \mathcal{O}_K : \mathcal{O}_L / Q_i \mathcal{O}_L][\mathcal{O}_L / Q_i \mathcal{O}_L : \mathbb{F}_p]$$

Par hypothèse $[\mathcal{O}_K / \mathfrak{p}_j \mathcal{O}_K : \mathbb{F}_p] = 1$ et donc $f_i = [\mathcal{O}_L / Q_i \mathcal{O}_L : \mathbb{F}_p] = 1$, ainsi $N_{K/\mathbb{Q}}(Q_i) = p$ pour tout $1 \leq i \leq r$ et donc p se décompose en $[\mathbb{Q}(\xi_m) : \mathbb{Q}] = \varphi(m)$ idéaux premiers distincts dans $\mathbb{Q}(\xi(m))$.
De la même manière p se décompose en $[\mathbb{Q}(\sqrt[m']{a}) : \mathbb{Q}] = m'$ idéaux premiers distincts dans $\mathbb{Q}(\sqrt[m']{a})$. □

On déduit des trois proposions précédentes la proposition suivante :

Proposition 2.13. *Les propriétés $p \equiv 1(m)$ et $a \in \mathfrak{R}(m', p)$ sont ensembles équivalentes au fait que $p \nmid m$ et p se factorise complètement dans $K = \mathbb{Q}(\sqrt[m']{a}, \xi_m)$ comme produit d'idéaux premiers distincts de norme p.*

Démonstration. Les propositions 2.9 et 2.11 entraînent que les conditions $p \equiv 1(m)$ et $a \in \mathfrak{R}(m', p)$ sont ensembles équivalentes au fait que $p \nmid m'$ et p se factorise dans $\mathbb{Q}(\xi_m)$ en un produit de $\varphi(m)$ idéaux premiers distincts et se factorise dans $\mathbb{Q}(\sqrt[m']{a})$ en un produit de m' idéaux premiers distincts.

Enfin la proposition 2.12 permet de ramener ces conditions à des conditions dans $\mathbb{Q}(\sqrt[m']{a}, \xi_m)$. □

Nous allons maintenant calculer explicitement le degré de $\mathbb{Q}(\sqrt[m']{a}, \xi_m)$.

Proposition 2.14. *Soient m', m deux entiers naturels tels que $m'|m$, m' sans facteur carré et $a \neq -1$ un entier qui ne soit pas un carré. Notons $K = \mathbb{Q}(\sqrt[m']{a}, \xi_m)$, où ξ_m est une racine m-ième de l'unité. Alors,*

$$[K : \mathbb{Q}] = \frac{m'\varphi(m)}{\epsilon(m', m)},$$

où $\epsilon(m', m)$ est donné par la formule suivante, en prenant a_1 la partie sans facteur carré de a (i.e $a = a_1 a_2^2$, avec a_1 sans facteur carré),

$$\epsilon(m', m) = \begin{cases} 2 \text{ si } 2|m',\ 2||m,\ a_1|m \text{ et } a_1 \equiv 1 \pmod 4 \\ 2 \text{ si } 2|m',\ 4||m,\ a_1|m \text{ et } a_1 \equiv 1 \pmod 2 \\ 2 \text{ si } 2|m',\ 8|m \text{ et } a_1|m \\ 1 \text{ sinon.} \end{cases} \tag{2.8}$$

Démonstration. Remarquons que :

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\xi_m)][\mathbb{Q}(\xi_m) : \mathbb{Q}] = \varphi(m)[K : \mathbb{Q}(\xi_m)].$$

Comme $\mathbb{Q}(\xi_m)/\mathbb{Q}$ est une extension galoisienne on a

$$[K : \mathbb{Q}(\xi_m)]|m'.$$

Posons $m' = \delta[K : \mathbb{Q}(\xi_m)]$. Alors, si q est un facteur premier de δ, le degré $[\mathbb{Q}(\xi_m)(\sqrt[q]{a}) : \mathbb{Q}(\xi_m)]$ vaut soit 1 soit q. De plus,

$$[\mathbb{Q}(\xi_m)(\sqrt[q]{a}) : \mathbb{Q}(\xi_m)] \text{ divise } [K : \mathbb{Q}(\xi_m)] = \frac{m'}{\delta}.$$

Or $(\frac{m'}{\delta}, q) = 1$ car m' est sans facteur carré, donc $[\mathbb{Q}(\xi_m)(\sqrt[q]{a}) : \mathbb{Q}(\xi_m)] = 1$ et ainsi $\sqrt[q]{a} \in \mathbb{Q}(\xi_m)$. Montrons que $q < 3$.
Déjà $\mathbb{Q}(a^{\frac{1}{q}}, \xi_q) \subset \mathbb{Q}(\xi_m)$ et $\mathbb{Q}(\xi_m)/\mathbb{Q}$ est une extension abélienne car son groupe de Galois est $(\mathbb{Z}/m\mathbb{Z})^*$. Soit L une sous extension galoisienne de $\mathbb{Q}(\xi_m)$, alors

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\xi_m)/L)}$$

et donc $\mathrm{Gal}(L/\mathbb{Q})$ est abélien.
Supposons que $q > 2$ et montrons que le groupe de galois de $\mathbb{Q}(a^{\frac{1}{q}}, \xi_q)/\mathbb{Q}$ n'est pas abélien. Par l'absurde on suppose que ce dernier est abélien.

Alors l'extension $\mathbb{Q}(a^{\frac{1}{q}}, \xi_q)/\mathbb{Q}(a^{\frac{1}{q}})$ est galoisienne et son groupe de Galois H est un sous-groupe de $G_q := \mathrm{Gal}\left(\mathbb{Q}(a^{\frac{1}{q}}, \xi_q)/\mathbb{Q}\right)$. Comme G_q est abélien H est un sous-groupe invariant de G_q. D'après la correspondance de Galois, cela entraîne que $\mathbb{Q}(a^{\frac{1}{q}})/\mathbb{Q}$ est galoisienne de groupe de Galois G_q/H.
Mais $\mathbb{Q}(a^{\frac{1}{q}})/\mathbb{Q}$ n'est pas galoisienne car $\mathbb{Q}(a^{\frac{1}{q}})$ ne contient pas toutes les racines du polynôme $X^q - a$ si $q \geq 3$.
On en déduit que q ne peut être impair et donc δ vaut 1 ou 2, car m' est sans facteur carré.
Comme $(q, \frac{m'}{q}) = 1$, il existe deux entiers u et v tels que $uq + v\frac{m'}{q} = 1$ et donc $a^{\frac{1}{m'}} = a^{\frac{uq+v\frac{m'}{q}}{m'}} = a^{\frac{uq}{m'}} a^{\frac{v}{q}}$, ainsi

$$K = \mathbb{Q}(\xi_m)(\sqrt[\frac{m'}{q}]{a}, \sqrt[q]{a}).$$

Il vient que si $\sqrt{a} \in \mathbb{Q}(\xi_m)$ alors $\delta = 2$. On en déduit que $\delta = 2$ si et seulement si $\sqrt{a} \in \mathbb{Q}(\xi_m)$.
Posons

$$a = a_1 a_2^2$$

où a_1 est sans facteur carré et éventuellement négatif.
On utilise la caractérisation des sous-corps quadratiques d'un corps cyclotomique ([40], Cor 4.5.4).

Si $2||m$, comme a_1 est sans facteur carré, $\mathbb{Q}(\sqrt{a_1})$ est contenu dans $\mathbb{Q}(\xi_m)$ si et seulement si a_1 est de la forme $(-1|D)D$, où $(\cdot|\cdot)$ est le symbole de Jacobi et D est un diviseur positif impair de m différent de 1.
Ainsi δ vaut 2 si et seulement si $a_1|m$ et a_1 est un entier impair de même signe que le symbole de Jacobi $(-1\,||a_1|)$. Comme a n'est pas un carré parfait, $a_1 \neq 1$ et on peut calculer $(-1\,||a_1|)$:

$$\begin{aligned}
(-1\,||a_1|) &= (-1)^{\frac{|a_1|-1}{2}} \\
&= \begin{cases} 1 & \text{si} \quad |a_1| \equiv 1 \pmod 4 \\ -1 & \text{si} \quad |a_1| \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} 1 & \text{si} \quad a_1 \equiv 1 \pmod 4 \quad \text{et} \quad a_1 > 0 \\ 1 & \text{si} \quad a_1 \equiv 3 \pmod 4 \quad \text{et} \quad a_1 < 0 \\ -1 & \text{si} \quad a_1 \equiv 3 \pmod 4 \quad \text{et} \quad a_1 > 0 \\ -1 & \text{si} \quad a_1 \equiv 1 \pmod 4 \quad \text{et} \quad a_1 < 0 \end{cases}
\end{aligned}$$

Ainsi, on a $\delta = 2$ avec $2||m$ si et seulement si $2|m'$, $a_1|m$ et $a_1 \equiv 1 \pmod 4$.
Si $4||m$, alors $\mathbb{Q}(\sqrt{a_1})$ est dans $\mathbb{Q}(\xi_m)$ si et seulement si a_1 ou $-a_1$ est comme

ci-dessus, et on a donc $\delta = 2$ avec $4||m$ si et seulement si $2|m'$, $a_1|m$ et $a_1 \equiv 1 \pmod 2$.
Si $8|m$, alors $\mathbb{Q}(\sqrt{a_1})$ est dans $\mathbb{Q}(\xi_m)$ si et seulement si a_1, $-a_1$, $a_1/2$ ou $-a_1/2$ est comme ci-dessus, et on a donc $\delta = 2$ avec $8|m$ si et seulement si $2|m'$ et $a_1|m$.

□

2.5 Méthode de Selberg-Delange

D'après les sections précédentes, la quantité que l'on souhaite évaluer est :

$$\sum_{\substack{p_1\cdots p_\ell \leq x \\ (a,p_1\cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 (u_i d_i)}} 1 = \sum_{\substack{m_1\cdots m_\ell \leq x \\ p|m_i \Rightarrow p \in P_i \\ m_i \text{ premier}}} 1,$$

$$a \in \mathfrak{R}\left(\prod_{\substack{L \subset E' \\ i \in L}} k'_L, p_i \right)$$

où P_i est l'ensemble des nombres premiers p tels que $p \nmid au_i d_i$ et p se factorise dans K_i comme produits d'idéaux premiers distincts de norme p, $K_i := \mathbb{Q}(\sqrt[k'_i]{a}, \xi_{u_i d_i})$ et $k'_i := \prod_{\substack{L \subset E' \\ i \in L}} k'_L$. Les notations des conditions sur la somme de droite peuvent sembler inutilement lourde, mais cela nous sera utile plus tard afin de voir le lien entre cette somme et une somme plus générale dans la suite. Rappelons que l'en prenant C_1 et C_5 comme des constantes arbitrairement grandes, les diviseurs de $u_i d_i$ sont bornés pour $1 \leq i \leq \ell$.

Le cas $\ell = 1$ a été traité par Hooley [14], en utilisant un résultat proche du théorème de densité de Tchebotarev et une majoration du discriminant de l'extension considérée. Pour $\ell = 2$, il est possible de procéder de la même façon que pour $\ell = 1$ en utilisant la méthode de l'hyperbole. Cependant pour $\ell \geq 3$ il devient trop compliqué de contrôler les termes d'erreur qui émergent de la méthode de l'hyperbole, nous allons donc utiliser la méthode de Selberg-Delange. Nous suivrons la méthode de Selberg-Delange telle que décrite par Tenenbaum [37] chapitre II.5, en comparant une fonction à un produit de puissances de fonctions zêta de Dedekind associées aux corps K_i, similairement à un cas traité par Hanrot, Tenenbaum et Wu [10].
Définissons, pour $\boldsymbol{r} := (r_1, \ldots, r_\ell) \in \mathbb{N}^\ell$, $n \in \mathbb{N}$,

$$c_{\boldsymbol{r}}(n) := \sum_{m_1\cdots m_\ell = n} \mu^2(n) \prod_{i=1}^{\ell} \left(\mathbb{1}\left(\Omega(m_i) = r_i\right) \mathbb{1}\left(p|m_i \Rightarrow p \in P_i\right) \right),$$

et donc, en posant $\overline{1} = (1, \dots, 1)$, $\sum_{\substack{m_1 \cdots m_\ell \leq x \\ p|m_i \Rightarrow p \in P_i \\ m_i \text{ premier}}} 1 = \sum_{n \leq x} c_{\overline{1}}(n)$.

Notons alors $\boldsymbol{r} \geq 0$ lorsque pour tout $1 \leq i \leq \ell$, $r_i \geq 0$, puis pour $\boldsymbol{z} := (z_1, \dots, z_\ell) \in \mathbb{C}^\ell$:

$$\alpha_{\boldsymbol{z}}(n) := \sum_{\boldsymbol{r} \geq 0} c_{\boldsymbol{r}}(n) \prod_{i=1}^{\ell} z_i^{r_i} = \sum_{\substack{m_1 \cdots m_\ell = n \\ p|m_i \Rightarrow p \in P_i}} \mu^2(n) \prod_{i=1}^{\ell} z_i^{\omega(m_i)}.$$

Remarquons que $\alpha_{\boldsymbol{z}}(n)$ est multiplicative, vu que c'est un produit de convolutions de fonctions multiplicatives.
Enfin, pour $\Re(s) > 1$, la série de Dirichlet associée à $\alpha_{\boldsymbol{z}}$ est :

$$F(s, \boldsymbol{z}) := \sum_{n \geq 0} \frac{\alpha_{\boldsymbol{z}}(n)}{n^s} = \prod_p \left(1 + \sum_{\nu \geq 1} \frac{\alpha_{\boldsymbol{z}}(p^\nu)}{p^{\nu s}} \right) = \prod_i \left(\prod_{p \in P_i} \left(1 + \frac{z_i}{p^s} \right) \right).$$

F admet alors un prolongement analytique en une fonction méromorphe sur $\mathbb{C}\backslash\{1\}$. L'étude de F par la méthode de Selberg-Delange nous donnera une expression de $\sum_{n \leq x} \alpha_{\boldsymbol{z}}(n)$, dont nous extrairons la quantité qui nous intéresse par la formule de Cauchy.
Définissons les objets dont nous aurons besoin pour appliquer la méthode de Selberg-Delange. Pour $i \in \{1, \dots, \ell\}$, on notera ζ_{K_i} la fonction zêta de Dedekind associée à K_i et n_i le degré de K_i sur $\mathbb{Q}$. On définit $\zeta_{K_i,f}(s)$ comme étant la partie de ζ_{K_i} portant sur les idéaux premiers de norme une puissance f-ième : $\zeta_{K_i,f}(s) := \prod_{\substack{\mathfrak{p} \\ \exists p,\ N(\mathfrak{p}) = p^f}} \left(1 - \frac{1}{p^{fs}}\right)^{-1}$.
De plus on décompose $F(s, \boldsymbol{z})$ en un produit de fonctions F_i :
$F_i(s, z_i) := \prod_{p \in P_i} \left(1 + \frac{z_i}{p^s}\right)$. Nous allons voir que les fonctions F_i se comportent similairement à des puissances des fonctions zêta de Dedekind associées à K_i, pour ce faire on pose pour $\sigma > 1$:

$$\begin{aligned} G_i(s, z_i) :&= F_i(s, z_i) \zeta_{K_i}^{-\frac{z_i}{n_i}}(s) \qquad (2.9) \\ &= \prod_{p \in P_i} \left(\left(1 + \frac{z_i}{p^s}\right) \left(1 - \frac{1}{p^s}\right)^{z_i} \right) \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) | a u_i d_i \\ N(\mathfrak{p}) = p}} \left(1 - \frac{1}{p^s}\right)^{\frac{z_i}{n_i}} \prod_{\substack{f | n_i \\ f \geq 2}} \zeta_{K_i,f}(s)^{-\frac{z_i}{n_i}}, \end{aligned}$$

et $G(s, \boldsymbol{z}) := \prod_i G_i(s, z_i)$.

Nous définissons aussi les fonctions $Z_i(s,z_i) := ((s-1)\zeta_{K_i}(s))^{\frac{z_i}{n_i}}$ et la fonction $Z(s,\boldsymbol{z}) := \prod_i Z_i(s,z_i)$, qui joueront un rôle important dans la suite.

Les fonctions zêta de Dedekind disposent de régions sans zéro semblables à celle de la fonction zêta de Riemann ([19]), comme nous travaillons avec des extensions dont le degré est borné on peut trouver une région sans zéro commune à toutes nos fonctions zêta de Dedekind, ce que l'on résume dans la proposition suivante.

Proposition 2.15. *Il existe des constantes C_6, C_7 et C_8 ne dépendant que de C_1 et C_5 telles que ζ_{K_i} ne s'annule pas pour*

$$\sigma \geq 1 - \frac{1}{C_6 \log t + C_7}, \quad \text{et } |t| \geq 1,$$
$$\sigma \geq 1 - C_8, \quad \text{et } |t| \leq 1,$$

et cela pour tout $i \in \{1,\dots,l\}$.

Afin d'appliquer la méthode de Selberg-Delange nous devons nous assurer que la fonction G se comporte convenablement dans la région sans zéro décrite ci-dessus. Nous noterons $|\boldsymbol{z}| \leq A$ si, pour tout $1 \leq i \leq \ell$, $|z_i| \leq A$.

Proposition 2.16. *Soit A un réel strictement positif. Pour $|\boldsymbol{z}| \leq A$ et s dans la région sans zéro décrite dans la proposition 2.15, et $\mathfrak{Re}\ s \leq 2$ on a :*

$$G(s,\boldsymbol{z}) \ll_{A,\varepsilon} 1.$$

Démonstration. Déjà pour tout i, comme tous les $u_i d_i$ sont bornés,

$$\prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p})|au_id_i \\ N(\mathfrak{p})=p}} \left(1-\frac{1}{p^s}\right)^{\frac{z_i}{n_i}} \prod_{\substack{f|n_i \\ f\geq 2}} \zeta_{K_i,f}(s)^{-\frac{z_i}{n_i}} \ll_A 1.$$

Définissons pour tout i, $\tilde{G}_i(s,\boldsymbol{z}) := \prod_{p\in P_i} \left(\left(1+\frac{z_i}{p^s}\right)\left(1-\frac{1}{p^s}\right)^{z_i}\right) = \sum_{n\geq 1} \frac{b_{i,z_i}(n)}{n^s}$, où b_{i,z_i} est la fonction multiplicative dont les valeurs sur les puissances de nombres premiers sont déterminées par l'identité :

$$1 + \sum_{\nu\geq 1} b_{i,z_i}(p^\nu)\xi^\nu = (1+\xi z_i)\,(1-\xi)^{z_i}\,,\ |\xi|<1,\ p\in P_i,$$

et $b_{i,z_i}(p^\nu) = 0$ pour $p \notin P_i$.
Ensuite pour $p \in P_i$, on a

$$b_{i,z_i}(p) = \left.\frac{\partial (1+\xi z_i)(1-\xi)^{z_i}}{\partial \xi}\right|_{\xi=0} = 0.$$

Puis l'inégalité de Cauchy prise sur le cercle $|\xi| = \frac{1}{\sqrt{2}}$ implique, pour $|z_i| \leq A$, $|b_{i,z_i}(p^\nu)| \leq M2^{\frac{\nu}{2}}$, avec $M := \sup_{|z_i|\leq A,\ |\xi|\leq\frac{1}{\sqrt{2}}} [(1+\xi z_i)(1-\xi)^{z_i}]$. Ainsi, pour $\sigma > \frac{1}{2}$, comme $b_{i,z_i}(p) = 0$,

$$\sum_p \sum_{\nu\geq 1} \frac{|b_{i,z_i}(p^\nu)|}{p^{\nu\sigma}} \leq 2M \sum_p \frac{1}{p^\sigma(p^\sigma - \sqrt{2})} \leq \frac{cM}{\sigma - \frac{1}{2}},$$

où c est une constante absolue. Ainsi $G_i(s, z_i)$ est absolument convergent pour $\sigma > \frac{1}{2}$, et pour $\sigma \geq \frac{1}{2} + \varepsilon$,

$$G_i(s, z_i) \ll_{A,\varepsilon} 1.$$

□

Nous aurons aussi besoin de contrôler ζ_{K_i} à droite de la droite critique. Pour cela on utilise un lemme de Wang [38] qui découle d'une majoration de Heath-Brown [12] pour ζ_{K_i} sur la droite critique.

Lemme 2.17 (Wang)**.** *Soient K une extension algébrique de degré n et $\eta > 0$. Alors par le principe de Phragmén-Lindelöf dans la bande $\frac{1}{2} \leq \sigma \leq 1 + \varepsilon$:*

$$\zeta_K(\sigma + it) \ll_\eta (1 + |t|)^{\frac{n}{3}(1-\sigma)+\varepsilon}, \text{ pour } |t| \geq \eta.$$

Enfin nous avons besoin du développement de Taylor de Z autour de 1.

Proposition 2.18. *La fonction $Z(s, \boldsymbol{z})$ est holomorphe dans le disque $|s - 1| < C_8$, et y admet la représentation en série de Taylor suivante :*

$$Z(s, \boldsymbol{z}) = \sum_{j\geq 0} \frac{1}{j!}\gamma_j(\boldsymbol{z})(s-1)^j,$$

où les $\gamma_j(\boldsymbol{z})$ sont des fonctions entières en chacun des z_i, satisfaisant, pour tout $\frac{1}{\ell} > A > 0$, $\frac{1-C_8}{C_8} \geq \varepsilon > 0$,

$$\frac{1}{j!}\gamma_j(\boldsymbol{z}) \ll_{A,\epsilon} (1+\varepsilon)^j \qquad (|\boldsymbol{z}| \leq A).$$

Démonstration. Le résultat est immédiat comme les ζ_{K_i} n'ont pas de zéro dans ce cercle, il suffit alors d'appliquer le théorème de Cauchy (Théorème II.5.1, [37] ou [36]) :

$$\frac{1}{j!}\gamma_j(\boldsymbol{z}) = \frac{1}{2\pi i} \oint_{|s-1|=c} \frac{Z(s, \boldsymbol{z})}{(s-1)^{j+1}} ds,$$

et la majoration découle de l'inégalité de Cauchy. □

On peut alors appliquer la méthode de Selberg-Delange et obtenir l'estimation escomptée.

Proposition 2.19. *Par la méthode de Selberg-Delange, on a pour* $|z_i| \leq A$ *pour tout* $1 \leq i \leq \ell$,

$$\sum_{n\leq x} \alpha_{\boldsymbol{z}}(n) = x(\log x)^{\sum_i \frac{z_i}{n_i}-1}\left(\frac{G(1,\boldsymbol{z})\gamma_0(\boldsymbol{z})}{\Gamma(\sum_i \frac{z_i}{n_i})} + \mathcal{O}_{C_1,C_5}\left(\frac{1}{\log x}\right)\right) + \mathcal{O}\left(xe^{-c_6\sqrt{\log x}}\right).$$

Démonstration. Posons $A(x,\boldsymbol{z}) := \sum_{n\leq x} \alpha_{\boldsymbol{z}}(n)$. Alors par la formule de Perron on a ([37] ou [36], Théorème II.2.5) :

$$\int_0^x A(t)dt = \frac{1}{2i\pi}\int_{\kappa-i\infty}^{\kappa+i\infty} F(s)x^{s+1}\frac{ds}{s(s+1)},$$

avec $\kappa := 1 + \frac{1}{\log x}$.
Définissons le domaine $\mathcal{D}$ comme la région sans zéro commune à nos fonctions zêta de Dedekind donnée par la proposition 2.15 et $\tilde{\mathcal{D}} := \mathcal{D}\backslash[\frac{1}{2}+\varepsilon, 1]$.
Ainsi, pour $s = \sigma + it \in \mathcal{D}$, $|s-1| \gg 1$, $|\boldsymbol{z}| \leq A$, $A < \frac{1}{l}$, par la proposition 2.16 et le lemme 2.17,

$$F(s,\boldsymbol{z}) \ll \prod_{i=1}^{\ell}\left((1+|t|)^{\frac{n_i}{3}(1-\sigma)+\frac{1}{\log x}}\right)^{\frac{A}{n_i}} \ll (1+|t|)^{\frac{\ell A}{3}(1-\sigma)+\frac{\ell A}{\log x}}.$$

Alors, avec $T > 1$ un paramètre à définir, les contributions des demi-droites verticales $[\kappa \pm iT, \kappa \pm i\infty[$ sont :

$$\int_{\kappa+iT}^{\kappa+i\infty} F(s,\boldsymbol{z})x^{s+1}\frac{ds}{s(s+1)} \ll x^2\int_T^{+\infty} t^{\frac{4\ell A}{3\log x}-2}dt$$

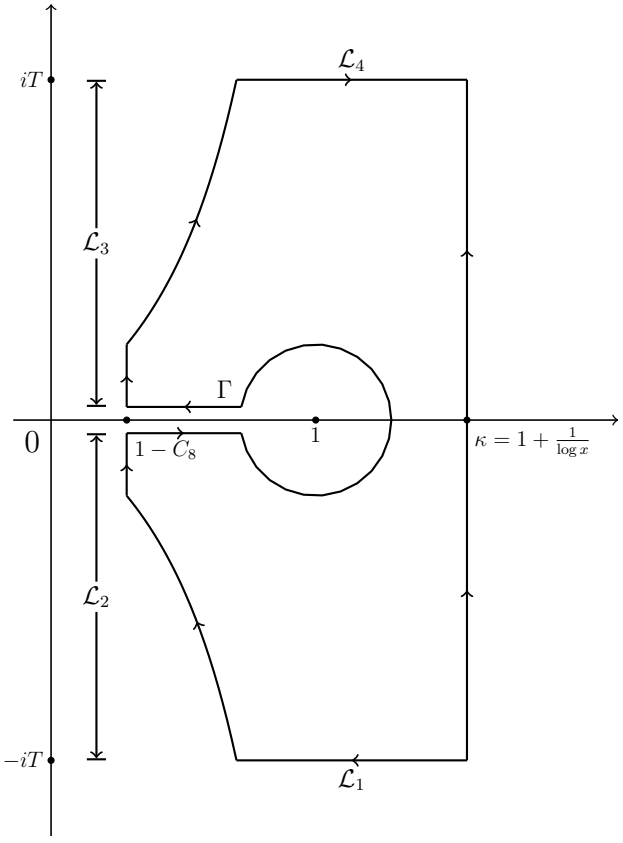
et donc,

$$\int_{\kappa+iT}^{\kappa+i\infty} F(s,\boldsymbol{z})x^{s+1}\frac{ds}{s(s+1)} \ll x^2 T^{\frac{4\ell A}{3\log x}-1},$$

et il en va de même pour l'autre demi-droite.
Posons $C_9(T) := \frac{1}{C_6\log T + C_7}$.

Il reste à évaluer $\int_{\kappa-iT}^{\kappa+iT} F(s,\boldsymbol{z})x^{s+1}\frac{ds}{s(s+1)}$, pour ce faire, on va déformer le chemin d'intégration comme suit :

- $\mathcal{L}_1$ le segment $[\kappa - iT, 1 - C_9(T) - iT]$;
- $\mathcal{L}_2$ la courbe $\sigma(t) = 1 - \frac{1}{C_6 \log t + C_7}$, pour $t \in [1 - C_9(T) - iT, 1 - C_8]$;
- un contour de Hankel tronqué Γ, entourant 1 de rayon $\frac{1}{2\log x}$ et de partie rectiligne joignant $1 - \frac{1}{2\log x}$ à $1 - C_8$;
- on complète le contour par symétrie par rapport à l'axe réel.



Pour le segment $\mathcal{L}_1$ on a la majoration :

$$\int_{\kappa-iT}^{1-C_9(T)-iT} F(s,\boldsymbol{z})x^{s+1}\frac{ds}{s(s+1)} \ll x^2 T^{\ell A\left(\frac{C_9(T)}{3}+\frac{1}{\log x}\right)-2},$$

et il vient la même majoration pour $\mathcal{L}_4$.
Puis sur la courbe $\mathcal{L}_2$:

$$\int_{1-C_9(T)-iT}^{1-C_8} F(s,\boldsymbol{z})x^{s+1}\frac{ds}{s(s+1)} \ll x^{2-C_9(T)}\left(\int_T^{+\infty} t^{\ell A\left(\frac{C_9(T)}{3}+\frac{1}{\log x}\right)-2}dt + \mathcal{O}(1)\right) \ll x^{2-C_9(T)},$$

car $A < \frac{1}{\ell}$, et il vient la même majoration pour $\mathcal{L}_3$.
Posons alors

$$\Phi(x) := \frac{1}{2\pi i}\int_{\Gamma} F(s,\boldsymbol{z})x^{s+1}\frac{ds}{s(s+1)}.$$

On a donc, en prenant $T = x^{c_1\sqrt{\log x}}$,

$$\int_0^x A(t)dt = \Phi(x) + \mathcal{O}\left(x^2 e^{-c_2\sqrt{\log x}}\right). \tag{2.10}$$

Pour $s \in \mathcal{D}$, on a

$$F(s,\boldsymbol{z}) = sG(s,\boldsymbol{z})Z(s,\boldsymbol{z})(s-1)^{-\sum_i \frac{z_i}{n_i}}, \tag{2.11}$$

et donc par la proposition 2.18, et comme $|s-1| < 1$ pour s dans Γ,

$$F(s,\boldsymbol{z}) \ll |s-1|^{-A}, \quad (s \in \Gamma). \tag{2.12}$$

Notons, dans le domaine d'holomorphie de $G(s,\boldsymbol{z})$,

$$G^{(k)}(s,\boldsymbol{z}) := \frac{\partial^k}{\partial s^k}G(s,\boldsymbol{z}).$$

On a alors, pour $s \in \Gamma$,

$$G(s,\boldsymbol{z})Z(s,\boldsymbol{z}) = \sum_{k\geq 0}\mu_k(\boldsymbol{z})(s-1)^k,$$

avec $\mu_k(\boldsymbol{z}) := \sum\limits_{h+j=k}\frac{1}{h!j!}G^{(h)}(1,\boldsymbol{z})\gamma_j(\boldsymbol{z})$. Comme $G(s,\boldsymbol{z})Z(s,\boldsymbol{z})$ est holomorphe pour $|s-1| \leq C_8$ l'inégalité de Cauchy fournit la majoration de $\mu_k(\boldsymbol{z})$ suivante :

$$\mu_k(\boldsymbol{z}) \ll C_8^{-k}.$$

De plus Γ est inclus dans le disque $|s-1| \leq C_8$, donc on a pour $s \in Gamma$,

$$G(s,\boldsymbol{z})Z(s,\boldsymbol{z}) = \mu_0(\boldsymbol{z}) + \mathcal{O}\left(|s-1|\right). \tag{2.13}$$

De plus $\Phi(x)$ est indéfiniment dérivable sur $\mathbb{R}_+$ et sa dérivée est :

$$\Phi'(x) = \frac{1}{2\pi i}\int_{\Gamma} F(s)x^s\frac{ds}{s}.$$

Reprenons alors (2.11) et (2.13) dans $\Phi'(x)$, ce qui donne :

$$\Phi'(x) = \mu_0(\boldsymbol{z})\frac{1}{2\pi i}\int_{\Gamma} x^s(s-1)^{-\sum_i \frac{z_i}{n_i}}ds + \mathcal{O}\left(\frac{R(x)}{C_8}\right), \tag{2.14}$$

avec

$$\begin{aligned} R(x) &:= \int_{\Gamma} \left| x^s (s-1)^{1-\sum_i \frac{z_i}{n_i}} \right| |ds| \\ &\ll \int_{1-C_8}^{1-\frac{1}{2\log x}} x^{\sigma} (1-\sigma)^{1-\Re\left(\sum_i \frac{z_i}{n_i}\right)} d\sigma + x^{1+\frac{1}{2\log x}} (2\log x)^{-2+\Re\left(\sum_i \frac{z_i}{n_i}\right)}. \end{aligned}$$

Puis en effectuant le changement de variable $t = -(\sigma-1)\log x$,

$$\begin{aligned} R(x) &\ll x(\log x)^{-2+\Re\left(\sum_i \frac{z_i}{n_i}\right)} \left(\int_{\frac{1}{2}}^{+\infty} t^{1-\Re\left(\sum_i \frac{z_i}{n_i}\right)} e^{-} t dt + 1 \right) \\ &\ll x(\log x)^{-2+\Re\left(\sum_i \frac{z_i}{n_i}\right)} \Gamma(2+\ell A) \\ &\ll x(\log x)^{\sum_i \frac{z_i}{n_i}-1} \frac{(\ell A+1)^{\ell A+1}}{\log x}. \end{aligned}$$

En effectuant le le changement de variable $t = (s-1)\log x$ dans le terme principal de (2.14) on obtient :

$$\frac{1}{2\pi i} \int_{\Gamma} x^s (s-1)^{-\sum_i \frac{z_i}{n_i}} ds = \frac{x}{2\pi i} (\log x)^{\sum_i \frac{z_i}{n_i}-1} \int_{\Gamma'} t^{-\sum_i \frac{z_i}{n_i}} e^t dt,$$

où Γ' est le contour de Hankel tronqué pour $\sigma \geq -C_8 \log x$, on obtient en utilisant le corollaire II.0.18 de [37],

$$\int_{\Gamma} x^s (s-1)^{-\sum_i \frac{z_i}{n_i}} ds \ll x(\log x)^{\sum_i \frac{z_i}{n_i}-1} \left(\frac{1}{\Gamma(\sum_i \frac{z_i}{n_i})} + \mathcal{O}\left(x^{\frac{-C_8}{2}} \right) \right).$$

Le terme principal de (2.14) est alors

$$\begin{aligned} & x(\log x)^{\sum_i \frac{z_i}{n_i}-1} \left(\frac{\mu_0(\boldsymbol{z})}{\Gamma(\sum_i \frac{z_i}{n_i})} + \mathcal{O}\left(x^{\frac{-C_8}{2}} |\mu_0(\boldsymbol{z})| \right) \right) \\ &= x(\log x)^{\sum_i \frac{z_i}{n_i}-1} \left(\frac{\mu_0(\boldsymbol{z})}{\Gamma(\sum_i \frac{z_i}{n_i})} + \mathcal{O}\left(x^{\frac{-C_8}{2}} \right) \right). \end{aligned}$$

En reportant cela dans (2.14), cela donne :

$$\Phi'(x) = x(\log x)^{\sum_i \frac{z_i}{n_i}-1} \left(\frac{\mu_0(\boldsymbol{z})}{\Gamma(\sum\limits_i \frac{z_i}{n_i})} + \mathcal{O}\left(\frac{1}{\log x} \right) \right).$$

Remarquons également que l'on a :

$$\Phi''(x) = \frac{1}{2\pi i}\int_\Gamma F(s)x^{s-1}ds.$$

Il reste à montrer que $\Phi'(x)$ est une bonne approximation de $A(x)$. Pour cela, on procède comme dans [37] p243. Soit $0 < h < \frac{x}{2}$, on a alors, par (2.10),

$$\int_x^{x+h} A(t)dt = \Phi(x+h) - \Phi(x) + \mathcal{O}\left(x^2 e^{-c_3\sqrt{\log x}}\right).$$

Puis, en utilisant la formule de Taylor,

$$\begin{aligned}\Phi(x+h) - \Phi(x) &= h\Phi'(x+h) - h^2\int_0^1 t\Phi''(x+th)dt \\ &= h\Phi'(x) + h^2\int_0^1 (1-t)\Phi''(x+th)dt.\end{aligned}$$

Puis par (2.12), on a $\Phi''(x) \ll (\log x)^A$, ainsi $\Phi(x+h) - \Phi(x) = h\Phi'(x) + \mathcal{O}\left(h^2(\log x)^A\right)$, et donc

$$\begin{aligned}A(x) &= \frac{1}{h}\int_x^{x+h} A(t)dt + \frac{1}{h}\int_x^{x+h}(A(x) - A(t))dt \\ &= \Phi'(x) + \mathcal{O}\left(x^2 e^{-c_3\sqrt{\log x}} + h(\log x)^A + \frac{1}{h}\int_x^{x+h}(A(t) - A(x))dt\right).\end{aligned}$$

Or

$$\int_x^{x+h}(A(t) - A(x))dt \leq \int_x^{x+h} A(t)dt - \int_{x-h}^{x} A(t)dt = \mathcal{O}\left(hx^2 e^{-c_4\sqrt{\log x}} + h^2(\log x)^A\right).$$

Ainsi on a finalement, en prenant $h = xe^{-c_5\sqrt{\log x}}$

$$A(x) = x(\log x)^{\sum_i \frac{z_i}{n_i} - 1}\left(\frac{\mu_0(\boldsymbol{z})}{\Gamma(\sum\limits_i \frac{z_i}{n_i})} + \mathcal{O}\left(\frac{1}{\log x}\right)\right) + \mathcal{O}\left(xe^{-c_6\sqrt{\log x}}\right). \quad (2.15)$$

□

Il ne reste plus qu'à appliquer le théorème de Cauchy à ce résultat pour obtenir l'estimation attendue, similairement au Théorème II.6.3 de [37].

Proposition 2.20. *En appliquant la formule de Cauchy au résultat de la proposition 2.19 on obtient :*

$$\sum_{\substack{p_1\cdots p_\ell\le x\\(a,p_1\cdots p_\ell)=1\\ \forall i,\ p_i\equiv 1(u_id_i)\\ a\in\mathfrak{R}\left(\prod\limits_{\substack{L\subset E'\\ i\in L}} k'_{L,p_i}\right)}} 1=\frac{\ell x}{\log x\prod\limits_i n_i}(\log\log x)^{\ell-1}+\mathcal{O}_{C_1,C_5}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right),$$

où $n_i:=[K_i:\mathbb{Q}]$.

Démonstration. On a

$$G(1,\boldsymbol{z})\gamma_0(\boldsymbol{z})=\prod_i\left(G_i(1,z_i)Z_i(1,z_i)\right)$$

Notons alors $\Lambda_i(z_i):=G_i(1,z_i)Z_i(1,z_i)$, i.e,

$$\Lambda_i(z_i)=\prod_{p\in P_i}\left(\left(1+\frac{z_i}{p}\right)\left(1-\frac{1}{p}\right)^{z_i}\right)\prod_{\substack{\mathfrak{p}\in O_{K_i}\\ N(\mathfrak{p})|au_id_i\\ N(\mathfrak{p})\text{ premier}}}\left(1-\frac{1}{N(\mathfrak{p})}\right)^{\frac{z_i}{n_i}}\beta_{K_i}^{\frac{z_i}{n_i}},\quad(2.16)$$

où $\beta_{K_i}:=\lim\limits_{s\to1}(s-1)\prod\limits_{\substack{\mathfrak{p}\in O_{K_i}\\ N(\mathfrak{p})\text{ premier}}}\left(1-\frac{1}{N(\mathfrak{p})}\right)$, qui est bien défini et non nul car ζ_{K_i} a un pôle simple en 1.
Soit Ω le produit de ℓ cercles autour de l'origine de rayon r, $\overline{1}:=(1,\dots,1)$. On a donc par la proposition 2.19,

$$\begin{aligned}\sum_{n\le x}c_{\overline{1}}(n)&=\sum_{n\le x}\frac{1}{(2i\pi)^\ell}\iint\limits_{\Omega}\frac{\alpha_{\boldsymbol{z}}(n)}{\prod\limits_i z_i^2}\prod_i dz_i\\&=\frac{1}{(2i\pi)^\ell}\iint\limits_{\Omega}A(x)\prod_i\frac{dz_i}{z_i^2}\\&=S+\mathcal{O}(E).\end{aligned}$$

où $S:=\frac{x}{(2i\pi)^\ell\log x}\iint_\Omega\frac{(\log x)^{\sum\limits_i\frac{z_i}{n_i}}}{\Gamma\left(\sum\limits_i\frac{z_i}{n_i}\right)}\prod\limits_i\Lambda_i(z_i)\frac{dz_i}{z_i^2}$,
et $E:=\frac{1}{(2\pi)^\ell}\iint_\Omega\left(x(\log x)^{\ell r-2}+xe^{-c_6\sqrt{\log x}}\right)\prod\limits_i\frac{dz_i}{|z_i|^2}$.

On a alors, en prenant $r = \frac{1}{\log\log x}$,

$$E \ll \frac{x(\log\log x)^\ell}{\log^2 x}.$$

Ensuite, on utilise la formule $\Gamma(u+1) = u\Gamma(u)$ avec $u = \sum_j \frac{z_j}{n_j}$ afin de s'écarter de la singularité de Γ en 0. De plus $\Lambda_i(0) = 1$, et ainsi en appliquant la formule de Cauchy :

$$\begin{aligned} S &= \frac{x}{(2i\pi)^\ell \log x} \sum_i \frac{1}{n_i} \oiint_\Omega \frac{(\log x)^{\sum_j \frac{z_j}{n_j}}}{\Gamma\left(\sum_j \frac{z_j}{n_j} + 1\right)} \Lambda_i(z_i) \frac{dz_i}{z_i} \prod_{j\neq i} \Lambda_j(z_j) \frac{dz_j}{z_j^2} \\ &= \frac{x}{(2i\pi)^{\ell-1} \log x} \sum_i \frac{1}{n_i} \oiint_{\Omega'} \frac{(\log x)^{\sum_{j\neq i} \frac{z_j}{n_j}}}{\Gamma\left(\sum_{j\neq i} \frac{z_j}{n_j} + 1\right)} \prod_{j\neq i} \Lambda_j(z_j) \frac{dz_j}{z_j^2}, \end{aligned}$$

où Ω' est le produit de $\ell - 1$ cercles autour de l'origine de rayon r.
On utilise la représentation de $\frac{1}{\Gamma}$ avec le contour de Hankel $\mathscr{H}$ ([37] ou [36], II.0.17),

$$\frac{1}{\Gamma(z)} = \frac{1}{2i\pi} \int_{\mathscr{H}} s^{-z} e^s ds,$$

où $\mathscr{H}$ est composé d'un cercle centré en 0 de rayon r privé du point $-r$ et de la demie-droite $]-\infty, -r]$ parcourue dans les deux sens.
On inverse les intégrales sur les z_j et sur ξ en notant que $\Lambda_j(z_j)$ est borné pour z_j borné, puis en appliquant la formule de Cauchy on a :

$$\begin{aligned} S &= \frac{x}{2i\pi \log x} \sum_i \frac{1}{n_i} \int_{\mathscr{H}} \prod_{j\neq i} \left(\frac{1}{2i\pi} \int_{|z_j|=r} \left(\frac{\log x}{\xi}\right)^{\frac{z_j}{n_j}} \Lambda_j(z_j) \frac{dz_j}{z_j^2} \right) \frac{e^\xi}{\xi} d\xi \\ &= \frac{x}{2i\pi \log x} \sum_i \frac{1}{n_i} \int_{\mathscr{H}} \prod_{j\neq i} \frac{\partial}{\partial z_j} \left(\left(\frac{\log x}{\xi}\right)^{\frac{z_j}{n_j}} \Lambda_j(z_j) \right)_{|z_j=0} \frac{e^\xi}{\xi} d\xi. \end{aligned}$$

Puis, comme $\Lambda_i(0) = 1$,

$$\frac{\partial}{\partial z_j} \left(\left(\frac{\log x}{\xi}\right)^{\frac{z_j}{n_j}} \Lambda_j(z_j) \right)_{|z_j=0} = \frac{\log\log x - \log\xi}{n_j} + \frac{\partial}{\partial z_j} \Lambda_j(0).$$

Pour la dérivée en zéro de $\Lambda_j(z_j)$ on calcul sa dérivée logarithmique :

$$\begin{aligned}\frac{\partial}{\partial z_j}\Lambda_j(0) = \frac{\Lambda_j'(0)}{\Lambda_j(0)} &= \sum_{p\in P_j}\left(\frac{1}{p}+\log\left(1-\frac{1}{p}\right)\right)\\ &+ \sum_{\substack{\mathfrak{p}\in O_{K_i}\\ N(\mathfrak{p})|au_id_i\\ N(\mathfrak{p})\text{ premier}}} \frac{1}{n_j}\log\left(1-\frac{1}{N(\mathfrak{p})}\right)+\frac{1}{n_j}\log(\beta_{K_j})\\ &= \mathcal{O}(u_id_i).\end{aligned}$$

Ainsi

$$\begin{aligned}S &= \frac{x}{2i\pi\log x}\sum_i\frac{1}{n_i}\int_{\mathscr{H}}\prod_{j\neq i}\left(\frac{\log\log x-\log\xi}{n_j}+\mathcal{O}(1)\right)\frac{e^\xi}{\xi}d\xi\\ &= \frac{\ell x}{\log x\prod_i n_i}(\log\log x)^{\ell-1}+\mathcal{O}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\int_{\mathscr{H}}\frac{e^{\Re\xi}}{|\xi|^{1-\varepsilon}}d\xi\right).\end{aligned}$$

On prend 1 pour le rayon du cercle autour de l'origine de $\mathscr{H}$, on obtient $\int_{\mathscr{H}}\frac{e^{\Re\xi}}{|\xi|^{1-\varepsilon}}d\xi \ll 1$, et donc

$$\sum_{\substack{p_1\cdots p_\ell\leq x\\ (a,p_1\cdots p_\ell)=1\\ \forall i,\ p_i\equiv 1(u_id_i)\\ a\in\mathfrak{R}\left(\prod_{\substack{L\subset E'\\ i\in L}}k'_L,p_i\right)}} 1 = \sum_{n\leq x}c_1(n) = \frac{\ell x}{\log x\prod_i n_i}(\log\log x)^{\ell-1}+\mathcal{O}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right). \tag{2.17}$$

□

2.6 Contrôle des termes d'erreur

Dans cette section nous traitons tous les termes d'erreur accumulés jusqu'ici, ce que nous regroupons dans la proposition suivante.

Proposition 2.21. *On a avec C_1 et C_5 des constantes arbitrairement grandes, $\varepsilon > 0$,*

$$\begin{aligned}\mathcal{N}_{a,\ell}(x, C_1) =& \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}\sum_{k}\mu(k)\mathcal{P}'_{a,0}(k) + \mathcal{O}\left(\frac{e^{(1+\varepsilon)C_1}x}{C_5^{1-\varepsilon}\log x}(\log\log x)^{\ell-1}\right)\\ &+ \mathcal{O}_{C_1,C_5}\left(\frac{x(\log\log x)^{\ell-2}}{\log x}\left(C_5\log C_5\right)^{2^\ell}\right)\\ &+ \mathcal{O}\left(\frac{x(\log\log x)^{\ell-1}}{C_5(\ell-1)!\log x}e^{\frac{C_1}{\log C_1}}\left(\log\log C_1\right)^{\ell}\right)\\ &+ \mathcal{O}\left(\frac{x(\log\log x)^{\ell-1}}{C_1^{1-\varepsilon}(\ell-1)!\log x}\right),\end{aligned}$$

où

$$\mathcal{P}'_{a,0}(k) = \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\}\\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}}\ \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\}\\ g_L\mid k_L^\infty\\ k_L\mid g_L}}\ \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\}\\ c_{iL}\mid \frac{g_L}{k_L}}}\ \sum_{\substack{\{d_i,\ i\in\{1,\dots,\ell\}\}\\ d_i\mid k}}\ \prod_{i\in\{1,\dots,\ell\}}\frac{\mu(d_i)}{n_i},$$

et $n_i := [\mathbb{Q}(\sqrt[k'_i]{a}, \xi_{u_i d_i}), \mathbb{Q}]$.

Démonstration. Rappelons que $\mathcal{N}_{a,\ell}(x, C_1) = \sum_{P^+(k)\le C_1}\mu(k)\mathcal{P}_a(x,k)$.

Commençons par majorer le terme d'erreur apporté par la proposition 2.8, il faut alors sommer sur les k sans facteur carré C_1-friables. Ainsi,

$$\sum_{P^+(k)\le C_1}\mu^2(k)\frac{x}{C_5^{1-\varepsilon}\log x}(\log\log x)^{\ell-1} \le \frac{2^{\pi(C_1)}x}{C_5^{1-\varepsilon}\log x}(\log\log x)^{\ell-1}.$$

C_1 et C_5 étant des constantes, la contribution des termes d'erreur issus de la proposition 2.20, est $\mathcal{O}_{C_1,C_5}\left(\frac{x(\log\log x)^{\ell-2}}{\log x}\left(C_5\log C_5\right)^{2^\ell}\right)$.
Il reste à estimer la somme associée aux termes principaux :

$$\begin{aligned}T :=& \sum_{P^+(k)\le C_1}\mu(k)\sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\}\\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}}\ \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\}\\ g_L\le C_5\\ g_L\mid k_L^\infty\\ k_L\mid g_L}}\\ &\sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\}\\ c_{iL}\mid \frac{g_L}{k_L}}}\ \sum_{\substack{\{d_i,\ i\in\{1,\dots,\ell\}\}\\ d_i\mid k}}\ \prod_{i\in\{1,\dots,\ell\}}\frac{\mu(d_i)}{n_i}.\end{aligned}$$

On souhaite enlever la condition $g \leq C_5$. Commençons par majorer

$$E_{L_0} := \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\setminus L_0\} \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{g_{L_0} > C_5 \\ g_{L_0} | k_{L_0}^\infty \\ k_{L_0} | g_{L_0}}} \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\} \\ c_{iL} | \frac{g_L}{k_L}}} \sum_{\substack{\{d_i,\ i\in\{1,\dots,\ell\}\} \\ d_i | k}} \prod_{i\in\{1,\dots,\ell\}} \frac{1}{n_i}.$$

Remarquons que pour $\varepsilon_1 > 0$, $\frac{1}{n_i} \ll \frac{1}{k_i \varphi(u_i d_i)} \ll \prod_{\substack{L\in\mathcal{P}^*(E) \\ i\in L}} \frac{1}{{g_L}^{1-\varepsilon_1}}$. En reportant dans E_{L_0} on obtient :

$$E_{L_0} = \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\setminus L_0\} \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{g_{L_0} > C_5 \\ g_{L_0} | k_{L_0}^\infty \\ k_{L_0} | g_{L_0}}} \tau(k)^\ell \prod_{L\in\mathcal{P}^*(E)} \left(\tau(g_L)^{|E\setminus L|} \left(\frac{1}{{g_L}^{1-\varepsilon_1}} \right)^{|L|} \right),$$

où τ est la fonction nombre de diviseurs. Soit $\varepsilon_2 > 0$, on utilise la majoration classique pour tout entier $\mathbf{n}$, $\tau(\mathbf{n}) \ll \mathbf{n}^{\varepsilon_2}$. De plus comme k est sans facteur carré et C_1-friable on a la majoration suivante : $k \ll e^{C_1}$. En reportant cela dans l'expression de E_{L_0} on obtient :

$$E_{L_0} \ll e^{\varepsilon_2 \ell C_1} \sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod_{L\in\mathcal{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\setminus L_0\} \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{g_{L_0} > C_5 \\ g_{L_0} | k_{L_0}^\infty \\ k_{L_0} | g_{L_0}}} \prod_{L\in\mathcal{P}^*(E)} \left(\frac{1}{{g_L}^{1-\varepsilon_1-\varepsilon_2}} \right).$$

Soient $L \neq L_0$, $\varepsilon_3 > 0$,

$$\sum_{\substack{g_L \\ g_L | k_L^\infty \\ k_L | g_L}} \frac{1}{{g_L}^{1-\varepsilon_1-\varepsilon_2}} \ll \prod_{p | k_L} \left(1 + \frac{1}{p^{1-\varepsilon_1-\varepsilon_2} - 1} \right) \ll (1+\varepsilon_3)^{\omega(k_L)} \ll e^{\varepsilon_3 C_1}.$$

Occupons nous de la somme sur g_{L_0}, soit $\varepsilon_4 > 0$ tel que $\varepsilon_1 + \varepsilon_2 + \varepsilon_4 < 1$, on a

$$\sum_{\substack{g_{L_0} > C_5 \\ g_{L_0} | k_{L_0}^\infty \\ k_{L_0} | g_{L_0}}} \frac{1}{{g_{L_0}}^{1-\varepsilon_1-\varepsilon_2}} \ll \frac{1}{C_5^{\varepsilon_4}} \sum_{g_{L_0} | k_{L_0}^\infty k_{L_0} | g_{L_0}} \frac{1}{{g_{L_0}}^{1-\varepsilon_1-\varepsilon_2-\varepsilon_4}} \ll \frac{e^{\varepsilon_3 C_1}}{C_5^{\varepsilon_4}}.$$

Soit $\varepsilon_5 > \varepsilon_2 + \varepsilon_3$, en reportant dans E_{L_0},

$$E_{L_0} \ll \frac{2^{C_1} e^{(\varepsilon_2+\varepsilon_3)\ell C_1}}{C_5^{\varepsilon_4}} \ll \frac{e^{\varepsilon_5 \ell C_1}}{C_5^{\varepsilon_4}}.$$

Puis comme le nombre de C_1-friable sans facteur carré est majoré par e^{C_1} on a la majoration souhaitée.
Il ne reste qu'à compléter la somme sur les k.
La somme que l'on souhaite majorer est :

$$E_{C_1} := \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x} \sum_{\substack{P^+(k)>C_1 \\ \mu^2(k)=1}} \sum_{\{k_L,\ L\in\mathcal{P}^*(E)\}\ \prod_{L\in\mathcal{P}^*(E)} k_L=k} \sum_{\{g_L,\ L\in\mathcal{P}^*(E)\}\ \substack{g_L | k_L^\infty \\ k_L | g_L}}$$
$$\sum_{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\}\ \substack{c_{iL} | \frac{g_L}{k_L}}} \sum_{\{d_i,\ i\in\{1,\dots,\ell\}\}\ d_i | k} \prod_{i\in\{1,\dots,\ell\}} \frac{1}{n_i}.$$

Soit $\varepsilon_1 > 0$, on a la majoration suivante pour tout i : $\frac{1}{n_i} \ll \frac{1}{d_i^{1-\varepsilon_1} \prod\limits_{L,\ i\in L} k_L g_L^{1-\varepsilon_1}}$.
On majore simplement les sommes sur le d_i :

$$\sum_{d_i|k} \frac{1}{d_i^{1-\varepsilon_1}} = \prod_{p|k} \left(1 + \frac{1}{p^{1-\varepsilon_1}}\right) \ll \left(\frac{k}{\varphi(k)}\right)^{1-\varepsilon_1} \ll (\log\log k)^{1-\varepsilon_1}.$$

Soit $\varepsilon_2 > 0$, pour tous i et L la somme sur $c_{i,L}$ est petite devant $\left(\frac{g_L}{k_L}\right)^{\varepsilon_2}$.
Notons $\varepsilon_3 = \ell(\varepsilon_1 + \varepsilon_2)$, et choisissons ε_1 et ε_2 de sorte que $0 < \varepsilon_3 < 1$. Les sommes sur les g_L sont alors :

$$\sum_{\substack{g_L | k_L^\infty \\ k_L | g_L}} \frac{1}{g_L^{|L|(1-\varepsilon_1)-|E\setminus L|\varepsilon_2}} \ll \frac{1}{k_L^{|L|-\varepsilon_3}} \sum_{g_L | k_L^\infty} \frac{1}{g_L^{|L|-\varepsilon_3}} \ll \prod_{p|k_L} \frac{1}{p^{|L|-\varepsilon_3}-1}.$$

Soit $\varepsilon_4 > 0$ tel quel $\varepsilon_4 > \varepsilon_3$, en reportant dans E_{C_1} on obtient :

$$E_{C_1} \ll \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x} \sum_{\substack{P^+(k)>C_1 \\ \mu^2(k)=1}} (\log\log k)^{\ell(1-\varepsilon_1)} \sum_{\{k_L,\ L\in\mathcal{P}^*(E)\}\ \prod_{L\in\mathcal{P}^*(E)} k_L=k} \prod_{p|k_L} \frac{1}{p^{|L|}(p^{|L|-\varepsilon_3}-1)}$$
$$\ll \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x} \sum_{\substack{P^+(k)>C_1 \\ \mu^2(k)=1}} (\log\log k)^{\ell(1-\varepsilon_1)} \sum_{\{k_L,\ L\in\mathcal{P}^*(E)\}\ \prod_{L\in\mathcal{P}^*(E)} k_L=k} \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{k_L^{2|L|-\varepsilon_4}}\right).$$

Posons $f(k) := \mu^2(k) \sum\limits_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\} \\ \prod\limits_{L\in\mathcal{P}^*(E)} k_L = k}} \prod\limits_{L\in\mathscr{P}^*(E)} \left(\frac{1}{k_L^{2|L|-\varepsilon_4}}\right)$, alors f est multiplicative et pour p premier,

$$f(p) = \sum_{m=1}^{\ell} \binom{l}{m} \frac{1}{p^{2m-\varepsilon_4}} = p^{\varepsilon_4} \sum_{m=0}^{\ell-1} \binom{l}{m} p^{2(m-l)} = \frac{1}{p^{2-\varepsilon_4}} \left(1+\frac{1}{p^2}\right)^{\ell-1}.$$

Ainsi $f(k) = \frac{1}{k^{2-\varepsilon_4}} \prod\limits_{p|k} \left(1+\frac{1}{p^2}\right)^{\ell-1} \ll \frac{1}{k^{2-\varepsilon_4}}$.
Soit $\varepsilon_5 > \varepsilon_4$, en reportant le résultat précédent dans E_{C_1} on a :

$$E_{C_1} \ll \frac{x(\log\log x)^{\ell-1}}{C_1^{1-\varepsilon_5}(\ell-1)!\log x}.$$

Or on peut prendre ε_1 et ε_2 arbitrairement petits et donc par extension ε_5 aussi, ce qui permet de conclure.

□

Il ne nous reste alors plus qu'à évaluer le terme principal.

2.7 Calcul du terme principal

Dans cette section on notera pour tout nombre premier $p \geq 3$ et tout entier $i \geq 1$ $R_p(i) := \sum\limits_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j (p-1)^{\ell-i-j}}{(p^{i+j}-1)(p-2)^{\ell-i}}$ et pour tout entier $i \geq 1$, $R_2(i) := \sum\limits_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j 2^{-j}}{2^{i+j}-1}$.
On veut calculer : $\sum\limits_k \mu(k)\mathcal{P}'_{a,0}(k)$, avec

$$\mathcal{P}'_{a,0}(k) = \sum_{\substack{\prod\limits_{L\in\mathscr{P}^*(E)} k_L = k}} \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)} \\ g_L | k_L^\infty \\ k_L | g_L}} \sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)} \\ b\notin L \\ c_{bL} | \frac{g_L}{k_L}}} \sum_{\substack{\{d_i\}_{i\in E} \\ d_i | k}} \prod_{i\in E} \frac{\mu(d_i)}{n_i}$$

où $\mathscr{P}^*(E) := \{L \subset E,\ L \neq \emptyset\}$ et $n_i := n(\prod\limits_{\substack{L\in\mathscr{P}^*(E) \\ i\in L}} k'_L, u_i d_i)$ le degré de l'extension K_i, où $k'_L = \frac{k_L}{(h,k_L)}$, avec h impair, dépendant de a.

D'après la proposition 2.14, $n(\ell,m) := [\mathbb{Q}(\sqrt[\ell]{a},\xi_m),\mathbb{Q}] = \frac{\ell\varphi(m)}{\varepsilon(\ell,m)}$ où ℓ est sans facteur carré, $\ell|m$ et

$$\varepsilon(\ell,m) = \begin{cases} 2 \text{ si } 2|\ell,\ 2|m,\ a_1|m \text{ et } a_1 \equiv 1 \mod 4 \\ 2 \text{ si } 2|\ell,\ 4|m,\ a_1|m \text{ et } a_1 \equiv 3 \mod 4 \\ 2 \text{ si } 2|\ell,\ 8|m,\ a_1|m \text{ et } a_1 \equiv 0 \mod 2 \\ 1 \text{ sinon} \end{cases}.$$

Notons alors $u_i := \prod_{\substack{L\in\mathscr{P}^*(E)\\ i\in L}} g_L \prod_{\substack{L\in\mathscr{P}^*(E)\\ i\notin L}} c_{iL}$.

Le résultat principal sera la proposition suivante, en sommant les $\mathcal{P}'_{a,0}(k)$ sur les k.

Proposition 2.22. *On obtient :*

$$\sum_k \mu(k)\mathcal{P}'_{a,0}(k) = M(E)\left(1+V_\ell(a_1)\right)$$

où

- $M(E) := (1-H_1(E))\prod_{\substack{p\\ p\geq 3}}\left(1-\left(\frac{p-2}{p-1}\right)^\ell \sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)\right)$, *est la contribution ne dépendant que de h,*
- $V_\ell(a_1) := \mu(2\tilde{a_1})^{\frac{H_2(\ell,a_1)}{1-H_1(E)}}\prod_{\substack{p\\ p|a_1\\ p\geq 3}}\left(1-\left(\frac{p-2}{p-1}\right)^\ell \sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)\right)^{-1}$, *est la contribution spécifique dépendant de a,*
- $\tilde{a_1} := \frac{a_1}{(2,a_1)}$,
- *Les F_i sont des fonctions multiplicatives définies pour les nombres premiers impairs par :*

$$F_i(p) := \left(\frac{(h,p)(p-1)}{p^2(p-2)}\right)^i (1+R_p(i))$$

- $H_1(E) := 2^{-\ell}\left(\sum_{i=1}^{\ell}\binom{\ell}{i}2^{-2i}\left(1+2^{\ell-i}R_2(i)\right)+2^{-\ell}\right)$, *la contribution à $M(E)$ de $p=2$,*

•

$$H_2(\ell, a_1) := \sum_{L_0 \in \mathscr{P}^*(E)} 2^{-\ell-|L_0|} \sum_{L_1 \in \mathscr{P}^*(L_0)} \delta_5(L_0, L_1)\mu(\tilde{a_1})^{|L_1|} \prod_{\substack{p|\tilde{a_1} \\ p\geq 3}} \left(\frac{(p-2)^{\ell-|L_1|}}{(p-1)^{\ell}}\right) \underset{L\in\mathscr{P}^*(E)}{*} \left(G_L^{L_1}\right)(\tilde{a_1})$$

la contribution de a à $V_\ell(a_1)$, avec $\delta_5(L_0, L_1) = \widehat{\delta}(L_0, L_1) + \tilde{\delta}(L_0, L_1)$,

$$\widehat{\delta}(L_0, L_1) = \begin{cases} 2^{-|L_0|}\left((-1)^{|L_1|} + 2^{\ell-|L_0|}R_2(|L_0|)\right) & \text{si } a_1 \equiv 0 \mod 2, \\ 2^{-|L_0|}\left(1 + 2^{\ell-|L_0|}R_2(|L_0|)\right) & \text{sinon,} \end{cases}$$

$$\tilde{\delta}(L_0, L_1) = \begin{cases} 1 \text{ si } L_0 = E \text{ et } a_1 \equiv 1 \mod 4, \\ (-1)^{|L_1|} \text{ si } L_0 = E \text{ et } a_1 \equiv 3 \mod 4, \\ 0 \text{ sinon,} \end{cases}$$

les $G_L^{L_1}$ sont des fonctions multiplicatives définies pour les nombres premiers impairs par :

$$G_L^{L_1}(p) := \left(\frac{(p-1)(h,p)}{p^2(p-2)}\right)^{|L|} (2-p)^{|L_1\cap L|}\left(1 + R_p(|L\cup L_1|)\right),$$

et $\underset{L\in\mathscr{P}^*(E)}{*}\left(G_L^{L_1}\right)(\tilde{a_1})$ désigne la convolution de toutes fonctions $G_L^{L_1}$ prise en a_1.

Afin de démontrer cette proposition nous allons expliciter $\mathcal{P}_{a,0}(k)$ en fonction de la parité de k.

2.7.1 $\mathcal{P}'_{a,0}(k)$ pour k impair

Nous commençons par démontrer un lemme sur la somme sur les diviseurs d'un entier sans facteur carré d'une certaine fonction.

Lemme 2.23. *Soit α un entier, β un entier sans facteur carré, alors*

$$\sum_{d|\beta} \frac{\mu(d)}{\varphi(\alpha d)} = \frac{1}{\varphi(\alpha)} \prod_{\substack{p|\beta \\ p|\alpha}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|\beta \\ p\nmid\alpha}} \left(1 - \frac{1}{p-1}\right).$$

Démonstration. On a trivialement,

$$\sum_{d|\beta} \frac{\mu(d)}{\varphi(\alpha d)} = \frac{1}{\varphi(\alpha)} \sum_{d|\beta} \frac{\mu(d)\varphi(\alpha)}{\varphi(\alpha d)}.$$

La fonction $d \to \frac{\mu(d)\varphi(\alpha)}{\varphi(\alpha d)}$ est multiplicative et on a pour $p|\alpha$, $\frac{\mu(p)\varphi(\alpha)}{\varphi(\alpha p)} = -\frac{1}{p}$ et pour $p \nmid \alpha$, $\frac{\mu(p)\varphi(\alpha)}{\varphi(\alpha p)} = -\frac{1}{p-1}$. On obtient alors la formule en exprimant la somme sur les diviseurs de β sous forme de produit eulérien. □

Proposition 2.24. *Pour k impair, sans facteur carré, on a :*

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^{\ell} \underset{i=1}{\overset{\ell}{\ast}} \left(F_i^{*\binom{\ell}{i}}\right)(k),$$

où $F^{*n} := \underbrace{F * \cdots * F}_{n \ fois}$.

Démonstration. Comme k est impair, les k_L le sont aussi et donc $\forall i$, le terme correctif de n_i vérifie :

$$\varepsilon(\prod_{\substack{L\in\mathscr{P}^*(E) \\ i\in L}} k'_L, u_i d_i) = 1.$$

Nous allons calculer successivement les sommes sur les d_i, $c_{i,L}$ et g_L. En utilisant le lemme 2.25, celles sur les d_i sont de la forme :

$$\begin{aligned}\sum_{d|k} \frac{\mu(d)}{\varphi(u_i d)} &= \frac{1}{\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i \\ p\geq 3}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|k \\ p\nmid u_i \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right) \\ &= \frac{1}{\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right).\end{aligned}$$

On décompose u_i en $\prod_{\substack{L\in\mathscr{P}^*(E) \\ i\in L}} g_L \prod_{\substack{L\in\mathscr{P}^*(E) \\ i\notin L}} c_{iL}$.
Rappelons que g_L et k_L ont les mêmes facteurs premiers et que ceux de $c_{i,L}$ divisent k_L.

La somme sur les d_i devient pour $1 \leq i \leq \ell$:

$$\sum_{d_i|k} \frac{\mu(d)}{\varphi(u_i d_i)} = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{L\in\mathcal{P}^*(E) \\ i\in L}} \left(\frac{1}{\varphi(g_L)} \prod_{\substack{p|k_L \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) \right) \prod_{\substack{L\in\mathcal{P}^*(E) \\ i\notin L}} \left(\frac{1}{\varphi(c_{i,L})} \prod_{\substack{p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) \right).$$

On calcule ensuite le produit pour $i = 1, \ldots, \ell$ de cette expression.

$$\prod_{i=1}^{\ell} \left(\sum_{d_i|k} \frac{\mu(d)}{\varphi(u_i d_i)} \right) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^{\ell} \prod_{L\in\mathcal{P}^*(E)} \left(\frac{1}{\varphi(g_L)} \prod_{\substack{p|k_L \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) \right)^{|L|} \prod_{L\in\mathcal{P}^*(E)} \prod_{\substack{i=1 \\ i\notin L}}^{\ell} \left(\frac{1}{\varphi(c_{i,L})} \prod_{\substack{p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) \right).$$

En reportant cela dans $\mathcal{P}'_{a,0}(k)$ on obtient :

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^{\ell} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{{k'_L}^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right)^{|L|} \right) \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)} \\ g_L | k_L^{\infty} \\ k_L | g_L}} \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{\varphi(g_L)^{|L|}} \prod_{\substack{i\in E \\ i\notin L}} \left(\sum_{c | \frac{g_L}{k_L}} \frac{1}{\varphi(c)} \prod_{\substack{p|c \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) \right) \right).$$

Calculons la somme sur c à part en l'exprimant sous forme de produit eulérien, et en posant pour p un nombre premier ≥ 2 et n un entier $f_p(n) := 1 + \frac{1-p^{-n}}{p-2} = \frac{p-1-p^{-n}}{p-2}$,

$$\sum_{c|\frac{g_L}{k_L}} \frac{1}{\varphi(c)} \prod_{\substack{p|c \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) = \prod_{\substack{p|\frac{g_L}{k_L} \\ p\geq 3}} \left(1 + \frac{p-1}{p-2} \sum_{n=1}^{\nu_p(g_L)-1} \frac{1}{p^n} \right)$$
$$= \prod_{\substack{p|k_L \\ p\geq 3}} f_p(\nu_p(g_L) - 1).$$

Alors en reprenant $\mathcal{P}'_{a,0}(k)$:

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^{\ell} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{{k'_L}^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right)^{|L|} \right)$$
$$\prod_{L\in\mathscr{P}^*(E)} \left(\sum_{\substack{g|k_L^\infty \\ k_L|g}} \frac{1}{\varphi(g)^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(f_p(\nu_p(g_L) - 1)\right)^{\ell-|L|} \right). \tag{2.18}$$

Puis, comme pour c, calculons la somme sur g en commençant par se débarrasser de la condition $k_L|g$:

$$\sum_{\substack{g|k_L^\infty \\ k_L|g}} \frac{1}{\varphi(g)^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(f_p(\nu_p(g_L) - 1)\right)^{\ell-|L|} = \frac{1}{\varphi(k_L)^{|L|}} \sum_{g|k_L^\infty} \frac{1}{g^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(f_p(\nu_p(g_L))\right)^{\ell-|L|}$$
$$= \frac{1}{\varphi(k_L)^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(1 + \sum_{n=1}^{\infty} \left(\frac{1}{p^{n|L|}} \left(f_p(n)\right)^{\ell-|L|} \right) \right).$$

Pour exprimer la somme à l'intérieur du produit on applique la formule du binôme puis celle des sommes géométriques, et en posant pour n un entier strictement positif $R_p(n) := \sum_{j=0}^{\ell-n} \binom{\ell-n}{j} \frac{(-1)^j (p-1)^{\ell-n-j}}{(p^{j+n}-1)(p-2)^{\ell-n}}$ on obtient :

$$\sum_{\substack{g|k_L^\infty \\ k_L|g}} \frac{1}{\varphi(g)^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(1 + \frac{1-p^{-\nu_p(g)+1}}{p-2}\right)^{\ell-|L|}$$
$$= \frac{1}{\varphi(k_L)^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} (1 + R_p(|L|)) . \tag{2.19}$$

Alors en reportant (2.19) dans (2.18) :

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^{\ell} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k}$$
$$\prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{{k'_L}^{|L|} \varphi(k_L)^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|} (1 + R_p(|L|)) \right) . \tag{2.20}$$

Définissons pour tout $1 \leq i \leq \ell$ les fonctions multiplicatives F_i par :

$$F_i(p) := \left(\frac{(h,p)(p-1)}{p^2(p-2)}\right)^i (1 + R_p(i)) ,$$

pour $p \geq 3$.
Enfin en exprimant la somme sur les k_L de (2.20) sous forme de produit eulérien, on obtient bien :

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^{\ell} \overset{\ell}{\underset{i=1}{\ast}} \left(F_i^{*\binom{\ell}{i}}\right)(k) . \tag{2.21}$$

□

2.7.2 Découpage selon le diviseur pair de k parmi les k_L.

Pour le cas pair nous allons introduire une somme sur les sous-ensembles non-vides de E afin de distinguer le $L_0 \subset E$ tel que $2|k_{L_0}$. Par souci de lisibilité nous noterons $k'_i := \prod_{\substack{L\in\mathscr{P}^*(E)\\ i\in L}} k'_L$. Ainsi,

$$\mathcal{P}'_{a,0}(k) = \sum_{L_0\in\mathscr{P}^*(E)} \sum_{\substack{\prod_{L\in\mathscr{P}^*(E)} k_L = k}} \mathbb{1}(2|k_{L_0}) \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)}\\ g_L|k_L^\infty\\ k_L|g_L}} \sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}|\frac{g_L}{k_L}}} \prod_{i\in E}\left(\sum_{d|k} \frac{\mu(d)\varepsilon\left(k'_i, u_i d\right)}{\varphi(u_i d)k'_i}\right)$$

$$= \sum_{L_0\in\mathscr{P}^*(E)} \sum_{\substack{\prod_{L\in\mathscr{P}^*(E)} k_L = k}} \mathbb{1}(2|k_{L_0}) \prod_{L\in\mathscr{P}^*(E)}\left(\frac{1}{{k'_L}^{|L|}}\right) \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)}\\ g_L|k_L^\infty\\ k_L|g_L}} S_c, \qquad (2.22)$$

où $S_c := \sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}|\frac{g_L}{k_L}}} \prod_{i\in E}\left(\sum_{d|k} \frac{\mu(d)\varepsilon\left(k'_i, u_i d\right)}{\varphi(u_i d)}\right)$.

Afin de calculer les dernières sommes sur les diviseurs de k nous utilisons le lemme suivant.

Lemme 2.25. *On a :*

$$\sum_{d|k} \frac{\mu(d)\varepsilon\left(k'_i, u_i d\right)}{\varphi(u_i d)} = \frac{1}{2\varphi(u_i)} \prod_{\substack{p|k\\ p|u_i\\ p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|k\\ p\geq 3}}\left(1-\frac{1}{p-1}\right) B(i, L_0)$$

où

$$B(i,L_0) := \begin{cases} \mathbb{1}(2|c_{i,L_0}) & \text{si } i\in E\backslash L_0,\\ 1+\mathbb{1}(2\tilde{a_1}|k)\delta_2(g_{L_0})\mu(\tilde{a_1})\mu\left((\tilde{a_1},u_i)\right)\prod_{\substack{p|\tilde{a_1}\\ p\nmid u_i\\ p\geq 3}}\left(\frac{1}{p-2}\right) & \text{si } i\in L_0. \end{cases},$$

$$\delta_2(g_{L_0}) = \begin{cases} 1 \text{ si } \nu_2(g_{L_0}) \geq s(a_1) \\ -1 \text{ si } \nu_2(g_{L_0}) = s(a_1)-1 \\ 0 \text{ sinon} \end{cases},$$

avec $\tilde{a_1} := a_1/(2,a_1)$ *et* $s(a_1) := \begin{cases} 1 \text{ si } a_1 \equiv 1 \mod 4,\\ 2 \text{ si } a_1 \equiv 3 \mod 4,\\ 3 \text{ si } a_1 \equiv 0 \mod 2. \end{cases}$

Démonstration. Notons $b := 2^{s(a_1)}\tilde{a_1}$, on a

$$\varepsilon(\ell, m) = \begin{cases} 2 \text{ si } 2|\ell, \text{et } b|m \\ 1 \text{ sinon.} \end{cases}$$

Alors si $i \in E\backslash L_0$, k_i' est impair et donc $\varepsilon(k_i', u_i d_i) = 1$. Ce qui nous donne :

$$\sum_{d|k} \frac{\mu(d)\varepsilon\left(k_i', u_i d\right)}{\varphi(u_i d)} = \sum_{d|k} \frac{\mu(d)}{\varphi(u_i d)} = \frac{1}{\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|k \\ p\nmid u_i}} \left(1 - \frac{1}{p-1}\right).$$

Puis en traitant à part la contribution donnée par $p = 2$:

$$\sum_{d|k} \frac{\mu(d)\varepsilon\left(k_i', u_i d\right)}{\varphi(u_i d)} = \mathbb{1}(2|c_{i,L_0}) \frac{1}{2\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right), \tag{2.23}$$

car $\prod\limits_{\substack{p|k \\ p\nmid u_i}} \left(1 - \frac{1}{p-1}\right) = 0$ si $2 \nmid u_i$, c'est-à-dire si $2 \nmid c_{i,L_0}$.

Puis, lorsque $i \in L_0$, $\varepsilon(k_i', u_i d) = 1 + \mathbb{1}(b|u_i d)$, ainsi, en utilisant le lemme 2.23 :

$$\begin{aligned} \sum_{d|k} \frac{\mu(d)\varepsilon\left(k_i', u_i d\right)}{\varphi(u_i d)} &= \sum_{d|k} \frac{\mu(d)}{\varphi(u_i d)} + \sum_{\substack{d|k \\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)} \\ &= \frac{1}{2\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right) + \sum_{\substack{d|k \\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)}. \end{aligned} \tag{2.24}$$

Calculons cette dernière somme, en notant que si b divise $u_i d$ alors $\frac{b}{(b,u_i)}$ divise d et a fortiori k.

$$\sum_{\substack{d|k \\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)} = \mathbb{1}\left(\frac{b}{(u_i, b)}|k\right) \sum_{d'|k/\frac{b}{(u_i,b)}} \frac{\mu(d'\frac{b}{(u_i,b)})}{\varphi(u_i d'\frac{b}{(u_i,b)})}.$$

Puis comme k est sans facteur carré, les diviseurs d' de la somme précédente vérifient $\left(\frac{b}{(b,u_i)}, d'\right) = 1$, ainsi, en appliquant le lemme 2.23 :

$$\begin{aligned}\sum_{\substack{d|k \\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)} &= \mathbb{1}\left(\frac{b}{(u_i,b)}|k\right) \frac{\mu\left(\frac{b}{(u_i,b)}\right)}{\varphi\left(u_i \frac{b}{(u_i,b)}\right)} \sum_{d'|k/\frac{b}{(u_i,b)}} \frac{\mu(d')\varphi\left(u_i \frac{b}{(u_i,b)}\right)}{\varphi(u_i d' \frac{b}{(u_i,b)})} \\ &= \mathbb{1}\left(\frac{b}{(u_i,b)}|k\right) \frac{\mu\left(\frac{b}{(u_i,b)}\right)}{\varphi\left(u_i \frac{b}{(u_i,b)}\right)} \prod_{\substack{p|\frac{k(u_i,b)}{b} \\ p|u_i}} \left(1-\frac{1}{p}\right) \prod_{\substack{p|\frac{k(u_i,b)}{b} \\ p\nmid u_i}} \left(1-\frac{1}{p-1}\right).\end{aligned} \tag{2.25}$$

Décomposons chaque élément de cette dernière égalité :

$$\mathbb{1}\left(\frac{b}{(u_i,b)}|k\right) = \mathbb{1}(2\tilde{a_1}|k)\mathbb{1}(\nu_2(g_{L_0}) \geq s(a_1) - 1), \tag{2.26}$$

car $\nu_2\left(\frac{b}{(b,u_i)}\right) = s(a_1) - \min\left(\nu_2(g_{L_0}), s(a_1)\right)$ et $\nu_2(k) = 1$.

Alors, comme on a $\nu_2(g_{L_0}) \geq s(a_1) - 1$ cela implique que :

$$\mu\left(\frac{b}{(u_i,b)}\right) = \mu(\tilde{a_1})\mu\left((\tilde{a_1}, u_i)\right)\mu\left(2^{\mathbb{1}\left(\nu_2(g_{L_0}) = s(a_1)-1\right)}\right). \tag{2.27}$$

Puis, comme $2||\frac{b}{(u_i,b)}$ ou $2 \nmid \frac{b}{(u_i,b)}$,

$$\begin{aligned}\frac{1}{\varphi\left(u_i \frac{b}{(u_i,b)}\right)} &= \frac{1}{\varphi(u_i)\varphi\left(\frac{b}{(u_i,b)}\right)} \left(1 - \frac{1}{2}\mathbb{1}\left(\nu_2(g_{L_0}) = s(a_1) - 1\right)\right) \\ &= \frac{1}{\varphi(u_i)\varphi\left(\frac{\tilde{a_1}}{(u_i,\tilde{a_1})}\right)} \left(1 - \frac{1}{2}\mathbb{1}\left(\nu_2(g_{L_0}) = s(a_1) - 1\right)\right),\end{aligned}$$

et en rappelant que $\tilde{a_1}$ est sans facteur carré on obtient :

$$\frac{1}{\varphi\left(u_i \frac{b}{(u_i,b)}\right)} = \frac{1}{\varphi(u_i)} \prod_{\substack{p|\tilde{a_1} \\ p\nmid u_i}} \left(\frac{1}{p-1}\right) \left(1 - \frac{1}{2}\mathbb{1}\left(\nu_2(g_{L_0}) = s(a_1) - 1\right)\right). \tag{2.28}$$

Décomposons ensuite les deux produits de (2.25) :

$$\prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p|u_i}}\left(1-\frac{1}{p}\right)=\prod_{\substack{p|k\\ p|u_i}}\left(1-\frac{1}{p}\right)\prod_{\substack{p|\frac{b}{(u_i,b)}\\ p|u_i}}\left(1-\frac{1}{p}\right)^{-1},$$

or pour $p\geq 3$, $\nu_p(b)\leq 1$ et ainsi $\nu_p\left(u_i,\frac{b}{(u_i,b)}\right)=0$, donc

$$\prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p|u_i}}\left(1-\frac{1}{p}\right)=\frac{1}{2}\prod_{\substack{p|k\\ p|u_i\\ p\geq 3}}\left(1-\frac{1}{p}\right)\left(1+\mathbb{1}\left(\nu_2(g_{L_0})=s(a_1)-1\right)\right). \tag{2.29}$$

et, comme $2|u_i$,

$$\begin{aligned}\prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)&=\prod_{\substack{p|k\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p|\frac{b}{(u_i,b)}\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)^{-1}\\ &=\prod_{\substack{p|k\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p|\tilde{a_1}\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)^{-1}.\end{aligned} \tag{2.30}$$

Notons :

$$\delta_2(g_{L_0})=\begin{cases}1 \text{ si } \nu_2(g_{L_0})\geq s(a_1)\\ -1 \text{ si } \nu_2(g_{L_0})=s(a_1)-1\\ 0 \text{ sinon}\end{cases}$$

Ainsi en reprenant (2.26), (2.27), (2.28), (2.29) et (2.30) dans (2.25) :

$$\begin{aligned}\sum_{\substack{d|k\\ b|u_id}}\frac{\mu(d)}{\varphi(u_id)}=&\mathbb{1}(2\tilde{a_1}|k)\delta_2(g_{L_0})\frac{\mu(\tilde{a_1})\mu\left((\tilde{a_1},u_i)\right)}{2\varphi(u_i)}\\ &\prod_{\substack{p|\tilde{a_1}\\ p\nmid u_i\\ p\geq 3}}\left(\frac{1}{p-2}\right)\prod_{\substack{p|k\\ p|u_i\\ p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right)\prod_{\substack{p|k\\ p\geq 3}}\left(1-\frac{1}{p-1}\right).\end{aligned} \tag{2.31}$$

Ce qui, en reprenant (2.23) et (2.24), permet de conclure.

□

On a donc dans l'expression (2.22) de $\mathcal{P}'_{a,0}(k)$ un terme $\prod_{i\in E} B(i,L_0)$, intéressons-nous dans ce dernier au produit sur les $i \in L_0$. Nous développons le produit $\prod_{i\in E} B(i,L_0)$ ce qui nous amène à introduire une somme sur les sous-ensembles $L_1 \subset L_0$ non vides.

$$\prod_{i\in L_0}\left(1+\mathbb{1}(2\tilde{a_1}|k)\delta_2(g_{L_0})\mu(\tilde{a_1})\mu\left((\tilde{a_1},u_i)\right)\prod_{\substack{p|\tilde{a_1}\\ p\nmid u_i\\ p\geq 3}}\left(\frac{1}{p-2}\right)\right)$$

$$=1+\sum_{L_1\in\mathscr{P}^*(L_0)}\mathbb{1}(2\tilde{a_1}|k)\delta_2(g_{L_0})^{|L_1|}\mu(\tilde{a_1})^{|L_1|}\prod_{\substack{p|\tilde{a_1}\\ p\geq 3}}\left(\frac{1}{p-2}\right)^{|L_1|}\prod_{i\in L_1}\left(\prod_{\substack{p|\tilde{a_1}\\ p|u_i\\ p\geq 3}}(2-p)\right), \tag{2.32}$$

car $\mu\left((\tilde{a_1},u_i)\right)=\prod_{\substack{p|\tilde{a_1}\\ p|u_i}}(-1)$. Notons $\mathcal{P}'_\alpha(k)$ la contribution à $\mathcal{P}'_{a,0}(k)$ du terme 1 dans l'expression qui précède, et $\mathcal{P}'_\beta(k)$ la contribution à $\mathcal{P}'_{a,0}(k)$ du terme $\sum_{L_1\in\mathscr{P}^*(L_0)}\mathbb{1}(2\tilde{a_1}|k)\delta_2(g_{L_0})^{|L_1|}\mu(\tilde{a_1})^{|L_1|}\prod_{\substack{p|\tilde{a_1}\\ p\geq 3}}\left(\frac{1}{p-2}\right)^{|L_1|}\prod_{i\in L_1}\left(\prod_{\substack{p|\tilde{a_1}\\ p|u_i\\ p\geq 3}}(2-p)\right)$. Les deux prochains paragraphes ont pour objectif d'évaluer ces deux quantités.

2.7.3 Évaluation de $\mathcal{P}'_\alpha(k)$.

L'évaluation de $\mathcal{P}'_\alpha(k)$ est semblable à celle de $\mathcal{P}'_{a,0}(k)$ dans le cas k impair, nous allons exprimer successivement les sommes sur les $c_{i,L}$, g_L et k_L en produits eulériens.

Proposition 2.26. *On a, en reprenant les définitions de H_1 et F_i de la proposition 2.22,*

$$\mathcal{P}'_\alpha(k) = H_1(E) \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^\ell \overset{\ell}{\underset{i=1}{\ast}} \left(F_i^{*\binom{\ell}{i}}\right) \left(\frac{k}{2}\right).$$

où $F_i^{*\binom{\ell}{i}}$ désigne la convolution de F_i avec elle-même $\binom{\ell}{i}$ fois, et $\overset{\ell}{\underset{i=1}{\ast}} \left(F_i^{*\binom{\ell}{i}}\right)$ désigne la convolution de toutes fonctions $F_i^{*\binom{\ell}{i}}$.

Démonstration. Commençons par expliciter $\mathcal{P}'_\alpha(k)$ en utilisant le lemme 2.25, on obtient

$$\begin{aligned}\mathcal{P}'_\alpha(k) :=& \alpha_1(k) \sum_{L_0 \in \mathscr{P}^*(E)} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)} \\ g_L | k_L^\infty \\ k_L | g_L}} \\ & \prod_{L\in\mathscr{P}^*(E)} \Big(\alpha_2(k_L)\alpha_3(g_L)\Big) \sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)} \\ b\notin L \\ c_{bL} | \frac{g_L}{k_L}}} \prod_{\substack{\{i,L\} \\ L\in\mathscr{P}^*(E) \\ i\notin L}} \alpha_4(c_{i,L}), \end{aligned} \tag{2.33}$$

où

- $\alpha_1(k) := 2^{-\ell} \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^\ell$,
- $\alpha_2(k_L) := \begin{cases} \frac{\mathbb{1}(2|k_{L_0})}{{k'_{L_0}}^{|L_0|}} \prod_{\substack{p|k_{L_0} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L_0|} & \text{si } L = L_0, \\ \frac{1}{{k'_L}^{|L|}} \prod_{\substack{p|k_L \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|} & \text{sinon,} \end{cases}$,
- $\alpha_3(g_L) := \frac{1}{\varphi(g_L)^{|L|}}$,
- $\alpha_4(c_{i,L}) := \begin{cases} \frac{\mathbb{1}(2|c_{i,L_0})}{\varphi(c_{i,L})} \prod_{\substack{p|k \\ p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) & \text{si } L = L_0, \\ \frac{1}{\varphi(c_{i,L})} \prod_{\substack{p|k \\ p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) & \text{sinon,} \end{cases}$.

Occupons-nous d'abord des somme sur les c, pour ce faire on introduit une autre fonction indicatrice pour tenir compte des $\mathbb{1}(2|c_{i,L_0})$:

$$\delta_3(g_{L_0}) = \begin{cases} \left(2\left(1-2^{-\nu_2(g_{L_0})+1}\right)\right)^{\ell-|L_0|} \text{ si } 4|g_{L_0} \text{ et} L_0 \neq E, \\ 1 \text{ si } 2|g_{L_0} \text{ et } L_0 = E, \\ 0 \text{ sinon} \end{cases}$$

En effet, si $L_0 \neq E$ alors il existe $i \in E\backslash L_0$ avec $2|c_{i,L_0}|\frac{g_{L_0}}{k_{L_0}}$ et donc $4|g_{L_0}$et dans ce cas

$$\begin{aligned} &\sum_{\substack{c_{i,L_0}|\frac{g_{L_0}}{k_{L_0}} \\ 2|c_{i,L_0}}} \frac{1}{\varphi(c_{i,L_0})} \prod_{\substack{p|k \\ p|c_{i,L_0} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \\ &= \left(2\left(1-2^{-\nu_2(g_{L_0})+1}\right)\right) \sum_{\substack{c_{i,L_0}|\frac{g_{L_0}}{k_{L_0}} \\ 2\nmid c_{i,L_0}}} \frac{1}{\varphi(c_{i,L_0})} \prod_{\substack{p|k \\ p|c_{i,L_0} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right). \end{aligned}$$

Ainsi

$$\sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)} \\ b\notin L \\ c_{bL}|\frac{g_L}{k_L}}} \prod_{\substack{\{i,L\} \\ L\in\mathscr{P}^*(E) \\ i\notin L}} \alpha_4(c_{i,L}) = \delta_3(g_{L_0}) \prod_{i\in E} \left(\prod_{\substack{L\in\mathscr{P}^*(E) \\ i\notin L}} \left(\sum_{\substack{c|\frac{g_L}{k_L} \\ 2\nmid c}} \frac{1}{\varphi(c)} \prod_{\substack{p|k \\ p|c \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \right) \right)$$

Puis en exprimant la somme sur c comme un produit eulérien :

$$\begin{aligned} \sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)} \\ b\notin L \\ c_{bL}|\frac{g_L}{k_L}}} \prod_{\substack{\{i,L\} \\ L\in\mathscr{P}^*(E) \\ i\notin L}} \alpha_4(c_{i,L}) &= \delta_3(g_{L_0}) \prod_{L\in\mathscr{P}^*(E)} \left(\prod_{\substack{p|k_L \\ p\geq 3}} \left(1 + \frac{p-1}{p-2} \sum_{n=1}^{\nu_p(g_L)-1} \frac{1}{p^n} \right)^{\ell-|L|} \right) \\ &= \delta_3(g_{L_0}) \prod_{L\in\mathscr{P}^*(E)} \left(\prod_{\substack{p|k_L \\ p\geq 3}} \left(1 + \frac{1-p^{-\nu_p(g_L)+1}}{p-2} \right)^{\ell-|L|} \right) \end{aligned} \tag{2.34}$$

Puis exprimons séparément la somme sur g_{L_0}.

$$\sum_{\substack{\{g_{L_0}\}_{L_0\in\mathscr{P}^*(E)}\\ g_{L_0}|k_{L_0}^\infty\\ k_{L_0}|g_{L_0}}} \delta_3(g_{L_0})\frac{1}{\varphi(g_{L_0})^{|L_0|}}\prod_{\substack{p|k_{L_0}\\ p\geq 3}}\left(1+\frac{1-p^{-\nu_p(g_L)+1}}{p-2}\right)^{\ell-|L_0|}$$

$$=\frac{1}{\varphi(k_{L_0})^{|L_0|}}\sum_{\substack{\{g_{L_0}\}_{L_0\in\mathscr{P}^*(E)}\\ g_{L_0}|k_{L_0}^\infty}} \delta_3(2g_{L_0})\frac{1}{g_{L_0}^{|L_0|}}\prod_{\substack{p|k_{L_0}\\ p\geq 3}}\left(1+\frac{1-p^{-\nu_p(g_L)}}{p-2}\right)^{\ell-|L_0|}. \tag{2.35}$$

Alors en posant :

$$\delta_4(L_0)=\begin{cases} 2^{-|L_0|}\left(1+2^{\ell-|L_0|}R_2(|L_0|)\right) \text{ si } L_0\neq E,\\ \frac{2^\ell}{2^\ell-1} \text{ si } L_0=E,\end{cases}$$

on obtient en reprenant (2.35) dans (2.33) et en en procédant de la même manière que pour (2.21) :

$$\mathcal{P}'_\alpha(k)=2^{-\ell}\sum_{L_0\in\mathscr{P}^*(E)}\frac{\delta_4(L_0)}{2^{|L_0|}}\prod_{\substack{p|k\\ p\geq 3}}\left(1-\frac{1}{p-1}\right)^\ell \underset{i=1}{\overset{\ell}{*}}\left(F_i^{*\binom{\ell}{i}}\right)\left(\frac{k}{2}\right).$$

Reste à évaluer $2^{-\ell}\sum\limits_{L_0\in\mathscr{P}^*(E)}\frac{\delta_4(L_0)}{2^{|L_0|}}$, on a

$$2^{-\ell}\sum_{L_0\in\mathscr{P}^*(E)}\frac{\delta_4(L_0)}{2^{|L_0|}}=2^{-\ell}\left(\sum_{i=1}^{\ell-1}\binom{\ell}{i}2^{-2i}\left(1+2^{\ell-i}R_2(i)\right)+\frac{1}{2^\ell-1}\right)$$

$$=2^{-\ell}\left(\sum_{i=1}^{\ell}\binom{\ell}{i}2^{-2i}\left(1+2^{\ell-i}R_2(i)\right)+2^{-\ell}\right).$$

□

2.7.4 Évaluation de $\mathcal{P}'_\beta(k)$.

L'évaluation de $\mathcal{P}'_\beta(k)$ va se dérouler dans le même esprit que celle de $\mathcal{P}'_\alpha(k)$, mais avec quelques subtilités importantes. En effet la présence de termes dépendants de $\tilde{a_1}$, et notamment $\mathbb{1}(2\tilde{a_1}|k)$, va nous imposer d'introduire une somme sur toutes les décompositions possibles de $\tilde{a_1}$ en produits de $|\mathscr{P}^*(E)|$ facteurs.

Proposition 2.27. *On a, en reprenant les définitions de H_2 et F_i de la proposition 2.22,*

$$\mathcal{P}'_\beta(k) = H_2(\ell, a_1)\mathbb{1}(2\tilde{a_1}|k) \prod_{\substack{p|\frac{k}{2\tilde{a_1}}\\ p\geq 3}} \left(1-\frac{1}{p-1}\right)^\ell \overset{\ell}{\underset{i=1}{*}} \left(F_i^{*\binom{\ell}{i}}\right)(\frac{k}{2\tilde{a_1}}).$$

Démonstration. Commençons par expliciter $\mathcal{P}'_\alpha(k)$, en remarquant que

$$\prod_{\substack{p|\tilde{a_1}\\ p|u_i\\ p\geq 3}}(2-p) = \prod_{\substack{L\in(P)^*(E)\\ i\in L}} \left(\prod_{\substack{p|\tilde{a_1}\\ p|g_L\\ p\geq 3}}(2-p)\right) \prod_{\substack{L\in(P)^*(E)\\ i\notin L}} \left(\prod_{\substack{p|\tilde{a_1}\\ p|c_{i,L}\\ p\geq 3}}(2-p)\right)$$

et en utilisant le lemme 2.25, on obtient

$$\begin{aligned}\mathcal{P}'_\beta(k) :=& \beta_1(k) \sum_{L_0\in\mathscr{P}^*(E)} \sum_{L_1\in\mathscr{P}^*(L_0)} \beta_2(L_1) \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \prod_{L\in\mathscr{P}^*(E)} \beta_3(k_L) \quad (2.36)\\ & \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)}\\ g_L|k_L^\infty\\ k_L|g_L}} \prod_{L\in\mathscr{P}^*(E)} \beta_4(g_L) \sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}|\frac{g_L}{k_L}}} \prod_{\substack{\{i,L\}\\ L\in\mathscr{P}^*(E)\\ i\notin L}} \beta_5(c_{i,L})\end{aligned}$$

où

- $\beta_1(k) := 2^{-\ell}\mathbb{1}(2\tilde{a_1}|k) \prod_{\substack{p|k\\ p\geq 3}} \left(1-\frac{1}{p-1}\right)^\ell$,
- $\beta_2(L_1) := \mu(\tilde{a_1})^{|L_1|} \prod_{\substack{p|\tilde{a_1}\\ p\geq 3}} \left(\frac{1}{p-2}\right)^{|L_1|}$,
- $\beta_3(k_L) := \begin{cases} \frac{\mathbb{1}(2|k_{L_0})}{{k'_{L_0}}^{|L_0|}} \prod_{\substack{p|k_{L_0}\\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L_0|} \prod_{\substack{p|\tilde{a_1}\\ p|k_{L_0}\\ p\geq 3}} (2-p)^{|L_0\cap L_1|} & \text{si } L = L_0,\\ \frac{1}{{k'_L}^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|} \prod_{\substack{p|\tilde{a_1}\\ p|k_L\\ p\geq 3}} (2-p)^{|L\cap L_1|} & \text{sinon,}\end{cases}$,

- $\beta_4(g_L) := \begin{cases} \frac{\delta_2(g_{L_0})^{|L_1|}}{\varphi(g_{L_0})^{|L_0|}} & \text{si } L = L_0, \\ \frac{1}{\varphi(g_L)^{|L|}} & \text{sinon,} \end{cases}$, avec $\delta_2(g_{L_0}) = \begin{cases} 1 \text{ si } \nu_2(g_{L_0}) \geq s(a_1) \\ -1 \text{ si } \nu_2(g_{L_0}) = s(a_1) - 1 \\ 0 \text{ sinon} \end{cases}$,

- $\beta_5(c_{i,L}) := \begin{cases} \frac{1}{\varphi(c_{i,L})} \prod\limits_{\substack{p|k \\ p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod\limits_{\substack{L\in\mathscr{P}^*(E) \\ i\notin L}} \left(\prod\limits_{\substack{p|\tilde{a_1} \\ p|c_{i,L} \\ p\geq 3}} (2-p) \right) & \text{si } i \in L_1, \\ \frac{\mathbb{1}(2|c_{i,L_0})}{\varphi(c_{i,L})} \prod\limits_{\substack{p|k \\ p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) & \text{si } i \in E\backslash L_0, \\ \frac{1}{\varphi(c_{i,L})} \prod\limits_{\substack{p|k \\ p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) & \text{sinon,} \end{cases}$.

Les sommes sur les $c_{i,L}$ pour $i \notin L_1$ sont exactement les mêmes que pour (2.34), intéressons-nous au cas $i \in L_1$ et $i \notin L$ (et donc $2 \nmid k_L$) :

$$\sum_{c_{i,L}|\frac{g_L}{k_L}} \frac{1}{\varphi(c_{i,L})} \prod_{\substack{p|k \\ p|c_{i,L} \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|\tilde{a_1} \\ p|c_{i,L} \\ p\geq 3}} (2-p) = \prod_{\substack{p|k_L \\ p\nmid\tilde{a_1} \\ p\geq 3}} (f_p(\nu_p(g_L)-1)) \prod_{\substack{p|k_L \\ p|\tilde{a_1} \\ p\geq 3}} p^{-\nu_p(g_L)+1},$$

où on a posé pour $n \geq 1$, et $p \geq 3$, $f_p(n) := 1 + \frac{1-p^{-n}}{p-2}$.
et ainsi en reprenant le calcul de (2.34),

$$\sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}\mid \frac{g_L}{k_L}}} \prod_{\substack{\{i,L\}\\ L\in\mathscr{P}^*(E)\\ i\notin L}} \left(\frac{1}{\varphi(c_{i,L})} \prod_{\substack{p\mid k\\ p\mid c_{i,L}\\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)} \right) \right)$$

$$\prod_{\substack{i\in L_1,\ L\in\mathscr{P}^*(E)\\ i\notin L}} \left(\prod_{\substack{p\mid \tilde{a_1}\\ p\mid c_{i,L}\\ p\geq 3}} (2-p) \right) \prod_{i\in E\setminus L_0} (\mathbb{1}(2|c_{i,L_0}))$$

$$= \delta_3(g_{L_0}) \prod_{L\in\mathscr{P}^*(E)} \left(\prod_{\substack{p\mid k_L\\ p\geq 3}} (f_p(\nu_p(g_L)-1))^{\ell-|L\cup L_1|} \right.$$

$$\left. \prod_{\substack{p\mid k_L\\ p\nmid \tilde{a_1}\\ p\geq 3}} (f_p(\nu_p(g_L)-1))^{|L_1\setminus L|} \prod_{\substack{p\mid k_L\\ p\mid \tilde{a_1}\\ p\geq 3}} \left(p^{-\nu_p(g_L)+1}\right)^{|L_1\setminus L|} \right)$$

Passons aux sommes sur les g, en commençant par g_{L_0} :

$$\sum_{\substack{g_{L_0}\mid k_{L_0}^\infty\\ k_{L_0}\mid g_{L_0}}} \delta_2(g_{L_0})^{|L_1|}\delta_3(g_{L_0}) \frac{1}{\varphi(g_{L_0})^{|L|}} \prod_{\substack{p\mid k_{L_0}\\ p\geq 3}} (f_p(\nu_p(g_{L_0})-1))^{\ell-|L_0|}$$

$$= \frac{1}{\varphi(k_{L_0})^{|L_0|}} \sum_{g_{L_0}\mid k_{L_0}^\infty} \delta_2(2g_{L_0})^{|L_1|}\delta_3(2g_{L_0}) \frac{1}{g_{L_0}^{|L_0|}} \prod_{\substack{p\mid k_{L_0}\\ p\geq 3}} (f_p(\nu_p(g_{L_0})))^{\ell-|L_0|}\,.$$

Exprimons les valeurs prisent par $\delta_2(2g_{L_0})$ suivant les valeurs de $s(a_1)$ et celles prisent par $\delta_3(2g_{L_0})$ suivant si $E = L_0$ ou $E \neq 0$.

$s(a_1)$	$\delta_2(2g_{L_0})$	$\delta_3(2g_{L_0})$	
		$L_0 = E$	$L_0 \neq E$
1	1	1	$\begin{cases} \left(2\left(1-2^{-\nu_2(g_{L_0})}\right)\right)^{\ell-\lvert L_0\rvert} & \text{si } 2 \mid g_{L_0}, \\ 0 \text{ sinon} \end{cases}$
2	$\begin{cases} 1 \text{ si } \nu_2(g_{L_0}) \geq 1 \\ -1 \text{ si } \nu_2(g_{L_0}) = 0 \end{cases}$	1	$\begin{cases} \left(2\left(1-2^{-\nu_2(g_{L_0})}\right)\right)^{\ell-\lvert L_0\rvert} & \text{si } 2 \mid g_{L_0}, \\ 0 \text{ sinon} \end{cases}$
3	$\begin{cases} 1 \text{ si } \nu_2(g_{L_0}) \geq 2 \\ -1 \text{ si } \nu_2(g_{L_0}) = 1 \\ 0 \text{ sinon} \end{cases}$	1	$\begin{cases} \left(2\left(1-2^{-\nu_2(g_{L_0})}\right)\right)^{\ell-\lvert L_0\rvert} & \text{si } 2 \mid g_{L_0}, \\ 0 \text{ sinon} \end{cases}$

Définissons une fonction $\delta_5(L_0, L_1)$ comme suit :

$s(a_1)$	$\delta_5(L_0, L_1)$	
	$E = L_0$	$E \neq L_0$
1	$\frac{2^\ell}{2^\ell-1}$	$2^{-\lvert L_0\rvert}\left(1+2^{\ell-\lvert L_0\rvert}R_2(\lvert L_0\rvert)\right)$
2	$(-1)^{\lvert L_1\rvert}\left(\frac{2^\ell-1+(-1)^{\lvert L_1\rvert}}{2^\ell-1}\right)$	$2^{-\lvert L_0\rvert}\left(1+2^{\ell-\lvert L_0\rvert}R_2(\lvert L_0\rvert)\right)$
3	$\frac{(-1)^{\lvert L_1\rvert}}{2^\ell}\left(\frac{2^\ell-1+(-1)^{\lvert L_1\rvert}}{2^\ell-1}\right)$	$(-1)^{\lvert L_1\rvert}2^{-\lvert L_0\rvert}\left(1+(-1)^{\lvert L_1\rvert}2^{\ell-\lvert L_0\rvert}R_2(\lvert L_0\rvert)\right)$

On obtient, en exprimant la somme sur g_{L_0} sous forme de produit eulérien :

$$\begin{aligned} &\sum_{\substack{g_{L_0} \mid k_{L_0}^\infty \\ k_{L_0} \mid g_{L_0}}} \delta_2(g_{L_0})^{\lvert L_1\rvert}\delta_3(g_{L_0})\frac{1}{\varphi(g_{L_0})^{\lvert L\rvert}} \prod_{\substack{p \mid k_{L_0} \\ p \geq 3}} \left(f_p(\nu_p(g_{L_0})-1)\right)^{\ell-\lvert L_0\rvert} \\ &\qquad = \delta_5(L_0, L_1)\frac{1}{\varphi(k_{L_0})^{\lvert L_0\rvert}} \prod_{\substack{p \mid k_{L_0} \\ p \geq 3}} \left(1+R_p(\lvert L_0\rvert)\right). \end{aligned} \tag{2.37}$$

Définissons

$$\widehat{\delta}(L_0, L_1) = \begin{cases} (-1)^{\lvert L_1\rvert}2^{-\lvert L_0\rvert}\left(1+(-1)^{\lvert L_1\rvert}2^{\ell-\lvert L_0\rvert}R_2(\lvert L_0\rvert)\right) & \text{si } s(a_1) = 3, \\ 2^{-\lvert L_0\rvert}\left(1+2^{\ell-\lvert L_0\rvert}R_2(\lvert L_0\rvert)\right) & \text{sinon.} \end{cases}$$

Et une fonction $\tilde{\delta}(L_0, L_1)$,

$$\tilde{\delta}(L_0, L_1) = \begin{cases} 1 \text{ si } L_0 = E \text{ et } s(a_1) = 1, \\ (-1)^{\lvert L_1\rvert} \text{ si } L_0 = E \text{ et } s(a_1) = 2, \\ 0 \text{ sinon.} \end{cases}$$

On a alors $\delta_5(L_0,L_1)=\widehat{\delta}(L_0,L_1)+\tilde{\delta}(L_0,L_1)$.
Puis pour $L\neq L_0$:

$$\sum_{\substack{g|k_L^\infty\\ k_L|g}}\frac{1}{\varphi(g)^{|L|}}\prod_{\substack{p|k_L\\ p\geq 3}}\left(f_p(\nu_p(g)-1)\right)^{\ell-|L\cup L_1|}\prod_{\substack{p|k_L\\ p\nmid\tilde{a_1}\\ p\geq 3}}\left(f_p(\nu_p(g)-1)\right)^{|L_1\setminus L|}\prod_{\substack{p|k_L\\ p|\tilde{a_1}\\ p\geq 3}}\left(p^{-\nu_p(g)+1}\right)^{|L_1\setminus L|}$$
$$=\frac{1}{\varphi(k_L)^{|L|}}\prod_{\substack{p|k_L\\ p\nmid\tilde{a_1}\\ p\geq 3}}\left(1+R_p(|L|)\right)\prod_{\substack{p|k_L\\ p|\tilde{a_1}\\ p\geq 3}}\left(1+R_p(|L\cup L_1|)\right). \tag{2.38}$$

On va ensuite exprimer $\mathbb{1}(2\tilde{a_1}|k)$ en décomposant $\tilde{a_1}$ en $\prod_{L\in\mathscr{P}^*(E)}a'_L$ où $a'_L|\frac{k_L}{(2,k_L)}$,
et en reprenant (2.37) et (2.38) dans (2.36) cela donne :

$$\begin{aligned}\mathcal{P}'_\beta(k)=&\beta_1(k)\sum_{L_0\in\mathscr{P}^*(E)}2^{-|L_0|}\sum_{L_1\in\mathscr{P}^*(L_0)}\beta_6(L_1)\\ &\sum_{\prod_{L\in\mathscr{P}^*(E)}a'_L=\tilde{a_1}}\prod_{L\in\mathscr{P}^*(E)}\beta_7(a'_L)\sum_{\prod_{L\in\mathscr{P}^*(E)}k_L=\frac{k}{2\tilde{a_1}}}\prod_{L\in\mathscr{P}^*(E)}\beta_8(k_L),\end{aligned}$$

où

- $\beta_6(L_1):=\delta_5(L_0,L_1)\mu(\tilde{a_1})^{|L_1|}\prod_{\substack{p|\tilde{a_1}\\ p\geq 3}}\left(\frac{1}{p-2}\right)^{|L_1|}$,
- $\beta_7(a'_L):=\left(\frac{(h,a'_L)}{a'_L\varphi(a'_L)}\right)^{|L|}\prod_{p|a'_L}\left(\left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|}(2-p)^{|L\cap L_1|}\right)\prod_{p|a'_L}(1+R_p(|L\cup L_1|))$,
- $\beta_8(k_L):=\frac{1}{{k'_L}^{|L|}\varphi(k_L)^{|L|}}\prod_{\substack{p|k_L\\ p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|}\prod_{\substack{p|k_L\\ p\geq 3}}(1+R_p(|L|))$.

Définissons pour tout $L\in\mathscr{P}^*(E)$ les fonctions multiplicatives $G_L^{L_1}$ par :

$$G_L^{L_1}(p):=\left(\frac{(p-1)(h,p)}{p^2(p-2)}\right)^{|L|}(2-p)^{|L_1\cap L|}\left(1+R_p(|L\cup L_1|)\right),$$

et la fonction

$$H_2(\ell, a_1) := 2^{-\ell} \sum_{L_0 \in \mathscr{P}^*(E)} 2^{-|L_0|} \sum_{L_1 \in \mathscr{P}^*(L_0)} \left(\widehat{\delta}(L_0, L_1) + \tilde{\delta}(L_0, L_1) \right) \mu(\tilde{a_1})^{|L_1|} \prod_{\substack{p | \tilde{a_1} \\ p \geq 3}} \left(\frac{(p-2)^{\ell - |L_1|}}{(p-1)^\ell} \right) \underset{L \in \mathscr{P}^*(E)}{*} \left(G_L^{L_1} \right)(\tilde{a_1}).$$

On a alors

$$\mathcal{P}'_\beta(k) = H_2(\ell, a_1) \mathbb{1}(2\tilde{a_1} | k) \prod_{\substack{p | \frac{k}{2\tilde{a_1}} \\ p \geq 3}} \left(1 - \frac{1}{p-1} \right)^\ell \overset{\ell}{\underset{i=1}{*}} \left(F_i^{*\binom{\ell}{i}} \right) (\frac{k}{2\tilde{a_1}}).$$

□

2.7.5 Preuve de la proposition 2.22.

Nous sommes maintenant en mesure de démontrer la proposition 2.22.

Preuve de la proposition 2.22. En utilisant les propositions 2.24, 2.26 et 2.27 on a,

$$\begin{aligned}
\sum_k \mu(k) \mathcal{P}'_{a,0}(k) &= \sum_{\substack{k \\ 2 \nmid k}} \mu(k) \mathcal{P}'_{a,0}(k) + \sum_{\substack{k \\ 2 | k}} \mu(k) \left(\mathcal{P}'_\alpha(k) + \mathcal{P}'_\beta(k) \right) \\
&= \sum_{\substack{k \\ 2 \nmid k}} \mu(k) \left(\mathcal{P}'_{a,0}(k) - \mathcal{P}'_\alpha(x, 2k) \right) + \mu(2\tilde{a_1}) \sum_{\substack{k \\ 2\tilde{a_1} \nmid k}} \mu(k) \mathcal{P}'_\beta(x, 2\tilde{a_1} k) \\
&= \prod_{\substack{p \\ p \geq 3}} \left(1 - \left(\frac{p-2}{p-1} \right)^\ell \sum_{i=1}^{\ell} \binom{\ell}{i} F_i(p) \right) \\
&\quad \left(1 - H_1(E) + \mu(2\tilde{a_1}) H_2(\ell, a_1) \prod_{\substack{p \\ p | a_1 \\ p \geq 3}} \left(1 - \left(\frac{p-2}{p-1} \right)^\ell \sum_{i=1}^{\ell} \binom{\ell}{i} F_i(p) \right)^{-1} \right),
\end{aligned}$$

ce qui donne la proposition 2.22.

□

2.8 Lien entre le terme principal de la proposition 2.22 et les théorèmes 0.3 et 0.4

2.8.1 Équivalence entre le terme principal de la proposition 2.22 et le résultat heuristique

Nous allons commencer par montrer que le coefficient correspondant à un nombre premier impair p dans le produit $M(E)$ de la proposition 2.22 coïncide avec celui obtenu par l'approche heuristique.

Proposition 2.28. *En reprenant les notations de la proposition 2.22, on a*

$$\left(\frac{p-2}{p-1}\right)^{\ell}\sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)=\sum_{i=1}^{\ell}\binom{\ell}{i}\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}\frac{(-1)^j p^{i+j}(h,p)^i}{p^{2i}(p-1)^j(p^{i+j}-1)}=W_\ell(p),$$

et $H_1(E)=W_\ell(2)$.

Démonstration. On a trivialement,

$$\begin{aligned}\left(\frac{p-2}{p-1}\right)^{\ell}\sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)&=\sum_{i=1}^{\ell}\binom{\ell}{i}\left(\frac{p-2}{p-1}\right)^{\ell-i}\frac{(h,p)^i}{p^{2i}}\\&\quad+\sum_{i=1}^{\ell}\binom{\ell}{i}\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}\frac{(-1)^j(p-1)^{-j}(h,p)^i}{p^{2i}(p^{i+j}-1)}.\end{aligned}$$

On écrit dans le premier terme, $\left(\frac{p-2}{p-1}\right)^{\ell-i}=\left(1-\frac{1}{p-1}\right)^{\ell-i}=\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}\frac{(-1)^j}{(p-1)^j}$.
Ainsi

$$\begin{aligned}\left(\frac{p-2}{p-1}\right)^{\ell}\sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)&=\sum_{i=1}^{\ell}\binom{\ell}{i}\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}\frac{(-1)^j(h,p)^i}{p^{2i}(p-1)^j}\left(1+\frac{1}{p^{i+j}-1}\right)\\&=\sum_{i=1}^{\ell}\binom{\ell}{i}\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}\frac{(-1)^j p^{i+j}(h,p)^i}{p^{2i}(p-1)^j(p^{i+j}-1)}=W_\ell(p).\end{aligned}$$

Montrons maintenant que $H_1(E) = W_\ell(2)$. Pour ce faire on va montrer que $Q(2) := 2^\ell W_\ell(2) - \sum_{i=1}^{\ell} \binom{\ell}{i} 2^{-2i} \left(1 + 2^{\ell-i} \sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j 2^{-j}}{2^{i+j}-1}\right) = 2^{-\ell}$. On a

$$\begin{aligned} Q(2) &= \sum_{i=1}^{\ell} \binom{\ell}{i} \left(\sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \left(\frac{(-1)^j 2^\ell \left(2^{i+j} - 2^{-i-j}\right)}{2^{2i}(2^{i+j}-1)} \right) - 2^{-2i} \right) \\ &= \sum_{i=1}^{\ell} \binom{\ell}{i} \left(\sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \left((-1)^j \left(2^{\ell-2i} + 2^{\ell-3i-j}\right) \right) - 2^{-2i} \right). \end{aligned}$$

Or $\sum_{j=0}^{\ell-i} \binom{\ell-i}{j} (-1)^j 2^{\ell-2i} = \begin{cases} 2^{-l} & \text{si } i = \ell, \\ 0 & \text{sinon.} \end{cases}$ et $\sum_{j=0}^{\ell-i} \binom{\ell-i}{j} (-1)^j 2^{\ell-3i-j} = 2^{-2i}$, et ainsi $Q(2) = 2^{-l}$. □

2.8.2 Égalité entre le terme $H_2(\ell, a_1)$ de la proposition 2.22 et de celui des théorèmes 0.3 et 0.4

Les contributions dans $H_2(\ell, a_1)$ des sous-ensembles L_0 et L_1 ne dépendant que de leurs tailles il est naturel de préférer exprimer $H_2(\ell, a_1)$ sans faire intervenir des sous-ensembles de $\mathcal{P}^*(E)$. Ce que nous faisons dans la proposition suivante.

Proposition 2.29. *Soit $H_2(\ell, a_1)$ tel que définit dans la proposition 2.22,*

$$H_2(\ell, a_1) = \sum_{k=1}^{\ell} \binom{\ell}{k} 2^{-\ell-k} \delta_\ell(k) \mu(\tilde{a_1})^k \prod_{\substack{p \mid \tilde{a_1} \\ p \geq 3}} \left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell} \right) \sum_{\prod_{\{i,j\} \in \mathcal{D}} a_{i,j} = \tilde{a_1}} \prod_{\{i,j\} \in \mathcal{D}} G_{i,j}^k(a_{i,j}),$$

où $\mathcal{D} = [0,k] \times [0, \ell-k] \backslash \{0,0\}$, pour $(i,j) \in \mathcal{D}$, $G_{i,j}^k$ est la fonction multiplicative définie pour les nombres premiers impairs par :

$$G_{i,j}^k(p) = \binom{k}{i} \binom{\ell-k}{j} \left(\frac{(p-1)(h,p)}{p^2(p-2)} \right)^{i+j} (2-p)^i \left(1 + R_p(k+j)\right),$$

et

$$\delta_\ell(k) = \sigma(a_1, k) + 2^{\ell-2k} \sum_{m=0}^{\ell-k} \binom{\ell-k}{m} 2^{-3m} \sum_{r=0}^{\ell-k-m} \binom{\ell-k-m}{r} \frac{(-1)^r 2^{-r}}{2^{k+m+r}-1},$$

avec $\sigma(a_1, k) := \begin{cases} 2^{-\ell+k} + 2^{-2\ell+k} 5^{\ell-k} & \text{si } a_1 \equiv 1 \pmod 4, \\ (-1)^k 2^{-\ell+k} + 2^{-2\ell+k} 5^{\ell-k} & \text{si } a_1 \equiv 3 \pmod 4, \\ (-1)^k 2^{-2\ell+k} 5^{\ell-k} & \text{sinon.} \end{cases}$

Démonstration. Fixons L_1. Soient L_α et L_β deux sous-ensembles non-vides de E. Alors $G_{L_\alpha}^{L_1} = G_{L_\beta}^{L_1}$ si et seulement si $|L_1 \cap L_\alpha| = |L_1 \cap L_\beta|$ et $|L_\alpha \backslash L_1| = |L_\beta \backslash L_1|$. En effet si $|L_1 \cap L_\alpha| = |L_1 \cap L_\beta|$ et $|L_\alpha \backslash L_1| = |L_\beta \backslash L_1|$ alors $|L_\alpha| = |L_1 \cap L_\alpha| + |L_\alpha \backslash L_1| = |L_\beta|$ et $|L_1 \cup L_\alpha| = |L_1| + |L_\alpha \backslash L_1| = |L_1 \cup L_\beta|$.
Soit $\mathcal{D} = [0, |L_1|] \times [0, \ell - |L_1|] \backslash \{0, 0\}$,

$$\underset{L \in \mathscr{P}^*(E)}{*} \left(G_L^{L_1}\right)(\tilde{a_1}) = \sum_{\prod\limits_{L \in \mathcal{P}^*(E)} a_L = \tilde{a_1}} \prod_{\{i,j\} \in \mathcal{D}} \prod_{\substack{L \in \mathcal{P}^*(E) \\ |L_1 \cap L| = i \\ |L \backslash L_1| = j}} G_L^{L_1}(a_L).$$

Soit $(i,j) \in \mathcal{D}$, notons $a_{i,j} = \prod\limits_{\substack{L \in \mathcal{P}^*(E) \\ |L \cap L_1| = i \\ |L \backslash L_1| = j}} a_L$ et $\tilde{G}_{i,j}^{L_1} = G_L^{L_1}$ où L est tel que $|L \cap L_1| = i$ et $|L \backslash L_1| = j$.

$$\underset{L \in \mathscr{P}^*(E)}{*} \left(G_L^{L_1}\right)(\tilde{a_1}) = \sum_{\prod\limits_{L \in \mathcal{P}^*(E)} a_L = \tilde{a_1}} \prod_{\{i,j\} \in \mathcal{D}} \tilde{G}_{i,j}^{L_1}(a_{i,j}). \tag{2.39}$$

Nous allons remplacer la somme sur les décompositions de a_1 en $\prod\limits_{L \in \mathcal{P}^*(E)} a_L$ en une somme sur les décompositions de a_1 en $\prod\limits_{\{i,j\} \in \mathcal{D}} a_{i,j}$. Il faut donc calculer le nombre de décompositions en $\prod\limits_{L \in \mathcal{P}^*(E)} a_L$ qui aboutissent à une même décomposition en $\prod\limits_{\{i,j\} \in \mathcal{D}} a_{i,j}$.
Soit $(i,j) \in \mathcal{D}$, $\mathcal{E} = \{L \in \mathcal{P}^*(E), |L \cap L_1| = i,\ |L \backslash L_1| = j\}$ et $\gamma = |\mathcal{E}|$. Soit $p | a_{i,j}$ alors il existe $L \in \mathcal{E}$ tel que $p | a_L$, et il y a γ choix possible pour L. Ainsi le nombre décomposition en $\prod\limits_{L \in \mathcal{P}^*(E)} a_L$ qui correspondent à une même décomposition $\prod\limits_{\{i,j\} \in \mathcal{D}} a_{i,j}$ est $\gamma^{\omega(a_{i,j})}$. De plus L_1 a $\binom{|L_1|}{i}$ sous-ensembles de taille i et $E \backslash L_1$ a $\binom{|E \backslash L_1|}{j}$ sous-ensembles de taille j et ainsi

$$\gamma = \binom{|L_1|}{i} \binom{|E \backslash L_1|}{j}.$$

En reportant cela dans (2.39), on a :

$$\underset{L \in \mathscr{P}^*(E)}{*} \left(G_L^{L_1}\right)(\tilde{a_1}) = \sum_{\prod\limits_{\{i,j\} \in \mathcal{D}} a_{i,j} = \tilde{a_1}} \prod_{\{i,j\} \in \mathcal{D}} G_{i,j}^{|L_1|}(a_{i,j}),$$

avec pour $k \leq \ell$, $i \leq k$ et $j \leq \ell - k$, $G_{i,j}^k$ est la fonction multiplicative telle que pour p un nombre premier impair :

$$G_{i,j}^k(p) = \binom{k}{i}\binom{\ell-k}{j}\left(\frac{(p-1)(h,p)}{p^2(p-2)}\right)^{i+j}(2-p)^i\left(1+R_p(k+j)\right).$$

Nous pouvons maintenant remplacer les sommes sur L_0 et L_1 dans $H_2(\ell, a_1)$ par des sommes sur $1 \leq m \leq \ell$ et $1 \leq k \leq m$. L_0 a $\binom{|L_0|}{k}$ sous-ensembles de taille k et E a $\binom{\ell}{m}$ sous-ensembles de taille m. Ainsi en notant de manière transparente $\widehat{\delta}(m,k) := \widehat{\delta}(L_0, L_1)$ et $\tilde{\delta}(m,k) := \tilde{\delta}(L_0, L_1)$ avec $|L_0| = m$ et $|L_1| = k$, on obtient :

$$\begin{aligned} H_2(\ell, a_1) := &\sum_{m=1}^{\ell}\binom{l}{m}2^{-\ell-m}\sum_{k=1}^{m}\binom{m}{k}\left(\widehat{\delta}(m,k)+\tilde{\delta}(m,k)\right)\mu(\tilde{a_1})^k \\ &\prod_{\substack{p|\tilde{a_1}\\ p\geq 3}}\left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell}\right)\sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}=\tilde{a_1}}\prod_{\{i,j\}\in\mathcal{D}}G_{i,j}^k(a_{i,j}). \end{aligned} \tag{2.40}$$

Inversons alors les sommes sur m et k,

$$H_2(\ell, a_1) := \sum_{k=1}^{\ell}\binom{\ell}{k}2^{-\ell-k}\delta_\ell(k)\mu(\tilde{a_1})^k\prod_{\substack{p|\tilde{a_1}\\ p\geq 3}}\left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell}\right)\sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}=\tilde{a_1}}\prod_{\{i,j\}\in\mathcal{D}}G_{i,j}^k(a_{i,j}). \tag{2.41}$$

avec $\delta_\ell(k) := \sum_{m=0}^{\ell-k}\binom{\ell-k}{m}2^{-m}\left(\widehat{\delta}(m+k,k)+\tilde{\delta}(m+k,k)\right)$.

Simplifions maintenant l'écriture de $\delta_\ell(k)$. Notons $c := \begin{cases} (-1)^k & \text{si } a_1 \equiv 0 \pmod 2, \\ 1 & \text{sinon.} \end{cases}$.

$$\begin{aligned} \sum_{m=0}^{\ell-k}\binom{\ell-k}{m}2^{-m}\widehat{\delta}(m+k,k) &= \sum_{m=0}^{\ell-k}\binom{\ell-k}{m}2^{-2m-k}\left(c+2^{\ell-k-m}\sum_{r=0}^{\ell-k-m}\binom{\ell-k-m}{r}\frac{(-1)^r2^{-r}}{2^{k+m+r}-1}\right) \\ &= c2^{-2\ell+k}5^{\ell-k}+2^{\ell-2k}\sum_{m=0}^{\ell-k}\binom{\ell-k}{m}2^{-3m}\sum_{r=0}^{\ell-k-m}\binom{\ell-k-m}{r}\frac{(-1)^r2^{-r}}{2^{k+m+r}-1}. \end{aligned}$$

De plus

$$\sum_{m=0}^{\ell-k}\binom{\ell-k}{m}2^{-m}\tilde{\delta}(m+k,k) = \begin{cases} 2^{-\ell+k} & \text{si } a_1 \equiv 1 \pmod 4, \\ (-1)^k2^{-\ell+k} & \text{si } a_1 \equiv 3 \pmod 4, \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, en notant $\sigma(a_1,k) := \begin{cases} 2^{-\ell+k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1\equiv 1 \pmod 4,\\ (-1)^k 2^{\ell-k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1\equiv 3 \pmod 4,\\ (-1)^k 2^{-2\ell+k}5^{\ell-k} & \text{sinon.}\end{cases}$,

$$\delta_\ell(k)=\sigma(a_1,k)+2^{\ell-2k}\sum_{m=0}^{\ell-k}\binom{\ell-k}{m}2^{-3m}\sum_{r=0}^{\ell-k-m}\binom{\ell-k-m}{r}\frac{(-1)^r2^{-r}}{2^{k+m+r}-1}.$$

Ce qui permet de conclure. □

2.8.3 Preuve des théorèmes 0.3 et 0.4

En regroupant la proposition 2.4 et les propositions 2.21, 2.22, 2.28, 2.29 et en prenant, par exemple, $C_5=e^{2C_1}$, on obtient le théorème 0.3.
De plus en reportant les résultats des propositions 2.21, 2.22, 2.28, 2.29 dans (2.4) on obtient la majoration inconditionnelle du théorème 0.4.

2.9 Le cas $\ell=2$ avec un meilleur terme d'erreur

2.9.1 Principe de l'hyperbole

On s'intéresse ici au cas $\ell=2$. Ainsi $E=\{1,2\}$, $\mathscr{P}^*(E)=\big\{\{1\},\{2\},\{1,2\}\big\}$. Pour alléger les notations on pose $k_1=k_{\{1\}}$, $k_2=k_{\{2\}}$, $k_{12}=k_{\{1,2\}}$, $g_1=g_{\{1\}}$, $g_2=g_{\{2\}}$, $g_{12}=g_{\{1,2\}}$, $c_{1,\{2\}}=c_{12}$ et $c_{2,\{1\}}=c_{21}$. Dans ce cas il n'est pas nécessaire d'utiliser la méthode de Selberg-Delange pour calculer la dernière somme de ${\mathcal{P}_a}'(x,k)$ car la méthode de l'hyperbole suffit ([37], Théorème I.3.1). Il est à noter que les majorations ne sont pas les meilleures possibles, principalement pour écourter la longueur des démonstrations.

Proposition 2.30 (GRH)**.** *En reprenant les notations de la section 2.3 on a*

$$\sum_{\substack{p_1\le\frac{x}{2}\\(a,p_1)=1\\p_1\equiv 1(u_1d_1)\\a\in\mathfrak{R}(k_1'k_{1,2}',p_1)}}\ \sum_{\substack{p_2\le\frac{x}{p_1}\\(a,p_2)=1\\p_2\equiv 1(u_2d_2)\\a\in\mathfrak{R}(k_2'k_{1,2}',p_2)}} 1=2\frac{\epsilon\left(k_1'k_{1,2}',u_1d_1\right)\epsilon\left(k_2'k_{1,2}',u_2d_2\right)x\log\log x}{k_1'k_2'{k_{1,2}'}^2\varphi(u_1d_1)\varphi(u_2d_2)\log x}$$

$$+\mathcal{O}\left(\frac{x\log\log(u_1d_1u_2d_2)}{\sqrt{u_1d_1u_2d_2}\log x}+x^{\frac{3}{4}}\right).$$

Démonstration. Posons

$$f_1(n) = \begin{cases} 1 \text{ si } n \text{ premier, } (a,n)=1,\ n \equiv 1(u_1 d_1),\ a \in \mathfrak{R}(k_1' k_{1,2}', n) \\ 0 \text{ sinon.} \end{cases}$$

$$f_2(n) = \begin{cases} 1 \text{ si } n \text{ premier, } (a,n)=1,\ n \equiv 1(u_2 d_2),\ a \in \mathfrak{R}(k_2' k_{1,2}', n) \\ 0 \text{ sinon.} \end{cases}$$

ainsi que F_1 et F_2 leurs fonctions sommatoires respectives. Alors, d'après le principe de l'hyperbole :

$$\sum_{p_1 p_2 \leq x} f_1(p_1) f_2(p_2) = \sum_{n \leq \sqrt{x}} f_2(n) F_1\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} f_1(n) F_2\left(\frac{x}{n}\right) - F_1(\sqrt{x}) F_2(\sqrt{x}).$$

Commençons par majorer le dernier terme. D'après le lemme 2.2 de Hooley,

$$F_1(\sqrt{x}) F_2(\sqrt{x}) \ll \frac{x}{\varphi(u_1 d_1)\varphi(u_2 d_2) \log^2 x} + \mathcal{O}\left(x^{\frac{3}{4}}\right) \tag{2.42}$$

Nous montrons plus loin que la contribution de ces termes est négligeable. Puis calculons la première somme :

$$\sum_{n \leq \sqrt{x}} f_2(n) F_1(\frac{x}{n}) = \sum_{\substack{p_2 \leq \sqrt{x} \\ (a,p_2)=1 \\ p_2 \equiv 1(u_2 d_2) \\ a \in \mathfrak{R}(k_2' k_{1,2}', p_2)}} \ \sum_{\substack{p_1 \leq \frac{x}{p_2} \\ (a,p_1)=1 \\ p_1 \equiv 1(u_1 d_1) \\ a \in \mathfrak{R}(k_1' k_{1,2}', p_1)}} 1$$

Puis par sommation d'Abel et en utilisant le lemme de Hooley 2.2 :

$$\sum_{n \leq \sqrt{x}} f_2(n) F_1(\frac{x}{n}) = \sum_{\substack{p_2 \leq \sqrt{x} \\ (a,p_2)=1 \\ p_2 \equiv 1(u_2 d_2) \\ a \in \mathfrak{R}(k_2' k_{1,2}', p_2)}} \left(\epsilon\left(k_1' k_{1,2}', u_1 d_1\right) \frac{\mathrm{Li}(\frac{x}{p_2})}{k_1' k_{1,2}' \varphi(u_1 d_1)} + \mathcal{O}\left(\sqrt{\frac{x}{p_2}} \log x\right) \right) \tag{2.43}$$

Occupons nous du terme d'erreur. Par sommation d'Abel on a :

$$\sum_{\substack{p_2 \leq \sqrt{x} \\ (a,p_2)=1 \\ p_2 \equiv 1(u_2 d_2) \\ a \in \mathfrak{R}(k_2' k_{1,2}', p_2)}} \left(\sqrt{\frac{x}{p_2}} \log x\right) \ll \sum_{p_2 \leq \sqrt{x}} \left(\sqrt{\frac{x}{p_2}} \log x\right) \ll x^{\frac{3}{4}}. \tag{2.44}$$

Passons maintenant au terme principal. Toujours par sommation d'Abel, et en utilisant le lemme 2.2,

$$\sum_{\substack{p_2\leq\sqrt{x}\\(a,p_2)=1\\p_2\equiv 1(u_2d_2)\\a\in\mathfrak{R}(k_2'k_{1,2}',p_2)}} \epsilon\left(k_1'k_{1,2}',u_1d_1\right)\frac{\mathrm{Li}(\frac{x}{p_2})}{k_1'k_{1,2}'\varphi(u_1d_1)}$$

$$= x\frac{\epsilon\left(k_1'k_{1,2}',u_1d_1\right)\epsilon\left(k_2'k_{1,2}',u_2d_2\right)}{k_1'k_2'{k_{1,2}'}^2\varphi(u_1d_1)\varphi(u_2d_2)}\int_{u_2d_2}^{\sqrt{x}}\frac{\mathrm{Li}(t)}{t^2\log\left(\frac{x}{t}\right)}dt+\mathcal{O}(R), \tag{2.45}$$

avec $R=\mathcal{O}\left(\frac{x}{k_1'k_{1,2}'\varphi(u_1d_1)}\int_{u_2d_2}^{\sqrt{x}}\frac{\log t}{t^{\frac{3}{2}}\log\left(\frac{x}{t}\right)}dt\right)+\mathcal{O}\left(x^{\frac{3}{4}}\right)$.
Pour l'intégrale du terme d'erreur on a :

$$\frac{x}{k_1'k_{1,2}'\varphi(u_1d_1)}\int_{u_2d_2}^{\sqrt{x}}\frac{\log t}{t^{\frac{3}{2}}\log\left(\frac{x}{t}\right)}dt\ll\frac{x\log(u_2d_2)}{k_1'k_{1,2}'\varphi(u_1d_1)\sqrt{u_2d_2}\log x}. \tag{2.46}$$

Calculons l'intégrale à part. On procède ici comme dans la preuve de Landau [17] pour la formule asymptotique des 2-presque premiers. En effectuant le changement de variable $u=\log x$, on a

$$\int_{u_2d_2}^{\sqrt{x}}\frac{\mathrm{Li}(t)}{t^2\log\left(\frac{x}{t}\right)}dt=\int_{\log(u_2d_2)}^{\frac{1}{2}\log x}\frac{1}{u(\log x-u)}du+\mathcal{O}\left(\frac{1}{\log x}\right)$$

Puis en effectuant la décomposition en éléments simples $\frac{1}{u(\log x-u)}=\frac{1}{\log x}\left(\frac{1}{u}+\frac{1}{\log x-u}\right)$ on obtient :

$$\begin{aligned}\int_{u_2d_2}^{\sqrt{x}}\frac{\mathrm{Li}(t)}{t^2\log\left(\frac{x}{t}\right)}dt&=\frac{1}{\log x}\left(-\log\log(u_2d_2)+\log\log\left(\frac{x}{u_2d_2}\right)\right)+\mathcal{O}\left(\frac{1}{\log x}\right)\\&=\frac{\log\log x}{\log x}+\mathcal{O}\left(\frac{\log\log(u_2d_2)}{\log x}\right).\end{aligned} \tag{2.47}$$

Puis on obtient par symétrie un résultat analogue pour $\sum_{n\leq\sqrt{x}}f_1(n)F_2(\frac{x}{n})$.
Ainsi en reprenant (2.42), (2.43), (2.44), (2.45), (2.46) et (2.47) on a

$$\sum_{\substack{p_1\leq\frac{x}{2}\\(a,p_1)=1\\p_1\equiv 1(u_1d_1)\\a\in\mathfrak{R}(k_1'k_{1,2}',p_1)}}\ \sum_{\substack{p_2\leq\frac{x}{p_1}\\(a,p_2)=1\\p_2\equiv 1(u_2d_2)\\a\in\mathfrak{R}(k_2'k_{1,2}',p_2)}} 1=2\frac{\epsilon\left(k_1'k_{1,2}',u_1d_1\right)\epsilon\left(k_2'k_{1,2}',u_2d_2\right)x\log\log x}{k_1'k_2'{k_{1,2}'}^2\varphi(u_1d_1)\varphi(u_2d_2)\log x}+\mathcal{O}\left(R\right),$$

avec $R := \frac{x \log\log(u_1 d_1 u_2 d_2)}{\sqrt{u_1 d_1 u_2 d_2}\log x} + x^{\frac{3}{4}}$.

□

2.9.2 Contrôle des termes d'erreur

Commençons par estimer le terme d'erreur provenant de $x^{\frac{3}{4}}$. Notons $T_1(x, C_1, C_5)$ cette contribution,

$$T_1(x, C_1, C_5) := \sum_{P^+(k)\leq C_1} \mu^2(k) \sum_{k_1k_2k_{1,2}=k} \sum_{\substack{g_1\leq C_5\\ g_1|k_1^\infty\\ k_1|g_1}} \sum_{\substack{g_2\leq C_5\\ g_2|k_2^\infty\\ k_2|g_2}} \sum_{\substack{g_{12}\leq C_5\\ g_{12}|k_{1,2}^\infty\\ k_{1,2}|g_{12}}} \sum_{c_{12}|\frac{g_2}{k_2}} \sum_{c_{21}|\frac{g_1}{k_1}} \sum_{\substack{d_1|k\\ d_2|k}} x^{\frac{3}{4}}$$

$$\ll x^{\frac{3}{4}} \sum_{P^+(k)\leq C_1} \mu^2(k) 4^{\omega(k)} \sum_{k_1k_2k_{1,2}=k} \sum_{\substack{g_1\leq C_5\\ g_1|k_1^\infty}} \tau(g_1) \sum_{\substack{g_2\leq C_5\\ g_2|k_2^\infty}} \tau(g_2) \sum_{\substack{g_{12}\leq C_5\\ g_{12}|k_{1,2}^\infty}} 1.$$

En exprimant la somme comme un produit eulérien on a

$$\sum_{\substack{g_1\leq C_5\\ g_1|k_1^\infty}} \tau(g_1) \ll \prod_{p|k_1} \left(\sum_{n=0}^{\log C_5} (n+1) \right)$$

$$\ll (\log C_5)^{2\omega(k)}.$$

De la même manière on obtient $\sum_{\substack{g_{12}\leq C_5\\ g_{12}|k_{1,2}^\infty}} 1 \ll (\log C_5)^{\omega(k)}$.

Ainsi

$$T_1(x, C_1, C_5) \ll x^{\frac{3}{4}} \sum_{P^+(k)\leq C_1} \mu^2(k) 4^{\omega(k)} (\log C_5)^{5\omega(k)} \sum_{k_1k_2k_{1,2}=k} 1$$

$$\ll x^{\frac{3}{4}} \sum_{P^+(k)\leq C_1} \mu^2(k) 12^{\omega(k)} (\log C_5)^{5\omega(k)} \ll \left(13(\log C_5)^5\right)^{\frac{C_1}{\log C_1}} x^{\frac{3}{4}}.$$

Passons maintenant à $T_2(x, C_1, C_5)$ la contribution du terme $\frac{x \log\log(u_1 d_1 u_2 d_2)}{\sqrt{u_1 d_1 u_2 d_2}\log x}$.

$$T_2(x, C_1, C_5) := \sum_{P^+(k)\leq C_1} \sum_{k_1k_2k_{1,2}=k} \sum_{\substack{g_1\leq C_5\\ g_1|k_1^\infty\\ k_1|g_1}} \sum_{\substack{g_2\leq C_5\\ g_2|k_2^\infty\\ k_2|g_2}} \sum_{\substack{g_{12}\leq C_5\\ g_{12}|k_{1,2}^\infty\\ k_{1,2}|g_{12}}} \sum_{c_{12}|\frac{g_2}{k_2}} \sum_{c_{21}|\frac{g_1}{k_1}} \sum_{\substack{d_1|k\\ d_2|k}} \frac{x \log\log(u_1 d_1 u_2 d_2)}{\sqrt{u_1 d_1 u_2 d_2}\log x}$$

$$\ll \frac{x}{\log x} \sum_{P^+(k)\leq C_1} \sum_{k_1k_2k_{1,2}=k} \sum_{\substack{g_1\leq C_5\\ g_1|k_1^\infty\\ k_1|g_1}} g_1^{-\frac{1}{2}+\varepsilon} \sum_{\substack{g_2\leq C_5\\ g_2|k_2^\infty\\ k_2|g_2}} g_2^{-\frac{1}{2}+\varepsilon} \sum_{\substack{g_{12}\leq C_5\\ g_{12}|k_{1,2}^\infty\\ k_{1,2}|g_{12}}} g_{12}^{-1+\varepsilon}$$

pour $\varepsilon > 0$.
En procédant encore par sommation d'Abel on a

$$\sum_{\substack{g_1 \leq C_5 \\ g_1 | k_1^\infty \\ k_1 | g_1}} g_1^{-\frac{1}{2}+\varepsilon} \ll \prod_{p | k_1} \left(\sum_{n=0}^{\log C_5} \frac{1}{p^{n(1/2-\varepsilon)}} \right) \ll 2^{\omega(k_1)}$$

D'autre part

$$\sum_{\substack{g_{12} \leq C_5 \\ g_{12} | k_{1,2}^\infty \\ k_{1,2} | g_{12}}} g_{12}^{-1+\varepsilon} \ll 2^{\omega(k_1)}.$$

Ainsi $T_2(x, C_1, C_5) \ll 48^{\frac{C_1}{\log C_1}} \frac{x}{\log x}$.
On peut donc reformuler le théorème 0.3 pour $\ell = 2$, en prenant par exemple $C_1 = \log\log\log x$ et $C_5 = \log x$ cela donne le théorème 0.5.

Chapitre 3

Racines primitives généralisées parmi les entiers criblés

3.1 Majoration de $\mathcal{M}_{a,\ell}$ et $\mathcal{P}_{a,\ell}$ pour le cas des entiers criblés

Soit $0 < \theta < \frac{1}{2}$. Dans cette partie, on étudie le cas de l'ensemble des entiers x^θ criblés pour lesquels un entier a est racine primitive généralisée, et nous montrons qu'il admet une densité parmi tous les entiers x^θ criblés si $a \neq -1$ et n'est pas le carré d'un entier.
Un entier x^θ criblé est un entier n'ayant aucun facteur premier plus petit que x^θ. Buchstab [4] a montré que le nombre d'entiers x^θ criblés plus petit que x est asymptotiquement équivalent à $\omega\left(\frac{1}{\theta}\right)\frac{x}{\theta^2\log^2 x}$, où ω est la fonction de Buchstab. Cette fonction est l'unique solution continue pour $u > 1$ de l'équation différentielle aux différences :

$$\frac{\partial(u\omega(u))}{\partial u} = \omega(u-1) \quad \text{pour } u > 2,$$

avec la condition initiale pour $1 \leq u \leq 2$, $u\omega(u) = 1$.
Un entier x^θ criblé a au plus $\left\lfloor \frac{1}{\theta} \right\rfloor$ facteurs premiers. En notant

$$\mathcal{N}_{a,\ell}(x,y) = \#\{n \leq x | P^-(n) > y,\ \Omega(n) = \ell,\ a \text{ est racine primitive généralisée } \pmod n\},$$

on a alors

$$\mathcal{N}_a(x,x^\theta) = \sum_{\ell=1}^{\left\lfloor \frac{1}{\theta} \right\rfloor} \mathcal{N}_{a,\ell}(x,x^\theta).$$

D'après le lemme 1.3, a est une racine primitive modulo m si a ne vérifie pas $\mathcal{R}(q,m)$ pour tout q. Posons

$$\mathcal{N}_{a,\ell}(x,y,\eta) = \#\{n \leq x | P^-(n) > y, \Omega(n) = \ell,\ a \text{ ne vérifie pas } \mathcal{R}(q,n),\ \forall q \leq \eta\},$$

et

$$\mathcal{M}_{a,\ell}(x,y,\eta_1,\eta_2)=\#\{n\leq x|P^-(n)>y,\Omega(n)=\ell,\exists\eta_1<q\leq\eta_2,\ a \text{ vérifie } \mathcal{R}(q,n)\}.$$

Soit $\eta\leq x$, alors similairement à (2.4) et (2.5),

$$\mathcal{N}_{a,\ell}(x,x^\theta)\leq\mathcal{N}_{a,\ell}(x,x^\theta,\eta) \tag{3.1}$$

et $\mathcal{N}_{a,\ell}(x,x^\theta)\geq\mathcal{N}_{a,\ell}(x,x^\theta,\eta)-\mathcal{M}_{a,\ell}(x,x^\theta,\eta,x)$, ainsi

$$\mathcal{N}_{a,\ell}(x,x^\theta)=\mathcal{N}_{a,\ell}(x,x^\theta,\eta)+\mathcal{O}\left(\mathcal{M}_{a,\ell}(x,x^\theta,\eta,x)\right).$$

Soit C_1 une constante arbitrairement grande, on va alors découper l'intervalle $[C_1,x]$ en deux parties de part et d'autre de $x^{\frac{1-\theta}{2}}\log x$. Ainsi

$$\mathcal{N}_{a,\ell}(x,x^\theta)=\mathcal{N}_{a,\ell}(x,x^\theta,C_1)+\mathcal{O}\left(\mathcal{M}_{a,\ell}(x,x^\theta,C_1,x^{\frac{1-\theta}{2}}\log x)\right)+\mathcal{O}\left(\mathcal{M}_{a,\ell}(x,x^\theta,x^{\frac{1-\theta}{2}}\log x,x)\right). \tag{3.2}$$

On va alors procéder à des majorations analogues à celles obtenues dans la section 2.2.

3.1.1 Majoration des $\mathcal{M}_{a,\ell}$

Dans la proposition suivante on majore le dernier terme d'erreur de (3.2).

Proposition 3.1. *Pour $\ell\geq 2$, on a*

$$\mathcal{M}_{a,\ell}(x,x^\theta,x^{\frac{1-\theta}{2}}\log x,x)\ll\frac{x}{\theta\log^2 x}.$$

Démonstration. Nous procédons ici de la même façon que Hooley [14, p212]. Observons que, comme les rôles des p_i sont symétriques dans la condition $\mathcal{R}(q,p_1\dots p_\ell)$ on peut supposer que $a^{\frac{p_1-1}{q}}\equiv 1(\pmod{p_1})$ et donc $a^{2\frac{p_1-1}{q}}\equiv 1\pmod{p_1}$.
Par conséquent, comme $q>x^{\frac{1-\theta}{2}}\log x$, pour $p_2\cdots p_\ell\leq x^{1-\theta}$ fixés, les nombres p_1 tels que $p_1\cdots p_\ell$ soit compté dans $\mathcal{M}_{a,\ell}(x,x^{\frac{1-\theta}{2}}\log x,x)$ doivent diviser le produit positif (éventuellement vide) :

$$\prod_{m<x^{\frac{1+\theta}{2}}\log^{-1}x\prod_{i=2}^{\ell}p_i^{-1}}(a^{2m}-1). \tag{3.3}$$

Posons $S_a(\eta_1,\eta_2)=\{p:\ \exists q\in]\eta_1,\eta_2]$ tel que $q|p-1,\ a\in\mathfrak{R}(q,p)\}$. Ainsi

$$\mathcal{M}_{a,\ell}(x,x^{\frac{1-\theta}{2}}\log x,x)\ll\sum_{p_2\cdots p_\ell\leq x^{1-\theta}}\sum_{\substack{p_1\leq\frac{x}{p_2\cdots p_\ell}\\ p_1\in S_a(x^{\frac{1-\theta}{2}}\log x,x)}}1.$$

Les éléments de $S_a(x^{\frac{1-\theta}{2}}\log x, x)$ étant des nombres premiers, leur produit divise (3.3). En minorant par 2 chaque $p \in S_a(x^{\frac{1-\theta}{2}}\log x, x)$ on obtient :

$$2^{\#\{p_1 \leq \frac{x}{p_2\cdots p_\ell}:\ p_1 \in S_a(x^{\frac{1-\theta}{2}}\log x, x)\}} < \prod_{m<x^{\frac{1}{2}}\log^{-1}x\prod_{i=2}^{\ell}p_i^{-1}} a^{2m}.$$

Ainsi, en prenant le logarithme :

$$\#\Big\{p_1 \leq \frac{x}{p_2\cdots p_\ell}:\ p_1 \in S_a(x^{\frac{1-\theta}{2}}\log x, x)\Big\} < \frac{2\log|a|}{\log 2}\sum_{m<x^{\frac{1}{2}}\log^{-1}x\prod_{i=2}^{\ell}p_i^{-1}} m$$
$$= \mathcal{O}\left(\frac{x}{\log^2 x\prod_{i=2}^{\ell}p_i^2}\right),$$

et ainsi $\mathcal{M}_{a,\ell}(x, x^{\frac{1-\theta}{2}}\log x, x) \ll \sum_{p_2\cdots p_\ell \leq x^{1-\theta}} \frac{x}{\log^2 x\prod_{i=2}^{\ell}p_i^2} \ll \frac{x}{\log^2 x}$. □

Occupons nous maintenant de l'autre terme d'erreur.

Proposition 3.2. *Pour $C_1 \ll \frac{\log x}{\log\log x}$, on a*

$$\mathcal{M}_{a,\ell}(x, x^\theta, C_1, x^{\frac{1-\theta}{2}}\log x) \ll \frac{x}{C_1\log x}.$$

Démonstration. Dans $\mathcal{M}_{a,\ell}$ la condition "a vérifie $\mathcal{R}(q, p_1\dots p_\ell)$"implique qu'il existe $p \in \{p_1, \dots, p_\ell\}$ tel que a vérifie $\mathcal{R}(q,p)$. Le rôle des p_i étant symétriques, on peut supposer que a vérifie $\mathcal{R}(q,p_1)$.
Écrivons

$$\mathcal{M}_{a,\ell}(x, C_1, x^{\frac{1-\theta}{2}}\log x) \leq \#\left\{p_1\cdots p_\ell \leq x,\ p_i > x^\theta,\ \exists q \in]C_1, x^{\frac{1-\theta}{2}}\log x],\ a \text{ vérifie } \mathcal{R}(q,p_1)\right\}.$$

Posons $S := \#\left\{p_1\cdots p_\ell \leq x,\ p_i > x^\theta,\ \exists q \in]C_1, x^{\frac{1-\theta}{2}}\log x],\ a \text{ vérifie } \mathcal{R}(q,p_1)\right\}$.
Réécrivons maintenant S :

$$S \ll \sum_{C_1<q\leq x^{\frac{1-\theta}{2}}\log x}\ \sum_{p_2\cdots p_\ell \leq \frac{x}{q}}\ \sum_{\substack{q\leq p_1\leq \frac{x}{p_2\cdots p_\ell}\\ q|p_1-1\\ a\in\mathfrak{R}(q,p_1)}} 1.$$

On découpe la somme sur $p_2 \cdots p_\ell$ en trois parties selon la taille de $p_2 \cdots p_\ell$:

$$S_1 := \sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \sum_{p_2 \cdots p_\ell \leq \frac{x}{q^2 \log^6 x}} \sum_{\substack{q \leq p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1 \\ a \in \mathfrak{R}(q, p_1)}} 1,$$

$$S_2 := \sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \sum_{\frac{x}{q^2 \log^6 x} < p_2 \cdots p_\ell \leq \frac{x}{q^2} \log^2 x} \sum_{\substack{q \leq p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1}} 1,$$

$$S_3 := \sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \sum_{\frac{x}{q^2} \log^2 x < p_2 \cdots p_\ell \leq \frac{x}{q}} \sum_{\substack{q \leq p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1 \\ a \in \mathcal{R}(q, p_1)}} 1,$$

et ainsi $S \ll S_1 + S_2 + S_3$.
Pour majorer S_1 on utilise le lemme 2.2, qui est intéressant du moment que $\sqrt{x} \log x \ll \frac{x}{q^2 \log x}$, ce qui correspond à la zone $p_2 \cdots p_\ell \ll \frac{x}{q^2 \log^6 x}$.
Ainsi on peut majorer S_1 par

$$S_1 \ll \sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \sum_{p_2 \cdots p_\ell \leq \frac{x}{q^2 \log^6 x}} \left(\mathrm{Li}\left(\frac{x}{p_2 \cdots p_\ell} \right) \frac{1}{q(q-1)} + \sqrt{\frac{x}{p_2 \cdots p_\ell}} \log x \right).$$

Par sommation d'Abel on vérifie que le terme de reste est assez petit :

$$\sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \sum_{p_2 \cdots p_\ell \leq \frac{x}{q^2 \log^6 x}} \sqrt{\frac{x}{p_2 \cdots p_\ell}} \log x \ll \sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \frac{x}{q \log^2 x} \ll \frac{x}{\log^2 x} \log \log x.$$

Puis pour le terme principal, on ne peut que majorer trivialement :

$$\sum_{\substack{p_2 \cdots p_\ell \leq \frac{x}{q^2 \log^6 x} \\ x^\theta < p_i > x^{1-(\ell-1)\theta}}} \mathrm{Li}\left(\frac{x}{p_2 \cdots p_\ell} \right) \ll \frac{x}{\log x}.$$

Comme la somme sur q est un reste de série convergente on peut majorer S_1 :

$$S_1 \ll \frac{x}{C_1 \log x} + \frac{x}{\log^2 x} \log \log x.$$

Passons à la majoration de S_2.

Notons $E(x,n) := \{q,\ \sqrt{\frac{x}{n\log^6 x}} < q \leq \sqrt{\frac{x}{n}\log^2 x}\}$, en appliquant le Théorème de Brun-Titchmarsh on obtient :

$$\begin{aligned} S_2 &\ll \sum_{p_2\cdots p_\ell \leq x^{1-\theta}} \sum_{q\in E(x,p_2\cdots p_\ell)} \sum_{\substack{q<p_1\leq \frac{x}{p_2\cdots p_\ell}\\ q|p_1-1}} 1 \\ &\ll \sum_{p_2\cdots p_\ell \leq x^{1-\theta}} \sum_{q\in E(x,p_2\cdots p_\ell)} \frac{x}{qp_2\cdots p_\ell \log\left(\frac{x}{qp_2\cdots p_\ell}\right)}. \end{aligned}$$

On a $\sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-1} x \leq \frac{x}{qp_2\cdots p_\ell} \leq \sqrt{\frac{x}{p_2\cdots p_\ell}}\log^3 x$ et donc $\log\left(\frac{x}{qp_2\cdots p_\ell}\right) \sim \log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)$. Alors en appliquant le Théorème de Mertens,

$$\begin{aligned} \sum_{q\in E(x,p_2\cdots p_\ell)} \frac{1}{q} &\leq \log\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\log x\right) - \log\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-3} x\right) + \mathcal{O}\left(\log^{-1}\left(\frac{x}{p_2\cdots p_\ell}\right)\right) \\ &\leq \log\left(1+\frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}\right) - \log\left(1-\frac{3\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}\right) + \mathcal{O}\left(\log^{-1}\left(\frac{x}{p_2\cdots p_\ell}\right)\right) \\ &\leq \log\left(1+\frac{4}{1-\frac{3\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}}\frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}\right) + \mathcal{O}\left(\log^{-1}\left(\frac{x}{p_2\cdots p_\ell}\right)\right) \\ &\leq 4\frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)} + \mathcal{O}\left(\left(\frac{\log\log x}{\log\left(\sqrt{\frac{x}{p_2\cdots p_\ell}}\right)}\right)^2\right). \end{aligned}$$

Ainsi,

$$\begin{aligned} S_2 &\ll x\log\log x \sum_{\substack{p_2\cdots p_\ell \leq x^{1-\theta}\\ <x^\theta p_i<x^{1-(\ell-1)\theta}}} \frac{1}{p_2\cdots p_\ell \log^2\left(\frac{x}{p_2\cdots p_\ell}\right)}. \\ &\ll \frac{x\log\log x}{\log^2 x}. \end{aligned}$$

Passons à la majoration de S_3. On va procéder comme dans la proposition 3.1.

$$S_3 := \sum_{C_1 < q \leq x^{\frac{1-\theta}{2}} \log x} \sum_{\frac{x}{q^2} \log^2 x < p_2 \cdots p_\ell \leq \frac{x}{q}} \sum_{\substack{q \leq p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ q | p_1 - 1 \\ a \in \mathcal{R}(q, p_1)}} 1$$

Comme $a^{\frac{p_1-1}{q}} \equiv 1 (p_1)$ et donc $a^{2\frac{p_1-1}{q}} \equiv 1 (p_1)$, et $\frac{p_1-1}{q} \leq \frac{x}{q p_2 \cdots p_\ell} \leq \sqrt{\frac{x}{p_2 \cdots p_\ell}} \log^{-1} x$.
Ainsi il existe $m \leq \sqrt{\frac{x}{p_2 \cdots p_\ell}} \log^{-1} x$ tel que $p_1 | a^m - 1$. On en déduit l'inégalité

$$C_1^{\#\{x^\theta \leq p_1 \leq \frac{x}{p_2 \cdots p_\ell} :\ \exists q \geq \sqrt{\frac{x}{p_2}} \log x,\ a \equiv b^q \pmod{p)_1\}}} \leq \prod_{m \leq \sqrt{\frac{x}{p_2 \cdots p_\ell}} \frac{1}{\log x}} a^{2m}$$

et en prenant les logarithmes,

$$\begin{aligned} \#\{x^\theta \leq p_1 \leq \frac{x}{p_2 \cdots p_\ell} :\ \exists q \geq \sqrt{\frac{x}{p_2 \cdots p_\ell}} \log x,\ a \equiv b^q \pmod{p)_1\} &\leq \frac{2 \log a}{\log C_1} \sum_{m \leq \sqrt{\frac{x}{p_2 \cdots p_\ell}} \frac{1}{\log x}} m \\ &\ll \frac{x}{p_2 \cdots p_\ell \log C_1 \log^2 x}. \end{aligned}$$

En reportant cela dans S_3 on parvient à la majoration

$$\begin{aligned} S_3 &\ll \sum_{\substack{p_2 \cdots p_\ell \leq x^{1-\theta} \\ p_i > x^\theta}} \frac{x}{p_2 \cdots p_\ell \log C_1 \log^2 x} \\ &\ll \frac{x}{\log C_1 \log^2 x}. \end{aligned}$$

Les majorations de S_1, S_2 et S_3 obtenues précédemment impliquent que

$$\mathcal{M}_{a,\ell}(x, x^\theta, C_1, x^{\frac{1-\theta}{2}} \log x) \ll \frac{x}{C_1 \log x} + \frac{x (\log \log x)}{\log^2 x}.$$

□

Posons

$$\mathcal{P}_{a,\ell}(x, y, k) = \#\{n \leq x | P^-(n) > y, \Omega(n) = \ell,\ a \text{ vérifie } \mathcal{R}(q, n),\ \forall q | k\}.$$

On exprime $\mathcal{N}_{a,\ell}(x, x^\theta, C_1)$ en fonction de termes $\mathcal{P}_{a,\ell}(x, x^\theta, k)$. On a, par inclusion-exclusion :

$$\mathcal{N}_{a,\ell}(x, x^\theta, C_1) = \sum_{P^+(l') \leq C_1} \mu(l') \mathcal{P}_{a,\ell}(x, x^\theta, l').$$

3.1.2 Expression de $\mathcal{P}_{a,\ell}$

En reprenant la proposition 2.7 on obtient, *mutatis mutandis*, la proposition suivante.

Proposition 3.3. *Avec les notations précédentes, on a :*

$$\mathcal{P}_{a,\ell}(x,x^\theta,k)=\frac{1}{\ell!}\sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\}\\ \prod_{L\in\mathcal{P}^*(E)}k_L=k}}\ \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\}\\ g_L|k_L^\infty\\ k_L|g_L}}\ \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\}\\ c_{iL}|\frac{g_L}{k_L}}}\ \sum_{\substack{\left\{p_i>x^\theta,\ i\in\{1,\dots,\ell\}\right\}\\ p_1\cdots p_\ell\le x\\ (a,p_1\cdots p_\ell)=1\\ \forall i,\ (\frac{p_i-1}{u_i},k)=1\\ \forall i,\ a\in\mathfrak{R}\left(k_i',p_i\right)}}1, \tag{3.4}$$

où pour tout $i\in\{1,\dots,\ell\}$, $u_i:=\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}}g_L\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\notin L}}c_{iL}$, $k_i':=\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}}k_L'$, $\mathfrak{R}(l,n):=\{m\in\mathbb{N},\ \exists b\in\mathbb{N},\ m\equiv b^l\pmod n\}$ *et* $\mathcal{P}^*(E)$ *désigne l'ensemble des parties non-vides de* $E:=\{1,\dots,\ell\}$.

Afin de pouvoir calculer la dernière somme de $\mathcal{P}_{a,\ell}(x,x^\theta,k)$ nous aurons besoin de contrôler la taille des g_L , pour ce faire on reprend la proposition 2.8 et en remarquant que pour $u\ll\log^c x$ pour un certain entier c, on a par sommation d'Abel que $\sum_{\substack{x^\theta<p\le x\\ p\equiv 1\pmod u}}\frac{1}{p}\ll-\frac{\log\theta}{\varphi(u)}$.

Proposition 3.4. *Soient* C_1, C_5, t *tel que* $0<t<1$. *Alors dans la somme* $\mathcal{P}_{a,\ell}(x,x^\theta,k)$ *donnée par* (3.4) *on peut imposer* $g_L\le C_5$ *pour tout* $L\in\mathscr{P}^*(E)$, *au prix d'une erreur en* $\mathcal{O}_t\left(\frac{x}{C_5^t\log x}\right)$. *On a :*

$$\mathcal{P}_{a,\ell}(x,x^\theta,k)=\mathcal{P}_{a,\ell}{}'(x,x^\theta,k)+\mathcal{O}_t\left(\frac{x}{C_5^t\log x}\right),$$

où

$$\mathcal{P}_{a,\ell}{}'(x,x^\theta,k):=\frac{1}{\ell!}\sum_{\substack{\{k_L,\ L\in\mathcal{P}^*(E)\}\\ \prod_{L\in\mathcal{P}^*(E)}k_L=k}}\ \sum_{\substack{\{g_L,\ L\in\mathcal{P}^*(E)\}\\ g_L\le C_5\\ g_L|k_L^\infty\\ k_L|g_L}}\ \sum_{\substack{\{c_{iL},\ L\in\mathcal{P}^*(E),\ i\notin L\}\\ c_{iL}|\frac{g_L}{k_L}}}\ \sum_{\substack{\{d_i,\ i\in\{1,\dots,\ell\}\}\\ d_i|k}}\ \prod_{i\in\{1,\dots,\ell\}}\mu(d_i)Q(\boldsymbol{u},\boldsymbol{d}),$$

avec $Q(\boldsymbol{u},\boldsymbol{d}):=\sum_{\substack{\left\{p_i>x^\theta,\ i\in\{1,\dots,\ell\}\right\}\\ p_1\cdots p_\ell\le x\\ (a,p_1\cdots p_\ell)=1\\ \forall i,\ p_i\equiv 1(u_id_i)\\ \forall i,\ a\in\mathfrak{R}\left(k_i',p_i\right)}}1.$

3.2 Calcul du nombre de nombres premiers se factorisant convenablement

On pose, pour $1 \leq i \leq \ell$, $K_i := \mathbb{Q}(\sqrt[k_i']{a}, \xi_{u_i d_i})$ et on définit les ensembles de nombres premiers suivants P_{i,x^θ} constitués des premiers p tels que $p > x^\theta$, p est premier avec au_id_i et p se factorise dans $\mathcal{O}_{K_i}$ comme produit d'idéaux premiers distincts de norme p.
La quantité que l'on souhaite évaluer s'écrit alors d'après les propositions 2.9, 2.11 et 2.12, $\sum_{\substack{m_1\cdots m_\ell \leq x \\ p|m_i \Rightarrow p\in P_{i,x^\theta} \\ m_i \text{ premier}}} 1$.
Définissons, pour $\boldsymbol{r} := (r_1, \ldots, r_\ell) \in \mathbb{N}^\ell$, $n \in \mathbb{N}$,

$$c_{\boldsymbol{r}}(n) := \sum_{m_1\cdots m_\ell = n} \mu^2(n) \prod_{i=1}^{\ell} \left(\mathbb{1}\left(\Omega(m_i) = r_i\right) \mathbb{1}\left(p|m_i \Rightarrow p \in P_{i,x^\theta}\right)\right),$$

de sorte qu'en écrivant $\overline{1} = (1, \ldots, 1)$, on a l'égalité : $\sum_{\substack{m_1\cdots m_\ell \leq x \\ p|m_i \Rightarrow p\in P_{i,x^\theta} \\ m_i \text{ premier}}} 1 = \sum_{n\leq x} c_{\overline{1}}(n)$.

Notons $'\boldsymbol{r} \geq 0'$ lorsque pour tout $1 \leq i \leq \ell$, $r_i \geq 0$, puis pour $\boldsymbol{z} := (z_1, \ldots, z_\ell) \in \mathbb{C}^\ell$:

$$\alpha_{\boldsymbol{z}}(n) := \sum_{\boldsymbol{r}\geq 0} c_{\boldsymbol{r}}(n) \prod_{i=1}^{\ell} z_i^{r_i} = \sum_{\substack{m_1\cdots m_\ell = n \\ p|m_i \Rightarrow p\in P_{i,x^\theta}}} \mu^2(n) \prod_{i=1}^{\ell} z_i^{\omega(m_i)},$$

la fonction $\alpha_{\boldsymbol{z}}(n)$ est le produit de ℓ fonctions multiplicatives, elle est donc multiplicative. De plus, on a la majoration suivante :

Lemme 3.5. *En reprenant la définition de $\alpha_{\boldsymbol{z}}(n)$ ci-dessus, et pour $|z_i| \leq A$ pour tout i, on a :*

$$|\alpha_{\boldsymbol{z}}(n)| \leq n^{\frac{\log \ell A}{\theta \log x}}.$$

Démonstration. En majorant les $|z_i|$ par A il vient :

$$|\alpha_{\boldsymbol{z}}(n)| \leq \sum_{\substack{m_1\cdots m_\ell = n \\ p|m_i \Rightarrow p\in P_{i,x^\theta}}} \mu^2(n) A^{\omega(n)}.$$

Il y a $\ell^{\omega(n)}$ façons d'écrire n comme produit de ℓ nombres sans facteur carré. De plus, comme n est x^θ-criblé, $x^{\theta\omega(n)} \leq n$, et donc $\omega(n) \leq \frac{\log n}{\theta \log x}$.
On a donc bien $|\alpha_{\boldsymbol{z}}(n)| \leq n^{\frac{\log \ell A}{\theta \log x}}$. □

Enfin, pour $\Re(s) > 1$, on définit la série de Dirichlet associée à $\alpha_{\boldsymbol{z}}(n)$:

$$F(s,z) := \sum_{n\geq 0} \frac{\alpha_{\boldsymbol{z}}(n)}{n^s} = \prod_p \left(1 + \sum_{\nu\geq 1} \frac{\alpha_{\boldsymbol{z}}(p^\nu)}{p^{\nu s}}\right) = \prod_i \left(\prod_{p\in P_{i,x^\theta}} \left(1 + \frac{z_i}{p^s}\right)\right),$$

qui admet alors un prolongement analytique en une fonction méromorphe sur $\mathbb{C}\backslash\{1\}$. On réécrit $F(s,z)$ comme $F(s,z) = \prod_{i=1}^{\ell} F_i(s,z)$, où $F_i(s,z) := \prod_{p\in P_{i,x^\theta}} \left(1 + \frac{z_i}{p^s}\right)$.

On note $\zeta_{K_i}(s)$ la fonction zêta de Dedekind associée au corps K_i et $\zeta_{K_i}(s,y)$ le facteur initial de son produit eulérien, c'est-à-dire :

$$\zeta_{K_i}(s,y) := \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p})\leq y}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

De plus, soit $\zeta_{K_i,f}(s) := \prod_{\substack{\mathfrak{p} \\ \exists p,\ N(\mathfrak{p})=p^f}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$ et le facteur initial de ce produit eulérien $\zeta_{K_i,f}(s,y)$.

Enfin on définit $G(s,z) := \prod_{i=1}^{\ell} G_i(s,z)$, avec $G_i(s,z) := F_i(s,z) \left(\frac{\zeta_{K_i}(s,x^\theta)}{\zeta_{K_i}(s)}\right)^{\frac{z_i}{n_i}}$, et donc, pour $x^\theta > au_id_i$:

$$G_i(s,z) = \prod_{p\in P_{i,x^\theta}} \left[\left(1 + \frac{z_i}{p^s}\right)\left(1 - \frac{1}{p^s}\right)^{z_i}\right] \prod_{\substack{f|n_i \\ f\geq 2}} \left(\frac{\zeta_{K_i,f}(s)}{\zeta_{K_i,f}(s,x^\theta)}\right)^{-\frac{z_i}{n_i}}.$$

Proposition 3.6. *Soient $\theta \in]0, \frac{1}{2}[$, A un réel strictement positif. Pour $|z| \leq A$ et $\frac{1}{2} + \nu \leq \mathfrak{Re}\ s \leq 2$, avec $\nu > 0$, on a, pour x suffisamment grand :*

$$G(s, x^\theta, z) = 1 + \mathcal{O}_{C_1}\left(\frac{A^2}{x^{2\theta\nu}}\right).$$

Démonstration. Déjà pour tout i, et quand $x^\theta > au_id_i$,

$$\prod_{\substack{\mathfrak{p}\\ N(\mathfrak{p})|au_id_i\\ N(\mathfrak{p})=p\\ N(\mathfrak{p})>x^\theta}} \left(1-\frac{1}{p^s}\right)^{\frac{z_i}{n_i}} = 1,$$

car ce produit est alors vide. La contribution des degrés $f \geq 2$ est :

$$\prod_{\substack{f|n_i\\ f\geq 2}} \left(\frac{\zeta_{K_i,f}(s)}{\zeta_{K_i,f}(s,y)}\right)^{-\frac{z_i}{n_i}} = 1+\mathcal{O}_{C_1}\left(\frac{A}{x^{2\theta\nu}}\right).$$

En effectuant un développement limité, on montre que le premier produit dans la définition de $G_i(s,z)$ est également proche de 1 :

$$\prod_{\substack{p>x^\theta\\ p\in P_{i,x^\theta}}} \left(\left(1+\frac{z_i}{p^s}\right)\left(1-\frac{1}{p^s}\right)^{z_i}\right) = \prod_{\substack{p>x^\theta\\ p\in P_{i,x^\theta}}} \left(1+\mathcal{O}\left(\frac{A^2}{p^{1+2\nu}}\right)\right) = 1+\mathcal{O}_{C_1}\left(\frac{A^2}{x^{2\theta\nu}}\right).$$

□

La proposition suivante montre que l'on peut remplacer nos fonction zêta de Dedekind tronquées par des fonctions zêta de Riemann tronquées au prix d'un très petit terme d'erreur. Cela permet de simplifier grandement la suite du raisonnement.

Proposition 3.7. *Soit $\eta \in]0,3/5[$. Pour $s=\sigma+i\tau \in \mathbb{C}$ tel que $\sigma>1$ et $|\tau| \leq x$ on a*

$$\prod_{i=1}^{\ell}\left(\frac{\zeta_{K_i}(s)}{\zeta_{K_i}(s,x^\theta)}\right)^{\frac{z_i}{n_i}} = \left(\frac{\zeta(s)}{\zeta(s,x^\theta)}\right)^{\sum_{i=1}^{\ell}\frac{z_i}{n_i}} \left(1+\mathcal{O}_{A,\theta,\ell,C_1}\left(e^{-(\theta\log x)^\eta}\right)\right).$$

Démonstration. D'après le lemme III.5.5.16 de [37] (ou [36]) on a pour $\varepsilon>0$, $|\tau| \leq \exp\left((\theta\log x)^{\frac{3}{2}-3\varepsilon}\right)$, $\sigma > 1-\frac{1}{(\theta\log x)^{\frac{2}{5}-\varepsilon}+\left(\log(2+|\tau|)\right)^{\frac{2}{3}+\varepsilon}}$:

$$\zeta(s,x^\theta) = \zeta(s)(s-1)\theta\log x\hat{\rho}\big((s-1)\theta\log x\big)\left(1+\mathcal{O}\left(e^{-(\theta\log x)^\eta}\right)\right),$$

où $\hat{\rho}$ est la transformée de Laplace de la fonction de Dickman.

De même, d'après l'équation (4.2) du lemme 4.1 de [10], on a dans le même domaine,

$$\zeta_{K_i}(s,x^\theta)=\zeta_{K_i}(s)(s-1)\theta\log x\hat{\rho}\big((s-1)\theta\log x\big)\left(1+\mathcal{O}_{C_1}\left(e^{-(\theta\log x)^\eta}\right)\right).$$

En rassemblant les deux équations précédentes on obtient pour tout $i\in\{1,\dots,\ell\}$:

$$\frac{\zeta_{K_i}(s)}{\zeta_{K_i}(s,x^\theta)}=\frac{\zeta(s)}{\zeta(s,x^\theta)}\left(1+\mathcal{O}_{A,\theta,\ell,C_1}\left(e^{-(\theta\log x)^\eta}\right)\right).$$

Prenons le produits sur les $i\in\{1,\dots,\ell\}$ pour $\Re(s)>1$,

$$\prod_{i=1}^{\ell}\left(\frac{\zeta_{K_i}(s)}{\zeta_{K_i}(s,x^\theta)}\right)^{\frac{z_i}{n_i}}=\left(\frac{\zeta(s)}{\zeta(s,x^\theta)}\right)^{\sum\limits_{i=1}^{\ell}\frac{z_i}{n_i}}\left(1+\mathcal{O}_{A,\theta,\ell,C_1}\left(e^{-(\theta\log x)^\eta}\right)\right).$$

□

Proposition 3.8. *Avec les notations ci-dessus et pour $\kappa:=1+\frac{1}{\log x}$ on a :*

$$\sum_{n\le x}\alpha_{\boldsymbol{z}}(n)=\frac{1}{2i\pi}\int_{\kappa-ix}^{\kappa+ix}\left(\frac{\zeta(s)}{\zeta(s,x^\theta)}\right)^{\sum\limits_i\frac{z_i}{n_i}}\frac{x^s}{s}ds+\mathcal{O}_{A,\theta,\ell,C_1}\left(\frac{x\log x}{e^{(\theta\log x)^\eta}}\right).$$

Démonstration. En utilisant la première formule de Perron effective (Théorème II.2.3 [37] ou [36]) on obtient

$$\sum_{n\le x}\alpha_{\boldsymbol{z}}(n)=\frac{1}{2i\pi}\int_{\kappa-ix}^{\kappa+ix}F(s,x^\theta,z)\frac{x^s}{s}ds+\mathcal{O}\left(x\sum_{n\ge1}\frac{|\alpha_{\boldsymbol{z}}(n)|}{n^\kappa(1+x|\log(x/n)|)}\right).$$

Occupons nous du terme d'erreur. Si n n'est pas x^θ-criblé, $\alpha_{\boldsymbol{z}}(n)=0$. Ensuite pour n x^θ-criblé, on a par le lemme 3.5,

$$|\alpha_{\boldsymbol{z}}(n)|\le n^{\frac{\log lA}{\theta\log x}}.$$

Pour calculer la somme du terme d'erreur on la découpe en deux parties, suivant si n est entre $\frac{x}{2}$ et $2x$ ou non. La contribution des $n\notin[\frac{x}{2},2x]$ est :

$$x\sum_{n\notin[\frac{x}{2},2x]}\frac{|\alpha_{\boldsymbol{z}}(n)|}{n^\kappa(1+x|\log(x/n)|)}\ll\sum_{n\ge1}n^{-(1+\frac{1}{\log x}(1-\frac{\log lA}{\theta}))}\ll_{A,\theta}\log x.$$

Puis pour $n \in [\frac{x}{2}, 2x]$, on a $|\alpha_{\boldsymbol{z}}(n)| \leq (2x)^{\frac{\log lA}{\theta \log x}} \ll (lA)^{\frac{1}{\theta}}$. On considère maintenant que $\{x\} = \frac{1}{2}$, et on écrit $n = N + \Delta$, où N est l'entier le plus proche de x. On a $|\log\left(\frac{x}{n}\right)| \gg \frac{|\Delta|}{x}$. La contribution des $n \in [\frac{x}{2}, 2x]$ à la somme du terme d'erreur est :

$$\begin{aligned} x \sum_{\frac{x}{2} \leq n \leq 2x} \frac{|\alpha_{\boldsymbol{z}}(n)|}{n^{\kappa}(1 + x|\log(x/n)|)} &\ll (\ell A)^{\frac{1}{\theta}} \sum_{\frac{x}{2} \leq n \leq 2x} \frac{1}{1 + x|\log(x/n)|} \\ &\ll (\ell A)^{\frac{1}{\theta}} \sum_{0 \leq \Delta \leq \frac{3}{2}x+1} \frac{1}{1+|\Delta|} \ll_{\ell, A, \theta} \log x. \end{aligned}$$

En utilisant les propositions 3.6 et 3.7 on a

$$\sum_{n \leq x} \alpha_{\boldsymbol{z}}(n) = \frac{1}{2i\pi} \int_{\kappa - ix}^{\kappa + ix} \left(\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right)^{\sum_{i=1}^{\ell} \frac{z_i}{n_i}} \frac{x^s}{s} ds + \mathcal{O}_{A,\theta,\ell,C_1}\left(x \int_{\kappa - ix}^{\kappa + ix} \left|\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right|^{\ell A} \frac{e^{-(\theta \log x)^{\eta}}}{|s|} ds\right).$$

Or $\left|\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right| \leq \sum_{\substack{n \\ P^-(n) > x^{\theta}}} \frac{1}{n^{1 + \frac{1}{\log x}}} \ll e^{\theta}$ pour $\Re(s) > \kappa$. Ainsi,

$$\sum_{n \leq x} \alpha_{\boldsymbol{z}}(n) = \frac{1}{2i\pi} \int_{\kappa - ix}^{\kappa + ix} \left(\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right)^{\sum_{i=1}^{\ell} \frac{z_i}{n_i}} \frac{x^s}{s} ds + \mathcal{O}_{A,\theta,\ell,C_1}\left(\frac{x \log x}{e^{(\theta \log x)^{\eta}}}\right).$$

□

Pour obtenir l'estimation désirée on va appliquer la formule de Cauchy ℓ fois à $\sum_{n \leq x} \alpha_{\boldsymbol{z}}(n)$, ainsi :

$$\begin{aligned} \sum_{\substack{m_1 \cdots m_{\ell} \leq x \\ p | m_i \Rightarrow p \in P_{i, x^{\theta}} \\ m_i \text{ premier}}} 1 &= \oiint_{\Omega} \sum_{n \leq x} \alpha_{\boldsymbol{z}}(n) \prod_i dz_i \\ &= \frac{1}{(2i\pi)^{\ell+1}} \oiint_{\Omega} \int_{\kappa - ix}^{\kappa + ix} \left(\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right)^{\sum_{i=1}^{\ell} \frac{z_i}{n_i}} \frac{x^s}{s} ds \prod_i dz_i + \mathcal{O}_{A,\theta,\ell,C_1}\left(\frac{x \log x}{e^{(\theta \log x)^{\eta}}}\right). \end{aligned}$$

Où Ω est le produit de ℓ cercles autour de l'origine de rayon plus petit que A. En faisant les ℓ changements de variable $z_i' := \frac{z_i}{n_i}$, on obtient :

$$\oiint_{\Omega} \int_{\kappa - ix}^{\kappa + ix} \left(\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right)^{\sum_{i=1}^{\ell} \frac{z_i}{n_i}} \frac{x^s}{s} ds \prod_i dz_i = \frac{1}{\prod_i n_i} \oiint_{\Omega} \int_{\kappa - ix}^{\kappa + ix} \left(\frac{\zeta(s)}{\zeta(s, x^{\theta})}\right)^{\sum_{i=1}^{\ell} z_i'} \frac{x^s}{s} ds \prod_i dz_i'.$$

Voyons maintenant que ces intégrales correspondent au nombre d'entiers x^θ-criblés ayant ℓ facteurs premiers. On définit la fonction de comptage de ces entiers :

$$\pi(x,y,k) := \{n,\ P^-(n) > y,\ \Omega(n) = k\}.$$

Proposition 3.9. *Avec les notations précédentes, on a :*

$$\sum_{\substack{m_1\cdots m_\ell \le x \\ p|m_i \Rightarrow p\in P_{i,x^\theta} \\ m_i \text{ premier}}} 1 = \frac{1}{\prod_i n_i}\pi(x,x^\theta,\ell) + \mathcal{O}_{A,\theta,\ell,C_1}\left(\frac{x\log x}{e^{(\theta\log x)^\eta}}\right).$$

Démonstration. Définissons, pour $\boldsymbol{r} := (r_1,\dots,r_\ell) \in \mathbb{N}^\ell$, $n \in \mathbb{N}$,

$$c'_{\boldsymbol{r}}(n) := \sum_{m_1\cdots m_\ell = n} \mu^2(n) \prod_{i=1}^{\ell} \left(\mathbb{1}\left(\Omega(m_i) = r_i\right)\mathbb{1}\left(P^-(m_i) > x^\theta\right)\right).$$

puis, en posant $\overline{1} = (1,\dots,1)$, $\sum_{n\le x} c'_{\overline{1}}(n) = \#\{n \le x,\ P^-(n) > x^\theta,\ \Omega(n) = \ell\}$.

En posant $\alpha'_{\boldsymbol{z}}(n) := \sum_{\boldsymbol{r}\ge 0} c'_{\boldsymbol{r}}(n)\prod_{i=1}^{\ell} z_i^{r_i}$, $F'(s,z) := \sum_{n\ge 0}\frac{\alpha'_{\boldsymbol{z}}(n)}{n^s}$ et $G'(s,z) := F'(s,z)\left(\frac{\zeta(s,x^\theta)}{\zeta(s)}\right)^{\sum_i z'_i}$ et en procédant comme précédemment il vient pour $\frac{1}{2} < \nu < 1$:

$$\sum_{n\le x} c'_{\overline{1}}(n) = \frac{1}{(2i\pi)^{\ell+1}} \oiint_{\Omega} \int_{\kappa-ix}^{\kappa+ix} \left(\frac{\zeta(s)}{\zeta(s,x^\theta)}\right)^{\sum_{i=1}^{\ell} z'_i} \frac{x^s}{s} ds \prod_i dz'_i + \mathcal{O}_{A,\theta,\ell,C_1}\left(x^{1-2\theta\nu}\log x\right),$$

ce qui permet de conclure. □

Enfin une formule asymptotique pour $\pi(x,y,k)$ a été démontrée par Balazard ([2], lemme 8).

Lemme 3.10 (Balazard)**.** *Soit $R > 0$. On a uniformément pour $x \geq 3$, $\exp\left((\log\log x)^3\right) < y < x^{1/\max(2,\ell)}$ et $1 \leq \ell \leq R(\log\log x - \log\log y)$:*

$$\pi(x,y,\ell) = f_\ell\left(\frac{\log x}{\log y}\right)\frac{x}{\log x} + \mathcal{O}_R\left(\frac{x}{\log^2 x}\sqrt{\ell}\frac{(\log\log x - \log\log y)^\ell}{\ell!}\right),$$

où les fonctions f_ℓ sont définies par récurrence telles que :

- $f_1(u) := 1$ *pour* $u \geq 1$,
- $f_{k+1}(u) := \int_k^{u-1} f_k(v)\frac{dv}{v}$ *pour* $u > k+1$.

Ainsi, en prenant $R = \frac{1}{\theta\log\frac{1}{\theta}}$, on obtient dans notre cas pour $2 \leq \ell \leq \left\lfloor\frac{1}{\theta}\right\rfloor$,

$$\pi(x,x^\theta,\ell) = f_\ell\left(\frac{1}{\theta}\right)\frac{x}{\log x} + \mathcal{O}_\theta\left(\frac{x}{\log^2 x}\sqrt{\ell}\frac{(\log\frac{1}{\theta})^\ell}{\ell!}\right),$$

puis en injectant ce résultat dans la proposition 3.9 on obtient la proposition suivante.

Proposition 3.11. *En reprenant les notations de la proposition 3.9 et du lemme 3.10 on a :*

$$\sum_{\substack{\{p_i > x^\theta,\ i\in\{1,\dots,\ell\}\}\\ p_1\cdots p_\ell \leq x\\ (a,p_1\cdots p_\ell)=1\\ \forall i,\ p_i\equiv 1(u_i d_i)\\ \forall i,\ a\in\mathfrak{R}\left(k_i',p_i\right)}} 1 = \frac{1}{\prod_i n_i} f_\ell\left(\frac{1}{\theta}\right)\frac{x}{\log x} + \mathcal{O}_{A,\theta,\ell,C_1}\left(\frac{x\log x}{e^{(\theta\log x)^\eta}}\right).$$

3.3 Preuve des théorèmes 0.6 et 0.7

Le calcul de $\mathcal{P}_{a,\ell}{}'(x,x^\theta,k)$ est identique à celui de la section 2.7. Ainsi on obtient le théorème 0.6 avec les propositions 3.1, 3.2, 3.4, 3.11 et l'équation 3.2 et le théorème 0.7 avec les propositions 3.4, 3.11 et l'équation (3.1).

Annexe A

Valeurs particulières pour le théorème 0.3

Les différentes valeurs reproduites dans cette annexe ont été obtenues en utilisant le logiciel SageMath.

A.1 $W_\ell(p)$

A.1.1 Valeurs de $W_\ell(p)$

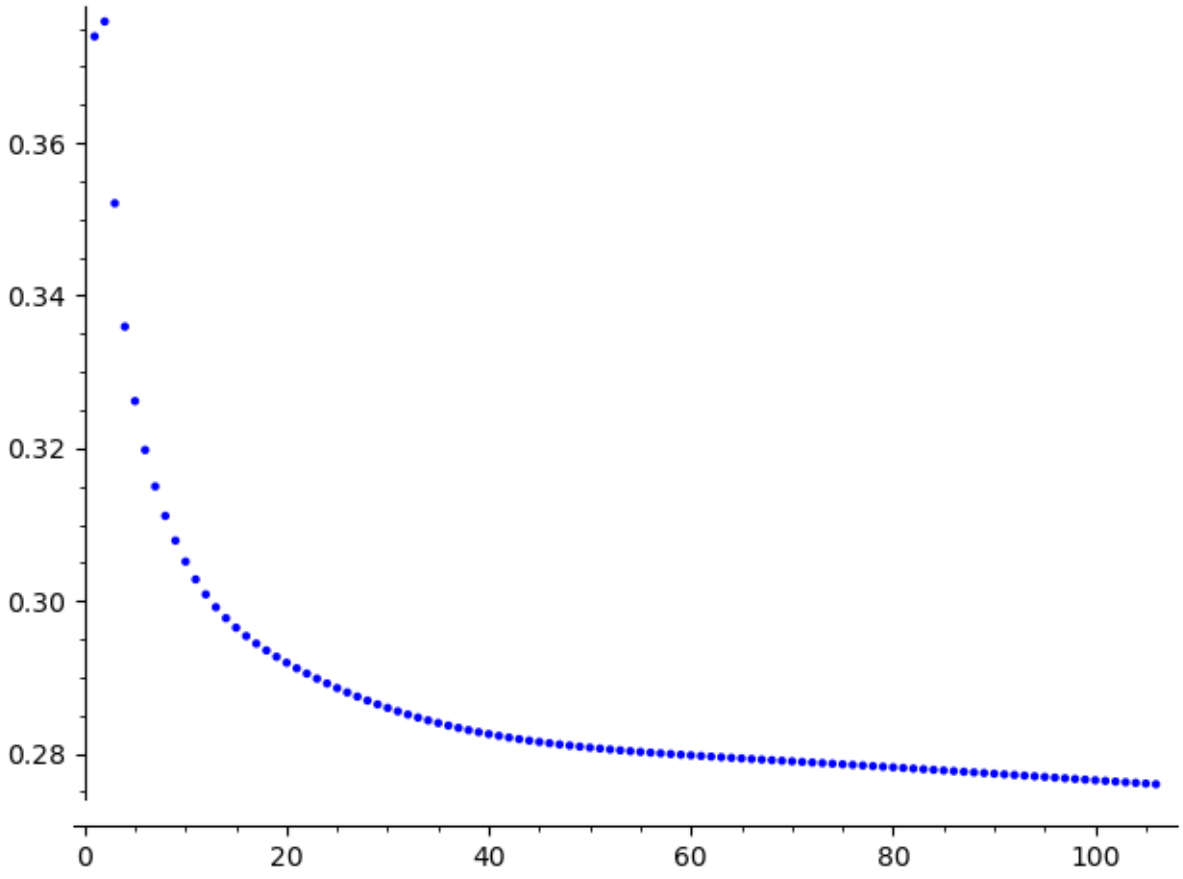
On donne dans le tableau ci-dessous les valeurs de $W_\ell(p)$ pour les premières valeurs de ℓ, dans le cas où $h = 1$.

ℓ	$W_\ell(p)$
1	$\frac{1}{p(p-1)}$
2	$\frac{2p^3-2p^2-p-1}{p^2(p-1)^2(p+1)}$
3	$\frac{3p^7-6p^6+3p^5-6p^4+7p^3+2p^2+2p+1}{p^3(p-1)^3(p+1)(p^2+p+1)}$
4	$\frac{4p^9-16p^8+26p^7-28p^6+28p^5-14p^4-p^3-2p^2-2p-1}{p^4(p-1)^4(p+1)(p^2+p+1)}$
5	$\frac{5p^{15}-25p^{14}+55p^{13}-70p^{12}+60p^{11}-40p^{10}+35p^9-65p^8+76p^7-57p^6+35p^5+6p^4+6p^3+5p^2+3p+1}{p^5(p-1)^5(p+1)(p^2+p+1)(p^4+p^3+p^2+p+1)}$

Pour $\ell \geq 6$ les formules deviennent trop longues pour être reproduites ici.

A.1.2 Valeurs approchées de $\prod_p (1 - W_\ell(p))$

Ci-dessous un graphe de $\prod_p (1 - W_\ell(p))$ en fonction de ℓ dans le cas où $h = 1$. Le produit est pris pour $p \leq 48623$, c'est-à-dire pour les 5000 premiers nombres premiers.



A.2 $V_\ell(a_1)$

On donne dans le tableau ci-dessous les valeurs tronquées de $V_\ell(a_1)$ pour différentes valeurs de a_1 et ℓ.

$V_\ell(a_1)$	$a=2$	$a=3$	$a=5$	$a=6$	$a=7$	$a=8$
$\ell=1$	0	0	$\simeq 0.052632$	0	0	0
$\ell=2$	$\simeq -0.142857$	$\simeq 0.05102$	$\simeq 0.031732$	$\simeq 0.012755$	$\simeq 0.008699$	$\simeq -0.142857$
$\ell=3$	$\simeq -0.310606$	$\simeq 0.017713$	$\simeq 0.018778$	$\simeq 0.007895$	$\simeq 0.009314$	$\simeq -0.310606$
$\ell=4$	$\simeq -0.467005$	$\simeq 0.001676$	$\simeq 0.010461$	$\simeq 0.001283$	$\simeq 0.007427$	$\simeq -0.467005$
$\ell=5$	$\simeq -0.595831$	$\simeq -0.002917$	$\simeq 0.005125$	$\simeq -0.001839$	$\simeq 0.00522$	$\simeq -0.595831$
$\ell=6$	$\simeq -0.695917$	$\simeq -0.002907$	$\simeq 0.001828$	$\simeq -0.002189$	$\simeq 0.003336$	$\simeq -0.695917$
$\ell=10$	$\simeq -0.90375$	$\simeq 0.000572$	$\simeq -0.001548$	$\simeq 0.000537$	$\simeq -0.000436$	$\simeq -0.90375$
$\ell=15$	$\simeq -0.977154$	$\simeq 9.4e-05$	$\simeq -0.000349$	$\simeq 9.4e-05$	$\simeq -0.000984$	$\simeq -0.977154$
$\ell=20$	$\simeq -0.994579$	$\simeq -0.000206$	$\simeq 0.00039$	$\simeq -0.000205$	$\simeq -0.000477$	$\simeq -0.994579$
$\ell=25$	$\simeq -0.998714$	$\simeq -8.2e-05$	$\simeq 0.000452$	$\simeq -8.2e-05$	$\simeq -1.4e-05$	$\simeq -0.998714$
$\ell=50$	$\simeq -0.999999$	$\simeq -8e-06$	$\simeq -0.000169$	$\simeq -8e-06$	$\simeq 0.000189$	$\simeq -0.999999$

$V_\ell(a_1)$	$a=10$	$a=12$	$a=15$	$a=21$	$a=27$	$a=50$
$\ell=1$	0	0	0	$\simeq -0.004878$	0	0
$\ell=2$	$\simeq 0.004339$	$\simeq 0.05102$	$\simeq -0.001452$	$\simeq -0.001243$	$\simeq 0.571429$	$\simeq -0.142857$
$\ell=3$	$\simeq 0.005844$	$\simeq 0.017713$	$\simeq -0.000332$	$\simeq -0.000232$	$\simeq 0.787879$	$\simeq -0.310606$
$\ell=4$	$\simeq 0.004995$	$\simeq 0.001676$	$\simeq -1.5e-05$	$\simeq -6e-06$	$\simeq 0.893401$	$\simeq -0.467005$
$\ell=5$	$\simeq 0.003154$	$\simeq -0.002917$	$\simeq 1.5e-05$	$\simeq 2e-05$	$\simeq 0.946556$	$\simeq -0.595831$
$\ell=6$	$\simeq 0.001322$	$\simeq -0.002907$	$\simeq 5e-06$	$\simeq 1.1e-05$	$\simeq 0.973267$	$\simeq -0.695917$
$\ell=10$	$\simeq -0.001442$	$\simeq 0.000572$	$\simeq 1e-06$	$\simeq 0.0$	$\simeq 0.998331$	$\simeq -0.90375$
$\ell=15$	$\simeq -0.000346$	$\simeq 9.4e-05$	$\simeq 0.0$	$\simeq 0.0$	$\simeq 0.999948$	$\simeq -0.977154$
$\ell=20$	$\simeq 0.000389$	$\simeq -0.000206$	$\simeq 0.0$	$\simeq -0.0$	$\simeq 0.999998$	$\simeq -0.994579$
$\ell=25$	$\simeq 0.000452$	$\simeq -8.2e-05$	$\simeq 0.0$	$\simeq -0.0$	$\simeq 1.0$	$\simeq -0.998714$
$\ell=50$	$\simeq -0.000169$	$\simeq -8e-06$	$\simeq -0.0$	$\simeq 0.0$	$\simeq 1.0$	$\simeq -0.999999$

Dans les cas où a est le double d'un carré (c'est-à-dire $a \in \{2, 8, 50\}$) $V_\ell(a_1)$ est proche de -1 et donc $1+V_\ell(a_1) \simeq 0$, car a est dans l'ensemble exceptionnel $\mathcal{E}$ décrit par Li [20].
Pour $a = 27$, $V_\ell(a_1)$ est proche de 1 car 27 est une puissance parfaite.
Quant aux autres valeurs de $V_\ell(a_1)$ elles deviennent toutes très proches de 0.

A.3 $C_\ell(a)$

À partir des quantités $\prod_p (1 - W_\ell(p))$ et $V_\ell(a_1)$ calculées précédemment on peut estimer la valeur de $C_\ell(a) = \lim_{x\to\infty} \mathcal{N}_{a,\ell}(x)/\frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}$.

$C_\ell(a)$	$a=2$	$a=3$	$a=5$	$a=6$	$a=7$	$a=8$
$\ell=1$	$\simeq 0.373956$	$\simeq 0.373956$	$\simeq 0.393638$	$\simeq 0.373956$	$\simeq 0.373956$	$\simeq 0.224374$
$\ell=2$	$\simeq 0.322212$	$\simeq 0.395093$	$\simeq 0.387842$	$\simeq 0.380709$	$\simeq 0.379184$	$\simeq 0.103568$
$\ell=3$	$\simeq 0.242734$	$\simeq 0.358334$	$\simeq 0.358709$	$\simeq 0.354877$	$\simeq 0.355377$	$\simeq 0.039683$
$\ell=4$	$\simeq 0.179054$	$\simeq 0.336502$	$\simeq 0.339453$	$\simeq 0.33637$	$\simeq 0.338434$	$\simeq 0.014625$
$\ell=5$	$\simeq 0.131835$	$\simeq 0.325237$	$\simeq 0.327861$	$\simeq 0.325589$	$\simeq 0.327891$	$\simeq 0.00536$
$\ell=6$	$\simeq 0.097239$	$\simeq 0.318848$	$\simeq 0.320362$	$\simeq 0.319078$	$\simeq 0.320844$	$\simeq 0.00197$
$\ell=10$	$\simeq 0.029372$	$\simeq 0.305336$	$\simeq 0.304689$	$\simeq 0.305326$	$\simeq 0.305029$	$\simeq 3.7e-05$
$\ell=15$	$\simeq 0.006774$	$\simeq 0.296534$	$\simeq 0.296402$	$\simeq 0.296534$	$\simeq 0.296214$	$\simeq 0.0$
$\ell=20$	$\simeq 0.001583$	$\simeq 0.291857$	$\simeq 0.29203$	$\simeq 0.291857$	$\simeq 0.291777$	$\simeq 0.0$
$\ell=25$	$\simeq 0.000371$	$\simeq 0.288571$	$\simeq 0.288725$	$\simeq 0.288571$	$\simeq 0.28859$	$\simeq 0.0$
$\ell=50$	$\simeq 0.0$	$\simeq 0.28079$	$\simeq 0.280744$	$\simeq 0.28079$	$\simeq 0.280845$	$\simeq 0.0$

$C_\ell(a)$	$a=10$	$a=12$	$a=15$	$a=21$	$a=27$	$a=50$
$\ell=1$	$\simeq 0.373956$	$\simeq 0.373956$	$\simeq 0.373956$	$\simeq 0.372132$	$\simeq 0.224374$	$\simeq 0.373956$
$\ell=2$	$\simeq 0.377545$	$\simeq 0.395093$	$\simeq 0.375368$	$\simeq 0.375447$	$\simeq 0.189875$	$\simeq 0.322212$
$\ell=3$	$\simeq 0.354155$	$\simeq 0.358334$	$\simeq 0.35198$	$\simeq 0.352016$	$\simeq 0.102914$	$\simeq 0.242734$
$\ell=4$	$\simeq 0.337617$	$\simeq 0.336502$	$\simeq 0.335934$	$\simeq 0.335937$	$\simeq 0.051953$	$\simeq 0.179054$
$\ell=5$	$\simeq 0.327217$	$\simeq 0.325237$	$\simeq 0.326194$	$\simeq 0.326195$	$\simeq 0.025815$	$\simeq 0.131835$
$\ell=6$	$\simeq 0.3202$	$\simeq 0.318848$	$\simeq 0.319779$	$\simeq 0.319781$	$\simeq 0.012782$	$\simeq 0.097239$
$\ell=10$	$\simeq 0.304722$	$\simeq 0.305336$	$\simeq 0.305162$	$\simeq 0.305162$	$\simeq 0.000771$	$\simeq 0.029372$
$\ell=15$	$\simeq 0.296403$	$\simeq 0.296534$	$\simeq 0.296506$	$\simeq 0.296506$	$\simeq 2.3e-05$	$\simeq 0.006774$
$\ell=20$	$\simeq 0.29203$	$\simeq 0.291857$	$\simeq 0.291917$	$\simeq 0.291917$	$\simeq 1e-06$	$\simeq 0.001583$
$\ell=25$	$\simeq 0.288725$	$\simeq 0.288571$	$\simeq 0.288594$	$\simeq 0.288594$	$\simeq 0.0$	$\simeq 0.000371$
$\ell=50$	$\simeq 0.280744$	$\simeq 0.28079$	$\simeq 0.280792$	$\simeq 0.280792$	$\simeq 0.0$	$\simeq 0.0$

On retrouve ici les deux cas de figure possibles, suivant si a est dans l'ensemble $\mathcal{E}$ décrit par Li ou non.

Bibliographie

[1] K. Alladi. The distribution of $\nu(n)$ in the sieve of Eratosthenes. *Q. J. Math., Oxf. II. Ser.*, 33 :129–148, 1982.

[2] M. Balazard. Unimodality of the distribution of the number of prime divisors of an integer. *Ann. Inst. Fourier*, 40(2) :255–270, 1990.

[3] H. Bilharz. Primdivisoren mit vorgegebener Primitivwurzel. *Math. Ann.*, 114 :476–492, 1937.

[4] A. Buchstab. Asymptotische Abschätzung einer allgemeinen zahlentheoretischen Funktion. *Rec. Math. Moscou, n. Ser.*, 2 :1239–1246, 1937.

[5] R. D. Carmichael. Note on a new number theory function. *Bull. Am. Math. Soc.*, 16 :232–238, 1910.

[6] A. Emil. *The collected papers of Emil Artin / edited by Serge Lang, John T. Tate.* Addison-Wesley publishing company, Reading (Massachusetts) Palo Alto [etc, C 1965.

[7] C. F. Gauss. Recherches arithmétiques. Traduction *Poullet-Delisle.*

[8] É. Goudout. Local laws of the ω function in almost all short intervals. *Proc. Lond. Math. Soc. (3)*, 115(3) :599–637, 2017.

[9] R. Gupta and M. R. Murty. A remark on Artin's conjecture. *Invent. Math.*, 78(1) :127–130, 1984.

[10] G. Hanrot, G. Tenenbaum, and J. Wu. Averages of certain multiplicative functions over friable integers. II. *Proc. Lond. Math. Soc. (3)*, 96(1) :107–135, 2008.

[11] H. Hasse. *Vorlesungen über Zahlentheorie*, volume 59 of *Grundlehren Math. Wiss.* Springer, Cham, 1950.

[12] D. R. Heath-Brown. The growth rate of the Dedekind zeta-function on the critical line. *Acta Arith.*, 49(4) :323–339, 1988.

[13] A. Hildebrand and G. Tenenb aum. On the number of prime factors of an integer. *Duke Math. J.*, 56(3) :471–501, 1988.

[14] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225 :209–220, 1967.

[15] S. Kerner. *Répartition d'entiers avec contraintes sur les diviseurs*. Theses, Université Henri Poincaré - Nancy 1, Dec. 2002. Texte intégral accessible uniquement aux membres de l'Université de Lorraine.

[16] E. Landau. On some problems concerning the distribution of prime numbers. *Bull. Soc. Math. Fr.*, 28 :25–38, 1900.

[17] E. Landau. *Einführung in die elemetare und analytische Theorie der algebraischen Zahlen und der Ideale*. B. G. Teubner, 1918.

[18] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Am. Math. Soc.*, 83 :289–292, 1977.

[19] E. S. Lee. On an explicit zero-free region for the Dedekind zeta-function. *J. Number Theory*, 224 :307–322, 2021.

[20] S. Li. On extending Artin's conjecture to composite moduli. *Mathematika*, 46(2) :373–390, 1999.

[21] S. Li and C. Pomerance. Primitive roots : a survey. In *Number theoretic methods. Future trends. Proceedings of the 2nd China-Japan seminar, Iizuka, Fukuoka, Japan, March 12–16, 2001*, pages 219–231. Dordrecht : Kluwer Academic Publishers, 2002.

[22] S. Li and C. Pomerance. On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.*, 556 :205–224, 2003.

[23] S. Li and C. Pomerance. The Artin-Carmichael primitive root problem on average. *Mathematika*, 55(1-2) :167–176, 2009.

[24] G. Martin. The least prime primitive root and the shifted sieve. *Acta Arith.*, 80(3) :277–288, 1997.

[25] P. Moree. Artin's primitive root conjecture – a survey. *Integers*, 12(6) :1305–1416, a13, 2012.

[26] M. R. Murty. Artin's conjecture for primitive roots. *Math. Intell.*, 10(4) :59–67, 1988.

[27] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[28] J.-L. Nicolas. Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers. *Acta Arith.*, 44 :191–200, 1984.

[29] L. G. Sathe. On a problem of Hardy on the distribution of integers having a given number of prime factors. I. *J. Indian Math. Soc., New Ser.*, 17 :63–82, 1953.

[30] L. G. Sathe. On a problem of Hardy on the distribution of integers having a given number of prime factors. II. *J. Indian Math. Soc., New Ser.*, 17 :83–141, 1953.

[31] L. G. Sathe. On a problem of Hardy on the distribution of integers having a given number of prime factors. III. *J. Indian Math. Soc., New Ser.*, 18 :27–42, 1954.

[32] L. G. Sathe. On a problem of Hardy on the distribution of integers having a given number of prime factors. IV. *J. Indian Math. Soc., New Ser.*, 18 :43–81, 1954.

[33] A. Selberg. Note on a paper by L. G. Sathe. *J. Indian Math. Soc., New Ser.*, 18 :83–87, 1954.

[34] P. J. Stephens. An average result for Artin's conjecture. *Mathematika*, 16 :178–188, 1969.

[35] P. Stevenhagen. The correction factor in Artin's primitive root conjecture. *J. Théor. Nombres Bordx.*, 15(1) :383–391, 2003.

[36] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[37] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. Sciences sup. Dunod, Malakoff, [5e édition] edition, DL 2022.

[38] D. Wang. The Selberg-Delange method in short intervals for the Dedekind zeta function. *Acta Arith.*, 192(3) :301–311, 2020.

[39] A. Weil. On the Riemann hypothesis in function-fields. *Proc. Natl. Acad. Sci. USA*, 27 :345–347, 1941.

[40] S. H. Weintraub. *Galois theory.* Universitext. Springer, New York, second edition, 2009.