Sommes de Gauss

Malo Cossec et Léo Théodon

Université de Rennes 1

TER supervisé par Christophe Mourougane

Mardi, 27st Avril 2009

Table des matières

Introduction

Introduction

Dans le cadre de notre Master de Mathématiques Fondamentales à l'université de Rennes 1, un travail d'étude et de recherche nous a été demandé. Plusieurs thèmes nous étaient proposés, et nous avons opté pour un sujet d'arithmétique sous la direction de Christophe Mourougane : « Les Sommes de Gauss ».
Nous avons commencé nos recherches par l'étude d'un document fourni par notre tuteur, puis nous nous sommes rapidement appuyés sur quelques livres consultés à la bibliothèque universitaire de Beaulieu. Nous avons rencontré certaines difficultés à poser les limites de notre étude et à concrétiser l'outil des Sommes de Gauss proprement dites. Après plusieurs réflexions sur les méthodes et les démonstrations nous nous sommes familiarisé avec notre sujet. Ensuite la recherche d'une application intéressante a fait l'objet de notre préoccupation, car nous voulions trouver quelque chose de concret lié à la géométrie. En mathématiques, et plus précisément en arithmétique modulaire, la somme de Gauss est un nombre complexe. Elle utilise les outils de l'analyse harmonique sur un groupe abélien fini sur le corps fini $\mathbb{Z}/p\mathbb{Z}$ où p désigne un nombre premier impair et $\mathbb{Z}$ l'ensemble des entiers relatifs. Elles sont introduites par le mathématicien Carl Friedrich Gauss, dont nous feront une brève biographie, qui les utilise dans ses Disquisitiones Arithmeticae, parues en 1801. Ces sommes sont utilisées pour établir la théorie des polynômes cyclotomiques et possèdent de nombreuses applications. On peut citer par exemple une démonstration de la loi de réciprocité quadratique que nous détaillerons par la suite. Nous avons donc choisi de commencer notre travail par certains rappels et résultats importants d'arithmétique et de théorie des nombres, puis nous parlerons des sommes de Gauss en étudiant leurs propriétés et les théorèmes les plus connus. Et nous terminerons par l'analyse de quelques applications.

Biographie de Carl Friedrich Gauss

Biographie de Carl Friedrich Gauss

Carl Friedrich Gauss est né le 30 avril 1777 à Brunswick. Il était, aux yeux de tous, un enfant prodige des mathématiques. Il a également appris à compter et à lire seul à l'âge de 3 ans. Le duc de Brunswick a reconnu ses aptitudes et lui accorda une bourse, en 1792, pour qu'il puisse poursuivre son instruction.

Lorsqu'il était jeune, Gauss s'intéressait beaucoup aux langues anciennes. Vers l'âge de 17 ans, il eut la piqûre pour les mathématiques. Ses premiers travaux ont porté sur la géométrie. Sachant qu'il était doué dans cette matière, il abandonna définitivement l'étude des langues anciennes pour s'attaquer aux mathématiques. Il a fréquenté le Collège de Caroline de 1792 à 1795 et il a formulé la méthode des moindres carrés et la conjoncture sur la répartition des nombres premiers. Par la suite, il a étudié, de 1795 à 1798, à l'Université de Göttingen. Il est très important de savoir qu'en 1807, il fut nommé professeur de mathématiques et qu'il a été directeur de l'observatoire de Göttingen jusqu'à sa mort, le 23 février 1855.

Un élève en mathématique rencontra Gauss alors qu'il avait 80 ans et le décrivit comme suit : «Un homme vénérable, distingué avec l'expression d'un homme heureux. Son aspect et chacun de ses mots dégageaient une extraordinaire impression de puissance. Il avait environ 80 ans, mais on n'apercevait aucune trace de vieillesse.»

Durant sa vie de mathématicien, il s'intéressa également l'astronomie et la physique. Du côté des mathématiques, il toucha un peu à tout : les probabilités, la géométrie, l'algèbre et la théorie des nombres. Dans le domaine de la probabilité, il attacha son nom à la loi normale, aussi appelée la loi de Laplace-Gauss, qui a pour but la répartition de la courbe en cloche. Lorsqu'il pratiquait l'algèbre, il fit une première démonstration du théorème fondamental. Il a d'ailleurs remporté le titre de docteur pour cette démonstration, en 1799, à l'Université de Helmstedt. En 1801, il développa un intérêt pour l'astronomie. Il s'est amusé à trouver la trajectoire de l'astéroïde Cérès qu'il avait aperçu en 1801.

Il a entrepris également des travaux en physique à partir de 1829. Il s'intéressa au domaine du magnétisme terrestre et à l'électricité. Une unité d'induction magnétique porte aujourd'hui son nom. À 24 ans, Gauss publia une théorie qui se nomme Disquisitiones arithmeticae et qui a pour thème la théorie des nombres. Cette théorie fut l'un des travaux les plus remarquables dans l'histoire des mathématiques.

Il a inventé un instrument utilisé en géodésie, en 1820, qui se nomme l'héliotrope. Il a pour but de refléter les rayons du soleil à l'aide d'un miroir mobile. En 1833, il inventa et construisit le premier télégraphe.

1 Rappels et Généralités

Dans cette partie, nous exposerons les résultats classiques d'arithmétiques, généralement connu de tous, qui seront pour la plupart utiles dans la suite. Nous effectuerons en particuliers quelques rappels sur les groupes finis et les groupes $(\mathbb{Z}/m\mathbb{Z})^*$ ainsi que $\mathbb{F}_q$ que nous définirons. Nous rappellerons également la définition du symbole de Legendre ainsi que quelques propriétés élémentaires, conduisant à l'établissement de la loi de réciprocité quadratique.

Notations Si X est un ensemble fini, on note $\sharp X$ ou encore $Card(X)$ le nombre d'éléments de X. On note $\mathbb{N}$ (respectivement $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$) l'ensemble des nombres naturels (respectivement entiers relatifs, nombres rationnels, nombres réels et nombres complexes).

1.1 Les groupes finis et les groupes $(\mathbb{Z}/m\mathbb{Z})^*$ et $\mathbb{F}_q$

Soit $\mathbb{K}$ un corps. L'image de $\mathbb{Z}$ dans $\mathbb{K}$ par un morphisme d'anneau est un anneau intègre, donc isomorphe à $\mathbb{Z}$, ou à $\mathbb{Z}/p\mathbb{Z}$, avec p premier. Son corps des fractions est isomorphe à $\mathbb{Q}$ ou à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Dans le premier cas, on dit que $\mathbb{K}$ est de caractéristique 0, et dans le second cas, que $\mathbb{K}$ est de caractéristique p. On a alors que $p = n$, où n est le plus petit entier plus grand que 1 tel que $n.1_{\mathbf{K}} = 0$ dans $\mathbb{K}$.

Remarque: La caractéristique d'un corps fini $\mathbb{K}$ est donc nécessairement un nombre premier.

Nous allons montrer maintenant quelques propriétés sur les corps fini à l'aide d'un premier théorème. Pour cela, nous aurons besoin du lemme suivant.

Lemme 1.1. *Si $\mathbb{K}$ est de caractéristique $p > 0$, l'application $\sigma : x \mapsto x^p$ est un isomorphisme de $\mathbb{K}$.*

Preuve. *On a $\sigma(x.y) = \sigma(x).\sigma(y)$. De plus, le coefficient binomial C_p^k est congru à 0 modulo p si $1 < k < p$. On en déduit que $\sigma(x+y) = \sigma(x)+\sigma(y)$, donc σ est un morphisme d'anneau. Enfin, σ est injective, car $\mathbb{K}$ est un corps, et surjective. Ainsi, σ est bien un isomorphisme.*

Théorème 1.1. *Sur les corps finis.*

1. *La caractéristique d'un corps fini $\mathbb{K}$ est un nombre premier $p \neq 0$. Si $f = [\mathbb{K}:\mathbb{F}_p]$, le nombre d'éléments de $\mathbb{K}$ est $q = p^f$.*
2. *Soit p un nombre premier et soit $q = p^f, f \geq 1$, une puissance de p. Soit Ω un corps algébriquement clos de caractéristique p. Il existe un sous-corps $\mathbb{F}_q$ de Ω et un seul de cardinal égal à q. C'est l'ensemble des racines du polynôme $X^q - X$.*
3. *Tout corps fini à $q = p^f$ éléments est isomorphe à $\mathbb{F}_q$.*

Démonstration. *Soit $\mathbb{K}$ un corps fini.*
Il vient alors que $\mathbb{K}$ ne contient pas le corps $\mathbb{Q}$. Sa caractéristique est donc un nombre premier que l'on note p. Notons maintenant f le degré de l'extension $\mathbb{K}/\mathbb{F}_p$. Il vient alors que $Card(\mathbb{K}) = p^f$, d'où 1., $\mathbb{K}$étant un $\mathbb{F}_p$-espace vectoriel de dimension f.
De plus, si Ω est algébriquement clos de caractéristique p, on a d'après le lemme précédent que l'application $\tilde{\sigma} : x \mapsto s^q$ (avec $q = p^f, f \geq 1$) est un automorphisme de Ω. En effet, il s'agit de la puissance f-ième de l'automorphisme $\sigma : x \mapsto x^p$ (σ étant bien surjectif, Ω

étant algébriquement clos). Les éléments $x \in \Omega$ invariants par $\tilde{\sigma}$ forment donc un sous-corps $\mathbb{F}_q$ de Ω. Ce corps a q éléments.
En effet, la dérivée du polynôme $X^q - X$ est

$$qX^{q-1} - 1 = p.p^{f-1}.X^{q-1} - 1 = -1$$

et ne s'annule donc pas. Il est résulte (puisque Ω est algébriquement clos) que $X^q - X$ a q racines distinctes car il est alors séparable. On a donc bien $Card(\mathbb{F}_q) = q$.
Inversement, si $\mathbb{K}$ est un sous-corps de Ω à q éléments, le groupe multiplicatif $\mathbb{K}^*$ des éléments non-nuls de $\mathbb{K}$ a $q-1$ éléments. On a donc $x^{q-1} = 1$ si $x \in \mathbb{K}^*$, d'où $x^q = x$ si $x \in \mathbb{K}^*$, ce qui montre que $\mathbb{K}$ est contenu dans $\mathbb{K}_q$. Puisque

$$Card(\mathbb{K}) = Card(\mathbb{F}_q)$$

on a $\mathbb{K}$=$\mathbb{F}_q$, et l'assertion 2. est bien vérifiée.

Enfin, l'assertion 3. résulte de 2. et du fait que tout corps à p^f éléments peut être plongé dans Ω puisque ce dernier est algébriquement clos.

Soit p un nombre premier, $f \geq 1$ un entier et soit $q = p^f$.

Théorème 1.2. *Le groupe multiplicatif $\mathbb{F}_q^*$ du corps fini $\mathbb{F}_q$ est cyclique d'ordre $q-1$.*

Démonstration. *Si d est un entier supérieur ou égal à 1, on note $\varphi(d)$ l'**indicateur d'Euler** de d, c'est à dire le nombre d'entiers x, avec $1 \leq x \leq q$, qui sont premiers à q, autrement dit, dont l'image dans $\mathbb{Z}/d\mathbb{Z}$ est un générateur de ce groupe.*
Il est clair que le nombre des générateurs d'un groupe cyclique d'ordre q est égal à $\varphi(d)$.

Il nous reste à présent à montrer que dans notre cas, $\varphi(d) = q - 1$. Pour cela, nous allons faire appel à deux lemmes.

Lemme 1.2. *Si n est un entier, $n \geq 1$, alors on a $n = \sum_{d|n} \varphi(d)$.*

On rappelle que la notation $d \mid n$ signifie que d divise n.

Preuve. *Si d divise n, soit C_d l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre q, et soit Φ_d l'ensemble des générateurs de C_d. Comme tout élément de $\mathbb{Z}/n\mathbb{Z}$ engendre l'un des C_d, le groupe $\mathbb{Z}/n\mathbb{Z}$ est r"union disjointe des Φ_d et l'on a :*

$$n = Card(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} Card(\Phi_d) = \sum_{d|n} \varphi(d)$$

D'où le résultat.

Lemme 1.3. *Soit H un groupe d'ordre fini noté n. On suppose que, pour tout diviseur d de n, l'ensemble des $x \in H$ tels que $x^d = 1$ a au plus d éléments. Alors H est cyclique.*

Preuve. *Soit d un diviseur de n.*
S'il existe $x \in H$ d'ordre d, le sous-groupe $(x) = \{1, x, ..., x^{d-1}\}$ engendré par x est d'ordre d. par hypothèse, tout élément $y \in H$ tel que $y^d = 1$ appartient à (x). En particulier, les seuls éléments de H d'ordre d sont les générateurs de (x), et ceux-ci sont en nombre $\varphi(d)$. Ainsi, le nombre d'éléments de H d'ordre d est 0 ou $\varphi(d)$. Si cela était 0 pour une certaine valeur de d, la formule $n = \sum_{d|n} \varphi(d)$ montrerait que le nombre d'éléments de H est strictement inférieur à n, ce qui entre en contradiction avec l'hypothèse de départ. En particulier, il existe un élément $x \in H$ d'ordre n, et H coïncide avec le groupe cyclique (x).

Le théorème résulte du dernier lemme, appliqué à $H = \mathbb{F}_q^*$ et $n = q - 1$. Il est en effet immédiat que l'équation $x^d = 1$, de degré d, a au plus d solutions dans $\mathbb{F}_q$.

Remarque: La démonstration ci-dessus montre que, plus généralement, tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

1.2 Le symbole de Legendre

Dans cette partie, nous introduirons le symbole de Legendre, et donnerons quelques exemple qui nous permettrons de mieux comprendre la loi de réciprocité quadratique que nous étudierons dans la partie suivante.

1.2.1 Symbole de Legendre

Soit m et n des entiers supérieurs ou égaux à 1. On dit que m est un résidu quadratique modulo n si $m + n\mathbb{Z}$ est un carré dans $\mathbb{Z}/n\mathbb{Z}$, autrement dit, s'il existe $a\ in\mathbb{Z}$ tel que l'on ait

$$m \equiv a^2 \, mod \, n$$

. Dans ce cas, on dit aussi que m est un carré modulo n.

Définition 1.1. *Soient p un nombre premier et n un entier relatif. On note $\left(\frac{n}{p}\right)$ l'entier défini comme suit. On a :*

1. $\left(\frac{n}{p}\right) = 0$ *si p divise n.*
2. $\left(\frac{n}{p}\right) = 1$ *si p ne divise pas n et si n est un résidu quadratique modulo p.*
3. $\left(\frac{n}{p}\right) = -1$ *si n n'est pas un résidu quadratique modulo p.*

L'expression $\left(\frac{n}{p}\right)$ s'appelle le symbole de Legendre. l'entier $\left(\frac{n}{p}\right)$ ne dépend que de la classe de n modulo p.

Exemple 1.1. *Étudions les deux cas suivants :*

1. *On a $\left(\frac{n}{2}\right)$ si n est impair et $\left(\frac{n}{2}\right) = 0$ si n est pair. On a ainsi $\left(\frac{n}{2}\right) \equiv n \, mod \, 2$.*
2. *Vérifions la congruence*

$$\left(\frac{n}{3}\right) \equiv n \, mod \, 3.$$

Si 3 divise n, on a $\left(\frac{n}{3}\right) = 0$. Si $n \equiv 1 \, mod \, 3$, on a $\left(\frac{n}{3}\right) = 1$. Si $n \equiv -1 \, mod \, 3$, et comme -1 n'est pas un carré modulo 3, on obtient $\left(\frac{n}{3}\right) = \left(\frac{-1}{3}\right) = -1$, d'où la formule annoncée.

Proposition 1.1. *Soit p un nombre premier impair. On a :*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{1}$$

Ainsi, -1 est un carré modulo p si et seulement si on a $p \equiv 1 \, mod \, 4$.

Preuve. *Supposons $\left(\frac{-1}{p}\right) = 1$. Il existe $n \in \mathbb{Z}$ tel que l'on ait $-1 \equiv n^2 mod p$. Le sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ engendré par la classe de n est d'ordre 4, d'où $p \equiv 1 \, mod \, 4$. Inversement, si 4 divise $p - 1$, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ étant cyclique, il possède un sous-groupe cyclique d'ordre 4. Si x est un générateur de ce sous-groupe, on a $x^2 = -1$, d'où $\left(\frac{-1}{p}\right) = 1$. par suite, on a $\left(\frac{-1}{p}\right) = 1$ si et seulement si p est congru à 1 modulo 4, ce qui entraîne l'équation (1).*

1.2.2 Le critère d'Euler

Le critère d'Euler est une relation qui permet de calculer effectivement le symbole de Legendre. De plus, il nous sera très utile dans la démonstration de la loi de réciprocité quadratique faisant appel aux sommes de Gauss.

Théorème 1.3. *Critère d'Euler Soit p un nombre premier impair. On a alors que pour tout entier relatif n la relation suivante :*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \, mod \, p \tag{2}$$

Démonstration. *Nous allons commencer par établir le lemme suivant :*

Lemme 1.4. *Soit p un nombre premier impair. L'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $\frac{p-1}{2}$.*

Preuve. *L'application $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ qui à x associe x^2 est un morphisme de groupes. son noyau est $\{\pm 1\}$. Il est d'ordre 2 car $p \neq 2$. l'image de ce morphisme, qui est le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$, est donc d'ordre $\frac{p-1}{2}$.*

Le théorème 1.3 se déduit comme suit. Soit n un entier relatif. La congruence (2) est vraie si p divise n. Supposons que p ne divise pas n. on a $n^{p-1} \equiv 1 mod p$. Puisque $\mathbb{Z}/p\mathbb{Z}$est un corps, on a donc

$$n^{\frac{p-1}{2}} \equiv \pm 1 \, mod \, p. \tag{3}$$

Par ailleurs, le polynôme $X^{\frac{p-1}{2}} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ a au plus $\frac{p-1}{2}$ racines. On déduit du lemme 1.4 que ses racines sont exactement les $\frac{p-1}{2}$ carrées de $(\mathbb{Z}/p\mathbb{Z})^*$. On obtient l'équivalence

$$\left(\frac{n}{p}\right) = 1 \Longleftrightarrow n^{\frac{p-1}{2}} \equiv \pm 1 \, mod \, p.$$

La condition (3) permet alors de conclure.

Remarque 1.1. *Soit p un nombre premier impair. Parmi les entiers compris entre 1 et $p-1$, il y en a exactement la moitié qui sont des résidus quadratiques modulo p, c'est à dire qu'il y a autant de carrés que de non-carrés dans $(\mathbb{F}p)^*$) (voir lemme 1.4). On a donc la formule*

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0. \tag{4}$$

Exemple 1.2. *Le critère d'Euler permet de calculer $\left(\frac{n}{p}\right)$ en utilisant le calcul « rapide »de la puissance d'un entier. Par exemple, on obtient que*

$$\left(\frac{5}{23}\right) = -1$$

en écrivant que l'on a

$$11 = 2^3 + 2 + 1 \; puis \; 5^{11} = 5^{2^3} \times 5^2 \times 5 \equiv -1 \, mod \, 23.$$

Corollaire. *Soit p un nombre premier. Quels que soient les entiers m et n, on a*

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{5}$$

De plus, si n n'est pas divisible par p, on a

$$\left(\frac{mn^2}{p}\right) = \left(\frac{m}{p}\right) \tag{6}$$

Preuve. *Si $p = 2$, l'égalité (5) provient du fait que mn est pair si et seulement si m ou n l'est. Si $p \neq 2$, elle se déduit du critère d'Euler. Quant à l'égalité (6), elle résulte de (5) et de la définition du symbole de Legendre.*

Remarque 1.2. *On peut déduire de la formule (5) l'énoncé suivant :*

Proposition 1.2. *Soit p un nombre premier impair. soit n le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p. On a*

$$n < 1 + \sqrt{p}.$$

Preuve. *Soit m le plus petit entier naturel tel que $mn > p$. Puisque p est premier, on a donc $n(m-1) < p$, c'est à dire que $mn - p < n$. D'après le caractère minimal de n, on a donc d'après la formule (5) les égalités*

$$1 = \left(\frac{mn-p}{p}\right) = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = -\left(\frac{m}{p}\right)$$

.

Par suite, on a $m \geq n$. On obtient donc le résultat voulu puisque l'on a

$$(n-1)^2 < n(n-1) \leq n(m-1) < p.$$

On peut d'ailleurs à ce propos citer la conjecture suivante que l'on doit à Vinogradov :

Conjecture. *Soit ε un nombre réel strictement positif. Pour tout nombre premier p assez grand, le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p est inférieur à p^{ε}.*

Par exemple, Hudson et Williams ont démontré en 1979 que si p est un nombre premier impair non congru à 1 modulo 8 le plus petit entier naturel n qui ne soit pas un résidu quadratique modulo p est inférieur à $p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33$. On a ainsi $n < 1,54p^{\frac{2}{5}}$ dès que p (non congru à 1 modulo 8) est plus grand que 10^7.

1.2.3 Le symbole $\left(\frac{2}{p}\right)$

Dans cette partie, nous allons étudier le cas particulier $\left(\frac{2}{p}\right)$.

Proposition 1.3. *Soit p un nombre premier impair. On a*

$$\left(\frac{2}{p}\right) = (-1)^{(\frac{p^2-1}{8})} \tag{7}$$

Ainsi, 2 est un carré modulo p si et seulement si on a $p \equiv \mp 1 mod\, 8$.

Preuve. *Posons*

$$S = \{1, ..., \frac{p-1}{2}\}.$$

Étant donné $a \in \mathbb{Z}$ *non divisible par* p*, pour tout* $s \in S$*, il existe un unique élément* $s_a \in S$*, tel que l'on ait*

$$as \equiv e_s(a).s_a \, mod\, p \; avec \; e_s(a) = \pm 1.$$

Nous allons maintenant avoir besoin du lemme suivant.

Lemme 1.5 (Gauss)**.** *Soit* a *un entier relatif non divisible par* p*. On a*

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a).$$

Preuve. *Vérifions que l'application* $f : S \to S$ *définie par* $f(s) = s_a$ *est une bijection de* S*. Soient* s *et* s' *des éléments de* S *tels que* $f(s) = f(s')$*. On obtient* $e_s(a)s = e_{s'}(a)s' \, mod\, p$*, d'où* $s \equiv \pm s' \, mod\, p$*, ce qui implique* $s = s'$*. Par suite,* f *est injective, donc bijective. il en résulte que l'on a*

$$a^{\frac{p-1}{2}} \prod_{s \in S} s = \prod_{s \in S} (as) \equiv \prod_{s \in S} e_s(a) \prod_{s \in S} s_a \, mod\, p,$$

d'où

$$a^{\frac{p-1}{2}} \prod_{s \in S} s \equiv \prod_{s \in S} e_s(a) \prod_{s \in S} s \, mod\, p,$$

puis la congruence

$$a^{\frac{p-1}{2}} \equiv \prod_{s \in S} e_s(a) \, mod\, p.$$

D'après le critère d'Euler, on obtient ainsi

$$\prod_{s \in S} e_s(a) \equiv \frac{a}{p} \, mod\, p,$$

d'où le résultat, car les deux membres de cette congruence valent ± 1 *et* p *est impair.*

La proposition se déduit de la façon suivante. On utilise le lemme précédent avec $a = 2$*. Pour tout* $s \in S$*, on a*

$$e_s(2) = 1 \; si \; 2s \in S \; et \; e_s(2) = -1 \; sinon.$$

On a ensuite

$$\left(\frac{2}{p}\right) = (-1)^{n(p)},$$

où $n(p)$ *est le nombre d'entiers* u *tels que*

$$\frac{p-1}{4} < u < \frac{p-1}{2}.$$

Supposons $p \equiv \pm 1 \, mod\, 8$*. On a* $p = \pm 1 + 8k$ *où* $k \in \mathbb{N}$*, et l'on vérifie que* $n(p) = 2k$*. Si l'on a* $p = 3 + 8k$ *où* $k \in \mathbb{N}$*, on obtient* $n(p) = 2k + 1$*. Si* $p = -3 + 8k$ *où* $k \in \mathbb{N}$*, on a* $n(p) = 2k - 1$*. Cela conduit à la formule (7), et achève la preuve de la proposition.*

Exemple 1.3. *Démontrons qu'il existe une infinité de nombres premiers congrus à 7 modulo 8. Supposons le contraire. Soit $\{p_1, ..., p_n\}$ l'ensemble des nombres premiers congrus à 7 modulo 8. Posons*

$$N = (4p_1...p_n)^2 - 2.$$

Soit p un diviseur impair de N. On a $2 \equiv (4p_1...p_n)^2 \, mod p$, donc 2 est un carré modulo p. Ainsi, on a $p \equiv \pm 1 \, mod \, 8$ (d'après la propriété précédente). Compte tenu du fait que

$$\frac{N}{2} = 8(p_1...p_n)^2 - 1,$$

il existe donc un diviseur premier p de N qui est congru à -1 modulo 8. Ainsi, q est l'un des p_i, ce qui conduit à une contradiction. D'où le résultat.

Exemple 1.4. *Soit p un nombre premier. Supposons que p soit de la forme*

$$p = 1 + 4q \text{ avec } q \text{ premier.}$$

Vérifions que la classe de 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit d l'ordre multiplicatif de 2 modulo p. Puisque q est premier, on a $d \in \{1, 2, 4, q, 2q, 4q\}$. Oon a $p \neq 3$ et $p \neq 5$, d'où $q = q$, $2q$ ou $4q$. Supposons $d \neq 4q$. Dans ce cas, on obtient la congruence

$$2^{\frac{p-1}{2}} \equiv 1 \, mod \, p.$$

D'après le critère d'Euleur, 2 est donc un résidu quadratique modulo p. Cela conduit à une contradiction, étant donné que p est congru à 5 modulo 8.

1.3 La loi de réciprocité quadratique

Cette loi a été conjecturée par Euler en 1783, et a été démontrée par Gauss en 1796.

Théorème 1.4 (Gauss)**.** *Soient p et q deux nombres premiers impairs distincts. On a*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Autrement dit, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ si p ou q est congru à 1 modulo 4, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ sinon.

Nous verrons la démonstration plus tard, nous appuyant sur les propriétés du symbole de Legendre, des sommes de Gauss.

Corollaire. *Si p et q sont premiers impairs et ne sont pas de la forme $4n + 3$, alors :*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Si p et q sont premiers impairs, et de la forme $4n + 3$, alors :

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

Exemple 1.5. *On a par exemple :* $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1.$

Démonstration. *Si p et q sont de la forme $4n + 3$, l'exposant s'écrit*

$$\frac{(4n+2)(4m+2)}{4} = (2n+1)(2m+1).$$

Il est donc impair, ce qui justifie la relation. Dans les autres cas, sa valeur est paire.

2 Sommes de Gauss

2.1 Historique et Notes

Nous allons développer dans cette partie les origines des sommes de Gauss.

Gauss introduit ses sommes en Juillet 1801, sous la forme suivante

$$\sum_{n=0}^{k-1} e^{2i\pi mn^2/k},$$

que nous appelons aujourd'hui *Somme de Gauss quadratique*. Cette somme est difficile à évaluer, même dans le cas particulier où $m = 1$ et k un entier positif impair. Dans ce cas, Gauss montra que cette somme prenait la valeur $\pm\sqrt{k}$ ou $\pm i\sqrt{k}$, selon si k est de la forme $4u+1$ ou $4u+3$, respectivement. Gauss conjectura après l'étude d'exemples que le signe devait être toujours positif. Le 30 Août 1805, Gauss écrit dans son journal qu'il était capable de prouver sa conjecture sur le signe des ces sommes, et quelques années plus tard il publiait une évaluation de sa somme quadratique dans le cas où k est un entier positif.

Dans son étude sur les nombres premiers dans les progressions arithmétiques, Dirichlet introduit ce que l'on appellera le caractère multiplicatif χ modulo k et la somme

$$G(\chi) = \sum_{n=0}^{k-1} e^{2i\pi mn/k}.$$

Ceci est également appelé somme de Gauss, puisqu'elle coïncide avec la somme quadratique de Gauss ci-dessus pour χ d'ordre 2 et k un nombre premier qui ne divise pas m.

Dans la section suivante, nous présenterons les sommes de Gauss à travers la théorie des caractères sur les corps finis, pour ensuite nous concentrer sur le cas particulier qui nous intéresse.

2.2 Caractères et définition générale des Sommes de Gauss

Dans cette partie, nous allons définir les caractères additifs et multiplicatifs et les sommes de Gauss dans leur définition la plus générale.

2.2.1 Caractères

Cas général pour un groupe fini abélien Soit G un groupe abélien fini multiplicatif (respectivement additif).

Définition 2.1. *On appelle caractère multiplicatif (respectivement additif) de G tout homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$ des nombres complexes.*

Les caractères de G forment un groupe $Hom(G,\mathbb{C}^*)$ que l'on note $\hat{G}$ et que l'on appelle le *dual* de G.

Remarque 2.1. *En pratique, si p est un nombre premier, le groupe G sera identifié à $(\mathbb{F}_p^*, .)$ dans le cas multiplicatif et $(\mathbb{F}_p, +)$ dans le cas additif.*

Exemple 2.1. *Supposons que G soit cyclique d'ordre n, de générateur s. Si $\chi : G \to \mathbb{C}^*$ est un caractère de G, l'élément $x = \chi(s)$ vérifie la relation $x^n = 1$, c'est à dire que x est une racine n-ième de l'unité. Inversement, toute racine n-ième de l'unité x défini un caractère de G au moyen de $s^a \mapsto x^a$. On voit ainsi que l'application $\chi \mapsto \chi(s)$ est un isomorphisme de $\hat{G}$ sur le groupe U_n des racines n-ièmes de l'unité. En particulier, $\hat{G}$ est un groupe cyclique d'ordre n.*

Proposition 2.1. *Soit H un sous-groupe de G. Tout caractère de H peut être prolongé en un caractère de G.*

Preuve. *On admet cette proposition, qui se démontre par récurrence sur l'indice $(G : H)$ de H dans G.*

Remarque 2.2. *L'opération de restriction définit un homomorphisme*

$$\rho : \hat{G} \to \hat{H}$$

et la proposition 2.1 affirme que ρ est surjectif. De plus, le noyau de ρ est formé des caractères de G qui sont triviaux sur H. Il est donc isomorphe au groupe $(G/H)\hat{}$ dual de G/H. On a alors une suite exacte :

$$\{1\} \to (G/H)\hat{} \to \hat{G} \to \hat{H} \to \{1\}.$$

Proposition 2.2. *Le groupe $\hat{G}$ est un groupe abélien fini de même ordre que G.*

Cela signifie que le groupe des caractères de G est de même cardinal que G. Cette propriété de $\hat{G}$ nous sera fort utile par la suite.

Preuve. *On raisonne par récurrence sur l'ordre n de G, le cas $n = 1$ étant clair.*
Si $n \geq 2$, on choisit un sous-groupe cyclique H, non trivial, de G (licite car G est fini). D'après la remarque ci-dessus, l'ordre de $\hat{G}$ est le produit des ordres de $\hat{H}$ et de $(G/H)\hat{}$. Mais l'ordre de H (respectivement de G/H) est égal à celui de son dual, puisque H est cyclique (respectivement, puisque G/H est d'ordre plus petit que n). On en conclut que l'ordre de $\hat{G}$ est produit des ordres de H et de G/H, et il est bien égal à l'ordre de $\hat{G}$.

Remarque 2.3. *On peut prouver que $\hat{G}$ est en réalité isomorphe à G. Cela se démontre en décomposant G en produit de groupes cycliques.*

Proposition 2.3. *Soit $n = Card(G)$, et soit $\chi \in \hat{G}$. On a :*

$$\sum_{x \in G} \chi(x) = n \ \ si \ \ \chi = 1,$$

$$\sum_{x \in G} \chi(x) = 0 \ \ si \ \ \chi \neq 1.$$

Preuve. *La première formule est évidente. Pour prouver la deuxième, choisissons $y \in G$ tel que $\chi(y) \neq 1$. On a :*

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x),$$

d'où

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0.$$

Comme $\chi(y) \neq 1$, on en déduit bien $\sum_{x \in G} \chi(x) = 0$.

Corollaire. *Soit $x \in G$. On a :*

$$\sum_{\chi \in \hat{G}} \chi(x) = n \ \ si \ \ x = 1,$$

$$\sum_{\chi \in \hat{G}} \chi(x) = 0 \ \ si \ \ x \neq 1.$$

Preuve. *La seul point à prouver est le premier, qui vient du fait que si $\chi = 1$, alors $1(0) = 1$.*

Cela résulte de la proposition 2.3, appliquée au groupe $\hat{G}$.

Cas du groupe $\mathbb{F}_q^*$ et application Un caractère du groupe $(\mathbb{F}_q^*, \times)$ est un morphisme χ du groupe multiplicatif $(\mathbb{F}_q^*, \times)$ (on laisse ici de côté le cas additif) vers le groupe multiplicatif $\mathbb{C}^*$. Nous allons maintenant étudier une application directe des caractères. Pour $a \in \mathbb{F}_q$, notons $N(x^n = a)$ le nombre de solutions de $x^n = a$ pour $n \in \mathbb{N}$.

Proposition 2.4. *Si $n \mid q-1$, alors $N(x^n = a) = \sum_{\chi^n = 1} \chi(a)$.*

Lemme 2.1. *Si $a \in \mathbb{F}_q^*$, $n \mid q-1$, et $x^n = a$ n'a pas de solutions, alors il y a un caractère χ tel que $\chi^n = 1$ et $\chi(a) = \neq 1$.*

Preuve. *Soit g un générateur de $\mathbb{F}_q$, et soit λ définie comme suit :*

$$\begin{array}{rccc} \lambda & : & \mathbb{F}_q & \to & \mathbb{C} \\ & & g^k & \mapsto & e^{2i\pi k/(q-1)} \end{array}$$

Notons que λ est un caractère d'ordre $q-1$. C'est le générateur du groupe des caractères de $\mathbb{F}_q$.

Posons $\chi = \lambda^{\frac{p-1}{n}}$. Alors $\chi(g) = e^{2i\pi/n}$. Maintenant, si $a = g^l$, $x^n = a$ n'a pas de solutions, alors $n \nmid l$. Donc $\chi(a) = \chi(g)^l = e^{2i\pi n/l} \neq 1$.
Enfin, on a $\chi^n = \lambda^{p-1} = 1$.
On peut alors démontrer la proposition 2.4.
Montrons tout d'abord qu'il y a exactement n caractères d'ordre divisant n : comme la valeur de $\chi(g)$ pour un tel caractère doit être une racine n-ième de l'unité, il y a au plus n tels caractères. Si on prend, comme dans le lemme, $\chi = \lambda^{\frac{p-1}{n}}$, alors $\chi(g) = e^{2i\pi/n}$ et on a n caractères distincts d'ordre n : $1, \chi, \chi^2, ..., \chi^{n-1}$.

Il reste à montrer la formule.
- *Si $a = 0$, le résultat est clair.*
- *Si $a \neq 0$ et $x^n = a$ a des solutions, il existe donc $b \in \mathbb{F}_q$ tel que $\chi(b^n) = \chi(a)$. Si $\chi^n = 1$, alors $\chi(b^n) = \chi^n(b) = 1$. Ainsi,*

$$\sum_{\chi^n = 1} \chi(a) = n,$$

  ce qui correspond bien à $N(x^n = a)$.
- *Si $a \neq 0$ et $x^n = a$ n'a pas de solutions, on doit alors montrer que*

$$\sum_{\chi^n = 1} \chi(a) = 0.$$

Appelons T cette somme. D'après le lemme, il existe un caractère ρ tel que $\rho \neq 1$ et $\rho^n = 1$. Nous avons donc :

$$\rho(a)T = \sum_{\chi^n=1} \rho(a)\chi(a) = \sum_{\chi^n=1} (\rho - \chi)(a) = T.$$

Ainsi, $(\rho(a) - 1)T = 0$, et donc $T = 0$.

2.2.2 Définition générale des Sommes de Gauss

Nous allons donner ici la définition générale de ce que l'on appelle communément *Somme de Gauss.*

Définition 2.2. *Soit $\alpha \in \mathbb{F}_q^*$, soit ψ un caractère du groupe additif $(\mathbb{F}_q, +)$ et soit χ un caractère du groupe multiplicatif $(\mathbb{F}_q^*, \times)$. On défini la Somme de Gauss des caractères ψ etχ selon α comme suit :*

$$\mathcal{G}_a(\chi, \psi) = \sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t)$$

Dans toute la suite, on notera $\mathcal{G}(\chi, \psi) = \mathcal{G}_1(\chi, \psi)$. Notons par ailleurs que :
- $\mathcal{G}_a(1, 1) = 0$ avec $a \neq 0$.
- $\mathcal{G}_0(\chi, \psi) = 0$ avec $\chi \neq 0$.
- $\mathcal{G}_0(1, \psi) = q$.
- $\mathcal{G}_a(\chi, \psi) = \chi(a^{-1})\mathcal{G}(\chi, \psi)$.

Montrons à présent une proposition importante des Sommes de Gauss.

Proposition 2.5. *Si $\chi \neq 1$, alors $\mid \mathcal{G}(\chi, \psi) \mid = \sqrt{q}$*

Preuve. *Nous allons évaluer la somme*

$$\sum_{a \in \mathbb{F}_q} \mathcal{G}(\chi, \psi)\overline{\mathcal{G}_a(\chi, \psi)}$$

de deux façons différentes.

- *si $a \neq 0$, alors $\mathcal{G}(\chi, \psi)\overline{\mathcal{G}_a(\chi, \psi)} = \chi(a^{-1})\mathcal{G}(\chi, \psi)\overline{\chi(a^{-1})\mathcal{G}_a(\chi, \psi)}$. Or, $\chi(a)$ étant une racine $(q-1)$-ième de l'unité, on a que $\chi(a^{-1}) = \overline{\chi(a)}$ et donc*

$$\mathcal{G}(\chi, \psi)\overline{\mathcal{G}_a(\chi, \psi)} = \mid \mathcal{G} \mid^2 .$$

  Comme $\mathcal{G}_0(\chi, \psi) = 0$, on a :

$$\sum_{a \in \mathbb{F}_q} \mathcal{G}(\chi, \psi)\overline{\mathcal{G}_a(\chi, \psi)} = (q-1) \mid \mathcal{G} \mid^2 .$$

- *D'un autre côté,*

$$\begin{aligned}
\sum_{a \in \mathbb{F}_q} \mathcal{G}(\chi, \psi)\overline{\mathcal{G}_a(\chi, \psi)} &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(ax)\overline{\psi(ay)} \\
&= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \chi(x)\chi(y)^{-1}\psi(a(x-y)) \\
&= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \chi(x)\chi(y)^{-1}\delta_{x,y}q \\
&= (q-1)q \qquad (8)
\end{aligned}$$

Ainsi, on obtient l'égalité $(q-1)q = (q-1) \mid \mathcal{G}(\chi, \psi) \mid^2$, d'où le résultat.

2.3 Analyse et exemple de Sommes de Gauss

Dans cette partie, nous développerons quelques cas particuliers de Sommes de Gauss. De plus, nous verrons dans le paragraphe 2.3.4 la somme qui nous servira lors de la démonstration de la loi de réciprocité quadratique.

2.3.1 Sommes de la forme $H = \sum_{n=0}^{k-1} e^{2i\pi n^2/k}$

Nous allons parler ici des premières sommes de Gauss, introduites en 1801, et nous montrerons une évaluation de cette somme dans le cas où $m = 1$ et k est un entier positif, généralisant ainsi le premier résultat de Gauss, où $m = 1$ mais k est seulement un entier positif et impair.

Théorème 2.1. *Soit k un entier positif, et soit*

$$H = \sum_{n=0}^{k-1} e^{2i\pi n^2/k} \tag{9}$$

Alors,

$$H = \begin{cases} (1+i)\sqrt{k} & si \quad k \equiv 0 \pmod 4, \\ \sqrt{k} & si \quad k \equiv 1 \pmod 4, \\ 0 & si \quad k \equiv 2 \pmod 4, \\ i\sqrt{k} & si \quad k \equiv 3 \pmod 4, \end{cases}$$

où $\sqrt{k}$ est positif.

Démonstration. *La fonction $\{x \mapsto e^{2i\pi mx/k}\}_{m\in\mathbb{Z}}$ est une famille orthogonale pour le produit scalaire*

$$< f, g >= \frac{1}{k}\int_0^k f(t)\overline{g(t)}dt.$$

La série de Fourier de la fonction $x \mapsto e^{2i\pi x^2/k}$ nous montre que

$$e^{2i\pi n^2/k} = \sum_{m=-\infty}^{\infty} \left(\frac{1}{k}\int_0^k e^{2i\pi x^2/k} e^{-2i\pi mx/k} dx\right) e^{2i\pi mn/k},$$

donc

$$\begin{aligned} H &= \sum_{n=0}^{k-1}\sum_{m=-\infty}^{\infty} \left(\frac{1}{k}\int_0^k e^{2i\pi x^2/k} e^{-2i\pi mx/k} dx\right) e^{2i\pi mn/k} \\ &= \sum_{m=-\infty}^{\infty} \left(\frac{1}{k}\int_0^k e^{2i\pi x^2/k} e^{-2i\pi mx/k} dx\right) \sum_{n=0}^{k-1} e^{2i\pi mn/k} \end{aligned} \tag{10}$$

Les relations de la propriété (2.3) du paragraphe 2.2.1 appliquées au groupe fini abélien $\mathbb{Z}/k\mathbb{Z}$nous donne

$$\sum_{n=0}^{k-1} e^{2i\pi mn/k} = \begin{cases} k & si \quad k \mid m \\ 0 & si \quad k \nmid m \end{cases}$$

On peut aussi noter qu'il s'agit d'une somme d'unité ou de racines de l'unité.

Ainsi, l'équation (10) se simplifie alors pour donner

$$\begin{aligned} H &= \sum_{m=-\infty}^{\infty} \int_0^k e^{2i\pi x^2/k} e^{-2i\pi mx/k} dx \\ &= \sum_{m=-\infty}^{\infty} \int_0^k e^{2i\pi(x^2-kmx)/k} dx \\ &= N \sum_{m=-\infty}^{\infty} e^{-i\pi m^2 k/2} \int_{-n/2}^{1-n/2} e^{2i\pi k v^2} dv \end{aligned} \tag{11}$$

avec $v = \frac{x}{k} - \frac{m}{2}$, *et de plus,*

$$e^{-i\pi m^2 k/2} = \begin{cases} 1 & si \quad m \text{ est pair}, \\ i^{-k} & si \quad m \text{ est impair} \end{cases}$$

Puisque les racines impaires sont congrues à 1 *modulo* 4, *alors la somme dans l'équation (11) peut être coupée en deux sommes sur* $m = 2m' + 1$ *et* $m = mm'$, *donnant*

$$H = N \sum_{m'=-\infty}^{\infty} \int_{-m'}^{-m'} e^{2i\pi k v^2} dv + i^{-k} \sum_{m'=-\infty}^{\infty} \int_{-m'-1/2}^{-m'+1/2} e^{2i\pi k v^2} dv.$$

ce qui nous donne alors

$$\begin{aligned} H &= k(1 + i^{-k}) \int_{-\infty}^{\infty} e^{2i\pi k v^2} dv \\ &= \sqrt{k}(1 + i^{-k}) \int_{-\infty}^{\infty} e^{2i\pi w^2} dw \end{aligned} \tag{12}$$

avec $w = v\sqrt{k}$. *Pour calculer l'intégrale, on remarque que l'équation (12) est vraie pour tout* k, *et en particulier pour* $k = 1$. *Quand* $k = 1$, *alors* $H = 1$, *d'après l'équation (9), et donc*

$$\int_{-\infty}^{\infty} e^{2i\pi w^2} dw = \frac{1}{1 + i^{-1}}.$$

On obtient alors que

$$H = \frac{1 + i^{-k}}{1 + i^{-1}} \sqrt{k},$$

ce qui donne le résultat, selon les congruences, et termine la preuve du théorème.

2.3.2 Sommes de la forme $\tau(a) = \sum_{x=0}^{p-1} e^{2i\pi a x^2/p}$

Nous allons ici discuter du cas particulier des sommes de Gauss en prenant $k = p$ un nombre premier impair, et m premier avec p.

On remarque en particulier que $e^{2i\pi a/p}$ ne dépend que de a modulo p et garde un sens pour $a \in \mathbb{F}_p$. Nous utiliserons les propriétés générales des caractères ainsi que la formule suivant

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) = 0.$$

Cela résultant du fait qu'il y a autant de carrés que de non-carrés dans $\mathbb{F}_p^*$, comme nous l'avons vu.

Définition 2.3. *Soit p un nombre premier impair, et soit $a \in \mathbb{F}_p$. On appelle Somme quadratique de Gauss la somme suivante :*

$$\tau(a) = \sum_{x=0}^{p-1} e^{2i\pi a x^2/p}.$$

Proposition 2.6. *Les sommes $\tau(a)$ vérifient les formules suivantes :*

1. $\tau(a) = \left(\frac{a}{p}\right) \tau(1)$.
2. $\mid \tau(a) \mid^2 = p$.
3. $\tau(1)^2 = \left(\frac{-1}{p}\right) p$.

Preuve. *Soit a un résidu quadratique et b un non-résidu quadratique modulo p.*

$$\tau(a) + \tau(b) = \sum_{x=0}^{p-1} e^{2i\pi a x^2/p} + \sum_{x=0}^{p-1} e^{2i\pi b x^2/p} = 2 + 2 \sum_{u \in a\mathbb{F}_p^{*2}} e^{2i\pi u/p} + 2 \sum_{v \in b\mathbb{F}_p^{*2}} e^{2i\pi v/p} = 0.$$

En effet,

$$2 \sum_{u \in a\mathbb{F}_p^{*2}} e^{2i\pi u/p} + 2 \sum_{v \in b\mathbb{F}_p^{*2}} e^{2i\pi v/p} = 2 \sum_{u \mathbb{F}_p^{*}} e^{2i\pi u/p} = -2$$

Ainsi, on a $\tau(b) = -\tau(1)$ et $\tau(a) = \tau(1)$ puisque 1 est un résidu quadratique, d'où (1). Maintenant, en appliquant la proposition 2.5 vue à la partie 2.2.2 à notre cas précis, on en déduit immédiatement (2).
Enfin, on a que $\overline{\tau(1)} = \tau(-1) = \left(\frac{-1}{p}\right) \tau(1)$, donc, en passant au conjugué, il vient que $\tau(1)^2 = \left(\frac{-1}{p}\right) \mid \tau(1) \mid^2 = \left(\frac{-1}{p}\right) p$, d'où (3).

2.3.3 Sommes de la forme $\mathcal{G}(\chi, a) = \sum_{x \in \mathbb{F}_p^*} \chi(x) e^{2i\pi a x/p}$

Nous analysons ici une généralisation de cas précédent des Sommes quadratiques de Gauss (liées à un élément $a \in \mathbb{F}_p$) avec k premier et a premier avec k, en considérant les sommes de Gauss d'un caractère χ de $\mathbb{F}_p^*$ que l'on prolonge à $\mathbb{F}_p$ en prenant $\chi(0) = 0$.

Définition 2.4. *Soit p un nombre premier impair, et soit $a \in \mathbb{F}_p$. On appelle Somme de Gauss associée au caractère multiplicatif χ selon a la somme suivante :*

$$\mathcal{G}(\chi, a) = \sum_{x \in \mathbb{F}_p} \chi(x) e^{2i\pi a x/p}.$$

Proposition 2.7. *Les sommes $\mathcal{G}(\chi, a)$ vérifient les formules suivantes :*

1. $\mathcal{G}(\chi, a) = \overline{\chi}(a) \mathcal{G}(\chi, 1)$.
2. $\mid \mathcal{G}(\chi, a) \mid^2 = p$.
3. $\mathcal{G}(\chi, 1) = \chi(-1) \mathcal{G}(\overline{\chi}, a)$.

Preuve. *Notons avant tout que* $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi}(a)$. *Ainsi :*

$$\mathcal{G}(\chi, a) = \sum_{x \in \mathbb{F}_p^*} \chi(x) e^{2i\pi ax/p} = \chi(a^{-1}) \sum_{x \in \mathbb{F}_p^*} \chi(ax) e^{2i\pi ax/p} = \chi(a^{-1}) \mathcal{G}(\chi, 1).$$

On en déduit alors (1). *Les deux autres points découlent directement des propriétés des Sommes de Gauss vues dans le cas général au chapitre 2.2.2.*

2.3.4 Sommes de la forme $\tau = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \alpha^x$

Nous introduisons ici un nouvel aspect des Sommes de Gauss qui nous sera fort utile pour la démonstration de la loi de réciprocité quadratique que nous aborderons au chapitre 3.1.

Définition 2.5. *Soient* p *et* q *deux nombres premiers impairs distincts, et* α *une racine primitive* p*-ième de l'unité dans une extension de* $\mathbb{F}_q$. *On a par ailleurs que* α *est racine de l'équation :*

$$\alpha^{p-1} + \alpha^{p-2} + ... + \alpha + 1 = 0.$$

On appelle alors Somme de Gauss dans $\mathbb{F}_q(\alpha)$ *la somme suivante :*

$$\tau = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \alpha^x$$

Voici à présent une proposition qui nous servira lors de la démonstration de la loi de réciprocité quadratique.

Proposition 2.8. *Soit* τ *comme ci-dessus. Alors* τ *vérifient les égalités suivantes.*

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

Preuve. *Calculons :*

$$\tau^2 = \sum_{x,y \in \mathbb{F}_p} \left(\frac{xy}{p}\right) \alpha^{x+y} = \sum_{u \in \mathbb{F}_p} S(u) \alpha^u,$$

avec $S(u) = \sum_{x+y=u} \left(\frac{xy}{p}\right) = \sum_{x \in \mathbb{F}_p} \left(\frac{x(u-x)}{p}\right)$. *Pour* $u = 0$, *on a* $S(0) = \sum_{x \in \mathbb{F}_p} \left(\frac{-x^2}{p}\right) = \left(\frac{-1}{p}\right)(p-1)$. *Pour* $u \in \mathbb{F}_p^*$, *on a :*

$$S(u) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x(u-x)}{p}\right) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{-x^2(1-ux^{-1})}{p}\right) = \left(\frac{-1}{p}\right) \sum_{x \in \mathbb{F}_p^*} \left(\frac{1-ux^{-1}}{p}\right) = \left(\frac{-1}{p}\right) \{\sum_{y \in \mathbb{F}_p^*} \left(\frac{y}{p}\right) - 1\},$$

donc $S(u) = -\left(\frac{-1}{p}\right)$. *Ainsi,*

$$\tau^2 = \left(\frac{-1}{p}\right)(p - 1 - \sum_{u=1}^{p-1} \alpha^u) = \left(\frac{-1}{p}\right) p.$$

Cela permet de prouver la première formule. En ce qui concerne la seconde, on écrit, puisque la caractéristique de q *est impaire :*

$$\tau^q = \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right)^q \alpha^{qx} = \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right) \alpha^{qx} = \left(\frac{q}{p}\right) \sum_{x\in\mathbb{F}_p} \left(\frac{qx}{p}\right) \alpha^{qx} = \left(\frac{q}{p}\right) \tau.$$

Comme $\tau \neq 0$, d'après la première formule, on obtient alors la seconde.

3 Applications

3.1 Démonstration de la loi de réciprocité quadratique

Grâce aux propriétés démontrées précédemment sur les Sommes de Gauss du type $\tau = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \alpha^x$ dans la partie 2.3.4, nous pouvons à présent démontrer la loi de réciprocité quadratique dont on rappelle l'énoncé ci-dessous.

Théorème (Gauss)**.** *Soient p et q deux nombres premiers impairs distincts. On a*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Démonstration (Loi de réciprocité quadratique)**.** *Soient p et q deux nombres premiers impairs distincts.*
Notons avant tout que si q ne divise pas $a \in \mathbb{Z}$, alors $a^{(q-1)/2} \equiv \left(\frac{a}{q}\right)$ mod q.
En effet, si q divise a, alors la formule est claire. Si $q = b^2 \in \mathbb{F}_q^{*2}$, alors $a^{(q-1)/2} = b^{q-1} = 1 = \left(\frac{a}{q}\right)$, modulo q, et enfin, si $\left(\frac{a}{q}\right) = -1$, en prenant g un générateur de $\mathbb{F}_q^*$, alors $\left(\frac{g}{q}\right) = -1$, et $a = g^m$, avec m impair (sinon a serait un carré), donc $\left(\frac{a}{q}\right) = \left(\frac{g}{q}\right)^m = -1$ modulo q, d'où le résultat.
En prenant maintenant $a = p$, on obtient les égalités suivantes modulo q :

$$\left(\frac{p}{q}\right) = p^{(q-1)/2} = \left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2},$$

et ce d'après le point 1. de la propriété 2.8, puis que

$$\left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2} = (-1)^{(q-1)(p-1)/4}\tau^{q-1},$$

d'après la définition du symbole de Legendre. Enfin, on a que

$$(-1)^{(q-1)(p-1)/4}\tau^{q-1} = (-1)^{(q-1)(p-1)/4}\left(\frac{q}{p}\right),$$

d'après le point 2. de la propriété 2.8. Ainsi, il vient que

$$\left(\frac{p}{q}\right) = (-1)^{(q-1)(p-1)/4}\left(\frac{q}{p}\right)$$

ce qui termine la démonstration de la Loi de réciprocité quadratique.

Exemple 3.1. *Nous allons voir ici un exemple montrant comment la Loi de réciprocité quadratique permet de calculer des valeurs du symbole de Legendre.*

$$\begin{aligned}\left(\frac{1965}{2311}\right) &= \left(\frac{3}{2311}\right)\left(\frac{5}{2311}\right)\left(\frac{131}{2311}\right),\\ \left(\frac{3}{2311}\right) &= \left(\frac{2311}{3}\right)(-1)^{1155\times 1} = -\left(\frac{1}{3}\right) = -1\end{aligned}$$

Car $2311 \equiv 1$ *mod* 3.

$$\left(\frac{5}{2311}\right) = \left(\frac{2311}{5}\right)(-1)^{1155\times 2} = \left(\frac{1}{5}\right) = 1$$

Car $2311 \equiv 1 \ mod\ 5$.

$$\left(\frac{131}{2311}\right) = \left(\frac{2311}{131}\right)(-1)^{1155\times 65} = -\left(\frac{84}{131}\right)$$

Car $2311 \equiv 84 \ mod\ 1331$.

$$\begin{aligned} -\left(\frac{84}{131}\right) &= -\left(\frac{4}{131}\right)\left(\frac{3}{131}\right)\left(\frac{7}{131}\right) = -\left(\frac{3}{131}\right)\left(\frac{7}{131}\right) \\ &= -\left(\frac{131}{3}\right)(-1)^{65\times 1}\left(\frac{131}{7}\right)(-1)^{65\times 3} \\ &= -\left(\frac{2}{3}\right)\left(\frac{5}{7}\right) = -(-1)\left(\frac{7}{5}\right)(-1)^{3\times 2} = \left(\frac{2}{5}\right) = -1 \end{aligned}$$

Donc

$$\left(\frac{18151}{2311}\right) = (-1)(+1)(-1) = 1.$$

3.2 Équations sur les corps finis et théorème de Chevalley

Nous allons à présent donner une autre application des Sommes de Gauss, qui touche cette fois à la connaissance du nombre de solutions d'équations.

3.2.1 Théorème de Chevalley-Warning

Théorème 3.1 (Chevalley-Warning)**.** *Soit* $\mathbb{K}=\mathbb{F}_q$ *un corps fini de caractéristique* p*. Si* $P \in \mathbb{K}[x_1, ..., x_n]$*, avec* $deg(P) < n$*, alors*

$$Card\{x \in \mathbb{K}^n | P(x) = 0\} \equiv 0 \ mod\ p.$$

En particulier, si P *est homogène de degré* $d < n$*, alors* P *possède un zéro non trivial (c'est à dire distinct de* 0*).*

Démonstration. *On commence par calculer la somme des valeurs d'un monôme.*

Lemme 3.1. *Soit* $x^m = x_1^{m_1}...x_n^{m_n}$ *un monôme, alors* $\sum_{x\in\mathbb{K}^n} x^m$ *est nul sauf si chaque* m_i *est non-nul et divisible par* $(q-1)$*. En particulier, cette somme est nulle dès que* $m_1 + ... + m_n < (n-1)q$*.*

Preuve. *Remarquons que, comme le polynôme "*X^0*" est le polynôme constant, il est naturel de prendre ici la convention* $0^0 = 1$*. Le calcul*

$$\sum_{x\in\mathbb{K}^n} x^m = \sum_{(x_1,...,x_n)\in\mathbb{K}^n} x_1^{m_1}...x_n^{m_n} = \left(\sum_{x_1\in\mathbb{K}} x_1^{m_1}\right)...\left(\sum_{x_n\in\mathbb{K}} x_n^{m_n}\right)$$

permet de se ramener au cas d'une seule variable ; Si $m = 0$*, alors* $\sum_{y\in\mathbb{K}} y^0 = q.1_{\mathbb{K}} = 0$*. Si* m *n'est pas divisible par* $q-1$*, prenons* y_0 *un générateur de* $\mathbb{K}^*$*, alors* $y_0^m \neq 1$ *et donc*

$$\sum_{y\in\mathbb{K}} y^m = \sum_{y\in\mathbb{K}} (y_0 y)^m = y_0^m \sum_{y\in\mathbb{K}} y^m$$

ce qui entraine $\sum y \in \mathbb{K} y^m = 0$*.*

On en déduit que si $Q \in \mathbb{K}[x_1, ..., x_n]$ *avec* $deg(Q) < (q-1)n$, *alors* $\sum x \in \mathbb{K}^n Q(x) = 0$. *Soit maintenant* P *le même polynôme que celui de l'énoncé du Théorème. Nous allons appliquer le résultat précédent au polynôme* $Q = 1 - P^{q-1}$.
Observons que $deg(Q) = (q-1)deg(P) < (q-1)n$, *et que* $Q(x) = 1$ *si* $P(x) = 0$, *alors que* $Q(x) = 0$ *si* $P(x) \neq 0$ *et* $x \in mathbbK^n$, *donc on a l'égalité dans* $\mathbb{K}$:

$$0 = \sum_{y \in \mathbb{K}^n} Q(x) = \sum_{\substack{y \in \mathbb{K}^n \\ P(x)=0}} 1 = Card\{x \in \mathbb{K}^n | p(x) = 0\}.1_{\mathbb{K}}$$

ce qui achève la démonstration, car $\mathbb{K}$ *est de caractéristique* p *et donc* $m.1_{\mathbb{K}} = 0$ *équivaut à* $m \equiv 0 \; mod \; p$.

3.2.2 Nombre de zéros d'une forme quadratique

Si $Q(x) = \sum_{1 \leq i,j \leq n} a_{ij} x_i y_j$ est une forme quadratique, on dit qu'elle est *non dégénérée* si $D_Q = det(a_{ij}) \neq 0$.
Si la caractéristique de $\mathbb{K}$ est différente de 2 alors, on peut supposer que Q est diagonale (on ne fera pas la démonstration ici).

Théorème 3.2. *Soit* Q *une forme quadratique en* n *variables, non dégénérée, à coefficients dans* $\mathbb{F}_p$ *(où* $p \neq 2$*), alors :*

$$Card\{x \in \mathbb{F}_p^n \mid Q(x) = 0\} = p^{n-1} + \varepsilon(p-1)p^{\frac{n}{2}-1}$$

avec

$$\varepsilon = \begin{cases} 0 & si \; n \; est \; impair \\ \left(\dfrac{(-1)^{n/2} D_Q}{p}\right) & si \; n \; est \; pair \end{cases}$$

Démonstration. *On suppose que* Q *est diagonale, donc* $Q(x) = a_1 x_1^2 + ... + a_n x_n^2$. *Notons* N_p *le cardinal que nous voulons calculer. On a :*

$$\begin{aligned}
pN_p &= \sum_{a=0}^{p-1} \sum_{x \in \mathbb{F}_p^n} e^{2i\pi a Q(x)/p} \\
&= p^n + \sum_{a=1}^{p-1} \sum_{x \in \mathbb{F}_p^n} e^{2i\pi a Q(x)/p} \\
&= p^n + \sum_{a=1}^{p-1} \sum_{x_1,...,x_n \in \mathbb{F}_p} e^{2i\pi a(a_1 x_1^2 + ... + a_n x_n^2)/p} \\
&= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \sum_{x_j \in \mathbb{F}_p} e^{2i\pi a a_j x_j^2/p} \\
&= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \tau(a a_j) \\
&= p^n + \tau(1)^n \left(\frac{a_1 ... a_n}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n
\end{aligned}$$

Or $a_1...a_n = D_Q$, et la somme $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n$ vaut 0 (respectivement $(p-1)$) si n est impair (respectivement pair). On en déduit que $N_p = p^{n-1}$ si n est impair. Si n est pair, on remarque que

$$\tau(1)^n = (\tau(1)^2)^{n/2} = \left(\frac{-1}{p}\right)^{n/2} p^{n/2}$$

et on obtient bien la formule annoncée pour N_p.

3.2.3 Nombre de solutions d'équations du type $a_0x_0^{n_0} + ... + a_rx_r^{n_r} = 0$

Soit n un entier fixé, q un premier impair, et $d = (n, q-1)$ le *pgcd* de n et $(q-1)$. Soit $r \in \mathbb{N}^*$, $n_0, ..., n_r \in \mathbb{N}^*$, et $a_0, ..., a_r \in \mathbb{F}_q^*$, et on cherche à compter les solutions d'équations du type

$$a_0x_0^{n_0} + ... + a_rx_r^{n_r} = 0,$$

avec les x_i dans le corps fini $\mathbb{F}_q$. On note N le nombre de solutions de l'équation.

Partition de l'ensemble solution On note $L : \mathbb{F}_q^{r+1} \to \mathbb{F}_q$ la forme linéaire définie par

$$\forall u = (u_0, ..., u_r) \in \mathbb{F}_q^{r+1},\ L(u) = \sum_{i=0}^{r} a_iu_i.$$

On définit p et f par :

$$\begin{array}{rccc} p : & \mathbb{F}_q^{r+1} & \to & \mathbb{F}_q^{r+1} \\ & (x_i)_{i=0,...,r} & \mapsto & (x_i^{n_i})_{i=1,....,r} \end{array} \qquad f = L \circ p$$

Alors $f((x_i)_i) = 0$ si et seulement si $u = p(x_i)_i) \in L^{-1}(0)$. Ainsi,

$$N = Card(f^{-1}(0)) = \sum_{u \in L^{-1}(0)} Card(p^{-1}(u)) = \sum_{u \in ker(L)} N_0(u_0)...N_r(u_r).$$

On a donc la proposition suivante.

Proposition 3.1. *Soit N le nombre de solutions de l'équation $\sum_{i=0}^{r} a_ix_i^{n_i} = 0$, alors*

$$N = \sum_{u \in L^{-1}(0)} N_0(u_0)...N_r(u_r),$$

la somme portant sur les $u \in \mathbb{F}_q^{r+1}$ appartenant au sous-espace vectoriel $ker(L)$ de dimension r (L est une forme linéaire non-nulle).

Utilisation des Sommes de Gauss

Proposition 3.2. *Soit χ un caractère sur $\mathbb{F}q$. On note $d_i = Card\{x / x^{n_i} = 0\}$. On peut calculer N à l'aide des sommes de Gauss :*

$$N = \sum_{u \in ker(L)} \sum_{\alpha \in X} \chi_{\alpha_0}(u_0)...\chi_{\alpha_r}(u_r),$$

où l'on note α le multi-indice $(\alpha_0, ..., \alpha_r) \in [0; 1[^{r+1}$ et X est l'ensemble des α qui vérifient $\alpha_0d_0 \equiv 0[1], ..., \alpha_rd_r \equiv 0[1]$.

Preuve. *On utilise la proposition 3.1 précédente, ainsi que le résultat de la proposition 2.4 de la partie 2.2.1 que l'on applique à notre cas.*

Pour u quelconque, et $\alpha = (0, ..., 0)$ on a :

$$\prod_{j=0}^{r} \chi_{\alpha_j}(u_j) = \prod_{j=0}^{r} \chi_0(u_j) = \prod_{j=0}^{r} 1 = 1.$$

Ainsi :

$$\begin{aligned} N &= \sum_{u \in ker(L)} 1 + \sum_{u \in ker(L)} \sum_{\alpha \in X \setminus \{(0,...,0)\}} \chi_{\alpha_0}(u_0)...\chi_{\alpha r}(u_r) \\ &= q^r + \sum_{\alpha \in X \setminus \{(0,...,0)\}} \sum_{u \in ker(L)} \chi_{\alpha_0}(u_0)...\chi_{\alpha r}(u_r) \end{aligned}$$

Le multi-indice $(0, ..., 0)$ fait donc apparaitre un q^r. Parmi les autres multi-indices, beaucoup ne contribuent pas. en effet, on a le lemme suivant :

Lemme 3.2. *Soit* $\alpha \in X \setminus \{(0, ..., 0)\}$ *tel que* $\alpha_j = 0$ *pour un certain* $j \in \{0, ..., r\}$. *Alors*

$$\sum_{u \in ker(L)} \chi_{\alpha_0}(u_0)...\chi_{\alpha r}(u_r) = 0.$$

Preuve. *Quitte à permuter les indices, on suppose qu'il existe* $s \in \{1, ..., r\}$ *tel que* $\alpha_s = \alpha_{s+1} = ... = \alpha_r = 0$ *et les* $\alpha_0, ..., \alpha_{s-1}$ *sont non-nuls. On a :*

$$\begin{aligned} A &= \sum_{u \in ker(L)} \chi_{\alpha_0}(u_0)...\chi_{\alpha r}(u_r) \\ &= \sum_{u \in ker(L)} \chi_{\alpha_0}(u_0)...\chi_{\alpha\, s-1}(u_{s-1}) \times 1 \times ... \times 1 \\ &= \sum_{(u_s,...,u_r) \in \mathbb{F}_q^{r-s+1}} \sum_{(u_0,...,u_{s-1}) \in \mathbb{F}_q^s} \chi_{\alpha_0}(u_0)...\chi_{\alpha\, s-1}(u_{s-1}) \\ &= q^{r-s+1} \sum_{(u_0,...,u_{s-1}) \in \mathbb{F}_q^s} \chi_{\alpha_0}(u_0)...\chi_{\alpha\, s-1}(u_{s-1}) \\ &= q^{r-s+1} \prod_{i=0}^{s-1} \sum_{u_i \in \mathbb{F}_q} \chi_{\alpha_i}(u_i) \end{aligned}$$

Or, comme $\alpha_0, ..., \alpha_{s-1}$ *sont tous nuls, chacun des facteurs, à savoir chaque somme* $\sum_{u_i \in \mathbb{F}_q} \chi_{\alpha_i}(u_i)$, *est nulle. Finalement, A est nul, ce qui termine la preuve du lemme.*

Proposition 3.3. *On a :*

$$N = q^r + \sum_{u,\alpha} \chi_{\alpha_0}(u_0)...\chi_{\alpha r}(u_r),$$

où u parcourt $ker(L)$ *et les* $\alpha = (\alpha_0, ..., \alpha_r)$ *vérifient* $\alpha_i d_i \equiv 0[1]$ *et* $\alpha_i \notin \mathbb{Z}$ *(ce qui revient à dire que* χ_{α_i} *n'est pas le caractère trivial).*

Notons qu'il existe des résultats sur le nombre de solutions de telles équations avec second membre non-nul. Ces derniers font notamment intervenir les Sommes de Jacobi (que nous évoquerons plus loin) mais nous ne développerons pas cet aspect.

3.3 Constructibilité des polygones réguliers

La question de savoir quels sont les figures et les nombres constructibles à la règle et au compas date de l'Antiquité, étant alors au centre des recherches mathématiques. C'est en un sens, un thème fondateur. Il a fallu pas moins de 2000 ans avant que ne soient réalisés des progrès significatifs dans ce domaine, grâce notamment aux travaux de Gauss. Pourquoi la règle et le compas ? Probablement parce que ces instruments à la fois simples et relativement précis restent les seuls que nous possédons. Dès lors, une des questions les plus simples à formuler dans ce domaine est la suivante : Quels sont les polygones réguliers constructibles ? C'est d'ailleurs le quatrième grand problème qu'ont laissé derrière elles les écoles de Mathématiques Grecques, avec les problèmes de la quadrature du cercle, de la duplication du cube, et de la trisection de l'angle. C'est de ce problème que nous allons parler ici.

3.3.1 Avant-propos et Théorème de Gauss

Dans cette dernière partie, nous donnons la caractérisation des polygones réguliers constructibles, qui résulte du théorème dit de Gauss, publié pour la première fois en 1801. Nous aborderons une partie de la preuve qui met en application certaines des propriétés que nous avons étudiés sur les Sommes de Gauss dans la partie 3.3.3.

Définition 3.1. *Un nombre de Fermat est un nombre p tel qu'il existe un $n \in \mathbb{N}$ pour lequel $p = 2^{2^n} + 1$.*

Théorème 3.3 (Gauss)**.** *Les polygones réguliers constructibles sont ceux dont le nombre de côtés n est de la forme 2^α, $\alpha \geq 2$ ou de la forme $2^\alpha p_1 p_2 ... p_r$ avec $\alpha \in \mathbb{N}$ et où les p_i sont des nombres premiers distincts qui sont des nombres de Fermat et $r \in \mathbb{N}^*$.*

3.3.2 Résultats préliminaires

Définition 3.2. *Un nombre $\alpha \in \mathbb{R}$ est dit constructible si il existe des sous-corps de $\mathbb{R} = K_0 \subset K_1 \subset K_2 \subset ... \subset K_n$, avec $n \in \mathbb{N}$, tels que $\alpha \in K_n$ et $K_i = K_{i-1}(\sqrt{\alpha_{i-1}})$ pour tout $\alpha_i \in K_i$, $i = 1, ..., n$.*

Remarque: Cette définition est équivalente à dire qu'un nombre est constructible s'il est la mesure d'une longueur associée à deux points constructibles à la règle (non-graduée) et au compas, à partir d'un repère constitué des trois points déterminés à l'avance.
On remarque également que $[K_i : K_{i-1}] = 2$, pour $i \leq m$. On en déduit que $[K_n : K] = n^2$, et donc que si un nombre est constructible, alors son polynôme minimal a pour degré une puissance de 2. Ce résultat est une conséquence du Théorème de Wantzel.

Nous proposons maintenant deux Lemmes nécessaires à la démonstration du théorème de Gauss.

Lemme 3.3. *Si m et n sont premiers entre eux, l'angle de mesure $\frac{\hat{2\pi}}{mn}$ est constructible si et seulement si $\frac{\hat{2\pi}}{n}$ et $\frac{\hat{2\pi}}{m}$ le sont.*

Preuve. *Soient m et n premiers entre eux.*

- *Si $\frac{\hat{2\pi}}{mn}$ est constructible, alors $\frac{\hat{2\pi}}{n}$ et $\frac{\hat{2\pi}}{2}$ le sont aussi car $\frac{\hat{2\pi}}{n} = m\frac{\hat{2\pi}}{mn}$ et $\frac{\hat{2\pi}}{m} = n\frac{\hat{2\pi}}{mn}$, et il est facile de construire à partir d'un angle un multiple de cet angle en reportant avec le compas, autant de fois que nécessaire, la corde déterminée par cet angle sur le cercle unité.*

– *Si* $\frac{\hat{2\pi}}{n}$ *et* $\frac{\hat{2\pi}}{m}$ *sont constructibles, alors,* m *et* n *étant premiers entre eux, d'après Claude-Gaspard Bachet de Méziriac, il existe* λ *et* μ *dans* $\mathbb{Z}$ *tels que* $\lambda n + \mu m = 1$*, d'où* $\frac{\hat{2\pi}}{mn} = \lambda\frac{\hat{2\pi}}{m} + \mu\frac{\hat{2\pi}}{n}$*. Il suffit alors de savoir construire la somme de deux angles constructibles, ce qui se fait en construisant des représentants de ces angles avec un côté adjacent.*

Lemme 3.4. *Si* $n \geq 3$ *se décompose en facteurs premiers de la façon suivante*

$$n = p_1^{\alpha_1}...p_k^{\alpha_k},$$

le polygone régulier à n *côtés est constructible si et seulement si les angles* $\frac{\hat{2\pi}}{p_1^{\alpha_1}}, ..., \frac{\hat{2\pi}}{p_k^{\alpha_k}}$ *le sont aussi.*

Preuve. *Ce lemme résulte immédiatement du lemme 3.3 précédent par récurrence sur* k*.*

Dans toute la suite, on pose $\zeta_t = e^{2i\pi/t}$, pour tout t. De plus, on notera $\zeta = \zeta_p$ par commodité d'écriture, p étant un nombre premier impair.

Théorème 3.4. *Avec les notations précédentes, on a :*

1. *Les angles de la forme* $\frac{\hat{2\pi}}{2^\alpha}$ *sont constructibles.*
2. *Si* p *est premier impair, alors* $\frac{\hat{2\pi}}{p^\alpha}$ *est constructible si et seulement si* $\alpha = 1$ *et* p *est un nombre de Fermat.*

Démonstration. *Le premier point est immédiat, par récurrence sur* α*, dès lors que l'on sait construire des bissectrices. Nous allons maintenant prouver le sens direct.*
Supposons que $\frac{\hat{2\pi}}{p^\alpha}$ *est constructible. Cela revient à dire que* ζ_{p^α} *est constructible. Par soucis de commodité, posons* $q = p^\alpha$*. La partie réelle d'un nombre constructible étant constructible, il vient que* $\cos(\frac{2\pi}{q})$ *est constructible, et d'après Wantzel, on a :*

$$[\mathbb{Q}(\cos\frac{2\pi}{q}) : \mathbb{Q}] = 2^m,\ m \in \mathbb{N}. \tag{13}$$

On a maintenant que ζ_q *est racine du polynôme* $X^q - 1$*. On a que le polynôme minimal de* ζ_q *sur* $\mathbb{Q}$ *est donné par :* $P(X) = \prod_{k=1}^{h}(X - \zeta_q^k)$*, résultat admis (car preuve longue et hors de propos). Pour trouver le degré* h *de* $P(X)$*, il suffit de connaitre le nombre d'entiers* k *tels que* $1 \leq k \leq q$*, et* k *premier avec* $q = p^\alpha$*.*
On obtient $h = p^{\alpha-1}(p-1)$*. Nous avons donc :*

$$[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = p^{\alpha-1}(p-1). \tag{14}$$

D'autre part, nous avons que $\zeta_q + \zeta_q^{-1} = 2\cos\frac{2\pi}{p^\alpha}$*, donc* $\cos\frac{2\pi}{p^\alpha} \in \mathbb{Q}(\zeta_q)$
et $\zeta_q^2 - 2\zeta_q\cos\frac{2\pi}{p^\alpha} + 1 = 0$*. Ainsi,* ζ_q *est algébrique et de degré* 2 *sur* $\mathbb{Q}(\cos\frac{2\pi}{p^\alpha})$*, d'où :*

$$[\mathbb{Q}(\zeta_q) : \mathbb{Q}(\cos\frac{2\pi}{p^\alpha})] = 2. \tag{15}$$

A partir des relations (13), (14) et (15), sachant que

$$[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = [\mathbb{Q}(\zeta_q) : \mathbb{Q}(\cos\frac{2\pi}{p^\alpha})] \times [\mathbb{Q}(\cos\frac{2\pi}{p^\alpha}) : \mathbb{Q}],$$

on obtient : $p^{\alpha-1}(p-1) = 2^{m+1}$*. Comme* p *est premier impair, il en résulte que* $\alpha = 1$ *et* $p = 1 + 2^{m+1}$*.*

Montrons à présent que $m+1$ est une puissance de 2. A partir de la décomposition en facteurs premiers, on obtient que $m+1 = \lambda 2^{\beta}$, avec $\beta \in \mathbb{N}$, et $\lambda \in \mathbb{N}^*$ impair. Or, si λ est impair, le polynôme $X^{\lambda}+1$ est divisible par $X+1$.
On a de plus que $p = 1+2^{m+1} = 1+(2^{2^{\beta}})^{\lambda}$, donc il en résulte que p est divisible par $1+2^{(2^{\beta})}$, mais comme p est premier, on a :

$$p = 1+2^{2^{\beta}}.$$

Ceci termine donc la première partie de la preuve du sens direct. Le sens indirect va, quant à lui nécessiter l'emploi des Sommes de Gauss, comme nous allons le voir dans la suite.

On rappelle le résultat du corollaire 2.2.1 de la partie 2.2.1 que l'on prolonge à $\mathbb{F}_p$.

Proposition 3.4. *Soit $x \in \mathbb{F}_p$, p étant un nombre premier. On a :*

$$\begin{aligned}
\sum_{\chi \in \hat{\mathbb{F}_p^*}} \chi(x) &= 1 \ \ si \ \ x = 0, \\
\sum_{\chi \in \hat{\mathbb{F}_p^*}} \chi(x) &= p-1 \ \ si \ \ x = 1, \\
\sum_{\chi \in \hat{\mathbb{F}_p^*}} \chi(x) &= 0 \ \ si \ \ x \neq 0,1.
\end{aligned}$$

Maintenant, par commodité d'écriture, et par soucis de clarté, nous allons introduire les Sommes Jacobi, fortement liées aux Sommes de Gauss comme nous l'allons voir tout à l'heure à travers deux propriétés dont nous aurons besoin pour démontrer le théorème de Gauss.

Définition 3.3. *Soient χ et λ des caractères sur $\mathbb{F}_p$. On note*

$$J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

$J(\chi,\lambda)$ est appelée Somme de Jacobi de χ et de λ.

Dans toute la suite, on considère la Somme de Gauss définie comme suit pour un caractère χ de $\mathbb{F}_p$.

$$g(\chi) = \sum_{x \ in \mathbb{F}_p} \chi(x)\zeta^x$$

Ainsi, on a $g(\chi) \cong \mathcal{G}(\chi,1)$, somme définie au paragraphe 2.3.3, que l'on prolonge à $\mathbb{F}_p$. Nous allons maintenant voir comment les Sommes de Gauss et de Jacobi sont liées à travers deux propositions.

Proposition 3.5. *Soient χ et λ des caractères non-triviaux sur $\mathbb{F}_p$. Si $\chi\lambda \neq 1$, alors :*

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Preuve. *On remarque que :*

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{x\in\mathbb{F}_p}\chi(x)\zeta^x\right)\left(\sum_{y\in\mathbb{F}_p}\lambda(y)\zeta^y\right) \\ &= \sum_{x,y\in\mathbb{F}_p}\chi(x)\lambda(y)\zeta^{x+y} \\ &= \sum_{t\in\mathbb{F}_p}\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)\zeta^t. \end{aligned} \tag{16}$$

Si $t=0$, alors $\sum_{x+y=0}\chi(x)\lambda(y)=\sum_{x\in\mathbb{F}_p}\chi(x)\lambda(-x)=\lambda(-1)\sum_{x\in\mathbb{F}_p}\chi\lambda(x)=0$, puisque $\chi\lambda\neq 0$ par hypothèse.
Si $t\neq 0$, soit x' et y' tels que $x=tx'$ et $y=ty'$. Si $x+y=t$, alors $x'+y'=1$. Ainsi,

$$\sum_{x+y=t}\chi(x)\lambda(y)=\sum_{x'+y'=1}\chi(tx')\lambda(ty')=\chi\lambda(t)J(\chi,\lambda).$$

En remplaçant dans l'équation (16), on obtient

$$g(\chi)g(\lambda)=\sum_{t\in\mathbb{F}_p}\chi\lambda(t)J(\chi,\lambda)\zeta^t=J(\chi,\lambda)g(\chi\lambda).$$

Proposition 3.6. *Supposons que $p\equiv 1\ (n)$ et que χ est un caractère d'ordre $n>2$. Alors :*

$$g(\chi)^n=\chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^{n-2}).$$

Preuve. *D'après le troisième point de la proposition précédente, nous avons que $g(\chi)^2=J(\chi,\chi)g(\chi^2)$. En multipliant des deux côtés par $g(\chi)$, on obtient que $g(\chi)^3=J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$. En continuant ainsi, on a que*

$$g(\chi)^{n-1}=J(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^{n-2})g(\chi^{n-1}). \tag{17}$$

De plus, on a que $\chi^{n-1}=\chi^{-1}=\overline{\chi}$. Ainsi, $g(\chi)g(\chi^{n-1})=g(\chi)g(\overline{\chi})=\chi(-1)p$, d'après les propriétés sur les caractères. On obtient le résultat en multipliant par $g(\chi)$ les deux membres de l'équation (17).

Maintenant, nous allons pouvoir prouver le théorème de Gauss sur les polygones réguliers constructibles.

3.3.3 Démonstration du Théorème de Gauss

Lemme 3.5. *ζ_{2^n} est constructible pour tout $n=1,2,...$.*

Preuve. *Il s'agit du premier point du théorème 3.4.*

Théorème 3.5. *Si p est un nombre de Fermat premier, alors ζ_p est constructible.*

Remarque: Dire que ζ_p est constructible revient à dire que l'angle $\frac{\hat{2\pi}}{p}$ l'est.

Démonstration. *Soit* $g(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta_p^t$ *la Somme de Gauss associée à* χ. *Alors*

$$\begin{aligned}\sum_{\chi\in\hat{\mathbb{F}_p^*}} g(\chi) &= \sum_{t=0}^{p-1}\left(\sum_{\chi\in\hat{\mathbb{F}_p^*}}\chi(t)\right)\zeta_p^t \\ &= 1+(p-1)\zeta_p.\end{aligned}$$

Ainsi, $\zeta_p = (p-1)^{-1}(-1+\sum_{\chi\in\hat{\mathbb{F}_p^*}} g(\chi))$ *et alors* ζ_p *est constructible si chaque* $g(\chi)$ *l'est, pour tout* $\chi \in \hat{\mathbb{F}_p^*}$.

De plus, il existe n *tel que* $p-1 = 2^n$ *car* p *est un nombre de Fermat, et puisque les caractères forment un groupe d'ordre* $(p-1)$, *il vient qu'il existe un* m *tel que* χ *soit d'ordre* 2^m. *Ensuite, d'après la proposition 3.6, on a que :*

$$g(\chi)^{2m} = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^l)$$

avec $l = 2^m - 2$. *Or, on a que* $J(\chi,\chi^j) \in \mathbb{Z}[\zeta_{2^n}]$, *quel que soit* j. *En effet, si* χ *est un caractère, alors* $\chi^{p-1} = 1$, *donc en particulier,* $\chi(x)$ *est une racine* $(p-1)$*-ième de l'unité, pour tout* $\chi \in \hat{\mathbb{F}_p^*}$, *et pour tout* $x \in \mathbb{F}_p$. *Ainsi, d'après le résultat du Lemme 3.5 précédent, il vient que* $g(\chi)^{2^m}$ *est constructible. On en déduit que* $g(\chi)$ *est constructible,* $\sqrt{\alpha}$ *étant constructible pour tout* α *qui l'est, ce qui achève la démonstration.*

Ce théorème permet alors de montrer le sens indirect du théorème 3.4. Nous avons alors tous les éléments pour prouver le Théorème de Gauss qui se déduit immédiatement du Théorème 3.4 et des Lemmes qui le précèdent.

Anecdote Les cinq premiers nombres de Fermat sont : $3, 5, 17, 257, 65537$, obtenus à partir de la formule $p = 1 + 2^{(2^\beta)}$ pour $b = 0, 1, 2, 3, 4$. Ces cinq nombres sont premiers, ce qui fut vérifié en 1640 par Pierre de Fermat (1601-1665). Mais Fermat avait affirmé aussi que tous les nombres de la forme $1 + 2^{(2^\beta)}$ sont des nombres premiers. C'est seulement en 1732 que Léonard Euler (1707-1783) s'aperçut que pour $\beta = 5$ le nombre de Fermat correspondant 4 294 967 297 n'était pas premier car divisible par 641. Bien que l'on ait étudié les nombres de Fermat pour de nombreuses valeurs de β, les seuls nombres de Fermat connus qui sont premiers sont les cinq nombres $3, 5, 17, 257, 65537$. Le problème de savoir s'il en existe d'autres est à l'heure actuelle un problème ouvert.

Pour $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20$ les polygones réguliers à n cotés sont constructibles, pour $n = 7, 9, 11, 13, 14, 18, 19$ ils ne le sont pas. Euclide connaissait les constructions pour $n = 3, 4, 5, 15$ et il savait bien sûr doubler le nombre de côtés d'un polygone constructible. On ne sût rien faire de mieux jusqu'en 1796 où K.F. Gauss, alors âgé de 19 ans, montra que le polygone régulier à 17 cotés était constructible.

Conclusion

Les Sommes de Gauss sont des objets mathématiques bien particuliers. Elles peuvent en effet avoir des applications dans de nombreux domaines différents. Qui pourrait penser qu'un somme de nombres complexes servirait à prouver si simplement un théorème d'arithmétique tel que celui de la réciprocité quadratique, ou encore à déterminer quels polygones réguliers sont constructibles, et même à connaitre le nombre de solutions d'équations diophantiennes. Nous avons vu à travers ce rapport, que les sommes de Gauss se rapprochaient également par certains aspects aux Séries de Fourier, et l'analogie n'est pas hors de propos. Ces objets sont donc tout à fait exceptionnels tant par leur profondeur que par l'étendue de leur champ d'application.
Nous tenons à remercier Mr. Mourougane qui nous aura encadré pendant toute la durée de nos travaux et qui nous aura donné d'excellentes pistes de recherches.

Références

[1] E.M. Wright G.H. Hardy. *An Introduction to the theory of numbers.* Fifth Edition.

[2] Marc Hindry. *Arithmétique.* Calvage & Mounet.

[3] Graduate Texts in Mathematics. *Théorie Algébrique des nombres.* Springer.

[4] Michael Rosen Kenneth Ireland. *A classical introduction to number theory.* Hardcover.

[5] Paulo Ribenboim. *L'arithmétique des corps.* Hermann Paris.

[6] Pierre Samuel. *Théorie Algébrique des nombres.* Hermann.

[7] Jean-Pierre Serre. *Cours d'Arithmétique.* Presse Universitaire de France.