Université de Montréal

Étude du nombre de polynômes irréductibles dans les corps finis avec certaines contraintes imposées aux coefficients

par

Gabriel Beauchamp Houde

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

24 août 2016

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

Étude du nombre de polynômes irréductibles dans les corps finis avec certaines contraintes imposées aux coefficients

présenté par

Gabriel Beauchamp Houde

a été évalué par un jury composé des personnes suivantes :

Dimitrios Koukoulopoulos
(président-rapporteur)

Matilde Lalin
(directeur de recherche)

Abraham Broer
(membre du jury)

Mémoire accepté le
Date d'acceptation

SOMMAIRE

L'objectif de ce mémoire est de dénombrer les polynômes irréductibles unitaires sur un corps fini en prescrivant des contraintes sur les coefficients. Dans les prochaines pages, il sera question de fixer simplement des coefficients, ou simplement de fixer leur signe, leur cubicité ou leur quarticité.

Mots clés : polynôme irréductible, somme de Gauss, corps fini, trace, caractère

SUMMARY

The objective of this thesis is to count monic irreducible polnomials over a finite field under some conditions on the coefficients of the polynomial. These conditions will be simply to fix some coefficients, or to fix their sign, cubicity or quarticity.

Keywords : irreducible polynomial, Gauss sum, finite field, trace, character

TABLE DES MATIÈRES

REMERCIEMENTS

D'entrée de jeu, je voudrais remercier Matilde, qui malgré son emploi du temps très chargé, a pris mon projet à coeur et a accepté de m'épauler. Je remercie aussi mes parents, qui m'ont toujours encouragé dans mes études et qui m'ont permis de me consacrer pleinement à ce mémoire.

INTRODUCTION

Soit $\mathbb{F}_q$ un corps fini de $q = p^k$ éléments, avec p un nombre premier et k un entier positif. Considérons un polynôme $M(x) \in \mathbb{F}_q[x]$ unitaire de degré n de la forme

$$x^n + t_1 x^{n-1} + t_2 x^{n-2} + t_3 x^{n-3} + \cdots + t_n. \tag{0.0.1}$$

Commençons notre étude par énoncer un résultat très connu dans la littérature qui constitue en quelques sortes le résultat pionnier de ce mémoire.

Théorème 0.0.1. *Soit $N(n, q)$ le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$. Alors*

$$N(n, q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}},$$

où μ dénote la fonction de Möbius.

Une question naturelle est de se demander ce qui arrive lorsque nous imposons une ou plusieurs contraintes aux coefficients d'un polynôme de la forme (0.0.1). Le but de ce mémoire est de répondre à cette question dans certains cas bien précis. Pour ce faire, nous utiliserons une méthode qui consiste à étudier une fonction L, dénotée par $L(s, \chi)$, qui est associée à un caractère χ d'un certain groupe abélien. Cette méthode, qui sera décrite et utilisée plusieurs fois au cours de ce mémoire, a permis à Carlitz [**4**] de trouver une formule exacte pour le nombre de polynômes irréductibles unitaires avec le premier coefficient, t_1, fixé. Cette méthode lui a aussi permis de trouver une formule asymptotique pour le nombre de polynômes irréductibles unitaires avec les premier et dernier coefficients fixés. Par la suite, Kuz'min [**9**] a été en mesure de trouver une formule exacte en fixant les deux premiers coefficients, $(t_1, t_2) = (a_1, a_2)$. Plus le nombre de coefficients fixés augmentent, plus cette méthode nous réserve des difficultés. C'est pourquoi les chercheurs ont commencé à fixer des contraintes un peu moins fortes sur les coefficients. Par exemple, si nous définissons le signe d'un élément quelconque

d'un corps $a \in \mathbb{F}_q$ par le symbole de Legendre

$$sgn(a) = \left(\frac{a}{q}\right) = \begin{cases} 0 & a = 0, \\ 1 & a \text{ est un carré dans } \mathbb{F}_q^*, \\ -1 & a \text{ n'est pas un carré dans } \mathbb{F}_q^*, \end{cases}$$

alors nous pouvons nous questionner sur le nombre de polynômes irréductibles unitaires dont le premier coefficient, t_1, et le signe du dernier, $\left(\frac{t_n}{q}\right)$, sont fixés. Alors, le caractère associé à la fonction $L(s, \chi)$ devient plus facile à manipuler, ce qui a permis à Carlitz de fournir un résulat exact (voir [**4**]).

Pour ce qui est de la suite des choses, quelques résultats partiels concernant le cas où les trois premiers coefficients sont fixés ont été publiés par Kuz'min [**10**]. En effet, il a travaillé avec des polynômes de degré 4 et 5 et est parvenu à établir certaines formules.

Présentons maintenant le résultat asymptotique général. Soit $f(x) \in \mathbb{F}_q[x]$ un polynôme de la forme (0.0.1). Fixons les k premiers coefficients : $a_1 = t_1$, $a_2 = t_2$, ... , $a_k = t_k$. Posons $M(x) \in \mathbb{F}_q[x]$ un polynôme unitaire de degré $m < n$ et $R(x) \in \mathbb{F}_q[x]$ tel que $\deg R < \deg M$. Supposons que k est un entier positif tel que $k + m < n$. Définissons $\pi(n, \mathbf{a}_k, M, R)$ le nombre de polynômes irréductibles unitaires $f(x) \in \mathbb{F}_q[x]$ de degré n dont les k premiers coefficients sont $\mathbf{a}_k = (a_1, \ldots, a_k)$ et qui respectent la congruence

$$f \equiv R \mod M.$$

Lorsque $M(x) = x^m$ and $R(0) \neq 0$, ceci prescrit les m derniers coefficients de m, en plus des k premiers. Hayes, en se basant sur la théorie des caractères et des fonctions L dans un contexte général, a démontré que

Théorème 0.0.2 (Hayes, p. 339, [**5**])**.**

$$\pi(n, \boldsymbol{a}_k, M, R) = \frac{q^{n-k}}{n\Phi(M)} + O\left(\frac{q^{\alpha n}}{n}\right),$$

pour un certain $\alpha < 1$ fixé et où Φ représente la fonction d'Euler pour les polynômes.

Dans ce mémoire, nous fournirons un résultat concernant le cas où $(t_1, t_2, sgn(t_n))$ est fixé et égal à $(a_1, a_2, sgn(a_n))$. Selon le Théorème 0.0.2, le nombre de polynômes irréductibles de cette forme vaut

$$\frac{q^{n-2}}{2n} + O\left(\frac{q^{\alpha n}}{n}\right),$$

pour $\alpha < 1$.

À la Section 1 du Chapitre 2, nous montrerons, en utilisant la méthode développée par Carlitz, que le nombre de polynômes irréductibles unitaires de cette forme suit la relation

$$\frac{q^{n-2}}{2n} + O\left(\frac{(18,0625q)^{\frac{n}{2}}}{n}\right),$$

ce qui donne une certaine précision sur le α du Théorème 0.0.2.

Par la suite, dans le même ordre d'idées, nous démontrerons une formule semblable, qui traite le cas où les trois premiers coefficients, (t_1, t_2, t_3), sont fixés à (a_1, a_2, a_3). Toujours selon le Théorème 0.0.2, il est clair que le nombre de polynômes irréductibles unitaires de cette forme vaut

$$\frac{q^{n-3}}{n} + O\left(\frac{q^{\alpha n}}{n}\right),$$

encore une fois pour un certain $\alpha < 1$.

Nous apporterons une précision sur ce α dans la deuxième section du Chapitre 2. En effet, nous montrerons que le nombre de polynômes irréductibles unitaires de cette forme est

$$\frac{q^{n-3}}{n} + O\left(\frac{(6,25q)^{\frac{n}{2}}}{n}\right).$$

Malheureusement, ces résultats asympotiques qui seront démontrés au Chapitre 2 ne représentent pas les meilleures approximations qui sont connues à ce jour. En effet, dans [**3**], Car, en utilisant une théorie plus approfondie des fonctions L, prouve, avec les notations introduites ci-haut et utilisées dans [**5**], que

Théorème 0.0.3 (Car, Théorème 2.1, [**5**])**.**
$$\frac{1}{n}\left(\frac{q^{n-k}}{\Phi(M)} - (k+m+1)q^{\frac{n}{2}}\right) \leq \pi(n, \boldsymbol{a}_k, M, R) \leq \frac{1}{n}\left(\frac{q^{n-k}}{\Phi(M)} + (k+m-1)q^{\frac{n}{2}}\right).$$

Nous voyons qu'en fait, le terme d'erreur est de l'ordre de $\frac{q^{\frac{n}{2}}}{n}$. De plus, lorsque nous fixons le signe, le terme d'erreur devient $\frac{q^{\frac{n}{2}+1}}{n}$. Tout de même, au Chapitre 2, nous expliquerons en détails la méthode de Carlitz, ce qui servira d'introduction pour la suite des choses.

En poursuivant, tel que mentionné ci-haut, Carlitz, dans [**4**], a montré que le nombre de polynômes irréductibles avec le premier et le dernier coefficient qui sont fixés suit la relation
$$\frac{q^{n-1}}{n(q-1)} + O\left(q^{\frac{n}{2}}\right).$$

Aux Chapitres 3 et 4, suivant les traces qui ont mené à ce dernier résultat, nous nous intéresserons à la cubicité et à la quarticité de t_n, et ce pour trouver une expression presqu'exacte (à un signe près) du nombre de polynômes irréductibles dont le premier coefficient et la cubicité/quarticité du dernier sont fixés. En effet, nous montrerons que, si $p \equiv 1 \mod 3$, alors le nombre de polynômes irréductibles unitaires dont le premier coefficient et la cubicité du dernier sont fixés suit la relation
$$\frac{q^{n-1}}{3} + g_1(n, q, t_1, t_n),$$
où $g_1(n, q, t_1, t_n) = O\left(q^{\frac{n}{3}}\right)$ est une fonction qui dépend du premier et du dernier coefficient, et qui sera explicitée dans ce mémoire.

De plus, nous fournirons un résultat semblable, mais en fixant la quarticité du dernier coefficient au lieu de la cubicité. Nous montrerons que, si $p \equiv 1 \mod 4$, alors le nombre de polynômes irréductibles de cette forme est
$$\frac{q^{n-1}}{4} + g_2(n, q, t_1, t_n),$$
où $g_1(n, q, t_1, t_n) = O\left(q^{\frac{n}{4}}\right)$ est une fonction qui encore une fois dépend du premier et du dernier coefficient et qui sera explicitée dans ce mémoire.

Enfin, avant de nous lancer dans la démonstration de ces résultats, nous prendrons le temps d'établir toutes les notions mathématiques nécessaires afin d'assurer une bonne compréhension du sujet. Tout d'abord, puisque nous travaillons dans $\mathbb{F}_q$, nous ferons quelques rappels de base concernant les corps finis. Ensuite, nous présenterons plusieurs éléments pertinents concernant la théorie des sommes de Gauss sur laquelle nous nous appuierons en grande partie afin de démontrer nos résultats.

Chapitre 1

THÉORIE

1.1. Quelques éléments de la théorie des corps finis

Dans cette section, tel que mentionné dans l'introduction, quelques concepts de base en théorie des corps qui serviront grandement pour la suite des choses sont présentés.

Prenons un corps corps fini à $q = p^k$ éléments dénoté par $\mathbb{F}_q$. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique, et possède donc un générateur. De plus, tous les sous-corps de $\mathbb{F}_q$ sont les corps $\mathbb{F}_{p^d}$, avec $d|k$.

Le restant de cette section est dédié à l'introduction de deux applications très importantes en théorie des corps : la trace et la norme. La trace sera omniprésente dans ce mémoire puisqu'elle sera utilisée dans les caractères que nous poserons et qui seront associés à la fonction L. Quant à la norme, supposons que nous avons un résultat bien connu dans $\mathbb{F}_p$ et que nous voulons l'étendre dans $\mathbb{F}_q$. Alors, la norme joue un rôle primordial dans cette quête. Ainsi, la trace et la norme font l'objet des deux prochaines définitions.

Définition 1.1.1. *Soit $q = p^k$. Nous définissons la trace d'un élément du corps de la manière suivante :*

$$Tr = Tr_{\mathbb{F}_q/\mathbb{F}_p} : \begin{cases} \mathbb{F}_q \to \mathbb{F}_p \\ x \mapsto x + x^p + \cdots + x^{p^{k-1}}. \end{cases}$$

Définition 1.1.2. *Soit $q = p^k$. Nous définissons la norme d'un élément du corps de la manière suivante :*

$$N = N_{\mathbb{F}_q/\mathbb{F}_p} : \begin{cases} \mathbb{F}_q \to \mathbb{F}_p \\ x \mapsto x \cdot x^p \cdot \ldots \cdot x^{p^{k-1}} = x^{\frac{q-1}{p-1}}. \end{cases}$$

Remarque 1.1.1. *Les éléments $x, x^p, \cdots, x^{p^{k-1}}$ des deux définitions précédentes sont appelés les conjugués de x. La trace est donc la somme des conjugués de x, tandis que la norme représente le produit des conjugués de x.*

Cette section se termine avec un théorème sur la trace qui est essentiel pour l'évaluation de sommes de Gauss, sujet que nous traiterons dans les prochaines sections.

Théorème 1.1.1. *L'application trace, $Tr_{\mathbb{F}_q/\mathbb{F}_p}$, avec $q = p^k$, est une application surjective.*

Démonstration. Nous allons tout d'abord commencer par montrer qu'il s'agit d'une transformation linéaire entre $\mathbb{F}_p$-espaces vectoriels. Par la suite, pour montrer qu'elle est surjective, nous devons montrer l'existence d'un élément $\alpha \in \mathbb{F}_q$ tel que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \neq 0$. Alors, pour $a, b \in \mathbb{F}_q$, nous avons que

$$\begin{aligned} Tr_{\mathbb{F}_q/\mathbb{F}_p}(a+b) &= a + b + (a+b)^p + ... + (a+b)^{p^{k-1}} \\ &= a + b + a^p + b^p + ... + a^{p^{k-1}} + b^{p^{k-1}} \\ &= Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) + Tr_{\mathbb{F}_q/\mathbb{F}_p}(b), \end{aligned}$$

où nous avons utilisé le fait que, dans un corps de caractéristique p, $(x+y)^{p^i} = x^{p^i} + y^{p^i}$, et ce, quelque soit $x, y \in \mathbb{F}_q$ et $i \in \mathbb{N}$.

Ensuite, pour $c \in \mathbb{F}_p$, il est clair que $c^{p^j} = c$ pour tout $j \geq 0$. Alors, pour $a \in \mathbb{F}_q$, nous avons que

$$\begin{aligned} Tr_{\mathbb{F}_q/\mathbb{F}_p}(ca) &= ca + c^p a^p + ... + c^{p^{k-1}} a^{p^{k-1}} \\ &= ca + ca^p + ... + ca^{p^{k-1}} \\ &= cTr_{\mathbb{F}_q/\mathbb{F}_p}(a). \end{aligned}$$

Ces deux dernières propriétés, combinées au fait que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) \in \mathbb{F}_p$ pour tout $a \in \mathbb{F}_q$, montre que l'application est bel et bien linéaire. Ensuite, pour $\alpha \in \mathbb{F}_q$, $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$ si et seulement si α est une racine du polynôme $x^{p^{k-1}} + ... + x^p + x$. Ce polynôme, de degré p^{k-1}, a au plus p^{k-1} racines dans $\mathbb{F}_q$, et $\mathbb{F}_q$ contient p^k éléments. Il existe donc un élément $\alpha \in \mathbb{F}_q$ tel que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \neq 0$.

□

Ceci met fin au bref résumé de la théorie des corps finis. Dans les prochaines sections, nous aborderons des concepts qui sont plus intimement liés à notre problématique.

1.2. Réciprocité quadratique

Beaucoup de résultats présentés dans ce mémoire se basent sur la résolution d'équations du second degré dans les corps finis. Dans cette section, d'autres définitions et théorèmes de base seront explicités. Reprenons $\mathbb{F}_q$ un corps fini à $q = p^k$ éléments, p étant un nombre premier impair. Soit une équation quadratique définie comme suit :

$$aX^2 + bX + c = 0,$$

où $a, b, c \in \mathbb{F}_q$ et $a \neq 0$.

Par hypothèse, $(4, p) = 1$. Donc, $4a \neq 0$, et nous pouvons ainsi multiplier l'équation quadratique ci-haut par $4a$:

$$4a^2X^2 + 4abX + 4ac = 0 \Leftrightarrow (2aX + b)^2 = b^2 - 4ac.$$

Puisque l'équation $Y = 2aX + b$ possède toujours une solution, ce problème revient donc à trouver un élément du corps Y qui est solution de :

$$Y^2 = b^2 - 4ac.$$

Donc, nous n'avons qu'à étudier l'équation $Y^2 = n$ pour tout connaître sur les équations quadratiques. Il est bien à ce stade de rappeler le signe d'un élément quelconque $a \in \mathbb{F}_q$, que nous avons déjà introduit et qui a son importance en théorie des nombres (et particulièrement dans ce mémoire) :

$$sgn(a) = \left(\frac{a}{q}\right) = \begin{cases} 0 & a = 0, \\ 1 & a \text{ est un carré dans } \mathbb{F}_q^*, \\ -1 & a \text{ n'est pas un carré dans } \mathbb{F}_q^*. \end{cases}$$

Le symbole $\left(\frac{a}{q}\right)$ est appelé symbole de Legendre, et sera énormément utilisé pour la suite des choses. Nous sommes maintenant prêts à prouver un premier théorème le concernant.

Théorème 1.2.1 (Critère d'Euler)**.** *Soit $\mathbb{F}_q$ un corps de $q = p^k$ éléments. Alors, $\forall a \in \mathbb{F}_q$, nous avons*

$$\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}}.$$

Démonstration. Supposons que $a \neq 0$ est un carré dans $\mathbb{F}_q$. Alors, il existe $x \in \mathbb{F}_q^*$ tel que $x^2 = a$. En élevant cette équation à la puissance $\frac{q-1}{2}$ et en utilisant

le fait que $\mathbb{F}_q^*$ est un groupe abélien d'ordre $q-1$, nous obtenons :

$$a^{\frac{q-1}{2}} = (x^2)^{\frac{q-1}{2}} = x^{q-1} = 1 = \left(\frac{a}{q}\right).$$

Supposons maintenant que a n'est pas un carré dans $\mathbb{F}_q^*$. Pour chaque $b \in \mathbb{F}_q^*$, il existe un seul $c \in \mathbb{F}_q^*$ tel que $bc = a$. Nous pouvons grouper b et c en $\frac{q-1}{2}$ couples, et en les multipliant, nous obtenons :

$$\prod_{\alpha \in \mathbb{F}_q^*} \alpha = \left(\prod_{b \in \mathbb{F}_q^*; bc=a} (bc) \right)^{\frac{1}{2}} = a^{\frac{q-1}{2}}.$$

Nous obtenons $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$ en choisissant une racine primitive γ du corps :

$$\prod_{\alpha \in \mathbb{F}_q^*} \alpha = \gamma^{\sum_{i=1}^{q-1} i} = \gamma^{\frac{q(q-1)}{2}} = \left(\gamma^{\frac{q-1}{2}}\right)^q = (-1)^q = -1,$$

car q est impair.

Nous concluons donc que

$$a^{\frac{q-1}{2}} = -1 = \left(\frac{a}{q}\right).$$

□

Du critère d'Euler suit immédiatement un corollaire d'une grande utilité : le signe de -1 dans un corps fini.

Corollaire 1.2.1. *Nous avons que*

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 & q \equiv 1 \mod 4, \\ -1 & q \equiv 3 \mod 4. \end{cases}$$

D'autres propriétés découlent du critère d'Euler :

$$\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right) \tag{1.2.1}$$

$$\left(\frac{a}{q}\right) = \left(\frac{a^{-1}}{q}\right) \tag{1.2.2}$$

$$\left(\frac{a^2}{q}\right) = 1 \tag{1.2.3}$$

$$\left(\frac{1}{q}\right) = 1. \tag{1.2.4}$$

La propriété (1.2.1) indique que le symbole de Legendre est une fonction multiplicative. Notons aussi que (1.2.2) et (1.2.3) ne sont valides que pour $a \neq 0$. Bref, ces propriétés seront grandement utilisées lors du calcul des sommes de Gauss, que nous entamons dès la prochaine section.

1.3. Sommes de Gauss

1.3.1. Caractères

Les sommes de Gauss sont au coeur de la technique que nous employerons afin de procéder au dénombrement des polynômes irréductibles sur un corps fini. Dans cette section, nous introduisons la notion de caractères, essentielle dans l'étude de ce type de sommes. Il y a deux types de caractères d'importance : les caractères additifs et les caractères multiplicatifs. Commençons par définir le caractère additif que nous utiliserons tout au long de ce mémoire.

Définition 1.3.1.1. *Soit ψ un caractère additif défini pour tout $a \in \mathbb{F}_q$ par :*

$$\psi(a) = e^{\frac{2\pi i Tr(a)}{p}}.$$

Nous disons que le caractère est additif dans le sens où, pour $a, b \in \mathbb{F}_q$, $\psi(a+b) = \psi(a)\psi(b)$. Ceci découle simplement des propriétés de la trace.

Avec cette définition, nous sommes déjà en mesure de prouver deux théorèmes de base.

Théorème 1.3.1.1. *Nous avons que*

$$\sum_{a \in \mathbb{F}_q} \psi(a) = 0.$$

Démonstration. Par la surjectivité de la trace, il existe $b \in \mathbb{F}_q$ tel que $\psi(b) \neq 1$. Donc,

$$\psi(b) \sum_{a \in \mathbb{F}_q} \psi(a) = \sum_{a \in \mathbb{F}_q} \psi(a+b) = \sum_{a \in \mathbb{F}_q} \psi(a).$$

D'où

$$(\psi(b) - 1) \sum_{a \in \mathbb{F}_q} \psi(a) = 0.$$

□

Remarque 1.3.1.1. *Ce dernier théorème est valide quelque soit le caractère non trivial et le groupe abélien choisi.*

Corollaire 1.3.1.1. *Soit $\lambda_1, \lambda_2 \in \mathbb{F}_q$, avec $\lambda_1 \neq 0$. Alors,*

$$\sum_{a \in \mathbb{F}_q} \psi(\lambda_1 a + \lambda_2) = 0.$$

DÉMONSTRATION. Comme il y a bijection entre les ensembles $\{a | a \in \mathbb{F}_q\}$ et $\{\lambda_1 a + \lambda_2 | a, \lambda_1, \lambda_2 \in \mathbb{F}_q, \lambda_1 \neq 0\}$, alors le résultat suit. □

Passons maintenant à la définition des caractères multiplicatifs de $\mathbb{F}_q$.

Définition 1.3.1.2. *Soit γ une racine primitive de $\mathbb{F}_q$. Alors, pour tout $j = 0, 1, 2, , , , q-2$, la fonction φ_j donnée par*

$$\varphi_j(\gamma^r) = e^{\frac{2\pi i j r}{q-1}}$$

et

$$\varphi_j(0) = 0,$$

pour $r = 0, 1, 2, ..., q-2$, définit un caractère multiplicatif, dans le sens où, pour $a, b \in \mathbb{F}_q$, alors $\varphi_j(ab) = \varphi_j(a)\varphi_j(b)$.

Dans ce mémoire, trois caractères multiplicatifs bien précis seront utilisés. Reprenons une racine primitive γ et un élément quelconque $a \in \mathbb{F}_q$ tel que $a = \gamma^r$. Tout d'abord, en posant $j = \frac{q-1}{2}$ dans la Definition 1.3.1.2, nous avons le caractère multiplicatif suivant bien connu, qui est simplement le symbole de Legendre :

$$\left(\frac{a}{q}\right).$$

Ensuite, en supposant que $3|q-1$, nous pouvons poser $j = \frac{q-1}{3}$ et obtenir le caractère d'ordre 3 suivant :

$$\left(\frac{a}{q}\right)_{(3)} = \begin{cases} 0 & a = 0, \\ 1 & 3|r, \\ e^{\frac{2\pi i}{3}} & r \equiv 1 \mod 3, \\ e^{\frac{4\pi i}{3}} & r \equiv 2 \mod 3. \end{cases}$$

Enfin, en supposant que $4|q-1$, nous pouvons poser $j = \frac{q-1}{4}$ et obtenir le caractère d'ordre 4 suivant :

$$\left(\frac{a}{q}\right)_{(4)} = \begin{cases} 0 & a = 0, \\ 1 & 4|r, \\ i & r \equiv 1 \mod 4, \\ -1 & r \equiv 2 \mod 4, \\ -i & \equiv 3 \mod 4. \end{cases}$$

Terminons avec quelques propriétés utiles sur ces caractères multiplicatifs.

Lemme 1.3.1.1. *Soient $\lambda_1, \lambda_2 \in \mathbb{F}_q$, avec $\lambda_1 \neq 0$. Alors,*

$$\sum_{a \in \mathbb{F}_q} \left(\frac{\lambda_1 a + \lambda_2}{q}\right) = \sum_{a \in \mathbb{F}_q} \left(\frac{a}{q}\right) = 0.$$

Démonstration. Comme, dans $\mathbb{F}_q$, il y a l'élément nul, $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés, il est facile de voir que

$$\sum_{a \in \mathbb{F}_q} \left(\frac{a}{q}\right) = 0.$$

Comme il y a bijection entre les ensembles $\{a | a \in \mathbb{F}_q\}$ et $\{\lambda_1 a + \lambda_2 | a, \lambda_1, \lambda_2 \in \mathbb{F}_q, \lambda_1 \neq 0\}$, le résultat suit.

□

De manière similaire, pour nos caractères d'ordre 3 et 4, il est assez facile d'obtenir ces relations :

Lemme 1.3.1.2. *Nous avons que*

$$\sum_{a \in \mathbb{F}_q} \left(\frac{a}{q}\right)_{(3)} = \sum_{a \in \mathbb{F}_q} \left(\frac{a^2}{q}\right)_{(3)} = 0,$$

pour $3|q-1$, et

$$\sum_{a \in \mathbb{F}_q} \left(\frac{a}{q}\right)_{(4)} = \sum_{a \in \mathbb{F}_q} \left(\frac{a^3}{q}\right)_{(4)} = 0,$$

pour $4|q-1$.

1.3.2. Sommes de Gauss quadratiques

Nous avons traité, dans la section précédente, du type de sommation de la forme :

$$\sum_{a\in\mathbb{F}_q} \psi(\lambda_1 a + \lambda_2),$$

avec $\lambda_1, \lambda_2 \in \mathbb{F}_q$.

La suite naturelle des choses serait de vouloir fournir une expression pour

$$\sum_{a\in\mathbb{F}_q} \psi(\lambda_1 a^2 + \lambda_2 a + \lambda_3), \tag{1.3.1}$$

avec $\lambda_1 \neq 0$.

Le but de cette section est de répondre à ce besoin, essentiel lorsque nous poserons des contraintes sur plusieurs coefficients. Commençons d'entrée de jeu avec une définition de base.

Définition 1.3.2.1. *Soit $b \in \mathbb{F}_q$. Nous définissons une somme de Gauss par*

$$G_\psi(b) = \sum_{a\in\mathbb{F}_q} \left(\frac{a}{q}\right) \psi(ba).$$

Soit b un élément quelconque du corps $\mathbb{F}_q$. Le prochain théorème montre une relation entre $G_\psi(b)$ et $G_\psi(1)$, en plus de fournir une expression pour $G_\psi(1)^2$.

Théorème 1.3.2.1. *Nous avons les deux relations suivantes :*

$$G_\psi(b) = \left(\frac{b}{q}\right) G_\psi(1), \tag{1.3.2}$$

$$G_\psi(1)^2 = \left(\frac{-1}{q}\right) q. \tag{1.3.3}$$

Démonstration. Commençons par l'équation (1.3.2) : Le cas $b = 0$ est trivial. Supposons $b \neq 0$. Alors,

$$G_\psi(b) = \sum_{a\in\mathbb{F}_q} \left(\frac{a}{q}\right) \psi(ba) = \sum_{a\in\mathbb{F}_q} \left(\frac{ab^{-1}}{q}\right) \psi(a) = \left(\frac{b}{q}\right) G_\psi(1),$$

où la dernière égalité découle du fait que $\left(\frac{b^{-1}}{q}\right) = \left(\frac{b}{q}\right)$.

Pour l'équation (1.3.3), nous avons que

$$\begin{aligned} G_\psi(1)^2 &= \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\left(\frac{ab}{q}\right)\psi(a+b) = \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\left(\frac{ab^{-1}}{q}\right)\psi(a+b) \\ &= \sum_{u\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\left(\frac{u}{q}\right)\psi(b(u+1)) = \sum_{u\neq -1}\left(\frac{u}{q}\right)\sum_{b\in\mathbb{F}_q}\psi(b(u+1)) + \left(\frac{-1}{q}\right)q \\ &= \left(\frac{-1}{q}\right)q, \end{aligned}$$

où le changement de variable $u = ab^{-1}$ a été effectué et le Théorème 1.3.1.1 a été utilisé. □

Continuons avec une petite astuce qui nous aidera à résoudre (1.3.1). Soit $a \in \mathbb{F}_q^*$, alors

$$1 + \left(\frac{a}{q}\right) = \begin{cases} 2 & a \text{ est un carré dans } \mathbb{F}_q^*, \\ 0 & a \text{ n'est pas un carré dans } \mathbb{F}_q^*. \end{cases}$$

Nous pouvons donc écrire que

$$\sum_{a\in\mathbb{F}_q}\psi(a^2) = \sum_{a\in\mathbb{F}_q}\left(1+\left(\frac{a}{q}\right)\right)\psi(a), \tag{1.3.4}$$

puisqu'il y a exactement $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q$, et qu'ils seront sommés deux fois.

Avec le Théorème 1.3.2.1 et (1.3.4), nous sommes en mesure de donner une expression pour (1.3.1).

Théorème 1.3.2.2. *Soient $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ et $\lambda_1 \neq 0$. Alors,*

$$\sum_{a\in\mathbb{F}_q}\psi(\lambda_1 a^2 + \lambda_2 a + \lambda_3) = \psi\left(\lambda_3 - \frac{\lambda_2^2}{4\lambda_1}\right)\left(\frac{\lambda_1}{q}\right)G_\psi(1).$$

Démonstration. En complétant le carré et en utilisant (1.3.4), nous obtenons :

$$\begin{aligned} \sum_{a\in\mathbb{F}_q}\psi(\lambda_1 a^2 + \lambda_2 a + \lambda_3) &= \psi\left(\lambda_3 - \frac{\lambda_2^2}{4\lambda_1}\right)\sum_{a\in\mathbb{F}_q}\psi\left(\lambda_1\left(a + \frac{\lambda_2}{2\lambda_1}\right)^2\right) \\ &= \psi\left(\lambda_3 - \frac{\lambda_2^2}{4\lambda_1}\right)\sum_{a\in\mathbb{F}_q}\psi(\lambda_1 a^2) \\ &= \psi\left(\lambda_3 - \frac{\lambda_2^2}{4\lambda_1}\right)\sum_{a\in\mathbb{F}_q}\left(1+\left(\frac{a}{q}\right)\right)\psi(\lambda_1 a) \end{aligned}$$

$$= \psi\left(\lambda_3 - \frac{\lambda_2^2}{4\lambda_1}\right) \sum_{a\in\mathbb{F}_q} \left(\frac{a}{q}\right) \psi(\lambda_1 a)$$
$$= \psi\left(\lambda_3 - \frac{\lambda_2^2}{4\lambda_1}\right) \left(\frac{\lambda_1}{q}\right) G_\psi(1).$$

□

Soit $f(x) \in \mathbb{F}_q[x]$, un polynôme de degré n. Pour $n \geq 3$, nous devons la plupart du temps nous limiter à des résultats non exacts pour $\sum_{a\in\mathbb{F}_q} \psi(f(a))$. Voici un théorème qui nous donnera un bon coup de main au prochain chapitre.

Théorème 1.3.2.3 (Weil, Théorème 5.38, [**11**]). *Soit $f \in \mathbb{F}_q[x]$ un polynôme de degré $n \geq 1$ avec $pgcd(n, q) = 1$ et soit Ψ un caractère additif non trivial de $\mathbb{F}_q$. Alors,*

$$\left|\sum_{a\in\mathbb{F}_q} \Psi(f(a))\right| \leq (n-1)\sqrt{q}.$$

Soulignons qu'une borne triviale pour $\left|\sum_{a\in\mathbb{F}_q} \Psi(f(a))\right|$ est q. Le dernier théorème peut apporter une meilleure estimation.

Pour la suite, nous allons étudier de plus près la somme de Gauss $G_\psi(1)$. Ces démarches ont leur importance, puisque nous aurons besoin de cette valeur dans le Chapitre 4, lorsque nous travaillerons avec la quarticité du dernier coefficient. D'après l'équation (1.3.3) du Théorème 1.3.2.1, nous pouvons voir que

$$G_\psi(1) = \begin{cases} \pm\sqrt{q} & q \equiv 1 \mod 4, \\ \pm i\sqrt{q} & q \equiv 3 \mod 4. \end{cases}$$

Il y a donc un questionnement quant au signe d'une somme de Gauss. Considérons le cas $q = p$. Gauss a réussi à trouver le signe de $G_\psi(1)$ dans ce cas bien particulier.

Théorème 1.3.2.4 (Gauss, p. 109-110, [**2**]). *Sous le corps $\mathbb{F}_p$, nous avons le résultat suivant :*

$$G_\psi(1) = \begin{cases} \sqrt{p} & p \equiv 1 \mod 4, \\ i\sqrt{p} & p \equiv 3 \mod 4. \end{cases}$$

Nous venons de donner la valeur exacte de $G_\psi(1)$ dans le cas $\mathbb{F}_q = \mathbb{F}_p$, mais nous sommes plutôt intéressés à avoir cette formule dans le cas général d'un corps

$\mathbb{F}_q$. Donnons d'abord une définition qui introduit un concept essentiel pour le passage de $\mathbb{F}_p$ vers $\mathbb{F}_q$.

Définition 1.3.2.2. *Soient Ψ un caractère additif et φ un caractère multiplicatif, tous les deux de $\mathbb{F}_q$. Nous pouvons alors étendre ces deux caractères vers l'extension $\mathbb{F}_{q^s}$ en posant $\Psi^{(s)}(\delta) = \Psi(Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\delta))$ pour $\delta \in \mathbb{F}_{q^s}$ et $\varphi^{(s)}(\delta) = \varphi(N_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\delta))$ pour $\delta \in \mathbb{F}_{q^s}^*$.*

Énonçons maintenant le théorème qui permettra de passer d'un corps à l'autre.

Théorème 1.3.2.5 (Davenport-Hasse, Théorème 5.14, [**11**])**.** *Soient deux caractères de $\mathbb{F}_q$: Ψ qui est additif et φ qui est multiplicatif. Au plus un de ces deux caractères est trivial. Supposons que Ψ et φ sont prolongés vers $\Psi^{(s)}$ et $\varphi^{(s)}$, deux caractères de $\mathbb{F}_{q^s}$. Alors*

$$G(\varphi^{(s)}, \Psi^{(s)}) = (-1)^{s-1} G(\varphi, \Psi)^s.$$

Avec les Théorèmes 1.3.2.4 et 1.3.2.5, nous pouvons déterminer la valeur de $G_\psi(1)$ tant recherchée.

Théorème 1.3.2.6. *Soit $\mathbb{F}_q$ un corps fini à $q = p^k$, $k \geq 1$ éléments. Alors,*

$$G_\psi(1) = \begin{cases} (-1)^{k-1}\sqrt{q} & p \equiv 1 \mod 4, \\ (-1)^{k-1} i^k \sqrt{q} & p \equiv 3 \mod 4. \end{cases}$$

Démonstration. En se servant du Théorème 1.3.2.4, nous n'avons qu'à prolonger les deux caractères (ψ, qui est additif, et $\left(\frac{\bullet}{q}\right)$, qui est multiplicatif) vers $\mathbb{F}_{p^k}$, et nous arrivons au résultat. □

Nous terminons la section en montrant la relation entre le symbole de Legendre et une somme de Gauss quadratique. En effet, il est possible d'écrire l'un en fonction de l'autre. Le prochain lemme le démontre. Il sera utilisé au prochain chapitre.

Lemme 1.3.2.1. *Soit $a \in \mathbb{F}_q^*$. Alors,*

$$\left(\frac{a}{q}\right) = \frac{c}{\sqrt{q}} \sum_{b \in \mathbb{F}_q} \psi(ab^2),$$

avec

$$c = \begin{cases} (-1)^{k-1} & p \equiv 1 \mod 4, \\ -i^k & p \equiv 3 \mod 4. \end{cases}$$

DÉMONSTRATION. En utilisant le Théorème 1.3.2.2 avec $\lambda_1 = a$ et $\lambda_2 = \lambda_3 = 0$, nous obtenons

$$\sum_{b \in \mathbb{F}_q} \psi(ab^2) = G_\psi(1) \left(\frac{a}{q} \right).$$

Par le Théorème 1.3.2.6, nous voyons que

$$\frac{c}{\sqrt{q}} G_\psi(1) = 1,$$

et nous pouvons conclure.

□

C'est ce qui met fin à cette section sur les sommes de Gauss quadratiques, indispensables pour les calculs qui nous ferons dans le prochain chapitre.

1.3.3. Sommes de Jacobi

Notre objectif pour les prochaines pages est simplement d'introduire de nouveaux types de sommes qui seront grandement utilisés lorsque nous aborderons les sommes de Gauss cubiques et quartiques. Dans cette section, φ et ϕ représentent deux caractères multiplicatifs quelconques modulo p. Alors, rappelons que pour $a, b \in \mathbb{F}_q$, nous avons que $\varphi(ab) = \varphi(a)\varphi(b)$ et $\phi(ab) = \phi(a)\phi(b)$. Remarquons aussi que $\varphi(0) = \phi(0) = 0$.

Commençons par deux définitions.

Définition 1.3.3.1. *Une somme de Jacobi $J(\varphi, \phi)$ est définie par*

$$J(\varphi, \phi) = \sum_{a \in \mathbb{F}_q} \varphi(a)\phi(1-a).$$

De plus, posons, pour simplifier la notation, $J(\varphi) = J(\varphi, \varphi)$.

Définition 1.3.3.2. *Rappelons que ψ est un caractère additif. Définissons la somme de Gauss généralisée $G_b(\varphi)$ de la manière suivante :*

$$G_b(\varphi) = \sum_{a \in \mathbb{F}_q} \varphi(a)\psi(ba).$$

Pour abréger l'écriture, écrivons $G_1(\varphi) = G(\varphi)$.

Avant de rentrer plus en détails, généralisons l'équation (1.3.3) du Théorème 1.3.2.1 :

Théorème 1.3.3.1. *Nous avons les deux relations suivantes :*

$$G(\varphi)G(\bar{\varphi}) = \varphi(-1)q$$

et

$$|G(\varphi)| = \sqrt{q}.$$

Démonstration. Les étapes de la preuve de la première relation sont les mêmes que celles de l'équation (1.3.3) du Théorème 1.3.2.1. Pour montrer que $|G(\varphi)| = \sqrt{q}$, nous allons évaluer

$$\sum_{b \in \mathbb{F}_q} G_b(\varphi)\overline{G_b(\varphi)}$$

de deux manières différentes.

Premièrement, si $b \neq 0$,

$$\overline{G_b(\varphi)} = \overline{\varphi(b^{-1})G(\varphi)} = \varphi(b)\overline{G(\varphi)}$$

et

$$G_b(\varphi) = \varphi(b^{-1})G(\varphi).$$

Donc,

$$G_b(\varphi)\overline{G_b(\varphi)} = G(\varphi)\overline{G(\varphi)} = |G(\varphi)|^2.$$

Si $b = 0$,

$$G_0(\varphi) = 0.$$

Nous pouvons conclure que

$$\sum_{b \in \mathbb{F}_q} G_b(\varphi)\overline{G_b(\varphi)} = (q-1)|G(\varphi)|^2.$$

Deuxièmement,

$$G_b(\varphi)\overline{G_b(\varphi)} = \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \varphi(x)\overline{\varphi(y)}\psi(bx - by).$$

D'où

$$\sum_{b\in\mathbb{F}_q} G_b(\varphi)\overline{G_b(\varphi)} = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \varphi(x)\overline{\varphi(y)} \sum_{b\in\mathbb{F}_q} \psi(b(x-y))$$
$$= \sum_{\substack{x=y\\ x\neq 0}} \varphi(x)\overline{\varphi(y)}q = (q-1)q.$$

En comparant, nous obtenons

$$(q-1)|G(\varphi)|^2 = (q-1)q.$$

□

En poursuivant, nous allons prouver deux résultats d'importance concernant les sommes de Jacobi qui aideront à comprendre les sommes de Gauss cubiques et quartiques.

Théorème 1.3.3.2. *Soient φ, ϕ et $\varphi\phi$ non triviales. Alors, les sommes de Gauss et de Jacobi suivent la relation suivante :*

$$J(\varphi,\phi) = \frac{G(\varphi)G(\phi)}{G(\varphi\phi)}.$$

De plus, il s'ensuit que

$$|J(\varphi,\phi)| = \sqrt{q}.$$

Démonstration. Nous devons montrer que $G(\varphi)G(\phi) = J(\varphi,\phi)G(\varphi\phi)$. Donc,

$$G(\varphi)G(\phi) = \sum_{a,b\in\mathbb{F}_q} \varphi(a)\phi(b)\psi(a+b)$$
$$= \sum_{u,a\in\mathbb{F}_q} \varphi(a)\phi(u-a)\psi(u)$$
$$= \sum_{a\in\mathbb{F}_q} \varphi(a)\phi(-a) + \sum_{\substack{u\in\mathbb{F}_q^*\\ c\in\mathbb{F}_q}} \varphi(uc)\phi(u(1-c))\psi(u),$$

en effectuant successivement les changements de variables $u = a+b$ et $a = cu$.

Nous allons montrer que $\sum_{a\in\mathbb{F}_q} \varphi(a)\phi(-a) = 0$. Puisque $\varphi\phi$ est non trivial, il existe $v \in \mathbb{F}_q^*$ tel que $\varphi(v)\phi(v) \neq 1$. Nous pouvons alors écrire

$$\sum_{a\in\mathbb{F}_q} \varphi(a)\phi(-a) = \sum_{a\in\mathbb{F}_q} \varphi(av)\phi(-av) = \varphi(v)\phi(v)\sum_{a\in\mathbb{F}_q} \varphi(a)\phi(-a).$$

D'où

$$(1-\varphi(v)\phi(v))\sum_{a\in\mathbb{F}_q}\varphi(a)\phi(-a)=0.$$

Comme $1-\varphi(v)\phi(v)\neq 0$, nous concluons que $\sum_{a\in\mathbb{F}_q}\varphi(a)\phi(-a)=0$. Ainsi,

$$\begin{aligned}G(\varphi)G(\phi)&=\sum_{\substack{u\in\mathbb{F}_q^*\\ c\in\mathbb{F}_q}}\varphi(uc)\phi(u(1-c))\psi(u)\\&=\sum_{u,c\in\mathbb{F}_q}\varphi(uc)\phi(u(1-c))\psi(u)\\&=J(\varphi,\phi)G(\varphi\phi).\end{aligned}$$

Finalement, le fait que $|J(\varphi,\phi)|=\sqrt{q}$ découle simplement de la seconde partie du Théorème 1.3.3.1.

□

Théorème 1.3.3.3. *Soit ℓ un entier supérieur ou égal à 3 et φ un caractère multiplicatif non trivial dont l'ordre divise ℓ. Alors,*

$$G(\varphi)^\ell=\varphi(-1)q\prod_{j=1}^{\ell-2}J(\varphi,\varphi^j).$$

Démonstration. Il est clair que, par le Théorème 1.3.3.2,

$$\prod_{j=1}^{\ell-2}J(\varphi,\varphi^j)=\prod_{j=1}^{\ell-2}\frac{G(\varphi)G(\varphi^j)}{G(\varphi^{j+1})}=\frac{G(\varphi)^{\ell-1}}{G(\varphi^{\ell-1})}=\frac{G(\varphi)^{\ell-1}}{G(\bar{\varphi})}.$$

Enfin, par le Théorème 1.3.3.1, nous avons que

$$\varphi(-1)q=G(\varphi)G(\bar{\varphi})$$

Ceci implique donc que

$$\varphi(-1)q\prod_{j=1}^{\ell-2}J(\varphi,\varphi^j)=G(\varphi)G(\bar{\varphi})\frac{G(\varphi)^{\ell-1}}{G(\bar{\varphi})}=G(\varphi)^\ell.$$

□

Dans les Sections 1.3.4 et 1.3.5, qui traiteront des sommes de Gauss cubiques et des sommes de Gauss quartiques, il est plus aisé de travailler avec $\varphi(4)J(\varphi)$ au lieu de $J(\varphi)$ simplement. Introduisons pour le moment la notation

$$K(\varphi)=\varphi(4)J(\varphi),$$

sachant que nous utiliserons cette notation plus tard.

Nous terminons cette section en prouvant un théorème impliquant $K(\varphi)$, qui nous sera d'une certaine utilité dans l'analyse des sommes de Gauss quartiques.

Théorème 1.3.3.4. *Reprenons notre caractère non trivial φ. Posons $\phi = \left(\frac{\bullet}{q}\right)$ le caractère quadratique. Alors,*

$$K(\varphi) = J(\varphi, \phi).$$

Démonstration. Soit $b \in \mathbb{F}_q$. Le nombre de solutions de l'équation $a(1-a) = b$ dans $\mathbb{F}_q$ est $1 + \phi(1-4b)$. Donc,

$$\begin{aligned} J(\varphi) &= \sum_{a\in\mathbb{F}_q} \varphi(a(1-a)) = \sum_{b\in\mathbb{F}_q} \varphi(b)(1+\phi(1-4b)) \\ &= \sum_{b\in\mathbb{F}_q} \varphi(b)\phi(1-4b) = \varphi(4)^{-1} \sum_{b\in\mathbb{F}_q} \varphi(b)\phi(1-b) \\ &= \varphi(4)^{-1} J(\varphi, \phi), \end{aligned}$$

en utilisant le fait que φ n'est pas triviale et donc que $\sum_{b\in\mathbb{F}_q} \varphi(b) = 0$, par une démarche identique à celle que nous avons utilisée à la démonstration du Théorème 1.3.3.2, pour montrer que $\sum_{a\in\mathbb{F}_q} \varphi(a)\phi(-a) = 0$.

Alors, il est clair que $K(\varphi) = J(\varphi, \phi)$.

□

Alors, nous avons maintenant les outils pour aborder les sommes de Gauss cubiques...

1.3.4. Sommes de Gauss cubiques

Dans cette section, nous devons avoir $p \equiv 1 \mod 3$, où p est la caractéristique du corps. De plus, φ représente un caractère multiplicatif modulo p d'ordre 3 sur $\mathbb{F}_p$. Observons tout d'abord que $\varphi(-1) = 1$. De plus, notons par Ω l'ensemble des entiers algébriques. Mentionnons qu'un entier algébrique est une racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. Pour ce qui suit, nous nous basons grandement sur les résultats qu'ont publiés Berndt et Evans (voir [**1**]). Ceux-ci ont par contre travaillé dans $\mathbb{F}_p$. Nous utiliserons le théorème de Davenport-Hasse pour étendre à $\mathbb{F}_q$.

Cette section est très théorique. Son importance va de soi, puisque dans celle-ci, nous montrerons le résultat pionnier qui permet de dénombrer (à un signe près)

le nombre de polynômes irréductibles dans un corps fini en fixant le premier coefficient et la cubicité du dernier. Le résultat que nous voulons établir est le suivant :

Proposition 1.3.4.1. *Soit $\mathbb{F}_q$ un corps de $q = p^k$ éléments et $\phi = \left(\frac{\bullet}{q}\right)_{(3)}$ le caractère multiplicatif d'ordre 3 introduit à la Section 1.3.1. Supposons que $p \equiv 1 \mod 3$. Alors,*

$$G(\phi)^3 = (-1)^{k-1}\left(\frac{ps \pm 3p|t|i\sqrt{3}}{2}\right)^k, \tag{1.3.5}$$

où s et $|t|$ sont des entiers relatifs entièrement déterminés par

$$4p = s^2 + 27t^2$$
$$s \equiv 1 \mod 3.$$

Dans ce qui suit, nous sommes dans $\mathbb{F}_p$. Supposons donc que $p \equiv 1 \mod 3$. Commençons tout d'abord avec un résultat qui met en relation $G(\varphi)^3$ avec la somme de Jacobi $J(\varphi)$.

Théorème 1.3.4.1. *Nous avons que*

$$G(\varphi)^3 = pJ(\varphi).$$

Démonstration. Par les Théorèmes 1.3.3.1 et 1.3.3.2,

$$pJ(\varphi) = p\frac{G(\varphi)^2}{G(\varphi^2)} = p\frac{G(\varphi)^3}{G(\varphi^2)G(\varphi)} = p\frac{G(\varphi)^3}{G(\bar{\varphi})G(\varphi)} = p\frac{G(\varphi)^3}{p\varphi(-1)} = G(\varphi)^3.$$

□

Poursuivons avec un théorème qui sera très utile pour la suite des choses.

Théorème 1.3.4.2. *La relation suivante est valide :*

$$J(\varphi) \equiv -1 \mod 3\Omega.$$

Démonstration. D'entrée de jeu, nous pouvons écrire que

$$G(\varphi) = \sum_{a \in \mathbb{F}_p} \varphi(a)\psi(a).$$

Ensuite, considérons

$$\sum_{a\in\mathbb{F}_p^*}\varphi(a)\psi(a)-\sum_{a\in\mathbb{F}_p^*}\psi(a)=-\sum_{a\in\mathbb{F}_p^*}(1-\varphi(a))\psi(a).$$

En séparant cette dernière sommation selon de valeur prise par $\varphi(a)$, nous obtenons, en posant $\omega_3=e^{\frac{2\pi i}{3}}$,

$$-\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3}(1-\varphi(a))\psi(a)-\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3^2}(1-\varphi(a))\psi(a), \tag{1.3.6}$$

puisque si a est un cube, alors $\varphi(a)=1$ et

$$\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3^3=1}(1-\varphi(a))\psi(a)=0.$$

Nous pouvons ainsi récrire (1.3.6) de la manière suivante :

$$\begin{aligned}(1.3.6)&=(1-\omega_3)\left(-\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3}\psi(a)\right)+(1-\omega_3^2)\left(-\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3^2}\psi(a)\right)\\&=(1-\omega_3)\left(-\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3}\psi(a)-(1+\omega_3)\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3^2}\psi(a)\right).\end{aligned}$$

Pour tout $a\in\mathbb{F}_q$, $\psi(a)\in\Omega$. De plus, $1+\omega_3\in\Omega$, et Ω forme un anneau. Par conséquent, toute somme, différence ou produit d'un entier algébrique reste un entier entier algébrique et

$$-\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3}\psi(a)-(1+\omega_3)\sum_{a\in\mathbb{F}_p:\varphi(a)=\omega_3^2}\psi(a)\in\Omega.$$

Nous concluons donc que

$$\sum_{a\in\mathbb{F}_p^*}\varphi(a)\psi(a)-\sum_{a\in\mathbb{F}_p^*}\psi(a)\equiv 0 \mod (1-\omega_3)\Omega$$

et que

$$G(\varphi)=\sum_{a\in\mathbb{F}_p}\varphi(a)\psi(a)=\sum_{a\in\mathbb{F}_p^*}\varphi(a)\psi(a)\equiv\sum_{a\in\mathbb{F}_p^*}\psi(a)\equiv -1 \mod (1-\omega_3)\Omega,$$

par le Théorème 1.3.1.1.

Comme $1-\omega_3 = i\sqrt{3}e^{\frac{4\pi i}{3}}$, il est clair que $G(\varphi) \equiv -1 \mod \sqrt{3}\Omega$. Donc,

$$(G(\varphi)+1)^3 = G(\varphi)^3 + 1 + 3G(\varphi)^2 + 3G(\varphi) = 3\sqrt{3}w,$$

pour un certain $w \in \Omega$.

Alors,

$$G(\varphi)^3 + 1 = 3(\sqrt{3}w - G(\varphi)^2 - G(\varphi)),$$

d'où

$$G(\varphi)^3 \equiv -1 \mod 3\Omega$$

et de même

$$pJ(\varphi) \equiv -1 \mod 3\Omega,$$

par le Théorème 1.3.4.1.

Puisque $p \equiv 1 \mod 3$, il est évident que

$$J(\varphi) \equiv -1 \mod 3\Omega.$$

□

Poursuivons avec un théorème qui permet tranquillement d'établir un lien avec l'équation (1.3.5).

Théorème 1.3.4.3. *Nous avons que*

$$K(\varphi) = c + id\sqrt{3},$$

où c et d sont des entiers de $\mathbb{Z}$ tels que $c^2 + 3d^2 = p$ et $c \equiv -1 \mod 3$.

Démonstration. Il est clair que

$$\begin{aligned}
K(\varphi) &= \varphi(4)J(\varphi) \\
&= \varphi(4)\sum_{a\in\mathbb{F}_p} \varphi(a)\varphi(1-a) \\
&= \varphi(4)\sum_{a\in\mathbb{F}_p} \varphi(a(1-a)) \\
&= \sum_{a=1-a} \varphi(4a(1-a)) + \sum_{a\neq 1-a} \varphi(4a(1-a)) \\
&= \varphi(2(1-2^{-1})) + \sum_{a\neq 1-a} \varphi(4a(1-a)) \\
&= \varphi(1) + \sum_{a\neq 1-a} \varphi(4a(1-a))
\end{aligned}$$

$$= 1 + \sum_{a \neq 1-a} \varphi(4a(1-a)),$$

où nous avons utilisé la multiplicativité de la fonction φ.

Par la suite, numérotons $\alpha_1, \alpha_2, ..., \alpha_{\frac{p-1}{2}}, \alpha_{\frac{p-1}{2}+1}, ..., \alpha_{p-1}$ les $p-1$ éléments de la dernière sommation de manière à ce que $\alpha_1 = 1 - \alpha_{\frac{p-1}{2}+1}, ..., \alpha_{\frac{p-1}{2}} = 1 - \alpha_{p-1}$. Nous pouvons donc écrire que

$$K(\varphi) = 1 + 2\sum_{i=1}^{\frac{p-1}{2}} \varphi(4\alpha_i(1-\alpha_i)).$$

Comme $\varphi(a)$ prend la valeur 1 ou $\frac{-1 \pm i\sqrt{3}}{2}$, il s'ensuit que $K(\varphi) = c + id\sqrt{3}$, où c et d sont des entiers. En vertu du Théorème 1.3.3.2, $|K(\varphi)|^2 = p = c^2 + 3d^2$. Enfin, il faut voir que

$$\begin{aligned} K(\varphi)^3 &= (c + di\sqrt{3})^3 \\ &\equiv c^3 \mod 3\Omega \\ &\equiv c \mod 3\Omega, \end{aligned}$$

puisque $c^3 - c = c(c^2 - 1) = c(p - 1 - 3d^2)$ et que $3|(p - 1 - 3d^2)$.

De plus,

$$K(\varphi)^3 = \varphi(4)^3 J(\varphi)^3 = J(\varphi)^3.$$

Par le Théorème 1.3.4.2, nous savons que $J(\varphi) \equiv -1 \mod 3\Omega$. Par conséquent, $J(\varphi)^3 \equiv -1 \mod 3\Omega$. Comme nous avons aussi que $J(\varphi)^3 \equiv c \mod 3\Omega$, nous concluons que

$$c \equiv -1 \mod 3.$$

□

Prouvons un dernier théorème avec lequel nous nous rapprocherons encore un peu plus de l'équation (1.3.5).

Théorème 1.3.4.4. *Nous avons que*

$$2J(\varphi) = s + ti\sqrt{3},$$

où s et $|t|$ sont des entiers entièrement déterminés par $s^2 + 3t^2 = 4p$, $s \equiv 1 \mod 3$ et $t \equiv 0 \mod 3$.

Démonstration. Par le dernier théorème, nous avons que

$$2J(\varphi) = 2\varphi(4)^2 K(\varphi) = 2\varphi(4)^2(c + id\sqrt{3})$$
$$= \begin{cases} 2c + 2id\sqrt{3} & \varphi(4) = 1, \\ -c - 3d + (c-d)i\sqrt{3} & \varphi(4) = e^{\frac{4\pi i}{3}}, \\ -c + 3d - (c+d)i\sqrt{3} & \varphi(4) = e^{\frac{2\pi i}{3}}. \end{cases}$$

Nous pouvons donc conclure que

$$s = \begin{cases} 2c & \varphi(4) = 1, \\ -c - 3d & \varphi(4) = e^{\frac{4\pi i}{3}}, \\ -c + 3d & \varphi(4) = e^{\frac{2\pi i}{3}}, \end{cases}$$

$$t = \begin{cases} 2d & \varphi(4) = 1, \\ c - d & \varphi(4) = e^{\frac{4\pi i}{3}}, \\ -c - d & \varphi(4) = e^{\frac{2\pi i}{3}}. \end{cases}$$

Nous déduisons que $s^2 + 3t^2 = 4p$. Par le Théorème 1.3.4.2,

$$2J(\varphi) - 1 = (s-1) + it\sqrt{3} \equiv 0 \mod 3\Omega,$$

d'où $s \equiv 1 \mod 3$ et $t \equiv 0 \mod 3$.

Nous terminons en montrant que s et $|t|$ sont uniques. Comme $\mathbb{Z}\left[\frac{1+\sqrt{3}i}{2}\right]$ est un domaine de factorisation unique et que $p \equiv 1 \mod 3$, nous pouvons écrire que $p = (\frac{e+\sqrt{3}if}{2})(\frac{e-\sqrt{3}if}{2})$, où $\frac{e+\sqrt{3}if}{2}$ est unique à conjugués près. Donc, nous avons une des six situations suivantes :

$$\frac{s + ti\sqrt{3}}{2} = \frac{\pm(e + \sqrt{3}if)}{2}, \tag{1.3.7}$$
$$\frac{s + ti\sqrt{3}}{2} = \frac{\pm\omega_3(e + \sqrt{3}if)}{2} = \frac{\pm(-e - 3f) + \sqrt{3}i(e - f)}{4}, \tag{1.3.8}$$
$$\frac{s + ti\sqrt{3}}{2} = \frac{\pm\omega_3^2(e + \sqrt{3}if)}{2} = \frac{\pm(-e + 3f) - \sqrt{3}i(e + f)}{4}, \tag{1.3.9}$$

avec $\omega_3 = e^{\frac{2\pi i}{3}}$.

Nous avons que $3 \nmid e$ puisque $3 \nmid p = \frac{e^2+3f^2}{4}$. Si $3|f$, alors nous choisissons l'équation (1.3.7), et nous prenons le bon signe pour e afin d'avoir $s = \pm e \equiv 1$

mod 3. Si $3 \nmid f$, alors soit nous avons $e \equiv f \mod 3$, auquel cas nous choisissons l'équation (1.3.8), ou soit nous avons $e \equiv -f \mod 3$, auquel cas nous choisissons l'équation (1.3.9). Une fois la bonne équation choisie, nous choisissions le bon signe pour e afin d'avoir $s \equiv \mp e \equiv 1 \mod 3$. Nous concluons que s et $|t|$ sont uniques.

□

Remarque 1.3.4.1. *Comme $3|t$, nous pouvons écrire le dernier théorème de la manière suivante :*

$$2J(\varphi) = s + 3ti\sqrt{3},$$

où s et $|t|$ sont des entiers déterminés par

$$\begin{aligned} 4p &= s^2 + 27t^2 \\ s &\equiv 1 \mod 3. \end{aligned}$$

Nous voyons, à partir de cette remarque et du Théorème 1.3.4.1, que

$$G(\varphi)^3 = \frac{ps \pm 3p|t|i\sqrt{3}}{2},$$

où s et $|t|$ sont entièrement déterminés par

$$\begin{aligned} 4p &= s^2 + 27t^2 \\ s &\equiv 1 \mod 3. \end{aligned}$$

En utilisant le Théorème 1.3.2.5, et en notant $G(\varphi^{(k)})$ la somme de Gauss dont les caractères prennent leurs valeurs dans $\mathbb{F}_q$, avec $q = p^k$, nous avons que

$$G(\varphi^{(k)}) = (-1)^{k-1} G(\varphi)^k,$$

d'où

$$\begin{aligned} G(\varphi^{(k)})^3 &= \left((-1)^{k-1}\right)^3 G(\varphi)^{3k} \\ &= (-1)^{k-1} \left(\frac{ps \pm 3p|t|i\sqrt{3}}{2}\right)^k, \end{aligned}$$

avec les mêmes conditions sur p, t et s que dans la Remarque 1.3.4.1.

Remarque 1.3.4.2. *Supposons que, dans $\mathbb{F}_p$, nous ayons pris le caractère d'ordre 3, $\varphi = \left(\frac{\bullet}{p}\right)_3$, défini à la Section* 1.3.1. *Par le théorème de Davenport-Hasse, ce caractère s'est étendu vers $\mathbb{F}_q$ et vaut, pour γ une racine primitive et $a \in \mathbb{F}_q$ tel*

que $a = \gamma^r$ *:*

$$\varphi^{(k)}(a) = \left(\frac{N_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p}\right)_{(3)} = \left(\frac{a^{\frac{q-1}{p-1}}}{p}\right)_{(3)} = \left(\frac{\gamma^{r\left(\frac{q-1}{p-1}\right)}}{p}\right)_{(3)} = \left(\frac{\left(\gamma^{\left(\frac{q-1}{p-1}\right)}\right)^r}{p}\right)_{(3)}.$$

Il est facile de voir que $\gamma^{\frac{q-1}{p-1}}$ *est une racine primitive de* $\mathbb{F}_p$*. Nous voyons donc que ce caractère est équivalent à*

$$\left(\frac{a}{q}\right)_{(3)},$$

introduit à la section 1.3.1*. C'est ce caractère que nous utiliserons dans notre preuve au Chapitre* 3*.*

De ce fait, la Proposition 1.3.4.1 est démontrée, et nous savons tout ce que nous avons besoin de savoir sur les sommes de Gauss cubiques.

1.3.5. Sommes de Gauss quartiques

Dans cette section, $p \equiv 1 \mod 4$ et φ est un caractère multiplicatif modulo p d'ordre 4 sur $\mathbb{F}_p$, De plus, ψ représente toujours notre caractère additif. Reprenons aussi Ω l'ensemble des entiers algébriques. Ces résultats sont encore tirés de l'article de Berndt et de Evant (voir [**1**]). Nous allons commencer par travailler dans $\mathbb{F}_p$, avant d'étendre sur $\mathbb{F}_q$.

Cette section est très similaire à la précédente, dans le sens où nous voulons montrer un résultat qui nous aidera grandement à trouver une expression pour le nombre de polynômes irréductibles où sont prescrits le premier coefficient et la quarticité du dernier. Donc, voici ce que nous voulons montrer :

Proposition 1.3.5.1. *Soit* $\mathbb{F}_q$ *un corps fini à* $q = p^k$ *éléments tel que* $p \equiv 1 \mod 4$*. Soit* $\phi = \left(\frac{\bullet}{q}\right)_{(4)}$ *le caractère d'ordre* 4 *défini à la Section* 1.3.1*. Alors,*

$$G(\phi)^2 = \sqrt{q}(c \pm |d|i)^k, \tag{1.3.10}$$

où c *et* $|d|$ *sont des entiers entièrement déterminés par les relations*

$$p = c^2 + d^2$$
$$c \equiv -1 \mod 4.$$

Dans ce qui suit, nous sommes dans $\mathbb{F}_p$, et ce jusqu'à ce que nous utilisions le Théorème 1.3.2.5 (Davenport-Hasse). Commençons par mettre en relation $G(\varphi)^2$ avec la somme de Jacobi $J(\varphi)$.

Théorème 1.3.5.1. *Soit $\mathbb{F}_p$ le corps de p éléments. Alors, la relation suivante est valide :*

$$G(\varphi)^2 = \sqrt{p}J(\varphi).$$

Démonstration. Par le Théorème 1.3.3.2,

$$J(\varphi) = \frac{G(\varphi)^2}{G(\varphi^2)}.$$

Travaillons $G(\varphi^2)$. Soit γ une racine primitive de $\mathbb{F}_p$ telle que $\varphi(\gamma) = \omega_4 = e^{\frac{\pi i}{2}} = i$. Donc, pour $a \in \mathbb{F}_p$ tel que $a = \gamma^r$, nous avons que

$$\varphi(a)^2 = \varphi(a^2) = \omega_4^{2r} = (-1)^r,$$

ce qui implique que $\varphi(a)^2 = \left(\frac{a}{p}\right)$ et $G(\varphi^2) = G_\psi(1)$.

Enfin, par les Théorèmes 1.3.2.6 et 1.3.3.2, il est clair que

$$G(\varphi)^2 = G_\psi(1)J(\varphi) = \sqrt{p}J(\varphi).$$

□

Il ne nous manque qu'une expression pour $J(\varphi)$, qui sera fournie dans les deux prochains énoncés.

Théorème 1.3.5.2. *Nous avons que*

$$K(\varphi) = a + ib,$$

où a et $|b|$ sont des entiers entièrement déterminés par $a^2 + b^2 = p$ et $a \equiv -\left(\frac{2}{p}\right)$ mod 4.

Démonstration. $\varphi(\alpha) \in \mathbb{Z}[i]$ pour tout $\alpha \in \mathbb{F}_p$. Donc, il est facile de voir que $K(\varphi) = a + bi$, où a et b sont des entiers. De plus, par les Théorèmes 1.3.3.2 et 1.3.3.4, $|K(\varphi)|^2 = p = a^2 + b^2$.

En se servant du Théorème 1.3.3.4,

$$a + bi = K(\varphi)$$

$$
\begin{aligned}
&= J(\varphi, \varphi^2) \\
&= \sum_{\alpha \in \mathbb{F}_p} \varphi(1-\alpha) \left(\frac{\alpha}{p}\right) \\
&= \sum_{\alpha \notin \{0,1\}} \varphi(1-\alpha) \left(\frac{\alpha}{p}\right) \\
&= \sum_{\alpha \notin \{0,1\}} \varphi(1-\alpha) \left(\frac{\alpha}{p}\right) - \sum_{\alpha \notin \{0,1\}} \varphi(1-\alpha) - 1 \\
&= \sum_{\alpha \notin \{0,1\}} \varphi(1-\alpha) \left(\left(\frac{\alpha}{p}\right) - 1\right) - 1,
\end{aligned}
$$

où nous avons utilisé le fait que $\sum_{\alpha \notin \{0,1\}} \varphi(1-\alpha) = -1$.

Remarquons que, pour $\alpha \neq 0$ et $\alpha \neq 1$,

$$
\begin{aligned}
\left(\frac{\alpha}{q}\right) - 1 &\equiv 0 \mod 2 \\
\varphi(1-\alpha) &\equiv 1 \mod (1-i)\Omega,
\end{aligned}
$$

parce que $1-i | 1 \pm i$ et $1-i | 2$.

Donc, nous pouvons conclure que

$$
(\varphi(1-\alpha) - 1)\left(\left(\frac{\alpha}{p}\right) - 1\right) \equiv 0 \mod 2(1-i)\Omega.
$$

En sommant sur tous les α différents de 0 et 1, nous arrivons à

$$
\sum_{\alpha \notin \{0,1\}} \varphi(1-\alpha)\left(\left(\frac{\alpha}{p}\right) - 1\right) - \sum_{\alpha \notin \{0,1\}} \left(\frac{\alpha}{p}\right) + p - 2 \equiv 0 \mod 2(1-i)\Omega.
$$

Ceci implique que

$$
a + bi + p \equiv 0 \mod 2(1-i)\Omega.
$$

Cette dernière équation signifie qu'il existe $w \in \Omega$ tel que

$$
a + bi + p = 2(1-i)w.
$$

En prenant la norme de chaque côté, et en élevant au carré, nous obtenons que $8 = |2(1-i)|^2$ divise

$$|a + bi + p|^2 = a^2 + b^2 + p^2 + 2ap = p(p + 1 + 2a).$$

Une simple vérification permet de constater que

$$a \equiv -\frac{p+1}{2} \equiv -\left(\frac{2}{p}\right) \mod 4.$$

Pour montrer que a et $|b|$ sont uniques, nous allons utiliser la factorisation sur $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est un domaine de factorisation unique et que $p \equiv 1 \mod 4$, nous pouvons écrire $p = (c + id)(c - id)$, où $c + id$ est unique à conjugués près. Donc, nous avons que

$$\begin{aligned} a + ib &= c + id, \\ a + ib &= -(c + id), \\ a + ib &= i(c + id), \\ a + ib &= -i(c + id). \end{aligned}$$

Donc, soit $|a| = |c|$ et $|b| = |d|$, soit $|a| = |d|$ et $|b| = |c|$. De plus, comme p est impair, alors exactement un de $\{a, b\}$ est impair, et l'autre est pair. Comme $a \equiv -\left(\frac{2}{p}\right) \mod 4$, nous pouvons conclure que a est impair et pouvons déterminer son signe. Enfin, il est clair que a est unique et que b est unique à signe près dans la représentation

$$\begin{aligned} p &= a^2 + b^2 \\ a &\equiv -\left(\frac{2}{p}\right) \mod 4. \end{aligned}$$

□

Voici enfin un simple corollaire qui permet de passer de $K(\varphi)$ à $J(\varphi)$, et l'équation (1.3.10) avec ses conditions sera presque démontrée.

Corollaire 1.3.5.1. *Nous avons que*

$$J(\varphi) = c + id,$$

où c et $|d|$ sont des entiers entièrement déterminés par $c^2+d^2=p$ et $c=\left(\frac{2}{p}\right)a \equiv -1 \mod 4$.

Démonstration. Par la relation entre $J(\varphi)$ et $K(\varphi)$, nous pouvons écrire que

$$J(\varphi)=\varphi(4)^{-1}K(\varphi)=\left(\frac{2}{p}\right)K(\varphi),$$

où nous avons utilisé le fait que $\varphi(4)^{-1}=\varphi(2^2)^{-1}=\varphi(2^{-1})^2=\left(\frac{2^{-1}}{p}\right)=\left(\frac{2}{p}\right)$.

Ensuite, par le théorème précédent, nous pouvons conclure.

□

En mettant le Théorème 1.3.5.1 et le Corollaire 1.3.5.1 ensemble, nous voyons que

$$G(\varphi)^2=\sqrt{p}J(\varphi)=\sqrt{p}(c\pm|d|i),$$

où c et $|d|$ sont déterminés par

$$\begin{aligned} p &= c^2+d^2 \\ c &\equiv -1 \mod 4. \end{aligned}$$

Maintenant, en utilisant le Théorème 1.3.2.5 (Davenport-Hasse), et en notant $G(\varphi^{(k)})$ la somme de Gauss avec le caractère étendu sur $\mathbb{F}_q$, nous avons que

$$G(\varphi^{(k)})=(-1)^{k-1}G(\varphi)^k,$$

d'où

$$\begin{aligned} G(\varphi^{(k)})^2 &= ((-1)^{k-1})^2G(\varphi)^{2k} \\ &= \sqrt{q}(c\pm|d|i)^k. \end{aligned}$$

Maintenant, par un raisonnement semblable à celui de la section précédente, si $\varphi=\left(\frac{\bullet}{p}\right)_{(4)}$, alors le caractère étendu $\varphi^{(k)}$ est le caractère $\left(\frac{a}{q}\right)_{(4)}$, et la Proposition 1.3.5.1 est démontrée.

C'est ce qui met fin à la partie théorique de ce mémoire. Nous avons maintenant tous les outils pour attaquer notre problématique.

Chapitre 2

RÉSULTATS EN FIXANT DES CONTRAINTES SUR TROIS COEFFICIENTS

2.1. Résultat asymptotique pour $(t_1, t_2, sgn(t_n))$ fixés

Soit M un polynôme dont les coefficients appartiennent à un corps fini quelconque $\mathbb{F}_q$ de caractéristique p :

$$M = x^n + a_1 x^{n-1} + a_2 x^{n-2} + t_3 x^{n-3} + \cdots + a_n. \tag{2.1.1}$$

Dans notre cas, (a_1, a_2) et $sgn(a_n)$ sont fixés, et les t_i, pour $3 \leq i \leq n-1$, sont quelconques. Nous dirons d'un polynôme dont les coefficients a ces contraintes qu'il est de la forme $(a_1, a_2, sgn(a_n))$. Soit $H_n(a_1, a_2, sgn(a_n))$ le nombre de polynômes irréductibles de cette forme. Nous allons montrer, en utilisant la méthode de Carlitz dans [**4**], le théorème suivant.

Théorème 2.1.1. *Soit $p \neq 2$ la caractéristique d'un corps fini de q éléments. Alors, nous avons que*

$$H_n(a_1, a_2, sgn(a_n)) = \frac{q^{n-2}}{2n} + O\left(\frac{(18,0625q)^{\frac{n}{2}}}{n}\right).$$

La première étape est de définir les caractères que nous utiliserons. Le caractère associé aux deux premiers coefficients, a_1 et a_2, sera un caractère multiplicatif sur les polynômes, construit à partir de la fonction additive ψ introduite à la Définition 1.3.1.1 :

$$\psi(a) = e^{\frac{2\pi i Tr(a)}{p}}.$$

À partir de cette définition, nous sommes en mesure de définir un premier caractère, et ce pour $\deg M \geqslant 2$:

$$\chi_{\lambda_1,\lambda_2}(M) = \chi_{\lambda_1,\lambda_2}(a_1, a_2) = \psi\left(\lambda_1 a_1 + \lambda_2\left(a_2 - \frac{a_1^2}{2}\right)\right),$$

avec $\lambda_1, \lambda_2 \in \mathbb{F}_q$.

Si $M = 1$, nous définissons

$$\chi_{\lambda_1,\lambda_2}(1) = \chi_{\lambda_1,\lambda_2}(0,0) = \psi(0) = 1.$$

Ensuite, si $M = x + a$, avec $a \in \mathbb{F}_q$, nous définissons

$$\chi_{\lambda_1,\lambda_2}(x+a) = \chi_{\lambda_1,\lambda_2}(a,0) = \psi\left(\lambda_1 a - \frac{\lambda_2}{2}a^2\right).$$

Remarque 2.1.1. *Ce caractère n'est pas valide pour les corps de caractéristique 2.*

Par le Théorème 1.3.1.1, il est clair que :

$$\sum_{\lambda_1,\lambda_2 \in \mathbb{F}_q} \chi_{\lambda_1\lambda_2}(a_1, a_2) = \begin{cases} 0 & (a_1, a_2) \neq (0,0), \\ q^2 & (a_1, a_2) = (0,0). \end{cases} \tag{2.1.2}$$

Le caractère que nous associerons au signe du dernier coefficient est construit à partir d'un caractère multiplicatif. Nous nous servirons donc de la fonction de Legendre :

$$\left(\frac{a}{q}\right) = \begin{cases} -1 & a \text{ n'est pas un carré dans } \mathbb{F}_q^*, \\ 0 & a = 0, \\ 1 & a \text{ est un carré dans } \mathbb{F}_q^*. \end{cases}$$

Posons alors notre deuxième caractère :

$$\Gamma(M) = \Gamma_c(M) = \begin{cases} \left(\frac{a_n^c}{q}\right) & a_n \neq 0, \\ 0 & a_n = 0, \end{cases}$$

pour $c \in \{0, 1\}$.

Nous avons maintenant nos deux caractères, et il est facile de vérifier qu'ils sont multiplicatifs. En effet, soient A et B deux polynômes de $\mathbb{F}_q[x]$:

$$A(x) = x^n + u_1 x^{n-1} + u_2 x^{n-2} + \cdots + u_n$$
$$B(x) = x^m + v_1 x^{m-1} + v_2 x^{m-2} + \cdots + v_m.$$

Alors,

$$A(x)B(x) = x^{n+m} + (u_1 + v_1)x^{m+n-1} + (u_2 + u_1 v_1 + v_2)x^{m+n-2} + \cdots + u_n v_m.$$

Il est évident que $\Gamma(AB) = \Gamma(A)\Gamma(B)$. Pour le caractère χ, nous avons que

$$\begin{aligned}
\chi(AB) &= \psi\left(\lambda_1(u_1 + v_1) + \lambda_2\left(u_2 + u_1 v_1 + v_2 - \frac{(u_1 + v_1)^2}{2}\right)\right) \\
&= \psi\left(\lambda_1 u_1 + \lambda_1 v_1 + \lambda_2\left(u_2 + v_2 - \frac{u_1^2}{2} - \frac{v_1^2}{2}\right)\right) \\
&= \psi\left(\lambda_1 u_1 + \lambda_2\left(u_2 - \frac{u_1^2}{2}\right)\right)\psi\left(\lambda_1 v_1 + \lambda_2\left(v_2 - \frac{v_1^2}{2}\right)\right) \\
&= \chi(A)\chi(B).
\end{aligned}$$

Alors, nous concluons que le caractère χ est lui aussi multiplicatif.

Pour le reste de la section, M parcourt l'ensemble des polynômes unitaires de $\mathbb{F}_q[x]$. Calculons maintenant quelques quantités concernant ces deux caractères.

Supposons que $\chi = \chi_{0,0}$:

$$\sum_{\deg M = m} \chi(M) = \sum_{\deg M = m} 1 = q^m. \tag{2.1.3}$$

Supposons que $\chi \neq \chi_{0,0}$:

$$\sum_{\deg M = 0} \chi(M) = \chi(1) = 1. \tag{2.1.4}$$

$$\sum_{\deg M=1} \chi(M) = \sum_{a\in\mathbb{F}_q} \psi\left(\lambda_1 a - \frac{\lambda_2}{2}a^2\right) = \begin{cases} \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{-\frac{\lambda_2}{2}}{q}\right) G_\psi(1) & \lambda_2 \neq 0, \\ 0 & \lambda_2 = 0, \end{cases} \tag{2.1.5}$$

où nous avons utilisé les Théorèmes 1.3.1.1 et 1.3.2.2.

Finalement, si $m \geqslant 2$, alors

$$\sum_{\deg M=m} \chi(M) = q^{m-2} \sum_{b_1,b_2\in\mathbb{F}_q} \psi\left(\lambda_1 b_1 + \lambda_2\left(b_2 - \frac{b_1^2}{2}\right)\right) = 0, \tag{2.1.6}$$

où nous avons utilisé le Théorème 1.3.1.1.

Faisons le même type de calculs pour le deuxième caractère, en rappelant que $a_n \neq 0$.

Supposons que $m = 0$:

$$\sum_{\deg M=0} \Gamma(M) = \Gamma(1) = 1 \tag{2.1.7}$$

Supposons que $c = 0$ et $m \geq 1$:

$$\sum_{\deg M=m} \Gamma(M) = q^{m-1} \sum_{a\in\mathbb{F}_q^*} \left(\frac{a^0}{q}\right) = q^{m-1}(q-1). \tag{2.1.8}$$

Supposons que $c = 1$ et $m \geq 1$:

$$\sum_{\deg M=m} \Gamma(M) = q^{m-1} \sum_{a\in\mathbb{F}_q^*} \left(\frac{a}{q}\right) = 0, \tag{2.1.9}$$

par le Lemme 1.3.1.1.

Avant de définir notre fonction L, introduisons le concept de la norme d'un polynôme. Soit $U(x)$ un polynôme quelconque de $\mathbb{F}_q[x]$. Alors, la norme de U est définie par

$$|U| = q^{\deg U}.$$

Définissons maintenant, selon les caractères introduits précédemment, la fonction L suivante.

Définition 2.1.1. *Nous avons, pour $Re(s) > 1$, que*

$$L(s, \chi, \Gamma) = \sum_{M} \chi(M)\Gamma(M)|M|^{-s} = \prod_{P}(1 - \chi(P)\Gamma(P)|P|^{-s})^{-1},$$

où P parcourt tous les polynômes irréductibles unitaires de $\mathbb{F}_q[x]$.

Posons aussi

$$\tau_m = \tau_m(\chi, \Gamma) = \sum_{\deg M = m} \chi(M)\Gamma(M).$$

Remarquons que nous aurions pu simplement utiliser les notations $L(s, \chi\Gamma)$ et $\tau_m(\chi\Gamma)$ au lieu de $L(s, \chi, \Gamma)$ et $\tau_m(\chi, \Gamma)$. Conservons la virgule pour éviter la confusion lorsqu'il y aura des éléments en indice de ces caractères.

Remarque 2.1.2. *Il est donc clair que :*

$$L(s, \chi, \Gamma) = \sum_{m=0}^{\infty} \tau_m(\chi, \Gamma)q^{-ms}.$$

Pour la suite des choses, il est essentiel de connaître $L(s, \chi, \Gamma)$ selon les différentes valeurs prises par λ_1, λ_2 et c.

Supposons que $(\lambda_1, \lambda_2) = (0, 0)$ et que $c = 0$. Alors,

$$\begin{aligned} L(s, \chi_{0,0}, \Gamma_0) &= \sum_{\substack{M \\ x \nmid M}} |M|^{-s} = 1 + \sum_{m=1}^{\infty} q^{-ms} \sum_{\substack{\deg M = m \\ x \nmid M}} 1 \\ &= 1 + \sum_{m=1}^{\infty} q^{-ms}q^{m-1}(q-1) = 1 + \frac{q-1}{q}\sum_{m=1}^{\infty} q^{m(1-s)} \\ &= 1 + \frac{q-1}{q}\left(\sum_{m=0}^{\infty} q^{m(1-s)} - 1\right) = 1 + \frac{q-1}{q}\left(\frac{1}{1-q^{1-s}} - 1\right) \\ &= 1 + \frac{q-1}{q}\left(\frac{1-(1-q^{1-s})}{1-q^{1-s}}\right) = \frac{1-q^{-s}}{1-q^{1-s}}, \end{aligned}$$

par les équations (2.1.7) et (2.1.8).

Supposons que $\lambda_2 \neq 0$ et que $c = 0$. Alors,

$$L(s, \chi_{\lambda_1,\lambda_2}, \Gamma_0) = \sum_{\substack{M \\ x \nmid M}} \chi(M)|M|^{-s} = \sum_{m=0}^{\infty} q^{-ms} \sum_{\substack{\deg M = m \\ x \nmid M}} \chi(M)$$
$$= 1 + q^{-s} \sum_{a \in \mathbb{F}_q^*} \psi\left(\lambda_1 a - \frac{\lambda_2}{2} a^2\right) = 1 + q^{-s}\left(\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{-\frac{\lambda_2}{2}}{q}\right) G_\psi(1) - 1\right),$$

par les équations (2.1.4), (2.1.5) et (2.1.6).

Supposons que $\lambda_1 \neq 0$, $\lambda_2 = 0$ et $c = 0$. Alors,

$$L(s, \chi_{\lambda_1,0}, \Gamma_0) = 1 + q^{-s} \sum_{a \in \mathbb{F}_q^*} \psi(\lambda_1 a) = 1 - q^{-s},$$

par l'équation (2.1.4) et par le Théorème 1.3.1.1.

Alors, si nous résumons, pour $c = 0$:

$$L(s, \chi, \Gamma_0) = \begin{cases} \frac{1-q^{-s}}{1-q^{1-s}} & \lambda_1 = 0, \lambda_2 = 0, \\ 1 + q^{-s}\left(\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{-\frac{\lambda_2}{2}}{q}\right) G_\psi(1) - 1\right) & \lambda_2 \neq 0, \\ 1 - q^{-s} & \lambda_1 \neq 0, \lambda_2 = 0. \end{cases} \tag{2.1.10}$$

Il reste maintenant à nous attaquer aux cas possibles lorsque $c = 1$.

Supposons que $(\lambda_1, \lambda_2) = (0, 0)$ et que $c = 1$. Alors,

$$L(s, \chi_{0,0}, \Gamma_1) = \sum_{M} \Gamma_1(M)|M|^{-s} = \sum_{m=0}^{\infty} q^{-ms} \sum_{\deg M = m} \Gamma_1(M)$$
$$= 1 + \sum_{m=1}^{\infty} q^{-ms} \sum_{\deg M = m} \Gamma_1(M) = 1,$$

par les équations (2.1.7) et (2.1.9).

Par la Remarque 2.1.3, nous avons que la fonction L peut être écrite de cette manière :

$$L(s, \chi, \Gamma) = \sum_{m=0}^{\infty} \tau_m(\chi, \Gamma) q^{-ms}.$$

Nous allons calculer les cas $(\lambda_1, \lambda_2) \neq (0,0)$ et $c = 1$ avec cette définition. Commençons d'abord par calculer τ_m pour $m \geq 0$.

Pour $m = 0$, nous avons que

$$\tau_0 = 1.$$

Pour $m = 1$, nous avons que

$$\tau_1 = \sum_{\deg M=1} \chi(M)\Gamma(M) = \sum_{a \in \mathbb{F}_q^*} \left(\frac{a}{q}\right) \psi\left(\lambda_1 a - \frac{\lambda_2}{2} a^2\right). \tag{2.1.11}$$

Pour $m = 2$, nous avons que

$$\begin{aligned}\tau_2 &= \sum_{\deg M=2} \chi(M)\Gamma(M) = \sum_{b_1 \in \mathbb{F}_q, b_2 \in \mathbb{F}_q^*} \left(\frac{b_2}{q}\right) \psi\left(\lambda_1 b_1 + \lambda_2\left(b_2 - \frac{b_1^2}{2}\right)\right) \\ &= \sum_{b_1 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 - \frac{\lambda_2}{2} b_1^2\right) \sum_{b_2 \in \mathbb{F}_q^*} \left(\frac{b_2}{q}\right) \psi(\lambda_2 b_2),\end{aligned}$$

d'où

$$\tau_2 = \sum_{b_1 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 - \frac{\lambda_2}{2} b_1^2\right) \sum_{b_2 \in \mathbb{F}_q^*} \left(\frac{b_2}{q}\right) \psi(\lambda_2 b_2). \tag{2.1.12}$$

Pour $m \geq 3$, nous avons que

$$\tau_m = q^{m-2} \sum_{b_n \in \mathbb{F}_q^*} \left(\frac{b_n}{q}\right) \sum_{b_1, b_2 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 + \lambda_2\left(b_2 - \frac{b_1^2}{2}\right)\right) = 0,$$

par le Lemme 1.3.1.1.

Nous donnerons des valeurs plus précises de τ_1 et de τ_2 selon les valeurs de λ_1 et de λ_2. Pour l'instant, nous concluons que

$$L(s, \chi, \Gamma) = 1 + \tau_1 q^{-s} + \tau_2 q^{-2s}. \tag{2.1.13}$$

Supposons que $\lambda_1 \neq 0$ et que $\lambda_2 \neq 0$. Alors, nous avons, par l'équation (2.1.11) et par le Lemme 1.3.2.1, que

$$\begin{aligned}\tau_1 &= \sum_{a\in\mathbb{F}_q^*} \left(\frac{a}{q}\right) \psi\left(\lambda_1 a - \frac{\lambda_2}{2}a^2\right) \\ &= \frac{c}{\sqrt{q}} \sum_{b\in\mathbb{F}_q} \sum_{a\in\mathbb{F}_q^*} \psi\left(a\left(b^2+\lambda_1\right) - \frac{\lambda_2}{2}a^2\right) \\ &= \frac{c}{\sqrt{q}} \sum_{b\in\mathbb{F}_q} \left(\psi\left(\frac{(b^2+\lambda_1)^2}{2\lambda_2}\right)\left(\frac{-\frac{\lambda_2}{2}}{q}\right) G_\psi(1) - 1\right),\end{aligned}$$

où nous avons utilisé le Théorème 1.3.2.2 ainsi que les mêmes notations que le Lemme 1.3.2.1.

En manipulant cette dernière équation, nous obtenons

$$\begin{aligned}\tau_1 &= \frac{c}{\sqrt{q}} G_\psi(1)\left(\frac{-\frac{\lambda_2}{2}}{q}\right) \sum_{b\in\mathbb{F}_q} \psi\left(\frac{(b^2+\lambda_1)^2}{2\lambda_2}\right) - c\sqrt{q} \\ &= \left(\frac{-\frac{\lambda_2}{2}}{q}\right) \sum_{b\in\mathbb{F}_q} \psi\left(\frac{(b^2+\lambda_1)^2}{2\lambda_2}\right) - c\sqrt{q} \\ &= 3\sigma_1\sqrt{q} - c\sqrt{q} \\ &= \sigma\sqrt{q},\end{aligned}$$

où $|\sigma_1| \leq 1$, $|\sigma| \leq 4$ et où nous avons utilisé le fait que $\frac{c}{\sqrt{q}} G_\psi(1) = 1$ (voir la preuve du Lemme 1.3.2.1). De plus, nous avons utilisé le Théorème 1.3.2.3 pour donner l'approximation suivante :

$$\left|\sum_{b\in\mathbb{F}_q} \psi\left(\frac{(b^2+\lambda_1)^2}{2\lambda_2}\right)\right| \leq 3\sqrt{q},$$

et nous nous sommes servis du fait que $|3\sigma_1 - c| \leq |3\sigma_1| + |c| \leq 4$ pour montrer la dernière égalité.

Maintenant, par les équations (1.3.2), (2.1.5) et (2.1.12),

$$\begin{aligned}\tau_2 &= \sum_{b_1\in\mathbb{F}_q} \psi\left(\lambda_1 b_1 - \frac{\lambda_2}{2}b_1^2\right) \sum_{b_2\in\mathbb{F}_q^*} \left(\frac{b_2}{q}\right) \psi(\lambda_2 b_2) \\ &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{-\frac{\lambda_2}{2}}{q}\right)\left(\frac{\lambda_2}{q}\right) G_\psi(1)^2 \\ &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{2}{q}\right) q,\end{aligned}$$

où nous avons utilisé le Théorème 1.3.2.1.

Donc, pour $\lambda_1 \neq 0$ et $\lambda_2 \neq 0$,

$$L(s,\chi,\Gamma) = 1 + \sigma q^{\frac{1}{2}-s} + \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{2}{q}\right)q^{1-2s},$$

avec $|\sigma| \leq 4$.

Supposons que $\lambda_1 \neq 0$ et que $\lambda_2 = 0$. Alors, par (2.1.11),

$$\tau_1 = \sum_{a\in\mathbb{F}_q^*}\left(\frac{a}{q}\right)\psi(\lambda_1 a) = \left(\frac{\lambda_1}{q}\right)G_\psi(1),$$

par (1.3.2).

De plus,

$$\tau_2 = \sum_{b_1\in\mathbb{F}_q}\psi(\lambda_1 b_1)\sum_{b_2\in\mathbb{F}_q^*}\left(\frac{b_2}{q}\right) = 0,$$

par le Lemme 1.3.1.1.

Donc, pour $\lambda_1 \neq 0$ et $\lambda_2 = 0$,

$$L(s,\chi,\Gamma) = 1 + \left(\frac{\lambda_1}{q}\right)G_\psi(1)q^{-s}.$$

Supposons enfin que $\lambda_1 = 0$ et que $\lambda_2 \neq 0$.

Si $q \equiv 3 \mod 4$, alors par l'équation (2.1.11), nous avons que

$$\tau_1 = \sum_{a\in\mathbb{F}_q^*}\left(\frac{a}{q}\right)\psi\left(-\frac{\lambda_2}{2}a^2\right).$$

Soit $\alpha \in \mathbb{F}_q^*$ un carré. Il existe donc $\alpha_1 \in \mathbb{F}_q^*$ tel que $\alpha_1^2 = \alpha$. L'autre élément dont le carré vaut α est $-\alpha_1$. Donc, nous avons que

$$\left(\frac{\alpha_1}{q}\right)\psi\left(-\frac{\lambda_2}{2}\alpha^2\right) + \left(\frac{-\alpha_1}{q}\right)\psi\left(-\frac{\lambda_2}{2}\alpha^2\right) = 0.$$

En répétant pour chaque carré de $\mathbb{F}_q^*$, nous arrivons à

$$\tau_1 = 0.$$

Si $q \equiv 1 \mod 4$, alors un raisonnement semblable à celui du cas $\lambda_1 \neq 0$ et $\lambda_2 \neq 0$ donne

$$\tau_1 = \mu\sqrt{q},$$

avec $|\mu| \leq 4$.

Finalement, peu importe la congruence de q, nous avons, en posant $\lambda_1 = 0$ dans l'équation (2.1.12) et en utilisant le Théorème 1.3.2.1 pour la valeur de $G_\psi(1)$, que

$$\begin{aligned}\tau_2 &= \sum_{b_1 \in \mathbb{F}_q} \psi\left(-\frac{\lambda_2}{2} b_1^2\right) \sum_{b_2 \in \mathbb{F}_q^*} \left(\frac{b_2}{q}\right) \psi(\lambda_2 b_2) \\ &= \left(\frac{-\frac{\lambda_2}{2}}{q}\right)\left(\frac{\lambda_2}{q}\right) G_\psi(1)^2 \\ &= \left(\frac{2}{q}\right) q.\end{aligned}$$

Nous avons donc que

$$L(s,\chi,\Gamma) = \begin{cases} 1 + \mu q^{\frac{1}{2}-s} + \left(\frac{2}{q}\right) q^{1-2s} & q \equiv 1 \mod 4, \\ 1 + \left(\frac{2}{q}\right) q^{1-2s} & q \equiv 3 \mod 4, \end{cases}$$

avec $|\mu| \leq 4$.

Résumons toutes les valeurs prises par la fonction $L(s,\chi,\Gamma_1)$:

$$L(s,\chi,\Gamma_1)$$

$$= \begin{cases} 1 & \lambda_1 = 0, \lambda_2 = 0, \\ 1 + \sigma q^{\frac{1}{2}-s} + \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{2}{q}\right) q^{1-2s} & \lambda_1 \neq 0, \lambda_2 \neq 0, \\ 1 + \left(\frac{\lambda_1}{q}\right) G_\psi(1) q^{-s} & \lambda_1 \neq 0, \lambda_2 = 0, \\ 1 + \mu q^{\frac{1}{2}-s} + \left(\frac{2}{q}\right) q^{1-2s} & \lambda_1 = 0, \lambda_2 \neq 0, q \equiv 1 \mod 4, \\ 1 + \left(\frac{2}{q}\right) q^{1-2s} & \lambda_1 = 0, \lambda_2 \neq 0, q \equiv 3 \mod 4, \end{cases} \tag{2.1.14}$$

où $|\sigma| \leq 4$ et $|\mu| \leq 4$.

L'astuce de la preuve du Théorème 2.1.1 est de calculer

$$\sum_{\substack{\lambda_1,\lambda_2 \in \mathbb{F}_q \\ c \in \{0,1\}}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1} \Gamma_c(a_n) \log L(s, \chi_{\lambda_1,\lambda_2}, \Gamma_c) \tag{2.1.15}$$

de deux manières différentes, et ensuite de les comparer.

Pour la première méthode, reprenons l'équation :

$$L(s,\chi,\Gamma) = \prod_P (1 - \chi(P)\Gamma(P)|P|^{-s})^{-1}.$$

En appliquant le logarithme naturel de chaque côté de l'équation et par la suite la série de Taylor du logarithme au membre de droite, nous obtenons :

$$\log(L(s,\chi,\Gamma)) = \sum_P \sum_{r=1}^{\infty} \frac{1}{r} \chi(P^r)\Gamma(P^r)|P|^{-rs}. \tag{2.1.16}$$

À l'aide de (2.1.16), nous obtenons une première méthode de calcul :

$$\begin{aligned}
&\sum_{\substack{\lambda_1,\lambda_2 \in \mathbb{F}_q \\ c \in \{0,1\}}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1} \Gamma_c(a_n) \log L(s, \chi_{\lambda_1,\lambda_2}, \Gamma_c) \\
&= \sum_{\substack{\lambda_1,\lambda_2 \in \mathbb{F}_q \\ c \in \{0,1\}}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1} \Gamma_c(a_n) \sum_P \sum_{r=1}^{\infty} \frac{1}{r} \chi_{\lambda_1,\lambda_2}(P^r)\Gamma_c(P^r)|P|^{-rs} \\
&= \sum_P \sum_{r=1}^{\infty} \frac{|P|^{-rs}}{r} \sum_{\substack{\lambda_1,\lambda_2 \in \mathbb{F}_q \\ c \in \{0,1\}}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1} \Gamma_c(a_n) \chi_{\lambda_1,\lambda_2}(P^r)\Gamma_c(P^r).
\end{aligned}$$

Travaillons

$$\sum_{\substack{\lambda_1,\lambda_2 \in \mathbb{F}_q \\ c \in \{0,1\}}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1} \Gamma_c(a_n) \chi_{\lambda_1,\lambda_2}(P^r)\Gamma_c(P^r). \tag{2.1.17}$$

Si P^r est de la forme $(a_1, a_2, sgn(a_n))$, alors il est clair que

$$\chi_{\lambda_1,\lambda_2}(P^r) = \chi_{\lambda_1,\lambda_2}(a_1,a_2)$$

$$\Gamma_c(P^r) = \Gamma_c(a_n)$$

et que

$$\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_c(a_n)\chi_{\lambda_1,\lambda_2}(P^r)\Gamma_c(P^r) = 1.$$

Si P^r n'est pas de cette forme, alors

$$\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_c(a_n)\chi_{\lambda_1,\lambda_2}(P^r)\Gamma_c(P^r) = \chi_{\lambda_1,\lambda_2}(c_1,c_2)\Gamma_c(c_n),$$

pour $(c_1,c_2) \neq (0,0)$ et $c_n \in \mathbb{F}_q^*$.

Par conséquent, dans ce cas, par l'équation (2.1.2),

$$\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_q \\ c\in\{0,1\}}} \chi_{\lambda_1,\lambda_2}(c_1,c_2)\Gamma_c(c_n) = 0.$$

Donc, si nous résumons :

$$(2.1.17) = \begin{cases} 2q^2 & P^r \sim \text{forme } (a_1,a_2,sgn(a_n)), \\ 0 & P^r \nsim \text{forme } (a_1,a_2,sgn(a_n)). \end{cases}$$

D'où

$$\begin{aligned}\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_q \\ c\in\{0,1\}}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_c(a_n)\log L(s,\chi_{\lambda_1,\lambda_2},\Gamma_c) &= 2q^2 \sum_{P:P^r\sim(a_1,a_2,sgn(a_n))} \sum_{r=1}^{\infty} \frac{|P|^{-rs}}{r} \\ &= 2q^2 \sum_{r=1}^{\infty} \sum_{P:P^r\sim(a_1,a_2,sgn(a_n))} \frac{q^{-\deg(P)rs}}{r} \\ &= 2q^2 \sum_{n=1}^{\infty} \sum_{d|n} \frac{d}{n} v(n,d,a_1,a_2,sgn(a_n)) q^{-sn},\end{aligned}$$

où, dans la dernière égalité, nous avons posé $d = \deg P$ et effectué le changement de variable $n = rd$.

Dans la dernière partie, $v(n,d,a_1,a_2,sgn(a_n))$ représente le nombre de polynômes P de degré d tels que $P^{\frac{n}{d}}$ est de la forme $(a_1,a_2,sgn(a_n))$. Notons que $H_n(a_1,a_2,sgn(a_n)) = v(n,n,a_1,a_2,sgn(a_n))$.

Nous concluons donc que

$$(2.1.15) = 2q^2 \sum_{n=1}^{\infty} \sum_{d|n} \frac{d}{n} v(n, d, a_1, a_2, sgn(a_n)) q^{-sn}. \tag{2.1.18}$$

Donc, nous avons une première méthode de calcul. La deuxième méthode consiste à séparer (2.1.15) selon la valeur que prennent λ_1, λ_2 et c. Nous séparons ainsi l'expression en trois expressions selon ces cas :

$$\lambda_1 = 0, \lambda_2 = 0, c = 0 \tag{2.1.19}$$

$$(\lambda_1, \lambda_2) \neq (0, 0), c = 0; \lambda_2 = 0, c = 1 \tag{2.1.20}$$

$$\lambda_2 \neq 0, c = 1. \tag{2.1.21}$$

Nous ferons référence à $(2.1.19) - (2.1.21)$ pour la suite.

Avant de commencer, nous allons donner une formule pour $\log L(s, \chi_{\lambda_1,\lambda_2}, \Gamma_c)$ pour chacun des cas, et ce en utilisant la formule de Taylor du logarithme.

Par l'équation (2.1.10), nous avons, avec une valeur de s qui assure la convergence ($Re(s) > \frac{1}{2}$ si q suffisamment grand), que

$$\log L(s, \chi, \Gamma_0) = \begin{cases} \sum_{n=1}^{\infty} q^{-sn} \frac{q^n - 1}{n} & \lambda_1 = 0, \lambda_2 = 0, \\ \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} q^{-sn} \left(\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right) \left(\frac{-\frac{\lambda_2}{2}}{q}\right) G_\psi(1) - 1 \right)^n & \lambda_2 \neq 0, \\ \sum_{n=1}^{\infty} -\frac{q^{-sn}}{n} & \lambda_1 \neq 0, \lambda_2 = 0. \end{cases}$$

Enfin, pour l'équation (2.1.14), toujours avec une valeur de s qui assure la convergence ($Re(s) > \frac{1}{2}$ si q suffisamment grand), nous avons que

$$\log L(s, \chi, \Gamma_1) = \begin{cases} 0 & \lambda_1 = 0, \lambda_2 = 0, \\ \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} (\sigma q^{\frac{1}{2}-s} + \left(\frac{2}{q}\right) \psi(\frac{\lambda_1^2}{2\lambda_2}) q^{1-2s})^n & \lambda_1 \neq 0, \lambda_2 \neq 0, \\ \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \left(\frac{\lambda_1}{q}\right)^n G_\psi(1)^n q^{-sn} & \lambda_1 \neq 0, \lambda_2 = 0, \\ \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} (\mu q^{\frac{1}{2}-s} + \left(\frac{2}{q}\right) q^{1-2s})^n & \lambda_1 = 0, \lambda_2 \neq 0, q \equiv 1 \mod 4, \\ \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \left(\frac{2}{q}\right)^n q^{n(1-2s)} & \lambda_1 = 0, \lambda_2 \neq 0, q \equiv 3 \mod 4, \end{cases}$$

toujours avec $|\sigma|, |\mu| \leq 4$.

Traitons le cas (2.1.19) :

$$\log(L(s,\chi_{0,0},\Gamma_0)) = \sum_{n=1}^{\infty} \frac{q^{-ns}}{n}(q^n-1).$$

Traitons le cas (2.1.20). Il est clair que

$$\sum_{\substack{(\lambda_1,\lambda_2)\neq(0,0),c=0\\ \lambda_2=0,c=1}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\log L(s,\chi_{\lambda_1,\lambda_2},\Gamma_0) = \sum_{n=1}^{\infty} q^{-sn} f_1(n,q),$$

avec $f_1(n,q) = O\left(\frac{q^{\frac{n}{2}}}{n}\right)$.

Traitons le cas (2.1.21). Considérons tout d'abord les cas $\lambda_1 \neq 0$, $\lambda_2 \neq 0$ et $\lambda_1 = 0$, $\lambda_2 \neq 0$, $q \equiv 1 \mod 4$:

$$\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\log L(s,\chi_{\lambda_1,\lambda_2},\Gamma_1)$$

$$= \sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}(\tau_1 q^{-s}+\tau_2 q^{-2s})^n. \tag{2.1.22}$$

Ensuite, travaillons simplement $\log(L(s,\chi_{\lambda_1,\lambda_2},\Gamma_1))$.

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\tau_1 q^{-s}+\tau_2 q^{-2s}\right)^n &= \sum_{n=1}^{\infty} q^{-sn}\frac{(-1)^{n+1}}{n}\left(\tau_1+\tau_2 q^{-s}\right)^n \\
&= \sum_{n=1}^{\infty}\sum_{k=0}^{n}\binom{n}{k}\frac{q^{-sn}(-1)^{n+1}}{n}\tau_1^{n-k}\tau_2^k q^{-sk} \\
&= \sum_{n=1}^{\infty}\sum_{k=0}^{n}\binom{n}{k}\frac{(-1)^{n+1}}{n}\tau_1^{n-k}\tau_2^k q^{-s(k+n)} \\
&= \sum_{u=1}^{\infty} q^{-su}\left(\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{(-1)^{n+1}}{n}\tau_1^{2n-u}\tau_2^{u-n}\right),
\end{aligned}$$

où nous avons fait le changement de variables $u = k+n$.

Donc,

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\tau_1 q^{-s}+\tau_2 q^{-2s}\right)^n=\sum_{u=1}^{\infty}q^{-su}\left(\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{(-1)^{n+1}}{n}\tau_1^{2n-u}\tau_2^{u-n}\right). \tag{2.1.23}$$

Alors,

(2.1.22)

$$=\sum_{u=1}^{\infty}q^{-su}\left(\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}}\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{(-1)^{n+1}}{n}\tau_1^{2n-u}\tau_2^{u-n}\right).$$

En poursuivant, nous avons que

$$\begin{aligned}
&\left|\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}}\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{(-1)^{n+1}}{n}\tau_1^{2n-u}\tau_2^{u-n}\right|\\
&\leq\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{|\tau_1|^{2n-u}|\tau_2|^{u-n}}{n}\\
&\leq\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{16^{n-\frac{u}{2}}q^{n-\frac{u}{2}}q^{u-n}}{n},
\end{aligned}$$

car $|\tau_1|\leq 4\sqrt{q}$ et $|\tau_2|=q$ (par les équations (2.1.13) et (2.1.14)).

De cette expression, nous pouvons sortir de la sommation les puissances qui ne dépendent pas de n, et nous obtenons

$$\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}}\left(\frac{q}{16}\right)^{\frac{u}{2}}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{16^n}{n}.$$

À partir d'ici, nous pouvons trouver une borne supérieure pour $\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{16^n}{n}$:

$$\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{16^n}{n}\leq\frac{2}{u}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}16^n$$

$$\leq \frac{2}{u}\sum_{n=0}^{u}\binom{u}{u-n}16^n$$
$$= 2\cdot\frac{17^u}{u},$$

en utilisant le binôme de Newton.

En mettant tous ces résultats ensemble, nous obtenons

$$\left|\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{(-1)^{n+1}}{n}\tau_1^{2n-u}\tau_2^{u-n}\right|$$
$$\leq 2\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}}\left(\frac{q}{16}\right)^{\frac{u}{2}}\frac{17^u}{u}$$
$$= 2\left((q-1)^2+(q-1)\mathbb{1}_{q\equiv 1 \mod 4}\right)\left(\frac{289q}{16}\right)^{\frac{u}{2}}\frac{1}{u}$$
$$= 2\left((q-1)^2+(q-1)\mathbb{1}_{q\equiv 1 \mod 4}\right)\frac{(18,0625q)^{\frac{u}{2}}}{u}.$$

Donc, nous pouvons conclure que

$$\sum_{\substack{\lambda_1\in\mathbb{F}_q^*,\lambda_2\in\mathbb{F}_q^*\\ \lambda_1=0,\lambda_2\in\mathbb{F}_q^*,q\equiv 1 \mod 4}} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\log L(s,\chi_{\lambda_1,\lambda_2},\Gamma_1)=\sum_{u=1}^{\infty}q^{-su}f_2(u,q),$$

avec $f_2(u,q)=O\left(\frac{(18,0625q)^{\frac{u}{2}}}{u}\right)$.

Maintenant, si $\lambda_1=0$, $\lambda_2\neq 0$ et $q\equiv 3 \mod 4$. Nous avons que

$$\sum_{\lambda_2\in\mathbb{F}_q^*}\chi_{0,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\log L(s,\chi_{0,\lambda_2},\Gamma_1)$$
$$=\sum_{\lambda_2\in\mathbb{F}_q^*}\chi_{0,\lambda_2}(a_1,a_2)^{-1}\Gamma_1(a_n)\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}\left(\frac{2}{q}\right)^n q^{n(1-2s)}.$$

En posant

$$\epsilon_u=\begin{cases}1 & u \text{ est pair},\\ 0 & u \text{ est impair},\end{cases}$$

il est clair que

$$\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \left(\frac{2}{q}\right)^n q^{n(1-2s)} = 2 \sum_{m=1}^{\infty} q^{-sm} \epsilon_m \frac{(-1)^{\frac{m}{2}+1}}{m} \left(\frac{2}{q}\right)^{\frac{m}{2}} q^{\frac{m}{2}}$$
$$= \sum_{m=1}^{\infty} q^{-sm} f_3(m,q),$$

où $n = \frac{m}{2}$ et avec $f_3(m,q) = O\left(\frac{q^{\frac{m}{2}}}{m}\right)$.

Nous pouvons donc dire que

$$\sum_{\lambda_2 \neq 0, c=1} \chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1} \Gamma_1(a_n) \log L(s, \chi_{\lambda_1,\lambda_2}, \Gamma_1) = \sum_{n=1}^{\infty} q^{-sn} f_4(n,q),$$

avec $f_4(n,q) = O\left(\frac{(18{,}0625q)^{\frac{n}{2}}}{n}\right)$.

En mettant tous ces résultats ensemble, nous voyons que

$$(2.1.15) = \sum_{n=1}^{\infty} q^{-sn} \left(\frac{q^n - 1}{n} + f_1(n,q) + f_4(n,q)\right).$$

En comparant cette expression avec (2.1.18), nous obtenons

$$2q^2 \sum_{d|n} \frac{d}{n} v(n,d,a_1,a_2,sgn(a_n)) = \frac{q^n}{n} + O\left(\frac{(18,0625q)^{\frac{n}{2}}}{n}\right)$$

ou encore

$$\sum_{d|n} \frac{d}{n} v(n,d,a_1,a_2,sgn(a_n)) = \frac{q^{n-2}}{2n} + O\left(\frac{(18,0625q)^{\frac{n}{2}}}{n}\right).$$

En utilisant la formule d'inversion de Möbius, nous obtenons

$$v(n,n,a_1,a_2,sgn(a_n)) = H_n(a_1,a_2,sgn(a_n)) = \frac{q^{n-2}}{2n} + O\left(\frac{(18,0625q)^{\frac{n}{2}}}{n}\right).$$

2.2. Résultat asympotique pour (t_1, t_2, t_3) fixés

Soit M un polynôme dont les coefficients appartiennent à un corps fini quelconque $\mathbb{F}_q$ de caractéristique p :

$$M = x^n + a_1 x^{n-1} + a_2 x^{n-2} + a_3 x^{n-3} + t_4 x^{n-4} + \cdots + t_n. \tag{2.2.1}$$

Dans notre cas, (a_1, a_2, a_3) est fixé, et les t_i, pour $i \geq 4$, sont quelconques. Nous dirons d'un polynôme dont les coefficients a ces contraintes qu'il est de la forme (a_1, a_2, a_3). Soit $H_n(a_1, a_2, a_3)$ le nombre de polynômes irréductibles de cette forme. Alors, nous allons prouver le théorème qui suit.

Théorème 2.2.1. *Soit p la caractéristique d'un corps quelconque $\mathbb{F}_q$. Supposons que $p \neq 2$ et que $p \neq 3$. Alors, nous avons que*

$$H_n(a_1, a_2, a_3) = \frac{q^{n-3}}{n} + O\left(\frac{(6, 25q)^{\frac{n}{2}}}{n}\right).$$

La première étape, encore une fois, est de définir le caractère que nous utiliserons. Le caractère associé aux trois premiers coefficients, a_1, a_2 et a_3 sera un caractère additif. C'est pourquoi nous avons encore besoin de la fonction ψ introduite à la Définition 1.3.1.1, que nous rappellons à l'instant :

$$\psi(a) = e^{\frac{2\pi i Tr(a)}{p}}.$$

À partir de cette fonction, nous pouvons introduire le caractère avec lequel nous travaillerons, et ce pour $\deg M \geqslant 3$:

$$\chi(M) = \chi_{\lambda_1\lambda_2,\lambda_3}(a_1, a_2, a_3) = \psi\left(\lambda_1 a_1 + \lambda_2\left(a_2 - \frac{a_1^2}{2}\right) + \lambda_3\left(a_3 - a_1 a_2 + \frac{a_1^3}{3}\right)\right).$$

D'entrée de jeu, définissons

$$\begin{aligned}
\chi(1) &= \chi_{\lambda_1\lambda_2,\lambda_3}(0, 0, 0) = 1 \\
\chi(x + a) &= \chi_{\lambda_1\lambda_2,\lambda_3}(a, 0, 0) = \psi\left(\lambda_1 a - \frac{\lambda_2}{2}a^2 + \frac{\lambda_3}{3}a^3\right) \\
\chi(x^2 + ax + b) &= \chi_{\lambda_1\lambda_2,\lambda_3}(a, b, 0) = \psi\left(\lambda_1 a + \lambda_2\left(b - \frac{a^2}{2}\right) - \lambda_3\left(ab - \frac{a^3}{3}\right)\right).
\end{aligned}$$

Remarque 2.2.1. *Notons que ce caractère n'est pas valide pour les corps de caractéristique 2 et 3.*

Montrons que ce caractère est multiplicatif. En effet, soient A et B deux polynômes de $\mathbb{F}_q[x]$:

$$\begin{aligned} A(x) &= x^n + u_1 x^{n-1} + u_2 x^{n-2} + u_3 x^{n-3} + \cdots + u_n \\ B(x) &= x^m + v_1 x^{m-1} + v_2 x^{m-2} + v_3 x^{m-3} + \cdots + v_m. \end{aligned}$$

Alors,

$$\begin{aligned} A(x)B(x) =& x^{n+m} + (u_1 + v_1)x^{m+n-1} + (u_2 + u_1 v_1 + v_2)x^{m+n-2} \\ &+ (u_3 + v_3 + u_1 v_2 + u_2 v_1)x^{m+n-3} + \cdots + u_n v_m. \end{aligned}$$

Nous avons donc que

$$\begin{aligned} &\chi(AB) \\ &= \psi\left(\lambda_1(u_1+v_1) + \lambda_2\left(u_2 + u_1v_1 + v_2 - \frac{(u_1+v_1)^2}{2}\right) + \lambda_3 f(u_i, v_i)\right) \\ &= \psi\left(\lambda_1 u_1 + \lambda_1 v_1 + \lambda_2\left(u_2 + v_2 - \frac{u_1^2}{2} - \frac{v_1^2}{2}\right)\right)\psi(\lambda_3 f(u_i, v_i)) \\ &= \psi\left(\lambda_1 u_1 + \lambda_2\left(u_2 - \frac{u_1^2}{2}\right)\right)\psi\left(\lambda_1 v_1 + \lambda_2\left(v_2 - \frac{v_1^2}{2}\right)\right)\psi(\lambda_3 f(u_i, v_i)), \end{aligned}$$

avec

$$\begin{aligned} f(u_i, v_i) =& u_3 + v_3 + u_1 v_2 + u_2 v_1 - (u_1 + v_1)(u_2 + v_2 + u_1 v_1) + \frac{(u_1+v_1)^3}{3} \\ =& u_3 + v_3 + u_1 v_2 + u_2 v_1 - u_1 u_2 - u_1 v_2 - u_1^2 v_1 - u_2 v_1 - v_1 v_2 - u_1 v_1^2 \\ &+ \frac{u_1^3 + 3u_1^2 v_1 + 3u_1 v_1^2 + v_1^3}{3} \\ =& u_3 + v_3 - u_1 u_2 - v_1 v_2 + \frac{u_1^3}{3} + \frac{v_1^3}{3}. \end{aligned}$$

Ainsi,

$$\begin{aligned} \psi(\lambda_3 f(u_i, v_i)) &= \psi\left(\lambda_3\left(u_3 + v_3 - u_1 u_2 - v_1 v_2 + \frac{u_1^3}{3} + \frac{v_1^3}{3}\right)\right) \\ &= \psi\left(\lambda_3\left(u_3 - u_1 u_2 + \frac{u_1^3}{3}\right)\right)\psi\left(\lambda_3\left(v_3 - v_1 v_2 + \frac{v_1^3}{3}\right)\right), \end{aligned}$$

et

$$\chi(AB) = \psi\left(\lambda_1 u_1 + \lambda_2\left(u_2 - \frac{u_1^2}{2}\right) + \lambda_3\left(u_3 - u_1 u_2 + \frac{u_1^3}{3}\right)\right)$$

$$\begin{aligned}&\psi\left(\lambda_1 v_1+\lambda_2\left(v_2-\frac{v_1^2}{2}\right)+\lambda_3\left(v_3-v_1v_2+\frac{v_1^3}{3}\right)\right)\\=&\chi(A)\chi(B),\end{aligned}$$

d'où nous concluons que le caractère est multiplicatif.

Calculons maintenant certaines quantités qui dépendent de $\chi_{\lambda_1\lambda_2,\lambda_3}(a_1,a_2,a_3)$. Tout d'abord, il est clair que

$$\chi_{0,0,0}=1.$$

Ensuite, par le Théorème 1.3.1.1, il est clair que

$$\sum_{\lambda_1\lambda_2,\lambda_3\in\mathbb{F}_q}\chi_{\lambda_1\lambda_2,\lambda_3}(a_1,a_2,a_3)=\begin{cases}0 & (a_1,a_2,a_3)\neq 0,\\ q^3 & (a_1,a_2,a_3)=0,\end{cases}$$

$$\sum_{a_1,a_2,a_3\in\mathbb{F}_q}\chi_{\lambda_1\lambda_2,\lambda_3}(a_1,a_2,a_3)=\begin{cases}0 & (\lambda_1\lambda_2,\lambda_3)\neq 0,\\ q^3 & (\lambda_1\lambda_2,\lambda_3)=0.\end{cases}$$

Reprenons notre fonction L, définie pour $Re(s)>1$, par

$$L(s,\chi)=\sum_M\chi(M)|M|^{-s}=\prod_P(1-\chi(P)|P|^{-s})^{-1},$$

où P parcourt les polynômes irréductibles unitaires de $\mathbb{F}_q[x]$.

Rappelons aussi que

$$L(s,\chi)=\sum_{m=0}^{\infty}\tau_m q^{-sm}, \tag{2.2.2}$$

où

$$\tau_m=\sum_{\deg M=m}\chi(M).$$

Nous devons calculer $L(s,\chi_{\lambda_1\lambda_2,\lambda_3})$ pour toutes les valeurs de $(\lambda_1\lambda_2,\lambda_3)$ possibles.

Pour le cas $(\lambda_1, \lambda_2, \lambda_3) = (0, 0, 0)$, il est clair que

$$L(s, \chi_{0,0,0}) = \sum_M |M|^{-s} = \sum_{m=0}^{\infty} q^{-sm} \sum_{\deg M = m} 1 \quad = \sum_{m=0}^{\infty} q^{m(1-s)} = \frac{1}{1 - q^{1-s}}. \quad (2.2.3)$$

Pour les cas $(\lambda_1, \lambda_2, \lambda_3) \neq (0, 0, 0)$, nous allons simplement écrire $L(s, \chi)$ comme (2.2.2).

Pour $m = 0$, nous avons que

$$\tau_0 = \sum_{\deg M = 0} \chi(M) = \chi(1) = \chi(0, 0, 0) = 1.$$

Pour $m = 1$, nous avons que

$$\tau_1 = \sum_{\deg M = 1} \chi(M) = \sum_{a \in \mathbb{F}_q} \chi(a, 0, 0) = \sum_{a \in \mathbb{F}_q} \psi\left(\lambda_1 a - \frac{\lambda_2}{2} a^2 + \frac{\lambda_3}{3} a^3\right). \quad (2.2.4)$$

Pour $m = 2$, nous avons que

$$\begin{aligned} \tau_2 &= \sum_{\deg M = 2} \chi(M) = \sum_{b_1 \in \mathbb{F}_q} \sum_{b_2 \in \mathbb{F}_q} \chi(b_1, b_2, 0) \\ &= \sum_{b_1 \in \mathbb{F}_q} \sum_{b_2 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 + \lambda_2 \left(b_2 - \frac{b_1^2}{2}\right) + \lambda_3 \left(-b_1 b_2 + \frac{b_1^3}{3}\right)\right) \\ &= \sum_{b_1 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 - \frac{\lambda_2}{2} b_1^2 + \frac{\lambda_3}{3} b_1^3\right) \sum_{b_2 \in \mathbb{F}_q} \psi(\lambda_2 b_2 - \lambda_3 b_1 b_2). \end{aligned}$$

D'où

$$\tau_2 = \sum_{b_1 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 - \frac{\lambda_2}{2} b_1^2 + \frac{\lambda_3}{3} b_1^3\right) \sum_{b_2 \in \mathbb{F}_q} \psi(\lambda_2 b_2 - \lambda_3 b_1 b_2). \quad (2.2.5)$$

Pour $m \geq 3$, nous avons que

$$\begin{aligned} \tau_m &= \sum_{\deg M = m} \chi(M) = q^{m-3} \sum_{b_1 \in \mathbb{F}_q} \sum_{b_2 \in \mathbb{F}_q} \sum_{b_3 \in \mathbb{F}_q} \chi(b_1, b_2, b_3) \\ &= q^{m-3} \sum_{b_1 \in \mathbb{F}_q} \sum_{b_2 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 + \lambda_2 \left(b_2 - \frac{a_1^2}{2}\right) + \lambda_3 \left(-b_1 b_2 + \frac{b_1^3}{3}\right)\right) \sum_{b_3 \in \mathbb{F}_q} \psi(\lambda_3 b_3) = 0, \end{aligned}$$

par le Théorème 1.3.1.1.

Encore une fois, l'astuce pour prouver le Théorème 2.2.1 est, supposant que les trois premiers coefficients sont fixés et égals à (a_1, a_2, a_3), de calculer

$$\sum_{\lambda_1,\lambda_2,\lambda_3} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1,a_2,a_3)^{-1} \log L(s, \chi_{\lambda_1,\lambda_2,\lambda_3}) \tag{2.2.6}$$

de deux manières différentes.

En effectuant une méthode essentiellement identique à celle qui a mené à l'équation (2.1.18) de la section précédente, nous obtenons

$$(2.2.6) = q^3 \sum_{n=1}^{\infty} \sum_{d|n} \frac{d}{n} v(n, d, a_1, a_2, a_3) q^{-sn}, \tag{2.2.7}$$

où $v(n, d, a_1, a_2, a_3)$ représente le nombre de polynômes P de degré d tels que $P^{\frac{n}{d}}$ est de la forme (a_1, a_2, a_3).

Notons aussi que $v(n, n, a_1, a_2, a_3) = H_n(a_1, a_2, a_3)$.

Remarquons la similitude entre (2.1.18) et (2.2.7). Dans la section précédente, nous avions q^2 manières de choisir les deux premiers coefficients, et le caractère multiplicatif ne prenait que deux valeurs, d'où le terme $2q^2$. Dans le cas présent, nous avons q^3 manières de choisir parmi les trois premiers coefficients.

L'autre méthode consiste à séparer (2.2.6) selon les valeurs que prennent $(\lambda_1, \lambda_2, \lambda_3)$. Nous allons considérer les cas suivants :

$$(\lambda_1, \lambda_2, \lambda_3) = (0, 0, 0) \tag{2.2.8}$$

$$(\lambda_1, \lambda_2, \lambda_3) = (a, b, 0) \tag{2.2.9}$$

$$\lambda_3 \neq 0, \tag{2.2.10}$$

où $a, b \in \mathbb{F}_q$, et au moins un des deux éléments n'est pas 0.

Donc,

$$\begin{aligned}(2.2.6) = &\log L(s, \chi_{0,0,0}) \\ &+ \sum_{(\lambda_1,\lambda_2)\neq(0,0)} \chi_{\lambda_1,\lambda_2,0}(a_1,a_2,a_3)^{-1} \log L(s, \chi_{\lambda_1,\lambda_2}) \\ &+ \sum_{\lambda_1,\lambda_2\in\mathbb{F}_q} \sum_{\lambda_3\in\mathbb{F}_q^*} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1,a_2,a_3)^{-1} \log L(s, \chi_{\lambda_1,\lambda_2,\lambda_3}).\end{aligned}$$

Traitons le cas (2.2.8) :

$$\log L(s, \chi_{0,0,0}) = \sum_{n=1}^{\infty} q^{-sn} \frac{q^n}{n}.$$

Traitons le cas (2.2.9) :

$$\begin{aligned} &\sum_{(\lambda_1,\lambda_2)\neq(0,0)} \chi_{\lambda_1,\lambda_2,0}(a_1,a_2,a_3)^{-1} \log L(s, \chi_{\lambda_1,\lambda_2,0}) \\ &= \sum_{(\lambda_1,\lambda_2)\neq(0,0)} \chi_{\lambda_1,\lambda_2,0}(a_1,a_2,a_3)^{-1} \log\left(1 + \tau_1 q^{-s} + \tau_2 q^{-2s}\right). \end{aligned}$$

Si $\lambda_3 = 0$, alors il est facile de voir que $\tau_2 = 0$, par l'équation (2.2.5) et le Théorème 1.3.1.1. Nous avons donc que

$$\begin{aligned} &\sum_{(\lambda_1,\lambda_2)\neq(0,0)} \chi_{\lambda_1,\lambda_2,0}(a_1,a_2,a_3)^{-1} \log\left(1 + \tau_1 q^{-s}\right) \\ &= \sum_{n=1}^{\infty} q^{-sn} \frac{(-1)^{n+1}}{n} \sum_{(\lambda_1,\lambda_2)\neq(0,0)} \chi_{\lambda_1,\lambda_2,0}(a_1,a_2,a_3)^{-1} \tau_1^n. \end{aligned}$$

Nous pouvons calculer la valeur exacte de τ_1, mais nous savons que nous n'avons pas de résultats exacts pour le cas où $\lambda_3 \neq 0$. Alors, une valeur asymptotique de τ_1 suffit ici. Par le Théorème 1.3.2.3, nous avons que

$$|\tau_1| \leq \sqrt{q}.$$

Donc, nous savons que

$$\sum_{(\lambda_1,\lambda_2)\neq(0,0)} \chi_{\lambda_1,\lambda_2,0}(a_1,a_2,a_3)^{-1} \log L(s, \chi_{\lambda_1,\lambda_2,0}) = \sum_{n=1}^{\infty} q^{-sn} f_1(n,q),$$

où $f_1(n,q) = O\left(\frac{q^{\frac{n}{2}}}{n}\right)$.

Traitons le cas (2.2.10) :

$$\begin{aligned} &\sum_{\lambda_1,\lambda_2\in\mathbb{F}_q} \sum_{\lambda_3\in\mathbb{F}_q^*} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1,a_2,a_3)^{-1} \log L(s, \chi_{\lambda_1,\lambda_2,\lambda_3}) \\ &= \sum_{\lambda_1,\lambda_2\in\mathbb{F}_q} \sum_{\lambda_3\in\mathbb{F}_q^*} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1,a_2,a_3)^{-1} \log\left(1 + \tau_1 q^{-s} + \tau_2 q^{-2s}\right). \end{aligned}$$

Par l'équation (2.2.4) et le Théorème 1.3.2.3, nous avons que

$$|\tau_1| = \left| \sum_{a \in \mathbb{F}_q} \psi\left(\lambda_1 a - \frac{\lambda_2}{2}a^2 + \frac{\lambda_3}{3}a^3\right)\right| \leq 2\sqrt{q}. \tag{2.2.11}$$

Calculons maintenant les différentes valeurs de τ_2.

Si $(\lambda_1, \lambda_2) = (0, 0)$, alors par l'équation (2.2.5)

$$\tau_2 = \sum_{b_1 \in \mathbb{F}_q} \psi\left(\frac{\lambda_3}{3}b_1^3\right) \sum_{b_2 \in \mathbb{F}_q} \psi(-\lambda_3 b_1 b_2) = q,$$

par le Théorème 1.3.1.1 et en considérant le cas $b_1 = 0$.

Si $\lambda_1 \neq 0$ et $\lambda_2 \neq 0$, alors

$$\tau_2 = \sum_{b_1 \in \mathbb{F}_q} \psi\left(\lambda_1 b_1 - \frac{\lambda_2}{2}b_1^2 + \frac{\lambda_3}{3}b_1^3\right) \sum_{b_2 \in \mathbb{F}_q} \psi(b_2(\lambda_2 - \lambda_3 b_1)) = \psi\left(\frac{\lambda_1\lambda_2}{\lambda_3} - \frac{\lambda_2^3}{6\lambda_3^2}\right) q,$$

par le Théorème 1.3.1.1 et en considérant le cas $b_1 = \frac{\lambda_2}{\lambda_3}$.

Nous voyons donc que

$$|\tau_2| = q, \tag{2.2.12}$$

et ce quelque soit les valeurs que prennent λ_1 et λ_2.

En utilisant l'équation (2.1.23) et une technique identique à celle de la section précédente, nous voyons que

$$\begin{aligned}
&\sum_{\lambda_1,\lambda_2 \in \mathbb{F}_q} \sum_{\lambda_3 \in \mathbb{F}_q^*} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1, a_2, a_3)^{-1} \log\left(1 + \tau_1 q^{-s} + \tau_2 q^{-2s}\right) \\
&= \sum_{\lambda_1,\lambda_2 \in \mathbb{F}_q} \sum_{\lambda_3 \in \mathbb{F}_q^*} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1, a_2, a_3)^{-1} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \left(\tau_1 q^{-s} + \tau_2 q^{-2s}\right)^n \\
&= \sum_{u=1}^{\infty} q^{-su} \left(\sum_{\lambda_1,\lambda_2 \in \mathbb{F}_q} \sum_{\lambda_3 \in \mathbb{F}_q^*} \chi_{\lambda_1,\lambda_2,\lambda_3}(a_1, a_2, a_3)^{-1} \sum_{n=\lfloor \frac{u+1}{2} \rfloor}^{u} \binom{n}{u-n} \frac{(-1)^{n+1}}{n} \tau_1^{2n-u} \tau_2^{u-n} \right).
\end{aligned}$$

Nous avons que

$$\begin{aligned}
&\left|\sum_{\lambda_1,\lambda_2\in\mathbb{F}_q}\sum_{\lambda_3\in\mathbb{F}_q^*}\chi_{\lambda_1,\lambda_2,\lambda_3}(a_1,a_2,a_3)^{-1}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{(-1)^{n+1}}{n}\tau_1^{2n-u}\tau_2^{u-n}\right|\\
&\leq\sum_{\lambda_1,\lambda_2\in\mathbb{F}_q}\sum_{\lambda_3\in\mathbb{F}_q^*}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{|\tau_1|^{2n-u}|\tau_2|^{u-n}}{u}\\
&\leq\sum_{\lambda_1,\lambda_2\in\mathbb{F}_q}\sum_{\lambda_3\in\mathbb{F}_q^*}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{2^{2n-u}q^{\frac{u}{2}}}{n}\\
&\leq q^2(q-1)\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{2^{2n-u}q^{\frac{u}{2}}}{n},
\end{aligned}$$

par les équations (2.2.11) et (2.2.12).

Comme dans la Section 2.1, nous pouvons dire que

$$\begin{aligned}
q^2(q-1)\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{2^{2n-u}q^{\frac{u}{2}}}{n}&=q^2(q-1)\left(\frac{q}{4}\right)^{\frac{u}{2}}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}\frac{4^n}{n}\\
&\leq\frac{2q^2(q-1)}{u}\left(\frac{q}{4}\right)^{\frac{u}{2}}\sum_{n=\lfloor\frac{u+1}{2}\rfloor}^{u}\binom{n}{u-n}4^n\\
&\leq\frac{2q^2(q-1)}{u}\left(\frac{q}{4}\right)^{\frac{u}{2}}\sum_{n=0}^{u}\binom{u}{u-n}4^n\\
&=\frac{2q^2(q-1)5^u}{u}\left(\frac{q}{4}\right)^{\frac{u}{2}}\\
&=2q^2(q-1)\frac{(6,25q)^{\frac{u}{2}}}{u}.
\end{aligned}$$

D'où

$$\sum_{\lambda_1,\lambda_2\in\mathbb{F}_q}\sum_{\lambda_3\in\mathbb{F}_q^*}\chi_{\lambda_1,\lambda_2,\lambda_3}(a_1,a_2,a_3)^{-1}\log L(s,\chi_{\lambda_1,\lambda_2,\lambda_3})=\sum_{u=1}^{\infty}q^{-su}f_2(u,q),$$

avec $f_2(u,q)=O\left(\frac{(6,25q)^{\frac{u}{2}}}{u}\right)$.

Donc, si nous résumons, nous avons que

$$(2.2.6)=\sum_{n=1}^{\infty}q^{-sn}\left(\frac{q^n}{n}+f_1(n,q)+f_2(n,q)\right).$$

En comparant avec (2.2.7), nous voyons que

$$\sum_{d|n} \frac{d}{n} v(n, d, a_1, a_2, a_3) = \frac{q^{n-3}}{n} + O\left(\frac{(6, 25q)^{\frac{n}{2}}}{n}\right).$$

Finalement, par la formule d'inversion de Möbius,

$$H_n(a_1, a_2, a_3) = \frac{q^{n-3}}{n} + O\left(\frac{(6, 25q)^{\frac{n}{2}}}{n}\right),$$

ce qui complète la démonstration du Théorème 2.2.1.

Chapitre 3

RÉSULTAT EN FIXANT LE PREMIER COEFFICIENT ET LA CUBICITÉ DU DERNIER

Soit M un polynôme dont les coefficients appartiennent à un corps fini quelconque $\mathbb{F}_q$ de caractéristique p :

$$M = x^n + a_1x^{n-1} + t_2x^{n-2} + t_3x^{n-3} + t_4x^{n-4} + \cdots + a_n. \tag{3.0.1}$$

Dans ce qui suit, nous allons supposer que $p \equiv 1 \mod 3$ et donc que $q \equiv 1 \mod 3$. De plus, nous demandons que le premier coefficient soit $a_1 \in \mathbb{F}_q$ et nous voulons aussi que le dernier coefficient ait la même cubicité que $a_n \in \mathbb{F}_q$. Nous dirons d'un tel polynôme qu'il est de la forme $\left(a_1, \left(\frac{a_n}{q}\right)_{(3)}\right)$. Soit $H_n\left(a_1, \left(\frac{a_n}{q}\right)_{(3)}\right)$ le nombre de tels polynômes irréductibles unitaires de degré n. Nous montrerons, en se basant sur la méthode utilisée par Carlitz dans [**4**], le théorème suivant.

Théorème 3.0.1. *Soit $\mathbb{F}_q$ un corps de caractéristique p, avec $p \equiv 1 \mod 3$ et $q = p^k$. Alors, nous avons que*

$$H_n\left(a_1, \left(\frac{a_n}{q}\right)_{(3)}\right) = \frac{1}{n}\sum_{\substack{d|n \\ p\nmid d}} \mu(d) f\left(\frac{n}{d}\right),$$

avec, pour $a_1 \neq 0$,

$$f(n) = \begin{cases} \frac{q^{n-1}}{3} + \frac{(-1)^n}{3q}\left(\left(\frac{a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n}{3}} + \left(\frac{a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n}{3}}\right) & 3|n, \\ \frac{q^{n-1}}{3} + \frac{(-1)^{n-1}}{3}\left(\left(\frac{a_1a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n-1}{3}} + \left(\frac{a_1^2a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n-1}{3}}\right) & n \equiv 1 \mod 3, \\ \frac{q^{n-1}}{3} + \frac{(-1)^{n-1}}{3q}\left(\left(\frac{a_1^2a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n+1}{3}} + \left(\frac{a_1a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n+1}{3}}\right) & n \equiv 2 \mod 3, \end{cases}$$

et pour $a_1 = 0$,

$$f(n) = \quad = \begin{cases} \frac{q^{n-1}-1}{3} + \frac{(-1)^{n-1}(q-1)}{3q}\left(\left(\frac{a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n}{3}} + \left(\frac{a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n}{3}}\right) & 3|n, \\ \frac{q^{n-1}-1}{3} & 3\nmid n. \end{cases}$$

Nous définissons ϑ *et* $\bar{\vartheta}$ *de la manière suivante :*

$$\vartheta(s,t) = (-1)^{k-1}\left(\frac{ps \pm 3p|t|i\sqrt{3}}{2}\right)^k$$
$$\bar{\vartheta}(s,t) = (-1)^{k-1}\left(\frac{ps \mp 3p|t|i\sqrt{3}}{2}\right)^k.$$

Dans ces expressions, s *et* $|t|$ *sont des entiers relatifs entièrement déterminés par*

$$4p = s^2 + 27t^2$$
$$s \equiv 1 \mod 3.$$

La première étape, comme toujours, consiste à définir nos caractères. Tout d'abord, commençons par le caractère à attribuer pour le premier coefficient a_1. Reprenons comme toujours notre fonction additive habituelle :

$$\psi(a) = e^{\frac{2\pi i Tr(a)}{p}}.$$

De cette fonction, nous sommes en mesure de poser un premier caractère :

$$\chi_{\lambda_1}(M) = \psi(\lambda_1 a_1),$$

avec

$$\chi_{\lambda_1}(1) = 1.$$

Soit γ une racine primitive du corps fini $\mathbb{F}_q$. Si $a = \gamma^r$, alors rappelons le caractère multiplicatif suivant pour les cubes :

$$\left(\frac{a}{q}\right)_{(3)} = \begin{cases} 0 & a = 0, \\ 1 & 3|r, \\ e^{\frac{2\pi i}{3}} & r \equiv 1 \mod 3, \\ e^{\frac{4\pi i}{3}} & r \equiv 2 \mod 3. \end{cases}$$

Ceci nous permet donc de poser un second caractère, pour $a_n \in \mathbb{F}_q^*$. Pour $c \in \{0, 1, 2\}$, posons

$$\Gamma_c(M) = \begin{cases} \left(\frac{a_n^c}{q}\right)_{(3)} & a_n \neq 0, \\ 0 & a_n = 0. \end{cases}$$

Remarque 3.0.1. *Ces deux caractères sont multiplicatifs. Soient $A, B \in \mathbb{F}_q[x]$, alors :*

$$\chi_{\lambda_1}(AB) = \chi_{\lambda_1}(A)\chi_{\lambda_1}(B),$$
$$\Gamma_c(AB) = \Gamma_c(A)\Gamma_c(B).$$

Calculons maintenant certaines quantités concernant ces deux caractères. Par le Théorème 1.3.1.1, il est facile de voir que

$$\sum_{\chi} \chi_{\lambda_1}(M) = \sum_{\lambda_1 \in \mathbb{F}_q} \psi(\lambda_1 a_1) = \begin{cases} q & a_1 = 0, \\ 0 & a_1 \neq 0. \end{cases} \tag{3.0.2}$$

De plus, pour $a_n \in \mathbb{F}_q^*$, il est facile de voir que

$$\sum_{\Gamma} \Gamma_c(M) = 1 + \Gamma_1(a_n) + \Gamma_2(a_n) = \begin{cases} 3 & a_n \text{ est un cube}, \\ 0 & a_n \text{ n'est pas un cube}. \end{cases} \tag{3.0.3}$$

Enfin, de manière similaire, nous avons que

$$\sum_{\substack{\deg M = m \\ m \geq 1}} \chi_{\lambda_1}(M) = \begin{cases} q^m & \lambda_1 = 0, \\ 0 & \lambda_1 \neq 0, \end{cases} \tag{3.0.4}$$

$$\sum_{\substack{\deg M=m \\ m\geq 1}} \Gamma_c(M) = \begin{cases} 0 & c \in \{1,2\}, \\ q^{m-1}(q-1) & c = 0. \end{cases} \tag{3.0.5}$$

Comme à l'habitude, définissons notre fonction L, pour $Re(s) > 1$, de la manière suivante :

$$\begin{aligned} L(s,\chi,\Gamma) &= \sum_{M} \chi(M)\Gamma(M)|M|^{-s} \\ &= \sum_{m=0}^{\infty} \tau_m q^{-ms} \\ &= \prod_{P} (1-\chi(P)\Gamma(P)|P|^{-s})^{-1}, \end{aligned}$$

où $\tau_m = \sum_{\deg M=m} \chi(M)\Gamma(M)$ et où P parcourt tous les polynômes irréductibles unitaires de $\mathbb{F}_q[x]$.

Calculons maintenant les valeurs que prend la fonction L selon λ_1 et c.

Supposons que $\lambda_1 = c = 0$. Alors, en se servant de (3.0.4) et de (3.0.5), nous pouvons faire une démarche identique à ce qui a mené au cas $\lambda_1 = \lambda_2 = 0$ de (2.1.10) pour obtenir

$$L(s,\chi_0,\Gamma_0) = \frac{1-q^{-s}}{1-q^{1-s}}. \tag{3.0.6}$$

Supposons que $\lambda_1 = 0$ et que $c \neq 0$. Alors, par (3.0.4) et (3.0.5), nous pouvons faire une démarche semblable à celle qui a mené au cas $\lambda_1 = \lambda_2 = 0$ de (2.1.14) pour obtenir

$$L(s,\chi_0,\Gamma_c) = 1. \tag{3.0.7}$$

Supposons que $\lambda_1 \neq 0$ et que $c = 0$. Alors, par (3.0.4) et (3.0.5), nous pouvons faire une démarche semblable au cas $\lambda_1 \neq 0$ et $\lambda_2 = 0$ de l'équation (2.1.10) pour obtenir

$$L(s,\chi_{\lambda_1},\Gamma_0) = 1 - q^{-s}. \tag{3.0.8}$$

Il nous reste le cas $\lambda_1 \neq 0$ et $c \neq 0$. Servons-nous de la forme $L(s,\chi,\Gamma) = \sum_{m=0}^{\infty} \tau_m q^{-ms}$ en commençant par calculer les τ_m, pour $m \geq 0$.

Pour $m = 0$, nous avons que

$$\tau_0 = \chi(1)\Gamma(1) = 1.$$

Pour $m = 1$, nous avons que

$$\begin{aligned}\tau_1 &= \sum_{\deg M=1} \chi(M)\Gamma(M) \\ &= \sum_{a\in\mathbb{F}_q^*} \left(\frac{a^c}{q}\right)_{(3)} \psi(\lambda_1 a) \\ &= \left(\frac{\lambda_1^{-c}}{q}\right)_{(3)} \sum_{u\in\mathbb{F}_q^*} \left(\frac{u^c}{q}\right)_{(3)} \psi(u),\end{aligned}$$

où nous avons fait le changement de variable $u = \lambda_1 a$.

D'où

$$\tau_1 = \left(\frac{\lambda_1^{-c}}{q}\right)_{(3)} \sum_{a\in\mathbb{F}_q^*} \left(\frac{a^c}{q}\right)_{(3)} \psi(a) \tag{3.0.9}$$

Pour $m \geq 2$, nous avons que

$$\tau_m = \sum_{\deg M=m} \chi(M)\Gamma(M) = q^{m-2} \sum_{b_1\in\mathbb{F}_q} \psi(\lambda_1 b_1) \sum_{b_m\in\mathbb{F}_q^*} \left(\frac{b_m}{q}\right) = 0,$$

par (3.0.4) et (3.0.5).

Donc, notre fonction L dans ce cas vaut

$$L(s,\chi,\Gamma) = 1 + \tau_1 q^{-s}. \tag{3.0.10}$$

Nous allons calculer

$$\sum_{\chi,\Gamma} \chi(M)^{-1}\Gamma(M)^{-1} \log L(s,\chi,\Gamma) \tag{3.0.11}$$

de deux manières différentes.

En utilisant un raisonnement pratiquement identique à celui qui a mené aux équations (2.1.18) et (2.2.7), nous obtenons une première méthode de calcul :

$$(3.0.11) = 3q \sum_{n=1}^{\infty} \sum_{d|n} \frac{d}{n} v\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(3)}\right) q^{-sn}, \tag{3.0.12}$$

où $v\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(3)}\right)$ représente le nombre de polynômes irréductibles de degré d tels que $P^{\frac{n}{d}}$ est un polynôme ayant a_1 comme premier coefficient et la même cubicité que a_n.

Remarquons que $v\left(n, n, a_1, \left(\frac{a_n}{q}\right)_{(3)}\right) = H_n\left(a_1, \left(\frac{a_n}{q}\right)_{(3)}\right)$.

Pour la suite, servons-nous de (3.0.6) − (3.0.8) et de (3.0.10) pour séparer (3.0.11) de la façon suivante :

$$\begin{aligned}(3.0.11) &= \sum_{\lambda_1 \in \mathbb{F}_q} \sum_{c \in \{0,1,2\}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(3)} \log L(s, \chi, \Gamma) \\ &= \log L(s, \chi_0, \Gamma_0) + \sum_{c \neq 0} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \log L(s, \chi_0, \Gamma_c) \\ &\quad + \sum_{\lambda_1 \in \mathbb{F}_q^*} \psi(-\lambda_1 a_1) \log L(s, \chi_{\lambda_1}, \Gamma_0) \\ &\quad + \sum_{\lambda_1 \in \mathbb{F}_q^*, c \neq 0} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \psi(-\lambda_1 a_1) \log L(s, \chi_{\lambda_1}, \Gamma_c).\end{aligned}$$

Il est facile de voir que

$$\log L(s, \chi_0, \Gamma_0) = \sum_{n=1}^{\infty} \frac{q^{-sn}(q^n - 1)}{n}.$$

Pour $c \neq 0$,

$$\log L(s, \chi_0, \Gamma_c) = 0.$$

Pour $\lambda_1 \neq 0$,

$$\log L(s, \chi_{\lambda_1}, \Gamma_0) = -\sum_{n=1}^{\infty} \frac{q^{-sn}}{n}.$$

Enfin, pour $c \neq 0$ et $\lambda_1 \neq 0$,

$$\log L(s, \chi_{\lambda_1}, \Gamma_c) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} q^{-sn} \tau_1^n}{n}.$$

En mettant ces quatre résultats ensemble, nous obtenons

$$\begin{aligned}(3.0.11) &= \sum_{\lambda_1 \in \mathbb{F}_q} \sum_{c \in \{0,1,2\}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(3)} \log L(s, \chi, \Gamma) \\ &= \sum_{n=1}^{\infty} \frac{q^{-sn}}{n} \left(q^n - 1 - \sum_{\lambda_1 \in \mathbb{F}_q^*} \psi(-\lambda_1 a_1) + (-1)^{n-1} \sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \psi(-\lambda_1 a_1) \tau_1^n \right).\end{aligned}$$

En considérant séparément les cas $a_1 \neq 0$ et $a_1 = 0$, nous avons que l'équation (3.0.11) est égale à

$$\begin{cases} \sum_{n=1}^{\infty} \frac{q^{-sn}}{n} \left(q^n + (-1)^{n-1} \sum_{\lambda_1 \in \mathbb{F}_q^*, c \neq 0} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n \right) & a_1 \neq 0, \\ \sum_{n=1}^{\infty} \frac{q^{-sn}}{n} \left(q^n - q + (-1)^{n-1} \sum_{\lambda_1 \in \mathbb{F}_q^*, c \neq 0} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n \right) & a_1 = 0. \end{cases} \tag{3.0.13}$$

En mettant (3.0.12) et (3.0.13) ensemble, nous avons que

$$3q \sum_{d|n} dv\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(3)}\right) = \begin{cases} q^n + (-1)^{n-1} \sum_{\lambda_1 \in \mathbb{F}_q^*, c \neq 0} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n & a_1 \neq 0, \\ q^n - q + (-1)^{n-1} \sum_{\lambda_1 \in \mathbb{F}_q^*, c \neq 0} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n & a_1 = 0. \end{cases} \tag{3.0.14}$$

Il ne nous reste qu'à évaluer cette expression.

Utilisant la même notation que dans la Section 1.3.4, posons

$$\begin{aligned} G_b = G_b\left(\left(\frac{a}{q}\right)_{(3)}\right) &= \sum_{a \in \mathbb{F}_q} \left(\frac{a}{q}\right)_{(3)} \psi(ba) \\ \bar{G}_b = \bar{G}_b\left(\left(\frac{a^2}{q}\right)_{(3)}\right) &= \sum_{a \in \mathbb{F}_q} \left(\frac{a^2}{q}\right)_{(3)} \psi(ba), \end{aligned}$$

pour $b \in \mathbb{F}_q$ et avec $G_1 = G$ et $\bar{G}_1 = \bar{G}$.

Il est clair que

$$G_b = \left(\frac{b^2}{q}\right)_{(3)} G$$
$$\bar{G}_b = \left(\frac{b}{q}\right)_{(3)} \bar{G}.$$

En effet, si $b = 0$, le résultat est trivial. Si $b \neq 0$, alors le changement de variable $u = ba$ permet d'arriver au résultat.

De plus, nous avons que

$$\begin{aligned}
G\bar{G} &= \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\left(\frac{ab^2}{q}\right)_{(3)}\psi(a+b)\\
&= \sum_{a\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q^*}\left(\frac{ab^{-1}}{q}\right)_{(3)}\psi(a+b)\\
&= \sum_{u\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q^*}\left(\frac{u}{q}\right)_{(3)}\psi(b(u+1))\\
&= \left(\frac{-1}{q}\right)_{(3)}(q-1) + \sum_{u\neq -1}\left(\frac{u}{q}\right)_{(3)}\sum_{b\in\mathbb{F}_q^*}\psi(b(u+1))\\
&= \left(\frac{-1}{q}\right)_{(3)} q\\
&= q.
\end{aligned}$$

Ici, nous nous sommes servis du fait que $\left(\frac{b^{-1}}{q}\right)_{(3)} = \left(\frac{b^2}{q}\right)_{(3)}$ et nous avons fait le changement de variable $u = ab^{-1}$. Enfin, comme $p \equiv 1 \mod 3$, rappelons que $\left(\frac{-1}{q}\right)_{(3)} = 1$.

Puis, par la Proposition 1.3.4.1, nous avons que

$$G^3 = (-1)^{k-1}\left(\frac{ps \pm 3p|t|i\sqrt{3}}{2}\right)^k,$$

où s et $|t|$ sont des entiers relatifs entièrement déterminés par

$$4p = s^2 + 27t^2$$
$$s \equiv 1 \mod 3.$$

Donc, si nous résumons les propriétés de G_b :

$$G_b = \left(\frac{b^2}{q}\right)_{(3)} G, \tag{3.0.15}$$

$$\bar{G}_b = \left(\frac{b}{q}\right)_{(3)} \bar{G}, \tag{3.0.16}$$

$$G\bar{G} = q, \tag{3.0.17}$$

$$G^3 = (-1)^{k-1}\left(\frac{ps \pm 3p|t|i\sqrt{3}}{2}\right)^k, \tag{3.0.18}$$

$$\bar{G}^3 = (-1)^{k-1}\left(\frac{ps \mp 3p|t|i\sqrt{3}}{2}\right)^k, \tag{3.0.19}$$

où le changement de signe découle simplement du fait que $G^3\bar{G}^3 = q^3$.

Posons

$$\vartheta(s,t) = (-1)^{k-1}\left(\frac{ps \pm 3p|t|i\sqrt{3}}{2}\right)^k$$

$$\bar{\vartheta}(s,t) = (-1)^{k-1}\left(\frac{ps \mp 3p|t|i\sqrt{3}}{2}\right)^k.$$

Revenons maintenant à l'expression (3.0.14). Nous pouvons écrire τ_1 de cette manière :

$$\tau_1 = \left(\frac{\lambda_1^{-c}}{q}\right)_{(3)} \sum_{a\in\mathbb{F}_q} \left(\frac{a^c}{q}\right)_{(3)} \psi(a) = \begin{cases} \left(\frac{\lambda_1^2}{q}\right)_{(3)} G & c = 1, \\ \left(\frac{\lambda_1}{q}\right)_{(3)} \bar{G} & c = 2, \end{cases} \tag{3.0.20}$$

par l'équation (3.0.9)

Supposons que $a_1 \neq 0$.

Si $3|n$, alors

$$\begin{aligned} \sum_{\substack{\lambda_1\in\mathbb{F}_q^* \\ c\neq 0}} \psi(-\lambda_1 a_1)\left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n &= \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n}{3}} \sum_{\lambda_1\in\mathbb{F}_q^*} \psi(-\lambda_1 a_1) \\ &\quad + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n}{3}} \sum_{\lambda_1\in\mathbb{F}_q^*} \psi(-\lambda_1 a_1) \\ &= -\left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n}{3}} - \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n}{3}}, \end{aligned}$$

par (3.0.2) et (3.0.20).

Si $n \equiv 1 \mod 3$, alors

$$\begin{aligned}
\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n &= \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-1}{3}} G \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1^2}{q}\right)_{(3)} \psi(-\lambda_1 a_1) \\
&\quad + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-1}{3}} \bar{G} \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1}{q}\right)_{(3)} \psi(-\lambda_1 a_1) \\
&= \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-1}{3}} G\bar{G}_{-a_1} + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-1}{3}} \bar{G} G_{-a_1} \\
&= \left(\frac{a_1 a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-1}{3}} G\bar{G} + \left(\frac{a_1^2 a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-1}{3}} \bar{G} G \\
&= \left(\frac{a_1 a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-1}{3}} q + \left(\frac{a_1^2 a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-1}{3}} q \\
&= q \left(\left(\frac{a_1 a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-1}{3}} + \left(\frac{a_1^2 a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-1}{3}} \right),
\end{aligned}$$

où nous avons utilisé les propriétés $(3.0.15) - (3.0.17)$ et (3.0.20), et où nous avons utilisé le fait que $\left(\frac{-1}{q}\right)_3 = 1$.

Si $n \equiv 2 \mod 3$, alors, de manière similaire,

$$\begin{aligned}
\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n &= \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-2}{3}} G^2 \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1}{q}\right)_{(3)} \psi(-\lambda_1 a_1) \\
&\quad + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-2}{3}} \bar{G}^2 \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1^2}{q}\right)_{(3)} \psi(-\lambda_1 a_1) \\
&= \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-2}{3}} G^2 G_{-a_1} + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-2}{3}} \bar{G}^2 \bar{G}_{-a_1} \\
&= \left(\frac{a_1^2 a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-2}{3}} G^3 + \left(\frac{-a_1 a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-2}{3}} \bar{G}^3 \\
&= \left(\frac{a_1^2 a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n+1}{3}} + \left(\frac{a_1 a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n+1}{3}},
\end{aligned}$$

où nous avons utilisé les propriétés (3.0.15), (3.0.16) et (3.0.18) − (3.0.20), et où nous avons utilisé le fait que $\left(\frac{-1}{q}\right)_3 = 1$.

En mettant ces résultats ensemble, pour $a_1 \neq 0$ et par l'équation (3.0.14), nous avons que

$$\sum_{d|n} dv\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(3)}\right)$$

$$= \begin{cases} \frac{q^{n-1}}{3} + \frac{(-1)^n}{3q}\left(\left(\frac{a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n}{3}} + \left(\frac{a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n}{3}}\right) & 3|n, \\ \frac{q^{n-1}}{3} + \frac{(-1)^{n-1}}{3}\left(\left(\frac{a_1a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n-1}{3}} + \left(\frac{a_1^2a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n-1}{3}}\right) & n \equiv 1 \mod 3, \\ \frac{q^{n-1}}{3} + \frac{(-1)^{n-1}}{3q}\left(\left(\frac{a_1^2a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n+1}{3}} + \left(\frac{a_1a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n+1}{3}}\right) & n \equiv 2 \mod 3. \end{cases}$$

En utilisant la formule d'inversion de Möbius, nous arrivons au théorème.

Considérons maintenant le cas où $a_1 = 0$.

Si $3|n$, alors

$$\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n = \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n}{3}} \sum_{\lambda_1 \in \mathbb{F}_q^*} 1 + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n}{3}} \sum_{\lambda_1 \in \mathbb{F}_q^*} 1$$

$$= (q-1)\left(\left(\frac{a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n}{3}} + \left(\frac{a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n}{3}}\right),$$

par (3.0.20).

Si $n \equiv 1 \mod 3$, alors

$$\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n = \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-1}{3}} G \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1^2}{q}\right)_{(3)} + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-1}{3}} \bar{G} \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1}{q}\right)_{(3)}$$

$$= 0,$$

par le Lemme 1.3.1.2.

Si $n \equiv 2 \mod 3$, alors

$$\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(3)} \tau_1^n = \left(\frac{a_n^2}{q}\right)_{(3)} \vartheta(s,t)^{\frac{n-2}{3}} G^2 \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1}{q}\right)_{(3)} + \left(\frac{a_n}{q}\right)_{(3)} \bar{\vartheta}(s,t)^{\frac{n-2}{3}} \bar{G}^2 \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1^2}{q}\right)_{(3)}$$

$$= 0,$$

pour les mêmes raisons que le cas précédent.

Donc, en mettant ces résultats ensemble, pour $a_1 = 0$ et par l'équation (3.0.14), nous avons que

$$\sum_{d|n} dv\left(n, d, 0, \left(\frac{a_n}{q}\right)_{(3)}\right)$$

$$= \begin{cases} \frac{q^{n-1}-1}{3} + \frac{(-1)^{n-1}(q-1)}{3q}\left(\left(\frac{a_n^2}{q}\right)_{(3)}\vartheta(s,t)^{\frac{n}{3}} + \left(\frac{a_n}{q}\right)_{(3)}\bar{\vartheta}(s,t)^{\frac{n}{3}}\right) & 3|n, \\ \frac{q^{n-1}-1}{3} & 3 \nmid n. \end{cases}$$

En utilisant la formule d'inversion de Möbius, nous arrivons au théorème.

Chapitre 4

RÉSULTAT EN FIXANT LE PREMIER COEFFICIENT ET LA QUARTICITÉ DU DERNIER

Ce chapitre est très semblable au précédent. Soit M un polynôme dont les coefficients appartiennent à un corps fini quelconque $\mathbb{F}_q$ de caractéristique p :

$$M = x^n + a_1x^{n-1} + t_2x^{n-2} + t_3x^{n-3} + t_4x^{n-4} + \cdots + a_n. \tag{4.0.1}$$

Dans ce qui suit, nous allons supposer que $p \equiv 1 \mod 4$. De plus, nous demandons que le premier coefficient soit $a_1 \in \mathbb{F}_q$ et nous voulons aussi que le dernier coefficient ait la même quarticité que $a_n \in \mathbb{F}_q^*$. Nous dirons d'un tel polynôme qu'il est de la forme $\left(a_1, \left(\frac{a_n}{q}\right)_{(4)}\right)$. Soit $H_n\left(a_1, \left(\frac{a_n}{q}\right)_{(4)}\right)$ le nombre de tels polynômes irréductibles unitaires de degré n. Nous montrerons, toujours en se basant sur la méthode utilisée par Carlitz dans [**4**], le théorème suivant dans ce chapitre.

Théorème 4.0.1. *Soit $\mathbb{F}_q$ un corps de caractéristique p, avec $p \equiv 1 \mod 4$. Alors, nous avons que*

$$H_n\left(a_1, \left(\frac{a_n}{q}\right)_{(4)}\right) = \frac{1}{n}\sum_{\substack{d|n \\ p\nmid d}} \mu(d) f\left(\frac{n}{d}\right),$$

avec, pour $a_1 \neq 0$,

$$f(n)$$

$$= \begin{cases} \frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4q}\left(-\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n}{2}} - \left(\frac{a_n}{q}\right)q^{\frac{n}{2}} - \left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n}{2}}\right) & 4|n, \\ \frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4}\left(\left(\frac{a_1a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n-1}{2}} + \left(\frac{a_1a_n}{q}\right)q^{\frac{n-1}{2}} + \left(\frac{a_1^3a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n-1}{2}}\right) & n \equiv 1(4), \\ \frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4}\left((-1)^{k-1}\left(\frac{a_1^2a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n}{2}}q^{\frac{-1}{2}} - \left(\frac{a_n}{q}\right)q^{\frac{n}{2}-1} + (-1)^{k-1}\left(\frac{a_1^2a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n}{2}}q^{\frac{-1}{2}}\right) & n \equiv 2(4), \\ \frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4q}\left(\left(\frac{-a_1^3a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n+1}{2}} + \left(\frac{a_1a_n}{q}\right)q^{\frac{n+1}{2}} + \left(\frac{-a_1a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n+1}{2}}\right) & n \equiv 3(4), \end{cases}$$

et pour $a_1 = 0$,

$$f(n)$$

$$= \begin{cases} \frac{q^{n-1}-1}{4} + \frac{(-1)^{n-1}}{4q}\left((q-1)\left(\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n}{2}} + \left(\frac{a_n}{q}\right)q^{\frac{n}{2}} + \left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n}{2}}\right)\right) & 4|n, \\ \frac{q^{n-1}-1}{4} + \frac{(-1)^{n-1}(q-1)q^{\frac{n}{2}-1}}{4}\left(\frac{a_n}{q}\right) & n \equiv 2(4), \\ \frac{q^{n-1}-1}{4} & 2 \nmid n. \end{cases}$$

Nous définissons ϑ *et* $\bar{\vartheta}$ *de la manière suivante :*

$$\vartheta(c,d) = \sqrt{q}(c \pm |d|i)^k$$
$$\bar{\vartheta}(c,d) = \sqrt{q}(c \mp |d|i)^k.$$

Ici, c *et* $|d|$ *sont entièrement déterminés par les relations suivantes*

$$p = c^2 + d^2$$
$$c \equiv -1 \mod 4.$$

La première étape est de poser nos caractères. Dans ce cas-ci, nous utiliserons

$$\chi_{\lambda_1}(M) = \psi(\lambda_1 a_1),$$
$$\Gamma_c(M) = \begin{cases} 0 & a_n = 0, \\ \left(\frac{a_n^c}{q}\right)_{(4)} & a_n \neq 0, \end{cases}$$

pour $c \in \{0,1,2,3\}$.

Rappelons que, comme $p \equiv 1 \mod 4$, alors le Corollaire 1.2.1 et la démonstration du Théorème 1.3.5.1 permettent de montrer que

$$\left(\frac{a^2}{q}\right)_{(4)} = \left(\frac{\pm a}{q}\right) = \left(\frac{a}{q}\right).$$

Les étapes de la preuve sont similaires à celles du chapitre précédent. Tout d'abord, nous voyons que nous pouvons écrire

$$\sum_{\chi,\Gamma} \chi(M)^{-1}\Gamma(M)^{-1} \log L(s,\chi,\Gamma) = 4q \sum_{n=1}^{\infty} \sum_{d|n} \frac{d}{n} v\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(4)}\right) q^{-sn}.$$

De plus, les équations (3.0.6) – (3.0.8) et (3.0.10) restent valides pour le caractère multiplicatif quartique, et par conséquent

$$\sum_{\chi,\Gamma} \chi(M)^{-1}\Gamma(M)^{-1} \log L(s,\chi,\Gamma)$$

$$= \sum_{n=1}^{\infty} \frac{q^{-sn}}{n} \left(q^n - 1 - \sum_{\lambda_1 \in \mathbb{F}_q^*} \psi(-\lambda_1 a_1) + (-1)^{n-1} \sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(4)} \psi(-\lambda_1 a) \tau_1^n \right),$$

avec

$$\tau_1 = \sum_{a \in \mathbb{F}_q} \left(\frac{a^c}{q}\right)_{(4)} \psi(\lambda_1 a). \tag{4.0.2}$$

En mettant ces deux résultats ensemble, nous voyons que

$$4q \sum_{d|n} dv\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(4)}\right)$$

$$= q^n - 1 - \sum_{\lambda_1 \in \mathbb{F}_q^*} \psi(-\lambda_1 a_1) + (-1)^{n-1} \sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(4)} \psi(-\lambda_1 a) \tau_1^n. \tag{4.0.3}$$

Posons

$$G = \sum_{a \in \mathbb{F}_q} \left(\frac{a}{q}\right)_{(4)} \psi(a)$$

$$\bar{G} = \sum_{a \in \mathbb{F}_q} \left(\frac{a^3}{q}\right)_{(4)} \psi(a).$$

Par la Proposition 1.3.5.1, nous avons que

$$G^2 = \sqrt{q}(c \pm |d|i)^k,$$

où c et $|d|$ sont entièrement déterminés par les relations

$$p = c^2 + d^2$$
$$c \equiv -1 \mod 4.$$

De plus, nous avons que

$$\begin{aligned} G\bar{G} &= \sum_{a\in\mathbb{F}_q} \left(\frac{a}{q}\right)_{(4)} \psi(a) \sum_{b\in\mathbb{F}_q} \left(\frac{b^3}{q}\right)_{(4)} \psi(b) \\ &= \sum_{a,b\in\mathbb{F}_q} \left(\frac{ab^3}{q}\right)_{(4)} \psi(a+b) \\ &= \sum_{\substack{a\in\mathbb{F}_q \\ b\in\mathbb{F}_q^*}} \left(\frac{ab^{-1}}{q}\right)_{(4)} \psi(a+b) \\ &= \sum_{\substack{u\in\mathbb{F}_q \\ b\in\mathbb{F}_q^*}} \left(\frac{u}{q}\right)_{(4)} \psi(b(u+1)) \\ &= \left(\frac{-1}{q}\right)_{(4)} (q-1) + \sum_{u\neq -1} \left(\frac{u}{q}\right)_{(4)} \sum_{b\in\mathbb{F}_q^*} \psi(b(u+1)) \\ &= \left(\frac{-1}{q}\right)_{(4)} q, \end{aligned}$$

où nous nous sommes servis du fait que $\left(\frac{b^3}{q}\right)_{(4)} = \left(\frac{b^{-1}}{q}\right)_{(4)}$ et avons effectué le changement de variable $u = ab^{-1}$.

Alors,

$$G\bar{G} = \left(\frac{-1}{q}\right)_{(4)} q. \tag{4.0.4}$$

De plus, il est clair que

$$(G\bar{G})^2 = q^2,$$

d'où

$$\bar{G}^2 = \sqrt{q}(c \mp |d|i)^k,$$

avec les mêmes c et $|d|$ que pour G^2.

Posons, pour simplifier la notation,

$$G^2 = \sqrt{q}(c \pm |d|i)^k = \vartheta(c,d) \tag{4.0.5}$$

$$\bar{G}^2 = \sqrt{q}(c \mp |d|i)^k = \bar{\vartheta}(c,d). \tag{4.0.6}$$

En poursuivant, pour $\lambda_1 \neq 0$, nous avons que

$$\tau_1 = \sum_{a\in\mathbb{F}_q} \left(\frac{a^c}{q}\right)_{(4)} \psi(\lambda_1 a) = \left(\frac{\lambda_1^{-c}}{q}\right)_{(4)} \sum_{u\in\mathbb{F}_q} \left(\frac{u^c}{q}\right)_{(4)} \psi(u) = \begin{cases} \left(\frac{\lambda_1^3}{q}\right)_{(4)} G & c=1, \\ \left(\frac{\lambda_1}{q}\right) G_\psi(1) & c=2, \\ \left(\frac{\lambda_1}{q}\right)_{(4)} \bar{G} & c=3, \end{cases} \tag{4.0.7}$$

par l'équation (4.0.2) et où nous avons effectué par le changement de variable $u = \lambda_1 a$.

Supposons que $a_1 \neq 0$. Alors, par (4.0.3), nous avons que

$$4q \sum_{d|n} dv = q^n + (-1)^{n-1} \sum_{\substack{\lambda_1\in\mathbb{F}_q^* \\ c\neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1^n, \tag{4.0.8}$$

avec $v = v\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(4)}\right)$.

Dans ce qui suit, nous nous servirons de (4.0.4) – (4.0.7).

Supposons que $2|n$. Alors, nous avons que

$$\begin{aligned} \sum_{\substack{\lambda_1\in\mathbb{F}_q^* \\ c\neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1^n &= \left(\frac{a_n^3}{q}\right)_{(4)} G^n \sum_{\lambda_1\in\mathbb{F}_q^*} \left(\frac{\lambda_1^{3n}}{q}\right)_{(4)} \psi(-\lambda_1 a_1) \\ &\quad + \left(\frac{a_n^2}{q}\right)_{(4)} G_\psi(1)^n \sum_{\lambda_1\in\mathbb{F}_q^*} \psi(-\lambda_1 a_1) \\ &\quad + \left(\frac{a_n}{q}\right)_{(4)} \bar{G}^n \sum_{\lambda_1\in\mathbb{F}_q^*} \left(\frac{\lambda_1^n}{q}\right)_{(4)} \psi(-\lambda_1 a_1) \\ &= \left(\frac{a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n}{2}} \sum_{\lambda_1\in\mathbb{F}_q^*} \left(\frac{\lambda_1^{\frac{3n}{2}}}{q}\right) \psi(-\lambda_1 a_1) \end{aligned}$$

$$- \left(\frac{(-1)^{\frac{n}{2}} a_n}{q}\right) q^{\frac{n}{2}}$$
$$+ \left(\frac{a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n}{2}} \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1^{\frac{n}{2}}}{q}\right) \psi(-\lambda_1 a_1).$$

Maintenant, si $4|n$, alors $\frac{n}{2}$ est pair, et en se fiant à ces derniers calculs, nous avons que

$$\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1^n = - \left(\frac{a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n}{2}} - \left(\frac{a_n}{q}\right) q^{\frac{n}{2}} - \left(\frac{a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n}{2}}.$$

Supposons maintenant que $\frac{n}{2}$ est impair, c'est-à-dire que $n \equiv 2 \mod 4$. Alors, nous avons que

$$\begin{aligned}
\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1^n =& \left(\frac{a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n}{2}} \left(\frac{-a_1}{q}\right) G_\psi(1) - \left(\frac{(-1)^{\frac{n}{2}} a_n}{q}\right) q^{\frac{n}{2}} \\
&+ \left(\frac{a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n}{2}} \left(\frac{-a_1}{q}\right) G_\psi(1) \\
=&(-1)^{k-1} \left(\frac{a_n^3}{q}\right)_{(4)} \left(\frac{-a_1}{q}\right) \vartheta(c,d)^{\frac{n}{2}} \sqrt{q} - \left(\frac{(-1)^{\frac{n}{2}} a_n}{q}\right) q^{\frac{n}{2}} \\
&+ (-1)^{k-1} \left(\frac{a_n}{q}\right)_{(4)} \left(\frac{-a_1}{q}\right) \bar{\vartheta}(c,d)^{\frac{n}{2}} \sqrt{q} \\
=&(-1)^{k-1} \left(\frac{a_n^3}{q}\right)_{(4)} \left(\frac{a_1}{q}\right) \vartheta(c,d)^{\frac{n}{2}} \sqrt{q} - \left(\frac{a_n}{q}\right) q^{\frac{n}{2}} \\
&+ (-1)^{k-1} \left(\frac{a_n}{q}\right)_{(4)} \left(\frac{a_1}{q}\right) \bar{\vartheta}(c,d)^{\frac{n}{2}} \sqrt{q},
\end{aligned}$$

où $G_\psi(1) = (-1)^{k-1}\sqrt{q}$ et par le Corollaire 1.2.1, avec $p \equiv 1 \mod 4$.

Supposons que $n \equiv 1 \mod 4$. Alors, nous avons que

$$\begin{aligned}
\sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1^n =& \sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \psi(-\lambda_1 a_1) \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1 \tau_1^{n-1} \\
=& \left(\frac{a_n^3}{q}\right)_{(4)} G^{n-1} G \sum_{\lambda_1 \in \mathbb{F}_q^*} \left(\frac{\lambda_1^{3(n-1)}}{q}\right)_{(4)} \left(\frac{\lambda_1^3}{q}\right)_{(4)} \psi(-\lambda_1 a_1)
\end{aligned}$$

$$
\begin{aligned}
&+\left(\frac{a_n}{q}\right)G_\psi(1)^n\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{n-1}}{q}\right)\left(\frac{\lambda_1}{q}\right)\psi(-\lambda_1 a_1)\\
&+\left(\frac{a_n}{q}\right)_{(4)}\bar{G}^{n-1}\bar{G}\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{n-1}}{q}\right)_{(4)}\left(\frac{\lambda_1}{q}\right)_{(4)}\psi(-\lambda_1 a_1)\\
&=\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n-1}{2}}\left(\frac{-a_1}{q}\right)_{(4)}G\bar{G}+\left(\frac{-a_1a_n}{q}\right)G_\psi(1)^{n+1}\\
&+\left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n-1}{2}}\left(\frac{-a_1^3}{q}\right)_{(4)}\bar{G}G\\
&=\left(\frac{a_1a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n-1}{2}}q+\left(\frac{(-1)^{\frac{n+3}{2}}a_1a_n}{q}\right)q^{\frac{n+1}{2}}\\
&+\left(\frac{a_1^3a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n-1}{2}}q\\
&=\left(\frac{a_1a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n-1}{2}}q+\left(\frac{a_1a_n}{q}\right)q^{\frac{n+1}{2}}\\
&+\left(\frac{a_1^3a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n-1}{2}}q,
\end{aligned}
$$

où nous avons utilisé le Corollaire 1.2.1 et le fait que $\left(\frac{\lambda_1^{n-1}}{q}\right)_{(4)}=1$.

Supposons que $n\equiv 3 \mod 4$. Alors, nous avons que

$$
\begin{aligned}
\sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\psi(-\lambda_1a_1)\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^n&=\sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\psi(-\lambda_1a_1)\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^3\tau_1^{n-3}\\
&=\left(\frac{a_n^3}{q}\right)_{(4)}G^{n-3}G^3\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{3(n-3)}}{q}\right)_{(4)}\left(\frac{\lambda_1^9}{q}\right)_{(4)}\psi(-\lambda_1a_1)\\
&+\left(\frac{a_n}{q}\right)G_\psi(1)^n\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{n-3}}{q}\right)\left(\frac{\lambda_1^3}{q}\right)\psi(-\lambda_1a_1)\\
&+\left(\frac{a_n}{q}\right)_{(4)}\bar{G}^{n-3}\bar{G}^3\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{n-3}}{q}\right)_{(4)}\left(\frac{\lambda_1^3}{q}\right)_{(4)}\psi(-\lambda_1a_1)\\
&=\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n-1}{2}}G\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1}{q}\right)_{(4)}\psi(-\lambda_1a_1)\\
&+\left(\frac{-a_1a_n}{q}\right)G_\psi(1)^{n+1}\\
&+\left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n-1}{2}}\bar{G}\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^3}{q}\right)_{(4)}\psi(-\lambda_1a_1)
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\frac{-a_1^3 a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n-1}{2}} G^2 + \left(\frac{(-1)^{\frac{n+3}{2}} a_1 a_n}{q}\right) q^{\frac{n+1}{2}} \\
&\quad + \left(\frac{-a_1 a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n-1}{2}} \bar{G}^2 \\
&= \left(\frac{-a_1^3 a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n+1}{2}} + \left(\frac{(-1)^{\frac{n+3}{2}} a_1 a_n}{q}\right) q^{\frac{n+1}{2}} \\
&\quad + \left(\frac{-a_1 a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n+1}{2}} \\
&= \left(\frac{-a_1^3 a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n+1}{2}} + \left(\frac{a_1 a_n}{q}\right) q^{\frac{n+1}{2}} \\
&\quad + \left(\frac{-a_1 a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n+1}{2}},
\end{aligned}
$$

où encore une fois nous nous sommes servis du Corollaire 1.2.1 pour la dernière égalité.

En mettant tous ces résultats ensemble, nous avons, par l'équation (4.0.8), les résultats suivants :

$$\sum_{d|n} dv\left(n, d, a_1, \left(\frac{a_n}{q}\right)_{(4)}\right)$$

$$
= \begin{cases}
\frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4q}\left(-\left(\frac{a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n}{2}} - \left(\frac{a_n}{q}\right) q^{\frac{n}{2}} - \left(\frac{a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n}{2}}\right) & 4|n, \\
\frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4}\left(\left(\frac{a_1 a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n-1}{2}} + \left(\frac{a_1 a_n}{q}\right) q^{\frac{n-1}{2}} + \left(\frac{a_1^3 a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n-1}{2}}\right) & n \equiv 1(4), \\
\frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4}\left((-1)^{k-1}\left(\frac{a_1^2 a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n}{2}} q^{\frac{-1}{2}} - \left(\frac{a_n}{q}\right) q^{\frac{n}{2}-1} + (-1)^{k-1}\left(\frac{a_1^2 a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n}{2}} q^{\frac{-1}{2}}\right) & n \equiv 2(4), \\
\frac{q^{n-1}}{4} + \frac{(-1)^{n-1}}{4q}\left(\left(\frac{-a_1^3 a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n+1}{2}} + \left(\frac{a_1 a_n}{q}\right) q^{\frac{n+1}{2}} + \left(\frac{-a_1 a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n+1}{2}}\right) & n \equiv 3(4).
\end{cases}
$$

Nous arrivons au résultat par la formule d'inversion de Möbius.

Supposons maintenant que $a_1 = 0$. Nous avons que

$$
4q \sum_{d|n} dv\left(n, d, 0, \left(\frac{a_n}{q}\right)_{(4)}\right) = q^n - q + (-1)^{n-1} \sum_{\substack{\lambda_1 \in \mathbb{F}_q^* \\ c \neq 0}} \left(\frac{a_n^{-c}}{q}\right)_{(4)} \tau_1^n. \qquad (4.0.9)
$$

Supposons que $2|n$. Alors, nous avons que

$$\begin{aligned}\sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^n &= \left(\frac{a_n^3}{q}\right)_{(4)} G^n \sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{3n}}{q}\right)_{(4)} + \left(\frac{a_n^2}{q}\right)_{(4)} G_\psi(1)^n \sum_{\lambda_1\in\mathbb{F}_q^*} 1\\ &\quad + \left(\frac{a_n}{q}\right)_{(4)} \bar{G}^n \sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^n}{q}\right)_{(4)}\\ &= \left(\frac{a_n^3}{q}\right)_{(4)} \vartheta(c,d)^{\frac{n}{2}} \sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{\frac{n}{2}}}{q}\right) + \left(\frac{(-1)^{\frac{n}{2}}a_n}{q}\right)(q-1)q^{\frac{n}{2}}\\ &\quad + \left(\frac{a_n}{q}\right)_{(4)} \bar{\vartheta}(c,d)^{\frac{n}{2}} \sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{\frac{n}{2}}}{q}\right).\end{aligned}$$

Maintenant, si $4|n$, nous voyons que $\left(\frac{\lambda_1^{\frac{n}{2}}}{q}\right) = 1$ et que

$$\begin{aligned}\sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^n &= (q-1)\left(\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n}{2}} + \left(\frac{(-1)^{\frac{n}{2}}a_n}{q}\right)q^{\frac{n}{2}} + \left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n}{2}}\right)\\ &= (q-1)\left(\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n}{2}} + \left(\frac{a_n}{q}\right)q^{\frac{n}{2}} + \left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n}{2}}\right),\end{aligned}$$

par le Corollaire 1.2.1.

Si $n \equiv 2 \mod 4$, alors $\frac{n}{2}$ est impair et $\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{\frac{n}{2}}}{q}\right) = 0$, par le Lemme 1.3.1.1. Alors, par le Corollaire 1.2.1, nous avons que

$$\sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^n = \left(\frac{a_n}{q}\right)(q-1)q^{\frac{n}{2}}.$$

Supposons que $n \equiv 1 \mod 4$. Alors, nous avons que

$$\begin{aligned}\sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^n &= \sum_{\substack{\lambda_1\in\mathbb{F}_q^*\\ c\neq 0}}\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1\tau_1^{n-1}\\ &= \left(\frac{a_n^3}{q}\right)_{(4)} G^{n-1}G \sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{3(n-1)}}{q}\right)_{(4)}\left(\frac{\lambda_1^3}{q}\right)_{(4)}\\ &\quad + \left(\frac{a_n}{q}\right)G_\psi(1)^n \sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{n-1}}{q}\right)\left(\frac{\lambda_1}{q}\right)\end{aligned}$$

$$+\left(\frac{a_n}{q}\right)_{(4)}\bar{G}^{n-1}\bar{G}\sum_{\lambda_1\in\mathbb{F}_q^*}\left(\frac{\lambda_1^{n-1}}{q}\right)_{(4)}\left(\frac{\lambda_1}{q}\right)_{(4)}$$
$$=0,$$

par les Lemmes 1.3.1.1 et 1.3.1.2.

D'une façon similaire, si $n\equiv 3 \mod 4$, alors

$$\sum_{\lambda_1\in\mathbb{F}_q^*;c\neq 0}\left(\frac{a_n^{-c}}{q}\right)_{(4)}\tau_1^n=0.$$

Donc, par l'équation (4.0.9), nous avons que, pour $a_1=0$:

$$\sum_{d|n}dv\left(n,d,0,\left(\frac{a_n}{q}\right)_{(4)}\right)$$

$$=\begin{cases}\frac{q^{n-1}-1}{4}+\frac{(-1)^{n-1}}{4q}\left((q-1)\left(\left(\frac{a_n^3}{q}\right)_{(4)}\vartheta(c,d)^{\frac{n}{2}}+\left(\frac{a_n}{q}\right)q^{\frac{n}{2}}+\left(\frac{a_n}{q}\right)_{(4)}\bar{\vartheta}(c,d)^{\frac{n}{2}}\right)\right) & 4|n,\\ \frac{q^{n-1}-1}{4}+\frac{(-1)^{n-1}(q-1)q^{\frac{n}{2}-1}}{4}\left(\frac{a_n}{q}\right) & n\equiv 2(4),\\ \frac{q^{n-1}-1}{4} & 2\nmid n.\end{cases}$$

Nous arrivons au résultat par la formule d'inversion de Möbius.

CONCLUSION

Dans ce mémoire, quelques résultats concernant le dénombrement de polynômes irréductibles ont été prouvés. Nous avons suivi la méthode développée par Carlitz [**4**] qui, en posant un ou plusieurs caractères, utilise les sommes de Gauss pour arriver au résultat. Nous pouvons voir que cette méthode a ses limites, puisque si la condition est trop importante, les sommes de Gauss auront des termes polynômiaux de degré de plus en plus élevé, et nous devrons ainsi nous contenter de résultats approximatifs.

En effet, cette méthode fonctionne très bien dans le cas où nous fixons simplement le premier ou le deuxième coefficient, puisque les sommes de Gauss avec des termes linéaires et quadratiques sont données par des formules fermées. D'ailleurs, Kuz'min a employé dans [**9**] cette méthode afin de trouver une formule fermée pour le cas où les deux premiers coefficients sont fixés. Déjà, en fixant les trois premiers coefficients, le résultat asymptotique qui est démontré à la Section 2 du Chapitre 2 représente à ce jour le meilleur de ce qui peut être tiré de cette méthode.

Pour ce qui est des deux derniers théorèmes, nous devons rappeler que Gauss (voir [**2**]) a mis quatre ans à résoudre le signe de

$$G_\psi(1) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) e^{\frac{2\pi i n}{p}}.$$

Depuis, plusieurs types de sommations ont été étudiées, dont

$$\sum_{n=0}^{p-1} \left(\frac{n}{p}\right)_{(3)} e^{\frac{2\pi i n}{p}}$$

et

$$\sum_{n=0}^{p-1} \left(\frac{n}{p}\right)_{(4)} e^{\frac{2\pi i n}{p}}.$$

Aujourd'hui, nous connaissons le cube de la première expression et le carré de la deuxième à un signe près, d'où l'ambiguité avec un signe dans les Théorèmes 3.0.1 et 4.0.1. Enfin, pour trouver d'autres expressions exactes du nombre de polynômes irréductibles avec cette méthode, nous devons approfondir nos recherches dans la détermination de sommes de Gauss avec des termes polynomiaux de degré supérieur ou égal à 3.

Bibliographie

[1] Berndt, Bruce C ; Evans, Ronald J, "Sums of Gauss, Jacobi, and Jacobsthal", Journal of number theory 11, p. 349-398 (1979).

[2] Berndt, Bruce C ; Evans, Ronald J, "The determination of Gauss sums", Bulletin of the American Mathematical Society, Volume 5, Number 2, September 1981

[3] Car, Mireille, "Distribution des polynômes irréductibles dans $\mathbb{F}_q[T]$", Acta Arith. 88 (1999) 141-153.

[4] Carlitz, L., "A theorem of Dickson on irreducible polynomials", Proc.Amer.Math.Soc., April 26, 1952.

[5] Cohen, Stephen D., "Explicit theorems on generator polynomials", Finite fields and their applications, University of Glasgow, December 2004, p. 337-357

[6] Hayes, D.R., "The distribution of irreducibles in GF[q,x]", Trans. Amer. Math. Soc. 117 (1965) 101-127

[7] Ireland, Kenneth ; Rosen, Michael, "A classical introduction to modern number theory",Second Edition, Springer(1998)

[8] Kuz'min, E.N., "On irreducible polynomials over finite fields. (Russian) Sibirsk. Mat. Zh. 30 (1989), no. 6, 98-109 ; translation in Siberian Math. J.

[9] Kuz'min, E.N., "A class of irreducible polynomials over a finite field. (Russian) Dokl. Akad. Nauk SSSR 313 (1990), no.3, 552-555 ; translation in Soviet Math. Dokl. 42 (1991), no.1, 45-48

[10] Kuz'min, E.N., "Irreducible polynomials over finite fields. I", Algebra and Logic, Vol. 33 (1994), No. 4, 216-232

[11] Lidl, Rudolf ; Niederreiter, Harald, "Encyclopedia of Mathematics and its applications : Finite fields", edited by G.-C. Rota, Volume 20 (1983)