Courses de polynômes irréductibles dans les corps de fonctions

Youssef Sedrati

École doctorale IAEM Lorraine

THÈSE

présentée pour obtenir le grade de

Docteur de l'Université de Lorraine

Mention: Mathématiques

par **Youssef SEDRATI**

16/06/2023

Courses de polynômes irréductibles dans les corps de fonctions

Composition du jury

Président	M. Régis DE LA BRETÉCHE	Professeur, Université Paris Cité
Examinateurs	Mme. Cécile DARTYGE	Maître de conférences, Université de Lorraine
	Mme. Anne DE ROTON	Maître de conférences, Université de Lorraine
	Mme. Lucile DEVIN	Maître de conférences, Université du Littoral Côte d'Opale
Rapporteurs	M. Florent JOUVE	Professeur, Université de Bordeaux
	M. Nathan NG	Professeur, University of Lethbridge
Directeurs de thèse	M. Youness LAMZOURI	Professeur, Université de Lorraine
	M. Manfred MADRITSCH	Maître de conférences, Université de Lorraine

Résumé

Depuis bien longtemps, beaucoup de mathématiciens ont été fascinés par les nombres premiers. Ils ont étudié les propriétés de ces nombres et ont établi de nombreux théorèmes les concernant. Parmi ces résultats, on trouve le théorème fondamental de l'arithmétique qui affirme que tout entier plus grand que 1 s'écrit de façon unique comme un produit de nombres premiers. Grâce à ce théorème, ces nombres peuvent être perçus comme les briques élémentaires dans la construction des entiers strictement positifs.

Les nombres premiers interviennent dans divers domaines, notamment dans l'algorithme RSA utilisé pour sécuriser les cartes bancaires. La puissance de cet algorithme réside dans la difficulté de factoriser un nombre qui est le produit de deux très grands nombres premiers.

Les nombres premiers cachent encore plusieurs mystères, en particulier en ce qui concerne leur répartition. En 1853, Chebyshev a observé une disparité dans la répartition des nombres premiers dans les progressions arithmétiques. Il a remarqué que pour la plupart des réels $x \geq 2$, il y a plus de nombres premiers inférieurs à x de la forme $4n+3$ que de la forme $4n+1$.

L'objectif de cette thèse est d'étudier une généralisation de ce phénomène aux courses des nombres premiers dans le contexte de l'anneau des polynômes à coefficients dans un corps fini $\mathbb{F}_q$, où q est une puissance d'un nombre premier impair. Pour ce faire, nous allons commencer par expliquer le biais de Chebyshev et présenter certains travaux connexes. Nous nous intéresserons ensuite à ce phénomène dans les corps de fonctions en s'appuyant sur les travaux de Cha.

Sur la base des travaux de Lamzouri relatifs aux courses des nombres premiers, nous allons présenter de nouveaux résultats et mettre en évidence la différence entre les courses à deux compétiteurs et celles à $r \geq 3$ (entier fixé) compétiteurs dans le cas des corps de fonctions. Nous donnerons aussi des exemples de courses dans le contexte des corps de fonctions où les densités associées s'annulent, ce qui n'est pas le cas dans les corps de nombres.

Dans la dernière partie de cette thèse, nous étudierons les courses des polynômes irréductibles unitaires modulo un polynôme unitaire m lorsque le nombre de compétiteurs r tend vers $+\infty$ avec le degré de m.

Mots clés : Biais de Chebyshev, Courses de nombre premiers, Corps de fonctions, Fonctions L.

Abstract

For a very long time, many mathematicians have been fascinated by prime numbers. They have studied the properties of these numbers and have established many theorems concerning them.

Among these results, we can mention the Fundamental Theorem of Arithmetic which states that any integer greater than 1 is uniquely written as a product of prime numbers. Thanks to this theorem, we can view the primes as the elementary bricks in the construction of positive integers. Prime numbers have many applications in various fields. For example, the RSA algorithm is used to secure credit cards. The power of this algorithm lies in the difficulty of factoring a number, which is a product of two very large primes.

Prime numbers still hide several mysteries, and their distribution is still not very well understood. In 1853, Chebyshev observed a disparity in the distribution of prime numbers in arithmetic progressions. He noticed that for most real numbers $x \geq 2$, there are more primes less than x of the form $4n + 3$ than of the form $4n + 1$.

The goal of this thesis is to study a generalization of this phenomenon to races of primes in the context of the ring of polynomials over a finite field $\mathbb{F}_q$, where q is a power of an odd prime.

To do this, we shall begin by explaining the origin of Chebyshev's bias. We then focus on this phenomenon in function fields, in particular the works of Cha.

Using Lamzouri's work concerning prime number races, we have been able to highlight the difference between races with two competitors and races with three or more competitors in the case of function fields. We will also give some examples of races in function fields where the associated densities vanish, which is not the case in number fields.

In the last part of this thesis, we shall investigate the races of monic irreducible polynomials modulo a monic polynomial m when the number of competitors r tends to $+\infty$ with the degree of m.

Key words : Chebyshev's bias, Prime number races, Function fields, L-functions.

À la mémoire de mes grands-parents

Remerciements

Tout d'abord, j'aimerais exprimer ma plus profonde gratitude à mon directeur de thèse M. Youness Lamzouri, professeur à l'université de Lorraine, de m'avoir confié ce travail de recherche très intéressant. Je saisis cette opportunité pour lui témoigner ma vive reconnaissance pour son encadrement et les différentes directives, recommandations et remarques qu'il m'a données tout au long de cette thèse.

Je voudrais remercier profondément aussi mon Co-directeur de thèse, M. Manfred Madritsch, maitre de conférence à l'université de Lorraine, pour son soutien et ses précieux conseils et différentes discussions qui m'ont aidé pour avancer dans mes travaux.

Je tiens à exprimer ma gratitude à M. Florent Jouve, mon professeur à l'université de Bordeaux, qui a renforcé mon souhait de faire de la recherche en théorie des nombres. Je le remercie d'autant plus qu'il m'a fait l'honneur d'être rapporteur de ma thèse.

Mes sincères remerciements sont aussi adressés à M. Nathan Ng, professeur à l'université de Lethbridge qui a accepté d'être un rapporteur de ma thèse et d'évaluer mes travaux de recherche.

J'adresse mes remerciements à M. Régis De La Bretèche pour son invitation aux Rencontres de théorie analytique et élémentaire des nombres à l'Institut Henri Poincaré, pour exposer les résultats de mon travail de recherche. Je le remercie aussi d'avoir accepté de faire parti du jury de la soutenance de ma thèse.

Je remercie fortement Mme Anne De Roton, maitresse de conférence à l'université de Lorraine, qui a bien voulu examiner et évaluer mes travaux de recherche et pour ses encouragements permanents et ses conseils tout au long de ma thèse.

Je remercie aussi Mme Cécile Dartyge, maitresse de conférence à l'université de Lorraine, qui a accepté d'être membre du jury de ma soutenance de thèse et la remercie aussi de son

aide et son soutien.

Je suis également reconnaissant à Mme Lucile Devin, maitresse de conférence à l'université du Littoral Côte d'Opale ULCO, pour tout l'intérêt qu'elle a porté à mes travaux de recherche depuis le début de mon parcours doctoral. Je la remercie aussi pour son invitation à présenter mes travaux au Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville (LMPA).

J'adresse mes remerciements à la professeure Anne Gégout-Petit, directrice actuelle de l'Institut d'Élie Cartan de Lorraine, ainsi qu'à l'ancien directeur, le professeur Xavier Antoine et au professeur Frédéric Robert directeur de l'école doctorale IAEM pour leur accueil au sein de l'IECL.

Un grand merci également à Élodie Cunat, Laurence Quirot, Paola Schneider et Nathalie Benito pour leur aide dans toutes les démarches administratives et logistiques.

Je remercie le professeur Thomas Stoll ainsi que tous les membres (anciens et nouveaux) de l'équipe d'Analyse et théorie des nombres de l'Institut Élie Cartan de Lorraine. J'adresse une pensée amicale particulièrement à Paul, Pierre, Renan, Robin, Johann, Jéremy, Pierre-Adrien.

J'aimerais aussi remercier tous mes collègues enseignants, et particulièrement Stéphane André, Didier Schmitt, Jérémie Unterberger qui m'ont permis d'enseigner dans de bonnes conditions.

Je remercie tous mes professeurs de mathématiques qui ont beaucoup contribué à ma formation mathématique.

Mes remerciements fraternels et amicaux vont à mes frères Oussama, Anass, ma belle soeur Douae et tous les membres de ma famille (mes oncles, mes tantes, mes cousin(e)s) ainsi que mes amis et collègues Yiming, Clara, Salim, Nathan, Khaoula, David, Chorouq, Nizar, Pierrick, Vincent, Jocelyn, Virgile, Yann qui ont été d'un grand soutien durant toute la période de ma thèse.

Je remercie mes voisins et voisines Jocelyne, Claire, Gaël, Thomas pour leur bienveillance envers moi.

Un Merci inestimable à mes chers parents, qui malgré la distance qui nous séparent n'ont jamais cessé de croire en moi, de m'aider et de me motiver . Qu'ils puissent trouver dans ce travail une modeste reconnaissance de tout ce qu'ils ont fait pour moi. Ce travail n'aurait pas pu aboutir sans leurs encouragements et soutiens.

Table des matières

Liste des tableaux

Liste des sigles et des abréviations

HRG	hypothèse de Riemann généralisée.
LI	hypothèse d'indépendance linéaire.
(LI ★)	hypothèse d'indépendance linéaire dans les corps de fonctions.

Notations

Les notations standards suivantes seront utilisées tout au long de cette thèse :

- $\boldsymbol{[\![1,n]\!]}$ est l'ensemble des entiers naturels compris entre 1 et n.
- $\boldsymbol{\|t\|}$ représente la norme du vecteur $t = (t_1, \ldots, t_r) \in \mathbb{R}^r$ qui est égale à $\sqrt{t_1^2 + \cdots + t_r^2}$.
- $\boldsymbol{t^T}$ représente la transposée du vecteur $t = (t_1, \ldots, t_r) \in \mathbb{R}^r$.
- $\boldsymbol{f \ll g}$ pour $x \in X$ ou $f = O(g)$ pour $x \in X$ lorsqu'il existe une constante $C > 0$ tel que $|f(x)| \leq C|g(x)|$ sur tout X (avec X un ensemble où f et g sont simultanément définies).
- $\boldsymbol{f \ll_s g}$ pour $x \in X$ ou $f = O_s(g)$ pour $x \in X$ si la constante C dépend d'un paramètre s.
- $\boldsymbol{f(x) \asymp g(x)}$ est utilisée si $f(x) \ll g(x)$ et $g(x) \ll f(x)$.
- $\boldsymbol{f(x) \sim g(x)}$ (x est au voisinage de $+\infty$) signifie que $\lim\limits_{x \to +\infty} \frac{f(x)}{g(x)} = 1$.
- $\boldsymbol{\#A}$ ou $\boldsymbol{|A|}$ représente le cardinal de A.
- Les symboles $\mathbb{P}$, $\mathbb{E}$ désignent respectivement la probabilité et l'espérance.
- $\boldsymbol{\mathcal{B}_r(q)}$ est l'ensemble des r-uplets de classes de résidus distinctes $(a_1, a_2, \ldots, a_r)$ modulo q qui sont premiers avec q (avec $q \geq 3$).
- $\boldsymbol{S_r}$ est l'ensemble des permutations de $\{1, \ldots, r\}$.
- $\boldsymbol{\mathbb{S}^1}$ est le cercle unité.
- $\boldsymbol{\mathbb{F}_q}$ désigne un corps fini à q éléments (où q est une puissance d'un premier impair).
- Les symboles $\boldsymbol{\mathcal{M}_q}$, $\boldsymbol{\mathcal{P}_q}$ désignent respectivement l'ensemble des polynômes unitaires et l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[T]$.

- $\boldsymbol{m}$ est un polynôme dans $\mathbb{F}_q[T]$.

- $\boldsymbol{\mathcal{A}_r(m)}$ est l'ensemble des r-uplets de classes de résidus distinctes $(a_1,a_2,\ldots,a_r)$ modulo m qui sont premiers avec m (avec $m \in \mathcal{M}_q$ un polynôme de degré ≥ 1).

- $\boldsymbol{\deg(m)}$ désigne le degré de $\boldsymbol{m}$.

- $\boldsymbol{|m|}$ désigne la norme de $\boldsymbol{m}$ définie par $q^{\deg(m)}$ si m est un polynôme non nul de $\mathbb{F}_q[T]$ et 0 sinon.

- $\boldsymbol{(m)}$ l'idéal engendré par m.

- $\boldsymbol{(a,m)}$ désigne le pgcd de a et m.

Introduction

Un problème majeur en théorie analytique des nombres est l'étude de la répartition des nombres premiers. Plusieurs mathématiciens se sont intéressés à ce sujet. Parmi eux, nous pouvons citer Hadamard et De la Vallée Poussin. En 1896, ces derniers ont prouvé indépendamment l'un des théorèmes les plus célèbres en théorie analytique des nombres. Il s'agit du théorème des nombres premiers.

Avant de l'énoncer on rappelle les notations suivantes :
Pour $x \geq 2$, on définit

$$\pi(x) := \#\{p \leq x \mid p \text{ est un nombre premier}\}$$

et on définit le logarithme intégral

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t} dt.$$

Le théorème des nombres premiers affirme que

$$\pi(x) \underset{x \longrightarrow +\infty}{\sim} \mathrm{Li}(x) \underset{x \longrightarrow +\infty}{\sim} \frac{x}{\log x}.$$

Quelques années plus tard, De la Vallée Poussin a démontré une généralisation naturelle de ce théorème, qui est le théorème des nombres premiers en progressions arithmétiques. Plus concrètement, il a montré que pour a et q deux entiers premiers entre eux (avec $q \geq 2$) on a

$$\pi(x; q,a) \underset{x \longrightarrow +\infty}{\sim} \frac{1}{\phi(q)} \frac{x}{\log x},$$

où $\pi(x; q,a)$ est le nombre de premiers inférieurs à x qui sont congrus à a modulo q. Ceci signifie que les nombres premiers sont équirépartis dans les classes inversibles modulo q (q un entier ≥ 2).

Ce résultat peut inciter à penser qu'il y a autant de nombres premiers de la forme $qn + a$ que ceux de la forme $qn + b$ pour a et b des entiers premiers avec q et a n'est pas congru à b modulo q.

Cependant cette conséquence ne donne pas une idée sur le signe de la différence $\pi(x; q,a) - \pi(x; q,b)$. Chebyshev a constaté une irrégularité dans la répartition des nombres premiers.

Il a remarqué que, pour la plupart des réels $x \geq 2$, il y a une prédominance des nombres premiers $\leq x$ congrus à 3 modulo 4 par rapport aux nombres premiers $\leq x$ congrus à 1 modulo 4.

En général, il a été observé que le nombre $\pi(x; q,a)$ est plus grand que $\pi(x; q,b)$, pour la plupart des réels $x \geq 2$ quand a est un non-résidu quadratique et b est un résidu quadratique modulo q.

Ce phénomène est appelé "le biais de Chebyshev". On peut concevoir ce phénomène comme une course entre deux compétiteurs "a mod q" et "b mod q" avec "a" un non-résidu quadratique modulo q et "b" un résidu quadratique modulo q. À l'instant $x \geq 2$, le compétiteur "a mod q" marque $\pi(x; q,a)$ points et le compétiteur "b mod q" marque $\pi(x; q,b)$ points. À l'instant $x \geq 2$, le compétiteur gagnant entre "a mod q" et "b mod q" est celui qui marque strictement plus de points à cet instant. Ainsi pour la plupart des instants $x \geq 2$, il a été remarqué que le compétiteur "a mod q" a plus de chance de gagner cette course par rapport au compétiteur "b mod q".

La théorie comparative des nombres est un sous-domaine de la théorie des nombres qui concerne l'étude de ces courses. Il est important de comprendre les irrégularités dans la répartition des nombres premiers et en particulier "le biais de Chebyshev".

Rubinstein et Sarnak ont étudié l'origine de ce phénomène sous les deux hypothèses suivantes :

- **HRG (hypothèse de Riemann généralisée)**: Pour tout caractère de Dirichlet χ, si s est un nombre complexe tel que $0 \leq \Re(s) \leq 1$ et $L(s,\chi) = 0$, alors $\Re(s) = \frac{1}{2}$.
- **LI (hypothèse d'indépendance linéaire)**: Le multi-ensemble $\left\{\gamma \geq 0 : L(\frac{1}{2} + i\gamma, \chi) = 0\right\}$ où χ parcourt l'ensemble de tous les caractères primitifs de Dirichlet, est linéairement indépendant sur $\mathbb{Q}$.

Ils ont été les premiers à démontrer la prédominance des premiers dans les classes des non-résidus quadratiques modulo q par rapport aux résidus quadratiques modulo q en supposant ces deux hypothèses.

Dès lors, de nombreux articles ont été écrits sur ce phénomène et sur des sujets connexes. Nous nous référons principalement aux articles de Granville et Martin [**GM06**], et de Ford et Konyagin [**FK02**] pour une revue détaillée de l'histoire de ce sujet. Mais vue la difficulté des études de ces questions, différents mathématiciens se sont orientés vers un autre ensemble de premiers, il s'agit des polynômes irréductibles unitaires sur un corps fini $\mathbb{F}_q$ (où q est une puissance d'un nombre premier impair). Cet ensemble s'avère très similaire à l'ensemble des nombres premiers. L'analogue de l'hypothèse de Riemann pour les courbes sur les corps finis a été prouvé par Weil en 1948. Ceci encourage à étudier les courses de polynômes irréductibles unitaires.

Cha [**Cha08**] était le premier à étudier les courses de polynômes irréductibles unitaires. Sous l'hypothèse d'indépendance linéaire dans le cas des corps de fonctions (LI ★) (voir la Définition 2.3.3), il a réussi à démontrer des résultats similaires à ceux de Rubinstein et Sarnak. Sauf que Cha a également construit des exemples explicites où (LI ★) est fausse, pour lesquels le biais de Chebyshev pour les polynômes irréductibles unitaires est totalement différent du cas des nombres premiers. D'autres généralisations ont été étudiées depuis lors dans [**Lam13**], [**FM13**], [**CK10**], [**DM18**], [**CFJ16**], [**Lam12**], [**LM22**] et [**FJ22**].

L'objectif principal de cette thèse est l'étude des courses de polynômes irréductibles unitaires à 2 compétiteurs ou plus dans les corps de fonctions.

Nous commencerons d'abord par définir un ensemble de notations qui seront utilisées par la suite.

On désigne par $\mathcal{M}_q$ l'ensemble des polynômes unitaires dans l'anneau des polynômes $\mathbb{F}_q[T]$. Soit $m \in \mathcal{M}_q$ de degré $M \geq 1$ et r un entier ≥ 2. On définit la norme de m ainsi $|m| = q^{\deg(m)}$ et dans ce cas $M = \deg(m) = \log_q |m|$, où $\log_q x = \frac{\log x}{\log q}$ pour tout $x > 0$. Pour $a \in \mathbb{F}_q[T]$ premier avec m et pour $N \in \mathbb{N}^*$, on désigne par $\pi_q(a,m,N)$ le nombre de polynômes irréductibles unitaires congrus à a modulo m et de degré N.

Soit $\mathcal{A}_r(m)$ l'ensemble des r-uplets de classes de résidus distinctes $(a_1,a_2,\ldots,a_r)$ modulo m qui sont premiers avec m. Pour $(a_1,a_2,\ldots,a_r) \in \mathcal{A}_r(m)$, on définit :

$$P_{m;a_1,..,a_r} := \left\{ X \in \mathbb{N}^* : \sum_{N=1}^{X} \pi_q(a_1,m,N) > \sum_{N=1}^{X} \pi_q(a_2,m,N) > ... > \sum_{N=1}^{X} \pi_q(a_r,m,N) \right\}.$$

Ainsi, l'étude des courses de polynômes irréductibles unitaires à $r \geq 2$ compétiteurs (ce qui consiste à comparer le nombre de "premiers" congrus à a_1 modulo m vs ceux congrus à a_2 modulo m vs ... vs ceux congrus à a_r modulo m) se réduit à l'étude de la densité naturelle suivante :

$$\delta_{m;a_1,..,a_r} := \lim_{X \longrightarrow +\infty} \frac{\#\left(P_{m;a_1,..,a_r} \cap \{1,2,..,X\}\right)}{X},$$

si elle existe. Sous l'hypothèse (LI ★), Cha [**Cha08**] a prouvé l'existence de cette densité et elle vaut $\mu_{m;a_1,...,a_r}(\{x_1 > \cdots > x_r\} \subset \mathbb{R}^r)$ où $\mu_{m;a_1,...,a_r}$ est une mesure de probabilité construite dans le théorème 3.2 de [**Cha08**].

Cha a aussi établi que $\delta_{m;a,b} \to 1/2$ quand $\deg(m) \to +\infty$, uniformément pour toutes les classes de résidus réduits distinctes a,b modulo m. En effet, il a prouvé qu'en général tous les biais se dissipent lorsque $M \to +\infty$. Soit

$$\Delta_r(m) := \max_{(a_1,a_2,...,a_r) \in \mathcal{A}_r(m)} \left| \delta_{m;a_1,...,a_r} - \frac{1}{r!} \right|. \tag{0.0.1}$$

Pour tout entier fixé $r \geq 2$, Cha a prouvé sous l'hypothèse (LI ★) que :

$$\Delta_r(m) \to 0 \text{ quand } M = \deg(m) \to +\infty. \tag{0.0.2}$$

L'un des principaux objectifs de cette thèse est d'étudier, pour r un entier fixé ≥ 2, les différentes densités $\delta_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}}$ pour toute permutation $\sigma \in S_r$ (quand elles existent). Il est également intéressant de savoir si les biais se dissipent quand le nombre de compétiteurs r varie en fonction du degré de m, lorsque r et $\deg(m)$ tendent vers $+\infty$.

Cette thèse est organisée de la manière suivante :

Dans le premier chapitre, nous ferons un tour d'horizon sur les courses de nombres premiers. Nous commencerons d'abord par énoncer les différents résultats relatifs à la théorie comparative des nombres. Nous évoquerons principalement les travaux de Rubinstein et Sarnak [**RS94**], de Fiorilli et Martin [**FM13**]. Ensuite, nous nous focaliserons sur les travaux de Feuerverger et Martin [**FM00**] et de Lamzouri [**Lam13**]. Nous évoquerons après les résultats obtenus dans [**Lam12**], [**FHL19**] et [**HL18**].

Dans le deuxième chapitre, nous nous intéresserons à la généralisation des travaux de Rubinstein et Sarnak [**RS94**] dans le cadre des corps de fonctions. Nous rappellerons quelques définitions et propriétés basiques, à savoir la fonction zêta et les fonctions L de Dirichlet dans les corps de fonctions, ainsi que quelques analogies entre corps de nombres et corps de fonctions (voir [**Ros02**]). Par la suite, nous énoncerons et démontrerons quelques résultats, qui sont extraits de [**Sed22**] et qui sont relatifs à l'arithmétique sur $\mathbb{F}_q[T]$. Ces derniers seront utilisés tout au long de cette thèse. À la fin de ce chapitre, nous exposerons les résultats de Cha [**Cha08**].

Dans le troisième chapitre, nous présenterons les travaux effectués dans l'article [**Sed22**]. Ces travaux représentent une continuité des travaux de [**Lam13**] dans le contexte des corps de fonctions. Nous donnerons quelques exemples de courses dans les corps de fonctions lorsque (LI ★) est fausse et les densités associées s'annulent.

Le quatrième et dernier chapitre est consacré particulièrement aux courses des polynômes irréductibles unitaires dont le nombre de compétiteurs r tend vers $+\infty$ quand $|m| \longrightarrow +\infty$. Pour clôturer ce chapitre, nous énoncerons quelques perspectives sur d'éventuels autres travaux de recherches.

Chapitre 1

Généralités sur les courses de nombres premiers

En 1853, dans une lettre adressée à Fuss [**Tsc53**], Chebyshev a constaté qu'il y a plus de nombres premiers congrus à 3 mod 4 que de nombres premiers congrus à 1 mod 4 dans les intervalles d'entiers [2,x], pour la plupart des entiers x.

L'observation de Chebyshev semble vraie dans les intervalles initiaux d'entiers, comme nous pouvons le constater dans le tableau suivant :

x	Nombre de premiers de la forme $4n+3$ inférieur à x	Nombre de premiers de la forme $4n+1$ inférieur à x
100	13	11
200	24	21
300	32	29
1000	87	80
2000	155	147
3000	218	211
10000	619	609
20000	1136	1125

Tableau 1. Nombre de premiers inférieurs à x de la forme $4n+3$ et de la forme $4n+1$.

Il semble qu'on ait plus souvent $\pi(x;4,3) > \pi(x;4,1)$. Cependant, cette inégalité n'est pas vraie pour tout $x \geq 2$. En effet pour $x = 26861$, on a $\pi(x;4,1) > \pi(x;4,3)$.
Puis, à l'instant $x = 26863$, les compétiteurs 3 mod 4 et 1 mod 4 sont à égalité. Ensuite le compétiteur 3 mod 4 reprend la tête de la course pour une longue série d'entiers x (voir [**GM06**]).

Une question naturelle qu'on pourrait se poser est la suivante : existe-t-il un instant $x_0 \geq 2$ à partir duquel le compétiteur 3 mod 4 sera toujours gagnant de la course contre le compétiteur 1 mod 4 ?

En 1914, Littlewood a répondu à cette question en démontrant qu'il n'existe pas de $x_0 \geq 2$ tel que pour tout $x \geq x_0$ le compétiteur 3 mod 4 est toujours gagnant contre le compétiteur 1 mod 4. Il a prouvé que la quantité $\pi(x;4,3) - \pi(x;4,1)$ change de signe pour une infinité d'entiers x [**Lit14**]. Cependant, le compétiteur 3 mod 4 est souvent en tête pendant une longue période. Afin de quantifier ce phénomène, on estime "la taille" de $S_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}$.
On propose alors deux méthodes pour estimer la taille d'un ensemble.
La première méthode est la densité naturelle définie comme suit :

Définition 1.0.1. *Soit A un sous ensemble de $\mathbb{N}$. La densité naturelle d'un ensemble A, si elle existe, est égale à :*

$$\lim_{x \longrightarrow +\infty} \frac{|A \cap [2,x]|}{x}.$$

Sinon, on dit que la densité naturelle de A n'existe pas.

La deuxième méthode est la densité logarithmique définie ainsi :

Définition 1.0.2. *La densité logarithmique d'un Borélien P de $\mathbb{R}^+$, quand elle existe, est égale à :*

$$\delta(P) = \lim_{X \longrightarrow +\infty} \frac{1}{\log X} \int_2^X \mathbb{1}_P(t) \frac{dt}{t} = \lim_{Y \longrightarrow +\infty} \frac{1}{Y} \int_{\log 2}^Y \mathbb{1}_P(e^t) dt \tag{1.0.1}$$

Remarque 1.0.3. *Si un ensemble A admet une densité naturelle, alors il admet une densité logarithmique et ces deux densités sont égales. Cependant, il existe des ensembles qui possèdent une densité logarithmique sans avoir de densité naturelle.*

Knapowski et Turán [**KT62**] ont conjecturé que la densité naturelle de $S_{4;3,1}$ existe et elle vaut 1. Cependant, Kaczorowski [**Kac95**] a montré sous l'hypothèse de Riemann pour la fonction L associée au caractère non principal χ_4 modulo 4 que la densité naturelle de l'ensemble $S_{4;3,1}$ n'existe pas.

Remarque 1.0.4. *Soit $(a,b) \in \mathcal{B}_2(q)$. Ford, Konyagin et Lamzouri* [**FLK13**] *ont prouvé que l'existence de certains ensembles hypothétiques de zéros de fonctions L de Dirichlet en dehors de la droite critique implique que la densité naturelle de $S_{q;a,b}$ (l'ensemble des réels $x \geq 2$ tels que $\pi(x;q,a) > \pi(x;q,b)$) est égale à 0. Ceci contredit un résultat conditionnel de Kaczorowski* [**Kac93**] *sous HRG qui affirme que pour tout $(a,q) = 1$, on a :*

$$\liminf_{x \longrightarrow +\infty} \frac{|S_{q;a,1} \cap [2,x]|}{x} > 0 \quad et \quad \liminf_{x \longrightarrow +\infty} \frac{|S_{q;1,a} \cap [2,x]|}{x} > 0.$$

Dans ce chapitre, nous allons énoncer des résultats relatifs aux courses des nombres premiers en utilisant la densité logarithmique.

Tout au long de ce chapitre, q désignera un entier ≥ 3.
Soit r un entier ≥ 2. On rappelle que $\mathcal{B}_r(q)$ est l'ensemble des r-uplets de classes de résidus distinctes $(a_1,a_2,\ldots,a_r)$ modulo q qui sont premiers avec q.

1.1. Courses de nombres premiers à 2 compétiteurs

Soit $(a,b) \in \mathcal{B}_2(q)$. On définit l'ensemble $S_{q;a,b}$ comme suit :

$$S_{q;a,b} := \{x \geq 2 \mid \pi(x;q,a) > \pi(x;q,b)\}.$$

En 1994, Rubinstein et Sarnak ont démontré que la densité logarithmique de $S_{q;a,b}$ existe sous les deux hypothèses suivantes :

- L'hypothèse de Riemann généralisée (HRG): les zéros non triviaux de la fonction zêta de Riemann ont tous pour partie réelle $\frac{1}{2}$.
- L'hypothèse d'indépendance linéaire (LI) : les parties imaginaires positives des zéros non triviaux de toutes les fonctions L de Dirichlet associées à tous les caractères de Dirichlet modulo q sont linéairement indépendantes sur $\mathbb{Q}$.

Remarques 1.1.1.

- *HRG et LI impliquent que pour tout caractère de Dirichlet χ modulo q, on a $L(s,\chi) \neq 0$ pour tout $s \in]0,1[$, ce qui confirme la conjecture de Chowla* [**Cho65**].
- *LI implique que les zéros des fonctions L de Dirichlet modulo q sont simples.*

Sous ces hypothèses, Rubinstein et Sarnak [**RS94**] ont prouvé que $\delta(4;3,1) \approx 0.9959$, ce qui confirme l'observation de Chebyshev.
Ils ont également démontré sous HRG et LI que $\delta(S_{q;a,b})$ est strictement comprise entre 0 et 1 et elle satisfait :

$$\delta(S_{q;a,b}) > \frac{1}{2} \Longleftrightarrow a \text{ est un non-résidu quadratique modulo } q$$
$$\text{et } b \text{ est un résidu quadratique modulo } q.$$

$$\delta(S_{q;a,b}) = \frac{1}{2} \Longleftrightarrow a \text{ et } b \text{ sont simultanément des résidus quadratiques}$$
$$\text{ou des non-résidus quadratiques modulo } q.$$

Rubinstein et Sarnak [**RS94**] ont également prouvé, sous HRG et LI, que si a,b sont fixés et q parcourt l'ensemble des entiers premiers avec a et b alors :

$$\lim_{\substack{q \longrightarrow +\infty \\ (q,ab)=1}} \delta(S_{q;a,b}) = \frac{1}{2}.$$

En 2009, Fiorilli et Martin [**FM13**] ont estimé la vitesse de convergence de $\delta(S_{q;a,b})$ vers $\frac{1}{2}$. Ils ont établi dans un premier temps une formule asymptotique pour $\delta(S_{q;a,b})$. Avant de l'énoncer, on donne la définition suivante :

Définition 1.1.2. *Pour tout caractère de Dirichlet modulo q. On définit*

$$b(\chi) = \sum_{\substack{\gamma\in\mathbb{R} \\ L(1/2+i\gamma,\chi)=0}} \frac{1}{\frac{1}{4}+\gamma^2},$$

et pour tout $(a,b) \in \mathcal{B}_2(q)$

$$V(q;a,b) = \sum_{\chi \bmod q} |\chi(b)-\chi(a)|^2 \, b(\chi).$$

Théorème 1.1.3. [**FM13**, Théorème 1.1]. *On suppose que GRH et LI sont vraies. Soit $(a,b) \in \mathcal{B}_2(q)$ tel que a est un non-résidu quadratique modulo q et b un résidu quadratique modulo q alors*

$$\delta(S_{q;a,b}) = \frac{1}{2} + \frac{\rho(q)}{\sqrt{2\pi V(q;a,b)}} + O\left(\frac{\rho(q)^3}{V(q;a,b)^{3/2}}\right), \tag{1.1.1}$$

où $\rho(q)$ désigne le nombre de solutions de $x^2 \equiv 1 \mod q$.

Remarque 1.1.4. *$\rho(q)$ est également le nombre de caractères réels modulo q.*

En utilisant le fait que $V(q;a,b) \sim 2\phi(q)\log q$ et que $\rho(q) \ll_\epsilon q^\epsilon$ pour tout $\epsilon > 0$, ils déduisent facilement sous les mêmes hypothèses le théorème suivant :

Théorème 1.1.5. *Sous GRH et LI on a*

$$\max_{(a,b)\in\mathcal{B}_2(q)} \left|\delta(S_{q;a,b}) - \frac{1}{2}\right| = \frac{1}{q^{1/2+o(1)}}.$$

Fiorilli et Martin [**FM13**] ont également établi de bonnes estimations de $V(q;a,b)$, ce qui leur a permis de calculer les densités $\delta(S_{q;a,b})$. Ils ont ainsi déterminé l'ensemble des 117 valeurs des densités qui dépassent $\frac{9}{10}$. Ils ont aussi prouvé que la course entre deux compétiteurs, la plus biaisée, est celle entre le compétiteur "5 mod 24" et le compétiteur "1 mod 24". Dans ce cas, $\delta(S_{24;5,1}) = 0.999988\ldots$

Il est possible de créer des courses de nombres premiers en combinant différentes classes de résidus modulo q. Pour A,B deux sous ensembles de $(\mathbb{Z}/q\mathbb{Z})^\times$, on définit l'ensemble :

$$O_{q,A,B} := \left\{ \frac{\sum_{a\in A}\pi(x;q,a)}{\#A} > \frac{\sum_{a\in B}\pi(x;q,b)}{\#B} \right\}.$$

On considère NR l'ensemble des premiers dans les classes des non-résidus quadratiques modulo q et R l'ensemble des premiers dans les classes des résidus quadratiques modulo q. Rubinstein et Sarnak se sont intéressés à la course entre NR et R. Ils ont ainsi obtenu le résultat suivant :

Théorème 1.1.6. *On considère l'ensemble $K = \{4, p^k, 2p^k\}$ où p est un nombre premier distinct de 2 et k un entier naturel non nul.*
Soit $q \in K$. Supposons GRH et LI vraies, alors :

$$\delta(O_{q;NR,R}) > \frac{1}{2},$$

et

$$\lim_{\substack{q' \in K \\ q' \longrightarrow +\infty}} \delta(O_{q';NR,R}) = \frac{1}{2}. \tag{1.1.2}$$

Cependant, l'égalité (1.1.2) n'est pas toujours vraie quand $q' \notin K$. En effet, Fiorilli a démontré le théorème suivant :

Théorème 1.1.7. [**Fio14**, Théorème 1.1] *Supposons GRH et LI vraies. Alors pour tout $\epsilon > 0$, il existe q tel que*

$$1 - \epsilon < \delta(O_{q;NR,R}) < 1.$$

En plus, pour tout $\frac{1}{2} \leq \nu \leq 1$ il existe une suite d'entiers naturels $\{q_n\}$ telle que

$$\lim_{n \longrightarrow +\infty} \delta(O_{q_n;NR,R}) = \nu.$$

Les travaux de Rubinstein et Sarnak [**RS94**] ont été généralisés dans plusieurs autres contextes. Ainsi, dans le cadre de leurs travaux de recherche, Nathan Ng [**Ng00**], Alexandre Bailleul [**Bai20**], Florent Jouve et Daniel Fiorilli [**FJ23**] ont respectivement étudié les courses de nombres premiers dans le contexte de la répartition des automorphismes de Frobenius au sein des groupes de Galois d'extensions de corps de nombres.

1.2. Courses de nombres premiers à $r \geq 3$ compétiteurs avec r fixé.

Knapowski et Turàn ont rédigé une série de travaux concernant le problème plus général des courses de nombres premiers. Ils ont pu le modéliser comme suit :
Soit r un entier ≥ 2 et a_1,...,$a_r \in \mathcal{B}_r(q)$. Plusieurs compétiteurs "$a_1 \bmod q, \ldots, a_r \bmod q$" participent à une course à points, le compétiteur gagnant à un instant x donné est celui qui a le plus de points à cet instant. Le nombre de points marqués à un instant x (≥ 2) par le compétiteur "$a_i \bmod q$" est $\pi(x; q,a_i)$.

Pour étudier ce problème, on généralise la définition de $S_{q;a,b}$ à plusieurs compétiteurs. Soit r un entier ≥ 2, on définit

$$S_{q,a_1,a_2,\ldots,a_r} = \{x \geq 2 : \pi(x; q,a_1) > \pi(x; q,a_2) > \ldots > \pi(x; q,a_r)\} \tag{1.2.1}$$

On peut poser les questions suivantes concernant cet ensemble :

- Est-ce que l'ensemble $S_{q;a_1,a_2,\ldots,a_r}$ est vide?

- Quelles sont les différentes informations disponibles sur $\delta(S_{q;a_1,a_2,\ldots,a_r})$ (dans le cas où cette dernière existe) ?
- Pour $r \geq 3$, peut-on déterminer des conditions sur a_i qui permettent d'avoir pour toute permutation σ de $\{1,2,\ldots,r\}$ l'égalité suivante $\delta(S_{q;a_{\sigma(1)},a_{\sigma(2)},\ldots,a_{\sigma(r)}}) = \frac{1}{r!}$?
- Pour r fixé et $q \longrightarrow +\infty$, est-ce que la densité logarithmique de $S_{q;a_1,a_2,\ldots,a_r}$ existe? Si c'est le cas, quelle est sa valeur?

Afin de répondre à certaines de ces questions, Rubinstein et Sarnak [**RS94**] ont introduit la fonction auxiliaire

$$E(x;q,a) = \frac{(\phi(q)\pi(x;q,a) - \pi(x))\log(x)}{\sqrt{x}},$$

qui mesure combien il y a plus (ou moins) de nombres premiers dans la classe résiduelle de a par rapport à la valeur attendue. Ils ont également défini le vecteur $\epsilon_{q;a_1,\ldots,a_r}(x) = (E(x;q,a_1),\ldots,E(x;q,a_r))$. On considère $E_{q;a_1,\ldots,a_r}(y) = \epsilon_{q;a_1,\ldots,a_r}(e^y)$.
On rappelle la définition d'une distribution limite :

Définition 1.2.1. *Soit $n \in \mathbb{N}^*$ et $F : \mathbb{N} \to \mathbb{R}^n$ une fonction. La distribution limite de la fonction F, si elle existe, est la mesure de probabilité μ sur $\mathbb{R}^n$ telle que pour toute fonction continue et bornée g sur $\mathbb{R}^n$, on a*

$$\lim_{X\to\infty} \frac{1}{X} \sum_{k\leq X} g(F(k)) = \int_{\mathbb{R}^n} g(t)d\mu(t).$$

Rubinstein et Sarnak ont utilisé l'hypothèse HRG afin de prouver l'existence d'une distribution limite de $E_{q;a_1,\ldots,a_r}$. Pour ce faire, ils ont d'abord démontré la proposition suivante:

Proposition 1.2.2. *Soit a un entier premier avec q. Supposons HRG vraie pour les fonctions L de Dirichlet modulo q, alors pour tout $x \geq 2$ on a*

$$E(x;q,a) = -c(q,a) - \sum_{\chi\neq\chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2} + i\gamma_\chi} + O\left(\frac{1}{\log x}\right),$$

où $c(q,a) := -1 + \sum_{\substack{b^2\equiv a \bmod q \\ b\in(\mathbb{Z}/q\mathbb{Z})^\times}} 1$ et γ_χ parcourt l'ensemble des parties imaginaires des zéros non triviaux de la fonction L associée au caractère χ.

En combinant cette proposition avec le théorème de Kronecker-Weyl [**Hum13**, Lemme 5.3], Rubinstein et Sarnak aboutissent au résultat suivant :

Théorème 1.2.3. *Supposons que HRG est vraie pour les fonctions L de Dirichlet modulo q, alors il existe une mesure Borélienne $\mu_{q,a_1,\ldots,a_r}$ sur $\mathbb{R}^r$ telle que*

$$\lim_{X\to+\infty} \frac{1}{\log X} \int_2^X f(E_{q,a_1,a_2,\ldots,a_r}(x))\frac{dx}{x} = \int_{\mathbb{R}^r} f(x)d\mu_{q,a_1,..,a_r}(x),$$

pour toute fonction $f : \mathbb{R}^r \to \mathbb{R}$ bornée et continue.

Ils ont également supposé l'hypothèse LI pour permettre d'assurer que la somme $\sum_{\chi\neq\chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi}$ se comporte comme une somme de variables aléatoires indépendantes

uniformes sur $\mathbb{S}^1$. Ceci permet par la suite d'étudier les propriétés de $\mu_{q;a_1,..,a_r}$ et de montrer l'existence de $\delta(S_{q;a_1,...,a_r})$.

Soit $(a_1,a_2,a_3) \in \mathcal{B}_3(q)$. Feuerverger et Martin se sont intéressés au calcul de la densité $\delta(S_{q;a_1,a_2,a_3})$. Pour $q \leq 12$, sous les mêmes hypothèses que ceux utilisés par Rubinstein et Sarnak, ils ont pu calculer certaines densités et ont alors démontré le théorème suivant :

Théorème 1.2.4. [**FM00**]. *Sous HRG et LI, on a :*

$$\delta(S_{8;3,5,7}) = \delta(S_{8;7,3,5}) > \frac{1}{6}, \quad \delta(S_{8;5,3,7}) = \delta(S_{8;7,3,5}) < \frac{1}{6}$$

et

$$\delta(S_{12;5,7,11}) = \delta(S_{12;11,7,5}) > \frac{1}{6}, \quad \delta(S_{12;5,11,7}) = \delta(S_{12;7,11,5}) < \frac{1}{6}.$$

Ce résultat montre que les courses à 2 compétiteurs et les courses à 3 compétiteurs ne se comportent pas exactement de la même manière. En effet, bien que 3, 5, et 7 soient des non-résidus quadratiques modulo 8, on remarque que $\delta(S_{8;3,5,7}) \neq \frac{1}{3!}$. Dans ce cas on dit que la course {8,3,5,7} est biaisée. On donne la définition suivante :

Définition 1.2.5. [**Lam13**, Définition 1] *Soit r un entier ≥ 2 et $(a_1, \ldots, a_r) \in \mathcal{B}_r(q)$. La course $\{q; a_1, \ldots, a_r\}$ est dite non biaisée si pour toute permutation σ de $\{1,2,\ldots,r\}$ on a*

$$\delta(S_{q;a_{\sigma(1)},\ldots,a_{\sigma(r)}}) = \frac{1}{r!},$$

où $\delta(S_{q;a_1,\ldots,a_r})$ désigne la densité logarithmique de l'ensemble $S_{q;a_1,\ldots,a_r}$.

Feuerverger et Martin ont été les premiers à donner des exemples explicites de courses biaisées avec trois compétiteurs pour $q \leq 12$. Cependant, dans leur article [**FM00**], ils n'ont pas pu déterminer l'existence de courses biaisées pour tout $q > 12$ et $3 \leq r \leq \phi(q)$.

Lamzouri [**Lam13**] a donné une réponse à cette question pour tout entier fixé $r \geq 3$ si q est un entier assez grand. En effet, il a démontré que contrairement aux courses entre deux résidus quadratiques (ou non-résidus quadratiques), des biais apparaissent dans les courses impliquant r résidus quadratiques (ou r non-résidus quadratiques).

Théorème 1.2.6. [**Lam13**, Théorème 1.4] *Soit r un entier ≥ 3. Supposons que HRG et LI sont vraies. Alors il existe une constante positive $q_0(r)$ telle que pour tout entier $q \geq q_0(r)$ il existe*

- *$(a_1, \ldots, a_r) \in \mathcal{B}_r(q)$ tel que $a_1, \ldots, a_r$ sont tous des **résidus quadratiques** modulo q et la course $\{q; a_1, a_2, \ldots, a_r\}$ est biaisée.*
- *$(b_1, \ldots, b_r) \in \mathcal{B}_r(q)$ tel que $b_1, \ldots, b_r$ sont tous des **non-résidus quadratiques** modulo q et la course $\{q; b_1, b_2, \ldots, b_r\}$ est biaisée.*

On donne la définition suivante :

Définition 1.2.7. *Soit r un entier ≥ 2, on définit*

$$\tilde{\Delta}_r(q) = \max_{(a_1,\ldots,a_r)\in\mathcal{B}_r(q)} \left|\delta(S_{q;a_1,\ldots,a_r}) - \frac{1}{r!}\right|.$$

Lamzouri a aussi prouvé le théorème suivant :

Théorème 1.2.8. [**Lam13**, Théorème 1.1] *Soit $r \geq 3$ un entier. Supposons que HRG et LI sont vraies. Il existe des constantes strictement positives $c_1(r)$, $c_2(r)$ et un entier $q_0 \in \mathbb{N}^*$ tel que si $q \geq q_0$ alors*

$$\frac{c_1(r)}{\log q} \leq \tilde{\Delta}_r(q) \leq \frac{c_2(r)}{\log q}.$$

Ce résultat montre que $\tilde{\Delta}_r(q)$ se comporte de manière complètement différente lorsque $r \geq 3$. En effet, $\tilde{\Delta}_2(q)$ converge plus rapidement que $\tilde{\Delta}_r(q)$ vers 0, lorsque $r \geq 3$.

1.3. Courses de nombres premiers lorsque le nombre des compétiteurs $r \longrightarrow +\infty$ quand $q \longrightarrow +\infty$.

Dans cette partie, on énonce les différents résultats obtenus concernant les courses des nombres premiers lorsque le nombre des compétiteurs $r \longrightarrow +\infty$ quand $q \longrightarrow +\infty$.

Rubinstein et Sarnak [**RS94**] ont déjà montré conditionnellement que pour r un entier fixé on a

$$\lim_{q \to +\infty} \max_{(a_1,\dots,a_r) \in \mathcal{B}_r(q)} \left| \delta(S_{q;a_1,\dots,a_r}) - \frac{1}{r!} \right| = 0. \tag{1.3.1}$$

Feuerverger et Martin [**FM00**] ont soulevé la question de l'existence d'une version uniforme de (1.3.1), dans laquelle le nombre de concurrents $r \to +\infty$ quand $q \to +\infty$. En réponse à cette question, Lamzouri parvient à prouver le théorème suivant :

Théorème 1.3.1. [**Lam12**, Théorème 1.1] *Supposons que HRG et LI sont vraies. Alors pour tout entier r tel que $2 \leq r \leq \sqrt{\log q}$ on a*

$$\delta(S_{q;a_1,\dots,a_r}) = \frac{1}{r!}\left(1 + O\left(\frac{r^2}{\log q}\right)\right),$$

uniformément pour tout r-uplet $(a_1, \dots, a_r) \in \mathcal{B}_r(q)$.

Feuerverger et Martin [**FM00**] se sont également demandés si pour r suffisamment grand en fonction de q la formule asymptotique $\delta(S_{q;a_1,\dots,a_r}) \sim 1/r!$ pourrait devenir fausse. En essayant de répondre à cette question, Ford et Lamzouri ont formulé la conjecture suivante :

Conjecture 1.3.2 (Ford et Lamzouri)**.** *Soit $\epsilon > 0$ un réel assez petit et q un entier suffisamment grand.*

(1) Si $2 \leq r \leq (\log q)^{1-\epsilon}$, alors on a $\delta(S_{q;a_1,\dots,a_r}) \sim 1/r!$ lorsque $q \to +\infty$ uniformément pour tout r-uplet $(a_1, \dots, a_r) \in \mathcal{B}_r(q)$.

(2) Si $(\log q)^{1+\epsilon} \leq r \leq \phi(q)$, alors ils existent des r-uplets $(a_1, \dots, a_r), (b_1, \dots, b_r) \in \mathcal{B}_r(q)$ pour lesquels $r! \cdot \delta(S_{q;a_1,\dots,a_r}) \to 0$ et $r! \cdot \delta(S_{q;b_1,\dots,b_r}) \to +\infty$ lorsque $q \to +\infty$.

Harper et Lamzouri [**HL18**] ont démontré la première partie de cette conjecture.

Théorème 1.3.3. [**HL18**, Théorème 1.2] *On suppose que HRG et LI sont vraies. Soit* $2 \leq r \leq \log q/(\log\log q)^4$ *un entier positif. On a*

$$\delta(S_{q;a_1,\dots,a_r}) = \frac{1}{r!}\left(1 + O\left(\frac{r(\log r)^4}{\log q}\right)\right),$$

uniformément pour tout r*-uplet* $(a_1,\dots,a_r) \in \mathcal{B}_r(q)$.

La deuxième partie de la Conjecture 1.3.2 implique, en particulier, que la formule asymptotique $\delta(S_{q;a_1,\dots,a_r}) \sim 1/r!$ n'est pas nécessairement valable pour tous les r-uplets $(a_1,\dots,a_r) \in \mathcal{B}_r(q)$. Le prochain résultat montre que c'est effectivement le cas dans l'intervalle $\phi(q)^\epsilon < r \leq \phi(q)$. Ainsi, dans cette région de r, Harper et Lamzouri ont pu montrer l'existence des courses de nombres premiers telles que $\delta(S_{q;a_1,\dots,a_r}) \not\sim 1/r!$ lorsque $q \to +\infty$ dans le théorème suivant :

Théorème 1.3.4. *On suppose que HRG et LI sont vraies. Soit* $\epsilon > 0$ *et* q *un entier assez grand en fonction de* ϵ. *Pour tout entier* $\phi(q)^\epsilon \leq r \leq \phi(q)$ *il existe un* r*-uplet* $(a_1,\dots,a_r) \in \mathcal{B}_r(q)$ *tel que*

$$\delta(S_{q;a_1,\dots,a_r}) < \big(1 - c_\epsilon\big)\frac{1}{r!},$$

pour une certaine constante $c_\epsilon > 0$ *qui dépend uniquement de* ϵ.

Ce dernier théorème ne répond pas à la deuxième partie de la Conjecture 1.3.2. Afin d'y donner une réponse, Ford, Harper et Lamzouri [**FHL19**] ont démontré le théorème suivant :

Théorème 1.3.5. *Supposons que HRG et LI sont vraies. Alors il existe une constante absolue* C *tel que l'assertion suivante est vraie.*
Supposons que r *est suffisamment grand et* $r \leq \phi(q)$ *alors il existe des classes de résidus distinctes* $a_1,\dots,a_r \bmod q$ *tel que*

$$\delta(S_{q;a_1,\dots,a_r}) \leq \exp\left(\frac{-\min\left\{r, \phi(q)^{1/50}\right\}}{C\log q}\right)\frac{1}{r!},$$

et il existe des classes de résidus distinctes $b_1,\dots,b_r \bmod q$ *tel que*

$$\delta(S_{q;b_1,\dots,b_r}) \geq \exp\left(\frac{\min\left\{r, \phi(q)^{1/50}\right\}}{C\log q}\right)\frac{1}{r!}.$$

Grâce à ce résultat, on déduit que si $\frac{r}{\log q} \longrightarrow +\infty$ quand $q \longrightarrow +\infty$ alors il existe des classes de résidus distinctes $a_1,\dots,a_r \bmod q$ tel que $r!\delta(S_{q;a_1,\dots,a_r}) \longrightarrow 0$ et des classes de résidus distinctes $b_1,\dots,b_r \bmod q$ tel que $r!\delta(S_{q;b_1,\dots,b_r}) \longrightarrow +\infty$. Ainsi, les biais ne dissipent pas toujours lorsque q tend vers $+\infty$.

Chapitre 2

Biais de Chebyshev dans les corps de fonctions

2.1. Fonction zêta et fonctions L de Dirichlet dans les corps de fonctions

Dans cette section, on rappelle quelques propriétés sur la fonction zêta et les fonctions L de Dirichlet dans le contexte de l'anneau des polynômes $A = \mathbb{F}_q[T]$.
On désigne respectivement par $\mathcal{M}_q$ l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$, et $\mathcal{P}_q$ l'ensemble des polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$.

La fonction zêta de Riemann classique s'est avérée être fondamentale dans l'étude de la répartition des nombres premiers. En effet, on peut constater le lien établi par Euler entre la fonction zêta de Riemann classique et les nombres premiers dans la relation suivante pour tout $s \in \mathbb{C}$ avec $\Re(s) > 1$:

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

D'une manière similaire, on définit ainsi l'analogue de la fonction zêta de Riemann classique dans les corps des fonctions :

$$\zeta_A(s) = \sum_{f \in \mathcal{M}_q} \frac{1}{|f|^s} \quad \text{pour tout } s \in \mathbb{C} \text{ avec } \Re(s) > 1, \text{ où } |f| = q^{\deg(f)}.$$

La fonction $\zeta_A(s)$ converge et est analytique sur $\Re(s) > 1$. De plus, puisque la norme $|f|$ est totalement multiplicative, alors on obtient :

$$\zeta_A(s) = \prod_{P \in \mathcal{P}_q} \left(1 - \frac{1}{|P|^s}\right)^{-1}.$$

Ainsi, comme pour la fonction zêta de Riemann classique, la fonction $\zeta_A(s)$ admet également un produit eulérien.

Puisque pour tout $n \in \mathbb{N}$, il y a exactement q^n polynômes irréductibles unitaires de degré n alors pour tout $d \in \mathbb{N}^*$ on a :

$$\sum_{\deg(f)\leq d} \frac{1}{|f|^s} = 1 + \frac{1}{q^{s-1}} + \cdots + \frac{1}{q^{d(s-1)}} = \frac{1-(q^{1-s})^{d+1}}{1-q^{1-s}}.$$

Donc pour tout $s \in \mathbb{C}$ avec $\Re(s) > 1$ on a :

$$\zeta_A(s) = \frac{1}{1-q^{1-s}}.$$

La fonction ζ_A est alors prolongeable par continuité sur tout le plan complexe à une fonction méromorphe avec des pôles simples en $s = 1 + \frac{2i\pi k}{\log q}$ (où $k \in \mathbb{Z}$).

Remarque 2.1.1. *L'étude du prolongement de la fonction ζ_A est plus facile que celui de la fonction ζ de Riemann.*

On rappelle également la définition suivante :

Définition 2.1.2. *Soit $m \in \mathcal{M}_q$ de degré $M \geq 1$. Un caractère de Dirichlet modulo m est une fonction $\chi : \mathbb{F}_q[T] \longrightarrow \mathbb{C}$ qui vérifie les conditions suivantes :*

(1) $\forall a,b \in \mathbb{F}_q[T]$, on a : $\chi(a+bm) = \chi(a)$.

(2) $\forall a,b \in \mathbb{F}_q[T]$, on a : $\chi(ab) = \chi(a)\chi(b)$.

(3) $\chi(a) \neq 0$ si et seulement si $(a,m) = 1$.

Un caractère de Dirichlet modulo m induit un morphisme H de $(A/mA)^\times$ vers $\mathbb{C}^*$. Inversement, étant donné un tel morphisme H, il existe un unique caractère de Dirichlet qui correspond à H.

On désigne par X_m l'ensemble des caractères de Dirichlet modulo m. Comme X_m est un groupe isomorphe à $(A/mA)^\times$, alors le nombre de caractères de Dirichlet modulo m est $\#X_m = \#(A/mA)^\times$. Le cardinal de X_m est noté $\phi(m)$. Ce nombre correspond également au nombre de polynômes non nuls de $\mathbb{F}_q[T]$ de degré strictement inférieur au degré de m et qui sont premiers avec m.

Le caractère principal (ou trivial) de Dirichlet χ_0 modulo m est défini ainsi :

$$\chi_0(a) = \begin{cases} 1 & \text{si } (a,m) = 1, \\ 0 & \text{sinon.} \end{cases}$$

Dans ce qui suit, la notation χ_0 sera utilisée pour désigner le caractère principal modulo m.

Définition 2.1.3. *Soit $m \in \mathcal{M}_q$ de degré $M \geq 1$. On dit que χ est un caractère primitif modulo m s'il n'existe pas de diviseur propre $m'|m$ tel que $\chi(f) = 1$ pour tout $f \in \mathbb{F}_q[T]$ vérifiant $f \equiv 1 \mod m'$.*

Si χ est un caractère non primitif modulo m alors il existe un caractère primitif $\psi \mod m'$ tel que $m'|m$ et $\chi(a) = \psi(a)\chi_0(a)$ pour tout $a \in (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^\times$, où χ_0 est le caractère principal modulo m. Dans ce cas, on dit que le caractère ψ induit le caractère χ.

Définition 2.1.4. *Soit $m \in \mathcal{M}_q$ de degré $M \geq 1$. Un caractère de Dirichlet χ modulo m est dit pair s'il est est égal à la fonction constante qui retourne 1 sur tout le groupe $\mathbb{F}_q^*$.*
On dit qu'un caractère de Dirichlet χ modulo m est impair s'il n'est pas pair.

Remarque 2.1.5. *Il y a exactement $\frac{\phi(m)}{q-1}$ caractères de Dirichlet modulo m qui sont pairs. Donc quand q tend vers $+\infty$, la plupart des caractères de Dirichlet modulo m sont impairs (voir* [**Tao19**]*).*

Les caractères de Dirichlet vérifient les relations d'orthogonalité énoncées dans la proposition ci-dessous :

Proposition 2.1.6. *Soit $m \in \mathcal{M}_q$ de degré ≥ 1. Soit χ, ψ deux caractères de Dirichlet modulo m et a, b deux éléments de $\mathbb{F}_q[T]$ qui sont premiers avec m. Alors*

$$\sum_{\chi \bmod m} \chi(a)\overline{\chi(b)} = \phi(m)\delta(a,b), \tag{2.1.1}$$

et

$$\sum_{c \in (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^\times} \chi(c)\overline{\psi(c)} = \phi(m)\delta'(\chi,\psi), \tag{2.1.2}$$

où $\delta(a,b) = \begin{cases} 1 & \text{si } a \equiv b \bmod m, \\ 0 & \text{sinon.} \end{cases}$ *et* $\delta'(\chi,\psi) = \begin{cases} 1 & \text{si } \chi = \psi, \\ 0 & \text{sinon.} \end{cases}$

On associe à chaque caractère de Dirichlet χ modulo m une fonction L définie ainsi :

$$L(s,\chi) := \sum_{f \in \mathcal{M}_q} \frac{\chi(f)}{|f|^s} = \prod_{P \in \mathcal{P}_q} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1} \text{ pour } \Re(s) > 1,$$

En particulier, on a

$$L(s,\chi_0) = \prod_{P \in \mathcal{P}_q} \left(1 - \frac{\chi_0(P)}{|P|^s}\right)^{-1} = \prod_{P|m} \left(1 - \frac{1}{|P|^s}\right) \zeta_A(s).$$

Ceci prouve que $L(s,\chi_0)$ se prolonge analytiquement sur tout le plan complexe à une fonction méromorphe avec un pôle simple en $s = 1$.

En outre, Rosen a démontré la proposition suivante :

Proposition 2.1.7 ([**Ros02**, Proposition 4.3])**.** *Soit χ un caractère non-principal modulo m. Alors la fonction $L(s,\chi)$ est polynomial en q^{-s} de degré au plus* $\deg(m) - 1$.

Remarque 2.1.8. *Soit $m \in \mathcal{M}_q$ un polynôme de degré ≥ 1. Soit χ un caractère primitif modulo m. On a $L(s,\chi)$ est polynomial en q^{-s} de degré* $\deg(m) - 1$ *(voir la Proposition* 4.8 *de* [**Emm**]*).*

Ceci montre que les fonctions L de Dirichlet associées aux caractères non-principaux modulo m ont un nombre fini de zéros. Donc les fonctions L de Dirichlet associées aux caractères non-principaux modulo m se prolongent analytiquement sur tout le plan complexe à des fonctions entières.

En effectuant le changement de variable $u = q^{-s}$ on définit : $\mathcal{L}(u,\chi) := L(s,\chi)$.

La proposition suivante est essentiellement une conséquence du théorème de Weil [**Ros02**, Théorème 5.10].

Proposition 2.1.9 ([**Cha08**, Proposition 6.4])**.** *Soit $m \in \mathcal{M}_q$ de degré $M \geq 1$. Soit χ^* un caractère de Dirichlet primitif modulo un polynôme $m(\chi^*)$ qui induit un caractère de Dirichlet non principal χ modulo m. Soit $M(\chi^*)$ le degré de $m(\chi^*)$. Alors on a :*

$$\mathcal{L}(u,\chi) = \mathcal{L}(u,\chi^*) \prod_{\substack{P|m \\ P\nmid m(\chi^*)}} (1-\chi^*(P)u^{\deg(P)}). \tag{2.1.3}$$

Si χ^* est pair, alors :

$$\mathcal{L}(u,\chi^*) = (1-u) \prod_{i=1}^{M(\chi^*)-2} (1-\gamma_{\chi_i}u), \tag{2.1.4}$$

et, sinon,

$$\mathcal{L}(u,\chi^*) = \prod_{i=1}^{M(\chi^*)-1} (1-\gamma_{\chi_i}u), \tag{2.1.5}$$

pour certains nombres complexes γ_{χ_i} avec $|\gamma_{\chi_i}| = \sqrt{q}$.

Ces γ_{χ_i} sont appelés les zéros inverses de module $\sqrt{q}$ de la fonction de Dirichlet L associée au caractère χ.

Remarque 2.1.10. *On note qu'il découle de* (2.1.3) *que les zéros inverses de la fonction L de Dirichlet associée à un caractère χ modulo m sont les mêmes que les zéros inverses de la fonction L de Dirichlet associée au caractère χ^* modulo $m(\chi^*)$.*

2.2. Arithmétique sur $\mathbb{F}_q[T]$

Dans cette section, on établit des estimations sur quelques sommes des polynômes irréductibles unitaires dans les corps de fonctions et des sommes arithmétiques sur les caractères de Dirichlet dans les corps de fonctions.

On commence d'abord par rappeler quelques définitions élémentaires qui seront utilisées par la suite. Soit $d(m)$ le nombre de diviseurs unitaires de m. La lettre P sera utilisée pour définir les polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$.

2.2.1. Analogies entre corps de nombres et corps de fonctions

Dans cette première sous-section, on évoquera certaines analogies entre corps de nombres et corps de fonctions.

Il a été constaté que $\mathbb{Z}$ et $\mathbb{F}_q[T]$ ont plusieurs propriétés en commun. Par exemple, $\mathbb{Z}$ a une infinité de nombres premiers et $\mathbb{F}_q[T]$ possède une infinité de polynômes irréductibles unitaires. $\mathbb{Z}$ et $\mathbb{F}_q[T]$ sont tous les deux des anneaux principaux. Chacun de leurs groupes d'unités contient un nombre fini d'éléments. Ceci nous incite à penser que de nombreux résultats valables pour $\mathbb{Z}$ ont des analogues pour l'anneau des polynômes $\mathbb{F}_q[T]$.

Soit $N \in \mathbb{N}^*$, on définit

$$\pi_q(N) := \#\{P \in \mathcal{P}_q \quad | \quad \deg(P) = N\}. \tag{2.2.1}$$

C'est le nombre de polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$ de degré N. Le théorème des nombres premiers pour les polynômes donne l'estimation suivante sur $\pi_q(N)$ (cf. [**Ros02**, Théorème 2.2]) :

$$\pi_q(N) = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right). \tag{2.2.2}$$

Pour tout $(a,m) = 1$, on définit également :

$$\pi_q(a,m,N) := \#\{P \in \mathcal{P}_q \quad | \quad P \equiv a \bmod m, \quad \deg(P) = N\}. \tag{2.2.3}$$

Une conséquence du théorème de Weil ([**Ros02**, Théorème 5.10]) est la suivante :

$$\pi_q(a,m,N) = \frac{1}{\phi(m)}\frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

On note par S_N le nombre de polynômes unitaire de degré N dans $\mathbb{F}_q[T]$. Il est facile de vérifier que ce nombre est égal à q^N. Dans ce cas $\pi_q(a,m,N) = \frac{S_N}{\phi(m)\log_q(S_N)} + O\left(\frac{\sqrt{S_N}}{\log_q(S_N)}\right)$. Il s'agit de l'analogue du théorème des nombres premiers en progression arithmétique dans le cas des corps de fonctions. On peut voir cette analogie frappante entre corps de nombres et corps des fonctions dans le tableau suivant:

Corps des nombres	Corps des fonctions
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Les nombres premiers	Les polynômes irréductibles unitaires
Les entiers naturels	Les polynômes unitaires
$n = p_1^{e_1}...p_t^{e_t}$	$f = P_1^{e'_1}...P_t^{e'_t}$
Valeur absolue $\lvert n\rvert$	Norme d'un polynôme $\lvert f\rvert = q^{\deg(f)}$
$d(n) := \sum_{d\mid n} 1 = (e_1+1)...(e_t+1)$	$d(f) = (e'_1+1)...(e'_t+1)$
$\phi(n) = \#\left(Z/nZ\right)^\times$	$\phi(m) = \#\left(\mathbb{F}_q[T]/m\mathbb{F}_q[T]\right)^\times$
Il y a un nombre fini d'éléments inversibles sur $\mathbb{Z}$	Il y a un nombre fini d'éléments inversibles sur $\mathbb{F}_q[T]$
$\pi(x) \sim \frac{x}{\log(x)}$	$\pi_q(N) = \frac{S_N}{\log_q(S_N)} + O\left(\frac{\sqrt{S_N}}{\log_q(S_N)}\right)$
$\pi(x,q,a) \sim \frac{x}{\phi(q)\log(x)}$	$\pi_q(a,m,N) = \frac{S_N}{\phi(m)\log_q(S_N)} + O\left(\frac{\sqrt{S_N}}{\log_q(S_N)}\right)$

Tableau 2. Analogies entre les corps des nombres et les corps de fonctions

Plusieurs mathématiciens ont étudié cette analogie entre les corps des nombres et les corps de

fonctions. Nous citons à titre d'exemples principalement les thèses de Paul Pollack [**Pol08**], et de Sam Porritt [**Por20**] et le cours de Julio Andrade [**And15**].

2.2.2. Estimation de quelques sommes sur les polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$

On définit $\Lambda(m) = \log|P|$ si $m = P^t$ où $P \in \mathcal{P}_q$, et 0 sinon.

Lemme 2.2.1 (Théorème de Mertens dans les corps de fonctions)**.** *Soit χ un caractère de Dirichlet non-principal modulo m, et soit $N \in \mathbb{N}^*$. Alors*

$$\sum_{|f|\leq N} \frac{\Lambda(f)}{|f|} = \log N + O(1).$$

Démonstration. En combinant les faits que

$$\sum_{|f|\leq N} \frac{\Lambda(f)}{|f|} = \sum_{k=1}^{\lfloor \frac{\log N}{\log q} \rfloor} \frac{1}{q^k} \sum_{\deg(f)=k} \Lambda(f),$$

et

$$\begin{aligned}\sum_{\deg(f)=k} \Lambda(f) &= \sum_{\deg(P)=k} \log|P| + \sum_{\substack{\alpha|k \\ \alpha\neq 1}} \sum_{\deg(P)=k/\alpha} \log|P| \\ &= \sum_{\deg(P)=k} \log|P| + O(kq^{k/2}) \\ &= k(\log q)\pi_q(k) + O(kq^{k/2}) = (\log q)q^k + O(kq^{k/2}),\end{aligned}$$

on en déduit l'estimation voulue. □

Lemme 2.2.2. [**Sed22**, Lemme 3.4] *Soit $m \in \mathcal{M}_q$ de degré assez grand, alors*

$$\sum_{P|m} \frac{\log|P|}{|P|-1} \ll \log\log_q|m|, \tag{2.2.4}$$

et

$$\frac{|m|}{\phi(m)} \ll \log\log_q|m|. \tag{2.2.5}$$

Démonstration. Soit $M = \deg(m)$ et $\alpha \in \mathbb{R}_+^*$. On considère $A_\alpha = \sharp\left\{P|m \mid \deg(P) \geq \left[\frac{M}{\alpha}\right] + 1\right\}$. Il est clair que $A_\alpha \leq \alpha$. En particulier, si on prend $\alpha = \frac{M}{\log_q M}$, alors $A_{\frac{M}{\log_q M}} \leq \frac{M}{\log_q M}$. Par conséquent, on a

$$\begin{aligned}\sum_{P|m} \frac{\log|P|}{|P|-1} &= \sum_{\substack{P|m \\ \deg(P)\leq \log_q M}} \frac{\log|P|}{|P|-1} + \sum_{\substack{P|m \\ \deg(P)>\log_q M}} \frac{\log|P|}{|P|-1} \\ &\leq \sum_{\substack{P|m \\ \deg(P)\leq \log_q M}} \frac{\log|P|}{|P|-1} + \log q \frac{M}{\log_q M} \frac{\log_q M}{q^{\log_q M}-1}.\end{aligned}$$

Ainsi, à partir du Lemme 2.2.1, on déduit que

$$\sum_{P|m} \frac{\log |P|}{|P|-1} \ll \log \log_q |m|.$$

On établit maintenant l'estimation (2.2.5). D'après la Proposition 1.7 de [**Ros02**], on a

$$\frac{|m|}{\phi(m)} = \prod_{P|m} \left(1 - \frac{1}{|P|}\right)^{-1}.$$

L'estimation souhaitée découle donc du Théorème 3 de [**Ros99**]. □

Lemme 2.2.3 ([**Cha08**, Lemme 6.3])**.** *Soit χ un caractère non-principal de Dirichlet modulo m. Alors*

$$\frac{L'}{L}(1,\chi) = O\left(\log \log_q |m|\right). \tag{2.2.6}$$

2.2.3. Sommes arithmétiques sur les caractères de Dirichlet dans les corps de fonctions

Dans cette partie, nous allons établir quelques identités arithmétiques préliminaires qui seront nécessaires par la suite. La plupart de ces résultats sont obtenus en utilisant les mêmes arguments que [**Cha08**, Sous section 3.1] mais nous préférons donner les preuves par souci d'exhaustivité.

Lemme 2.2.4. [**Sed22**, Lemme 3.6] *Soit $m \in \mathcal{M}_q$ de degré ≥ 1. On a*

$$\sum_{f|m} \Lambda(m/f)\,\phi(f) = \phi(m) \sum_{P|m} \frac{\log |P|}{|P|-1}. \tag{2.2.7}$$

Si s est un diviseur propre de m, alors

$$\sum_{f|s} \Lambda(m/f)\,\phi(f) = \phi(m) \frac{\Lambda(m/s)}{\phi(m/s)}. \tag{2.2.8}$$

Démonstration. On remarque d'abord que la somme $\Lambda(m/f)\,\phi(f)$ sur $f|m$ est la même que la somme $\Lambda(m/f)\,\phi(f)$ sur les diviseurs f tel que m/f est une puissance d'un polynôme irréductible unitaire sur $\mathbb{F}_q[T]$.

On utilise la notation $P^r||m$ pour désigner que r est le plus grand entier naturel tel que $P^r|m$. Alors si $P^r||m$, on écrit $m = QP^r$ avec $Q \in \mathcal{M}_q$ tel que $P \nmid Q$. On obtient alors une contribution à la somme uniquement lorsque $f = QP^{r-k}$ pour un certain $1 \leq k \leq r$.

Puisque $(Q,P) = 1$ et $\sum_{k=1}^{r} \phi(P^{r-k}) = |P|^{r-1}$ on a :

$$\begin{aligned}\sum_{f|m} \Lambda(m/f)\,\phi(f) &= \sum_{P^r||m} \sum_{k=1}^{r} \Lambda\left(P^k\right) \phi(QP^{r-k}),\\ &= \sum_{P^r||m} \phi(Q) \log|P||P|^{r-1}.\end{aligned}$$

En utilisant le fait que $\phi(Q) = \phi(m)/\phi(P^r)$ (car $P \nmid Q$), on déduit

$$\sum_{f|m} \Lambda(m/f)\,\phi(f) = \sum_{P^r||m} \frac{\phi(m)}{\phi(P^r)} \log|P||P|^{r-1} = \phi(m) \sum_{P^r||m} \frac{\log|P|}{|P|-1} = \phi(m) \sum_{P|m} \frac{\log|P|}{|P|-1}.$$

Nous allons maintenant établir la seconde identité. Si m/s est divisible par au moins deux polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$, alors clairement la partie droite de (2.2.8) vaut 0, et la partie gauche de (2.2.8) vaut également 0 car $\Lambda(m/f) = 0$ pour tout diviseur f de s et donc tous les termes $\Lambda(m/f)$ sont égaux à 0. Ainsi, il suffit donc de considérer le cas où m/s est une puissance d'un premier. Dans ce cas, $m/s = P^t$ avec P un polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
On écrit $m = QP^r$ avec $P \nmid Q$, donc $s = QP^{r-t}$. Ainsi, les seuls termes qui contribuent à la somme sont ceux où $f = QP^{r-k}$ avec $t \le k \le r$. Donc, par un calcul similaire au précédent, on obtient

$$\sum_{f|s} \Lambda(m/f)\,\phi(f) = \sum_{k=t}^{r} \Lambda(P^k)\phi(Q.P^{r-k}) = \phi(Q) \log|P| \sum_{k=t}^{r} \phi(P^{r-k}).$$

En combinant les faits que $\phi(Q) = \frac{\phi(m)}{\phi(P^r)}$, $\sum_{k=t}^{r} \phi(P^{r-k}) = |P|^{r-t}$ et $m/s = P^t$ on en déduit :

$$\sum_{f|s} \Lambda(m/f)\,\phi(f) = \frac{\phi(m)}{\phi(P^r)} \log|P||P|^{r-t} = \phi(m) \frac{\log|P|}{|P|^{t-1}(|P|-1)} = \phi(m) \frac{\Lambda(m/s)}{\phi(m/s)}.$$

□

Proposition 2.2.5. [**Sed22**, Proposition 3.7] *Soit $m \in \mathcal{M}_q$ de degré ≥ 1. Alors*

$$\sum_{\chi \bmod m} \log|m(\chi^*)| = \phi(m) \left(\log|m| - \sum_{P|m} \frac{\log|P|}{|P|-1} \right),$$

et si $a \not\equiv 1 \mod m$ on a

$$\sum_{\chi \bmod m} \chi(a) \log|m(\chi^*)| = -\phi(m) \frac{\Lambda(m/(m,a-1))}{\phi(m/(m,a-1))}.$$

Démonstration. Pour prouver les deux résultats précédents, il suffit de prouver pour un résidu $a \bmod m$ que :

$$\sum_{\chi \bmod m} \chi(a) \log |m(\chi^*)| = \log |m| \sum_{\chi \bmod m} \chi(a) - \sum_{f|m} \Lambda(m/f) \sum_{\chi \bmod f} \chi(a). \tag{2.2.9}$$

En effet, si $a \equiv 1 \bmod m$, en utilisant l'identité (2.2.9) on obtient

$$\sum_{\chi \bmod m} \log |m(\chi^*)| = \phi(m) \log |m| - \sum_{f|m} \Lambda(m/f)\phi(f).$$

Ainsi la première partie de cette proposition découle de (2.2.7).
Par ailleurs, si $a \not\equiv 1 \bmod m$, par la relation d'orthogonalité (2.1.1) on trouve $\sum_{\chi \bmod m} \chi(a) = 0$. Ainsi on déduit de l'identité (2.2.9) que

$$\sum_{\chi \bmod m} \chi(a) \log |m(\chi^*)| = -\sum_{f|m} \Lambda(m/f) \sum_{\chi \bmod f} \chi(a) = -\sum_{f|m} \Lambda(m/f)\phi(f)\iota_f(a),$$

où $\iota_f(a) = 1$, si $a \equiv 1 \bmod f$, et vaut 0 sinon. Donc

$$\sum_{\chi \bmod m} \chi(a) \log |m(\chi^*)| = -\sum_{f|(m,a-1)} \Lambda(m/f)\phi(f).$$

Puisque $(m,a-1)$ est un diviseur propre de m (car $a \not\equiv 1 \mod m$) alors la deuxième partie de cette proposition découle de l'identité (2.2.8).

Maintenant, nous allons prouver l'identité (2.2.9). Soit χ un caractère de Dirichlet modulo m et $f|m$, on sait que χ est induit par un caractère χ^* modulo f si et seulement si f est un multiple de $m(\chi^*)$. Alors

$$\sum_{f|m} \Lambda(m/f) \sum_{\chi \bmod f} \chi(a) = \sum_{\chi \bmod m} \chi(a) \sum_{\substack{f|m \\ m(\chi^*)|f}} \Lambda(m/f).$$

En effectuant le changement de variable $c = m/f$, on a

$$\sum_{f|m} \Lambda(m/f) \sum_{\chi \bmod f} \chi(a) = \sum_{\chi \bmod m} \chi(a) \sum_{c|m/(m(\chi^*))} \Lambda(c).$$

De plus, comme

$$\sum_{c|m/(m(\chi^*))} \Lambda(c) = \log \left| \frac{m}{m\,(\chi^*)} \right|,$$

alors

$$\sum_{f|m} \Lambda(m/f) \sum_{\chi \bmod f} \chi(a) = \sum_{\chi \bmod m} \chi(a) \log \left| \frac{m}{m(\chi^*)} \right| = \log |m| \sum_{\chi \bmod m} \chi(a) - \sum_{\chi \bmod m} \chi(a) \log |m\,(\chi^*)|\,.$$

D'où le résultat (2.2.9). □

2.3. Travaux de B. Cha

En constatant l'analogie frappante entre les corps de nombres et les corps de fonctions, B. Cha a établi dans son article [**Cha08**] des résultats analogues à ceux de Rubinstein et Sarnak.

Avant de les énoncer, on fera un petit rappel de certaines notations utilisées par Cha. Soit $a \in \mathbb{F}_q[T]$ tel que $(a,m) = 1$. On définit pour tout $X \in \mathbb{N}^*$, $E_{m;a}(X)$ comme suit :

$$E_{m;a}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} \left(\phi(m)\pi_q(a,m,N) - \pi_q(N)\right).$$

Soit r un entier ≥ 2 et $a_1, \ldots, a_r \in \mathbb{F}_q[T]$ deux à deux distincts et premiers avec m. Cha a défini pour tout entier $X \geq 2$ le vecteur suivant :

$$E_{m,a_1,\ldots,a_r}(X) = \left(E_{m,a_1}(X), \ldots, E_{m,a_r}(X)\right).$$

La fonction $E_{m;a}(X)$ décrit combien il y a plus (ou moins) de nombres premiers dans la classe résiduelle de a par rapport à la valeur attendue.

En analysant les coefficients de la série associée à la dérivée logarithmique de toutes les fonctions L de Dirichlet modulo m, Cha a pu établir la formule explicite suivante de $E_{m;a}(X)$:

Théorème 2.3.1. [**Cha08**, Théorème 2.5]

$$E_{m,a}(X) = -C_m(a)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1), \tag{2.3.1}$$

quand $X \longrightarrow +\infty$ *avec :*

$$\mathcal{B}_q(X) := \begin{cases} \frac{\sqrt{q}}{q-1} & \text{si } X \text{ est impair,} \\ \frac{q}{q-1} & \text{si } X \text{ est pair,} \end{cases}$$

et

$$C_m(a) := -1 + \sum_{\substack{b^2 \equiv a \bmod m \\ b \in (\mathbb{F}_q[T]/(m))^\times}} 1.$$

On rappelle que les γ_χ *sont les zéros inverses de module* $\sqrt{q}$ *de la fonction L de Dirichlet associée au caractère* χ *(voir la proposition 2.1.9).*

Remarque 2.3.2. *(1) On remarque que pour* $(a,m) = 1$*, la fonction* $C_m(a)$ *prend deux valeurs :* $C_m(a) = -1$ *si* a *est un non-résidu quadratique modulo* m*, et* $C_m(a) = C_m(1)$ *si* a *est un résidu quadratique modulo* m*. De plus, on a* $|C_m(a)| < d(m)$*, or* $d(m) = |m|^{o(1)}$ *et donc* $C_m(a) = |m|^{o(1)}$*.*

(2) Le terme $-C_m(a)\mathcal{B}_q(X)$ de la formule (2.3.1) *est l'origine du biais de Chebyshev dans ce cas.*

La formule (2.3.1) dans le contexte des corps de fonctions est équivalente à la formule (2.5) de [**RS94**] dans le cas des corps de nombres. Cette formule explicite a permis à Cha de prouver de nombreux résultats identiques à ceux de l'article [**RS94**] en adaptant les arguments de Rubinstein et Sarnak.

En utilisant la formule (2.3.1), Cha a étudié la distribution limite de $E_{m;a_1,\ldots,a_r}$.

Afin de réaliser son étude, Cha a utilisé l'hypothèse suivante (qui est l'analogue de l'hypothèse LI utilisée dans [**RS94**]):

Définition 2.3.3 (Hypothèse d'indépendance Linéaire)**.** *Soit $m \in \mathcal{M}_q$ un polynôme de degré ≥ 2 et V un ensemble de caractères non principaux de Dirichlet modulo m invariant par action de conjugaison complexe. On dit que m satisfait (LI ★) sur V si le multi-ensemble*

$$\bigcup_{\chi\in V}\{\gamma\in[0,\pi]: L\left(\frac{1}{2}+i\gamma,\chi\right)=0\}\cup\{\pi\}$$

est linéairement indépendant sur $\mathbb{Q}$.

Remarque 2.3.4. *Si l'ensemble V (de la Définition 2.3.3) n'est pas précisé, on considère que V est l'ensemble des caractères non principaux modulo m.*

Soit r un entier ≥ 2 et $m \in \mathcal{M}_q$ un polynôme de degré ≥ 2. On rappelle que $\mathcal{A}_r(m)$ est l'ensemble des r-uplets de classes de résidus distinctes $(a_1,a_2,\ldots,a_r)$ modulo m qui sont premiers avec m.
Pour $(a_1,a_2,\ldots,a_r)\in\mathcal{A}_r(m)$, on définit :

$$P_{m;a_1,..,a_r}:=\left\{X\in\mathbb{N}^*:\ \sum_{N=1}^{X}\pi_q(a_1,m,N)>\sum_{N=1}^{X}\pi_q(a_2,m,N)>...>\sum_{N=1}^{X}\pi_q(a_r,m,N)\right\}.$$

Sous l'hypothèse (LI ★), Cha a prouvé l'existence d'une distribution limite $\mu_{m;a_1,\ldots,a_r}$ de la fonction $E_{m;a_1,\ldots,a_r}$. De plus, il résulte de (1.2.1) que

$$\begin{aligned}\delta_{m;a_1,..,a_r}&:=\lim_{X\longrightarrow+\infty}\frac{\#\left(P_{m;a_1,..,a_r}\cap\{1,2,..,X\}\right)}{X}\\&=\mu_{m;a_1,\ldots,a_r}\left\{(x_1,\ldots,x_r)\in\mathbb{R}^r: x_1>x_2>\cdots>x_r\right\}.\end{aligned}$$

Remarque 2.3.5. *On remarque que dans ce cas, on utilise la densité naturelle de l'ensemble $P_{m;a_1,\ldots,a_r}$ alors que les travaux de Rubinstein et Sarnak se sont basées sur l'étude de la densité logarithmique de l'ensemble $S_{q;a_1,\ldots,a_r}$ (voir* (1.2.1)*).*

En utilisant des méthodes similaires à celles de Rubinstein et Sarnak [**RS94**], Cha a également démontré le théorème suivant :

Théorème 2.3.6. [**Cha08**, Théorème 3.4] *Soit $m \in \mathcal{M}_q$ un polynôme de degré ≥ 2. Sous l'hypothèse (LI ★), on a pour tout $t = (t_1, \ldots, t_r) \in \mathbb{R}^r$:*

$$\hat{\mu}_{m;a_1,\ldots,a_r}(t) = \mathcal{B}_{m;a_1,\ldots,a_r}(t) \prod_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| \left|\sum_{j=1}^{r} \chi(a_j) t_j\right|\right), \tag{2.3.2}$$

où

$$J_0(z) = \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2},$$

est la fonction de Bessel d'ordre 0*, et*

$$\mathcal{B}_{m;a_1,\ldots,a_r}(t) = \frac{1}{2}\left[\exp\left(i\frac{\sqrt{q}}{q-1}\sum_{j=1}^{r} C_m(a_j)t_j\right) + \exp\left(i\frac{q}{q-1}\sum_{j=1}^{r} C_m(a_j)t_j\right)\right].$$

Grâce à ce résultat, Cha a aussi démontré ce qui suit :

Théorème 2.3.7. [**Cha08**, Théorème 6.5] *Soit $(m_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathcal{M}_q$ vérifiant (LI ★) tel que* $\deg(m_n) \longrightarrow +\infty$*. Pour r un entier fixé ≥ 2 on a*

$$\lim_{n\to+\infty} \Delta_r(m_n) = 0, \tag{2.3.3}$$

où $\Delta_r(m_n) := \max_{(a_1,\ldots,a_r)\in\mathcal{A}_r(m_n)} \left|\delta_{m_n;a_1,\ldots,a_r} - \frac{1}{r!}\right|$.

Ce théorème affirme que quand $\deg(m)$ tend vers $+\infty$, les biais se dissipent.

Cha s'est aussi intéressé aux courses entre les résidus quadratiques et les non-résidus quadratiques modulo m quand $m \in \mathcal{M}_q$ est un polynôme irréductible.
Soit $m \in \mathcal{M}_q$ un polynôme irréductible et χ_{quad} le caractère quadratique réel non principal modulo m défini ainsi :

$$\chi_{quad}(f) = \begin{cases} 1 & \text{si } f \text{ est un résidu quadratique non nul modulo } m. \\ -1 & \text{si } f \text{ est un non-résidu quadratique modulo } m. \\ 0 & \text{si } m \text{ divise } f. \end{cases}$$

On définit $P_{m;N,R}$ (N désigne les polynômes irréductibles unitaires qui sont des non-résidus quadratiques modulo m et R les polynômes irréductibles unitaires qui sont des résidus quadratiques modulo m) comme étant l'ensemble des entiers $X \in \mathbb{N}^*$ tel que

$$\sum_{N=1}^{X} a(N) > \sum_{N=1}^{X} b(N),$$

où

$$a(N) := \#\{P \in \mathcal{P}_q \quad | \quad \chi_{quad}(P) = -1, \quad \deg(P) = N\}$$

et

$$b(N) := \#\{P \in \mathcal{P}_q \quad | \quad \chi_{quad}(P) = 1, \quad \deg(P) = N\}.$$

On définit également pour tout $X \in \mathbb{N}^*$, la quantité :

$$E_{m;N,R}(X) := \frac{X}{q^{X/2}} \left(\sum_{N=1}^{X} a(N) - \sum_{N=1}^{X} b(N) \right).$$

Soit $m \in \mathcal{M}_q$ un polynôme irréductible de degré ≥ 2. Supposons que (LI ★) est vraie sur le caractère quadratique réel non principal χ_{quad} modulo m, Cha a prouvé que

$$\delta_{m;N,R} := \lim_{X \longrightarrow +\infty} \frac{\#\{P_{m;N,R} \cap \{1, \ldots, X\}\}}{X}$$

existe et $\delta_{m;N,R} > \frac{1}{2}$. Dans ce cas, le bias est en faveur des non-résidus quadratiques modulo m par rapport aux résidus quadratiques modulo m.
Cha a montré également que pour $\deg(m) = 2$, on a $E_{m;N,R}(X) > 0$ pour la plupart des entiers $X \in \mathbb{N}^*$ (tous les entiers non nuls sauf pour un nombre fini). Alors $\delta_{m;N,R} = 1$ et donc

$$\delta_{m;R,N} = 1 - \delta_{m;N,R} = 0.$$

Soit $(m'_n)_{n \in \mathbb{N}}$ une suite de polynômes irréductibles de $\mathcal{M}_q$ vérifiant (LI ★) sur $\{\chi_{quad}\}$ tel que $\deg(m'_n) \longrightarrow +\infty$. Cha a démontré que

$$\lim_{n \longrightarrow +\infty} \delta_{m'_n;N,R} = \frac{1}{2}.$$

En étudiant les diverses propriétés de la distribution limite $\mu_{m;a_1,\ldots,a_r}$, Cha a donné une condition nécessaire et suffisante pour que la mesure $\mu_{m;a_1,\ldots,a_r}$ reste inchangée sous des permutations de $(x_1, \ldots, x_r)$.

Théorème 2.3.8. [**Cha08**, Théorème 6.1] *Soit $m \in \mathcal{M}_q$ de degré ≥ 2. Supposons que (LI ★) est vérifiée. La distribution limite $\mu_{m;a_1,\ldots,a_r}$ est symétrique en $(x_1, \ldots, x_r)$ si et seulement si l'une des deux conditions suivantes est vérifiée :*

- *$r = 2$ et $C_m(a_1) = C_m(a_2)$.*
- *$r = 3$ et il existe $\rho \not\equiv 1 \bmod m$ qui satisfait les conditions suivantes :*

$$\rho^3 \equiv 1 \mod m, \ a_2 \equiv a_1\rho \mod m, \ a_3 \equiv a_1\rho^2 \mod m.$$

On utilisera la définition suivante dans tout ce qui suit :

Définition 2.3.9. *Soit $r \geq 2$ un entier et $m \in \mathcal{M}_q$ un polynôme de degré ≥ 2. Soit $(a_1, \ldots, a_r) \in \mathcal{A}_r(m)$. La course $\{m; a_1, \ldots, a_r\}$ est dite non biaisée si pour toute permutation σ de $\{1,2,\ldots,r\}$ on a*

$$\delta_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}} = \frac{1}{r!}.$$

Remarque 2.3.10. *Si $\mu_{m;a_1,\ldots,a_r}$ est symétrique en $(x_1, \ldots, x_r)$ alors la course $\{m; a_1, \ldots, a_r\}$ est non biaisée.*

Soit m un polynôme irréductible dans $\mathbb{F}_q[T]$ de degré > 2. Dans cette partie, l'hypothèse (LI ★) ne concerne que les arguments des zéros inverses de la fonction L associée au caractère non-principal quadratique modulo m. Cha s'est aussi demandé, quand (LI ★) n'est pas vérifiée, si le biais persiste en faveur des premiers congrus aux non-résidus quadratiques modulo m par rapport aux premiers congrus aux résidus quadratiques modulo m.
Il a prouvé que si (LI ★) est fausse, il se peut que le biais soit en faveur des résidus quadratiques modulo m, comme illustré dans l'exemple suivant :

Exemple 2.3.11. *Pour $p = 5$ et $m = T^5 + 3T^4 + 4T^3 + 2T + 2$, on a*

$$\begin{aligned}\mathcal{L}(u, \chi_{quad}) &= 25u^4 - 25u^3 + 15u^2 - 5u + 1 \\ &= \left(1 - 2\sqrt{5}\cos(\frac{2\pi}{5})u + 5u^2\right)\left(1 - 2\sqrt{5}\cos(\frac{4\pi}{5})u + 5u^2\right) \\ &= (1 - \gamma_1 u)\,(1 - \overline{\gamma_1} u)\,(1 - \gamma_2 u)\,(1 - \overline{\gamma_2} u)\,,\end{aligned}$$

où $\gamma_1 = \sqrt{5}e^{i\frac{2\pi}{5}}$ et $\gamma_2 = \sqrt{5}e^{i\frac{4\pi}{5}}$ sont les zéros inversés de $\mathcal{L}(u, \chi_{quad})$.
Or comme $\frac{4\pi}{5} - 2 \times \frac{2\pi}{5} = 0$ alors (LI ★) n'est pas vérifiée.
Cha a démontré que

$$\begin{aligned}\delta_{m;N,R} &= \lim_{X \longrightarrow +\infty} \frac{\#\{P_{m;N,R} \cap \{1, \ldots, X\}\}}{X} \\ &= \lim_{X \to +\infty} \frac{\#\{S \in [\![1, X]\!] : E_{m;N,R}(S) > 0\}}{X} \\ &= \frac{\#\{S \in [\![0, 9]\!] : E_{m;N,R}(S) > 0\}}{10} \\ &= \frac{2}{5} < \frac{1}{2}.\end{aligned}$$

et donc $\delta_{m;R,N} = 1 - \delta_{m;N,R} = \frac{3}{5} > \frac{1}{2}$. Ce qui explique que lorsque (LI ★) est fausse, on peut avoir une prédominance des résidus quadratiques par rapport aux non-résidus quadratiques modulo m.

Cependant, ce dernier exemple n'est pas suffisant pour affirmer que si (LI ★) est fausse alors le biais est en faveur des résidus quadratiques modulo m. En effet, l'exemple suivant montre que bien que (LI ★) soit fausse, on peut avoir un biais en faveur des non-résidus quadratiques modulo m.

Exemple 2.3.12. *On prend $p = 3$ et $m = T^3 + 2T + 1$. Alors on a*

$$\begin{aligned}\mathcal{L}(u, \chi_{quad}) &= 3u^2 - 3u + 1 \\ &= (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),\end{aligned}$$

avec $\gamma_1 = \sqrt{3}e^{i\frac{\pi}{6}}$.
Ainsi l'unique zéro inversé dont l'argument est compris entre 0 *et* π *est* γ_1.
Comme $\frac{\pi}{6} - \frac{1}{6} \times \pi = 0$, *alors (LI* $\bigstar$*) est fausse. Cha a démontré que*

$$\delta_{m;N,R} = \frac{7}{12} > \frac{1}{2}.$$

Dans ce cas, le biais est en faveur des non-résidus quadratiques modulo m.

Il est également possible de n'avoir aucun biais.

Exemple 2.3.13. *Pour* $p = 5$ *et* $m = T^4 + 4T^3 + 4T^2 + 4T + 1$, *on a*

$$\begin{aligned}\mathcal{L}(u, \chi_{quad}) &= -5u^3 + 5u^2 - u + 1 \\ &= (1 - \gamma_1 u)(1 - \overline{\gamma_1} u),\end{aligned}$$

avec $\gamma_1 = \sqrt{5}e^{i\frac{\pi}{2}}$. *Dans ce cas, Cha a prouvé que*

$$\delta_{m;N,R} = \frac{1}{2},$$

bien que (LI $\bigstar$*) soit fausse.*

Chapitre 3

Courses des polynômes irréductibles unitaires à r compétiteurs (où $r \geq 2$ est fixé)

3.1. Énoncé des résultats

Ce chapitre concerne principalement l'article Inequities in the Shanks-Renyi prime number race over function fields [**Sed22**]. Nous commençons d'abord par énoncer les différents résultats obtenus dans cet article.

Soit $\{\gamma_\chi\}$ l'ensemble des zéros inverses de $L(s,\chi)$ de module $\sqrt{q}$ et $S = \bigcup_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \gamma_\chi$. Nous définissons $\{U(\gamma_\chi)\}_{\gamma_\chi \in S}$ comme étant l'ensemble de variables aléatoires indépendantes uniformément réparties sur le cercle unité et nous rappelons que $C_m(a) = -1 + \sum_{\substack{b^2 \equiv a \bmod m \\ b \in (\mathbb{F}_q[T]/(m))^\times}} 1$.

Il découle des résultats de [**Cha08**] que sous l'hypothèse (LI ★), la distribution limite $\mu_{m;a_1,\ldots,a_r}$ est la mesure de probabilité qui correspond à un certain vecteur aléatoire $X_{m;a_1,\ldots,a_r} = (X(m,a_1),\ldots,X(m,a_r))$, avec

$$X_{m;a} = -C_m(a)X' + \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} 2\Re(\chi(a)U(\gamma_\chi)) \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|,$$

où X' est une variable aléatoire indépendante des $U(\gamma_\chi)$, et qui prend les valeurs $\frac{\sqrt{q}}{q-1}$ et $\frac{q}{q-1}$ avec une probabilité égale à $\frac{1}{2}$.

Soit $\mathrm{Cov}_{m;a_1,\ldots,a_r}$ la matrice de covariance de $X_{m;a_1,\ldots,a_r}$. En effectuant des calculs simples, nous montrons le lemme suivant :

Lemme 3.1.1. *Les coefficients de* $\mathrm{Cov}_{m;a_1,\ldots,a_r}$ *sont*

$$\mathrm{Cov}_{m;a_1,\ldots,a_r}(j,k) = \begin{cases} N_m + \frac{1}{4}\left(\frac{q}{q-1} - \frac{\sqrt{q}}{q-1}\right)^2 C_m(a_j)^2 & \text{si } j = k \\ B_m(a_j,a_k) + \frac{1}{4}\left(\frac{q}{q-1} - \frac{\sqrt{q}}{q-1}\right)^2 C_m(a_j)C_m(a_k) & \text{si } j \neq k, \end{cases}$$

où

$$N_m := 2 \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2, \tag{3.1.1}$$

et

$$B_m(a_j,a_k) := \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} (\chi(a_j/a_k) + \chi(a_k/a_j)) \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2. \tag{3.1.2}$$

Démonstration du lemme 3.1.1. Comme $\mathbb{E}(U(\gamma_\chi)) = 0$ pour tout γ_χ alors

$$\mathbb{E}(X_{m;a}) = -C_m(a)\mathbb{E}(X') = -\frac{1}{2}\left(\frac{\sqrt{q}}{q-1} + \frac{q}{q-1}\right) C_m(a).$$

Ainsi $\mathrm{Cov}_{m;a_1,\dots,a_r}(j,k)$ est égale à

$$\mathbb{E}\left(\left(X_{m;a_j} + \frac{1}{2}\left(\frac{\sqrt{q}}{q-1} + \frac{q}{q-1}\right) C_m(a_j)\right)\left(X_{m;a_k} + \frac{1}{2}\left(\frac{\sqrt{q}}{q-1} + \frac{q}{q-1}\right) C_m(a_k)\right)\right).$$

On définit

$$Y_{a_j,a_k} = \mathbb{E}\left(\sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} \sum_{\substack{\psi \bmod m \\ \psi \neq \chi_0}} \sum_{\Im(\widetilde{\gamma}_\psi)>0} \frac{\left(\chi(a_j)U(\gamma_\chi) + \overline{\chi(a_j)U(\gamma_\chi)}\right)\left(\psi(a_k)U(\widetilde{\gamma}_\psi) + \overline{\psi(a_k)U(\widetilde{\gamma}_\psi)}\right)|\gamma_\chi\widetilde{\gamma}_\psi|}{|(\gamma_\chi - 1)(\widetilde{\gamma}_\psi - 1)|} \right).$$

Puisque $\mathbb{E}(U(\gamma_\chi)U(\widetilde{\gamma}_\psi)) = 0$ pour tout $\gamma_\chi, \widetilde{\gamma}_\psi$ et

$$\mathbb{E}\left(U(\gamma_\chi)\overline{U(\widetilde{\gamma}_\psi)}\right) = \begin{cases} 1 & \text{si } \chi = \psi \text{ et } \gamma_\chi = \widetilde{\gamma}_\psi \\ 0 & \text{sinon,} \end{cases}$$

alors

$$\begin{aligned}\mathrm{Cov}_{m;a_1,\dots,a_r}(j,k) = {} & C_m(a_j)C_m(a_k)\mathbb{E}((X')^2) + Y_{a_j,a_k} - \left(\frac{\sqrt{q}}{q-1} + \frac{q}{q-1}\right) C_m(a_j)C_m(a_k)\mathbb{E}(X') \\ & + \frac{1}{4}\left(\frac{\sqrt{q}}{q-1} + \frac{q}{q-1}\right)^2 C_m(a_j)C_m(a_k).\end{aligned}$$

On en déduit que

$$\begin{aligned}\mathrm{Cov}_{m;a_1,\dots,a_r}(j,k) = {} & \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} (\chi(a_j/a_k) + \chi(a_k/a_j)) \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2 \\ & + \frac{1}{2}\left(\frac{q}{(q-1)^2} + \frac{q^2}{(q-1)^2}\right) C_m(a_j)C_m(a_k) - \frac{1}{4}\left(\frac{\sqrt{q}}{q-1} + \frac{q}{q-1}\right)^2 C_m(a_j)C_m(a_k),\end{aligned}$$

$$\mathrm{Cov}_{m;a_1,\dots,a_r}(j,k) = \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} (\chi(a_j/a_k) + \chi(a_k/a_j)) \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2 + \frac{1}{4}\left(\frac{q}{q-1} - \frac{\sqrt{q}}{q-1}\right)^2 C_m(a_j)C_m(a_k).$$

Ce qui prouve le Lemme 3.1.1. □

Nous démontrerons des formules asymptotiques de N_m et $B_m(a,b)$ pour tout $(a,b) \in \mathcal{A}_2(m)$ dans la section 3.2. Nous déduirons ainsi (voir le Lemme 3.2.3 et le Corollaire 3.2.10) les estimations suivantes :

$$N_m \sim \frac{q}{q-1}\phi(m)\log_q|m| \text{ et } B_m(a,b) \ll \phi(m). \tag{3.1.3}$$

Sous l'hypothèse (LI ★), dans le cas $r = 2$, nous allons établir la formule asymptotique suivante pour les densités $\delta_{m;a,b}$.

Théorème 3.1.2. *Soit $m \in \mathcal{M}_q$ de degré assez grand. Supposons que (LI ★) est vraie. Soit $(a,b) \in \mathcal{A}_2(m)$, alors*

$$\delta_{m;a,b} = \frac{1}{2} - \frac{(\sqrt{q}+q)}{2(q-1)}\frac{(C_m(a)-C_m(b))}{\sqrt{2\pi V_m(a,b)}} + O\left(\frac{C_m(1)^2\log_q|m|}{\phi(m)}\right), \tag{3.1.4}$$

où $V_m(a,b) = 2\,(N_m - B_m(a,b))$.

Ce résultat est l'analogue de [**FM13**, Théorème 1.1]. En combinant le Théorème 3.1.2 avec (3.1.3) et en utilisant le fait que $\phi(m) = |m|^{1+o(1)}$ nous déduisons :

$$\Delta_2(m) = \frac{1}{|m|^{1/2+o(1)}} \quad \text{(voir (0.0.1))}. \tag{3.1.5}$$

Nous énonçons maintenant un résultat concernant la densité $\delta_{m;a_1,\dots,a_r}$ quand $r \geq 3$.
On définit pour tout $(a_1,\dots,a_r) \in \mathcal{A}_r(m)$:

$$C_m := \max_{1\leq i\leq r}|C_m(a_i)| \text{ et } B_m := \max_{1\leq j<k\leq r}|B_m(a_j,a_k)|\,. \tag{3.1.6}$$

En plus, pour $1 \leq j \neq k \leq r$ on rappelle les intégrales suivantes qui apparaissent dans l'article de Lamzouri [voir [**Lam13**]].

$$\alpha_j(r) := (2\pi)^{-r/2}\int_{x_1>\cdots>x_r} x_j \exp\left(-\frac{x_1^2+\cdots+x_r^2}{2}\right)dx_1\dots dx_r,$$

$$\lambda_j(r) := (2\pi)^{-r/2}\int_{x_1>\cdots>x_r} (x_j^2-1)\exp\left(-\frac{x_1^2+\cdots+x_r^2}{2}\right)dx_1\dots dx_r,$$

et

$$\beta_{j,k}(r) := (2\pi)^{-r/2}\int_{x_1>\cdots>x_r} x_jx_k \exp\left(-\frac{x_1^2+\cdots+x_r^2}{2}\right)dx_1\dots dx_r.$$

Nous obtenons alors le théorème suivant :

Théorème 3.1.3. *Soit $r \geq 3$ un entier et $m \in \mathcal{M}_q$ de degré assez grand. Supposons que (LI ★) est vraie. Si $(a_1, \ldots, a_r) \in \mathcal{A}_r(m)$ alors*

$$\begin{aligned}\delta_{m;a_1,\ldots,a_r} = \frac{1}{r!} - \frac{(q+\sqrt{q})}{2\sqrt{N_m}(q-1)} \sum_{j=1}^{r} \alpha_j(r) C_m(a_j) + \frac{1}{N_m} \sum_{1\leq j<k\leq r} \beta_{j,k}(r) B_m(a_j,a_k) \\ + \frac{1}{4N_m} \frac{q+q^2}{(q-1)^2} \left(\sum_{j=1}^{r} \lambda_j(r) C_m(a_j)^2 + 2 \sum_{1\leq j<k\leq r} \beta_{j,k}(r) C_m(a_j) C_m(a_k) \right) \\ + O_r\left(\frac{1}{N_m} + \frac{C_m B_m}{N_m^{3/2}} + \frac{B_m^2}{N_m^2} \right).\end{aligned}$$

Remarque 3.1.4. *Nous pouvons comparer ce résultat avec* [**Lam13**, Théorème 2.1] *où une formule asymptotique similaire est prouvée pour les densités dans les courses à trois compétiteurs ou plus dans le cas des corps de nombres. La différence majeure est que dans le contexte des corps de fonctions, nous observons certains nouveaux facteurs qui dépendent de q. Ceci est dû au facteur $\mathcal{B}_{m;a_1,\ldots,a_r}(t)$ de la formule explicite de la transformée de Fourier de $\mu_{m;a_1,\ldots,a_r}(t)$ (voir l'équation* (2.3.2) *dans la section 2.3).*

Un corollaire direct du dernier théorème est le suivant :

Corollaire 3.1.5. *Sous les mêmes hypothèses que le Théorème 3.1.3, on a*

$$\begin{aligned}\delta_{m;a_1,\ldots,a_r} = \frac{1}{r!} - \frac{q+\sqrt{q}}{2\sqrt{N_m}(q-1)} \sum_{j=1}^{r} \alpha_j(r) C_m(a_j) + \frac{1}{N_m} \sum_{1\leq j<k\leq r} \beta_{j,k}(r) B_m(a_j,a_k) \\ + O_r\left(\frac{C_m^2}{N_m} + \frac{B_m^2}{N_m^2} \right).\end{aligned}$$

On rappelle le Lemme 4.5 de [**Lam13**] :

Lemme 3.1.6 ([**Lam13**, Lemme 4.5])**.** *On a $\beta_{1,2}(2) = 0$. En plus, on a*

$$\alpha_1(3) = \frac{1}{4\sqrt{\pi}}, \quad \alpha_2(3) = 0, \quad \alpha_3(3) = -\frac{1}{4\sqrt{\pi}},$$

et

$$\beta_{1,2}(3) = \beta_{2,3}(3) = \frac{1}{4\pi\sqrt{3}}, \quad \beta_{1,3}(3) = -\frac{1}{2\pi\sqrt{3}}.$$

Ainsi, en particulier pour $r = 3$, en combinant le lemme précèdent et le Corollaire 3.1.5 nous obtenons le corollaire suivant :

Corollaire 3.1.7. *Sous les mêmes hypothèses que le Théorème 3.1.3, on a*

$$\begin{aligned}\delta_{m;a_1,a_2,a_3} = \frac{1}{6} + \frac{q+\sqrt{q}}{8\sqrt{\pi N_m}(q-1)} \left(C_m(a_3) - C_m(a_1) \right) \\ + \frac{1}{4\pi\sqrt{3}N_m} \left(B_m(a_1,a_2) + B_m(a_2,a_3) - 2B_m(a_1,a_3) \right) + O\left(\frac{C_m^2}{N_m} + \frac{B_m^2}{N_m^2} \right).\end{aligned}$$

Il est facile de vérifier que

$$\sum_{j=1}^{r}\alpha_j(r)=\sum_{j=1}^{r}\lambda_j(r)=\sum_{1\leq j<k\leq r}\beta_{j,k}(r)=0.$$

En outre, pour tout $a\in\mathbb{F}_q[T]$ vérifiant $(a,m)=1$ on sait que $C_m(a)=|m|^{o(1)}$. Ainsi nous déduisons du Théorème 3.1.3, le corollaire suivant :

Corollaire 3.1.8. *Soit $r\geq 3$ un entier et $m\in\mathcal{M}_q$ de degré assez grand. Supposons (LI ★). Alors pour tout $(a_1,\dots,a_r)\in\mathcal{A}_r(m)$ tel que tous les a_i sont des résidus quadratiques modulo m ou tous sont des non-résidus quadratiques modulo m, on a*

$$\delta_{m;a_1,\dots,a_r}=\frac{1}{r!}+\frac{1}{N_m}\sum_{1\leq j<k\leq r}\beta_{j,k}(r)B_m(a_j,a_k)+O_r\left(\frac{1}{N_m}+\frac{C_mB_m}{N_m^{3/2}}+\frac{B_m^2}{N_m^2}\right).$$

Remarque 3.1.9. *Nous remarquons d'abord que la formule asymptotique pour les densités $\delta_{m;a_1,\dots,a_r}$ quand $r\geq 3$ est toujours valable dans le cas $r=2$, mais n'implique pas le Théorème 3.1.2 car le terme d'erreur peut dépasser le terme principal. Cela est dû au fait que $\beta_{1,2}(2)=0$, et donc le terme impliquant $B_m(a_1,a_2)$ manque dans le cas $r=2$ dans la formule asymptotique pour $\delta_{m;a_1,a_2}$. En revanche, lorsque $r\geq 3$, nous montrerons plus loin que la contribution des termes $B_m(a_i,a_j)$ aux densités $\delta_{m;a_1,\dots,a_r}$ peut être $\gg_{r,q}\frac{1}{\log|m|}$. C'est la principale différence entre les cas $r=2$ et $r\geq 3$ qui explique pourquoi $\Delta_r(m)$ pour $r\geq 3$ se comporte différemment de $\Delta_2(m)$.*

Le résultat suivant est l'analogue de [**Lam13**, Théorème 2.8] dans le cas des corps de fonctions. Il montre que, comme dans le cas des corps de nombres, des biais apparaissent dans les courses impliquant trois résidus quadratiques ou plus (ou non-résidus quadratiques) modulo m, une fois que $\deg(m)$ est suffisamment grand.

Théorème 3.1.10. *Soit $r\geq 3$ un entier et $m\in\mathcal{M}_q$ un polynôme de degré assez grand. Supposons (LI ★). Alors il existe des classes de résidus $(a_1,\dots,a_r),(b_1,\dots,b_r)\in\mathcal{A}_r(m)$ où $a_1,\dots,a_r$ sont tous des résidus quadratiques modulo m et $b_1,\dots,b_r$ sont tous des non-résidus quadratiques modulo m, et il existe une permutation σ de l'ensemble $\{1,\dots,r\}$ telle que*

$$\delta_{m;a_1,\dots,a_r}=\delta_{m;b_1,\dots,b_r}<\frac{1}{r!}-\frac{c_1(q,r)}{(\log|m|)^3}\quad\text{et}\quad\delta_{m;a_{\sigma(1)},a_{\sigma(2)},\dots,a_{\sigma(r)}}=\delta_{m;b_{\sigma(1)},b_{\sigma(2)},\dots,b_{\sigma(r)}}>\frac{1}{r!}+\frac{c_1(q,r)}{(\log|m|)^3},$$

pour une constante $c_1(q,r)>0$ qui ne dépend que de q et r.

Il est également intéressant de déterminer la vitesse de convergence de $\Delta_r(m)$ quand r est un entier supérieur ou égale à 3. Pour ce faire, nous démontrons le résultat suivant en utilisant le Théorème 3.1.3.

Théorème 3.1.11. *Soit $r \geq 3$ un entier et $m \in \mathcal{M}_q$ un polynôme de degré assez grand. Supposons (LI ★), alors pour tout $(a_1, \ldots, a_r) \in \mathcal{A}_r(m)$ on a*

$$\left|\delta_{m;a_1,\ldots,a_r} - \frac{1}{r!}\right| \ll_r \frac{1}{\log_q |m|}.$$

De plus, il existe des classes de résidus $(b_1, \ldots, b_r)$,$(d_1, \ldots, d_r) \in \mathcal{A}_r(m)$ telles que

$$\delta_{m;b_1,\ldots,b_r} > \frac{1}{r!} + \frac{c_2(r)}{\log_q |m|} \text{ et } \delta_{m;d_1,\ldots,d_r} < \frac{1}{r!} - \frac{c_2(r)}{\log_q |m|},$$

où $c_2(r) > 0$ est une constante qui dépend uniquement de r.

Ce résultat implique que pour $r \geq 3$ entier on a

$$\Delta_r(m) \asymp_r \frac{1}{\log_q |m|}. \tag{3.1.7}$$

Ce qui prouve que $\Delta_2(m)$ converge plus rapidement vers 0 par rapport à $\Delta_r(m)$ quand r est un entier fixé ≥ 3.

Ce théorème incite à déterminer les classes de résidus $a_1, \ldots, a_r$ modulo m pour lesquelles la distance $\left|\delta_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}} - \frac{1}{r!}\right|$ peut être $\gg_{r,q} \frac{1}{\log |m|}$ pour une certaine permutation σ de l'ensemble $\{1, \ldots, r\}$. Pour atteindre cet objectif, nous commencons par donner la définition suivante :

Définition 3.1.12. *On fixe un entier $r \geq 3$. Soit $a_1, \ldots, a_r$ des polynômes distincts dans $\mathbb{F}_q[T]$ et M_0 un grand entier. On considère l'ensemble Z_{M_0} de polynômes $m \in \mathcal{M}_q$ tels que $(m,a_i) = 1$ pour tout $1 \leq i \leq r$ et $\deg(m) \geq M_0$. On dit que la course $\{Z_{M_0}; a_1, \ldots, a_r\}$ est extrêmement biaisée s'il existe une constante $C(q,r,Z_{M_0}) > 0$ (qui dépend de q, r et Z_{M_0}) et une permutation σ de l'ensemble $\{1, \ldots, r\}$ telles que pour tout $m \in Z_{M_0}$ on a*

$$\left|\delta_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}} - \frac{1}{r!}\right| \geq \frac{C(q,r,Z_{M_0})}{\log |m|}.$$

Si le degré de $a_1, \ldots, a_r$ est borné, alors on peut donner un critère pour avoir un biais extrême.

Théorème 3.1.13. *On fixe un entier $r \geq 3$. Soit $A \geq 1$ et $a_1, \ldots, a_r$ des polynômes distincts dans $\mathbb{F}_q[T]$ tels que $\deg(a_i) \leq A$ pour tout $1 \leq i \leq r$. Soient M_0 un grand entier et Z_{M_0} l'ensemble des polynômes $m \in \mathcal{M}_q$ tels que $(m,a_i) = 1$ pour tout $1 \leq i \leq r$ et $\deg(m) \geq M_0$. Supposons (LI ★) pour tout $m \in Z_{M_0}$. Alors la course $\{Z_{M_0}; a_1, \ldots, a_r\}$ est extrêmement biaisée si et seulement si l'une des conditions suivantes est vérifiée :*

(1) Il existe $1 \leq j \neq k \leq r$ tel que $a_j + a_k = 0$.

(2) Il existe $1 \leq j \neq k \leq r$ tel que a_j/a_k est une puissance d'un premier (polynôme irréductible unitaire dans $\mathbb{F}_q[T]$).

De plus, si aucune des deux conditions (1), (2) *n'est vérifiée, alors pour toute permutation* σ *de l'ensemble* $\{1,\dots,r\}$ *on a*

$$\left|\delta_{m;a_{\sigma(1)},\dots,a_{\sigma(r)}} - \frac{1}{r!}\right| = \begin{cases} O_{A,r,q}\left(\frac{M^2}{|m|}\right) & \text{si tous les } a_i \text{ sont des résidus quadratiques} \\ & \text{(ou des non-résidus quadratiques) mod } m, \\ O_{\epsilon,r,q}\left(|m|^{-1/2+\epsilon}\right) & \text{sinon.} \end{cases}$$

Afin de comprendre le comportement de $\delta_{m;a_1,\dots,a_r}$, nous devons étudier les termes $B_m(a_i,a_j)$ pour $1 \leq i < j \leq r$ en détails. Le théorème suivant détermine l'ordre de grandeur de $|B_m(a,b)|$ pour une paire générique $(a,b) \in \mathcal{A}_2(m)$. Nous montrons qu'en moyenne $|B_m(a,b)| \asymp \log_q |m|$. Ceci généralise [**Lam13**, Théorème 2.9].

Théorème 3.1.14. *Soit* $r \geq 3$ *un entier et* $m \in \mathcal{M}_q$ *un polynôme de degré assez grand. Supposons (LI* $\bigstar$*). Alors*

$$\frac{q}{q-1}\log_q|m| + O\left(\log\log_q|m|\right) \leq \frac{1}{|\mathcal{A}_2(m)|}\sum_{(a,b)\in\mathcal{A}_2(m)}|B_m(a,b)| \leq \frac{17q}{q-1}\log_q|m| + O\left(\log\log_q|m|\right).$$

Soit n un entier naturel non nul. On définit $\mathcal{D}_r(n)$ comme étant l'ensemble des r-uplets ordonnés $(e_1,e_2,\dots,e_r)$ de classes de résidus distincts modulo n qui sont premiers avec n.

Feuerverger et Martin [**FM00**] ont conjecturé qu'il devrait exister un "facteur de biais" $F_n(e_1,\dots,e_r)$, défini comme une combinaison linéaire de $G_n(e_j) := -1 + \sum_{\substack{b^2\equiv e_j \bmod n \\ 1\leq b\leq n}} 1$ tel que

$$F_n(e_1,\dots,e_r) > F_n(j_1,\dots,j_r) \implies \tilde{\delta}(n;e_1,\dots,e_r) > \tilde{\delta}(n;j_1,\dots,j_r), \tag{3.1.8}$$

où $\tilde{\delta}(n;e_1,\dots,e_r)$ est la densité logarithmique de l'ensemble des réels $x \geq 2$ tels que

$$\pi(x;n,e_1) > \pi(x;n,e_2) > \cdots > \pi(x;n,e_r).$$

Lamzouri [**Lam13**, Théorème 2.11] a montré (en supposant HRG et LI pour les fonctions L de Dirichlet) que cette conjecture n'est pas vérifiée lorsque $r \geq 3$. Ce résultat incite à une généralisation dans le cas des corps de fonctions. Ce qui nous amène à prouver le théorème suivant :

Théorème 3.1.15. *Soit* $m \in \mathcal{M}_q$ *de degré assez grand. Supposons (LI* $\bigstar$*). On fixe un entier* $r \geq 3$ *et soit* $(\kappa_1,\kappa_2,\dots,\kappa_r) \in \mathbb{R}^r$ *tel que* $(\kappa_1,\dots,\kappa_r) \neq (0,\dots,0)$. *Alors il existe deux* r*-uplets* $(a_1,\dots,a_r),(b_1,\dots,b_r) \in \mathcal{A}_r(m)$ *tels que*

$$\sum_{1\leq j\leq r}\kappa_j C_m(a_j) > \sum_{1\leq j\leq r}\kappa_j C_m(b_j) \quad \text{et} \quad \delta_{m;a_1,\dots,a_r} < \delta_{m;b_1,\dots,b_r}.$$

Ceci montre que l'analogue de la conjecture de Feuerverger et Martin dans le cas des corps de fonctions est fausse. En outre, en combinant les Théorèmes 3.1.3 et 3.1.14, nous établissons un analogue du résultat obtenu dans [**Lam13**, Théorème 2.12].

Théorème 3.1.16. *On fixe un entier $r \geq 3$ et soit $m \in \mathcal{M}_q$ un polynôme de degré assez grand. Supposons (LI ★). Alors il existe un ensemble $\Omega_r(m) \subset \mathcal{A}_r(m)$ avec $|\Omega_r(m)| = o(|\mathcal{A}_r(m)|)$ tel que pour tous les r-uplets $(a_1,\dots,a_r)$,$(b_1,\dots,b_r) \in \mathcal{A}_r(m) \setminus \Omega_r(m)$ on a*

$$-\sum_{j=1}^{r} \alpha_j(r) C_m(a_j) > -\sum_{j=1}^{r} \alpha_j(r) C_m(b_j) \implies \delta_{m;a_1,\dots,a_r} > \delta_{m;b_1,\dots,b_r}.$$

Dans la section 3.2, nous établirons les deux formules asymptotiques pour N_m et $B_m(a,b)$. Nous étudierons par la suite l'ordre de grandeur de $B_m(a,b)$, démontrant le Théorème 3.1.14.

Dans la section 3.3, nous nous intéresserons aux propriétés de la mesure $\mu_{m;a_1,\dots,a_r}$ et en particulier de sa transformée de Fourier.

Dans les sections 3.4 et 3.5, nous démontrerons respectivement des formules asymptotiques pour les densités dans le cas $r = 2$ et $r \geq 3$. Nous montrerons également le Théorème 3.1.16 dans la section 3.5.

Dans la section 3.6, nous nous consacrerons à la construction des courses biaisées et à la démonstration des Théorèmes 3.1.10, 3.1.11 et 3.1.15.

Dans la section 3.7, nous déterminerons un critère pour les courses extrêmement biaisées qui nous permet d'établir le Théorème 3.1.13.

Enfin, dans la section 3.8, nous donnerons quelques exemples de courses où (LI ★) est fausse et les densités associées s'annulent.

3.2. Formules asymptotiques de N_m et $B_m(a,b)$

Le but de cette section est d'établir des formules asymptotiques pour N_m et $B_m(a,b)$ et d'en déduire les conséquences associées. Pour atteindre cet objectif, nous utilisons la définition suivante :

Définition 3.2.1. *Pour tout caractère non principal de Dirichlet $\chi \bmod m$, on définit*

$$I(\chi) := \frac{1}{2} \sum_{\gamma_\chi} \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2 .$$

Nous mentionnons que Cha a déjà établi dans la preuve de [**Cha08**, Théorème 6.5] la formule asymptotique suivante pour $I(\chi)$:

$$I(\chi) = \frac{q}{2(q-1)} M(\chi^*) + O\left(\log M(\chi^*)\right). \tag{3.2.1}$$

Il s'avère que cette dernière formule n'est pas suffisante pour atteindre l'objectif souhaité. C'est pour cette raison que nous établirons une formule exacte de $I(\chi)$ sans termes d'erreur. Nous adapterons ensuite les techniques utilisées dans [**Lam13**] dans le contexte des corps de fonctions. Ceci nous permet par la suite de démontrer des formules asymptotiques pour N_m et $B_m(a,b)$ et de les estimer de façon précise.

Proposition 3.2.2. *Soit $m \in \mathcal{M}_q$ de degré ≥ 2. Soit χ^* un caractère de Dirichlet primitif modulo un polynôme $m(\chi^*)$ qui induit un caractère de Dirichlet non principal χ modulo m. Soit $M(\chi^*)$ le degré de $m(\chi^*)$. Alors*

$$2I(\chi) := \sum_{\gamma_\chi} \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2 = \frac{q}{q-1} M(\chi^*) + \frac{2q}{q-1} \frac{1}{\log q} \Re\left(\frac{L'}{L}(1,\chi^*) \right) - \frac{q^2+q}{2(q-1)^2} \chi^*(-1) - \frac{3q^2-q}{2(q-1)^2}.$$

Démonstration. - On considère d'abord le cas où χ^* est impair.
On définit $G(u,\chi^*) = \mathcal{L}(u,\chi^*)\overline{\mathcal{L}(\overline{u},\chi^*)}$. Alors par (2.1.5), on a

$$G(u,\chi^*) = \prod_{i=1}^{M(\chi^*)-1} (1-\gamma_{\chi_i} u)(1-\overline{\gamma_{\chi_i}} u). \tag{3.2.2}$$

Ainsi

$$-\frac{G'}{G}(1,\chi^*) = \sum_{i=1}^{M(\chi^*)-1} \left(\frac{\gamma_{\chi_i}}{1-\gamma_{\chi_i}} + \frac{\overline{\gamma_{\chi_i}}}{1-\overline{\gamma_{\chi_i}}} \right) = \sum_{i=1}^{M(\chi^*)-1} \frac{\gamma_{\chi_i} + \overline{\gamma_{\chi_i}}}{|\gamma_{\chi_i}-1|^2} - 4I(\chi^*). \tag{3.2.3}$$

En plus, on a

$$M(\chi^*) - 1 + \sum_{i=1}^{M(\chi^*)-1} \frac{\gamma_{\chi_i} + \overline{\gamma_{\chi_i}}}{|\gamma_{\chi_i}-1|^2} = \sum_{i=1}^{M(\chi^*)-1} \frac{1+q}{|\gamma_{\chi_i}-1|^2} = \frac{2(1+q)}{q} I(\chi^*). \tag{3.2.4}$$

En combinant (3.2.3) et (3.2.4), il en résulte

$$I(\chi^*) = \frac{q}{2(q-1)} \left(\frac{G'}{G}(1,\chi^*) - (M(\chi^*)-1) \right). \tag{3.2.5}$$

En utilisant (3.2.2) et le fait que $\gamma_\chi \overline{\gamma_\chi} = q$ on obtient

$$\begin{aligned} G(1/qu,\chi^*) &= \prod_{i=1}^{M(\chi^*)-1} \left(1 - \frac{\gamma_{\chi_i}}{qu}\right)\left(1 - \frac{\overline{\gamma_{\chi_i}}}{qu}\right) \\ &= \prod_{i=1}^{M(\chi^*)-1} \left(1 - \frac{1}{\overline{\gamma_{\chi_i}} u}\right)\left(1 - \frac{1}{\gamma_{\chi_i} u}\right) \\ &= \prod_{i=1}^{M(\chi^*)-1} \frac{1}{qu^2} \left(\gamma_\chi u - 1\right)\left(\overline{\gamma_\chi} u - 1\right). \end{aligned}$$

Ainsi on déduit facilement l'équation fonctionnelle suivante :

$$G(u,\chi^*) = q^{(M(\chi^*)-1)} u^{2(M(\chi^*)-1)} G(1/qu,\chi^*).$$

Or on sait d'après (2.1.5) que $\log \mathcal{L}(u,\chi^*) = \sum_{i=1}^{M(\chi^*)-1} \log(1-\gamma_{\chi_i} u)$, d'où

$$\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*) = \sum_{i=1}^{M(\chi^*)-1} \frac{-\gamma_{\chi_i}}{1-\gamma_{\chi_i}/q}$$

et

$$\overline{\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*)} = \sum_{i=1}^{M(\chi^*)-1} \frac{-\overline{\gamma_{\chi_i}}}{1-\overline{\gamma_{\chi_i}}/q}.$$

Alors

$$\frac{G'}{G}(1/q,\chi^*) = \frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*) + \overline{\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*)}.$$

Donc

$$\frac{G'}{G}(1,\chi^*) = 2\left(M(\chi^*)-1\right) - \frac{1}{q}\frac{G'}{G}(1/q,\chi^*) = 2\left(M(\chi^*)-1\right) - \frac{1}{q}\left(\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*) + \overline{\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*)}\right). \tag{3.2.6}$$

De plus, en utilisant le fait que $u = q^{-s}$ on obtient

$$\frac{-1}{q}\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*) = \frac{1}{\log q}\frac{L'}{L}(1,\chi^*). \tag{3.2.7}$$

Ainsi, en combinant (3.2.5), (3.2.6) et (3.2.7) on déduit

$$I(\chi^*) = \frac{q}{q-1}\left(\frac{M(\chi^*)-1}{2}\right) + \frac{q}{2(q-1)}\frac{1}{\log q}\left(\frac{L'}{L}(1,\chi^*) + \overline{\frac{L'}{L}(1,\chi^*)}\right). \tag{3.2.8}$$

- On traite maintenant le cas où χ^* est pair.

On définit

$$H(u,\chi^*) = \prod_{i=1}^{M(\chi^*)-2}(1-\gamma_{\chi_i}u)(1-\overline{\gamma_{\chi_i}}u).$$

En utilisant des arguments similaires qui nous ont permis d'établir la formule (3.2.5), on trouve

$$I(\chi^*) = \frac{q}{2(q-1)}\left(\frac{H'}{H}(1,\chi^*) - \left(M(\chi^*)-2\right)\right). \tag{3.2.9}$$

Puisque $\gamma_{\chi_i}\overline{\gamma_{\chi_i}} = q$ pour tout $i \in [\![1, M(\chi^*)-2]\!]$, alors

$$\begin{aligned} H(1/qu,\chi^*) &= \prod_{i=1}^{M(\chi^*)-2}\left(1-\frac{\gamma_{\chi_i}}{qu}\right)\left(1-\frac{\overline{\gamma_{\chi_i}}}{qu}\right) \\ &= \frac{1}{q^{M(\chi^*)-2}u^{2(M(\chi^*)-2)}}\prod_{i=1}^{M(\chi^*)-2}\left(\gamma_\chi u - 1\right)\left(\overline{\gamma_\chi}u - 1\right). \end{aligned}$$

Ainsi on obtient l'équation fonctionnelle suivante :

$$H(u,\chi^*) = q^{(M(\chi^*)-2)}u^{2(M(\chi^*)-2)}H(1/qu,\chi^*).$$

D'où

$$\log H(u,\chi^*) = (M(\chi^*)-2)\log q + 2(M(\chi^*)-2)\log u + \log H(1/qu,\chi^*).$$

En dérivant cette dernière expression par rapport à la variable u, on obtient

$$\frac{H'}{H}(u,\chi^*) = 2(M(\chi^*)-2)\frac{1}{u} - \frac{1}{qu^2}\frac{H'}{H}(1/qu,\chi^*).$$

Donc, en particulier pour $u=1$, on a

$$\frac{H'}{H}(1,\chi^*) = 2\left(M(\chi^*)-2\right) - \frac{1}{q}\frac{H'}{H}(1/q,\chi^*).$$

En utilisant (2.1.4), on a $H(u,\chi^*)(1-u)^2 = \mathcal{L}(u,\chi^*)\overline{\mathcal{L}(\overline{u},\chi^*)}$, alors

$$\frac{H'}{H}(1/q,\chi^*) = \frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*) + \overline{\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*)} + \frac{2}{1-\frac{1}{q}}.$$

Ainsi

$$\frac{H'}{H}(1,\chi^*) = 2\left(M(\chi^*)-2\right) - \frac{1}{q}\left(\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*) + \overline{\frac{\mathcal{L}'}{\mathcal{L}}(1/q,\chi^*)}\right) - \frac{2}{q-1}. \tag{3.2.10}$$

Il découle de (3.2.9) et (3.2.10) que

$$I(\chi^*) = \frac{q}{q-1}\left(\frac{M(\chi^*)-2}{2}\right) + \frac{q}{2(q-1)}\frac{1}{\log q}\left(\frac{L'}{L}(1,\chi^*) + \overline{\frac{L'}{L}(1,\chi^*)}\right) - \frac{q}{(q-1)^2}. \tag{3.2.11}$$

En combinant (3.2.8) et (3.2.11) on obtient

$$I(\chi^*) = \frac{q}{q-1}\frac{M(\chi^*)-1}{2} + \frac{q}{q-1}\frac{1}{\log q}\Re\left(\frac{L'}{L}(1,\chi^*)\right) + \frac{1}{2}\left(\chi^*(-1)+1\right)\left(\frac{-q}{2(q-1)} - \frac{q}{(q-1)^2}\right).$$

Donc en utilisant la Remarque 2.1.10, on déduit la Proposition 3.2.2. □

La formule asymptotique de N_m découle de la proposition précédente comme nous pouvons constater dans la démonstration du lemme suivant :

Lemme 3.2.3. *Soit $m \in \mathcal{M}_q$ de degré $M \geq 2$. Supposons que (LI ★) est vraie, alors*

$$N_m = \frac{q}{q-1}\phi(m)M + O\left(\phi(m)\log M\right).$$

Démonstration. Pour $\chi \neq \chi_0$, comme $\chi^*(-1) = \chi(-1)$, il découle de la Proposition 3.2.2

$$2I(\chi) = \frac{q}{q-1}M\left(\chi^*\right) + \frac{2q}{q-1}\frac{1}{\log q}\Re\left(\frac{L'}{L}(1,\chi^*)\right) - \frac{q^2+q}{2(q-1)^2}\chi(-1) - \frac{3q^2-q}{2(q-1)^2}.$$

Puisque $N_m = 2\sum\limits_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum\limits_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2 = \sum\limits_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\left(I(\chi)+I(\overline{\chi})\right)$, alors on a

$$N_m = \frac{q}{q-1}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}} M\left(\chi^*\right) + \frac{2q}{q-1}\frac{1}{\log q}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\Re\left(\frac{L'}{L}(1,\chi^*)\right) - \frac{q^2+q}{2(q-1)^2}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\chi(-1)$$
$$- \frac{3q^2-q}{2(q-1)^2}\left(\phi(m)-1\right).$$

Or on sait que $\sum\limits_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \chi(-1) = \sum\limits_{\chi \bmod m} \chi(-1) - 1 = -1$ donc

$$N_m = \frac{q}{q-1} \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} M\left(\chi^*\right) + \frac{2q}{q-1}\frac{1}{\log q} \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \Re\left(\frac{L^{'}}{L}(1,\chi^*)\right) + \frac{q^2+q}{2(q-1)^2} - \frac{3q^2-q}{2(q-1)^2}\left(\phi(m)-1\right).$$

En utilisant le Lemme 2.2.3 et la Proposition 2.2.5, on déduit finalement la formule suivante :

$$N_m = \frac{q}{q-1}\phi(m)M + O\left(\phi(m)\log M\right).$$

□

Remarque 3.2.4. *Soit $m \in \mathcal{M}_q$ et χ_m le caractère quadratique primitif de Dirichlet modulo m. On désigne par mult(χ_m) la multiplicité de $\pm\sqrt{q}$ comme un zéro inverse de $\mathcal{L}(u,\chi_m)$. Wanlin Li a prouvé dans* [**Li18**] *l'existence d'une famille de polynômes $m \in \mathcal{M}_q$ vérifiant mult$(\chi_m) > 0$. C'est la raison pour laquelle on suppose que (LI ★) est vraie dans le lemme précédent.*

Avant de donner une formule asymptotique pour $B_m(a,b)$ (Proposition 3.2.8), nous commençons par établir quelques lemmes utiles.

Lemme 3.2.5 ([**Cha08**], p 1371)**.** *Soit $m \in \mathcal{M}_q$ un polynôme de degré $M \geq 2$ et χ un caractère non principal de Dirichlet modulo m. Pour tout $x \geq 1$, on a*

$$\frac{L'}{L}(1,\chi) = -\sum_{f \in \mathcal{M}_q} \frac{\chi(f)\Lambda(f)}{|f|}\exp\left(-q^{\deg(f)}/x\right) + O\left(\frac{M}{x^{1/4}}\right).$$

Lemme 3.2.6. *Soit $m \in \mathcal{M}_q$ un polynôme de degré $M \geq 2$, $P \in \mathcal{P}_q$, $e \in \mathbb{N}^*$, et $r \in \mathbb{F}_q[T]$ tel que $(r,m) = 1$.*
Si $P \nmid m$ alors

$$\sum_{\chi \bmod m} \chi(r)\left(\chi^*(P^e) - \chi(P^e)\right) = 0.$$

Si $P|m$ alors

$$\sum_{\chi \bmod m} \chi(r)\left(\chi^*(P^e) - \chi(P^e)\right) = \begin{cases} \phi(m/P^\nu) & \text{si } rP^e \equiv 1 \bmod m/P^\nu, \\ 0 & \text{sinon,} \end{cases}$$

où $\nu \geq 1$ est l'entier tel que $P^\nu || m$.

Démonstration. Si $P \nmid m$, pour tout caractère $\chi \bmod m$, on a $\chi^*(P^e) = \chi(P^e)$. Par conséquent, la première égalité est établie.
Sinon $P \mid m$ et alors $\chi(P^e) = 0$ pour tout caractère $\chi \bmod m$. Puisque $(r,m) = 1$, alors

$\chi(r) = \chi^*(r)$ pour tout $\chi \bmod m$. Par conséquent, on a

$$\sum_{\chi \bmod m} \chi(r) \left(\chi^*(P^e) - \chi(P^e)\right) = \sum_{\chi \bmod m} \chi(r)\chi^*(P^e) = \sum_{\chi \bmod m} \chi^*(rP^e).$$

On sait également que $\chi^*(P^e) = 0$ pour tout caractère $\chi \bmod m$ tel que $P|m(\chi^*)$. Ainsi

$$\sum_{\chi \bmod m} \chi^*(rP^e) = \sum_{\substack{\chi \bmod m \\ m(\chi^*)|m/P^\nu}} \chi^*(rP^e),$$

car $(P^e, m/P^\nu) = 1$.
En utilisant la relation d'orthogonalité (2.1.1), on établit le deuxième résultat. □

Lemme 3.2.7. *Soit $m \in \mathcal{M}_q$ de degré assez grand M et $x \geq |m|$ un réel. Alors*

$$\sum_{\substack{f \in \mathcal{M}_q \\ \deg(f) \geq 1 \\ (f,m)=1}} \frac{\Lambda(f)}{|f|} \exp\left(-|f|/x\right) = \log(x) + O\left(\log(\log x)\right).$$

Démonstration. Par (2.2.4), on obtient

$$\sum_{\substack{f \in \mathcal{M}_q \\ \deg(f) \geq 1 \\ (f,m)>1}} \frac{\Lambda(f)}{|f|} \exp\left(-|f|/x\right) \leq \sum_{P|m} \sum_{k=1}^{\infty} \frac{\log|P|}{|P|^k} = \sum_{P|m} \frac{\log|P|}{|P|-1} \ll \log M \ll \log\log x.$$

Ainsi il suffit d'évaluer $\sum_{\substack{f \in \mathcal{M}_q \\ \deg(f) \geq 1}} \frac{\Lambda(f)}{|f|} \exp\left(-|f|/x\right)$.
On divise la somme ci-dessus en trois parties : $|f| > x\log^2 x$, $x\log\log x < |f| \leq x\log^2 x$, et $|f| \leq x\log\log x$. Puisque $\exp\left(-|f|/x\right) \leq \frac{1}{|f|^2}$ pour $|f| > x\log^2 x$ alors la contribution de la première partie est

$$\sum_{|f| > x\log^2 x} \frac{\Lambda(f)}{|f|} \exp\left(-|f|/x\right) \leq \sum_{|f| > x\log^2 x} \frac{1}{|f|^2} \ll \frac{1}{x}.$$

En utilisant le Lemme 2.2.1, il s'ensuit que la contribution de la deuxième partie est

$$\sum_{x\log\log x < |f| \leq x\log^2 x} \frac{\Lambda(f)}{|f|} \exp\left(-|f|/x\right) \leq \frac{1}{\log x} \sum_{|f| \leq x\log^2 x} \frac{\Lambda(f)}{|f|} \ll 1.$$

Enfin en combinant le fait que $e^{-t} = 1 + O(t)$ pour tout $t > 0$, avec (2.2.2) et le Lemme 2.2.1 on en déduit que la contribution de la dernière partie vaut

$$\sum_{|f| \leq x\log\log x} \frac{\Lambda(f)}{|f|} \exp\left(-|f|/x\right) = \sum_{|f| \leq x\log\log x} \frac{\Lambda(f)}{|f|} + O\left(\frac{1}{x} \sum_{|f| \leq x\log\log x} \Lambda(f)\right) = \log x + O\left(\log\log x\right).$$

□

La proposition suivante sera très utile dans les démonstrations ultérieures.

Proposition 3.2.8. *Soit $m \in \mathcal{M}_q$ de degré assez grand M et $(a,b) \in \mathcal{A}_2(m)$, et soit $x = (\phi(m)M)^4$. Supposons (LI ★), alors*

$$B_m(a,b) = \frac{8q}{(q-1)\log q}\log\phi(m) - \frac{q}{q-1}\frac{\phi(m)}{\log q}\frac{\Lambda(m/(m,a-b))}{\phi(m/(m,a-b))} - \frac{q^2+q}{2(q-1)^2}\phi(m)l_m(a,b)$$
$$+ \frac{q}{(q-1)\log q}\left(-\phi(m)\sum_{\substack{1\le|f|\le 2x\log x\\ af\equiv b \bmod m}}\Lambda(f)\frac{\exp(-|f|/x)}{|f|} - \phi(m)\sum_{\substack{1\le|f|\le 2x\log x\\ bf\equiv a \bmod m}}\Lambda(f)\frac{\exp(-|f|/x)}{|f|}\right.$$
$$-\phi(m)\sum_{P^v||m}\sum_{n=1}^{\infty}\sum_{\substack{1\le e\le 2\log x\\ \deg(P^e)=n\\ aP^e\equiv b \bmod m/P^v}}\frac{\log|P|}{|P|^{e+v-1}(|P|-1)}$$
$$\left.-\phi(m)\sum_{P^v||m}\sum_{n=1}^{\infty}\sum_{\substack{1\le e\le 2\log x\\ \deg(P^e)=n\\ bP^e\equiv a \bmod m/P^v}}\frac{\log|P|}{|P|^{e+v-1}(|P|-1)}\right) + O(\log M),$$

où $l_m(a,b) = 1$, si $a+b \equiv 0 \bmod m$, et vaut 0, sinon.

Démonstration. Puisque (LI ★) est vraie, alors $B_m(a,b) = 2\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\Re(\chi(a/b))I(\chi^*)$.

Donc à partir des Propositions 2.2.5 et 3.2.2 on a

$$B_m(a,b) = -\frac{q}{q-1}\frac{\phi(m)}{\log q}\frac{\Lambda(m/(m,a-b))}{\phi(m/(m,a-b))} - \frac{q^2+q}{2(q-1)^2}\phi(m)l_m(a,b)$$
$$+\frac{q}{(q-1)\log q}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}(\chi(a/b)+\chi(b/a))\,\Re\left(\frac{L'}{L}(1,\chi^*)\right) + \frac{3q^2-q}{2(q-1)^2} + \frac{q^2+q}{2(q-1)^2}.$$

Afin d'obtenir notre résultat, il suffit d'évaluer $\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}(\chi(a/b)+\chi(b/a))\,\frac{L'}{L}(1,\chi^*)$.

En utilisant le Lemme 3.2.5 on trouve

$$\frac{L'}{L}(1,\chi^*) = -\sum_{f\in\mathcal{M}_q}\frac{\chi^*(f)\Lambda(f)}{|f|}\exp\left(-q^{\deg(f)}/x\right) + O\left(\frac{1}{\phi(m)}\right).$$

Ainsi $\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}(\chi(a/b)+\chi(b/a))\,\Re\left(\frac{L'}{L}(1,\chi^*)\right)$ vaut

$$-\Re\left(\sum_{f\in\mathcal{M}_q}\frac{\Lambda(f)}{|f|}\exp\left(-q^{\deg(f)}/x\right)\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}(\chi(a/b)\chi^*(f)+\chi(b/a)\chi^*(f))\right) + O(1).$$

D'après le Lemme 3.2.6, on a

$$\sum_{\chi \bmod m} \chi(a/b)\chi^*(P^e) = \begin{cases} \phi(m) & \text{si } P \nmid m \text{ et } aP^e \equiv b \bmod m, \\ \phi(m/P^v) & \text{si } P^v || m \text{ et } aP^e \equiv b \bmod m/P^v, \\ 0 & \text{sinon.} \end{cases}$$

En outre, il est clair que $aP^e \equiv b \bmod m$ implique que $P \nmid m$, et en utilisant le Lemme 3.2.7 il s'ensuit que $\sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} (\chi(a/b) + \chi(b/a))\, \Re\left(\frac{L'}{L}(1,\chi^*)\right)$ vaut

$$8\log\phi(m) - \phi(m)\sum_{n=1}^{\infty} \sum_{\substack{\deg(f)=n \\ af \equiv b \bmod m}} \Lambda(f)\frac{\exp\left(-|f|/x\right)}{|f|}$$

$$-\phi(m)\sum_{n=1}^{\infty} \sum_{\substack{\deg(f)=n \\ bf \equiv a \bmod m}} \Lambda(f)\frac{\exp\left(-|f|/x\right)}{|f|} - \sum_{P^v || m} \phi\left(\frac{m}{P^v}\right) \sum_{n=1}^{\infty} \sum_{\substack{e \geq 1 \\ \deg(P^e)=n \\ aP^e \equiv b \bmod m/P^v}} \frac{\log|P|}{|P|^e} \exp\left(-|P|^e/x\right)$$

$$- \sum_{P^v || m} \phi\left(\frac{m}{P^v}\right) \sum_{n=1}^{\infty} \sum_{\substack{e \geq 1 \\ \deg(P^e)=n \\ bP^e \equiv a \bmod m/P^v}} \frac{\log|P|}{|P|^e} \exp\left(-|P|^e/x\right) + O\left(\log M\right).$$

Comme $|f| \geq 2x\log x$ on a $\exp\left(-|f|/x\right) \leq \frac{1}{|f|}$, alors on obtient

$$\sum_{\substack{|f|>2x\log x \\ bf \equiv a \bmod m}} \Lambda(f)\frac{\exp\left(-|f|/x\right)}{|f|} + \sum_{P^v || m} \sum_{n=1}^{\infty} \sum_{\substack{e > 2\log x \\ \deg(P^e)=n \\ aP^e \equiv b \bmod m/P^v}} \frac{\log|P|}{|P|^e} \exp\left(-|P|^e/x\right) \ll \sum_{|f|>2x\log x} \frac{\Lambda(f)}{|f|^2} \ll \frac{1}{|m|^2}.$$

On remarque que $\phi(m/P^v) = \phi(m)/\left(|P|^{v-1}(|P|-1)\right)$ (car $(P^v, m/P^v) = 1$) et $1 - \exp\left(-t\right) \leq 2t$ pour tout $t > 0$. Ainsi, on a

$$\sum_{P^v || m} \phi\left(\frac{m}{P^v}\right) \sum_{n=1}^{\infty} \sum_{\substack{1 \leq e \leq 2\log x \\ aP^e \equiv b \bmod m/P^v \\ \deg(P^e)=n}} \frac{\log|P|}{|P|^e}\left(1 - \exp\left(-|P|^e/x\right)\right) \ll \frac{\phi(m)}{x} \sum_{P^v || m} \sum_{n=1}^{\infty} \sum_{\substack{1 \leq e \leq 2\log x \\ \deg(P^e)=n \\ aP^e \equiv b \bmod m/P^v}} \frac{\log|P|}{|P|-1}$$

$$\ll \phi(m)\frac{\log x}{x} \sum_{P|m} \frac{\log|P|}{|P|-1} \ll \frac{\log M}{(\phi(m)M)^2}.$$

En combinant les estimations ci-dessus, on déduit la Proposition 3.2.8. □

Remarque 3.2.9. *Si* $|B_m(a,b)| > \frac{9q}{(q-1)\log q}\log\phi(m)$ *alors* $B_m(a,b) < 0$.

Une conséquence directe de la Proposition 3.2.8 est le corollaire suivant :

Corollaire 3.2.10. *Supposons que (LI ★) est vraie, alors pour tout* $(a,b) \in \mathcal{A}_2(m)$ *on a* $|B_m(a,b)| \ll \phi(m)$.

Remarque 3.2.11. *On a* $\max_{(a,b)\in\mathcal{A}_2(m)} |B_m(a,b)| \asymp \phi(m)$. *En effet, soit* $(a,-a) \in \mathcal{A}_2(m)$, *d'après la Proposition 3.2.8, on a* $B_m(a,-a) \gg \phi(m)$. *Ainsi en combinant cette estimation avec le Corollaire 3.2.10 on déduit que* $\max_{(a,b)\in\mathcal{A}_2(m)} |B_m(a,b)| \asymp \phi(m)$.

Pour déduire le Corollaire 3.2.10, nous avons besoin du lemme suivant :

Lemme 3.2.12. *Soit* $m \in \mathcal{M}_q$ *un polynôme de degré assez grand* M, $(a,b) \in \mathcal{A}_2(m)$, *et notons* s *le résidu de* ab^{-1} *mod* m *ayant le plus petit degré. De plus, posons* $x = (\phi(m)M)^4$. *Alors*

$$\sum_{\substack{1\le|f|\le 2x\log x\\ bf\equiv a \bmod m}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right) = \frac{\Lambda(s)}{|s|} + O_q\left(\frac{M^2}{q^M}\right).$$

Démonstration. On sait que

$$\sum_{\substack{1\le|f|\le 2x\log x\\ f\equiv s \bmod m}} \Lambda(f)\frac{\exp\left(-|f|/x\right)}{|f|} = \frac{\Lambda(s)}{|s|}\exp\left(-|s|/x\right) + \sum_{\substack{1\le|f|\le 2x\log x\\ f\equiv s \bmod m\\ f\neq s}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right).$$

En outre, si $f \neq s$ avec $f \equiv s \bmod m$, alors $f = s + rm$ avec $\deg(r) \geq 0$. Donc

$$\sum_{\substack{1\le|f|\le 2x\log x\\ f\equiv s \bmod m\\ f\neq s}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right) \ll_q \frac{M}{q^M}\left(\sum_{0\le\deg(r)\le 24M}\frac{1}{|r|}\right) \ll_q \frac{M^2}{q^M}.$$

En utilisant le fait que $e^{-t} = 1 + O(t)$ pour tout $t > 0$, on obtient

$$\frac{\Lambda(s)}{|s|}\exp\left(-|s|/x\right) = \frac{\Lambda(s)}{|s|} + O_q\left(\frac{1}{\phi(m)^4M^3}\right).$$

Puisque on a $\frac{|m|}{\phi(m)} \ll M$ (de (2.2.5)), le Lemme 3.2.12 découle de la combinaison des estimations ci-dessus. □

Démonstration du Corollaire 3.2.10. On désigne par s le résidu de ab^{-1} mod m de plus petit degré. Tout d'abord, on remarque que $\frac{\Lambda(s)}{|s|} \leq \frac{\log q}{q}$ pour $\deg(s) \geq 1$. De plus, on a que $\Lambda(m/(m,a-b))/\phi(m/(m,a-b)) \neq 0$ si et seulement si $m/(m,a-b) = P^l$ avec $P \in \mathcal{P}_q$, et $l \in \mathbb{N}^*$. Dans ce cas, on a

$$\frac{\Lambda(m/(m,a-b))}{\phi(m/(m,a-b)} = \frac{\log|P|}{|P|^{l-1}\left(|P|-1\right)} \leq \frac{\log|P|}{|P|-1} \leq \log 2.$$

En outre, on sait que

$$\sum_{P^\nu||m}\sum_{n=1}^{\infty}\sum_{\substack{1\le e\le 2\log x\\ b.P^e\equiv a \bmod m/P^v\\ \deg(P^e)=n}} \frac{\log|P|}{|P|^{e+\nu-1}\left(|P|-1\right)} \leq \sum_{P|m}\frac{\log|P|}{\left(|P|-1\right)^2} \ll 1.$$

Donc en combinant ces différentes estimations avec la Proposition 3.2.8 et le Lemme 3.2.12, le Corollaire 3.2.10 s'ensuit. □

Une autre conséquence de la Proposition 3.2.8 est le Théorème 3.1.14 qui stipule qu'il existe une borne inférieure et une borne supérieure pour le premier moment de $|B_m(a,b)|$ sur des paires de classes de résidus $(a,b) \in \mathcal{A}_2(m)$ ayant le même ordre de grandeur.

Démonstration du Théorème 3.1.14. On montre d'abord l'inégalité suivante :

$$\frac{q}{q-1}\log_q|m| + O\left(\log\log_q|m|\right) \leq \frac{1}{|\mathcal{A}_2(m)|}\sum_{(a,b)\in\mathcal{A}_2(m)}|B_m(a,b)|.$$

Par définition de $B_m(a,b)$, on a

$$\sum_{(a,b)\in\mathcal{A}_2(m)} B_m(a,b) = \sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\sum_{\substack{a \bmod m\\ (a,m)=1}}\sum_{\substack{b\neq a \bmod m\\ (b,m)=1}} (\chi(a/b)+\chi(b/a))\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2.$$

En utilisant les relations d'orthogonalité pour les caractères de Dirichlet modulo m, il est facile de vérifier que

$$\sum_{\substack{a \bmod m\\ (a,m)=1}}\sum_{\substack{b\neq a \bmod m\\ (b,m)=1}} (\chi(a/b)+\chi(b/a)) = -2\phi(m).$$

Ainsi $\sum_{(a,b)\in\mathcal{A}_2(m)} B_m(a,b) = -\phi(m)N_m$, et puisque $|\mathcal{A}_2(m)| = \phi(m)^2-\phi(m) \leq \phi(m)^2$, on a

$$\frac{1}{|\mathcal{A}_2(m)|}\sum_{(a,b)\in\mathcal{A}_2(m)}|B_m(a,b)| \geq -\frac{1}{|\mathcal{A}_2(m)|}\sum_{(a,b)\in\mathcal{A}_2(m)} B_m(a,b) = \frac{N_m}{\phi(m)-1}.$$

De plus, on sait que $N_m = \phi(m)\left(\frac{q}{q-1}M + O(\log M)\right)$, donc

$$\frac{1}{|\mathcal{A}_2(m)|}\sum_{(a,b)\in\mathcal{A}_2(m)}|B_m(a,b)| \geq \frac{q}{q-1}M + O(\log M).$$

Ensuite, il reste à établir la borne supérieure pour le premier moment de $|B_m(a,b)|$ sur des paires de classes de résidus $(a,b) \in \mathcal{A}_2(m)$.
Soit $(a,b) \in \mathcal{A}_2(m)$ et $d = (m,a-b)$. Alors $a-b = ds$ avec $0 \leq \deg(s) \leq \deg(m/d)$ et $(s,m/d) = 1$. Donc, pour tout choix de d et s satisfaisant ces conditions, il y a au plus $\phi(m)$ paires $(a,b) \in \mathcal{A}_2(m)$ telles que $a-b = ds$. On a donc

$$\begin{aligned}\sum_{(a,b)\in\mathcal{A}_2(m)}\frac{\Lambda\left(m/(m,a-b)\right)}{\phi\left(m/(m,a-b)\right)} &\leq \phi(m)\sum_{d|m}\frac{\Lambda(m/d)}{\phi(m/d)}\left(\sum_{\substack{0\leq\deg(s)\leq\deg(m/d)\\ (m/d,s)=1}} 1\right)\\ &\leq \phi(m)\sum_{d|m}\Lambda(m/d) = (\log q)\phi(m)M.\end{aligned}$$

On choisit $x = (\phi(m)M)^4$, alors par le Lemme 3.2.7 il s'ensuit que

$$\begin{aligned}\sum_{(a,b)\in\mathcal{A}_2(m)} \sum_{\substack{1\le|f|\le 2x\log x\\ f\equiv ab^{-1} \bmod m}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right) &= \sum_{\substack{1\le|f|\le 2x\log x\\ (f,m)=1}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right)\left(\sum_{\substack{(a,b)\in\mathcal{A}_2(m)\\ ab^{-1}\equiv f \bmod m}} 1\right)\\ &\le \phi(m)\sum_{\substack{1\le|f|\le 2x\log x\\ (f,m)=1}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right)\\ &\le \phi(m)\sum_{\substack{f\in\mathcal{M}_q\\ \deg(f)\ge 1\\ (f,m)=1}} \frac{\Lambda(f)}{|f|}\exp\left(-|f|/x\right)\\ &\le 4(\log q)\phi(m)M + O\left(\phi(m)\log M\right).\end{aligned}$$

En outre, on obtient

$$\sum_{(a,b)\in\mathcal{A}_2(m)}\sum_{P^v\|m}\sum_{\substack{1\le e\le 2\log x\\ aP^e\equiv b \bmod m/P^v\\ \deg(P^e)=n}} \frac{\log|P|}{|P|^{e+v-1}\left(|P|-1\right)} \le \phi(m)\sum_{P|m}\frac{\log|P|}{(|P|-1)^2} \ll \phi(m).$$

Le Théorème 3.1.14 découle ainsi de la Proposition 3.2.8 combinée à ces différentes estimations. □

3.3. Propriétés de $\mu_{m;a_1,\dots,a_r}$

Le but de cette section est d'étudier les propriétés de $\mu_{m;a_1,\dots,a_r}$, notamment celle de sa transformée de Fourier $\hat{\mu}_{m;a_1,\dots,a_r}$. Nous rappellons d'abord la formule explicite de la transformée de Fourier $\hat{\mu}_{m;a_1,\dots,a_r}$ obtenue par Cha dans [**Cha08**, Théorème 3.4].
Soit $m \in \mathcal{M}_q$ un polynôme de degré ≥ 2. Sous l'hypothèse (LI ★), pour tout $t = (t_1,\dots,t_r) \in \mathbb{R}^r$, on a

$$\hat{\mu}_{m;a_1,\dots,a_r}(t) = \mathcal{B}_{m;a_1,\dots,a_r}(t)\prod_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi-1}\right|\left|\sum_{j=1}^r \chi(a_j)t_j\right|\right), \tag{3.3.1}$$

où

$$J_0(z) = \sum_{n=0}^{\infty}\frac{(-1)^n(z/2)^{2n}}{(n!)^2}$$

est la fonction de Bessel d'ordre 0, et

$$\mathcal{B}_{m;a_1,\dots,a_r}(t) = \frac{1}{2}\left[\exp\left(i\frac{\sqrt{q}}{q-1}\sum_{j=1}^r C_m(a_j)t_j\right) + \exp\left(i\frac{q}{q-1}\sum_{j=1}^r C_m(a_j)t_j\right)\right].$$

Dans un premier temps, nous donnons les définitions suivantes :

Définition 3.3.1. *Pour tout caractère non principal de Dirichlet χ modulo m, on définit*

$$F(x,\chi) := \prod_{\Im(\gamma_\chi)>0} J_0\left(2x\left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|\right),$$

pour tout $x \in \mathbb{R}$.

Définition 3.3.2. *Pour $a = (a_1, \dots, a_r) \in \mathcal{A}_r(m)$ et $t = (t_1, \dots, t_r) \in \mathbb{R}^r$, on définit $V_{m,a}(t)$ comme étant l'ensemble des caractères de Dirichlet non principaux modulo m tels que*

$$\left|\sum_{j=1}^{r} \chi(a_j) t_j\right| \geq \frac{\|t\|}{2}.$$

Ensuite, nous montrons le lemme suivant :

Lemme 3.3.3. *Soit χ un caractère non principal de Dirichlet modulo m. Pour tout $x > 2\sqrt{q}$, on a*

$$|F(x,\chi)F(x,\overline{\chi})| \leq \exp\left(-\frac{\log x}{2}(M(\chi^*) - 2)\right).$$

Démonstration. On sait de [**RS94**, Equation 4.5] que $|J_0(x)| \leq \min\left\{1, \sqrt{\frac{2}{\pi x}}\right\}$ pour tout $x > 2\sqrt{q}$. Ainsi pour $x > 2|\gamma_\chi|$ on a

$$|F(x,\chi)F(x,\overline{\chi})| \leq \prod_{\gamma_\chi} J_0\left(2x\left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|\right) \leq \prod_{\gamma_\chi} \left|\frac{\gamma_\chi - 1}{\gamma_\chi}\right|^{\frac{1}{2}} \frac{1}{\sqrt{\pi x}}.$$

En outre, puisque $q > 2$ on a $\left|\frac{\gamma_\chi - 1}{\gamma_\chi}\right| \leq 1 + \frac{1}{|\gamma_\chi|} < 2$. D'où

$$|F(x,\chi)F(x,\overline{\chi})| \leq \prod_{\gamma_\chi} \sqrt{\frac{2}{\pi x}} \leq \prod_{\gamma_\chi} \frac{1}{\sqrt{x}} \leq \exp\left(-\frac{\log x}{2}\#\{\gamma_\chi\}\right).$$

Il résulte donc de la Proposition 2.1.9 que

$$|F(x,\chi)F(x,\overline{\chi})| \leq \exp\left(-\frac{\log x}{2}(M(\chi^*) - 2)\right).$$

□

Nous sommes maintenant en mesure de donner une borne supérieure décroissante pour $\hat{\mu}_{m;a_1,\dots,a_r}(t)$ dans la proposition suivante :

Proposition 3.3.4. *Soit $r \geq 2$ un entier fixé, $m \in \mathcal{M}_q$ de degré assez grand M et soit $\epsilon \in]0, \frac{1}{4}[$. Supposons (LI ★). Soit $(a_1, \dots, a_r) \in \mathcal{A}_r(m)$.*
Pour $t = (t_1, \dots, t_r) \in \mathbb{R}^r$ avec $\epsilon \leq \|t\| \leq 4\sqrt{q}$ on a

$$|\hat{\mu}_{m;a_1,\dots,a_r}(t_1, \dots, t_r)| \leq \exp\left(-c_1(r)\epsilon^2\phi(m)M\right),$$

et pour $\|t\| > 4\sqrt{q}$, on a

$$|\hat{\mu}_{m;a_1,\dots,a_r}(t_1, \dots, t_r)| \leq \exp\left(-c_2(r)\phi(m)M\log\|t\|\right),$$

où $c_1(r)$ et $c_2(r)$ sont des constantes positives qui dépendent uniquement de r.

Avant de prouver ce résultat, nous allons utiliser les lemmes intermédiaires suivants :

Lemme 3.3.5. *Soit $m \in \mathcal{M}_q$ de degré assez grand et $2 \leq r \leq \frac{\phi(m)}{4}$ un entier. Soient $a = (a_1, \dots, a_r) \in \mathcal{A}_r(m)$ et $t = (t_1, \dots, t_r) \in \mathbb{R}^r$, on a*

$$\#V_{m,a}(t) \geq \frac{\phi(m)}{2r} \quad \textit{(voir la Définition 3.3.2).}$$

Remarque 3.3.6. *On remarque que $\chi \in V_{m,a}(t)$ si et seulement si $\overline{\chi} \in V_{m,a}(t)$.*

Démonstration du Lemme 3.3.5. Soit

$$\begin{aligned} S(t) &:= \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \left| \sum_{j=1}^{r} \chi(a_j) t_j \right|^2 = \sum_{\chi \bmod m} \left| \sum_{j=1}^{r} \chi(a_j) t_j \right|^2 - \left(\sum_{j=1}^{r} t_j \right)^2 \\ &= \sum_{j=1}^{r} \sum_{k=1}^{r} t_j t_k \sum_{\chi \bmod m} \chi(a_j) \overline{\chi}(a_k) - \left(\sum_{j=1}^{r} t_j \right)^2. \end{aligned}$$

À partir de l'inégalité de Cauchy-Schwarz, on obtient

$$S(t) = \phi(m) \sum_{j=1}^{r} t_j^2 - \left(\sum_{j=1}^{r} t_j \right)^2 \geq (\phi(m) - r) \sum_{j=1}^{r} t_j^2 = (\phi(m) - r) \|t\|^2. \tag{3.3.2}$$

De plus, puisque $\left| \sum_{j=1}^{r} \chi(a_j) t_j \right|^2 \leq r \|t\|^2$ alors

$$S(t) = \sum_{\chi \in V_{m,a}(t)} \left| \sum_{j=1}^{r} \chi(a_j) t_j \right|^2 + \sum_{\chi \notin V_{m,a}(t)} \left| \sum_{j=1}^{r} \chi(a_j) t_j \right|^2 \leq r \#V_{m,a}(t) \|t\|^2 + \frac{\phi(m)}{4} \|t\|^2. \tag{3.3.3}$$

Ainsi en combinant (3.3.2) et (3.3.3) on déduit, si $\deg(m) = M$ est assez grand, que

$$\#V_{m,a}(t) \geq \frac{\phi(m)}{2r}. \tag{3.3.4}$$

□

Lemme 3.3.7. *Soit $m \in \mathcal{M}_q$ de degré assez grand et $2 \leq r \leq \frac{\phi(m)}{4}$ un entier. Soient $a = (a_1, \dots, a_r) \in \mathcal{A}_r(m)$ et $t = (t_1, \dots, t_r) \in \mathbb{R}^r$, on a*

$$\sum_{\chi \in V_{m,a}(t)} M(\chi^*) \geq \frac{\phi(m) M}{4r}. \tag{3.3.5}$$

Démonstration du Lemme 3.3.7. En utilisant la Proposition 2.2.5 on a

$$\begin{aligned}\sum_{\chi\in V_{m,a}(t)} M(\chi^*) &= \sum_{\chi \bmod m} M(\chi^*) - \sum_{\chi\notin V_{m,a}(t)} M(\chi^*)\\ &= \phi(m)M - \frac{\phi(m)}{\log q}\sum_{P|m}\frac{\log|P|}{|P|-1} - \sum_{\chi\notin V_{m,a}(t)} M(\chi^*)\\ &\geq \#V_{m,a}(t)M - \frac{\phi(m)}{\log q}\sum_{P|m}\frac{\log|P|}{|P|-1}.\end{aligned} \tag{3.3.6}$$

D'où pour M assez grand, on déduit en combinant (2.2.4) avec le Lemme 3.3.5 et (3.3.6) que

$$\sum_{\chi\in V_{m,a}(t)} M(\chi^*) \geq \frac{\phi(m)M}{4r}.$$

□

Démonstration de la Proposition 3.3.4. Soit $\epsilon \leq \|t\| \leq 4\sqrt{q}$. Si $\chi \in V_{m,a}(t)$, alors $2\left|\sum_{j=1}^{r}\chi(a_j)t_j\right| \geq \|t\| \geq \epsilon$. De plus, on sait que $\epsilon\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right| \leq \epsilon\left(1+\frac{1}{\sqrt{q}-1}\right) \leq 1$, J_0 est une fonction positive décroissante sur [0,1] et $|J_0(x)| \leq J_0(1)$ pour $x \geq 1$. En utilisant la formule explicite (2.3.2), on obtient

$$\begin{aligned}|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| &\leq \prod_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\prod_{\Im(\gamma_\chi)>0}\left|J_0\left(2\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|\right)\right|\\ &\leq \prod_{\chi\in V_{m,a}(t)}\prod_{\Im(\gamma_\chi)>0}\left|J_0\left(2\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|\right)\right|\\ &\leq \prod_{\chi\in V_{m,a}(t)}\prod_{\Im(\gamma_\chi)>0}\left|J_0\left(\epsilon\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|\right)\right|.\end{aligned}$$

En outre, pour $|x| \leq 1$ on a $J_0(x) \leq \exp(-x^2/4)$, ainsi

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| \leq \exp\left(\frac{-\epsilon^2}{4}D_m\right), \tag{3.3.7}$$

avec $D_m := \sum_{\chi\in V_{m,a}(t)}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2$. Puisque $\chi \in V_{m,a}(t) \iff \overline{\chi} \in V_{m,a}(t)$, il est clair que $D_m = \frac{1}{2}\sum_{\chi\in V_{m,a}(t)}(I(\chi)+I(\overline{\chi}))$. D'où on déduit de (3.2.1) que

$$\begin{aligned}D_m &= \frac{q}{2(q-1)}\sum_{\chi\in V_{m,a}(t)} M(\chi^*) + O\left(\sum_{\chi\in V_{m,a}(t)}\log M(\chi^*)\right)\\ &= \frac{q}{2(q-1)}\sum_{\chi\in V_{m,a}(t)} M(\chi^*) + O\left(\phi(m)\log M\right).\end{aligned} \tag{3.3.8}$$

Il découle donc du Lemme 3.3.7 et de (3.3.8) que pour M assez grand on a

$$D_m \geq \frac{\phi(m)M}{8r} + O\left(\phi(m)\log M\right). \tag{3.3.9}$$

Par conséquent, la première partie de cette proposition découle de la combinaison de (3.3.7) et (3.3.9).

On suppose maintenant que $\|t\| > 4\sqrt{q}$. Puisque $|J_0(x)| \leq 1$ pour tout $x \in \mathbb{R}$, alors

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)|^2 \leq \prod_{\chi\in V_{m,a}(t)} \left| F\left(\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|,\chi\right) F\left(\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|,\overline{\chi}\right)\right|.$$

Donc pour $\chi \in V_{m,a}(t)$ on a $\left|\sum\limits_{j=1}^{r}\chi(a_j)t_j\right| \geq \frac{\|t\|}{2} > 2\sqrt{q}$. Ainsi on déduit en utilisant le Lemme 3.3.3 que

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)|^2 \leq \prod_{\chi\in V_{m,a}(t)} \exp\left(-\frac{1}{2}\left(\log\|t\| - \log 2\right)\left(M(\chi^*)-2\right)\right). \tag{3.3.10}$$

Puisque $\log 2 \leq \frac{\log\|t\|}{2}$ alors

$$\begin{aligned}|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)|^2 &\leq \prod_{\chi\in V_{m,a}(t)} \exp\left(-\frac{\log\|t\|}{4}M(\chi^*)\right) \times \exp\left(\log\|t\|\right)\\ &\leq \exp\left(-\frac{\log\|t\|}{4}\sum_{\chi\in V_{m,a}(t)} M(\chi^*)\right) \times \exp\left(\phi(m)\log\|t\|\right).\end{aligned}$$

Ainsi d'après le Lemme 3.3.7 on obtient

$$\begin{aligned}|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)|^2 &\leq \exp\left(-\frac{\log\|t\|\phi(m)M}{16r} + \log\|t\|\phi(m)\right)\\ &\leq \exp\left(-\log\|t\|\phi(m)\left(\frac{M}{16r}-1\right)\right).\end{aligned} \tag{3.3.11}$$

Or comme $\deg(m) = M$ est assez grand on a $\frac{M}{16r} - 1 \geq \frac{M}{32r}$. Donc il suffit de prendre $c_2(r) = \frac{1}{64r}$ pour déduire la deuxième partie de cette proposition. □

Le résultat suivant est une formule asymptotique pour la transformée de Fourier dans la région $\|t\| \ll \phi(m)^{-1/2}$. C'est un outil crucial pour la démonstration du Théorème 3.1.3.

Proposition 3.3.8. *Soit $r \geq 2$ un entier fixé et $m \in \mathcal{M}_q$ de degré assez grand M. Supposons (LI ★). Alors pour toute constante $A = A(r) > 0$, il existe $L(A) > 0$ tel que pour tout*

$L \geq L(A)$ et $t = (t_1, \dots, t_r) \in \mathbb{R}^r$ avec $\|t\| \leq AM^{1/2}$ on a

$$\hat{\mu}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}}, \dots, \frac{t_r}{\sqrt{N_m}}\right) = \exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right)\left(1 + \frac{i}{2\sqrt{N_m}}\frac{\sqrt{q}+q}{q-1}\left(\sum_{j=1}^{r} C_m(a_j)t_j\right)\right.$$
$$- \frac{1}{4N_m}\frac{q+q^2}{(q-1)^2}\left(\sum_{j=1}^{r} C_m(a_j)^2 t_j^2\right) - \frac{1}{N_m}\sum_{1\leq j<k\leq r}\left(B_m(a_j,a_k) + \frac{1}{2}\frac{q+q^2}{(q-1)^2}C_m(a_j)C_m(a_k)\right)t_jt_k$$
$$\left. + \frac{Q_4(t_1,\dots,t_r)}{N_m} + \sum_{s=0}^{1}\sum_{d=0}^{2}\sum_{\substack{0\leq l\leq L\\ 2l\geq 3-2s-d}}\frac{1}{2}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right)\frac{C_m^d B_m^l}{N_m^{d/2+l+s}}P_{s,d,l}(t_1,\dots,t_r) + O\left(\frac{r^L B_m^L \|t\|^{2L}}{L!N_m^L}\right)\right),$$

où Q_4 est un polynôme homogène de degré 4 à coefficients bornés et les $P_{s,d,l}$ sont des polynômes homogènes de degré $d+2l+4s$ dont les coefficients sont bornés uniformément par une fonction de l.

Démonstration. De la formule explicite (2.3.2), on obtient

$$\log\hat{\mu}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}}, \dots, \frac{t_r}{\sqrt{N_m}}\right) = \log\mathcal{B}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}}, \dots, \frac{t_r}{\sqrt{N_m}}\right)$$
$$+ \sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\log J_0\left(\frac{2}{\sqrt{N_m}}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|\right).$$

D'après le [**FM13**, Lemme 2.8], pour $|s| \leq 1$, on sait que

$$\log J_0(s) = -\sum_{n=1}^{\infty} u_{2n}s^{2n},$$

avec $u_2 = 1/4$ et $u_{2n} \ll \left(\frac{5}{12}\right)^{2n}$ pour $n \geq 2$. Donc

$$\log\hat{\mu}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}}, \dots, \frac{t_r}{\sqrt{N_m}}\right) = \log\mathcal{B}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}}, \dots, \frac{t_r}{\sqrt{N_m}}\right)$$
$$- \sum_{n=1}^{\infty}\frac{u_{2n}2^{2n}}{N_m^n}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^{2n}\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|^{2n}. \tag{3.3.12}$$

La contribution du terme $n=1$ à la partie droite de (3.3.12) vaut

$$-\frac{1}{N_m}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\sum_{1\leq j,k\leq r}\chi(a_j)\overline{\chi}(a_k)t_jt_k = -\frac{1}{2}\left(\sum_{j=1}^{r}t_j^2\right) - \frac{1}{N_m}\sum_{1\leq j<k\leq r}B_m(a_j,a_k)t_jt_k.$$

La contribution du terme $n=2$ à la partie droite de (3.3.12) est égale à $\frac{Q_4(t_1,\dots,t_r)}{N_m}$, où

$$Q_4(t_1,\dots,t_r) := -\frac{16u_4}{N_m}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^4\left|\sum_{j=1}^{r}\chi(a_j)t_j\right|^4$$

$$= -\frac{16u_4}{N_m}\sum_{1\le j_1,j_2,j_3,j_4\le r}\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\chi(a_{j_1})\chi(a_{j_2})\overline{\chi}(a_{j_3})\overline{\chi}(a_{j_4})\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^4 t_{j_1}t_{j_2}t_{j_3}t_{j_4}.$$

Puisque $\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^4 \le \left(\sqrt{2}+1\right)^2 N_m$, alors $Q_4(t_1,\dots,t_r)$ est un polynôme homogène de degré 4 à coefficients bornés. De plus, puisque $\sum_{\substack{\chi \bmod m\\ \chi\neq\chi_0}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^{2n} \le 16^{n-1}N_m$ alors la contribution des termes $n\ge 3$ de la partie droite de (3.3.12) est $\ll \|t\|^6/N_m^2 \ll_r \frac{M}{\phi(m)^2}$. Ainsi

$$\begin{aligned}\log\hat{\mu}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right) &= \log\mathcal{B}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right)\\ &\quad -\frac{1}{2}\left(\sum_{j=1}^{r}t_j^2\right)-\frac{1}{N_m}\sum_{1\le j<k\le r}B_m(a_j,a_k)t_jt_k \qquad (3.3.13)\\ &\quad +\frac{Q_4(t_1,\dots,t_r)}{N_m}+O_r\left(\frac{M}{\phi(m)^2}\right).\end{aligned}$$

Afin d'établir la formule asymptotique de $\hat{\mu}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right)$, on va se focaliser sur l'exponentiation de la partie droite de (3.3.13). On a

$$\begin{aligned}\mathcal{B}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right) &= \frac{1}{2}\left[\exp\left(i\frac{\sqrt{q}}{(q-1)\sqrt{N_m}}\sum_{j=1}^{r}C_m(a_j)t_j\right)\right.\\ &\quad \left.+\exp\left(i\frac{q}{(q-1)\sqrt{N_m}}\sum_{j=1}^{r}C_m(a_j)t_j\right)\right].\end{aligned}$$

Donc dans cette région de t, il s'ensuit que

$$\begin{aligned}\mathcal{B}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right) &= \frac{1}{2}\left(\sum_{d=0}^{2}\frac{1}{d!N_m^{d/2}}\frac{q^{d/2}+q^d}{(q-1)^d}\left(i\sum_{j=1}^{r}C_m(a_j)t_j\right)^d\right)\\ &\quad +O_r\left(\frac{C_m^3}{\phi(m)^{3/2}}\right).\end{aligned}$$

En outre, on sait que

$$\exp\left(\frac{Q_4(t_1,\dots,t_r)}{N_m}\right)=1+\frac{Q_4(t_1,\dots,t_r)}{N_m}+O_r\left(\frac{M^2}{\phi(m)^2}\right),$$

et on a

$$\exp\left(-\frac{1}{N_m}\sum_{1\le j<k\le r}B_m(a_j,a_k)t_jt_k\right)=\sum_{l=0}^{\infty}\frac{\left(-\sum\limits_{1\le j<k\le r}B_m(a_j,a_k)t_jt_k\right)^l}{l!N_m^l}.$$

Donc en divisant $\hat{\mu}_{m;a_1,\dots,a_r}\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right)$ par $\exp\left(-\frac{1}{2}\sum\limits_{i=1}^{r}t_i^2\right)$, on obtient

$$\frac{1}{2}\sum_{s=0}^{1}\sum_{d=0}^{2}\sum_{l=0}^{\infty}\frac{Q_4(t_1,\dots,t_r)^s}{d!l!N_m^{d/2+s+l}}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right)\left(i\sum_{j=1}^{r}C_m(a_j)t_j\right)^d\left(-\sum_{1\le j<k\le r}B_m(a_j,a_k)t_jt_k\right)^l + O_r\left(\frac{C_m^3}{\phi(m)^{3/2}}\right). \tag{3.3.14}$$

On regroupe les sommes ci-dessus selon $D=d+2s+2l$. La contribution des termes $0\le D\le 2$ au terme principal de (3.3.14) est égale à

$$1+\frac{i}{2\sqrt{N_m}}\left(\frac{q+\sqrt{q}}{q-1}\right)\sum_{j=1}^{r}C_m(a_j)t_j-\frac{1}{4N_m}\left(\frac{q+q^2}{(q-1)^2}\right)\left(\sum_{j=1}^{r}C_m(a_j)t_j\right)^2 - \frac{1}{N_m}\left(\sum_{1\le j<k\le r}B_m(a_k,a_k)t_jt_k\right)+\frac{Q_4(t_1,\dots,t_r)}{N_m}.$$

Soit $P_{s,d,l}(t_1,\dots,t_r)$ le polynôme homogène de degré $d+2l+4s$ défini par

$$P_{s,d,l}(t_1,\dots,t_r)=\frac{1}{d!l!}C_m^{-d}B_m^{-l}Q_4(t_1,\dots,t_r)^s\left(i\sum_{j=1}^{r}C_m(a_j)t_j\right)^d\left(-\sum_{1\le j<k\le r}B_m(a_j,a_k)t_jt_k\right)^l.$$

Alors la contribution des termes avec $D\ge 3$ à (3.3.14) est

$$\sum_{s=0}^{1}\sum_{d=0}^{2}\sum_{\substack{l\ge 0\\ 2l\ge 3-2s-d}}\frac{1}{2}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right)\frac{C_m^dB_m^l}{N_m^{d/2+l+s}}P_{s,d,l}(t_1,\dots,t_r).$$

Puisque r est fixe et $s,d\le 2$, alors il est clair que les coefficients de $P_{s,d,l}$ sont uniformément bornés par une fonction de l. De plus, puisque $C_m=|m|^{o(1)}$ et $\frac{|m|}{\phi(m)}\ll M$ (d'après (2.2.5)), alors

$$\frac{1}{2}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right)\frac{C_m^dB_m^l}{N_m^{d/2+l+s}}P_{s,d,l}(t_1,\dots,t_r)\ll\frac{r^{d/2+l}C_m^dB_m^l}{d!l!N_m^{d/2+l+s}}\|t\|^{d+2l+4s}\ll\frac{r^lB_m^l\|t\|^{2l}}{l!N_m^l}.$$

De plus, en utilisant le Corollaire 3.2.10 on sait qu'il existe $c > 0$ tel que $B_m \leq c\phi(m)$. Ainsi pour $\|t\| \leq AM^{1/2}$ on a $r^2 B_m \|t\|^2/(lN_m) \ll r^2A^2/l$.
Donc pour une constante convenablement grande $L(A) > 0$ (qui dépend aussi de r), on en déduit que pour $L \geq L(A)$ on a

$$\sum_{s=0}^{1}\sum_{d=0}^{2}\sum_{\substack{l\geq L\\ 2l\geq 3-2s-d}}\frac{1}{2}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right)\frac{C_m^d B_m^l}{N_m^{d/2+l+s}}P_{s,d,l}(t_1,\dots,t_r) \ll \frac{r^L B_m^L\|t\|^{2L}}{L!N_m^L}.$$

Ceci complète la preuve. □

L'étape suivante consiste à majorer la queue de la mesure $\mu_{m;a_1,\dots,a_r}$.
Pour ce faire, nous démontrons le lemme suivant :

Lemme 3.3.9. *Soit $m \in \mathcal{M}_q$ un polynôme de degré assez grand M et $2 \leq r \leq \phi(m)$ un entier. Alors pour $R \geq \sqrt{\phi(m)M}$ on a*

$$\mu_{m;a_1,\dots,a_r}(|x|_\infty > R) \leq 2r\exp\left(-\frac{R^2}{32\phi(m)M}\right),$$

uniformément pour tout $(a_1,\dots,a_r) \in \mathcal{A}_r(m)$.

Démonstration. On remarque d'abord que

$$\mu_{m;a_1,\dots,a_r}(|x|_\infty > R) = \mathbb{P}(|X_{m;a_1,\dots,a_r}|_\infty > R) \leq \sum_{j=1}^{r}\mathbb{P}(X_{m;a_j} > R) + \sum_{j=1}^{r}\mathbb{P}(X_{m;a_j} < -R).$$

On commence par borner $\mathbb{P}(X_{m;a_j} > R)$. Soit $s > 0$ et $(a,m) = 1$. Alors on a

$$\mathbb{E}\left(\exp(sX_{m;a})\right) = \mathbb{E}\left(\exp(-sC_m(a)X')\right)\prod_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\prod_{\Im(\gamma_\chi)>0}\mathbb{E}\left(2\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|s\mathrm{Re}(\chi(a)U(\gamma_\chi))\right).$$

Or on sait que

$$\mathbb{E}\left(\exp(-sC_m(a)X')\right) = \frac{1}{2}\left(\exp\left(-s\frac{\sqrt{q}}{q-1}C_m(a)\right)+\exp\left(-s\frac{q}{q-1}C_m(a)\right)\right)$$

Donc

$$\mathbb{E}\left(\exp(sX_{m;a})\right) = \frac{1}{2}\left(\exp\left(-s\frac{\sqrt{q}}{q-1}C_m(a)\right)+\exp\left(-s\frac{q}{q-1}C_m(a)\right)\right)\prod_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\prod_{\Im(\gamma_\chi)>0}I_0\left(2s\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|\right),$$

où $I_0(t) := \sum_{n=0}^{\infty}(t/2)^{2n}/n!^2$ est la fonction de Bessel modifiée d'ordre 0. Ainsi, en utilisant la borne de Chernoff avec le fait que $I_0(s) \leq \exp(s^2/4)$ pour tout $s \in \mathbb{R}$, on obtient

$$\begin{aligned}\mathbb{P}(X_{m;a} > R) &\leq \exp(-sR)\mathbb{E}\left(\exp(sX_{m;a})\right)\\ &\leq \frac{1}{2}\left(\exp\left(-sR - s\frac{\sqrt{q}}{q-1}C_m(a)\right) + \exp\left(-sR - s\frac{q}{q-1}C_m(a)\right)\right)\\ &\quad\times \exp\left(s^2 \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2\right)\\ &\leq \frac{1}{2}\exp\left(-sR - s\frac{\sqrt{q}}{q-1}C_m(a) + \frac{s^2}{2}N_m\right) + \frac{1}{2}\exp\left(-sR - s\frac{q}{q-1}C_m(a) + \frac{s^2}{2}N_m\right)\end{aligned} \tag{3.3.15}$$

On choisit $s = R/(\phi(m)M)$. On traite les deux cas suivants :

- **Cas 1 :** a est non-résidu quadratique modulo m.
  On a alors $C_m(a) = -1$. Ainsi

  $$\mathbb{P}(X_{m;a} > R) \leq \exp\left(-\frac{R^2}{\phi(m)M} + \frac{q}{q-1}\frac{R}{\phi(m)M} + \frac{R^2}{2\phi(m)^2M^2}N_m\right).$$

  Or on sait d'après (3.1.3) que $\frac{R^2}{2\phi(m)^2M^2}N_m \leq \frac{R^2}{2\phi(m)^2M^2} \times \frac{5q}{4(q-1)}\phi(m)M = \frac{5q}{8(q-1)}\frac{R^2}{\phi(m)M}$ et que $\frac{q}{q-1} = 1 + \frac{1}{q-1} \leq \frac{3}{2}$ alors

  $$\frac{R^2}{2\phi(m)^2M^2}N_m \leq \frac{15}{16}\frac{R^2}{\phi(m)M}. \tag{3.3.16}$$

  Donc

  $$\mathbb{P}(X_{m;a} > R) \leq \exp\left(-\frac{1}{16}\frac{R^2}{\phi(m)M} + \frac{q}{q-1}\frac{R}{\phi(m)M}\right).$$

  Or puisque m est de degré assez grand on a $\frac{q}{q-1}\frac{R}{\phi(m)M} \leq \frac{1}{32}\frac{R^2}{\phi(m)M}$. Ainsi

  $$\mathbb{P}(X_{m;a} > R) \leq \exp\left(-\frac{1}{32}\frac{R^2}{\phi(m)M}\right).$$

- **Cas 2 :** a est résidu quadratique modulo m.
  On a $C_m(a) \geq 1$ alors $\frac{q}{q-1}C_m(a) \geq \frac{\sqrt{q}}{q-1}C_m(a)$ ainsi

  $$\mathbb{P}(X_{m;a} > R) \leq \exp\left(-\frac{R^2}{\phi(m)M} - \frac{\sqrt{q}}{q-1}\frac{R}{\phi(m)M}C_m(a) + \frac{R^2}{2(\phi(m)M}N_m\right).$$

  Donc d'après (3.3.16) on a

$$\mathbb{P}(X_{m;a} > R) \leq \exp\left(-\frac{1}{16}\frac{R^2}{\phi(m)M} - \frac{\sqrt{q}}{q-1}\frac{R}{\phi(m)M}C_m(a)\right) \leq \exp\left(-\frac{1}{16}\frac{R^2}{\phi(m)M}\right). \tag{3.3.17}$$

On s'intéresse maintenant à la majoration de $\mathbb{P}(X_{m;a} < -R)$. Soit $s < 0$ et $(a,m) = 1$. En utilisant l'inégalité de Chernoff on sait que $\mathbb{P}(X_{m;a} < -R) \leq e^{sR}\mathbb{E}\left(e^{-sX_{m;a}}\right)$. Par des arguments similaires utilisés pour obtenir (3.3.15), on trouve

$$\mathbb{P}(X_{m;a} < -R) \leq \frac{1}{2}\left(\exp\left(sR + s\frac{\sqrt{q}}{q-1}C_m(a) - \frac{s^2}{2}N_m\right) + \exp\left(sR + s\frac{q}{q-1}C_m(a) - \frac{s^2}{2}N_m\right)\right).$$

On prend $s = -\frac{R}{\phi(m)M}$. On distingue les deux cas suivants :

- **Cas 1 :** a est non-résidu quadratique modulo m.
  Il est clair que

$$\mathbb{P}(X_{m;a} < -R) \leq \frac{1}{2}\exp\left(-\frac{R^2}{\phi(m)M} + \frac{\sqrt{q}}{q-1}\frac{R}{\phi(m)M} - \frac{R^2}{2(\phi(m)M)}N_m\right) + \frac{1}{2}\exp\left(-\frac{R^2}{\phi(m)M} + \frac{q}{q-1}\frac{R}{\phi(m)M} - \frac{R^2}{2(\phi(m)M)}N_m\right).$$

  Puisque M est assez grand, en utilisant (3.1.3), on déduit facilement que

$$\mathbb{P}(X_{m;a} < -R) \leq \exp\left(-\frac{1}{32}\frac{R^2}{\phi(m)M}\right).$$

- **Cas 2 :** a est résidu quadratique modulo m.
  Comme $C_m(a) \geq 1$ et $N_m \geq \phi(m)M$ lorsque M est assez grand alors

$$\mathbb{P}(X_{m;a} < -R) \leq \exp\left(-\frac{3}{2}\frac{R^2}{\phi(m)M}\right) \leq \exp\left(-\frac{1}{32}\frac{R^2}{\phi(m)M}\right).$$

En combinant tous les cas, on déduit le Lemme 3.3.9.

□

3.4. Formule asymptotique des densités $\delta_{m;a_1,a_2}$

Le but de cette section est d'établir une formule asymptotique pour les densités lorsque $r = 2$ et de prouver le Théorème 3.1.2. Nous allons d'abord adapter la preuve de la Proposition 3.3.8 pour établir le lemme clé suivant :

Lemme 3.4.1. *Supposons que (LI ★) est vraie. Pour $t = (t_1,t_2) \in \mathbb{R}^2$ avec $||t|| \leq N_m^{1/4}$ on a*

$$\hat{\mu}_{m;a_1,a_2}\left(\frac{t_1}{\sqrt{N_m}},\frac{t_2}{\sqrt{N_m}}\right) = \exp\left(-\frac{t_1^2+t_2^2}{2} - \frac{B_m(a_1,a_2)}{N_m}t_1t_2\right)F_{m;a_1,a_2}(t_1,t_2),$$

où

$$F_{m;a_1,a_2}(t_1,t_2) = 1 + \frac{i}{2\sqrt{N_m}}\left(\frac{\sqrt{q}+q}{q-1}\right)(C_m(a_1)t_1 + C_m(a_2)t_2) + O\left(\frac{||t||^4}{N_m} + \frac{||t||^2C_m(1)^2}{N_m}\right).$$

Démonstration. Pour $||t|| \leq N_m^{1/4}$ la formule explicite (2.3.2) implique que $\log \hat{\mu}_{m;a_1,a_2}\left(t_1 N_m^{-1/2}, t_2 N_m^{-1/2}\right)$ vaut

$$\begin{aligned}
&\log \mathcal{B}_{m;a_1,a_2}\left(\frac{t_1}{\sqrt{N_m}}, \frac{t_2}{\sqrt{N_m}}\right) - \frac{1}{N_m} \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 |\chi(a_1)t_1 + \chi(a_2)t_2|^2 + O\left(\frac{||t||^4}{N_m}\right) \\
&= \log \mathcal{B}_{m;a_1,a_2}\left(\frac{t_1}{\sqrt{N_m}}, \frac{t_2}{\sqrt{N_m}}\right) - \frac{t_1^2 + t_2^2}{2} - \frac{B_m(a_1,a_2)}{N_m} t_1 t_2 + O\left(\frac{||t||^4}{N_m}\right).
\end{aligned} \tag{3.4.1}$$

En outre, on a

$$\begin{aligned}
\mathcal{B}_{m;a_1,a_2}\left(\frac{t_1}{\sqrt{N_m}}, \frac{t_2}{\sqrt{N_m}}\right) &= \frac{1}{2}\left[\exp\left(i\frac{\sqrt{q}}{q-1}\left(C_m(a_1)\frac{t_1}{\sqrt{N_m}} + C_m(a_2)\frac{t_2}{\sqrt{N_m}}\right)\right)\right. \\
&\quad \left. + \exp\left(i\frac{q}{q-1}\left(C_m(a_1)\frac{t_1}{\sqrt{N_m}} + C_m(a_2)\frac{t_2}{\sqrt{N_m}}\right)\right)\right] \\
&= 1 + \frac{i}{2\sqrt{N_m}}\left(\frac{\sqrt{q}+q}{q-1}\right)(C_m(a_1)t_1 + C_m(a_2)t_2) + O\left(\frac{||t||^2 C_m(1)^2}{N_m}\right).
\end{aligned} \tag{3.4.2}$$

Ainsi, en combinant (3.4.1) et (3.4.2) on déduit ce dernier lemme. □

Afin de prouver le Théorème 3.1.2, nous allons utiliser le lemme suivant :

Lemme 3.4.2 ([**Lam13**, Lemme 8.2])**.** *Soit ρ un nombre réel tel que $|\rho| \leq 1/2$, n_1, n_2 des entiers naturels fixés et S un nombre assez grand. Alors*

$$\begin{aligned}
&\int_{||t||\leq S} e^{i(t_1x_1+t_2x_2)} t_1^{n_1} t_2^{n_2} \exp\left(-\frac{t_1^2+t_2^2+2\rho t_1 t_2}{2}\right) dt_1 dt_2 \\
&= \frac{1}{i^{n_1+n_2}} \frac{\partial^{n_1+n_2}\Phi_\rho(x_1,x_2)}{\partial x_1^{n_1} \partial x_2^{n_2}} + O\left(\exp\left(-\frac{S^2}{8}\right)\right),
\end{aligned}$$

où

$$\Phi_\rho(x_1,x_2) = \frac{2\pi}{\sqrt{1-\rho^2}} \exp\left(-\frac{1}{2(1-\rho^2)}(x_1^2 + x_2^2 - 2\rho x_1 x_2)\right).$$

Démonstration du Théorème 3.1.2. On utilise μ_m pour désigner $\mu_{m;a_1,a_2}$. Soit $R = \sqrt{N_m}M$. D'après la Proposition 3.3.9, on a

$$\delta_{m;a_1,a_2} = \int_{-R<y_2<y_1<R} d\mu_m(y_1,y_2) + O\left(\exp\left(-\frac{M^2}{16}\right)\right).$$

En appliquant la transformée de Fourier inverse de la mesure μ_m, on a

$$\delta_{m;a_1,a_2} = \frac{1}{(2\pi)^2} \int_{-R<y_2<y_1<R} \int_{s\in\mathbb{R}^2} e^{i(s_1y_1+s_2y_2)} \hat{\mu}_m(s_1,s_2) ds dy + O\left(\exp\left(-\frac{M^2}{16}\right)\right). \tag{3.4.3}$$

De plus, en utilisant la Proposition 3.3.4 avec $\epsilon = MN_m^{-1/2}$ on obtient que

$$\int_{s\in\mathbb{R}^2} e^{i(s_1y_1+s_2y_2)}\hat{\mu}_m(s_1,s_2)ds = \int_{||s||\leq\epsilon} e^{i(s_1y_1+s_2y_2)}\hat{\mu}_m(s_1,s_2)ds + O\left(\exp\left(-cM^2\right)\right),$$

pour une certaine constante $c > 0$. En insérant cette estimation dans (3.4.3), et en effectuant les changements de variables $t_j = \sqrt{N_m}s_j$ et $x_j = y_j/\sqrt{N_m}$ pour $j \in \{1,2\}$, on déduit en utilisant le Lemme 3.4.1 que

$$\begin{aligned}\delta_{m;a_1,a_2} &= \frac{1}{(2\pi)^2}\int_{-M<x_2<x_1<M}\int_{||t||<M} e^{i(t_1x_1+t_2x_2)}\hat{\mu}_m\left(\frac{t_1}{\sqrt{N_m}},\frac{t_2}{\sqrt{N_m}}\right)dtdx \\ &\quad + O\left(\exp\left(-M^{3/2}\right)\right). \qquad (3.4.4)\\ &= I_0 + \frac{i(\sqrt{q}+q)}{2(q-1)}\frac{C_m(a_1)}{\sqrt{N_m}}I_1 + \frac{i(\sqrt{q}+q)}{2(q-1)}\frac{C_m(a_2)}{\sqrt{N_m}}I_2 + O\left(\frac{C_m(1)^2M^2}{N_m}\right),\end{aligned}$$

avec

$$I_0 = \frac{1}{(2\pi)^2}\int_{-M<x_2<x_1<M}\int_{||t||<M} e^{i(t_1x_1+t_2x_2)}\exp\left(-\frac{t_1^2+t_2^2}{2} - \frac{B_m(a_1,a_2)}{N_m}t_1t_2\right)dtdx,$$

et

$$I_j = \frac{1}{(2\pi)^2}\int_{-M<x_2<x_1<M}\int_{||t||<M} e^{i(t_1x_1+t_2x_2)}t_j\exp\left(-\frac{t_1^2+t_2^2}{2} - \frac{B_m(a_1,a_2)}{N_m}t_1t_2\right)dtdx,$$

pour $j \in \{1,2\}$. On doit d'abord évaluer I_0. Soit $\rho = B_m(a_1,a_2)/N_m$. Le Corollaire 3.2.10 implique que $|\rho| \leq 1/2$ pour M assez grand. Donc le Lemme 3.4.2 permet d'affirmer que

$$\begin{aligned}I_0 &= \frac{1}{2\pi\sqrt{1-\rho^2}}\int_{-M<x_2<x_1<M}\exp\left(-\frac{1}{2(1-\rho^2)}(x_1^2+x_2^2-2\rho x_1x_2)\right)dx_1dx_2 \\ &\quad + O\left(\exp\left(-\frac{M^2}{10}\right)\right).\end{aligned}$$

L'intégrale sur la partie droite de la dernière estimation est égale à

$$\frac{1}{2\pi\sqrt{1-\rho^2}}\int_{x_1>x_2}\exp\left(-\frac{1}{2(1-\rho^2)}(x_1^2+x_2^2-2\rho x_1x_2)\right)dx_1dx_2 + O\left(\exp\left(-\frac{M^2}{10}\right)\right).$$

En combinant le fait que l'intégrande est symétrique en x_1 et x_2, avec l'égalité suivante :

$$\frac{1}{2\pi\sqrt{1-\rho^2}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp\left(-\frac{1}{2(1-\rho^2)}(x_1^2+x_2^2-2\rho x_1x_2)\right)dx_1dx_2 = 1,$$

on obtient

$$I_0 = \frac{1}{2} + O\left(\exp\left(-\frac{M^2}{10}\right)\right). \qquad (3.4.5)$$

En utilisant le Lemme 3.4.2, on trouve par des arguments similaires que

$$\begin{aligned} I_1 &= \frac{1}{(2\pi)^2 i}\int_{x_1>x_2}\frac{\partial\Phi_\rho(x_1,x_2)}{\partial x_1}dx_1dx_2 + O\left(\exp\left(-\frac{M^2}{10}\right)\right) \\ &= -\frac{1}{(2\pi)^2 i}\int_{-\infty}^{\infty}\Phi_\rho(x_2,x_2)dx_2 + O\left(\exp\left(-\frac{M^2}{10}\right)\right). \end{aligned}$$

De plus, on sait que

$$\int_{-\infty}^{\infty}\Phi_\rho(y,y)dy = \frac{2\pi}{\sqrt{1-\rho^2}}\int_{-\infty}^{\infty}\exp\left(-\frac{y^2}{2}\left(\frac{2}{1+\rho}\right)\right)dy = \frac{2\pi^{3/2}}{\sqrt{1-\rho}}.$$

Puisque $2(1-\rho) = V_m(a_1,a_2)/N_m$, alors en combinant les estimations ci-dessus on obtient

$$I_1 = -\frac{\sqrt{N_m}}{i\sqrt{2\pi V_m(a_1,a_2)}} + O\left(\exp\left(-\frac{M^2}{10}\right)\right). \tag{3.4.6}$$

D'une manière similaire, il est facile de vérifier que

$$I_2 = \frac{\sqrt{N_m}}{i\sqrt{2\pi V_m(a_1,a_2)}} + O\left(\exp\left(-\frac{M^2}{10}\right)\right). \tag{3.4.7}$$

Enfin, en insérant les estimations (3.4.5)-(3.4.7) dans (3.4.4), et en utilisant le fait que $N_m \sim \frac{q}{q-1}\phi(m)\log_q|m|$, on en déduit le résultat souhaité. □

3.5. Formules asymptotiques de $\delta_{m;a_1,a_2,\ldots,a_r}$ pour $r \geq 3$

Dans cette section, nous allons démontrer une formule asymptotique pour $\delta_{m;a_1,\ldots,a_r}$ (Théorème 3.1.3) ainsi que le Théorème 3.1.16. Nous avons déjà trouvé une borne pour la queue de la mesure $\mu_{m;a_1,\ldots,a_r}$ dans la Proposition 3.3.9. Nous avons également établi une formule pour la transformée de Fourier $\hat{\mu}_{m;a_1,\ldots,a_r}$ dans la Proposition 3.3.8. Ainsi, en suivant la stratégie utilisée pour obtenir la formule asymptotique lorsque $r=2$, nous allons prouver le Théorème 3.1.3.

Démonstration du Théorème 3.1.3. On commence par raccourcir d'abord les notations en utilisant δ_m et μ_m pour faire respectivement référence à $\delta_{m;a_1,\ldots,a_r}$ et $\mu_{m;a_1,\ldots,a_r}$. On a

$$\delta_m = \int_{\substack{y_1>\cdots>y_r \\ |y|_\infty\leq R}} d\mu_m(y_1,\ldots,y_r) + \int_{\substack{y_1>\cdots>y_r \\ |y|_\infty> R}} d\mu_m(y_1,\ldots,y_r).$$

Il découle de la Proposition 3.3.9 l'inégalité suivante :

$$\mu_{m;a_1,\ldots,a_r}(|y|_\infty > R) \leq 2r\exp\left(\frac{-R^2}{32\phi(m)M}\right).$$

En particulier on prend $R = \sqrt{N_m}M$, et donc

$$\delta_m = \int_{\substack{y_1>\cdots>y_r \\ |y|_\infty\leq R}} d\mu_m(y_1,\ldots,y_r) + O_r\left(\exp\left(\frac{-M^2}{16}\right)\right).$$

En appliquant la formule d'inversion de Fourier à μ_m, on obtient

$$\int_{\substack{y_1>\cdots>y_r\\ |y|_\infty\leq R}} d\mu_m(y_1,\ldots,y_r) = (2\pi)^{-r}\int_{\substack{y_1>\cdots>y_r\\ |y|_\infty\leq R}}\int_{s\in\mathbb{R}^r} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)dsdy.$$

Soit $A=A(r)\geq r$ une constante convenablement grande. En utilisant la Proposition 3.3.4 avec $\epsilon = A(N_m)^{-1/2}M^{1/2}$, on trouve la formule suivante :

$$\int_{s\in\mathbb{R}^r} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)ds = \int_{\|s\|\leq\epsilon} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)ds + O\left(\exp\left(-2AM\right)\right).$$

Comme $R^r\exp\left(-2AM\right)\ll\exp\left(-AM\right)$, alors on a

$$\delta_m = (2\pi)^{-r}\int_{\substack{y_1>\cdots>y_r\\ |y|_\infty\leq R}}\int_{\|s\|\leq\epsilon} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)dsdy + O\left(\exp\left(-AM\right)\right).$$

En faisant le changement de variables suivant $t_j=\sqrt{N_m}s_j$ et $x_j=\frac{y_j}{\sqrt{N_m}}$, on déduit

$$\delta_m = (2\pi)^{-r}\int_{\substack{x_1>\cdots>x_r\\ |x|_\infty\leq M}}\int_{\|t\|\leq AM^{1/2}} e^{i(t_1x_1+\cdots+t_rx_r)}\hat{\mu}_m\left(\frac{t_1}{\sqrt{N_m}},\ldots,\frac{t_r}{\sqrt{N_m}}\right)dtdx + O\left(\exp\left(-AM\right)\right).$$

On prend $L=L(A)\geq 2r$ une constante convenablement grande. Ainsi, en utilisant la Proposition 3.3.8, on a

$$\begin{aligned}\delta_m = J_0 &+ \frac{i}{2\sqrt{N_m}}\left(\frac{q+\sqrt{q}}{q-1}\right)\sum_{j=1}^{r}C_m(a_j)G_j - \frac{1}{4N_m}\left(\frac{q+q^2}{(q-1)^2}\right)\sum_{j=1}^{r}C_m(a_j)^2R_j\\ &- \frac{1}{N_m}\sum_{1\leq j<k\leq r}\left[B_m(a_j,a_k)+\frac{1}{2}\left(\frac{q+q^2}{(q-1)^2}\right)C_m(a_j)C_m(a_k)\right]S_{j,k}\\ &+ \frac{T_0}{N_m} + \sum_{s=0}^{1}\sum_{d=0}^{2}\sum_{\substack{0\leq l\leq L\\ 2l\geq 3-2s-d}}\frac{1}{2}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right)\frac{C_m^dB_m^l}{N_m^{d/2+s+l}}Y_{s,d,l}+E_1,\end{aligned}\tag{3.5.1}$$

où $E_1\ll\frac{M^rB_m^L}{N_m^L}$ et

$$J_0 = (2\pi)^{-r}\int_{\substack{x_1>\cdots>x_r\\ |x|_\infty\leq M}}\int_{\|t\|\leq AM^{1/2}} e^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right)dtdx,$$

$$G_j = (2\pi)^{-r}\int_{\substack{x_1>\cdots>x_r\\ |x|_\infty\leq M}}\int_{\|t\|\leq AM^{1/2}} t_je^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right)dtdx,$$

$$R_j = (2\pi)^{-r}\int_{\substack{x_1>\cdots>x_r\\ |x|_\infty\leq M}}\int_{\|t\|\leq AM^{1/2}} t_j^2e^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right)dtdx,$$

$$S_{j,k} = (2\pi)^{-r}\int_{\substack{x_1>\cdots>x_r\\ |x|_\infty\leq M}}\int_{\|t\|\leq AM^{1/2}} t_jt_ke^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right)dtdx,$$

$$T_0 = (2\pi)^{-r}\int_{\substack{x_1>\cdots>x_r\\ |x|_\infty\leq M}}\int_{\|t\|\leq AM^{1/2}} e^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right)Q_4(t_1,\ldots,t_r)dtdx,$$

et

$$Y_{s,d,l} = (2\pi)^{-r} \int_{\substack{x_1>\cdots>x_r \\ |x|_\infty \leq M}} \int_{\|t\| \leq AM^{1/2}} e^{i(t_1x_1+\cdots+t_rx_r)} \exp\left(-\frac{t_1^2+\cdots+t_r^2}{2}\right) P_{s,d,l}(t_1,\ldots,t_r)dtdx.$$

De plus, en utilisant [**Lam13**, Lemme 4.3], on a

$$\frac{T_0}{N_m} + \sum_{s=0}^{1}\sum_{d=0}^{2} \sum_{\substack{0\leq l\leq L \\ 2l\geq 3-2s-d}} \frac{1}{2}\left(\frac{q^{d/2}+q^d}{(q-1)^d}\right) \frac{C_m^d B_m^l}{N_m^{d/2+s+l}} Y_{s,d,l} + E_1 \ll_r \frac{1}{N_m} + \frac{C_m B_m}{N_m^{3/2}} + \frac{B_m^2}{N_m^2}. \tag{3.5.2}$$

En outre, par [**Lam13**, Lemme 4.2], il s'ensuit

$$\begin{aligned} J_0 &= \frac{1}{(2\pi)^{r/2}} \int_{\substack{x_1>\cdots>x_r \\ |x|_\infty \leq M}} \exp\left(-\frac{x_1^2+\cdots+x_r^2}{2}\right)dx + O\left(\exp\left(-AM\right)\right) \\ &= \frac{1}{r!(2\pi)^{r/2}} \int_{x\in\mathbb{R}^r} \exp\left(-\frac{x_1^2+\cdots+x_r^2}{2}\right)dx + O\left(\exp\left(-AM\right)\right) = \frac{1}{r!} + O\left(\exp\left(-AM\right)\right). \end{aligned} \tag{3.5.3}$$

En utilisant le même argument, on peut montrer facilement, pour tout $1 \leq j \leq r$:

$$G_j = i\alpha_j(r) + O\left(\exp\left(-AM\right)\right), \tag{3.5.4}$$

et pour tout $1 \leq j \leq r$, on a

$$R_j = -\lambda_j(r) + O\left(\exp\left(-AM\right)\right). \tag{3.5.5}$$

On déduit par analogie que pour tout $1 \leq j < k \leq r$, on a

$$S_{j,k} = -\beta_{j,k}(r) + O\left(\exp\left(-AM\right)\right). \tag{3.5.6}$$

Ainsi, en combinant les estimations (3.5.1)-(3.5.6), on obtient le Théorème 3.1.3. □

Nous terminons cette section en démontrant le Théorème 3.1.16.

Démonstration du Théorème 3.1.16. Soit $M = \deg(m)$. On considère S_m l'ensemble des couples $(a,b) \in \mathcal{A}_2(m)$ tels que $|B_m(a,b)| \geq \sqrt{\phi(m)}$. Alors par le Théorème 3.1.14, on a

$$|S_m|\sqrt{\phi(m)} \leq \sum_{(a,b)\in\mathcal{A}_2(m)} |B_m(a,b)| \ll \phi(m)^2 M.$$

Ainsi

$$|S_m| \ll \phi(m)^{3/2} M.$$

Soit $\Omega_r(m)$ l'ensemble des r-uplets $(a_1,\ldots,a_r) \in \mathcal{A}_r(m)$ tels qu'il existe $1 \leq i \neq j \leq r$ avec $(a_i,a_j) \in S_m$. On a donc

$$|\Omega_r(m)| \ll_r \phi(m)^{r-\frac{1}{2}} M.$$

Comme $|\mathcal{A}_r(m)| = \phi(m)^r + O_r(\phi(m)^{r-1})$, on obtient $|\Omega_r(m)| = o\left(|\mathcal{A}_r(m)|\right)$.
De plus, si $(a_1,\ldots,a_r) \in \mathcal{A}_r(m) \setminus \Omega_r(m)$, alors pour tout $1 \leq i < j \leq r$ on a

$|B_m(a_i,a_j)| \leq \sqrt{\phi(m)}$. Il découle du Corollaire 3.1.5 la formule suivante :

$$\delta_{m;a_1,\dots,a_r} = \frac{1}{r!} - \frac{q+\sqrt{q}}{2\sqrt{N_m}(q-1)} \sum_{j=1}^{r} \alpha_j(r) C_m(a_j) + O_r\left(\frac{1}{\sqrt{N_m M}}\right).$$

Ainsi pour tous les r-uplets $(a_1,\dots,a_r), (b_1,\dots,b_r) \in \mathcal{A}_r(m) \setminus \Omega_r(m)$, on obtient

$$\delta_{m;a_1,\dots,a_r} - \delta_{m;b_1,\dots,b_r} = \frac{q+\sqrt{q}}{2\sqrt{N_m}(q-1)} \sum_{j=1}^{r} -\alpha_j(r)\left(C_m(a_j) - C_m(b_j)\right) + O_r\left(\frac{1}{\sqrt{N_m M}}\right).$$

De plus, comme pour tout $1 \leq j \leq r$ on sait que $C_m(a_j)$ et $C_m(b_j)$ sont des entiers, il s'ensuit que si $-\sum_{j=1}^{r} \alpha_j(r)\left(C_m(a_j) - C_m(b_j)\right) > 0$, alors $-\sum_{j=1}^{r} \alpha_j(r)\left(C_m(a_j) - C_m(b_j)\right) \gg_r 1$. Donc on déduit finalement $\delta_{m;a_1,\dots,a_r} > \delta_{m;b_1,\dots,b_r}$. □

3.6. Constructions explicites des courses biaisées

Le but de cette section est de démontrer les Théorèmes 3.1.10, 3.1.11 et 3.1.15. Les démonstrations de ces théorèmes sont inspirées de [**Lam13**, section 6].

Nous définissons d'abord

$$\Lambda_0(f) := \begin{cases} \frac{\Lambda(f)}{|f|} & \text{si } f \in \mathbb{F}_q[T] \setminus \{0\}, \\ 0 & \text{sinon.} \end{cases} \tag{3.6.1}$$

Ensuite, nous annoncerons une nouvelle estimation du terme $B_m(a,b)$ lorsque $0 \leq \deg(a), \deg(b) < M$.

Proposition 3.6.1. *Soit $m \in \mathcal{M}_q$ de degré assez grand M. Soit $(a,b) \in \mathcal{A}_2(m)$ tel que $0 \leq \deg(a), \deg(b) < M$.*

(1) Si $\deg(a) = \deg(b)$ alors

$$B_m(a,b) = -\frac{q^2+q}{2(q-1)^2}\phi(m) l(a,b) + O_q\left(\left(|a|+|b|\right) M^2\right),$$

avec $l(a,b) = 1$ si $a = -b$ et 0 sinon.

(2) Si $\deg(a) \neq \deg(b)$ alors

$$B_m(a,b) = \frac{-q}{(q-1)\log q}\phi(m)\Lambda_0\left(\frac{\mathbf{Pmax}(a,b)}{\mathbf{Pmin}(a,b)}\right) + O_q\left(\left(|a|+|b|\right) M^2\right),$$

avec

$$\mathbf{Pmax}(a,b) = \begin{cases} a & \text{si } \deg(a) > \deg(b), \\ b & \text{sinon.} \end{cases} \quad \text{et} \quad \mathbf{Pmin}(a,b) = \begin{cases} b & \text{si } \deg(a) > \deg(b), \\ a & \text{sinon.} \end{cases}$$

Pour prouver ce résultat, nous utilisons le lemme suivant :

Lemme 3.6.2. *Soit $m \in \mathcal{M}_q$ de degré assez grand M. Soit $a,b \in \mathbb{F}_q[T]$ tels que $a \neq b$, $(a,m) = 1$, $(b,m) = 1$ et $0 \leq \deg(a), \deg(b) < M$. Alors*

$$\sum_{P^v||m} \sum_{n=1}^{\infty} \sum_{\substack{1\leq e\leq (9\log q)M \\ aP^e \equiv b \bmod m/P^v \\ \deg(P^e)=n}} \frac{\log|P|}{|P|^{e+v-1}(|P|-1)} \ll_q \frac{(|a|+|b|)M^2}{|m|}.$$

Démonstration. Comme $P|m$ et $(b,m) = 1$, on a $aP^e - b \neq 0$. Ceci implique que si $(m/P^v)|(aP^e - b)$, on a $|m/P^v| \leq |aP^e - b| \leq |a||P|^e + |b|$. Donc $|m/P^v| \leq (|a| + |b|)\,|P|^e$, d'où $\frac{1}{|P|^{e+v}} \leq \frac{|a|+|b|}{|m|}$. Ainsi on obtient

$$\sum_{P^v||m} \sum_{n=1}^{\infty} \sum_{\substack{1\leq e\leq 9\log|m| \\ aP^e \equiv b \bmod m/P^v \\ \deg(P^e)=n}} \frac{\log|P|}{|P|^{e+v-1}(|P|-1)} \ll_q M \left(\sum_{P|m} \frac{|P|\log|P|}{|P|-1}\right) \frac{(|a|+|b|)}{|m|}. \tag{3.6.2}$$

De plus, m peut s'écrire ainsi $m = \alpha P_1^{t_1} \dots P_k^{t_k}$ où $\alpha \in \mathbb{F}_q^*$, chaque P_i est un polynôme irréductible unitaire dans $\mathbb{F}_q[T]$ et $P_i \neq P_j$ pour tout $1 \leq i \neq j \leq k$, et chaque t_i est un entier strictement positif. On a donc

$$\sum_{P|m} \log|P| \leq \sum_{i=1}^{k} t_i \log|P_i| = \log|m|. \tag{3.6.3}$$

Ainsi en combinant (3.6.2) et (3.6.3) on déduit le Lemme 3.6.2. □

Démonstration de la proposition 3.6.1. Puisque $0 \leq \deg(a), \deg(b) < \deg(m) = M$, alors $a + b \equiv 0 \bmod m$, implique que $a = -b$. En plus, en utilisant le fait que $|(m,a-b)| \leq |a| + |b|$ et (2.2.5), on obtient

$$\frac{\Lambda(m/(m,a-b))}{\phi(m/(m,a-b))} \ll_q \frac{M^2}{|m|}(|a| + |b|).$$

D'où en combinant la Proposition 3.2.8, et les Lemmes 3.2.12 et 3.6.2 on déduit

$$\begin{aligned} B_m(a,b) = -\phi(m) &\left(\frac{q^2+q}{2(q-1)^2} l(a,b) + \frac{q}{(q-1)\log q}\left(\frac{\Lambda(s_1)}{|s_1|} + \frac{\Lambda(s_2)}{|s_2|}\right)\right) \\ &+ O_q\left((|a|+|b|)M^2\right), \end{aligned} \tag{3.6.4}$$

où s_1 et s_2 désignent respectivement les résidus de plus petit degré de $ba^{-1} \bmod m$ et de $ab^{-1} \bmod m$.

On prouve d'abord la première partie de la Proposition 3.6.1. On suppose que $\deg(a) = \deg(b)$. Ainsi, si $s_1 a = b$ alors $\Lambda(s_1) = 0$. Sinon, puisque $m|s_1 a - b$ alors $|s_1| \geq \frac{|m|}{(|a|+|b|)}$, donc $\frac{\Lambda(s_1)}{|s_1|} \ll_q \frac{(|a|+|b|)M}{|m|}$. On distingue alors de façon similaire les cas $s_2 b = a$, $s_2 b \neq a$ et il s'ensuit que $\frac{\Lambda(s_1)}{|s_1|} + \frac{\Lambda(s_2)}{|s_2|} \ll_q \frac{(|a|+|b|)M}{|m|}$.

Par conséquent, on déduit de la formule (3.6.4) que

$$B_m(a,b) = -\frac{q^2+q}{2(q-1)^2}\phi(m)l(a,b) + O_q\left((|a|+|b|)\,M^2\right).$$

On suppose maintenant que $\deg(a) \neq \deg(b)$. Sans perte de généralité, on suppose que $\deg(a) < \deg(b)$. Dans ce cas, on a nécessairement $s_2 b \neq a$. Ceci implique que $\frac{\Lambda(s_2)}{|s_2|} \ll_q \frac{(|a|+|b|)M}{|m|}$.
Si $a \nmid b$ alors $s_1 a \neq b$ donc $\frac{\Lambda(s_1)}{|s_1|} \ll_q \frac{(|a|+|b|)M}{|m|}$. Sinon $\frac{\Lambda(s_1)}{|s_1|} = \Lambda_0\left(\frac{b}{a}\right)$ avec $\frac{b}{a} \in \mathbb{F}_q[T]$. Donc

$$\frac{\Lambda(s_1)}{|s_1|} = \Lambda_0\left(\frac{b}{a}\right) + O_q\left(\frac{(|a|+|b|)\,M}{|m|}\right).$$

En combinant ces estimations avec la formule (3.6.4), on obtient la deuxième partie de la Proposition 3.6.1. □

Soit P' l'un des polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$ ayant le plus grand degré tel que $P'|m$. Soit P_0 l'un des polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$ ayant le plus petit degré tel que P_0 est un non-résidu quadratique modulo P'.
D'après [**Hsu98**, Corollaire 2.2] on a $\deg(P_0) \leq 2+2\log_q(1+\deg(m))$, donc $|P_0| \leq q^2(1+M)^2$.

Soit S l'ensemble des premiers $P \in \mathbb{F}_q[T]$ tels que $|P| \leq 2qM$ et $P \nmid m$. On définit le produit suivant :

$$Q := \prod_{|P|\leq 2qM} |P| = \exp\left(\log q\left(\sum_{1\leq \deg(P)\leq \lfloor \frac{\log(2qM)}{\log q}\rfloor} \deg(P)\right)\right).$$

Ainsi en utilisant (2.2.2), on obtient

$$Q = \exp\left(\log q\left(\frac{q^{\lfloor \frac{\log(2qM)}{\log q}\rfloor+1}}{q-1} + O\left(\sqrt{q}^{\lfloor \frac{\log 2qM}{\log q}\rfloor}\right)\right)\right) \geq |m|^2(1+o(1)).$$

De plus, on sait que $\prod\limits_{P\in S}|P| = \frac{Q}{\prod\limits_{\substack{|P|\leq 2qM\\ P|m}}|P|} \geq \frac{|m|^2(1+o(1))}{\prod\limits_{\substack{|P|\leq 2qM\\ P|m}}|P|}$ et $\prod\limits_{\substack{|P|\leq 2qM\\ P|m}}|P| \leq \prod\limits_{P|m}|P| \leq |m|$, donc $\prod\limits_{P\in S}|P| \geq |m|(1+o(1))$. Puisque $P \in S$ alors $|P| \leq 2qM$. Donc

$$(2qM)^{|S|} \geq |m|(1+o(1)).$$

Par conséquent

$$|S| \geq \frac{M}{\log(2qM)} \geq 2.$$

Donc il existe P_1, $P_2 \neq P_0$ deux polynômes irréductibles unitaires distincts dans $\mathbb{F}_q[T]$ tels que $|P_1|,|P_2| \leq 2qM$.
On démontre par la suite les Théorèmes 3.1.10, 3.1.11 et 3.1.15.

Démonstration du Théorème 3.1.10. Puisqu'on sait du [**CK10**, Théorème 2.3] que $\delta_{m;ba_1,\dots,ba_r} = \delta_{m;a_1,\dots,a_r}$ pour toute classe b modulo m, alors il suffit de construire des résidus quadratiques a_j modulo m. En effet, on prend $b_j = ba_j$ pour tout non-résidu quadratique b modulo m pour obtenir le résultat analogue pour les non-résidus quadratiques modulo m.

Soient $a_1 = 1, a_r = P_1^2$ et $a_j = (P_1P_2)^{2j}$ pour tout $2 \leq j \leq r-1$. Par conséquent, pour tout $1 \leq j \leq r$, on a $|a_j| \leq (2qM)^{4(r-1)}$. De plus, on a $P_1P_2 | a_k/a_j$ pour tout $1 \leq j < k \leq r-1$. Ainsi, de la partie 2 de la Proposition 3.6.1, on déduit

$$B_m(a_j,a_k) \ll_q M^{4r} \quad \text{pour } 1 \leq j < k \leq r-1.$$

En outre, puisque $a_r/a_1 = P_1^2$ alors en utilisant la partie 2 de la Proposition 3.6.1 on a

$$B_m(a_1,a_r) = -\frac{\phi(m)q}{(q-1)\log q}\frac{\log|P_1|}{|P_1|^2} + O_q\left(M^{4r}\right).$$

Il découle du [**Lam13**, Lemme 6.3] que

$$\beta_{r-1,r}(r) > 0, \quad \text{et} \quad \beta_{1,r}(r) < 0. \tag{3.6.5}$$

Par conséquent, en combinant ces estimations avec le Corollaire 3.1.8, le Lemme 3.2.3 et (3.6.5), on trouve

$$\delta_{m;a_1,\dots,a_r} = \frac{1}{r!} + \frac{\beta_{1,r}(r)B_m(a_1,a_r)}{N_m} + O_q\left(\frac{M^{4r}}{\phi(m)}\right) > \frac{1}{r!} + \frac{|\beta_{1,r}(r)|}{10q^2M^3}.$$

D'autre part, soit σ une permutation de l'ensemble $\{1,\dots,r\}$ définie par $\sigma(1) = r-1$, $\sigma(r-1) = 1$ et $\sigma(j) = j$ pour toutes les autres valeurs de j. Ainsi, on déduit de (3.6.5)

$$\delta_{m;a_{\sigma(1)},\dots,a_{\sigma(r)}} = \frac{1}{r!} + \frac{\beta_{r-1,r}(r)B_m(1,P_1^2)}{N_m} + O_q\left(\frac{M^{4r}}{\phi(m)}\right) < \frac{1}{r!} - \frac{|\beta_{r-1,r}(r)|}{10q^2M^3}.$$

□

Démonstration du Théorème 3.1.11. Soit $M = \deg(m)$. En combinant l'estimation $|C_m| = |m|^{o(1)}$, avec le Théorème 3.1.3 et le Corollaire 3.2.10 on obtient

$$\left|\delta_{m;a_1,\dots,a_r} - \frac{1}{r!}\right| \ll_r \frac{1}{M}.$$

On choisit maintenant $a_1 = 1, a_r = -1$ et $a_j = (P_1P_2)^{2j}$ pour $2 \leq j \leq r-1$. Il s'ensuit que $|a_j| \leq (2qM)^{4(r-1)}$ pour tout $1 \leq j \leq r$. On sait que $P_1P_2 | a_k/a_j$, donc en utilisant la partie 2 de la Proposition 3.6.1 on a

$$B_m(a_j,a_k) \ll_q M^{4r} \quad \text{pour } 1 \leq j < k \leq r-1.$$

Comme $P_1P_2 | a_j/a_r$ pour tout $2 \leq j \leq r-1$ alors

$$B_m(a_j,a_k) \ll_q M^{4r} \quad \text{pour } 2 \leq j \leq r-1.$$

En outre, il découle de la partie 1 de la Proposition 3.6.1 que

$$B_m(a_1,a_r) = -\frac{q^2+q}{2(q-1)^2}\phi(m) + O_q\left(M^2\right).$$

Ainsi, en combinant le Théorème 3.1.3 avec le Lemme 3.2.3 et (3.6.5) on obtient

$$\delta_{m;a_1,\ldots,a_r} = \frac{1}{r!} + \frac{\beta_{1,r}(r)B_m(a_1,a_r)}{N_m} + O_{\epsilon,q}\left(\frac{1}{\phi(m)^{1/2-\epsilon}}\right) > \frac{1}{r!} + \frac{|\beta_{1,r}(r)|(q^2+q)}{6(q-1)^2M}.$$

Donc

$$\delta_{m;a_1,\ldots,a_r} > \frac{1}{r!} + \frac{|\beta_{1,r}(r)|}{6M}.$$

Si l'on prend $b_1 = a_{r-1}$, $b_{r-1} = a_1$ et $b_j = a_j$ pour toutes les autres valeurs de j alors en utilisant (3.6.5) on déduit

$$\delta_{m;b_1,\ldots,b_r} = \frac{1}{r!} + \frac{\beta_{r-1,r}(r)B_m(b_{r-1},b_r)}{N_m} + O_{\epsilon,q}\left(\frac{1}{\phi(m)^{1/2-\epsilon}}\right) < \frac{1}{r!} - \frac{|\beta_{r-1,r}(r)|(q^2+q)}{6(q-1)^2M}.$$

D'où

$$\delta_{m;b_1,\ldots,b_r} < \frac{1}{r!} - \frac{|\beta_{r-1,r}(r)|}{6M}.$$

□

Démonstration du Théorème 3.1.15. Soit $M = \deg(m)$. Comme $(\kappa_1,\ldots,\kappa_r) \neq (0,\ldots,0)$ alors il existe $1 \leq l \leq r$ tel que $\kappa_l \neq 0$.

Cas 1 : $\kappa_r \neq 0$ ou $\kappa_1 \neq 0$.

On ne traite que le cas $\kappa_r \neq 0$, puisque le cas $\kappa_1 \neq 0$ se déduit simplement en échangeant a_1 avec a_r, et b_1 avec b_r dans chaque construction qu'on fait ci-dessous.

On suppose que $\kappa_r > 0$. Dans ce cas, on prend $a_1 = 1, a_j = P_0\left(P_1P_2\right)^{2j}$ pour $2 \leq j \leq r-1$, et $a_r = \left(P_1P_2\right)^2$. Donc a_1 et a_r sont des résidus quadratiques modulo m et a_j est un non-résidu quadratique modulo m pour $2 \leq j \leq r-1$. On choisit $b_j = a_j$ pour tout $1 \leq j \leq r-1$ et $b_r = P_0$. Dans ce cas, b_1 est le seul résidu quadratique parmi les b_j modulo m. Puisque $C_m(1) > -1$ il s'ensuit

$$\sum_{j=1}^{r} \kappa_j C_m(a_j) - \sum_{j=1}^{r} \kappa_j C_m(b_j) = \kappa_r C_m(a_r) - \kappa_r C_m(b_r) = \kappa_r(C_m(1)+1) > 0.$$

On sait que $|a_j| \ll q^2M^2\left(2qM\right)^{4(r-1)}$ pour tout $1 \leq j \leq r$, et que P_1P_2 divise $\mathbf{Pmax}(a_j,a_k)/\mathbf{Pmin}(a_j,a_k)$ pour tout $1 \leq j < k \leq r$. Alors en utilisant la partie 2 de la Proposition 3.6.1, on obtient

$$|B_m(a_j,a_k)| \ll_q M^{4r+1} \text{ pour tout } 1 \leq j < k \leq r.$$

D'où par le Théorème 3.1.3 on déduit que

$$\delta_{m;a_1,\ldots,a_r} = \frac{1}{r!} + O_{\epsilon,q}\left(\frac{1}{\phi(m)^{1/2-\epsilon}}\right). \tag{3.6.6}$$

De même, en utilisant la partie 2 de la Proposition 3.6.1 on obtient $|B_m(b_j,b_k)| \ll_q M^{4r+1}$ pour tout $1 \leq j < k \leq r$ avec $\{j,k\} \neq \{1,r\}$, et

$$B_m(b_1,b_r) = -\frac{q\phi(m)}{(q-1)\log q}\frac{\log|P_0|}{|P_0|} + O_q\left(M^{4r+1}\right).$$

En combinant le Théorème 3.1.3 avec (3.6.5) et (3.6.6) on trouve

$$\delta_{m;b_1,\dots,b_r} = \frac{1}{r!} + \frac{\beta_{1,r}(r)B_m(b_1,b_r)}{N_m} + O_{\epsilon,q}\left(\frac{1}{\phi(m)^{1/2-\epsilon}}\right) > \frac{1}{r!} + \frac{|\beta_{1,r}(r)|\log|P_0|}{2|P_0|(\log q)M} > \delta_{m;a_1,\dots,a_r}.$$

On suppose maintenant que $\kappa_r < 0$. Dans ce cas, on choisit $a_1 = 1$, et $a_j = P_0(P_1P_2)^{2j}$ pour tout $2 \leq j \leq r$ (dans ce cas a_1 est le seul résidu quadratique parmi les a_j modulo m), et $b_j = a_j$ pour tout $1 \leq j \leq r-1$, et $b_r = P_1^2$ (dans ce cas, b_1 et b_r sont des résidus quadratiques modulo m). Par conséquent, en utilisant des arguments similaires au cas $\kappa_r > 0$, on déduit du Théorème 3.1.3 et de la partie 2 de la Proposition 3.6.1 combinée avec (3.6.5) le résultat suivant :

$$\sum_{j=1}^{r}\kappa_j C_m(a_j) - \sum_{j=1}^{r}\kappa_j C_m(b_j) = -\kappa_r\left(1 + C_m(1)\right) > 0,$$

$$\delta_{m;a_1,\dots,a_r} = \frac{1}{r!} + O_{\epsilon,q}\left(\frac{1}{\phi(m)^{1/2-\epsilon}}\right),$$

et

$$\delta_{m;b_1,\dots,b_r} = \frac{1}{r!} + \frac{\beta_{1,r}(r)B_m(b_1,b_r)}{N_m} + O_{\epsilon,q}\left(\frac{1}{\phi(m)^{1/2-\epsilon}}\right) > \frac{1}{r!} + \frac{|\beta_{1,r}(r)|\log|P_1|}{2(\log q)|P_1|^2M} > \delta_{m;a_1,\dots,a_r}.$$

Cas 2 : Il existe $2 \leq l \leq r-1$ tel que $\kappa_l \neq 0$.

On suppose d'abord que $\kappa_l > 0$. On prend $a_1 = 1, a_l = (P_1P_2)^2$, $a_j = P_0\left(P_1P_2\right)^{4j}$ pour $2 \leq j \neq l \leq r$ et $b_r = P_0$, $b_l = P_0\left(P_1P_2\right)^{4l}$, et $b_j = a_j$ pour tout $1 \leq j \neq l \leq r-1$. Ainsi, en utilisant des arguments similaires au cas 1, et si M est suffisamment grand on obtient

$$\sum_{j=1}^{r}\kappa_j C_m(a_j) - \sum_{j=1}^{r}\kappa_j C_m(b_j) = \kappa_l\left(C_m(1)+1\right) > 0, \quad \text{et} \quad \delta_{m;b_1,\dots,b_r} > \delta_{m;a_1,\dots,a_r}.$$

Autrement, si $\kappa_l < 0$, on choisit $a_1 = 1, a_r = \left(P_1P_2\right)^4$, $a_j = P_0\left(P_1P_2\right)^{4j}$ pour $2 \leq j \leq r-1$, $b_l = \left(P_1P_2\right)^4, b_r = P_1^2$ et $b_j = a_j$ pour les autres valeurs de j, ce qui conduit au résultat attendu. □

3.7. Courses extrêmement biaisées

Le but de cette section est de démontrer le Théorème 3.1.13. Pour ce faire, nous adapterons la démonstration du [**Lam13**, Théorème 2.6]. L'idée est de déterminer, pour $\deg(m)$ suffisamment grand, quand le terme $B_m(a_i,a_j)$ contribue largement à la densité $\delta_{m;a_1,\dots,a_r}$. Nous commencerons par réduire l'étude au cas $r = 3$ qui est traité dans le lemme suivant :

Lemme 3.7.1. *On fixe un entier $r \geq 3$, et $a_1,\ldots,a_r$ des polynômes deux à deux distincts dans $\mathbb{F}_q[T]$. Soit M_0 un entier assez grand. On considère l'ensemble Z_{M_0} des polynômes $m \in \mathcal{M}_q$ tels que $(m,a_i)=1$ pour tout $1 \leq i \leq r$ et $\deg(m) \geq M_0$. On suppose que (LI ★) est vraie pour $m \in Z_{M_0}$. S'il existe $1 \leq i_1 < i_2 < i_3 \leq r$ tels que la course $\{Z_{M_0}; a_{i_1},a_{i_2},a_{i_3}\}$ est extrêmement biaisée, alors la course $\{Z_{M_0}; a_1,\ldots,a_r\}$ est également extrêmement biaisée.*

Démonstration. Supposons qu'il existe $1 \leq i_1 < i_2 < i_3 \leq r$ tels que la course $\{Z_{M_0}; a_{i_1},a_{i_2},a_{i_3}\}$ est extrêmement biaisée. Il s'ensuit qu'il existe une permutation ν de l'ensemble $\{i_1,i_2,i_3\}$ et une constante $C(q,3,Z_{M_0}) > 0$ qui ne dépend que de q et Z_{M_0} tel qu'on ait pour tout $m \in Z_{M_0}$

$$\left|\delta_{m;a_{\nu(i_1)},a_{\nu(i_2)},a_{\nu(i_3)}} - \frac{1}{6}\right| \geq \frac{C(q,3,Z_{M_0})}{\log|m|}.$$

Soit $j_l = \nu(i_l)$ pour $l \in \{1,2,3\}$. On considère S l'ensemble des permutations σ de $\{1,2,\ldots,r\}$ telles qu'il existe $1 \leq i < k < l \leq r$ vérifiant $\sigma(i)=j_1$, $\sigma(k)=j_2$, et $\sigma(l)=j_3$.
Soit $m \in Z_{M_0}$. On note $H_{m;a_j,a_k}$ l'ensemble de tous les entiers positifs X tels que

$$\sum_{N=1}^{X} \pi_q(a_j,m,N) = \sum_{N=1}^{X} \pi_q(a_k,m,N).$$

On remarque que si (LI★) est vraie alors la densité naturelle de $H_{m;a_j,a_k}$ vaut 0 si $j \neq k$. D'où

$$\delta_{m;a_{j_1},a_{j_2},a_{j_3}} = \sum_{\sigma\in S} \delta_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}}.$$

En plus, comme $|S| = \frac{r!}{3!}$ alors

$$\begin{aligned}\frac{C(q,3,Z_{M_0})}{\log|m|} &\leq \left|\delta_{m;a_{j_1},a_{j_2},a_{j_3}} - \frac{1}{6}\right| \leq \sum_{\sigma\in S}\left|\delta_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}} - \frac{1}{r!}\right|,\\ &\leq \frac{r!}{6}\max_{\sigma\in S}\left|\delta_{m;a_{\sigma(1)},a_{\sigma(2)},\ldots,a_{\sigma(r)}} - \frac{1}{r!}\right|.\end{aligned}$$

Donc il existe une permutation σ de l'ensemble $\{1,2,\ldots,r\}$ et une constante $D(q,r,Z_{M_0}) > 0$ qui ne dépend que de q,r et Z_{M_0} et qui vérifient l'inégalité suivante :

$$\frac{D(q,r,Z_{M_0})}{\log|m|} \leq \left|\delta_{m;a_{\sigma(1)},a_{\sigma(2)},\ldots,a_{\sigma(r)}} - \frac{1}{r!}\right|,$$

ce qui implique que la course $\{Z_{M_0}; a_1,\ldots,a_r\}$ est extrêmement biaisée. □

Nous établirons par la suite quelques propriétés liées à la fonction $\Lambda_0(f)$ définie dans (3.6.1).

Lemme 3.7.2. *Le maximum de $\Lambda_0(f)$ dans $\mathbb{F}_q[T]$ est inférieur ou égal à* $\log(3)/3$.

Démonstration. Il est clair que $\Lambda_0(f) \neq 0 \Leftrightarrow f = P^l$, où $P \in \mathcal{P}_q$, et $l \in \mathbb{N}^*$. Dans ce cas, puisque $|P| = q^{\deg(P)} \geq 3$ alors il s'ensuit que

$$\Lambda_0(f) = \frac{\log|P|}{|P|^l} \leq \frac{\log|P|}{|P|} \leq \frac{\log 3}{3}.$$

□

Lemme 3.7.3. *Soient a_1,a_2,a_3 des éléments de $\mathbb{F}_q[T]$ qui sont premiers avec m, représentant des classes de résidus distinctes modulo m et de degrés distincts. On définit*

$$X_1 = \frac{\mathbf{Pmax}(a_1,a_2)}{\mathbf{Pmin}(a_1,a_2)},\ X_2 = \frac{\mathbf{Pmax}(a_2,a_3)}{\mathbf{Pmin}(a_2,a_3)},\ \textit{et}\quad X_3 = \frac{\mathbf{Pmax}(a_1,a_3)}{\mathbf{Pmin}(a_1,a_3)}.$$

Si une des valeurs $\Lambda_0(X_1)$, $\Lambda_0(X_2)$, $\Lambda_0(X_3)$ est non nulle alors il existe une permutation σ de $\{1,2,3\}$ telle que

$$\Lambda_0(X_{\sigma(1)}) + \Lambda_0(X_{\sigma(2)}) - 2\Lambda_0(X_{\sigma(3)}) \neq 0.$$

Démonstration. On suppose sans perte de généralité que $|a_1| > |a_2| > |a_3|$ (puisque a_1,a_2,a_3 jouent un rôle symétrique dans la preuve). Donc dans ce cas, on obtient $X_1 = \frac{a_1}{a_2}$, $X_2 = \frac{a_2}{a_3}$, $X_3 = \frac{a_1}{a_3}$. On suppose que pour toutes les permutations σ de l'ensemble $\{1,2,3\}$ on a $\Lambda_0(X_{\sigma(1)}) + \Lambda_0(X_{\sigma(2)}) - 2\Lambda_0(X_{\sigma(3)}) = 0$, alors il s'en suit que $\Lambda_0(X_1) = \Lambda_0(X_2) = \Lambda_0(X_3)$. Comme cette valeur est non nulle, il en découle que $X_1 = P^k$ et $X_2 = Q^j$ où k,$j \geq 1$ sont deux entiers et P,$Q \in \mathcal{P}_q$.
Puisque $X_3 = X_1X_2 = P^kX_2$ et $\Lambda_0(X_3) \neq 0$ alors $X_3 = P^{k+a}$ avec a un entier positif. D'où $\frac{\log|P|}{|P|^k} = \frac{\log|P|}{|P|^{k+a}}$, ce qui est possible si et seulement si $a = 0$. Ainsi $a = 0$, donc $X_1 = X_3$ et $X_2 = 1$, d'où $\Lambda_0(X_2) = 0$, et ainsi $\Lambda_0(X_1) = \Lambda_0(X_2) = \Lambda_0(X_3) = 0$.
Cependant, ce dernier résultat est en contradiction avec l'hypothèse affirmant que l'une des valeurs de $\Lambda_0(X_1), \Lambda_0(X_2), \Lambda_0(X_3)$ est non nulle. □

L'étape suivante consiste à observer ce qui arrive à la contribution principale de $B_m(a,b)$ lorsque $\deg(a), \deg(b)$ sont relativement petits par rapport à $M = \deg(m)$ et $\mathbf{Pmax}(a,b)/\mathbf{Pmin}(a,b)$ est égal à une puissance d'un premier. Ceci nous permet de démontrer le Théorème 3.1.13.

Démonstration du Théorème 3.1.13. Supposons d'abord que ni (1) ni (2) ne sont valables. Dans ce cas, d'après la Proposition 3.6.1 on obtient que $B_m(a_j,a_k) = O_{A,q}(M^2)$ pour tout $1 \leq j < k \leq r$ et tout $m \in Z_{M_0}$. Par conséquent, dans le cas où les a_i sont tous des résidus quadratiques modulo m (ou tous des non-résidus quadratiques modulo m), il découle du Corollaire 3.1.8 que $\left|\delta_{m;a_1,\ldots,a_r} - \frac{1}{r!}\right| \ll_{A,r,q} \frac{M^2}{|m|}$. De plus, si la dernière condition n'est pas vérifiée, alors on déduit du Théorème 3.1.3 que $\left|\delta_{m;a_1,\ldots,a_r} - \frac{1}{r!}\right| \ll_{\epsilon,r,q} |m|^{-1/2+\epsilon}$.
Ainsi, dans les deux cas, la course $\{Z_{M_0}; a_1, \ldots, a_r\}$ n'est pas extrêmement biaisée.

Ensuite, supposons qu'il existe $1 \leq j \neq k \leq r$ tel que $a_j = -a_k = a$. Puisque $r \geq 3$ alors il existe $b \in \{a_1, \ldots, a_r\}$ tel que $b \neq a$ et $b \neq -a$. D'après le Lemme 3.7.1, il suffit de prouver que la course $\{Z_{M_0}; a, -a, b\}$ est extrêmement biaisée. Afin de démontrer ceci, nous allons distinguer deux cas.

Cas 1 : Supposons que $\deg(a) \neq \deg(b)$. Soit $m \in Z_{M_0}$. Puisque M_0 est suffisamment grand, alors d'après la partie 2 de la Proposition 3.6.1 et le Lemme 3.7.2 on a

$$B_m(a,b) = -\frac{q}{(q-1)\log q}\phi(m)\Lambda_0\left(\frac{\mathbf{Pmax}(a,b)}{\mathbf{Pmin}(a,b)}\right) + O_{A,q}\left(M^2\right) \geq -\frac{\log 3}{3}\frac{q}{(q-1)\log q}\phi(m) + O_{A,q}\left(M^2\right).$$

La même formule est valable pour $B_m(b,-a)$. De plus, puisque $\deg(a) = \deg(-a)$, il découle de la partie 1 de la Proposition 3.6.1 que

$$B_m(a,-a) = -\frac{q^2+q}{2(q-1)^2}\phi(m) + O_{A,q}\left(M^2\right). \tag{3.7.1}$$

En outre, d'après le Corollaire 3.1.7 combiné au fait que $|C_m(a)| = |m|^{o(1)}$ et le Lemme 3.2.3 on a

$$\delta_{m;a,b,-a} \geq \frac{1}{6} + \frac{\frac{-2q}{(q-1)\log q}\frac{\log 3}{3} + \frac{q^2+q}{(q-1)^2}}{16\pi\sqrt{3}M}.$$

Comme $\frac{q^2+q}{(q-1)^2} \geq 1$ et $\frac{q}{(q-1)\log q} \leq \frac{4}{3\log 4}$ pour tout $q \geq 4$ alors $\frac{-2q}{(q-1)\log q}\frac{\log 3}{3} + \frac{q^2+q}{(q-1)^2} \geq 1 - \frac{4\log 3}{9\log 2}$ pour tout $q \geq 4$. En plus, lorsque $q = 3$ on a que $\frac{-2q}{(q-1)\log q}\frac{\log 3}{3} + \frac{q^2+q}{(q-1)^2} = 2$. Ainsi, dans tous les cas

$$\delta_{m;a,b,-a} \geq \frac{1}{6} + \frac{1 - \frac{4\log 3}{9\log 2}}{16\pi\sqrt{3}M}.$$

Il existe donc une constante $D(q,3) > 0$ telle que

$$\delta_{m;a,b,-a} - \frac{1}{6} \geq \frac{D(q,3)}{\log|m|},$$

ce qui montre que la course $\{Z_{M_0}; a, -a, b\}$ est extrêmement biaisée, puisque M_0 est suffisamment grand.

Cas 2 : Supposons que $\deg(a) = \deg(b)$. Soit $m \in Z_{M_0}$. Comme $b \neq a$ et $b \neq -a$, alors d'après la partie 1 de la Proposition 3.6.1, on obtient

$$B_m(a,b), B_m(b,-a) = O_{A,q}\left(M^2\right),$$

et l'expression de $B_m(a,-a)$ est la même que dans (3.7.1), donc

$$\delta_{m;a,b,-a} \geq \frac{1}{6} + \frac{1}{16\pi\sqrt{3}M}.$$

Ainsi, la course $\{Z_{M_0}; a, -a, b\}$ est extrêmement biaisée, puisque M_0 est suffisamment grand.

Supposons maintenant que $a_i \neq -a_j$ pour tout $1 \leq i < j \leq r$ et qu'il existe $b_1, b_2 \in \{a_1, \ldots, a_r\}$ tels que $b_1 = P^k b_2$ avec $P \in \mathcal{P}_q$ et k un entier positif. Dans ce cas,

on déduit de la partie 2 de la Proposition 3.6.1 que pour tout $m \in Z_{M_0}$, on a

$$B_m(b_1,b_2) = -\phi(m)\frac{q}{(q-1)\log q}\frac{\log|P|}{|P|^k} + O_{A,q}\left(M^2\right). \tag{3.7.2}$$

Puisque $r \geq 3$ alors il existe $b_3 \in \{a_1,\ldots,a_r\}$ avec $b_3 \neq b_i$ pour $i = 1,2$. On distingue deux sous cas :

Sous-cas 1 : Supposons qu'il existe $1 \leq i \neq j \leq 3$ tel que $\deg(b_i) = \deg(b_j)$. Sans perte de généralité, supposons que $\deg(b_3) = \deg(b_1)$. Puisque $b_1 \neq -b_3$ alors

$$B_m(b_1,b_3) \ll_{A,q} M^2.$$

Si b_3/b_2 est une puissance d'un premier, alors on a $b_3/b_2 = Q^j$ où j est un entier positif et Q est un nombre premier. Dans ce cas, d'après la partie 2 de la Proposition 3.6.1, on a

$$B_m(b_2,b_3) = -\phi(m)\frac{q}{(q-1)\log q}\frac{\log|Q|}{|Q|^j} + O_{A,q}\left(M^2\right). \tag{3.7.3}$$

Par conséquent, en insérant (3.7.2) et (3.7.3) dans le Corollaire 3.1.7, il découle du Lemme 3.2.3 l'estimation suivante :

$$\delta_{m;b_1,b_2,b_3} = \frac{1}{6} - \frac{1}{4\pi\sqrt{3}(\log q)M}\left(\frac{\log|P|}{|P|^k} + \frac{\log|Q|}{|Q|^j}\right)(1+o(1)).$$

Par conséquent, comme dans le cas 1, il s'ensuit que la course $\{Z_{M_0}; b_1,b_2,b_3\}$ est extrêmement biaisée.

Sous-cas 2 : Supposons que $\deg(b_1), \deg(b_2), \deg(b_3)$ sont deux à deux distincts. Soit S_3 l'ensemble des permutations de l'ensemble $\{1,2,3\}$. Puisque $\Lambda_0(b_1/b_2) \neq 0$, alors le Lemme 3.7.3 montre qu'il existe $\sigma \in S_3$ tel que

$$\Lambda_0(X_{\sigma(1)}) + \Lambda_0(X_{\sigma(2)}) - 2\Lambda_0(X_{\sigma(3)}) \neq 0,$$

avec

$$X_1 = \frac{b_1}{b_2},\ X_2 = \frac{\mathbf{Pmax}(b_2,b_3)}{\mathbf{Pmin}(b_2,b_3)},\ X_3 = \frac{\mathbf{Pmax}(b_1,b_3)}{\mathbf{Pmin}(b_1,b_3)}.$$

Par conséquent, en utilisant le Corollaire 3.1.7 et la Proposition 3.6.1, on déduit qu'il existe une constante $D(q,3) > 0$ telle que

$$\max_{\nu\in S_3}\left|\delta_{m;b_{\nu(1)},b_{\nu(2)},b_{\nu(3)}} - \frac{1}{6}\right| \geq \frac{D(q,3)}{\log|m|}.$$

Il s'ensuit que la course $\{Z_{M_0}; b_1,b_2,b_3\}$ est extrêmement biaisée. La preuve du Théorème 3.1.13 découle du Lemme 3.7.1. □

3.8. Exemples de courses dans le cas où (LI ★) est fausse

Dans ce qui suit, nous donnerons quelques exemples de courses de nombres premiers dans les corps de fonctions. Nous démontrerons que lorsque (LI ★) est fausse, les comportements des courses peuvent être différents de ceux lorsque (LI ★) est valide.

Nous commencerons par préciser la méthode qui permet de calculer certaines densités utilisées dans les exemples qui vont suivre.

Soit $a \in \mathbb{F}_q[T]$ tel que $(a,m) = 1$. Nous rappellons que pour tout $X \in \mathbb{N}^*$ on a :

$$E_{m;a}(X) = \frac{X}{q^{X/2}} \sum_{N=1}^{X} \left(\phi(m)\pi_q(a,m,N) - \pi_q(N)\right). \tag{3.8.1}$$

Remarque 3.8.1. *Soit r un entier ≥ 2, $(a_1,\dots,a_r) \in \mathcal{A}_r(m)$ et $X \in \mathbb{N}^*$ Alors*

$$E_{m;a_1}(X) > \cdots > E_{m;a_r}(X) \Leftrightarrow \sum_{N=1}^{X} \pi_q(a_1,m,N) > \cdots > \sum_{N=1}^{X} \pi_q(a_r,m,N).$$

Donc si $\delta_{m;a_1,\dots,a_r}$ existe alors elle vaut

$$\delta_{m;a_1,\dots,a_r} = \lim_{X\to+\infty} \frac{\#\{S \in [\![1,X]\!] : E_{m;a_1}(S) > \cdots > E_{m;a_r}(S)\}}{X}.$$

Soit r un entier ≥ 2 et $(a_1,\dots,a_r) \in \mathcal{A}_r(m)$. Il est facile de prouver que si pour tout $i \in [\![1,r]\!]$ $E_{m;a_i}$ a une période entière U_{a_i} alors la densité $\delta_{m;a_1,\dots,a_r}$ existe et elle vaut :

$$\delta_{m;a_1,\dots,a_r} = \frac{\#\{X \in [\![1, \vee_{i=1}^r U_{a_i}]\!] : E_{m;a_1}(X) > \cdots > E_{m;a_r}(X)\}}{\vee_{i=1}^r U_{a_i}},$$

où $\vee_{i=1}^r U_{a_i}$ est le ppcm de $U_{a_1},\dots,U_{a_r}$. Pour calculer les $E_{m;a_i}(X)$, l'usage de la formule (3.8.1) n'est pas judicieux car il est impératif de calculer les nombres $\pi(a_i,m,N)$ qui sont de l'ordre de grandeur de q^N/N ce qui prend énormément de temps lorsque N est grand indépendemment du degré de m. C'est pour cette raison que nous avons préféré faire usage de la formule (2.3.1) qui affirme que pour $X \in \mathbb{N}^*$ nous avons :

$$E_{m;a}(X) = -C_m(a)\mathcal{B}_q(X) - \sum_{\chi\neq\chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1),$$

où :

$$\mathcal{B}_q(X) := \begin{cases} \frac{\sqrt{q}}{q-1} & \text{si} \quad X \text{ est impair,} \\ \frac{q}{q-1} & \text{si} \quad X \text{ est pair.} \end{cases}$$

Nous avons alors pour tout $X \in \mathbb{N}^*$, $E_{m,a}(X) = S_{m;a}(X) + o(1)$ avec

$$S_{m;a}(X) := -C_m(a)\mathcal{B}_q(X) - \sum_{\chi\neq\chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1},$$

la partie principale de $E_{m;a}(X)$.

Remarque 3.8.2. *Ce choix ne permet pas de connaître exactement si les fonctions E_{m,a_i} ont une période entière ou pas. Ceci est dû à l'erreur $o(1)$. De plus, même si nous trouvons que pour $X \in \mathbb{N}^*$ on a $S_{m;a_i}(X) = S_{m;a_{i+1}}(X)$ pour $i \in [\![1, r-1]\!]$ nous ne pouvons pas déduire une inégalité ou une égalité entre les termes $E_{m,a_i}(X)$ et $E_{m,a_{i+1}}(X)$.*

Supposons maintenant que pour tout $i \in [\![1,r]\!]$, $S_{m;a_i}$ a une période entière U_{a_i}. Si pour tout $X \in [\![1, \vee_{j=1}^{r} U_{a_i}]\!]$ on a $S_{m;a_k}(X) \neq S_{m;a_{k+1}}(X)$ pour tout $k \in [\![1,r-1]\!]$ alors :

$$\delta_{m;a_1,\ldots,a_r} = \frac{\#\{X \in [\![1, \vee_{i=1}^{r} U_{a_i}]\!] : S_{m;a_1}(X) > \cdots > S_{m;a_r}(X)\}}{\vee_{i=1}^{r} U_{a_i}} \tag{3.8.2}$$

Il s'est avéré que nous pouvons rarement affirmer numériquement que les $S_{m;a_i}$ ont une période entière et il est plus simple de vérifier si cette hypothèse est vraie ou fausse quand $\deg(m)$ est petit. C'est pour cette raison que nous nous sommes focalisés sur les polynômes unitaires $m \in \mathbb{F}_q[T]$ de petit degré.

Exemple 3.8.3. *Soit $m = T^2 + T + 1 \in \mathbb{F}_3[T]$. Un simple calcul nous permet d'affirmer que $m = (T+2)^2$ donc m est réductible et $\phi(m) = 9 - 3 = 6$. Dans ce cas, $(\mathbb{F}_3[T]/(m))^\times$ est cyclique et nous vérifions facilement que $T+1$ est un générateur de $(\mathbb{F}_3[T]/(m))^\times$. Plus précisément, nous avons $(T+1)^2 \equiv T \bmod m$, $(T+1)^3 \equiv -1 \bmod m \equiv 2 \bmod m$, $(T+1)^4 \equiv 2T+2 \bmod m$, $(T+1)^5 \equiv 2(T+1)^2 \bmod m \equiv 2T \bmod m$ et finalement $(T+1)^6 \equiv -T^2 - T \bmod m \equiv 1 \bmod m$.*

Les caractères de Dirichlet modulo m sont alors entièrement déterminés par la connaissance de l'image du générateur $T+1$. Par conséquent, la table des caractères de $(\mathbb{F}_3[T]/(m))^\times$ est :

	1	2	T	$T+1$	$2T$	$2T+2$
χ_0	1	1	1	1	1	1
χ_1	1	-1	$\frac{-1+\sqrt{3}i}{2}$	$\frac{1+\sqrt{3}i}{2}$	$\frac{1-\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$
χ_2	1	1	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$
χ_3	1	-1	1	-1	-1	1
χ_4	1	1	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$
χ_5	1	-1	$\frac{-1-\sqrt{3}i}{2}$	$\frac{1-\sqrt{3}i}{2}$	$\frac{1+\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$

Tableau 3. Table de caractères de $(\mathbb{F}_3[T]/(m))^\times$.

Ainsi, en utilisant le fait que nous avons $\mathcal{L}(u,\chi_i) = 1 + (\chi_i(T) + \chi_i(T+1))u$ pour tout $1 \leq i \leq 5$, nous obtenons $\mathcal{L}(u,\chi_1) = (\sqrt{3}i)u + 1$, $\mathcal{L}(u,\chi_2) = \mathcal{L}(u,\chi_4) = -u + 1$, $\mathcal{L}(u,\chi_3) = 1$ et $\mathcal{L}(u,\chi_5) = (-\sqrt{3}i)u + 1$. Donc le seul zéro inversé des fonctions L associées aux caractères χ_2 et χ_4 est 1 et il n'y a pas de zéro inversé pour la fonction L associée à χ_3. Finalement, les seuls zéros inversés associés aux caractères χ_1 et χ_5 sont respectivement $\sqrt{3}e^{-i\frac{\pi}{2}}$ et $\sqrt{3}e^{i\frac{\pi}{2}}$. Par conséquent, le seul zéro inversé de toutes les fonctions L ci-dessus dont le module est

$\sqrt{3}$ *et dont l'argument est compris entre* 0 *et* π *est* $\gamma_5 = \sqrt{3}e^{i\frac{\pi}{2}}$, *donc (LI* ★*) est fausse.*
En utilisant la formule (2.3.1), *pour tout* $a \in \mathbb{F}_3[T]$ *tel que* $(a,m) = 1$ *on a*

$$E_{m;a}(X) = -C_m(a)\mathcal{B}_q(X) - \sum_{\chi\neq\chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1),$$

où $\gamma_\chi = \sqrt{3}e^{i\theta(\chi)}$ *un zéro inversé de* $\mathcal{L}(u,\chi)$ *dont le module est* $\sqrt{3}$ *et* $X \in \mathbb{N}^*$. *Dans ce cas, nous pouvons facilement vérifier que* $S_{m;a}(X+4) = S_{m;a}(X)$ *pour* $X \in \mathbb{N}^*$.
Ensuite, en utilisant la formule précédente, nous obtenons le tableau suivant :

X *mod* 4	$S_{m;T}(X)$	$S_{m;T+1}(X)$	$S_{m;2T}(X)$	$S_{m;2}(X)$
1	$\sqrt{3}/2$	$\sqrt{3}$	$-\sqrt{3}/2$	$\sqrt{3}$
2	$-3/2$	3	$3/2$	0
3	$-3\sqrt{3}/2$	0	$3\sqrt{3}/2$	0
4	$-3/2$	0	$3/2$	3

Tableau 4. Les valeurs de $S_{m;a}(X)$ pour $a \in \{T, T+1, 2T, 2\}$.

Nous déduisons que $\delta_{m;T+1,2T,2} = \frac{1}{4}$.
Nous remarquons que $2 \equiv -1 \bmod m$ *donc* $2T \equiv -T \bmod m$ *et on a* $2T^2 \equiv -T^2 \bmod m \equiv T+1 \bmod m$ *d'où* $-T^3 \equiv T(T+1) \bmod m \equiv -1 \bmod m$. *Ainsi, pour* $\rho = T \in \mathbb{F}_3[T]$, $a_1 = 2 \in \mathbb{F}_3[T], a_2 = 2T \in \mathbb{F}_3[T]$ *et* $a_3 = T+1 \in \mathbb{F}_3[T]$, *il s'en suit :*

$$\rho^3 \equiv 1 \bmod m, \quad a_2 \equiv a_1\rho \bmod m, \quad a_3 \equiv a_1\rho^2 \bmod m, \quad et \quad \rho \not\equiv 1 \bmod m.$$

D'autre part, nous avons montré que

$$\delta_{m;a_3,a_2,a_1} = \frac{1}{4} \neq \frac{1}{6}.$$

Ce qui implique que la course $\{m; a_1,a_2,a_3\}$ *est biaisée. Par conséquent,* [**Cha08**, le Théorème 6.1] *n'est pas toujours vraie quand (LI* ★*) n'est pas vérifiée.*

Exemple 3.8.4. *Avec le même* m, *nous pouvons trouver* $a_1, a_2 \in \mathbb{F}_3[T]$ *représentant des classes distinctes dans* $(\mathbb{F}_3[T]/(m))^\times$ *tels que* $\delta_{m;a_1,a_2} = 0$,. *En effet, par le tableau 4, nous pouvons voir que* $E_{m;T}(X) < E_{m;T+1}(X)$ *pour tous les entiers positifs suffisamment grands* X, *ce qui implique que* $\sum_{N=1}^{X} \pi_q(T,m,N) < \sum_{N=1}^{X} \pi_q(T+1,m,N)$. *Donc*

$$\delta_{m;T,T+1} = 0.$$

En particulier, nous obtenons que $\delta_{m;T,T+1,2T} = 0$.

Remarque 3.8.5. *En* 1914, *Littlewood a prouvé que* $\pi(x;4,3) - \pi(x;4,1)$ *change de signe pour une infinité d'entiers positifs* x. *L'exemple 3.8.4 réfute une généralisation du théorème de*

Littlewood [**Lit14**] *dans les corps de fonctions puisque* $\sum_{N=1}^{X} \pi_q(T,m,N) < \sum_{N=1}^{X} \pi_q(T+1,m,N)$ *pour tous les nombres entiers positifs suffisamment grands* X.

En outre, nous choisissons $a_1 = T+1$, $a_2 = T$ *et* $a_3 = 2$ *dans* $(\mathbb{F}_3[T]/(m))^\times$. *Nous déduisons alors du tableau 4 que* $\delta_{m;a_1,a_2} = 1$ *mais* $\delta_{m;a_1,a_2,a_3} = 0$.

Exemple 3.8.6. *Soit* $m = (T+1)^2 \in \mathbb{F}_3[T]$. *Il est clair que* $\phi(m) = 6$ *et* $(\mathbb{F}_3[T]/(m))^\times$ *est cyclique. En utilisant le fait que* T *est un générateur de* $(\mathbb{F}_3[T]/(m))^\times$, *nous obtenons facilement le tableau suivant :*

	1	2	T	$T+1$	$2T$	$2T+2$
χ_0	1	1	1	1	1	1
χ_1	1	-1	$\frac{1+\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$	$\frac{1-\sqrt{3}i}{2}$
χ_2	1	1	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$
χ_3	1	-1	-1	1	1	-1
χ_4	1	1	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$
χ_5	1	-1	$\frac{1-\sqrt{3}i}{2}$	$\frac{-1-\sqrt{3}i}{2}$	$\frac{-1+\sqrt{3}i}{2}$	$\frac{1+\sqrt{3}i}{2}$

Tableau 5. Table de caractères de $(\mathbb{F}_3[T]/(m))^\times$.

Par conséquent, nous avons $\mathcal{L}(u,\chi_1) = 1 + (\sqrt{3}i)u$, $\mathcal{L}(u,\chi_2) = \mathcal{L}(u,\chi_4) = 1-u$, $\mathcal{L}(u,\chi_3) = 1$ *et* $\mathcal{L}(u,\chi_5) = 1 - (\sqrt{3}i)u$. *Ainsi, le seul zéro inversé de toutes les fonctions* L *ci-dessus dont le module est* $\sqrt{3}$ *et dont l'argument est compris entre* 0 *et* π *est* $\gamma_5 = \sqrt{3}e^{i\frac{\pi}{2}}$. *D'où (LI* $\bigstar$*) est fausse.*
Soit $a \in \mathbb{F}_3[T]$ *tel que* $(a,m) = 1$. *Grâce à la formule* (2.3.1), *nous avons pour tout* $X \in \mathbb{N}^*$

$$E_{m;a}(X) = -C_m(a)\mathcal{B}_q(X) - 2\Re\left(\overline{\chi_5}(a)\frac{\sqrt{3}i}{\sqrt{3}i-1}e^{i\frac{\pi}{2}X}\right) + o(1).$$

En utilisant cette dernière formule, un simple calcul nous permet de vérifier que pour tout $X \in \mathbb{N}^*$ *nous avons* $S_{m;a}(X) = S_{m;a}(X+4)$. *Nous obtenons par la suite le tableau suivant :*

$X \bmod 4$	$S_{m;1}(X)$	$S_{m;T}(X)$	$S_{m;T+2}(X)$	$S_{m;2T+1}(X)$
1	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}/2$	$-\sqrt{3}/2$
2	0	3	$-3/2$	$3/2$
3	0	0	$-3\sqrt{3}/2$	$3\sqrt{3}/2$
4	-3	0	$-3/2$	$3/2$

Tableau 6. Les valeurs de $S_{m;a}(X)$ pour $a \in \{1, T, T+2, 2T+1\}$.

Nous avons donc

$$\delta_{m;1,2T+1} = 0.$$

Cependant, nous ne pouvons pas affirmer que si a_1 *est un résidu quadratique dans* $(\mathbb{F}_3[T]/(m))^\times$ *et* a_2 *est un non-résidu quadratique dans* $(\mathbb{F}_3[T]/(m))^\times$ *alors* $\delta_{m;a_1,a_2} = 0$. *En*

effet, nous avons :

$$\delta_{m;T+2,2T+1} = \frac{1}{4}.$$

Mais $\delta_{m;T+2,2T+1,T} = 0$. *Dans ce cas, nous pouvons toujours trouver* $(a_1, a_2, a_3, a_4, a_5) \in \mathcal{A}_5(m)$ *tel que* $\delta_{m;a_1,a_2,a_3,a_4,a_5} = 0$.

Remarque 3.8.7. *Soit* $m = (T+1)^2 \in \mathbb{F}_3[T]$ *et* $(a,m) = 1$. *Nous définissons pour tout entier* $N \in \mathbb{N}^*$, *la quantité suivante :*

$$W_{m;a}(N) := \frac{N}{q^{N/2}} \left(\phi(m)\pi_q(a,m,N) - \pi_q(N)\right).$$

Cha a établi pour tout entier $N \in \mathbb{N}^*$ *la formule suivante :*

$$W_{m;a}(N) = -\beta(a,m,N) - \sum_{\chi \neq \chi_0} \overline{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)N} + o(1). \tag{3.8.3}$$

où les γ_χ *sont les zéros inverses de module* $\sqrt{q}$ *de la fonction de Dirichlet* L *associée au caractère* χ *et*

$$\beta(a,m,N) = \begin{cases} C_m(a) & \text{si } N \text{ est pair,} \\ 0 & \text{sinon.} \end{cases}$$

Soit $2 \leq r \leq \phi(m)$ *un entier et* $(a_1,a_2,\ldots,a_r) \in \mathcal{A}_r(m)$. *Il est clair que*

$$W_{m;a_1}(N) > W_{m;a_2}(N) > \cdots > W_{m;a_r}(N) \Longleftrightarrow \pi_q(a_1,m,N) > \pi_q(a_2,m,N) > \cdots > \pi_q(a_r,m,N).$$

Nous noterons par $\delta'_{m;a_1,a_2,\ldots,a_r}$ *la densité naturelle de l'ensemble*

$$\{N \in \mathbb{N}^* \text{ tel que } \pi_q(a_1,m,N) > \pi_q(a_2,m,N) > \cdots > \pi_q(a_r,m,N)\}.$$

Une vérification facile permet de montrer que la partie principale de $W_{m;a_i}(N)$ *est périodique de période* 4. *Ceci nous permet d'établir le tableau suivant :*

$N \bmod 4$	$W_{m;1}(N) \pmod{o(1)}$	$W_{m;T}(N) \pmod{o(1)}$	$W_{m;2T+1}(N) \pmod{o(1)}$
1	0	$\sqrt{3}$	$-\sqrt{3}$
2	1	2	2
3	0	$-\sqrt{3}$	$\sqrt{3}$
4	-3	0	0

Tableau 7. Approximation des valeurs de $W_{m;a}(N)$ (modulo $o(1)$) pour $a \in \{1, T, 2T+1\}$.

Nous constatons que bien que $\delta_{m;1,2T+1} = 0$ *nous avons* $\delta'_{m;1,2T+1} = \frac{1}{4}$. *Mais il est possible de trouver des densités* $\delta'_{m;a_1,\ldots,a_r} = 0$. *En effet,* $\delta'_{m;1,2T+1,T} = 0$.

Exemple 3.8.8. *Soit* $m = T(T+1) \in \mathbb{F}_3[T]$. *Le groupe* $(\mathbb{F}_3[T]/m\mathbb{F}_3[T])^\times$ *n'est pas cyclique. Afin de déterminer les caractères de Dirichlet modulo* m, *nous utilisons le fait que la fonction*

$$\begin{array}{rccc} f & : & (\mathbb{F}_3[T]/(m))^\times & \to & (\mathbb{F}_3[T]/(T))^\times \times (\mathbb{F}_3[T]/(T+1))^\times \\ & & a & \mapsto & (a \bmod T, a \bmod T+1) \end{array}$$

est un isomorphisme.

Ceci nous permet de trouver facilement le tableau suivant :

	1	2	$T+2$	$2T+1$
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	-1	-1	1
χ_3	1	1	-1	-1

Tableau 8. Table des caractères de Dirichlet modulo m.

Nous déduisons alors que $\mathcal{L}(u,\chi_1) = 1+u$ *et* $\mathcal{L}(u,\chi_2) = \mathcal{L}(u,\chi_3) = 1-u$. *Donc les fonctions L associées aux* χ_1, χ_2 *et* χ_3 *n'admettent pas de zéro inversé de module* $\sqrt{3}$. *Ainsi, pour* $a \in \mathbb{F}_3[T]$ *premier avec m, on a* $S_{m;a}(X) = -C_m(a)\mathcal{B}_q(X)$. *Il est donc clair que pour tout* $X \in \mathbb{N}^*$ *nous avons* $S_{m;a}(X) = S_{m;a}(X+2)$. *Nous obtenons facilement le tableau suivant :*

X mod 2	$S_{m;1}(X)$	$S_{m;2}(X)$	$S_{m;T+2}(X)$	$S_{m;2T+1}(X)$
1	$-3\sqrt{3}/2$	$\sqrt{3}/2$	$\sqrt{3}/2$	$\sqrt{3}/2$
2	$-9/2$	$3/2$	$3/2$	$3/2$

Tableau 9. Les valeurs de $S_{m;a}(X)$ pour $a \in \{1, 2, T+2, 2T+1\}$.

Alors si a est un non-résidu quadratique modulo m on a :

$$\delta_{m;1,a} = 0.$$

Remarque 3.8.9. *Pour les polynômes* $(T+1)(T+2) \in \mathbb{F}_3[T]$ *et* $T(T+2) \in \mathbb{F}_3[T]$, *nous pouvons construire facilement des densités nulles.*

Exemple 3.8.10. *Soit* $m = T(T+1)(T+2) \in \mathbb{F}_3[T]$. *Nous donnons ci-dessous le tableau de tous les caractères de Dirichlet non-principaux modulo m :*

	1	2	T^2+1	T^2+T+2	T^2+2T+2	$2T^2+2$	$2T^2+T+1$	$2T^2+2T+1$
χ_1	1	-1	-1	1	-1	1	1	-1
χ_2	1	1	1	-1	-1	1	-1	-1
χ_3	1	-1	-1	-1	1	1	-1	1
χ_4	1	-1	1	-1	-1	-1	1	1
χ_5	1	1	-1	1	-1	-1	-1	1
χ_6	1	-1	1	1	1	-1	-1	-1
χ_7	1	1	-1	-1	1	-1	1	-1

Tableau 10. Table des caractères de Dirichlet non-principaux modulo m.

Nous déduisons directement que pour tous les $1 \leq i \neq 6 \leq 7$ *on a* $\mathcal{L}(u,\chi_i) = 1-u^2$ *et* $\mathcal{L}(u,\chi_6) = 1+3u^2 = (1-\sqrt{3}iu)(1+\sqrt{3}iu)$. *Donc l'unique zéro inversé de toutes les*

fonctions L ci-dessus dont le module est $\sqrt{3}$ *et dont l'argument est compris entre* 0 *et* π *est* $\sqrt{3}e^{i\frac{\pi}{2}}$*, ainsi (LI* $\bigstar$*) est fausse. Par conséquent, en utilisant la formule* (2.3.1)*, nous obtenons le tableau suivant :*

$X \ mod\ 4$	$S_{m;1}(X)$	$S_{m;T^2+1}(X)$	$S_{m;2T^2+2}(X)$
1	$-4\sqrt{3}$	0	$\sqrt{3}$
2	-9	3	0
3	$-3\sqrt{3}$	$\sqrt{3}$	0
4	-12	0	3

Tableau 11. Les valeurs de $S_{m;a}(X)$ pour $a \in \{1, T^2+1, 2T^2+2\}$.

Donc

$$\delta_{m;1,T^2+1} = \delta_{m;1,2T^2+2} = 0.$$

En utilisant encore une fois la formule (2.3.1)*, nous obtenons les tableaux suivants :*

$X \ mod\ 4$	$S_{m;2}(X)$	$S_{m;T^2+T+2}(X)$	$S_{m;T^2+2T+2}(X)$
1	$\sqrt{3}$	0	0
2	0	3	3
3	0	$\sqrt{3}$	$\sqrt{3}$
4	3	0	0

Tableau 12. Les valeurs de $S_{m;a}(X)$ pour $a \in \{2, T^2+T+2, T^2+2T+2\}$.

$X \ mod\ 4$	$S_{m;2T^2+T+1}(X)$	$S_{m;2T^2+2T+1}(X)$
1	$\sqrt{3}$	$\sqrt{3}$
2	0	0
3	0	0
4	3	3

Tableau 13. Les valeurs de $S_{m;a}(X)$ pour $a \in \{2T^2+T+1, 2T^2+2T+1\}$.

Dans ce cas nous déduisons facilement des tableaux 11, 12 et 13 que si a *est un non-résidu quadratique modulo* m *alors*

$$\delta_{m;1,a} = 0.$$

Remarque 3.8.11. *Pour* $m = T(T+1)(T+2) \in \mathbb{F}_3[T]$*, l'unique résidu quadratique modulo* m *est* 1*. Dans ce cas,* $C_m(1) = 7$*, alors que* $C_m(a) = -1$ *quand* a *est un non-résidu quadratique modulo* m*. Or on a seulement deux zéros inversés de module* $\sqrt{3}$*, ce qui explique le dernier résultat qui affirme que* $\delta_{m;1,a} = 0$*.*

Chapitre 4

Biais extrême dans les courses à r compétiteurs lorsque $r \longrightarrow +\infty$ quand $|m| \longrightarrow +\infty$

Dans ce chapitre, nous nous intéressons aux courses de polynômes irréductibles unitaires dans $\mathbb{F}_q[T]$ lorsque le nombre de compétiteurs r tend vers l'infini quand le degré de m tend vers l'infini.
Dans ce contexte, il s'agit de généraliser les travaux de Lamzouri [**Lam12**].

Nous nous posons alors les questions suivantes :

- Est-ce que $\Delta_r(m) \to 0$ lorsque $r \to +\infty$ et $M = \deg(m) \to +\infty$?
- Quel est l'ordre de grandeur des densités $\delta_{m;a_1,\ldots,a_r}$ quand le nombre de compétiteurs r tend vers $+\infty$ et $\deg(m)$ tend vers $+\infty$?

Nous allons répondre partiellement à ces questions dans la section 4.1.
Pour conclure, nous évoquerons quelques perspectives relatives à cette thèse.

4.1. Résultats concernant les courses des polynômes irréductibles unitaires lorsque $r \longrightarrow +\infty$ quand $|m| \longrightarrow +\infty$

4.1.1. Énoncé des résultats

Afin de donner une réponse à ces questions. Nous chercherons des résultats analogues à ceux de Lamzouri [**Lam12**] dans le cas des corps de fonctions. Ceci nous amène à prouver le théorème suivant :

Théorème 4.1.1. *Supposons que (LI ★) est vraie. Soit $m \in \mathcal{M}_q$ de degré assez grand. Alors pour tout entier r tel que $2 \leq r \leq \sqrt{\log_q |m|}$ on a*

$$\delta_{m;a_1,\ldots,a_r} = \frac{1}{r!}\left(1 + O\left(\frac{r^2}{\log_q |m|}\right)\right)$$

uniformément pour tout r-uplet $(a_1,\ldots,a_r) \in \mathcal{A}_r(m)$.

Une conséquence directe de ce théorème est que dans la région $r = o\left(\sqrt{\log_q |m|}\right)$ où $\deg(m) \longrightarrow +\infty$ on a

$$\lim_{\deg(m)\longrightarrow+\infty} \max_{(a_1,\ldots,a_r)\in\mathcal{A}_r(m)} \left|\delta_{m;a_1,\ldots,a_r} - \frac{1}{r!}\right| \longrightarrow 0.$$

On constate alors que dans cette région, la course $\{m; a_1,\ldots,a_r\}$ a tendance à devenir non biaisée quand $\deg(m) \longrightarrow +\infty$ (ce qui est également le cas quand le nombre de compétiteurs r est fixé).
En plus, si c_0 est une petite constante bien choisie et $r \leq c_0\sqrt{\log_q |m|}$ alors on obtient:

$$\delta_{m;a_1,\ldots,a_r} \asymp \frac{1}{r!},$$

uniformément sur tous les r-uplets $(a_1,\ldots,a_r) \in \mathcal{A}_r(m)$.

Dans le théorème qui suit, nous montrons que dans la région $\sqrt{\log_q |m|} \ll r \leq (1-\epsilon)\frac{\log_q |m|}{\log\log_q |m|}$, les densités $\delta_{m;a_1,\ldots,a_r}$ ont à peu près la même décroissance asymptotique.

Théorème 4.1.2. *Supposons que (LI ★) est vraie. Pour tout $\epsilon > 0$, si $\deg(m)$ est assez grand et que r est un entier tel que $\sqrt{\log_q |m|} \ll r \leq (1-\epsilon)\frac{\log_q |m|}{\log\log_q |m|}$, alors*

$$\delta_{m;a_1,\ldots,a_r} = \exp\left(-r\log r + r + O\left(\log r + \frac{r^2}{\log_q |m|}\right)\right),$$

uniformément pour tout r-uplets $(a_1,\ldots,a_r) \in \mathcal{A}_r(m)$.

Il est alors aussi intéressant de trouver un résultat dans la région $(1-\epsilon)\frac{\log_q |m|}{\log\log_q |m|} \ll r \leq \phi(m)$. En utilisant le théorème précédent, nous trouvons une borne de l'ordre de grandeur de ces densités dans la région $(1-\epsilon)\frac{\log_q |m|}{\log\log_q |m|} \ll r \leq \phi(m)$. Ce résultat est illustré dans le théorème suivant :

Théorème 4.1.3. *Supposons que (LI ★) est vraie. Pour tout $\epsilon > 0$, si $\deg(m)$ est assez grand et que r est un entier tel que $(1-\epsilon/4)\frac{\log_q |m|}{\log\log_q |m|} \ll r \leq \phi(m)$, alors*

$$\max_{(a_1,\ldots,a_r)\in\mathcal{A}_r(m)} \delta_{m;a_1,\ldots,a_r} \ll_\epsilon \frac{1}{\exp\left((1-\epsilon)\log_q |m|\right)}.$$

4.1.2. Transformée de Fourier de $\mu_{m;a_1,\dots,a_r}$

On rappelle la formule explicite de la transformée de Fourier de $\mu_{m;a_1,\dots,a_r}$ obtenu par Cha. Sous (LI ★) on a

$$\hat{\mu}_{m;a_1,\dots,a_r}(t) = \mathcal{B}_{m;a_1,\dots,a_r}(t) \prod_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| \left|\sum_{j=1}^{r} \chi(a_j)t_j\right|\right), \tag{4.1.1}$$

où

$$J_0(z) = \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2},$$

est la fonction de Bessel d'ordre 0, et

$$\mathcal{B}_{m;a_1,\dots,a_r}(t) = \frac{1}{2}\left[\exp\left(i\frac{\sqrt{q}}{q-1}\sum_{j=1}^{r} C_m(a_j)t_j\right) + \exp\left(i\frac{q}{q-1}\sum_{j=1}^{r} C_m(a_j)t_j\right)\right].$$

Grâce à cette formule, dans la région $\|t\| \leq N_m^{-1/2+o(1)}$, nous montrons que la transformée de Fourier $\hat{\mu}_{m;a_1,\dots,a_r}$ est très proche d'une gaussienne multivariée dont la matrice de covariance est $Cov_{m;a_1,\dots,a_r}$.

Proposition 4.1.4. *Soit $m \in \mathcal{M}_q$ de degré assez grand et $2 \leq r \leq \frac{\log_q |m|}{\log\log_q |m|}$ un entier. Soit $(a_1,\dots,a_r) \in \mathcal{A}_r(m)$, alors dans la région $||t|| \leq N_m^{-1/2}(\log_q |m|)^2$ on a*

$$\hat{\mu}_{m;a_1,\dots,a_r}(t_1,\dots,t_r) = \exp\left(-\frac{1}{2}t^T \mathrm{Cov}_{m;a_1,\dots,a_r} t\right)\left(1 + O\left(\frac{d(m)(\log_q |m|)^3}{\sqrt{|m|}}\right)\right).$$

Démonstration. La formule explicite (4.1.1) implique que

$$\log \hat{\mu}_{m;a_1,\dots,a_r}(t_1,\dots,t_r) = \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \log J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| \left|\sum_{j=1}^{r} \chi(a_j)t_j\right|\right) + O\left(\|t\| \sum_{j=1}^{r} |C_m(a_j)|\right).$$

En combinant le Lemme 3.2.3 avec l'estimation $\phi(m) \gg |m|/\log\log_q |m|$ (voir (2.2.5)), on déduit que le terme d'erreur ci-dessus est $\ll |m|^{-1/2} d(m)(\log_q |m|)^3$. On remarque également que si $\deg(m)$ est assez grand alors

$$\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| \left|\sum_{j=1}^{r} \chi(a_j)t_j\right| \ll \sqrt{r}\|t\| \leq 1.$$

Ainsi, en utilisant le fait $\log J_0(z) = -z^2/4 + O(z^4)$ pour $|z| \leq 1$ on obtient :

$$\log \hat{\mu}_{m;a_1,\dots,a_r}(t_1,\dots,t_r) = - \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 \left|\sum_{j=1}^{r} \chi(a_j) t_j\right|^2 + O\left(\sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^4 \left|\sum_{j=1}^{r} \chi(a_j) t_j\right|^4 + \frac{d(m)(\log_q |m|)^3}{\sqrt{|m|}} \right).$$

Or d'après l'inégalité de Cauchy-Schwarz on sait que $\left|\sum_{j=1}^{r} \chi(a_j) t_j\right|^4 \leq r^2 \|t\|^4$ donc

$$\log \hat{\mu}_{m;a_1,\dots,a_r}(t_1,\dots,t_r) = - \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 \left|\sum_{j=1}^{r} \chi(a_j) t_j\right|^2 + O\left(r^2\|t\|^4 \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 + \frac{d(m)(\log_q |m|)^3}{\sqrt{|m|}} \right). \tag{4.1.2}$$

Puisque $\sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 \ll N_m$, alors

$$r^2\|t\|^4 \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 \leq \frac{r^2(\log_q |m|)^7}{\phi(m)} \ll \frac{d(m)(\log_q |m|)^3}{\sqrt{|m|}}.$$

Il s'ensuit que le terme d'erreur dans l'estimation (4.1.2) est $\ll |m|^{-1/2} d(m)(\log_q |m|)^3$. D'autre part, en utilisant les Lemmes 3.1.1 et 3.2.3, on déduit que le terme principal de la partie droite de (4.1.2) est égal à

$$\begin{aligned} - \sum_{\substack{\chi \neq \chi_0 \\ \chi \bmod m}} \sum_{\Im(\gamma_\chi)>0} \left|\frac{\gamma_\chi}{\gamma_\chi - 1}\right|^2 \sum_{1 \leq j,k \leq r} \chi(a_j)\overline{\chi(a_k)} t_j t_k &= -\frac{1}{2} \sum_{1 \leq j,k \leq r} (\mathrm{Cov}_{m;a_1,\dots,a_r}(j,k) + O(d(m)^2)) t_j t_k \\ &= -\frac{1}{2} t^T \mathrm{Cov}_{m;a_1,\dots,a_r} t + O\left(d(m)^2 r |t|^2\right) \\ &= -\frac{1}{2} t^T \mathrm{Cov}_{m;a_1,\dots,a_r} t + O\left(\frac{d(m)(\log_q |m|)^3}{\sqrt{|m|}}\right), \end{aligned}$$

la Proposition 4.1.4 en découle.

□

Ensuite, nous démontrerons la décroissance rapide de $\hat{\mu}_{m;a_1,..,a_r}(t)$ dans la région $||t|| \geq N_m^{-1/2}$.

Proposition 4.1.5. *Il existe une constante $c_1 > 0$ tel que, si $\deg(m) = M$ est assez grand et $2 \leq r \leq c_1 M$, alors on obtient uniformément sur tout $(a_1, \ldots, a_r) \in \mathcal{A}_r(m)$ que*

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| \leq \begin{cases} \exp\left(-\dfrac{\phi(m)}{64r}\log\|t\|\right) & si\ \|t\| > 4\sqrt{q}, \\ \exp\left(-\dfrac{\phi(m)}{64M^5}\right) & si\ M^{-2} \leq \|t\| \leq 4\sqrt{q}, \\ \exp\left(-\dfrac{\phi(m)M}{4}\|t\|^2\right) & si\ \|t\| \leq M^{-2}. \end{cases}$$

Démonstration. On suppose que $\|t\| > 4\sqrt{q}$.
En utilisant le même raisonnement que dans la démonstration de la Proposition 3.3.4, on trouve facilement l'inégalité suivante :

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)|^2 \leq \exp\left(-\log\|t\|\phi(m)\left(\frac{M}{16r}-1\right)\right).$$

Avec un choix adéquat de c_1 on a pour M assez grand, $\frac{M}{16r} - 1 \geq \frac{M}{32r}$. Donc

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| \leq \exp\left(\frac{-\log\|t\|\phi(m)}{64r}\right).$$

On suppose que $M^{-2} \leq \|t\| \leq 4\sqrt{q}$.
On reprend la démonstration de la Proposition 3.3.4, avec en particulier $\epsilon = M^{-2}$. On obtient alors de la même manière que dans (3.3.7) que

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| \leq \exp\left(\frac{-1}{4M^4}\sum_{\chi\in V_{m,a}(t)}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\right),$$

or on a déjà prouvé dans (3.3.9) que pour M assez grand

$$\sum_{\chi\in V_{m,a}(t)}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2 \geq \frac{\phi(m)M}{8r} + O\left(\phi(m)\log M\right) \geq \frac{\phi(m)M}{16r}.$$

Ainsi

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| \leq \exp\left(\frac{-\phi(m)}{64rM^3}\right),$$

Or on sait que $2 \leq r \leq c_1 M \leq M^2$ donc

$$|\hat{\mu}_{m;a_1,\ldots,a_r}(t_1,\ldots,t_r)| \leq \exp\left(\frac{-\phi(m)}{64M^5}\right).$$

On suppose que $\|t\| \leq M^{-2}$.
Soit χ un caractère de Dirichlet non principal modulo m. Si $\deg(m) = M$ est assez grand alors

$$2\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|\left|\sum_{i=1}^{r}\chi(a_i)t_i\right| \ll \sqrt{r}\|t\| \leq 1.$$

En combinant le fait que $|J_0(x)| \leq \exp(-x^2/4)$ pour $|x| \leq 1$ avec (4.1.1), on trouve

$$|\hat{\mu}_{m;a_1,\dots,a_r}(t_1,\dots,t_r)| \leq \exp\left(-\sum_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\left|\sum_{i=1}^{r}\chi(a_i)t_i\right|^2\right).$$

D'une part, on sait que

$$\begin{aligned}\sum_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\left|\sum_{i=1}^{r}\chi(a_i)t_i\right|^2 &= \sum_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\sum_{1\leq k,j\leq r}\chi(a_k)\overline{\chi(a_j)}t_kt_j\\ &= \frac{N_m}{2}\|t\|^2+\sum_{1\leq k<j\leq r}B_m(a_k,a_j)t_kt_j.\end{aligned} \tag{4.1.3}$$

D'autre part, d'après l'inégalité de Cauchy-Schwarz on a

$$\sum_{1\leq k<j\leq r}|t_kt_j| \leq \left(\sum_{i=1}^{r}|t_i|\right)^2 \leq r\|t\|^2. \tag{4.1.4}$$

En combinant le Lemme 3.2.3, le Corollaire 3.2.10, (4.1.3), (4.1.4) on obtient

$$\sum_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\left|\sum_{i=1}^{r}\chi(a_i)t_i\right|^2 = \frac{q}{2(q-1)}\phi(m)M\|t\|^2\left(1+O\left(\frac{r+\log M}{M}\right)\right). \tag{4.1.5}$$

Donc avec un choix adéquat de $c_1>0$ tel que $r\leq c_1M$, on déduit que

$$\sum_{\substack{\chi\neq\chi_0\\ \chi \bmod m}}\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\left|\sum_{i=1}^{r}\chi(a_i)t_i\right|^2 \geq \frac{\phi(m)M}{4}\|t\|^2. \tag{4.1.6}$$

D'où

$$|\hat{\mu}_{m;a_1,\dots,a_r}(t_1,\dots,t_r)| \leq \exp\left(-\frac{\phi(m)M}{4}\|t\|^2\right).$$

□

4.1.3. Comportement asymptotique des densités $\delta_{m;a_1,\dots,a_r}$

Dans ce qui suit, nous démontrerons les Théorèmes 4.1.1,4.1.2, 4.1.3.

Nous commencerons par prouver le Théorème 4.1.1. Pour ce faire, on passe par les étapes suivantes:

- Découper l'intégrale en deux

$$\delta_{m;a_1,\dots,a_r} = \int_{\substack{t_1>\dots>t_r\\ |y|_\infty\leq R}} d\mu_{m;a_1,\dots,a_r}(t_1,\dots,t_r) + \int_{\substack{t_1>\dots>t_r\\ |y|_\infty> R}} d\mu_{m;a_1,\dots,a_r}(t_1,\dots,t_r).$$

- Appliquer la formule d'inversion de Fourier sur la mesure $\mu_{m;a_1,\dots,a_r}$.

- Étudier la transformée de Fourier $\hat{\mu}_{m;a_1,..,a_r}$.

- Prouver la décroissance rapide de $\hat{\mu}_{m;a_1,..,a_r}(t)$ dans la région $||t|| \geq N_m^{-1/2}$.

- Démontrer que dans la région $||t|| \leq N_m^{-1/2+o(1)}$, $\hat{\mu}_{m;a_1,...,a_r}(t_1,\ldots,t_r)$ est très proche de la transformée de Fourier d'une gaussienne multivariée dont la matrice de covariance est $Cov_{m;a_1,...,a_r}$.

Dans ce qui suit on utilisera la matrice $\mathcal{C}$ de taille $r \times r$ qui est symétrique et dont les entrées sont :

$$\mathcal{C}_{jk} = \begin{cases} 1 & \text{si } j = k, \\ \dfrac{B_m(a_j,a_k)}{N_m} & \text{sinon } j \neq k. \end{cases}$$

Remarque 4.1.6. *D'après le Lemme 3.2.3 et le Corollaire 3.2.10, si* $1 \leq j \neq k \leq r$ *alors* $\mathcal{C}_{jk} \ll \frac{1}{\log_q |m|}$.

On désignera également par $\mathcal{M}_r(\epsilon)$ l'ensemble des matrices symétriques de taille $r \times r$ dont les termes diagonaux valent 1 et les termes non diagonaux sont majorées en valeur absolue par ϵ.

Avant de démontrer les Théorèmes 4.1.1, 4.1.2, 4.1.3, on rappelle les lemmes suivants utilisés dans [**Lam12**] :

Lemme 4.1.7. [**Lam12**, Lemme 4.1]. *Si* $\epsilon \leq 1/(2r)$ *alors pour tout* $A \in \mathcal{M}_r(\epsilon)$ *on a* $\det(A) = 1 + O(\epsilon^2 r^2)$.

Lemme 4.1.8. [**Lam12**, Lemme 4.2]. *Si* $\epsilon \leq 1/(2r)$ *alors pour tout* $A \in \mathcal{M}_r(\epsilon)$ *on a*

$$\tilde{a}_{jk} = \begin{cases} 1 + O(\epsilon^2 r^2) & \text{si } j = k, \\ O(\epsilon) & \text{si } j \neq k. \end{cases}$$

Lemme 4.1.9. [**Lam12**, Lemme 4.3]. *Soit* $r \geq 2$ *un entier strictement positif,* $R \geq 10\sqrt{r}$ *est un nombre réel et* $x \in \mathbb{R}^r$. *Si* $\epsilon \leq 1/(2r)$ *alors pour tout* $A \in \mathcal{M}_r(\epsilon)$ *on a*

$$(2\pi)^{-r} \int_{\|t\| \leq R} e^{i(t_1x_1+\cdots+t_rx_r)} \exp\left(-\frac{1}{2}t^T A t\right) dt = \frac{1}{(2\pi)^{r/2}\det(A)} \exp\left(-\frac{1}{2}x^T A^{-1} x\right) + O\left(\exp\left(-\frac{R^2}{5}\right)\right).$$

Pour simplifier, on utilise respectivement les notations δ_m et μ_m pour désigner $\delta_{m;a_1,\dots,a_r}$ et $\mu_{m;a_1,\dots,a_r}$.

Démonstration du théorème 4.1.1. Soit $R = 9\sqrt{N_m}\log_q|m|$. Il est clair que

$$\delta_m = \int_{y_1>y_2>\cdots>y_r} d\mu_m(y_1,\dots,y_r) = \int_{\substack{y_1>y_2>\cdots>y_r\\ |y|_\infty\le R}} d\mu_m(y_1,\dots,y_r) + \int_{\substack{y_1>y_2>\cdots>y_r\\ |y|_\infty> R}} d\mu_m(y_1,\dots,y_r).$$

Or, en combinant le Lemme 3.3.9 avec (3.1.3) et pour $\deg(m)$ assez grand on a

$$\begin{aligned}\mu_{m;a_1,\dots,a_r}(|x|_\infty > R) &\le 2r\exp\left(-\frac{R^2}{32\phi(m)\log_q|m|}\right)\\ &\le 2\sqrt{\log_q|m|}\exp\left(-\frac{81}{32}(\log_q|m|)^2\right).\end{aligned}$$

Donc

$$\delta_m = \int_{y_1>y_2>\cdots>y_r} d\mu_m(y_1,\dots,y_r) = \int_{\substack{y_1>y_2>\cdots>y_r\\ |y|_\infty\le R}} d\mu_m(y_1,\dots,y_r) + O\left(\exp\left(-2(\log_q|m|)^2\right)\right). \tag{4.1.7}$$

Ensuite, on applique la formule d'inversion de Fourier à la mesure μ_m pour obtenir

$$\int_{\substack{y_1>y_2>\cdots>y_r\\ |y|_\infty\le R}} d\mu_m(y_1,\dots,y_r) = (2\pi)^{-r}\int_{\substack{y_1>y_2>\cdots>y_r\\ |y|_\infty\le R}}\int_{s\in\mathbb{R}^r} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\dots,s_r)dsdy.$$

Puisque la transformée de Fourier $\hat{\mu}_m(s_1,\dots,s_r)$ décroît rapidement, on déduit que la principale contribution à l'intégrale sur $\mathbb{R}^r$ de $e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\dots,s_r)$ provient d'une petite boule centrée en 0. En effet, on déduit de la Proposition 4.1.5 que

$$\begin{aligned}\int_{s\in\mathbb{R}^r} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\dots,s_r)ds &= \int_{\|s\|\le\epsilon} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\dots,s_r)ds\\ &\quad + O\left(\exp\left(-2M^2\right)\right),\end{aligned}$$

où $\epsilon = 9(N_m)^{-1/2}\log_q|m|$.
Comme $R = 9\sqrt{N_m}\log_q|m|$, alors d'après le Lemme 3.2.3 on a $R \le 18\sqrt{\phi(m)\log_q|m|}\log_q|m|$, or $\phi(m) = |m|^{1+o(1)}$ d'où $R^r \ll \exp(r\log|m|)$ donc

$$\delta_m = (2\pi)^{-r}\int_{\substack{y_1>y_2>\cdots>y_r\\ |y|_\infty\le R}}\int_{\|s\|\le\epsilon} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\dots,s_r)dsdy + O\left(\exp\left(-(\log_q|m|)^2\right)\right). \tag{4.1.8}$$

On effectue maintenant les changements de variables suivants :

$$t_j := \sqrt{N_m}s_j \text{ et } x_j := \frac{y_j}{\sqrt{N_m}}, \text{ pour tout } 1\le j\le r.$$

On a alors :

$$\begin{aligned}\delta_m =&(2\pi)^{-r}\int_{\substack{x_1>x_2>\cdots>x_r\\ |x|_\infty\le 9\log_q|m|}}\int_{\|t\|\le 9\log_q|m|} e^{i(t_1x_1+\cdots+t_rx_r)}\hat{\mu}_m\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right)dtdx\\ &+ O\left(\exp\left(-(\log_q|m|)^2\right)\right).\end{aligned} \tag{4.1.9}$$

On remplace $\hat{\mu}_m\left(\frac{t_1}{\sqrt{N_m}},\dots,\frac{t_r}{\sqrt{N_m}}\right)$ par son approximation dans la Proposition 4.1.4, ce qui implique que

$$\delta_m=(2\pi)^{-r}\int_{\substack{x_1>x_2>\cdots>x_r\\ |x|_\infty\leq 9\log_q|m|}}\int_{\|t\|\leq 9\log_q|m|} e^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{1}{2}t^T\mathcal{C}t\right)\left(1+O\left(\frac{d(m)(\log_q|m|)^3}{\sqrt{|m|}}\right)\right)dtdx. \tag{4.1.10}$$

On sait que

$$t^T\mathcal{C}t=\sum_{j=1}^r\sum_{k=1}^r\mathcal{C}_{jk}t_jt_k=\sum_{j=1}^r t_j^2+\sum_{1\leq j\neq k\leq r}\mathcal{C}_{jk}t_jt_k.$$

Or $\mathcal{C}_{jk}=\frac{B_m(a_j,a_k)}{N_m}\ll\frac{1}{\log_q|m|}$ pour $j\neq k$, alors d'après l'inégalité de Cauchy-Schwarz on a

$$\left|\sum_{1\leq j\neq k\leq r}\mathcal{C}_{jk}t_jt_k\right|\ll\frac{1}{\log_q|m|}\left(\sum_{j=1}^r|t_j|\right)^2\ll\frac{1}{\sqrt{\log_q|m|}}\sum_{j=1}^r t_j^2.$$

Donc il existe une constante strictement positive c_1 telle que

$$t^T\mathcal{C}t\geq\left(1-\frac{c_1}{\sqrt{\log_q|m|}}\right)\sum_{j=1}^r t_j^2\geq\frac{1}{2}\sum_{j=1}^r t_j^2. \tag{4.1.11}$$

En combinant (4.1.10), $t^T\mathcal{C}t\geq 0$ et $d(m)=|m|^{o(1)}$, on obtient

$$\delta_m=(2\pi)^{-r}\int_{\substack{x_1>x_2>\cdots>x_r\\ |x|_\infty\leq 9\log_q|m|}}\int_{\|t\|\leq 9\log_q|m|} e^{i(t_1x_1+\cdots+t_rx_r)}\exp\left(-\frac{1}{2}t^T\mathcal{C}t\right)dtdx+Er, \tag{4.1.12}$$

où

$$Er\ll|m|^{-1/3}(\log|m|)^{9r}\ll|m|^{-1/4}.$$

De plus, en appliquant le Lemme 4.1.9 on déduit que

$$\delta_m=\frac{1}{(2\pi)^{r/2}\det(\mathcal{C})}\int_{\substack{x_1>x_2>\cdots>x_r\\ |x|_\infty\leq 3\log_q|m|}}\exp\left(-\frac{1}{2}x^T\mathcal{C}^{-1}x\right)dx+O\left(|m|^{-1/4}\right). \tag{4.1.13}$$

D'après la Remarque 4.1.6, on a $\mathcal{C}_{jk}\ll\frac{1}{\log_q|m|}$ pour $j\neq k$, alors il existe une constante absolue $\alpha_0>0$ telle que $\mathcal{C}\in\mathcal{M}_r(\beta)$ avec $\beta=\frac{\alpha_0}{\log_q|m|}$. Par conséquent, en faisant appel au Lemme 4.1.8, on obtient en utilisant l'inégalité de Cauchy-Schwarz l'égalité suivante :

$$\begin{aligned}x^T\mathcal{C}^{-1}x&=\left(1+O\left(\frac{r^2}{(\log_q|m|)^2}\right)\right)\sum_{j=1}^r x_j^2+O\left(\frac{1}{\log_q|m|}\left(\sum_{j=1}^r|x_j|\right)^2\right)\\&=\left(1+O\left(\frac{r}{\log_q|m|}\right)\right)\|x\|^2.\end{aligned}$$

Ainsi on déduit l'encadrement de $-\frac{1}{2}x^T\mathcal{C}^{-1}x$:

$$-\frac{1}{2}\left(1+\frac{\alpha_1 r}{\log_q|m|}\right)\|x\|^2\leq-\frac{1}{2}x^T\mathcal{C}^{-1}x\leq-\frac{1}{2}\left(1-\frac{\alpha_1 r}{\log_q|m|}\right)\|x\|^2, \tag{4.1.14}$$

pour une certaine constante absolue $\alpha_1 > 0$. Ceci implique

$$\int_{\substack{x_1>x_2>\cdots>x_r \\ |x|_\infty>9\log_q|m|}} \exp\left(-\frac{1}{2}x^T\mathcal{C}^{-1}x\right)dx \leq \int_{|x|_\infty>9\log_q|m|} \exp\left(-\frac{1}{4}\|x\|^2\right)dx \ll \exp\left(-(\log_q|m|)^2\right).$$

En insérant cette estimation dans (4.1.13) et en utilisant le Lemme 4.1.7 on obtient

$$\delta_m = \left(1+O\left(\frac{r^2}{(\log_q|m|)^2}\right)\right)\frac{1}{(2\pi)^{r/2}}\int_{x_1>x_2>\cdots>x_r}\exp\left(-\frac{1}{2}x^T\mathcal{C}^{-1}x\right)dx + O\left(|m|^{-1/4}\right). \tag{4.1.15}$$

Soit κ un nombre réel tel que $|\kappa| \leq \frac{\alpha_1 r}{\log_q|m|}$. Puisque la fonction $\|x\|^2$ est symétrique par rapport aux variables $\{x_j\}_{1\leq j\leq r}$ on obtient

$$\begin{aligned}\frac{1}{(2\pi)^{r/2}}\int_{x_1>x_2>\cdots>x_r}\exp\left(-\frac{1}{2}(1+\kappa)\|x\|^2\right)dx &= \frac{1}{r!(2\pi)^r}\int_{\mathbb{R}^r}\exp\left(-\frac{1}{2}(1+\kappa)\|x\|^2\right)dx \\ &= \frac{1}{r!}\left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\exp\left(-\frac{1}{2}(1+\kappa)y^2\right)dy\right)^r \\ &= \frac{1}{r!(1+\kappa)^{r/2}} = \frac{1}{r!}\exp\left(O\left(\frac{r^2}{\log_q|m|}\right)\right).\end{aligned} \tag{4.1.16}$$

Ainsi, en combinant les estimations (4.1.14), (4.1.15) et (4.1.16) on déduit le Théorème 4.1.1. □

Démonstration du théorème 4.1.2. On choisit $R = 25\sqrt{N_m r\log r}$. En utilisant le Lemme 3.3.9, on trouve

$$\delta_m = \int_{y_1>y_2>\cdots>y_r} d\mu_m(y_1,\ldots,y_r) = \int_{\substack{y_1>y_2>\cdots>y_r \\ |y|_\infty\leq R}} d\mu_m(y_1,\ldots,y_r) + O\left(\exp\left(-8r\log r\right)\right). \tag{4.1.17}$$

En appliquant la formule d'inversion de Fourier à la mesure μ_m, on obtient

$$\int_{\substack{y_1>y_2>\cdots>y_r \\ |y|_\infty\leq R}} d\mu_m(y_1,\ldots,y_r) = (2\pi)^{-r}\int_{\substack{y_1>y_2>\cdots>y_r \\ |y|_\infty\leq R}}\int_{s\in\mathbb{R}^r} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)dsdy.$$

En utilisant la Proposition 4.1.5, on a

$$\begin{aligned}\int_{s\in\mathbb{R}^r} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)ds &= \int_{\|s\|\leq\epsilon} e^{i(s_1y_1+\cdots+s_ry_r)}\hat{\mu}_m(s_1,\ldots,s_r)ds \\ &\quad + O\left(\exp\left(-8r\log r\right)\right),\end{aligned}$$

où $\epsilon = 9(N_m)^{-1/2}\log_q|m|$. En effectuant les changements de variables $t_j := \sqrt{N_m}s_j$ et $x_j := \frac{y_j}{\sqrt{N_m}}$, pour tout $1\leq j\leq r$, on obtient l'estimation suivante :

$$\begin{aligned}\delta_m =& (2\pi)^{-r}\int_{\substack{x_1>x_2>\cdots>x_r \\ |x|_\infty\leq 25\sqrt{r\log r}}}\int_{\|t\|\leq 9\log_q|m|} e^{i(t_1x_1+\cdots+t_rx_r)}\hat{\mu}_m\left(\frac{t_1}{\sqrt{N_m}},\ldots,\frac{t_r}{\sqrt{N_m}}\right)dtdx \\ &+ O\left(\exp\left(-4r\log r\right)\right).\end{aligned} \tag{4.1.18}$$

Ainsi, on déduit de la Proposition 4.1.4 que

$$\delta_m = (2\pi)^{-r} \int_{\substack{x_1>x_2>\cdots>x_r \\ |x|_\infty \leq 25\sqrt{r\log r}}} \int_{\|t\|\leq 9\log_q|m|} e^{i(t_1x_1+\cdots+t_rx_r)} \exp\left(-\frac{1}{2}t^T\mathcal{C}t\right) dtdx + J, \qquad (4.1.19)$$

où

$$J \ll \frac{d(m)(\log_q|m|)^3}{\sqrt{|m|}}(2\pi)^{-r} \int_{\substack{x_1>x_2>\cdots>x_r \\ |x|_\infty \leq 25\sqrt{r\log r}}} dx \int_{\|t\|\leq 9\log_q|m|} \exp\left(-\frac{1}{2}t^T\mathcal{C}t\right) dt + \exp\left(-4r\log r\right). \qquad (4.1.20)$$

D'après la formule de Stirling, on a $\frac{r^r}{r!} \sim \frac{\exp(r)}{\sqrt{2\pi r}}$ donc

$$\int_{\substack{x_1>x_2>\cdots>x_r \\ |x|_\infty \leq 25\sqrt{r\log r}}} dx = \frac{1}{r!}\int_{|x|_\infty\leq 25\sqrt{r\log r}} dx = \frac{(50\sqrt{r\log r})^r}{r!} = \exp\left(-\frac{r\log r}{2} + O(r\log\log r)\right).$$

En outre, d'après (4.1.11) on a

$$\frac{1}{(2\pi)^r}\int_{\|t\|\leq 9\log_q|m|} \exp\left(-\frac{1}{2}t^T\mathcal{C}t\right) dt \leq \frac{1}{(2\pi)^r}\int_{t\in\mathbb{R}^r} \exp\left(-\frac{\|t\|^2}{4}\right) dt = \frac{1}{\pi^{r/2}}.$$

Par conséquent, en insérant ces estimations dans (4.1.20) et en utilisant la borne $d(m) = \exp\left(O(\log_q|m|/\log\log_q|m|)\right)$ ([**Afs20**, Proposition 3.1]) on obtient :

$$J \ll \exp\left(-\frac{1}{2}(\log_q|m| + r\log r) + O\left(\frac{\log_q|m|}{\log\log_q|m|} + r\log\log r\right)\right) + \exp\left(-4r\log r\right),$$

car $|m|^{-1/2} = \exp(-\frac{\log|m|}{2}) \leq \exp(-\frac{\log_q|m|}{2})$.
D'une manière similaire à la démonstration du Théorème 4.1.1, on trouve de manière analogue à (4.1.15) l'équation suivante :

$$\delta_m = \left(1 + O\left(\frac{r^2}{(\log_q|m|)^2}\right)\right)\frac{1}{(2\pi)^{r/2}}\int_{x_1>x_2>\cdots>x_r} \exp\left(-\frac{1}{2}x^T\mathcal{C}^{-1}x\right) dx + K, \qquad (4.1.21)$$

où

$$K \ll \exp\left(-\frac{1}{2}(\log_q|m| + r\log r) + O\left(\frac{\log_q|m|}{\log\log_q|m|} + r\log\log r\right)\right) + \exp\left(-4r\log r\right).$$

De plus, en utilisant la formule de Stirling, il découle de (4.1.14) et (4.1.16) que

$$\begin{aligned}\frac{1}{(2\pi)^{r/2}}\int_{x_1>x_2>\cdots>x_r} \exp\left(-\frac{1}{2}x^T\mathcal{C}^{-1}x\right) dx &= \frac{1}{r!}\exp\left(O\left(\frac{r^2}{\log_q|m|}\right)\right) \\ &= \exp\left(-r\log r + r + O\left(\log r + \frac{r^2}{\log_q|m|}\right)\right).\end{aligned}$$

En insérant cette estimation dans (4.1.21), on complète la preuve du Théorème 4.1.2.

□

Démonstration du théorème 4.1.3. On rappelle que si (LI ★) est vérifiée alors la densité de l'ensemble des entiers strictement positifs X tels que

$$\sum_{N=1}^{X} \pi_q(a_j,m,N) = \sum_{N=1}^{X} \pi_q(a_k,m,N),$$

est égale à 0 si $1 \leq j \neq k \leq r$. Donc

$$\delta_{m;a_1,\ldots,a_{r-1}} = \delta_{m;a_r,a_1,\ldots,a_{r-1}} + \delta_{m;a_1,a_r,\ldots,a_{r-1}} + \cdots + \delta_{m;a_1,\ldots,a_{r-1},a_r}.$$

Si $2 \leq s < r \leq \phi(m)$ sont des entiers strictement positifs alors

$$\max_{(a_1,\ldots,a_r)\in\mathcal{A}_r(m)} \delta_{m;a_1,\ldots,a_r} < \max_{(b_1,\ldots,b_s)\in\mathcal{A}_s(m)} \delta_{m;b_1,\ldots,b_s}. \tag{4.1.22}$$

On prend $s = [(1-\epsilon/4)\log_q|m|/\log\log_q|m|]$. D'après le Théorème 4.1.2, on a

$$\max_{(b_1,\ldots,b_s)\in\mathcal{A}_s(m)} \delta_{m;b_1,\ldots,b_s} = \exp\left(-s\log s + s + O\left(\log s + \frac{r^2}{\log_q|m|}\right)\right) \ll_\epsilon \frac{1}{\exp\left((1-\epsilon)\log_q|m|\right)}.$$

En combinant la dernière inégalité avec (4.1.22), le Théorème 4.1.3 est démontré. □

4.2. Perspectives

Comme perspectives de cette thèse, on pourrait explorer les pistes de réflexion suivantes:

- Il serait intéressant de trouver une famille infinie $\mathcal{F}$ de polynômes tels que pour tout $m \in \mathcal{F}$ il existe $(a,b) \in \mathcal{A}_2(m)$ vérifiant $\delta_{m;a,b} = 0$.

- Il serait pertinent de trouver un polynôme $m \in \mathcal{M}_q$ et $(a,b) \in \mathcal{A}_2(m)$ vérifiant $\delta'_{m;a,b} = 0$, où $\delta'_{m;a,b}$ est la densité naturelle de l'ensemble

$$\{N \in \mathbb{N}^* : \pi_q(a;m,N) > \pi_q(b;m,N)\}.$$

- Soient a et b deux polynômes distincts dans $\mathbb{F}_q[T]$. Peut-on trouver une famille infinie $\mathcal{F}$ de polynômes unitaires tel que pour tout $m \in \mathcal{F}$ on a $\delta_{m;a,b} = 0$?

- Il serait pertinent de démontrer la Conjecture 1.3.2 dans le cas des corps de fonctions.

- Peut-on trouver une hypothèse plus faible que $(LI\bigstar)$ de telle sorte que les résultats présentés dans le Chapitre 3 demeurent valables ?

Références bibliographiques

[Afs20] Ardavan Afshar. *Topics in the arithmetic of polynomials over finite fields*. PhD thesis, 2020. https://discovery.ucl.ac.uk/id/eprint/10106769/1/PhD%20Thesis%20-%20Final%20Submission%20-%20Ardavan%20Afshar.pdf.

[And15] Julio Andrade. Analytic number theory in function fields. http://julioandrade.weebly.com/analytic-number-theory-in-function-fields---tcc.html, 2015.

[Bai20] Alexandre Bailleul. *Étude de la répartition des automorphismes de Frobenius dans les groupes de Galois*. PhD thesis, Bordeaux, 2020.

[Bai21] Alexandre Bailleul. Chebyshev's bias in dihedral and generalized quaternion Galois groups. *Algebra Number Theory*, 15(4):999–1041, 2021.

[CFJ16] Byungchul Cha, Daniel Fiorilli, and Florent Jouve. Prime number races for elliptic curves over function fields. *Ann. Sci. Éc. Norm. Supér. (4)*, 49(5):1239–1277, 2016.

[Cha08] Byungchul Cha. Chebyshev's bias in function fields. *Compos. Math.*, 144(6):1351–1374, 2008.

[Cho65] S. Chowla. The Riemann hypothesis and Hilbert's tenth problem. *Norske Vid. Selsk. Forh. (Trondheim)*, 38:62–64, 1965.

[CI11] Byungchul Cha and Bo-Hae Im. Chebyshev's bias in Galois extensions of global function fields. *J. Number Theory*, 131(10):1875–1886, 2011.

[CK10] Byungchul Cha and Seick Kim. Biases in the prime number race of function fields. *J. Number Theory*, 130(4):1048–1055, 2010.

[Dev20] Lucile Devin. Limiting properties of the distribution of primes in an arbitrarily large number of residue classes. *Canad. Math. Bull.*, 63(4):837–849, 2020.

[DM18] Lucile Devin and Xianchang Meng. Chebyshev's bias for products of irreducible polynomials. *arXiv preprint arXiv:1809.09662*, 2018.

[Emm] Kowalski Emmanuel. Exponential sums over finite fields, i: elementary methods. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.400.6392&rep=rep1&type=pdf.

[FHL19] Kevin Ford, Adam J Harper, and Youness Lamzouri. Extreme biases in prime number races with many contestants. *Mathematische Annalen*, 374(1):517–551, 2019.

[Fio14] Daniel Fiorilli. Highly biased prime number races. *Algebra Number Theory*, 8(7):1733–1767, 2014.

[FJ22] Daniel Fiorilli and Florent Jouve. Unconditional Chebyshev biases in number fields. *J. Éc. polytech. Math.*, 9:671–679, 2022.

[FJ23] Daniel Fiorilli and Florent Jouve. Distribution of frobenius elements in families of galois extensions. *Journal of the Institute of Mathematics of Jussieu*, page 1–90, 2023.

[FK02] Kevin Ford and Sergei Konyagin. Chebyshev's conjecture and the prime number race. In *IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems,*

Part II (Russian) (Tula, 2001), pages 67–91. Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.

[FLK13] Kevin Ford, Youness Lamzouri, and Sergei Konyagin. The prime number race and zeros of Dirichlet L-functions off the critical line: Part III. *Q. J. Math.*, 64(4):1091–1098, 2013.

[FM00] Andrey Feuerverger and Greg Martin. Biases in the Shanks-Rényi prime number race. *Experiment. Math.*, 9(4):535–570, 2000.

[FM13] Daniel Fiorilli and Greg Martin. Inequities in the Shanks-Rényi prime number race: an asymptotic formula for the densities. *J. Reine Angew. Math.*, 676:121–212, 2013.

[GM06] Andrew Granville and Greg Martin. Prime number races. *Amer. Math. Monthly*, 113(1):1–33, 2006.

[HL18] Adam J Harper and Youness Lamzouri. Orderings of weakly correlated random variables, and prime number races with many contestants. *Probability Theory and Related Fields*, 170(3):961–1010, 2018.

[Hsu98] Chih-Nung Hsu. On certain character sums over $\mathbb{F}_q[T]$. *Proc. Amer. Math. Soc.*, 126(3):647–652, 1998.

[Hum13] Peter Humphries. The distribution of weighted sums of the liouville function and pólya's conjecture. *Journal of Number Theory*, 133(2):545–582, feb 2013.

[Kac93] Jerzy Kaczorowski. A contribution to the Shanks-Rényi race problem. *Quart. J. Math. Oxford Ser. (2)*, 44(176):451–458, 1993.

[Kac95] Jerzy Kaczorowski. On the distribution of primes (mod 4). *Analysis*, 15(2):159–171, 1995.

[KT62] S. Knapowski and Pál Turán. Comparative prime-number theory. I–III: Introduction. Comparison of the progressions $\equiv 1 \bmod k$ and $\equiv \ell \bmod k$, $\ell \not\equiv 1 \bmod k$. continuation of the study of comparison of the progressions $\equiv 1 \bmod k$ and $\equiv \ell \bmod k$. *Acta Math. Acad. Sci. Hung.*, 13:299–314, 315–342, 343–364, 1962.

[Lam12] Youness Lamzouri. The Shanks-Rényi prime number race with many contestants. *Math. Res. Lett.*, 19(3):649–666, 2012.

[Lam13] Youness Lamzouri. Prime number races with three or more competitors. *Math. Ann.*, 356(3):1117–1162, 2013.

[Li18] Wanlin Li. Vanishing of hyperelliptic L-functions at the central point. *J. Number Theory*, 191:85–103, 2018.

[Lit14] J. E. Littlewood. Distribution des nombres premiers. *CR Acad. Sci. Paris*, 158:1239–1277, 1914.

[LM22] Jiawei Lin and Greg Martin. Densities in certain three-way prime number races. *Canad. J. Math.*, 74(1):232–265, 2022.

[Ng00] Nathan Christopher Ng. *Limiting distributions and zeros of Artin L-functions*. PhD thesis, University of British Columbia, 2000.

[PG20] Corentin Perret-Gentil. Roots of L-functions of characters over function fields, generic linear independence and biases. *Algebra Number Theory*, 14(5):1291–1329, 2020.

[Pol08] Paul Pollack. *Prime polynomials over finite fields*. PhD thesis, May 2008. `http://pollack.uga.edu/thesis/thesis-final.pdf`.

[Por20] Sam Porritt. *Some topics in the analytic number theory of polynomials over a finite field*. PhD thesis, 2020. `https://discovery.ucl.ac.uk/id/eprint/10101953/1/Porritt%20theis.pdf`.

[Ros99] Michael Rosen. A generalization of Mertens' theorem. *J. Ramanujan Math. Soc.*, 14(1):1–19, 1999.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[RS94] Michael Rubinstein and Peter Sarnak. Chebyshev's bias. *Experiment. Math.*, 3(3):173–197, 1994.

[Sed22] Youssef Sedrati. Inequities in the Shanks-Renyi prime number race over function fields. *Mathematika*, 68(3):840–895, 2022.

[Tao19] Terence Tao. A function field analogue of riemann zeta statistics, May 2019. `https://terrytao.wordpress.com/tag/function-fields/`.

[Tsc53] PL Tschebyschef. Lettre de m. le professeur tchebychev à m. fuss, sur un nouveau théorème relatif aux nombres premiers contenus dans les formes 4 n±1 et 4 n±3. *Bulletin de l'Académie impériale des sciences de Saint-Pétersbourg*, 11:208, 1853.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann et Cie., Paris, 1948.