2 Caractères de Dirichlet, sommes de Gauss et théorème de Dirichlet

Cette section n'est pas un développement mais plutôt un extrait de cours dont on peut extraire un ou plusieurs développements de longueur et de difficulté variable. Ce qui suit est tiré (librement) de [IR] et [Davenport]

2.1 Caractère de Dirichlet

Définition 2.1 (Caractère de Dirichlet)**.** Soit $m \geq 1$.

- Un *caractère de Dirichlet modulo* m est un morphisme de groupes $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$.
- Le *conducteur* du caractère χ est le plus petit diviseur $f \geq 1$ de m tel que χ se factorise en un morphisme de groupes $\overline{\chi} : (\mathbb{Z}/f\mathbb{Z})^* \to \mathbb{C}^*$ avec le morphisme surjectif canonique $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/f\mathbb{Z})^*$.
- Un caractère de Dirichlet χ modulo m définit une fonction totalement multiplicative sur $\mathbb{Z}$ (renotée χ) par $\chi(a) = \chi(\overline{a})$ si $(a, m) = 1$ et 0 sinon. Cette fonction dépend du choix de m et pas seulement du conducteur de χ.

Définition 2.2 (Sommes de Gauss)**.**

Soit χ un caractère de Dirichlet de conducteur f et $\zeta_f = e^{2i\pi/f}$. On définit alors pour tout $a \in \mathbb{Z}$ la *somme de Gauss*

$$G(a, \chi) = \sum_{k \in (\mathbb{Z}/f\mathbb{Z})} \chi(k)\zeta_f^{ak}.$$

Les sommes de Gauss vérifient les propriétés suivantes :

(a) Pour tout $a \in \mathbb{Z}$, $G(a, \chi) = \overline{\chi(a)}G(1, \chi)$.

(b) $G(1, \chi)G(1, \overline{\chi}) = \chi(-1)f$.

Démonstration.

(a) Soit $a \in \mathbb{Z}$. Si a et f sont premiers entre eux, $k \mapsto ak$ est une bijection de $\mathbb{Z}/f\mathbb{Z}$ donc

$$G(a, \chi) = \sum_{k \in (\mathbb{Z}/f\mathbb{Z})} \chi(a^{-1}k)\zeta_f^k = \chi(a^{-1}) \sum_{k \in (\mathbb{Z}/f\mathbb{Z})} \chi(k)\zeta_f^k = \overline{\chi(a)}G(1, \chi).$$

Sinon, $(a, f) = d > 1$, on note alors $a' = a/d$, $f' = f/d$, de sorte que

$$G(a, \chi) = \sum_{k \in (\mathbb{Z}/f\mathbb{Z})} \chi(k)e^{2i\pi a'k/f'} = \sum_{k' \in (\mathbb{Z}/f'\mathbb{Z})} \left(\sum_{\substack{k \in (\mathbb{Z}/f\mathbb{Z}) \\ k = k'[f']}} \chi(k) \right) e^{2i\pi a'k'/f'}$$

mais comme χ est de conducteur f, il existe $u \in (\mathbb{Z}/f\mathbb{Z})^*$ tel que $u = 1 \mod f'$ et $\chi(u) \neq 1$, alors

$$\chi(u) \sum_{\substack{k \in (\mathbb{Z}/f\mathbb{Z}) \\ k = k'[f']}} \chi(k) = \sum_{\substack{k \in (\mathbb{Z}/f\mathbb{Z}) \\ k = k'[f']}} \chi(uk) = \sum_{\substack{k \in (\mathbb{Z}/f\mathbb{Z}) \\ k = k'[f']}} \chi(k)$$

donc la somme ci-dessus est nulle, et $G(a, \chi) = 0 = \overline{\chi(a)}G(1, \chi)$ car $\chi(a) = 0$.

(b) D'après le (a), on a

$$\begin{aligned} G(1,\chi)G(1,\overline{\chi}) &= \sum_{k\in(\mathbb{Z}/f\mathbb{Z})} \overline{\chi(k)}G(1,\chi)\zeta_f^k \\ &= \sum_{k\in(\mathbb{Z}/f\mathbb{Z})} G(k,\chi)\zeta_f^k \\ &= \sum_{k,\ell\in(\mathbb{Z}/f\mathbb{Z})} \chi(\ell)\zeta_f^{k+k\ell} \\ &= \sum_{\ell\in(\mathbb{Z}/f\mathbb{Z})} \chi(\ell) \sum_{k\in\mathbb{Z}/f\mathbb{Z}} \zeta_f^{k(1+\ell)} \\ &= \chi(-1)f \end{aligned}$$

car la somme des f premières puissances d'une racine f-ième de l'unité est nulle à moins que celle-ci soit 1, auquel cas elle vaut f. □

Les sommes de Gauss ont de nombreuses applications, par exemple la formule de réciprocité quadratique.

Théorème (Réciprocité quadratique)**.** *Soient p, q deux nombres premiers impairs distincts, alors*

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

Démonstration. Notons χ le symbole de Legendre $\left(\frac{\cdot}{p}\right)$. C'est un caractères de Dirichlet de conducteur p (car p est impair) à valeurs dans ± 1. Posons

$$G := G\left(1,\chi\right).$$

D'après la propriété (b) des sommes de Gauss, on a

$$G^2 = \chi(-1)p.$$

Par ailleurs, dans l'anneau $A = \mathbb{Z}[\zeta_p]/q\mathbb{Z}[\zeta_p]$, l'application $x \mapsto x^q$ est additive, donc

$$G^q = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \chi(k)^q\zeta_p^{kq} = G\left(q,\chi\right) = \chi(q)G \mod q\mathbb{Z}[\zeta_p],$$

car $\chi^q = \chi$, q étant impair. Or, p est inversible dans A car A est isomorphe à $\mathbb{F}_q^p$ en tant qu'espace vectoriel, et donc G est inversible dans A, d'où

$$\left(\frac{q}{p}\right) = \chi(q) = G^{q-1} = (\chi(-1)p)^{(q-1)/2} = (-1)^{(p-1)/2\cdot(q-1)/2}\left(\frac{p}{q}\right) \mod q\mathbb{Z}[\zeta_p]$$

car $p^{(q-1)/2} = \left(\frac{p}{q}\right) \mod q$. On en déduit donc que

$$x = 1 - (-1)^{(p-1)/2\cdot(q-1)/2}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \in q\mathbb{Z}[\zeta_p]$$

c'est-à-dire que q divise chacun des coefficients de x dans la base canonique de $\mathbb{Z}[\zeta_p]$, or $x = 0, 1$ ou 2 et q est impair donc $x = 0$, ce qui prouve la réciprocité quadratique. □

Remarque. Cette preuve se trouve dans beaucoup d'ouvrages de référence de théorie des nombres, au détail près que $\mathbb{Z}[\zeta_p]$ est identifié comme l'anneau des entiers algébriques de $\mathbb{Q}(\zeta_p)$, mais ce n'est en rien nécessaire dans le raisonnement ci-dessus (et un peu technique à montrer par ailleurs).

Théorème (Polya-Vinogradov)**.** *Soit p un nombre premier impair. Alors, pour tous $m \neq n$ entiers :*

$$\left|\sum_{k=m}^{n}\left(\frac{k}{p}\right)\right| \leq \sqrt{p}\ln(p).$$

Démonstration. Notons $\chi = \left(\frac{\cdot}{p}\right)$. Grâce aux deux propriétés des sommes de Gauss,

$$\begin{aligned}
\sqrt{p}\left|\sum_{k=m}^{n}\chi(k)\right| &= \left|\sum_{k=m}^{n}\chi(k)G(1,\chi)\right| \\
&= \left|\sum_{k=m}^{n}G(k,\chi)\right| \\
&= \left|\sum_{k=m}^{n}\sum_{\ell=1}^{p-1}\chi(\ell)e^{2i\pi k\ell/p}\right| \\
&\leq \sum_{\ell=1}^{p-1}\left|\sum_{k=m}^{n}e^{2i\pi k\ell/p}\right|
\end{aligned}$$

car $\chi(0) = 0$ par définition. Maintenant,

$$\begin{aligned}
\left|\sum_{k=m}^{n}e^{2i\pi k\ell/p}\right| &= \left|\frac{1-e^{2i\pi(n-m+1)\ell/p}}{1-e^{2i\pi\ell/p}}\right| \\
&= \left|\frac{\sin((n-m+1)\ell\pi/p)}{\sin(\ell\pi/p}\right| \\
&\leq \frac{1}{|\sin(\ell\pi/p)|}.
\end{aligned}$$

Or, pour tout $x \in [0,1/2]$, par convexité de la fonction sinus sur ce domaine, $\sin(\pi x) \geq 2\langle x\rangle$ où $\langle x\rangle$ est la distance de x à $\mathbb{Z}$. Il en est de même pour $x \in [1/2,1]$ par symétrie de sinus en $\pi/2$ (faire un dessin). On a donc

$$\begin{aligned}
\left|\sum_{k=m}^{n}\chi(k)\right| &\leq \frac{1}{\sqrt{p}}\sum_{\ell=1}^{p-1}\frac{1}{2\langle\ell/p\rangle} \\
&\leq \frac{2}{\sqrt{p}}\sum_{\ell=1}^{(p-1)/2}\frac{p}{2\ell} \\
&\leq \sqrt{p}\sum_{\ell=1}^{(p-1)/2}\frac{1}{\ell}
\end{aligned}$$

Maintenant, pour tout $x \geq 1$, $1/x \leq \ln((2x+1)/(2x-1))$: en effet, cette inégalité est vraie pour $x = 1$, et on en déduit l'inégalité par comparaison des dérivées. On a donc finalement

$$\left|\sum_{k=m}^{n}\chi(k)\right| \leq \sqrt{p}\sum_{\ell=1}^{(p-1)/2}\ln((2\ell+1)/(2\ell-1)) \leq \sqrt{p}\ln(p).$$

□

Remarque. Un corollaire évident de cette inégalité est que le premier résidu non quadratique modulo p est au plus $\sqrt{p}\ln(p)$, mais Polya-Vinogradov est inutile (et même non optimal) pour cela : en effet, soit m le plus petit résidu non-quadratique modulo p et n le premier entier tel que

$mn \geq p$. Alors, $m(n-1) < p$ donc $mn - p < m$ et est donc un carré modulo p, d'où n n'en est pas un, ce qui prouve que $n \geq m$ par hypothèse, ainsi $m(m-1) < p$ donc $m < \sqrt{p} + 1$.

Des applications intéressantes de Polya-Vinogradov sont donc plutôt à chercher du côté de majorations explicites de certaines sommes utilisant des caractères de Dirichlet, en utilisant une transformée d'Abel.

Une application majeure des caractère de Dirichlet est le théorème de Dirichlet sur la répartition des nombres premiers par classe de congruence, dont on démontre ici une version non quantitative, en admettant la partie technique, à savoir la non-annulation des fonctions L en 1.

Théorème (Dirichlet)**.** *Soient $a, b \in \mathbb{N}^*$ premiers entre eux, $b \geq 3$.*
Alors, il existe une infinité de nombres premiers congrus à a modulo b.

Soit χ un caractère de Dirichlet modulo b, on le note χ_0 si c'est le caractère trivial.
On définit la série de Dirichlet L associée à χ par la formule

$$L(s, \chi) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

Pour tout $\sigma > 1$, cette série converge uniformément sur tout domaine de la forme $\operatorname{Re} s \geq \sigma$,$\sigma > 1$, car

$$\sum_{n=1}^{+\infty} \frac{1}{n^\sigma} \leq 1 + \int_1^{+\infty} x^{-\sigma} dx < 1 + \frac{1}{(\sigma - 1)} < +\infty.$$

Elle définit donc une fonction holomorphe sur le domaine $\operatorname{Re} s > 1$. Plus précisément, si $\chi \neq \chi_0$, par transformation d'Abel,

$$\sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{+\infty} S_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$$

avec $S_n = \sum_{k=1}^{+\infty} \chi(k)$, or S_n est b-périodique car χ est non trivial, et donc bornée, et pour tout $\sigma > 0$ et s tel que $\operatorname{Re} s \geq \sigma$,

$$\sum_{n=1}^{+\infty} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| \leq \sum_{n=1}^{+\infty} \frac{1}{n^\sigma} \left| 1 - (1 + 1/n)^{-\sigma} \right| \leq \sum_{n=1}^{+\infty} \frac{1}{\sigma n^{\sigma+1}}$$

converge donc uniformément sur $\operatorname{Re} s \geq \sigma$, ainsi $L(s, \chi$ se prolonge analytiquement en une fonction holomorphe sur $\operatorname{Re} s > 0$. Dans le cas où $\chi = \chi_0$, pour tout $s > 1$ réel,

$$L(s, \chi) = \sum_{\substack{n \geq 1 \\ (b,n)=1}} \frac{1}{n^s} \geq \sum_{n=1}^{+\infty} \frac{1}{(bn+1)^s} \geq \frac{1}{b} \sum_{n=1}^{+\infty} \frac{1}{n^s} \geq \frac{1}{b(s-1)}$$

donc tend vers $+\infty$ lorsque s tend vers 1.

De plus, comme χ est une fonction totalement multiplicative sur $\mathbb{Z}$, pour tout nombre premier p,

$$(1 - \chi(p)p^{-s}) L(s, \chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} - \sum_{n=1}^{+\infty} \frac{\chi(np)}{(np)^s} = \sum_{\substack{n \geq 1 \\ (p,n)=1}} \frac{\chi(n)}{n^s}$$

Notons $\mathcal{P}$ l'ensemble des nombres premiers. Le produit eulérien $\prod_{p \in \mathcal{P}} (1 - \chi(p)p^{-s})$ converge uniformément sur tout domaine de la forme $\operatorname{Re} s \geq \sigma$,$\sigma > 1$, et en multipliant successivement $L(s, \chi)$ par chacun de ses facteurs, d'après la formule ci-dessus on obtient finalement

$$L(s, \chi) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \chi(p)p^{-s}}$$

pour tout s tel que $\operatorname{Re} s > 1$. De plus, pour tout nombre premier p, avec la définition usuelle du logarithme par série entière, on a

$$\log(1 - \chi(p)p^{-s}) = -\sum_{k=1}^{+\infty} \frac{\chi(p^k)}{kp^{ks}}$$

et on a donc $L(s,\chi) = e^{F(s,\chi)}$ avec

$$F(s,\chi) = \sum_{p\in\mathcal{P}} \sum_{k=1}^{+\infty} \frac{\chi(p^k)}{kp^{ks}}$$

Soit G le groupe des caractères de Dirichlet modulo b. Pour a premier à b et tout $n \in \mathbb{N}$, on a alors

$$\sum_{\chi\in G} \overline{\chi(a)}\chi(n) = \sum_{\chi\in G} \chi(a^{-1}n)$$

et ceci vaut $|G|$ lorsque $a = n \mod b$, et 0 sinon (c'est la somme des valeurs du caractère sur G d'évaluation en $a^{-1}n$). On en déduit donc que

$$\begin{aligned} F(s) := \sum_{\chi\in G} \overline{\chi(a)}F(s,\chi) &= \sum_{\substack{(p,k)\in\mathcal{P}\times\mathbb{N}^* \\ p^k = a[b]}} \frac{\varphi(b)}{kp^{ks}} \\ &= \varphi(b) \sum_{\substack{p\in\mathcal{P} \\ p=a[b]}} \frac{1}{p^s} + R(s) \end{aligned}$$

où, la série $R(s)$ est définie par

$$R(s) = \sum_{\substack{(p,k)\in\mathcal{P}\times\mathbb{N}_{\geq 2} \\ p^k = a[b]}} \frac{\varphi(b)}{kp^{ks}}$$

cette série convergant uniformément sur $\operatorname{Re} s \geq 3/4$, car sur ce domaine,

$$\sum_{\substack{(p,k)\in\mathcal{P}\times\mathbb{N}_{\geq 2} \\ p^k = a[b]}} \frac{1}{k|p^{ks}|} \leq \sum_{p\in\mathcal{P}} \frac{p^{-2\operatorname{Re} s}}{1 - p^{-\operatorname{Re} s}} \leq \frac{1}{1 - 2^{-3/4}} \sum_{n=1}^{+\infty} \frac{1}{n^{2s}} < +\infty.$$

En conséquence, R est une fonction holomorphe sur ce domaine.

On admet que pour χ non trivial, $L(1,\chi) \neq 0$. Alors, $F(s,\chi)$ est borné au voisinage (à droite) de 1 : en effet, $L(s,\chi) = e^{F(s,\chi)}$ tend vers une constante non nulle λ quand $s \to 1$, est borné non nul au voisinage de 1, donc si on choisit une détermination $\log\lambda$ $F(s,\chi)$ est proche de $\log\lambda + 2ik\pi, k \in \mathbb{Z}$ quand s est proche de 1, donc par continuité de $F(s,\chi)$ ce k est indépendant de s lorsque s est assez proche de 1 donc $F(s,\chi)$ est bornée au voisinage de 1 si $\chi \neq \chi_0$. Pour le caractère trivial, comme le module de $L(s,\chi_0)$ tend vers l'infini lorsque s tend vers 1, $F(s,\chi_0)$ ne peut pas être borné au voisinage de 1. Comme $\chi_0(a)$ est non nul car a est premier à b, $F(s)$ est donc la somme d'un terme non borné et de termes bornés au voisinage de 1, donc n'est pas borné au voisinage de 1, or R l'est donc que la somme des $1/p^s$ pour $p = a \mod b$ premier ne l'est pas au voisinage de 1, donc en particulier l'ensemble de ces nombres premiers est infini.

Remarque. L'essentiel de la preuve du théorème de Dirichlet consiste donc à montrer que $L(s,\chi)$ tend vers une limite finie non nulle lorsque s tend vers 1. En fait, ces fonctions (sauf pour χ_0 se prolongent analytiquement à $\operatorname{Re} s > 0$, et il reste donc à montrer que $L(1,\chi) \neq 0$ pour tout caractère non trivial.

Le raisonnement ci-dessus peut éventuellement faire l'objet d'un développement (en supposant l'assertion ci-dessus), mais je l'ai présenté égalemnt pour donner l'esquisse de la preuve d'un

résultat majeur utilisant les caractères de Dirichlet, qui peut donc s'écrire (en précisant que c'est surtout culturel) dans un plan de leçon.

Une référence complète pour le théorème de Dirichlet est le chapitre 4 de [Davenport].

Leçons liées aux caractères de Dirichlet et aux sommes de Gauss :

102 Groupe des nombres complexes de module 1, sous-groupe des racines de l'unité. Applications

110 Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications

120 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

121 Nombres premiers. Applications (surtout le théorème de Dirichlet)