Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

SUR UNE GÉNÉRALISATION DE LA CONJECTURE D'ARTIN PARMI LES PRESQUE-PREMIERS

Paul Péringuey

Tome 152
Fascicule 3

2024

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 377-442

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 3, tome 152, septembre 2024

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 160 € ($ 240),
avec supplément papier : Europe 244 €, hors Europe 330 € ($ 421)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Isabelle GALLAGHER

Bull. Soc. Math. France
152 (3), 2024, p. 377-442

SUR UNE GÉNÉRALISATION DE LA CONJECTURE D'ARTIN PARMI LES PRESQUE-PREMIERS

par Paul Péringuey

Résumé. — Un entier est une racine primitive modulo un premier p s'il génère le sous-groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. En 1927 Artin conjecture qu'un nombre a qui n'est ni -1 ni un carré parfait est racine primitive pour une infinité de nombres premiers, et que l'ensemble de ces premiers a une densité positive parmi tous les premiers. Cette conjecture a été démontrée, sous l'hypothèse de Riemann généralisée (GRH), en 1967 par Hooley.

Plus généralement, on dit qu'un entier est une racine primitive généralisée modulo n s'il génère un sous-groupe de taille maximale dans $(\mathbb{Z}/n\mathbb{Z})^*$. Li et Pomerance ont montré, sous GRH, que l'ensemble des entiers pour lesquels un entier est racine primitive généralisée n'admet pas de densité parmi tous les entiers.

On s'intéresse ici à l'ensemble des entiers ℓ-presque premiers, c'est-à-dire les entiers ayant au plus ℓ facteurs premiers, pour lesquels un entier $a \in \mathbb{Z} \setminus \{-1\}$ donné et différent d'un carré est racine primitive généralisée, et nous montrons, sous GRH, que cet ensemble admet une densité parmi tous les ℓ-presque premiers.

Texte reçu le 1er juin 2023, modifié le 16 février 2024, accepté le 22 février 2024.

Paul Péringuey, University of British Columbia, 1984 Mathematics Road, Vancouver BC V6T 1Z2, Canada • *E-mail :* peringuey@math.ubc.ca

Classification mathématique par sujets (2010). — 11A07, 11N25, 11R42, 11R44.

Mots clefs. — Théorie analytique des nombres, conjecture d'Artin, racines primitives, presque premiers, méthode de Selberg-Delange.

0037-9484/2024/377/$ 5.00
doi:10.24033/bsmf.2892

Abstract (*On a generalization of Artin's conjecture among almost primes*). — An integer is a primitive root modulo a prime p if it generates the whole multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. In 1927 Artin conjectured that an integer a which is not -1 or a square is a primitive root for infinitely many primes, and that the set of those primes has a positive asymptotic density among all primes. This conjecture was proved, under the generalized Riemann hypothesis (GRH), in 1967 by Hooley.

More generally, an integer is called a generalized primitive root modulo n if it generates a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ of maximal size. Li and Pomerance showed, under GRH, that the set of integers for which a given integer is a generalized primitive root doesn't have an asymptotic density among all integers.

We study here the set of the ℓ-almost primes, i.e. integers with at most ℓ prime factors, for which a given integer $a \in \mathbb{Z} \setminus \{-1\}$, which is not a square, is a generalized primitive root, and we prove, under GRH, that this set has an asymptotic density among all the ℓ-almost primes.

1. Introduction

Soient a un entier et p un nombre premier, on dit que a est une racine primitive modulo p si a engendre le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Une question qui émerge alors est de quantifier le nombre de nombres premiers pour lesquels un entier a est racine primitive. Notons $N_a(x)$ le nombre de premiers plus petits que x pour lesquels a est racine primitive, on cherche alors à apprécier $N_a(x)$ lorsque x tend vers l'infini.

En 1927 Emil Artin conjecture que tout entier a différent de -1 et d'un carré est racine primitive modulo une infinité d'autres entiers. Il stipule qu'un tel entier a serait générateur pour environ 37% des premiers, c'est-à-dire $N_a(x) \sim C_A\pi(x)$, où $C_A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$ est la constante d'Artin. Une démonstration conditionnelle est fournie par Hooley [6] en 1967, en supposant l'hypothèse de Riemann pour certains corps de nombres. Plus précisément il démontre que $N_a(x) \sim C_A(a)\pi(x)$, la constante dépend donc du nombre a considéré et est la constante conjecturée par Heilbronn (d'après [6]). Concernant des résultats inconditionnels Heath-Brown [4], améliorant un résultat de Gupta et Ram Murty [2], a démontré qu'au plus deux nombres premiers ne sont pas racines primitives pour une infinité de nombres premiers. Plus précisément si (q, r, s) est un triplet d'entiers multiplicativement indépendants tel que aucun élément de $\{q, r, s, -3qr, -3rs, -3qs, qrs\}$ ne soit un carré, alors l'ensemble des premiers pour lesquels au moins un entier parmi q, r et s est racine primitive est asymptotiquement $\gg \frac{x}{(\log x)^2}$. Pour un état de l'art concernant la conjecture d'Artin et les racines primitives généralisées, le lecteur pourra se référer aux articles de synthèse de Moree [13] et de Li et Pomerance [11].

On étend la notion de racine primitive au sous-groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, où n est un entier quelconque, en définissant les racines primitives généralisées modulo n comme étant les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ générant des sous-groupes de

taille maximale, c'est-à-dire $\{m \in (\mathbb{Z}/n\mathbb{Z})^*,\ |\langle m\rangle| = \lambda(n)\}$, où λ est la fonction lambda de Carmichael [1], définie telle que $\lambda(n)$ est la taille maximale atteinte par les sous-groupes cycliques de $(\mathbb{Z}/n\mathbb{Z})^*$. Il est alors naturel de se demander si des résultats similaires à la conjecture d'Artin existent dans le cadre des racines primitives généralisées. Notons $N'_a(x)$ le nombre d'entiers plus petits que x pour lesquels a est racine primitive généralisée, on espère alors que $N'_a(x) \sim C(a)x$. Malheureusement ce n'est pas le cas. Soit $\mathtt{E}$ l'ensemble des entiers qui sont soit une puissance d'exposant strictement plus grand que 1, soit un carré multiplié par -1 ou ± 2. Li [9] a démontré que pour tout a, $\liminf \frac{N'_a(x)}{x} = 0$ et Li et Pomerance [11] ont démontré que pour les entiers a n'appartenant pas à $\mathtt{E}$ on a, sous l'hypothèse de Riemann généralisée, $\limsup \frac{N'_a(x)}{x} > 0$. Ainsi le nombre d'entiers pour lesquels un certain entier a est racine primitive généralisée n'admet pas de densité parmi tous les entiers. Comme pour le cas classique de la conjecture d'Artin d'autres problèmes surgissent naturellement comme par exemple l'estimation de l'ordre de grandeur de la plus petite racine primitive généralisée pour un entier, dont Martin [12] fournit une majoration pour presque tout entier.

Soit ℓ un entier plus grand que 1. Dans cet article, on étudie une situation intermédiaire, celle de l'ensemble des nombres ℓ-presque premiers pour lesquels un entier a est racine primitive généralisée, et nous montrons qu'il admet une densité parmi tous les ℓ-presque premiers.

Pour le reste de l'article p et q représenteront toujours des nombres premiers, et nous noterons $\mathrm{ord}_n(b)$ l'ordre de b dans $(\mathbb{Z}/n\mathbb{Z})^*$, (b,c) le pgcd de b et c, $[b,c]$ le ppcm de b et c, $\nu_q(b)$ la valuation q-adique de b. On note $\mathscr{P}^*(A)$ l'ensemble des parties non-vides d'un ensemble A. On fixe $a \in \mathbb{Z}\setminus\{-1\}$ un entier différent d'un carré, et on écrit a sous la forme $a = a_1 a_2^2$ où a_1 est sans facteur carré et éventuellement négatif. De plus, on définit h comme le plus grand entier tel que a soit une h-ième puissance :

$$h := \max\{\nu,\ \exists b,\ a = b^\nu\}. \tag{1}$$

Un nombre ℓ-presque premier est un nombre ayant au plus ℓ diviseurs premiers comptés avec multiplicité. Landau [7] a montré que le nombre de ℓ-presque premiers plus petit que x est asymptotiquement $\frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}$. On s'intéresse ici au comportement asymptotique du nombre de ℓ-presque premiers pour lesquels a est une racine primitive généralisée. Nous obtenons sous l'hypothèse de Riemann généralisée (GRH) le théorème suivant :

THÉORÈME 1.1 (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 et qui ont a comme racine primitive généralisée. On a :*

$$\mathcal{N}_{a,\ell}(x) = \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}\prod_p (1 - W_\ell(p))\,(1 + V_\ell(a_1))\,(1+o(1))\,,$$

avec les notations suivantes :

1. $W_\ell(p) := \sum_{i=1}^{\ell} \binom{\ell}{i} \sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j p^{i+j} (h,p)^i}{p^{2i}(p-1)^j (p^{i+j}-1)}$, *est la contribution ne dépendant que de* h,
2. $V_\ell(a_1) := \mu(2\tilde{a}_1) \frac{H_2(\ell,a_1)}{1-W_\ell(2)} \prod_{\substack{p \\ p|a_1 \\ p\geq 3}} (1-W_\ell(p))^{-1}$, *est la contribution spécifique dépendant de* a, *où* $\tilde{a}_1 := \frac{a_1}{(2,a_1)}$,
3. $$H_2(\ell,a_1) := \sum_{k=1}^{\ell} \binom{\ell}{k} 2^{-\ell-k} \delta_\ell(k) \mu(\tilde{a}_1)^k \times \prod_{\substack{p|\tilde{a}_1 \\ p\geq 3}} \left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell} \right) \sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j} = \tilde{a}_1} \prod_{\{i,j\}\in\mathcal{D}} G_{i,j}^k(a_{i,j})$$

   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

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

   $\mathcal{D} = [0,k] \times [0,\ell-k] \setminus \{0,0\}$, *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 le résultat 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 (par exemple 1636 est une racine primitive généralisée modulo $4054051 = 1801 \times 2251$ mais n'est pas une racine primitive modulo 1801 ou 2251). Nous montrons dans la section suivante 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 [6], dont on retrouve ci-dessus le terme principal en prenant $\ell = 1$. En effet ce dernier ramène le problème à compter

les idéaux premiers d'un certain corps de nombres, ce qu'il peut alors faire en étudiant, sous GRH, la fonction zeta de Dedekind associée à ce corps. Dans notre cas, nous ramenons le problème à compter simultanément les idéaux premiers de plusieurs corps de nombres, ce qui n'est pas possible en appliquant classiquement la formule de Perron et en déformant le contour. Pour surmonter cette difficulté, nous démontrons le résultat inconditionnel suivant, qui découle d'une application atypique de la méthode de Selberg-Delange :

THÉORÈME 1.2. — *Soient ℓ un entier non nul, a un entier non nul qui n'est ni -1 ni un carré, C une constante. Soient $v_1, \dots, v_\ell$ des entiers plus petits que C et $\kappa_1, \dots, \kappa_\ell$ des entiers sans facteur carré tels que pour tout $1 \leq i \leq \ell$, $\kappa_i | v_i$, alors :*

$$\sum_{\substack{p_1 \cdots p_\ell \leq x \\ (a, p_1 \cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 (v_i) \\ a \in \mathfrak{R}(\kappa_i, p_i)}} 1 = \frac{\ell x}{\log x \prod_i n_i} (\log\log x)^{\ell-1} + \mathcal{O}_C\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right),$$

où $n_i := [\mathbb{Q}(\sqrt[\kappa_i]{a}, \xi_{v_i}) : \mathbb{Q}]$, ξ_{v_i} est une racine primitive v_i-ième de l'unité et $\mathfrak{R}(\kappa_i, p_i)$ est l'ensemble des entiers dont la classe $\pmod{p_i}$ est une puissance κ_i-ième.

De plus, inconditionnellement, on a la majoration suivante :

THÉORÈME 1.3. — *Avec les mêmes hypothèses que pour le Théorème 1.1, on a :*

$$\mathcal{N}_{a,\ell}(x) \leq \frac{x(\log\log x)^{\ell-1}}{(\ell-1)! \log x} \prod_p (1 - W_\ell(p))\,(1 + V_\ell(a_1))\,(1 + o(1)).$$

Posons $C_\ell(a) = \lim_{x\to\infty} \mathcal{N}_{a,\ell}(x) / \frac{x(\log\log x)^{\ell-1}}{(\ell-1)! \log x}$. Nous avons calculé numériquement plusieurs valeurs particulières, reprises dans le tableau suivant :

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	$\simeq 0.2807$	$\simeq 2 \times 10^{-7}$	$\simeq 0.2807$	$\simeq 0.2807$	$\simeq 0.2807$

On retrouve sur la première ligne la constante d'Artin, ainsi que la légère déviation pour $a = 5$. Dans les lignes suivantes, toutes les valeurs présentent une

déviation, qui semble s'estomper quand ℓ grandit, sauf pour $a = 2$ auquel cas $C_\ell(2)$ semble tendre vers 0, ce qui est en accord avec le fait que 2 est dans l'ensemble E décrit par Li et Pomerance [11].

Nous présentons ensuite une approche heuristique analogue à celle du cas classique. Nous transformons le problème en l'évaluation du nombre de ℓ-presque premiers ne vérifiant pas une certaine propriété pour tout nombre premier q. 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 $p_1 \cdots p_\ell$ comptés sont tels que chaque 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'erreurs, nous utilisons des méthodes combinatoires pour obtenir l'expression du terme principal.

2. Caractérisation des racines primitives généralisées

Nous donnons dans ce paragraphe un critère caractérisant les racines primitives généralisées. Ce critère est énoncé dans le lemme 2.2.

Nous commençons par introduire des notations qui nous serviront tout au long de l'article. 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 :

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

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 :

$$M_q(p_1,\ldots,p_\ell) = \{p \in \{p_1,\ldots,p_\ell\}, \nu_q(p-1) = \nu_q(\lambda(p_1 \cdots p_\ell))\}. \tag{3}$$

Cet ensemble est toujours non vide. En effet la fonction lambda de Carmichael 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 commence par donner un résultat classique sur les ordres des éléments dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Lemme 2.1. — *Pour tous a, n_1, n_2 dans $\mathbb{N}$, $(a, n_1 n_2) = 1$:*

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

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 $[n_1,n_2]|a^{[\mathrm{ord}_{n_1}(a),\mathrm{ord}_{n_2}(a)]} - 1$. □

Nous cherchons à compter les nombres m ℓ-presque premiers c'est-à-dire tels que $\Omega(m) \leq \ell$, où $\Omega(m)$ est le nombre de facteurs premiers de m comptés avec multiplicité, 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 $(\mathbb{Z}/2\mathbb{Z})^*$.

Nous allons montrer 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 que $\sum_{p_1\cdots p_{\ell-1}\leq x} 1 \ll \frac{x}{\log x}(\log\log x)^{\ell-2}$ et $\sum_{\substack{p_1\cdots p_\ell\leq x \\ p_1=p_2}} 1 \ll \frac{x}{\log x}(\log\log x)^{\ell-2}$. On ne s'intéresse dans la suite qu'aux a qui ne sont pas des carré et aux $m \leq x$ sans facteur carré ayant exactement ℓ facteurs premiers.

Lemme 2.2. — *Soient $p_1, \ldots, p_\ell$, ℓ nombres premiers distincts et a un entier tel que $(a, p_1\cdots p_\ell) = 1$.*

Alors a est une racine primitive généralisée modulo $p_1\cdots p_\ell$ si et seulement si pour tout $q|\lambda(p_1\cdots p_\ell)$, 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 $\mathrm{ord}_p(a)|\frac{p-1}{q}$.

Ainsi d'après le lemme 2.1,

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

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 $q|\lambda(p_1 \cdots p_\ell)$ tel que $a^{\frac{\lambda(p_1 \cdots p_\ell)}{q}} \equiv 1(p_1 \cdots p_\ell)$.

Soit $p \in M_q(p_1, \ldots, p_\ell)$, alors d'après le lemme 2.1, $\mathrm{ord}_p(a)|\frac{p-1}{q}$.

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 ℓ-presque premiers pour lesquels a n'est pas une racine primitive généralisée.

Définition 2.3. — On dit que a vérifie $\mathcal{R}(q, p_1 \cdots p_\ell)$ si $(a, p_1 \cdots p_\ell) = 1$ 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 $p_1 \cdots p_\ell$ si $(a, p_1 \cdots p_\ell) = 1$ et 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 [6, §3]. La section suivante étend une approche heuristique de la conjecture d'Artin à notre problème.

3. Approche heuristique expliquant le terme $W_\ell(p)$ des Théorèmes 1.1 et 1.3

Dans un premier temps nous rappelons l'approche heuristique de Heilbronn [10] 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 $(a, p) = 1$ et 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 premier avec a soit tel que a ne vérifie pas $\mathcal{R}(q, p)$.

$$\begin{aligned}&\mathbb{P}(\text{“}a \text{ ne vérifie pas } \mathcal{R}(q,p)\text{”})\\ &= 1 - \mathbb{P}(p \equiv 1 \pmod q)\mathbb{P}(\text{“}\exists b \text{ tel que } a \equiv b^q \pmod p\text{”}|\text{“}p \equiv 1 \pmod q\text{”}),\end{aligned}$$

où la dernière probabilité est une probabilité conditionnelle. 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 (1), 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 [13]).

Un argument plus rigoureux ([9] 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 $\mathrm{Gal}(L/\mathbb{Q})$.

Or $L/\mathbb{Q}$ est un extension abélienne, donc cette classe de conjugaison 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 [15]).

Passons maintenant au problème pour les ℓ-presque premiers. Soient $p_1, \dots, p_\ell$ des nombres premiers, ne divisant pas a. 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 $M_q(p_1, \dots, p_\ell)$.

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

Les événements impliquant les p_j sont maintenant indépendants :

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

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

$$\begin{aligned}&\mathbb{P}(\nu_q(p-1)=m,\ \text{“}\exists b \text{ tel que } a\equiv b^q \pmod p\text{”})\\&=\mathbb{P}(p\equiv 1 \pmod{q^m},\ \text{“}\exists b \text{ tel que } a\equiv b^q \pmod p\text{”})\\&\quad-\mathbb{P}(p\equiv 1 \pmod{q^{m+1}},\ \text{“}\exists b \text{ tel que } a\equiv b^q \pmod p\text{”})\\&=\frac{(h,q)}{q}\left(\frac{1}{\varphi(q^m)}-\frac{1}{\varphi(q^{m+1})}\right)=\frac{(h,q)(q-1)}{q^2\varphi(q^m)}.\end{aligned}$$

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

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

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.

La principale difficulté pour résoudre ce genre de problème est d'exclure les ℓ-presque premiers tels que a vérifie $\mathcal{R}(q,p_1\cdots p_\ell)$ pour un q grand, la section suivante est un premier pas dans ce sens.

4. Un premier découpage : le découpage initial de Hooley

Nous adaptons les notations du paragraphe puis procédons à un découpage de $\mathcal{N}_{a,\ell}(x)$ analogue à celui effectué par Hooley [6] pour le cas $\ell=1$.

On a vu dans la section 2 qu'un entier $p_1\cdots p_\ell$ était compté dans $\mathcal{N}_{a,\ell}(x)$ si a ne vérifie pas $\mathcal{R}(q,p_1\cdots p_\ell)$ 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 :

$$\mathcal{N}_{a,\ell}(x,\eta)=\#\{p_1\cdots p_\ell\le x|\ a \text{ ne vérifie pas } \mathcal{R}(q,p_1\dots p_\ell),\ \forall q\le\eta\},\tag{4}$$

$$\mathcal{P}_a(x,k)=\#\{p_1\cdots p_\ell\le x|\ a \text{ vérifie } \mathcal{R}(q,p_1\dots p_\ell),\ \forall q|k\}.\tag{5}$$

Enfin il nous reste à introduire l'analogue des $M_a(x,\eta_1,\eta_2)$ de Hooley que nous noterons $\mathcal{M}_a(x,\eta_1,\eta_2)$. 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 :

(6)
- C_1 une constante arbitrairement grande;
- $C_2 = x^{\frac{1}{2}} \log^{-8} x$;
- $C_3 = x^{\frac{1}{2}} \log x$.

Tout d'abord,

$$\mathcal{N}_{a,\ell}(x) \leq \mathcal{N}_{a,\ell}(x, C_1). \tag{7}$$

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 :

$$\begin{aligned}\mathcal{N}_{a,\ell}(x) = \mathcal{N}_{a,\ell}(x, C_1) &+ \mathcal{O}(\mathcal{M}_a(x, C_1, C_2)) \\ &+ \mathcal{O}(\mathcal{M}_a(x, C_2, C_3)) + \mathcal{O}(\mathcal{M}_a(x, C_3, x-1)).\end{aligned} \tag{8}$$

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.

5. Une deuxième série de découpages et distinction de la majoration nécessitant l'Hypothèse de Riemann Généralisée

Afin de majorer le terme d'erreur dans (8) nous allons procéder en effectuant des découpages successifs, d'abord suivant les valeurs de q puis suivant les valeurs de $p_2 \cdots p_\ell$. Par souci de clarté, ces découpages sont synthétisés dans l'arbre de la Figure 5.1, où les nœuds sont les différents découpages, et les commentaires sur les arrêtes indiquent la méthode utilisée pour parvenir à la majoration.

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

PROPOSITION 5.1. — *En reprenant les définitions de C_2 et C_3 de* (6)*, 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)
$$\mathcal{M}_a(x, C_3, x-1) = \mathcal{O}\left(\frac{x}{\log^2 x}\right)$$

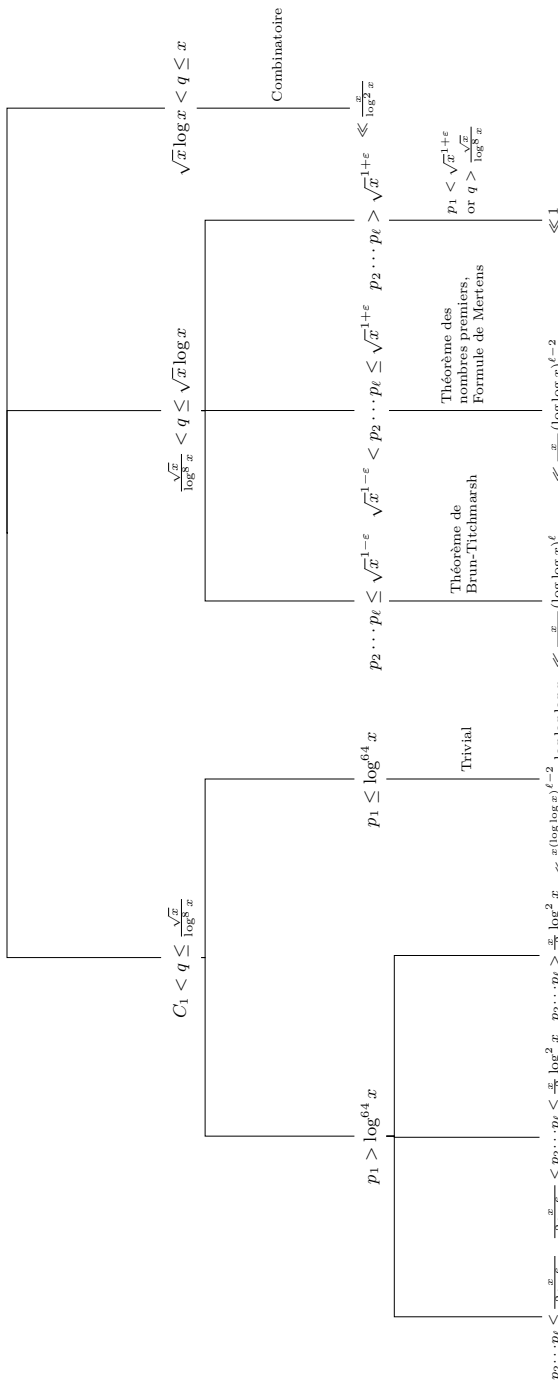


FIGURE 5.1. Résumé des coupes successives pour contrôler le terme d'erreur dans (8)

Démonstration. — i) Nous majorons $\mathcal{M}_a(x, C_2, C_3)$ à l'aide des cardinaux $\mathcal{P}_a(x,k)$ définis par (5) :

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

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

$$\begin{aligned}
S_1 &= \sum_{C_2 < q \leq C_3} \sum_{p_2 \cdots p_\ell < \sqrt{x}^{1-\varepsilon}} \sum_{\substack{p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ p_1 \equiv 1(q)}} 1, \\
S_2 &= \sum_{C_2 < q \leq C_3} \sum_{\sqrt{x}^{1-\varepsilon} \leq p_2 \cdots p_\ell \leq \sqrt{x}^{1+\varepsilon}} \sum_{\substack{p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ p_1 \equiv 1(q)}} 1, \\
S_3 &= \sum_{C_2 < q \leq C_3} \sum_{p_2 \cdots p_\ell \geq \sqrt{x}^{1+\varepsilon}} \sum_{\substack{p_1 \leq \frac{x}{p_2 \cdots p_\ell} \\ p_1 \equiv 1(q)}} 1.
\end{aligned}$$

Dans S_1 la somme sur p_1 est longue, on utilise le Théorème de Brun–Titchmarsh ([16], Th I.4.16),

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

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 :

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

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

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

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

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

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

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

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 $\sum_{\substack{C_2 < q \leq C_3 \\ q \mid p_1 - 1}} 1 = 0$.

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 [6, p212]. Observons que, comme les rôles des p_i sont symétriques dans la condition $\mathcal{R}(q, p_1 \ldots p_\ell)$ 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) :

$$\prod_{m < x^{\frac{1}{2}} \log^{-1} x \prod_{i=2}^{\ell} p_i^{-1}} (a^{2m} - 1) \tag{9}$$

Posons $S_a(\eta_1, \eta_2) = \{p : \exists q \in]\eta_1, \eta_2] \text{ tel que } q | p-1,\ a \text{ est une puissance } q\text{-ième } (\mathrm{mod}\ p)\}$. 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 (9). En minorant dans (9) 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 :

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

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

5.2. 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 [6] conditionnel à l'hypothèse de Riemann généralisée pour certains corps de nombres.

Lemme 5.2 (Hooley, GRH). — *Soit q un nombre premier, on a alors*

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

Nous sommes alors en mesure de fournir la majoration suivante pour $\mathcal{M}_a(x, C_1, C_2)$.

PROPOSITION 5.3 (GRH). — *Sous l'hypothèse de Riemann généralisée, et avec C_1 et C_2 comme dans* (6)*, 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

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

où $S := \#\left\{p_1 \cdots p_\ell \leq x,\ p_2 \cdots p_\ell \leq \frac{x}{\log^{64} x},\ \exists q \in]C_1, C_2],\ a \text{ vérifie } \mathcal{R}(q, p_1)\right\}$.

La contribution de $p_1 \leq (\log x)^{64}$ est négligeable :

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

Réécrivons maintenant S :

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

On découpe la somme sur $p_2 \cdots p_\ell$ en trois parties comme suit :

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

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

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

et on a donc $S \ll S_1 + S_2 + S_3$.

Pour majorer S_1 on utilise le lemme 5.2 dû à Hooley.

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

Par sommation d'Abel, et en utilisant le Théorème de Landau sur le nombre de presque premiers [7], 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 :

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

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 :

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

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 $u = \log x$ 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 5.1

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

Comme $a^{\frac{p_1-1}{q}} \equiv 1(p_1)$, $a^{2\frac{p_1-1}{q}} \equiv 1(p_1)$. De plus $\frac{p_1-1}{q} \leq \frac{x}{qp_2\cdots p_\ell} \leq \sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-1}x$. Ainsi il existe $m \leq \sqrt{\frac{x}{p_2\cdots p_\ell}}\log^{-1}x$ tel que $p_1|a^m-1$. On minore chaque p_i par

C_1 (au lieu de 2 contrairement à la preuve de la proposition 5.1)

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

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

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

5.3. Nouvelle équation fondamentale. — Maintenant en reprenant (8) et la proposition précédente, on obtient :

(10)

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

Exprimons alors $\mathcal{N}_{a,\ell}(x,C_1)$ en termes de $\mathcal{P}_a(x,k)$. Déjà, par inclusion-exclusion, on a :

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

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

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

Commençons par démontrer le lemme suivant.

LEMME 6.1. — *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. — On a trivialement 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

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

Notons $E = \{1, \dots, \ell\}$, $\mathcal{P}^*(E)$ 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 (5) et (1) les conditions suivantes pour les nombres $p_1 \cdots p_\ell$ contribuant à $\mathcal{P}_a(x, k)$.

PROPOSITION 6.2. — *Soit $(p_1 \dots, p_\ell)$ un ℓ-uplet de nombres premiers 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 $i \in E$, $a \in \mathfrak{R}\left(\prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} k'_L, p_i\right)$ et $p_i \equiv 1 \pmod{\prod_{\substack{L \in \mathcal{P}^*(E) \\ i \in L}} k_L}$.*
  - *Pour tout $j \in E$, et pour tout sous-ensemble L de E ne contenant pas j, on a pour chaque diviseur premier q de 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 $\prod_{L \in \mathcal{P}^*(E)} k_L = k$, 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 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

6.1, 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 6.1, $a \in \mathfrak{R}(k_L, p_i)$ 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 6.1

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

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

Grâce à la proposition 6.2, on peut exprimer $\mathcal{P}_a(x, k)$ comme suit :

$$\mathcal{P}_a(x,k) = \sum_{\prod_{L\in\mathcal{P}^*(E)} k_L = k} \ \sum_{\substack{p_1\cdots p_\ell \le x\\ (a, p_1\cdots p_\ell)=1\\ \forall i,\ p_i \equiv 1 \pmod{\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} k_L}\\ \forall i,\ a\in\mathfrak{R}\left(\prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} k'_L, p_i\right)}} 1 \tag{11}$$

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 $p_1, \dots, p_\ell$ sont indépendantes (mis à part la contrainte $p_1 \cdots p_\ell \le x$).

Proposition 6.3. — *On a :*

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

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

Démonstration. — À k et $p_1,\dots,p_\ell$ 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 $k_i := \prod_{\substack{L\in\mathcal{P}^*(E)\\ i\in L}} k_L$ 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 à : pour tout $i\in\{1,\dots,\ell\}$,

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

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 $i\in\{1,\dots,\ell\}$, $(\frac{p_i-1}{u_i}, k) = 1$.

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

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

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

$$\mathcal{P}_a(x,k)=\mathcal{P}_a{}'(x,k)+\mathcal{O}\left(\frac{C_1x}{C_5^t\log x}(\log\log x)^{\ell-1}\right),$$

où

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

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 :

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

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

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

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

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

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

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

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

$$\sum_{\substack{g_{L_0}\mid k_{L_0}^\infty\\ g_{L_0}>(\log x)^{10}}} \frac{1}{g_{L_0}} \leq \frac{1}{(\log x)^5} \sum_{g_{L_0}\mid k_{L_0}^\infty} \frac{1}{g_{L_0}^{\frac12}} \leq \frac{1}{(\log x)^5} \prod_{p\mid k_{L_0}} \left(\frac{p^{\frac12}}{p^{\frac12}-1}\right) \ll \frac{C_1}{(\log x)^5}.$$

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

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.

7. 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 égal à -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 7.1. — *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 $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, $\nu \mapsto \nu^{m'}$, 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 $m'|p-1$. □

D'après le Théorème de Kummer ([14] Prop I.8.3) cette propriété est aussi 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 7.2. — *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 7.3. — *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 que $p \equiv 1(m)$ 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.

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

PROPOSITION 7.4. — *Soient m', m deux entiers naturels tels que $m'|m$, m' sans facteur carré et a 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,*

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

Où $\varepsilon(m', m)$ est donné par la formule suivante, en prenant a_1 la partie sans facteur carré de a (i.e $a = a_1a_2^2$, avec a_1 sans facteur carré),

$$\varepsilon(m', m) = \begin{cases} 2 & \text{si } 2|m',\ 2\|m,\ a_1|m \text{ et } a_1 \equiv 1 \pmod 4 \\ 2 & \text{si } 2|m',\ 4\|m,\ a_1|m \text{ et } a_1 \equiv 1 \pmod 2 \\ 2 & \text{si } 2|m',\ 8|m \text{ et } a_1|m \\ 1 & \text{sinon} \end{cases}. \tag{12}$$

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 $\delta = 2$ et donc $\delta = 2$ 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 ([18], Cor 4.5.4).

Si $2\|m$, comme a_1 est sans facteur carré, $\mathbb{Q}(\sqrt{a_1})$ est 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 $(-1\big||a_1|)$. Comme a n'est pas un carré parfait, $a_1 \neq 1$ et on peut calculer $(-1\big||a_1|)$:

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

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 $a_1|m$. □

8. Méthode de Selberg-Delange

L'objectif de cette section est de démontrer le Théorème 1.2.

D'après la section précédente, la quantité que l'on souhaite évaluer est :

$$\sum_{\substack{p_1\cdots p_\ell \leq x \\ (a,p_1\cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 (v_i) \\ a \in \mathfrak{R}(\kappa_i,p_i)}} 1 = \sum_{\substack{m_1\cdots m_\ell \leq x \\ m_i \in P_i}} 1,$$

où les $v_1, \ldots, v_\ell$ sont des entiers plus petits qu'une constante C, les $\kappa_1, \ldots, \kappa_\ell$ sont des entiers sans facteur carré tels que pour tout $1 \leq i \leq \ell$, $\kappa_i|v_i$, P_i est l'ensemble des nombres premiers p tels que $p \nmid av_i$ et p se factorise dans $K_i := \mathbb{Q}(\sqrt[\kappa_i]{a}, \xi_{v_i})$ comme produits d'idéaux premiers distincts de norme p.

Le cas $\ell = 1$ a été traité par Hooley [6], 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'erreurs 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 [16] 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 [3].

Définissons, pour $\boldsymbol{r} := (r_1, \dots, r_\ell) \in \mathbb{N}^\ell$, $n \in \mathbb{N}$,

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

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 :

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

F admet alors un prolongement analytique en une fonction méromorphe sur $\mathbb{C} \setminus \{1\}$ en tant que fonction de s. 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 : $\zeta_{K_i, f}(s) := \prod_{\exists p,\ N(\mathfrak{p}) = p^f} \left(1 - \frac{1}{p^{fs}}\right)^{-1}$.

De plus on décompose $F(s, \boldsymbol{z})$ en un produit de fonction 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

$$G_i(s,z_i) := F_i(s,z_i)\zeta_{K_i}^{-\frac{z_i}{n_i}}(s) \tag{13}$$
$$= \prod_{p\in P_i}\left(\left(1+\frac{z_i}{p^s}\right)\left(1-\frac{1}{p^s}\right)^{z_i}\right)\prod_{\substack{\mathfrak{p}\\ N(\mathfrak{p})|av_i\\ N(\mathfrak{p})=p}}\left(1-\frac{1}{p^s}\right)^{\frac{z_i}{n_i}}\prod_{\substack{f|n_i\\ f\geq 2}}\zeta_{K_i,f}(s)^{-\frac{z_i}{n_i}},$$

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

Les fonction zêta de Dedekind disposent de régions sans zéro semblables à celle de la fonction zêta de Riemann ([8]), 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 8.1. — *Il existe des constantes C_6, C_7 et C_8 ne dépendant que de C 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 $i\in\{1,\dots,\ell\}$.

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. On note $|\boldsymbol{z}| := \max_i\{|z_i|\}$.

PROPOSITION 8.2. — *Soit A un réel strictement positif. Pour $|\boldsymbol{z}|\leq A$ et s dans la région sans zéro décrite dans la proposition 8.1, $\mathfrak{Re}\ s\leq 2$ on a :*

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

Démonstration. — Déjà pour tout i, comme tous les v_i sont bornés,

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

Définissons alors pour tout i, $\tilde{G}_i(s,z_i) := \prod_{p\in P_i}\left(\left(1+\frac{z_i}{p^s}\right)\left(1-\frac{1}{p^s}\right)^{z_i}\right) = \sum_{n\geq 1}\frac{b_{i,z_i}(n)}{n^s}$, 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 $\sigma\geq\frac{1}{2}+\varepsilon$,

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

Nous aurons aussi besoin de contrôler ζ_{K_i} à droite de la droite critique. Pour ce faire on va utiliser un lemme de Wang [17] qui découle d'une majoration de Heath-Brown [5] pour ζ_{K_i} sur la droite critique.

Lemme 8.3 (Wang). — *Soit K une extension algébrique de degré n et $\eta>0$. Alors par le principe de Phragmén-Lindelöf dans la bande $\frac{1}{2}\leq\sigma\leq 1+\varepsilon$:*

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

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

Proposition 8.4. — *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 de $\boldsymbol{z}$, satisfaisant, pour tout $\frac{1}{\ell}>A>0$, $\frac{1-C_8}{C_8}\geq\varepsilon>0$,

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

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, [16]). □

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

PROPOSITION 8.5. — *Par la méthode de Selberg-Delange, on a*

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

Démonstration. — Posons $A(x,\boldsymbol{z}):=\sum\limits_{n\leq x}\alpha_{\boldsymbol{z}}(n)$. Alors par la formule de Perron on a (Tenenbaum [16], Théorème II.2.5) :

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

avec $\kappa:=1+\frac{1}{\log x}$.

Définissons alors le domaine $\mathcal{D}$ comme la région sans zéro commune à nos fonctions zêta de Dedekind et $\tilde{\mathcal{D}}:=\mathcal{D}\setminus[\frac{1}{2}+\varepsilon,1]$.

Ainsi, pour $s=\sigma+it\in\mathcal{D}$, $|s-1|\gg 1$, $|\boldsymbol{z}|\leq A$, $A<\frac{1}{\ell}$, par la proposition 8.2 et le lemme 8.3,

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

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,

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

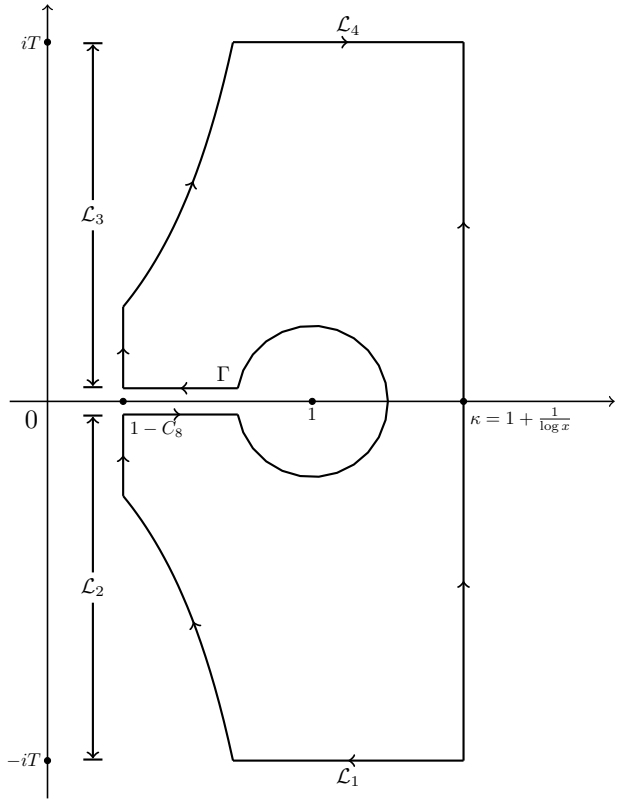
et il en va de même pour l'autre demi-droite.

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 $\frac{1}{\log x}$ et de partie rectiligne joignant $1-\frac{1}{\log x}$ 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 $T = x^{c_1\sqrt{\log x}}$,

$$\int_0^x A(t,\boldsymbol{z})dt = \Phi(x) + \mathcal{O}\left(x^2 e^{-c_2\sqrt{\log x}}\right). \tag{14}$$

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

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

et donc par la proposition 8.4, et comme $|s-1|<1$ pour s dans Γ,

$$F(s,\boldsymbol{z}) \ll |s-1|^{-A}, \quad (s\in\Gamma). \tag{15}$$

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 $\mu_k(\boldsymbol{z}) := \sum\limits_{h+j=k}\frac{1}{h!j!}G^{(h)}(1,\boldsymbol{z})\gamma_j(\boldsymbol{z})$, et donc

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

Alors on a, (pour le détail voir [16], p241-242),

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

Remarquons également que l'on a :

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

Il reste à montrer que $\Phi'(x)$ est une bonne approximation de $A(x,\boldsymbol{z})$. Pour ce faire on procède comme dans [16] p243. Soit $0<h<\frac{x}{2}$, on a alors, par (14),

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

Puis, en utilisant la formule de Taylor,

$$\Phi(x+h)-\Phi(x) = h\Phi'(x+h) - h^2\int_0^1 t\Phi''(x+th)dt$$
$$= h\Phi'(x) + h^2\int_0^1 (1-t)\Phi''(x+th)dt.$$

Puis par (15), 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

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

Or

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

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

(16)

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

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 [16].

Démonstration du Théorème 1.2. — On a

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

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

$$\Lambda_i(z_i) = \prod_{p\in P_i}\left(\left(1+\frac{z_i}{p}\right)\left(1-\frac{1}{p}\right)^{z_i}\right) \prod_{\substack{\mathfrak{p}\in O_{K_i}\\ N(\mathfrak{p})|a\upsilon_i\\ N(\mathfrak{p})\text{ premier}}}\left(1-\frac{1}{N(\mathfrak{p})}\right)^{\frac{z_i}{n_i}} \beta_{K_i}^{\frac{z_i}{n_i}}, \tag{17}$$

où $\beta_{K_i} := \lim_{s\to 1}(s-1)\prod_{\substack{\mathfrak{p}\in O_{K_i}\\ N(\mathfrak{p})\text{ premier}}}\left(1-\frac{1}{N(\mathfrak{p})}\right)$, 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 8.5,

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

où $S := \frac{x}{(2i\pi)^\ell \log x} \oiint_\Omega \frac{(\log x)^{\sum_i \frac{z_i}{n_i}}}{\Gamma\left(\sum_i \frac{z_i}{n_i}\right)} \prod_i \Lambda_i(z_i) \frac{dz_i}{z_i^2}$,

et $E := \frac{1}{(2\pi)^\ell} \oiint_\Omega \left(x(\log x)^{\ell r-2} + xe^{-c_6\sqrt{\log x}}\right) \prod_i \frac{dz_i}{|z_i|^2}$.

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 :

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

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 $\mathscr{H}$ ([16], 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 demi-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 :

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

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 calcule sa dérivée logarithmique :

$$\frac{\partial}{\partial z_j}\Lambda_j(0) = \frac{\Lambda_j'(0)}{\Lambda_j(0)} = \sum_{p\in P_j}\left(\frac{1}{p}+\log\left(1-\frac{1}{p}\right)\right)$$
$$+\sum_{\substack{\mathfrak{p}\in O_{K_i}\\ N(\mathfrak{p})\mid a v_i\\ N(\mathfrak{p})\text{ premier}}}\frac{1}{n_j}\log\left(1-\frac{1}{N(\mathfrak{p})}\right)+\frac{1}{n_j}\log(\beta_{K_j})$$
$$= \mathcal{O}(\upsilon_i).$$

Ainsi

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

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

$$\sum_{\substack{p_1\cdots p_\ell\leq x\\ (a,p_1\cdots p_\ell)=1\\ \forall i,\ p_i\equiv 1(\upsilon_i)\\ a\in\Re(\kappa_i,p_i)}} 1 = \sum_{n\leq x}c_1(n)$$
$$= \frac{\ell x}{\log x\prod_i n_i}(\log\log x)^{\ell-1}+\mathcal{O}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right). \quad \square \tag{18}$$

En appliquant le Théorème 1.2 à la dernière somme de l'expression de $\mathcal{P}_a{}'(x,k)$ de la Proposition 6.4 on obtient le résultat suivant (en prenant $\upsilon_i =$

$u_i d_i$ et $\kappa_i = k_i'$) :

(19)
$$\sum_{\substack{p_1\cdots p_\ell \le x \\ (a,p_1\cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 (u_i d_i) \\ a\in \mathfrak{R}\left(k_i', p_i\right)}} 1 = \frac{\ell x}{\log x \prod_i n_i} (\log\log x)^{\ell-1} + \mathcal{O}_{C_1,C_5}\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right),$$

où $n_i := [\mathbb{Q}(\sqrt[k_i']{a}; \xi_{u_i d_i}) : \mathbb{Q}]$.

9. Contrôle des termes d'erreurs

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

PROPOSITION 9.1. — *On a avec C_1 et C_5 des constantes arbitrairement grandes, $\varepsilon > 0$,*

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

où

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

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 6.4, 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, on a que la contribution des termes d'erreurs issus de l'équation (19), sont $\mathcal{O}_{C_1,C_5}\left(\frac{x(\log\log x)^{\ell-2}}{\log x}\left(C_5\log C_5\right)^{2^\ell}\right)$.

Il reste à estimer la somme associée aux termes principaux :

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

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

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

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

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

où τ est la fonction nombre de diviseurs. Soit $\varepsilon_2>0$, on a le résultat 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 :

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

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

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

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

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

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

$$E_{L_0} \ll \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x} \frac{2^{C_1} e^{(\varepsilon_2+\varepsilon_3)\ell C_1}}{C_5^{\varepsilon_4}} \ll \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x} \frac{e^{\varepsilon_5 \ell C_1}}{C_5^{\varepsilon_4}}.$$

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 :

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

Soit $\varepsilon_1 > 0$, on a la majoration suivante pour tout i : $\frac{1}{n_i} \ll \frac{1}{d_i^{1-\varepsilon_1} \prod_{L,\ i\in L} k_L {g_L}^{1-\varepsilon_1}}$.

On majore simplement les sommes sur le d_i :

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

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 :

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

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

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

Ainsi $f(k) \ll \frac{1}{k^{2-\varepsilon_4}}$.

Soit $\varepsilon_5 > \varepsilon_4$, en reportant le résultat précédent dans E_{C_1} on a :

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

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.

10. Calcul du terme principal

Dans cette section on notera pour tout nombre premier $p \geq 3$ et tout entier $i \geq 1$, $R_p(i) := \sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j (p-1)^{\ell-i-j}}{(p^{i+j}-1)(p-2)^{\ell-i}}$ et pour tout entier $i \geq 1$, $R_2(i) := \sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j 2^{-j}}{2^{i+j}-1}$.

On veut calculer : $\sum_k \mu(k)\mathcal{P}'_{a,0}(k)$, avec

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

où $\mathscr{P}^*(E) := \{L \subset E,\ L \neq \emptyset\}$ et $n_i := n(\prod_{\substack{L\in\mathscr{P}^*(E) \\ i\in L}} k'_L, u_i d_i)$ 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 7.4, $n(\ell,m) := [\mathbb{Q}(\sqrt[\ell]{a}, \xi_m) : \mathbb{Q}] = \frac{\ell\varphi(m)}{\varepsilon(\ell,m)}$ 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 10.1. — *On obtient :*

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

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 $p=2$,*
- $$H_2(\ell,a_1) := \sum_{L_0\in\mathscr{P}^*(E)} 2^{-\ell-|L_0|} \sum_{L_1\in\mathscr{P}^*(L_0)} \delta_5(L_0,L_1)\mu(\tilde{a}_1)^{|L_1|} \times \prod_{\substack{p|\tilde{a}_1\\ p\geq 3}}\left(\frac{(p-2)^{\ell-|L_1|}}{(p-1)^\ell}\right) \underset{L\in\mathscr{P}^*(E)}{*}\left(G_L^{L_1}\right)(\tilde{a}_1)$$

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

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

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

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

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

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

10.1. $\mathcal{P}_{a,0}(k)$ 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 10.2. — *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 10.3. — *Pour k impair, sans facteur carré, on a :*

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

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 :

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

Nous allons calculer successivement les sommes sur les d_i, $c_{i,L}$ et g_L. En utilisant le lemme 10.2, 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 $1 \leq i \leq \ell$:

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

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

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

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

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

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

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k\\ p\geq 3}} \left(1-\frac{1}{p-1}\right)^{\ell} \times \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{{k'_L}^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|}\right) \times \prod_{L\in\mathscr{P}^*(E)} \left(\sum_{\substack{g|k_L^\infty\\ k_L|g}} \frac{1}{\varphi(g)^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(f_p(\nu_p(g)-1)\right)^{\ell-|L|}\right). \tag{20}$$

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

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

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

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 :

$$\sum_{\substack{g|k_L^\infty\\ k_L|g}} \frac{1}{\varphi(g)^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(1+\frac{1-p^{-\nu_p(g)+1}}{p-2}\right)^{\ell-|L|} = \frac{1}{\varphi(k_L)^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(1+R_p(|L|)\right). \tag{21}$$

Alors en reportant (21) dans (20) :

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k\\ p\geq 3}} \left(1-\frac{1}{p-1}\right)^{\ell} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{{k'_L}^{|L|}\varphi(k_L)^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|} \left(1+R_p(|L|)\right)\right). \tag{22}$$

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 (22) sous forme de produit eulérien, on obtient bien :

$$\mathcal{P}'_{a,0}(k) = \prod_{\substack{p|k \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^\ell \overset{\ell}{\underset{i=1}{\ast}} \left(F_i^{*\binom{\ell}{i}}\right)(k). \quad \square \tag{23}$$

10.2. 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,

$$\begin{aligned}
\mathcal{P}'_{a,0}(k) = &\sum_{L_0\in\mathscr{P}^*(E)} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \mathbb{1}(2|k_{L_0}) \\
&\times \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)} \\ g_L|k_L^\infty \\ k_L|g_L}} \sum_{\substack{\{c_{bL}\}_{\substack{L\in\mathscr{P}^*(E)\\ b\notin L}} \\ c_{bL}|\frac{g_L}{k_L}}} \prod_{i\in E} \left(\sum_{d|k} \frac{\mu(d)\varepsilon(k'_i, u_i d)}{\varphi(u_i d) k'_i}\right) \\
= &\sum_{L_0\in\mathscr{P}^*(E)} \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L = k} \mathbb{1}(2|k_{L_0}) \prod_{L\in\mathscr{P}^*(E)} \left(\frac{1}{{k'_L}^{|L|}}\right) \\
&\times \sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)} \\ g_L|k_L^\infty \\ k_L|g_L}} \sum_{\substack{\{c_{bL}\}_{\substack{L\in\mathscr{P}^*(E)\\ b\notin L}} \\ c_{bL}|\frac{g_L}{k_L}}} \prod_{i\in E} \left(\sum_{d|k} \frac{\mu(d)\varepsilon(k'_i, u_i d)}{\varphi(u_i d)}\right).
\end{aligned} \tag{24}$$

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

LEMME 10.4. — *On a :*

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

où

$$B(i,L_0) := \begin{cases} \mathbb{1}(2|c_{i,L_0}) & \text{si } i \in E \setminus L_0 \\ 1 + \mathbb{1}(2\tilde{a}_1|k)\delta_2(g_{L_0})\mu(\tilde{a}_1)\mu\left((\tilde{a}_1,u_i)\right) \prod\limits_{\substack{p|\tilde{a}_1 \\ p\nmid u_i \\ p\geq 3}} \left(\frac{1}{p-2}\right) & \text{si } i \in L_0 \end{cases},$$

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

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 $i \in E \setminus L_0$, 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 $p=2$:

$$\sum_{d|k} \frac{\mu(d)\varepsilon\left(k_i', u_i d\right)}{\varphi(u_i d)} = \mathbb{1}(2|c_{i,L_0}) \frac{1}{2\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|k \\ p\geq 3}} \left(1-\frac{1}{p-1}\right), \tag{25}$$

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 10.2 :

$$\begin{aligned} \sum_{d|k} \frac{\mu(d)\varepsilon\left(k_i', u_i d\right)}{\varphi(u_i d)} &= \sum_{d|k} \frac{\mu(d)}{\varphi(u_i d)} + \sum_{\substack{d|k \\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)} \\ &= \frac{1}{2\varphi(u_i)} \prod_{\substack{p|k \\ p|u_i \\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right) \prod_{\substack{p|k \\ p\geq 3}} \left(1-\frac{1}{p-1}\right) + \sum_{\substack{d|k \\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)}. \end{aligned} \tag{26}$$

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 10.2 :

$$\begin{aligned}(27)\qquad \sum_{\substack{d|k\\ b|u_i d}} \frac{\mu(d)}{\varphi(u_i d)} &= \mathbb{1}\left(\frac{b}{(u_i,b)}|k\right) \frac{\mu\left(\frac{b}{(u_i,b)}\right)}{\varphi\left(u_i\frac{b}{(u_i,b)}\right)} \sum_{d'|k/\frac{b}{(u_i,b)}} \frac{\mu(d')\varphi\left(u_i\frac{b}{(u_i,b)}\right)}{\varphi(u_i d'\frac{b}{(u_i,b)})}\\ &= \mathbb{1}\left(\frac{b}{(u_i,b)}|k\right) \frac{\mu\left(\frac{b}{(u_i,b)}\right)}{\varphi\left(u_i\frac{b}{(u_i,b)}\right)} \prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p|u_i}} \left(1-\frac{1}{p}\right) \prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p\nmid u_i}} \left(1-\frac{1}{p-1}\right).\end{aligned}$$

Décomposons chaque élément de cette dernière égalité :

$$(28)\qquad \mathbb{1}\left(\frac{b}{(u_i,b)}|k\right) = \mathbb{1}(2\tilde{a}_1|k)\mathbb{1}(\nu_2(g_{L_0}) \geq s(a_1)-1),$$

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 :

$$(29)\qquad \mu\left(\frac{b}{(u_i,b)}\right) = \mu(\tilde{a}_1)\mu\left((\tilde{a}_1,u_i)\right)\mu\left(2^{\mathbb{1}\left(\nu_2(g_{L_0})=s(a_1)-1\right)}\right).$$

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 :

$$(30)\qquad \frac{1}{\varphi\left(u_i\frac{b}{(u_i,b)}\right)} = \frac{1}{\varphi(u_i)} \prod_{\substack{p|\tilde{a}_1\\ p\nmid u_i}} \left(\frac{1}{p-1}\right)\left(1-\frac{1}{2}\mathbb{1}\left(\nu_2(g_{L_0})=s(a_1)-1\right)\right).$$

Décomposons ensuite les deux produits de (27) :

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

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

$$\prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p|u_i}}\left(1-\frac{1}{p}\right)=\frac{1}{2}\prod_{\substack{p|k\\ p|u_i\\ p\geq 3}}\left(1-\frac{1}{p}\right)\left(1+\mathbb{1}\left(\nu_2(g_{L_0})=s(a_1)-1\right)\right). \tag{31}$$

et, comme $2|u_i$,

$$\begin{aligned}\prod_{\substack{p|\frac{k(u_i,b)}{b}\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)&=\prod_{\substack{p|k\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p|\frac{b}{(u_i,b)}\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)^{-1}\\ &=\prod_{\substack{p|k\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p|\tilde{a}_1\\ p\nmid u_i}}\left(1-\frac{1}{p-1}\right)^{-1}.\end{aligned} \tag{32}$$

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 (28), (29), (30), (31) et (32) dans (27) :

$$\begin{aligned}\sum_{\substack{d|k\\ b|u_id}}\frac{\mu(d)}{\varphi(u_id)}&=\mathbb{1}(2\tilde{a}_1|k)\delta_2(g_{L_0})\frac{\mu(\tilde{a}_1)\mu\left((\tilde{a}_1,u_i)\right)}{2\varphi(u_i)}\\ &\quad\times\prod_{\substack{p|\tilde{a}_1\\ p\nmid u_i\\ p\geq 3}}\left(\frac{1}{p-2}\right)\prod_{\substack{p|k\\ p|u_i\\ p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right)\prod_{\substack{p|k\\ p\geq 3}}\left(1-\frac{1}{p-1}\right).\end{aligned} \tag{33}$$

Ce qui, en reprenant (25) et (26), permet de conclure. □

On a donc dans l'expression (24) 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.

$$\prod_{i\in L_0}\left(1+\mathbb{1}(2\tilde{a}_1|k)\delta_2(g_{L_0})\mu(\tilde{a}_1)\mu\left((\tilde{a}_1,u_i)\right)\prod_{\substack{p|\tilde{a}_1\\ p\nmid u_i\\ p\geq 3}}\left(\frac{1}{p-2}\right)\right) \tag{34}$$

$$=1+\sum_{L_1\in\mathscr{P}^*(L_0)}\mathbb{1}(2\tilde{a}_1|k)\delta_2(g_{L_0})^{|L_1|}\mu(\tilde{a}_1)^{|L_1|}\times\prod_{\substack{p|\tilde{a}_1\\ p\geq 3}}\left(\frac{1}{p-2}\right)^{|L_1|}\prod_{i\in L_1}\left(\prod_{\substack{p|\tilde{a}_1\\ p|u_i\\ p\geq 3}}(2-p)\right),$$

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.

10.3. 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 10.5. — *On a, en reprenant les définitions de H_1 et F_i de la proposition 10.1,*

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

Démonstration. — Commençons par expliciter $\mathcal{P}'_\alpha(k)$ en utilisant le lemme 10.4, on obtient

$$\mathcal{P}'_\alpha(k):=\alpha_1(k)\sum_{L_0\in\mathscr{P}^*(E)}\sum_{\prod_{L\in\mathscr{P}^*(E)}k_L=k}\sum_{\substack{\{g_L\}_{L\in\mathscr{P}^*(E)}\\ g_L|k_L^\infty\\ k_L|g_L}}\prod_{L\in\mathscr{P}^*(E)}\left(\alpha_2(k_L)\alpha_3(g_L)\right)\sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}|\frac{g_L}{k_L}}}\prod_{\substack{\{i,L\}\\ L\in\mathscr{P}^*(E)\\ i\notin L}}\alpha_4(c_{i,L}), \tag{35}$$

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 $i \in E \setminus L_0$ 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

$$\sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}\mid \frac{g_L}{k_L}}} \prod_{\substack{\{i,L\}\\ L\in\mathscr{P}^*(E)\\ i\notin L}} \alpha_4(c_{i,L})$$

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

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

$$\sum_{\substack{\{c_{bL}\}_{L\in\mathscr{P}^*(E)}\\ b\notin L\\ c_{bL}\mid \frac{g_L}{k_L}}} \prod_{\substack{\{i,L\}\\ L\in\mathscr{P}^*(E)\\ i\notin L}} \alpha_4(c_{i,L}) \tag{36}$$

$$= \delta_3(g_{L_0}) \prod_{L\in\mathscr{P}^*(E)}\left(\prod_{\substack{p\mid k_L\\ p\geq 3}}\left(1+\frac{p-1}{p-2}\sum_{n=1}^{\nu_p(g_L)-1}\frac{1}{p^n}\right)^{\ell-|L|}\right)$$

$$= \delta_3(g_{L_0}) \prod_{L\in\mathscr{P}^*(E)}\left(\prod_{\substack{p\mid k_L\\ p\geq 3}}\left(1+\frac{1-p^{-\nu_p(g_L)+1}}{p-2}\right)^{\ell-|L|}\right)$$

Puis exprimons séparément la somme sur g_{L_0}.

$$\sum_{\substack{\{g_{L_0}\}_{L_0\in\mathscr{P}^*(E)}\\ g_{L_0}\mid k_{L_0}^\infty\\ k_{L_0}\mid g_{L_0}}} \delta_3(g_{L_0})\frac{1}{\varphi(g_{L_0})^{|L_0|}} \prod_{\substack{p\mid k_{L_0}\\ p\geq 3}}\left(1+\frac{1-p^{-\nu_p(g_L)+1}}{p-2}\right)^{\ell-|L_0|} \tag{37}$$

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

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 (37) dans (35) et en en procédant de la même manière que pour (23) :

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

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

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

10.4. 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 10.6. — *On a, en reprenant les définitions de H_2 et F_i de la proposition 10.1,*

$$\mathcal{P}'_\beta(k) = H_2(\ell, a_1) \mathbb{1}(2\tilde{a}_1|k) \prod_{\substack{p|\frac{k}{2\tilde{a}_1} \\ p\geq 3}} \left(1 - \frac{1}{p-1}\right)^\ell \overset{\ell}{\underset{i=1}{*}} \left(F_i^{*\binom{\ell}{i}}\right) (\tfrac{k}{2\tilde{a}_1}).$$

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 10.4, on obtient

$$\begin{aligned} (38)\quad \mathcal{P}'_\beta(k) := \beta_1(k) \sum_{L_0 \in \mathscr{P}^*(E)} \sum_{L_1 \in \mathscr{P}^*(L_0)} \beta_2(L_1) \sum_{\prod_{L \in \mathscr{P}^*(E)} k_L = k} \prod_{L \in \mathscr{P}^*(E)} \beta_3(k_L) \\ \times \sum_{\substack{\{g_L\}_{L \in \mathscr{P}^*(E)} \\ g_L | k_L^\infty \\ k_L | g_L}} \prod_{L \in \mathscr{P}^*(E)} \beta_4(g_L) \sum_{\substack{\{c_{bL}\}_{L \in \mathscr{P}^*(E)} \\ b \notin L \\ c_{bL} | \frac{g_L}{k_L}}} \prod_{\substack{\{i,L\} \\ L \in \mathscr{P}^*(E) \\ i \notin L}} \beta_5(c_{i,L}) \end{aligned}$$

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 $\delta_2(g_{L_0}) = \begin{cases}1 & \text{si } \nu_2(g_{L_0})\geq s(a_1)\\ -1 & \text{si } \nu_2(g_{L_0}) = s(a_1)-1,\\ 0 & \text{sinon}\end{cases}$
- $\beta_5(c_{i,L}) := \begin{cases}\frac{1}{\varphi(c_{i,L})}\prod_{\substack{p|k\\p|c_{i,L}\\p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right)\prod_{\substack{L\in\mathscr{P}^*(E)\\i\notin L}}\left(\prod_{\substack{p|\tilde{a}_1\\p|c_{i,L}\\p\geq 3}}(2-p)\right) & \text{si } i\in L_1\\ \frac{\mathbb{1}(2|c_{i,L_0})}{\varphi(c_{i,L})}\prod_{\substack{p|k\\p|c_{i,L}\\p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right) & \text{si } i\in E\setminus L_0\\ \frac{1}{\varphi(c_{i,L})}\prod_{\substack{p|k\\p|c_{i,L}\\p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right) & \text{sinon}\end{cases}$.

Les sommes sur les $c_{i,L}$ pour $i\notin L_1$ sont exactement les mêmes que pour (36), intéressons-nous au cas $i\in L_1$ et $i\notin L$ (et donc $2\nmid k_L$) :

$$\begin{aligned}&\sum_{c_{i,L}\,|\,\frac{g_L}{k_L}}\frac{1}{\varphi(c_{i,L})}\prod_{\substack{p|k\\p|c_{i,L}\\p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right)\prod_{\substack{p|\tilde{a}_1\\p|c_{i,L}\\p\geq 3}}(2-p)\\ &=\prod_{\substack{p|k_L\\p\nmid\tilde{a}_1\\p\geq 3}}\left(f_p(\nu_p(g_L)-1)\right)\prod_{\substack{p|k_L\\p|\tilde{a}_1\\p\geq 3}}p^{-\nu_p(g_L)+1},\end{aligned}$$

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 (36),

$$\sum_{\{c_{bL}\}_{\substack{L\in\mathscr{P}^*(E)\\ b\notin L\\ c_{bL}\mid \frac{g_L}{k_L}}}} \prod_{\substack{\{i,L\}\\ L\in\mathscr{P}^*(E)\\ i\notin L}} \left(\frac{1}{\varphi(c_{i,L})}\prod_{\substack{p\mid k\\ p\mid c_{i,L}\\ p\geq 3}}\left(\frac{(p-1)^2}{p(p-2)}\right)\right)$$
$$\times \prod_{i\in L_1}\left(\prod_{\substack{L\in\mathscr{P}^*(E)\\ i\notin L}}\left(\prod_{\substack{p\mid \tilde{a}_1\\ p\mid c_{i,L}\\ p\geq 3}}(2-p)\right)\right)\prod_{i\in E\setminus L_0}(\mathbb{1}(2|c_{i,L_0}))$$
$$= \delta_3(g_{L_0})\prod_{L\in\mathscr{P}^*(E)}\left(\prod_{\substack{p\mid k_L\\ p\geq 3}}(f_p(\nu_p(g_L)-1))^{\ell-|L\cup L_1|}\prod_{\substack{p\mid k_L\\ p\nmid \tilde{a}_1\\ p\geq 3}}(f_p(\nu_p(g_L)-1))^{|L_1\setminus L|}\right.$$
$$\left.\times\prod_{\substack{p\mid k_L\\ p\mid \tilde{a}_1\\ p\geq 3}}\left(p^{-\nu_p(g_L)+1}\right)^{|L_1\setminus L|}\right)$$

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 prises par $\delta_2(2g_{L_0})$ suivant les valeurs de $s(a_1)$ et celles prises 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	$\begin{cases}\left(2\left(1-2^{-\nu_2(g_{L_0})}\right)\right)^{\ell-\lvert L_0\rvert} & \text{si } 2\lvert g_{L_0},\\ 0 & \text{sinon}\end{cases}$
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	$\begin{cases}\left(2\left(1-2^{-\nu_2(g_{L_0})}\right)\right)^{\ell-\lvert L_0\rvert} & \text{si } 2\lvert g_{L_0}\\ 0 & \text{sinon}\end{cases}$
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	$\begin{cases}\left(2\left(1-2^{-\nu_2(g_{L_0})}\right)\right)^{\ell-\lvert L_0\rvert} & \text{si } 2\lvert g_{L_0}\\ 0 & \text{sinon}\end{cases}$

Définissons alors 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 :

$$\begin{aligned}(39)\qquad &\sum_{\substack{g_{L_0} \mid k_{L_0}^\infty \\ k_{L_0} \mid g_{L_0}}} \delta_2(g_{L_0})^{\lvert L_1\rvert} \delta_3(g_{L_0}) \frac{1}{\varphi(g_{L_0})^{\lvert L\rvert}} \prod_{\substack{p \mid k_{L_0} \\ p \geq 3}} \left(f_p(\nu_p(g_{L_0}) - 1)\right)^{\ell - \lvert L_0\rvert} \\ &= \delta_5(L_0, L_1) \frac{1}{\varphi(k_{L_0})^{\lvert L_0\rvert}} \prod_{\substack{p \mid k_{L_0} \\ p \geq 3}} \left(1 + R_p(\lvert L_0\rvert)\right).\end{aligned}$$

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 $L \neq L_0$:

$$\begin{aligned}(40)\qquad &\sum_{\substack{g \mid k_L^\infty \\ k_L \mid g}} \frac{1}{\varphi(g)^{\lvert L\rvert}} \prod_{\substack{p \mid k_L \\ p \geq 3}} \left(f_p(\nu_p(g) - 1)\right)^{\ell - \lvert L \cup L_1\rvert} \prod_{\substack{p \mid k_L \\ p \nmid \tilde{a}_1 \\ p \geq 3}} \left(f_p(\nu_p(g) - 1)\right)^{\lvert L_1 \setminus L\rvert} \\ &\qquad \times \prod_{\substack{p \mid k_L \\ p \mid \tilde{a}_1 \\ p \geq 3}} \left(p^{-\nu_p(g) + 1}\right)^{\lvert L_1 \setminus L\rvert} \\ &= \frac{1}{\varphi(k_L)^{\lvert L\rvert}} \prod_{\substack{p \mid k_L \\ p \nmid \tilde{a}_1 \\ p \geq 3}} \left(1 + R_p(\lvert L\rvert)\right) \prod_{\substack{p \mid k_L \\ p \mid \tilde{a}_1 \\ p \geq 3}} \left(1 + R_p(\lvert L \cup L_1\rvert)\right).\end{aligned}$$

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 (39) et (40) dans (38) cela donne :

$$\mathcal{P}'_\beta(k) = \beta_1(k) \sum_{L_0\in\mathscr{P}^*(E)} 2^{-|L_0|} \sum_{L_1\in\mathscr{P}^*(L_0)} \beta_6(L_1) \sum_{\prod_{L\in\mathscr{P}^*(E)} a'_L=\tilde{a}_1} \times \prod_{L\in\mathscr{P}^*(E)} \beta_7(a'_L) \sum_{\prod_{L\in\mathscr{P}^*(E)} k_L=\frac{k}{2\tilde{a}_1}} \prod_{L\in\mathscr{P}^*(E)} \beta_8(k_L),$$

où

- $\beta_6(L_1) := \delta_5(L_0,L_1)\mu(\tilde{a}_1)^{|L_1|} \prod_{\substack{p|\tilde{a}_1\\ p\geq 3}} \left(\frac{1}{p-2}\right)^{|L_1|}$,
- $\beta_7(a'_L) := \left(\frac{(h,a'_L)}{a'_L\varphi(a'_L)}\right)^{|L|} \prod_{p|a'_L} \left(\left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|} (2-p)^{|L\cap L_1|}\right) \times \prod_{p|a'_L} \left(1+R_p(|L\cup L_1|)\right),$
- $\beta_8(k_L) := \frac{1}{{k'_L}^{|L|}\varphi(k_L)^{|L|}} \prod_{\substack{p|k_L\\ p\geq 3}} \left(\frac{(p-1)^2}{p(p-2)}\right)^{|L|} \prod_{\substack{p|k_L\\ p\geq 3}} (1+R_p(|L|))$.

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

$$H_2(\ell,a_1) := 2^{-\ell} \sum_{L_0\in\mathscr{P}^*(E)} 2^{-|L_0|} \sum_{L_1\in\mathscr{P}^*(L_0)} \left(\widehat{\delta}(L_0,L_1)+\tilde{\delta}(L_0,L_1)\right) \mu(\tilde{a}_1)^{|L_1|} \times \prod_{\substack{p|\tilde{a}_1\\ p\geq 3}} \left(\frac{(p-2)^{\ell-|L_1|}}{(p-1)^\ell}\right) \underset{L\in\mathscr{P}^*(E)}{\ast} \left(G_L^{L_1}\right)(\tilde{a}_1).$$

On a alors

$$\mathcal{P}'_\beta(k) = H_2(\ell,a_1)\mathbb{1}(2\tilde{a}_1|k) \prod_{\substack{p|\frac{k}{2\tilde{a}_1}\\ p\geq 3}} \left(1-\frac{1}{p-1}\right)^\ell \overset{\ell}{\underset{i=1}{\ast}} \left(F_i^{*\binom{\ell}{i}}\right)\left(\frac{k}{2\tilde{a}_1}\right). \qquad \square$$

10.5. Preuve de la proposition 10.1. — Nous sommes maintenant en mesure de démontrer la proposition 10.1.

Preuve de la proposition 10.1. — En utilisant les propositions 10.3, 10.5 et 10.6 on a,

$$\begin{aligned}
&\sum_k \mu(k)\mathcal{P}'_{a,0}(k)\\
&= \sum_{\substack{k\\ 2\nmid k}} \mu(k)\mathcal{P}'_{a,0}(k) + \sum_{\substack{k\\ 2\mid k}} \mu(k)\left(\mathcal{P}'_{\alpha}(k) + \mathcal{P}'_{\beta}(k)\right)\\
&= \sum_{\substack{k\\ 2\nmid k}} \mu(k)\left(\mathcal{P}'_{a,0}(k) - \mathcal{P}'_{\alpha}(x,2k)\right) + \mu(2\tilde{a}_1)\sum_{\substack{k\\ 2\tilde{a}_1\nmid k}} \mu(k)\mathcal{P}'_{\beta}(x,2\tilde{a}_1 k)\\
&= \prod_{\substack{p\\ p\geq 3}}\left(1-\left(\frac{p-2}{p-1}\right)^{\ell}\sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)\right)\\
&\qquad\times\left(1-H_1(E)+\mu(2\tilde{a}_1)H_2(\ell,a_1)\prod_{\substack{p\mid a_1\\ p\geq 3}}\left(1-\left(\frac{p-2}{p-1}\right)^{\ell}\sum_{i=1}^{\ell}\binom{\ell}{i}F_i(p)\right)^{-1}\right),
\end{aligned}$$

ce qui donne la proposition 10.1. □

11. Lien entre le terme principal de la proposition 10.1 et les théorèmes 1.1 et 1.3

11.1. Équivalence entre le terme principal de la proposition 10.1 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 10.1 coïncide avec celui obtenu par l'approche heuristique.

Proposition 11.1. — *En reprenant les notations de la proposition 10.1, 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

$$\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}(-1)^j 2^{\ell-2i} = \begin{cases}2^{-\ell} & \text{si } i=\ell\\ 0 & \text{sinon}\end{cases}$$

et

$$\sum_{j=0}^{\ell-i}\binom{\ell-i}{j}(-1)^j 2^{\ell-3i-j} = 2^{-2i},$$

et ainsi $Q(2) = 2^{-\ell}$. □

11.2. Égalité entre le terme $H_2(\ell, a_1)$ de la proposition 10.1 et de celui des théorèmes 1.1 et 1.3. — 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 11.2. — *Soit $H_2(\ell, a_1)$ tel que définit dans la proposition 10.1,*

$$H_2(\ell,a_1)=\sum_{k=1}^{\ell}\binom{\ell}{k}2^{-\ell-k}\delta_\ell(k)\mu(\tilde{a}_1)^k \times\prod_{\substack{p\mid\tilde{a}_1\\ p\geq 3}}\left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell}\right)\sum_{\prod_{\{i,j\}\in\mathcal{D}}a_{i,j}=\tilde{a}_1}\prod_{\{i,j\}\in\mathcal{D}}G_{i,j}^k(a_{i,j}),$$

où $\mathcal{D}=[0,k]\times[0,\ell-k]\setminus\{0,0\}$, 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

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

avec $\sigma(a_1,k):=\begin{cases}2^{-\ell+k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1\equiv 1 \pmod 4\\ (-1)^k2^{-\ell+k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1\equiv 3 \pmod 4\\ (-1)^k2^{-2\ell+k}5^{\ell-k} & \text{sinon}\end{cases}.$

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 $|L_\alpha\setminus L_1|=|L_\beta\setminus L_1|$. En effet si $|L_1\cap L_\alpha|=|L_1\cap L_\beta|$ et $|L_\alpha\setminus L_1|=|L_\beta\setminus L_1|$ alors $|L_\alpha|=|L_1\cap L_\alpha|+|L_\alpha\setminus L_1|=|L_\beta|$ et $|L_1\cup L_\alpha|=|L_1|+|L_\alpha\setminus L_1|=|L_1\cup L_\beta|$.

Soit $\mathcal{D}=[0,|L_1|]\times[0,\ell-|L_1|]\setminus\{0,0\}$,

$$\underset{L\in\mathscr{P}^*(E)}{\ast}\left(G_L^{L_1}\right)(\tilde{a}_1)=\sum_{\prod_{L\in\mathcal{P}^*(E)}a_L=\tilde{a}_1}\prod_{\{i,j\}\in\mathcal{D}}\prod_{\substack{L\in\mathcal{P}^*(E)\\ |L_1\cap L|=i\\ |L\setminus L_1|=j}}G_L^{L_1}(a_L).$$

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

$$\underset{L\in\mathscr{P}^*(E)}{\ast}\left(G_L^{L_1}\right)(\tilde{a}_1)=\sum_{\prod_{L\in\mathcal{P}^*(E)}a_L=\tilde{a}_1}\prod_{\{i,j\}\in\mathcal{D}}\tilde{G}_{i,j}^{L_1}(a_{i,j}). \tag{41}$$

Nous allons remplacer la somme sur les décompositions de a_1 en $\prod_{L\in\mathcal{P}^*(E)} a_L$ en une somme sur les décompositions de a_1 en $\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}$. Il faut donc calculer le nombre de décompositions en $\prod_{L\in\mathcal{P}^*(E)} a_L$ qui aboutissent à une même décomposition en $\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}$.

Soit $(i,j)\in\mathcal{D}$, $\mathcal{E}=\{L\in\mathcal{P}^*(E), |L\cap L_1|=i,\ |L\setminus L_1|=j\}$ 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 $\prod_{L\in\mathcal{P}^*(E)} a_L$ qui correspondent à une même décomposition $\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}$ est $\gamma^{\omega(a_{i,j})}$. De plus L_1 a $\binom{|L_1|}{i}$ sous-ensembles de taille i et $E\setminus L_1$ a $\binom{|E\setminus L_1|}{j}$ sous-ensembles de taille j et ainsi

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

En reportant cela dans (41), on a :

$$\mathop{\ast}_{L\in\mathscr{P}^*(E)}\left(G_L^{L_1}\right)(\tilde{a}_1)=\sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}=\tilde{a}_1}\ \prod_{\{i,j\}\in\mathcal{D}} G_{i,j}^{|L_1|}(a_{i,j}),$$

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 :

$$\begin{aligned}(42)\quad H_2(\ell,a_1):=&\sum_{m=1}^{\ell}\binom{l}{m}2^{-\ell-m}\sum_{k=1}^{m}\binom{m}{k}\left(\widehat{\delta}(m,k)+\tilde{\delta}(m,k)\right)\mu(\tilde{a}_1)^k\\&\times\prod_{\substack{p|\tilde{a}_1\\p\geq3}}\left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell}\right)\sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}=\tilde{a}_1}\ \prod_{\{i,j\}\in\mathcal{D}} G_{i,j}^k(a_{i,j}).\end{aligned}$$

Inversons alors les sommes sur m et k,

$$H_2(\ell,a_1) := \sum_{k=1}^{\ell} \binom{\ell}{k} 2^{-\ell-k}\delta_\ell(k)\mu(\tilde{a}_1)^k \times \prod_{\substack{p\mid\tilde{a}_1\\ p\geq 3}} \left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell}\right) \sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j}=\tilde{a}_1} \prod_{\{i,j\}\in\mathcal{D}} G^k_{i,j}(a_{i,j}). \tag{43}$$

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 $\sigma(a_1,k) := \begin{cases}2^{-\ell+k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1\equiv 1 \pmod 4\\ (-1)^k2^{\ell-k}+2^{-2\ell+k}5^{\ell-k} & \text{si } a_1\equiv 3 \pmod 4\\ (-1)^k2^{-2\ell+k}5^{\ell-k} & \text{sinon}\end{cases}$,

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

Ce qui permet de conclure. □

11.3. Preuve des théorèmes 1.1 et 1.3. — En regroupant l'équation (10) et les propositions 9.1, 10.1, 11.1, 11.2 et en prenant, par exemple, $C_5 = e^{2C_1}$, on obtient le théorème 1.1.

De plus en reportant les résultats des propositions 9.1, 10.1, 11.1, 11.2 dans (7) on obtient la majoration inconditionnelle du théorème 1.3.

BIBLIOGRAPHIE

[1] R. D. Carmichael – « Note on a new number theory function. », *Bull. Am. Math. Soc.* **16** (1910), p. 232–238 (English).

[2] R. Gupta & M. R. Murty – « A remark on Artin's conjecture », *Invent. Math.* **78** (1984), no. 1, p. 127–130.

[3] G. Hanrot, G. Tenenbaum & J. Wu – « Averages of certain multiplicative functions over friable integers. II », *Proc. Lond. Math. Soc. (3)* **96** (2008), no. 1, p. 107–135 (French).

[4] D. R. Heath-Brown – « Artin's conjecture for primitive roots », *Quart. J. Math. Oxford Ser. (2)* **37** (1986), no. 145, p. 27–38.

[5] D. R. Heath-Brown – « The growth rate of the Dedekind zeta-function on the critical line », *Acta Arith.* **49** (1988), no. 4, p. 323–339 (English).

[6] C. Hooley – « On Artin's conjecture », *J. Reine Angew. Math.* **225** (1967), p. 209–220.

[7] E. Landau – « On some problems concerning the distribution of prime numbers. », *Bull. Soc. Math. Fr.* **28** (1900), p. 25–38 (French).

[8] E. S. Lee – « On an explicit zero-free region for the Dedekind zeta-function », *J. Number Theory* **224** (2021), p. 307–322 (English).

[9] S. Li – « On extending Artin's conjecture to composite moduli. », *Mathematika* **46** (1999), no. 2, p. 373–390 (English).

[10] S. Li & 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*, Dordrecht : Kluwer Academic Publishers, 2002, p. 219–231 (English).

[11] S. Li & C. Pomerance – « On generalizing Artin's conjecture on primitive roots to composite moduli », *J. Reine Angew. Math.* **556** (2003), p. 205–224 (English).

[12] G. Martin – « The least prime primitive root and the shifted sieve », *Acta Arith.* **80** (1997), no. 3, p. 277–288 (English).

[13] P. Moree – « Artin's primitive root conjecture – a survey », *Integers* **12** (2012), no. 6, p. 1305–1416, a13 (English).

[14] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[15] P. Stevenhagen – « The correction factor in Artin's primitive root conjecture. », *J. Théor. Nombres Bordx.* **15** (2003), no. 1, p. 383–391 (English).

[16] G. Tenenbaum – *Introduction à la théorie analytique et probabiliste des nombres*, [5e édition] éd., Sciences sup, Dunod, Malakoff, DL 2022 (fre).

[17] D. Wang – « The Selberg-Delange method in short intervals for the Dedekind zeta function », *Acta Arith.* **192** (2020), no. 3, p. 301–311.
[18] S. H. Weintraub – *Galois theory*, second éd., Universitext, Springer, New York, 2009.