# La formule du nombre de classes pour les corps quadratiques.

Benjamin Schraen

8 juin 2004

## 1 Séries de Dirichlet.

**Définition 1** *On appelle série de Dirichlet une série de la forme* $f(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ *où* $a_n \in \mathbb{C}$ *et* $s \in \mathbb{C}$.

Soit $f(s) = \sum \frac{a_n}{n^s}$ une série de Dirichlet. Posons pour $x > 0$, $s(x) = \sum_{n\leq x} a_n$, et si $\sigma \in \mathbb{R}$, $D(\sigma) = \{s \in \mathbb{C}, \Re(s) > \sigma\}$.

**Proposition 1** *Si* $s(x) \leq ax^b$ *avec* $a$ *et* $b$ *réels positifs,* $f(s)$ *converge et est analytique sur* $D(b)$.

Preuve : Soient $\delta > 0$ et $0 < \epsilon < \frac{\pi}{2}$. Posons $D(b,\delta,\epsilon) = \left\{s \in \mathbb{C}, \Re(s) \geq b + \delta, |\arg(s-b)| \leq \frac{\pi}{2} - \epsilon\right\}$. On va montrer que la série converge uniformément sur tout ensemble de la forme $D(b,\delta,\epsilon)$. La limite uniforme d'une suite de fonctions analytiques étant analytique, on aura que $f$ converge et est analytique sur tout $D(b,\delta,\epsilon)$. Comme $D(b)$ est une union de tels ensembles, on a le résultat. Fixons donc $\delta$ et $\epsilon$ et soit $s \in D(b,\delta,\epsilon)$. Posons $\sigma = \Re(s)$ et $s - b = |s-b|e^{i\theta}$

$$\begin{aligned}
\sum_{n=N}^{N+p} \frac{a_n}{n^s} &= \sum_{n=N}^{N+p} \frac{s(n) - s(n-1)}{n^s} \\
&= \sum_{n=N}^{N+p} \frac{s(n)}{n^s} - \sum_{n=N-1}^{N+p-1} \frac{s(n)}{(n+1)^s} \\
&\leq \sum_{n=N}^{N+p-1} |s(n)| \left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| + \frac{|s(N-1)|}{N^\sigma} + \frac{|s(N+p)|}{(N+p)^\sigma} \\
&\leq \frac{2a}{N^\delta} + \sum_{n=N}^{N+p-1} an^b|s| \left|\int_n^{n+1} \frac{dt}{t^s}\right| \\
&\leq \frac{2a}{N^\delta} + a|s| \int_N^{+\infty} \frac{dt}{t^{\sigma-b+1}} \\
&\leq \frac{2a}{N^\delta} + \frac{a|s|}{(\sigma-b)N^{\sigma-b}} \\
&\leq \frac{2a}{N^\delta} + a\frac{|s-b|+|b|}{(\sigma-b)N^{\sigma-b}} \\
&\leq \frac{1}{N^\delta}\left(2a + \frac{1}{\cos(\theta)} + \frac{|b|}{\delta}\right) \\
&\leq \frac{1}{N^\delta}\left(2a + \frac{1}{\sin(\epsilon)} + \frac{|b|}{\delta}\right)
\end{aligned}$$

D'où la convergence uniforme...

Exemples :
- Si on prend $a_n = 1$ pour tout $n$, on obtient la fonction $\zeta$ qui est donc analytique sur $D(1)$.
- Si $a_n = (-1)^{n+1}$, on obtient la série $\zeta_2$ qui est analytique sur $D(0)$.

**Proposition 2** *Si $s(x) = a_0 x + O(x^{1-d})$, $f$ admet un prolongement méromorphe à $D(1-d)$ avec un pôle simple en 1 de résidu $a_0$.*

Preuve : Montrons d'abord ce résultat pour la fonction $\zeta$. En effet pour $\Re(s) > 1$, on a $\zeta_2(s) = \sum \frac{1}{n^s} - 2\sum_{n\geq 1} \frac{1}{(2n)^s}$. Ainsi $\zeta(s) = \left(1 - \frac{1}{2^{s-1}}\right)^{-1} \zeta_2(s)$, et on a bien un prolongement méromorphe de $\zeta$ à $D(0,0,0)$. Déterminons le résidu en 1 :
pour $n \geq 2$ et $s > 1$, $\int_n^{n+1} \frac{dt}{t^s} \leq \frac{1}{n^s} \leq \int_{n-1}^{n} \frac{dt}{t^s}$. On voit ainsi que $(s-1)\zeta(s)$ tend vers 1 quand $s$ tend vers 1 avec $s$ réel strictement supérieur à 1. On a ainsi le résidu.
Soit maintenant $f$ une série de Dirichlet avec les hypothèses de la proposition. Il suffit d'appliquer la proposition 1 à la série $\sum \frac{a_n - a_0}{n^s}$ qui est ainsi analytique sur $D(1-d)$ et on conclut grâce au résultat pour $\zeta$.

On considère désormais $K$ un corps quadratique. Pour démontrer la formule des classes, l'idée va être de considérer la fonction $\zeta_K$ de Dedekind, définie par la série

$$\zeta_K(s) = \sum_{I \in \mathcal{I}} \frac{1}{NI^s}$$

où $\mathcal{I}$ désigne l'ensemble des idéaux entiers de $\mathcal{O}_K$.
Comme dans le cas des entiers $\mathbb{Z}$, on a un développement en produit eulérien. On note désormais $\mathcal{P}$ l'ensemble des idéaux premiers de $\mathcal{O}_K$.

**Théorème 1** *Le produit infini $\Pi_{\wp \in \mathcal{P}} \left(1 - \frac{1}{N\wp^s}\right)$ converge pour $\Re(s) > 1$. Ainsi la série $\zeta_K$ converge et est analytique sur $D(1)$. De plus pour $\Re(s) > 1$, $\zeta_K(s) = \Pi_{\wp \in \mathcal{P}} \left(1 - \frac{1}{N\wp^s}\right)^{-1}$.*

Preuve : Soit $\Re(s) > 1$. Si $p$ est un nombre premier, il y au plus deux idéaux premiers de $\mathcal{O}_K$ au-dessus de $p$. De plus les normes de ces idéaux sont des puissances de $p$. Ainsi $\sum_{\wp \in \mathcal{P}} \frac{1}{N\wp^{\Re(s)}} \leq 2\sum_p \frac{1}{p^{\Re(s)}}$ et on sait bien que cette dernière série converge. Le produit converge donc aussi, et le théorème de factorisation unique dans les anneaux de Dedekind nous montre que la série $\zeta_K$ est également convergente en même temps que la formule.

# 2 Estimation moyenne des coefficients.

Nous allons ici nous attacher à estimer la valeur moyenne des coefficients de $\zeta_K$ afin d'obtenir des information sur son comportement au voisinage de 1. On note $\zeta_K(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ pour $\Re(s) > 1$ et $s(n) = a_1 + \cdots + a_n$. $s(n)$ est donc le nombre d'idéaux entiers de $\mathcal{O}_K$ dont la norme est inférieure à $n$.

On rappelle que le groupe des classes $C_K$ de $\mathcal{O}_K$ est fini et on note $h_K$ son cardinal. Si $c \in C_K$, on note alors $s(n,c)$ le nombre d'idéaux entiers de la classe $c$ de norme inférieure à $n$. Désormais on fixe une classe $c \in C_K$.

**Lemme 1** *Il existe un idéal entier de $\mathcal{O}_K$ dans la classe $c^{-1}$.*

Preuve : Soit $I$ et $J$ deux idéaux entiers tels que $IJ^{-1} \in c^{-1}$. Alors comme $J^{h_K}$ est principal, $IJ^{h_K-1}$ est entier et dans la classe $c^{-1}$.

On fixe désormais un élément entier $I_0$ dans la classe $c^{-1}$.

**Lemme 2** *$s(n,c)$ est égal aux nombre d'idéaux principaux $(\alpha)$ avec $\alpha \in I_0$ et $|N\alpha| \leq nNI_0$.*

Preuve : En effet si $I$ est un idéal entier de la classe $c$. Alors $II_0$ est un idéal de la classe nulle, donc $II_0 = (\alpha)$ et il est clair que $\alpha \in I_0$. De plus $(\alpha)$ détermine entièrement $I$ et l'inégalité sur les normes est évidente. Réciproquement si $\alpha \in I_0$ avec $|N\alpha| \leq nNI_0$, alors $I = (\alpha)I_0^{-1}$ est entier, dans la classe $c$, et de norme inférieure à $n$.

On a donc montré $s(n,k) = |\{\alpha \in I_0, |N\alpha| \leq nNI_0\}/\mathcal{O}_K^*|$. Nous devons maintenant distinguer deux cas suivant que $K$ est un corps quadratique réel ou complexe. Posons désormais $N = NI_0$.

## 2.1 Le cas complexe.

On sait que dans ce cas le groupe $\mathcal{O}_K^*$ est un groupe fini constitué des racines de l'unité présentes dans $K$. Notons $w_K$ son cardinal. Si $K = \mathbb{Q}[i]$, $w_K = 4$, si $K = \mathbb{Q}[i\sqrt{3}]$, $w_K = 6$ et dans tous les autres cas $w_K = 2$ et $\mathcal{O}_K^*$ est réduit à $\{-1,1\}$.
On a $w_K s(n,c) = I_0 \cap \overline{B(0,\sqrt{Nn})}$ où $\overline{B(0,\sqrt{n})}$ désigne la boule de centre 0 et de rayon $\sqrt{n}$. De plus dans ce cas, $I_0$ est un réseau de $\mathbb{C}$ dont le volume élémentaire est $\frac{\sqrt{N|\delta_K|}}{2}$ où $\delta_K$ est le discriminant du corps $K$. Notons $d$ la plus petite distance entre deux points du réseau $I_0$, $P$ un parallélogramme élémentaire du réseau. $A = \{z \in I_0, z + P \subset \overline{B(0,\sqrt{Nn})}\}$, $B = \{z \in I_0, z + P \cap \overline{B(0,\sqrt{Nn})} \neq \varnothing\}$. On a alors $|A| \leq w_K s(n,c) \leq |B|$. De plus $\bigcup_{z\in B} z + P \subset \overline{B(0,\sqrt{Nn}+d)}$ et $\overline{B(0,\sqrt{Nn}-d)} \subset \bigcup_{z\in A} z + P$. Ainsi $|B|\text{vol}(P) \leq \pi(\sqrt{Nn}+d)^2$ et $|A|\text{vol}(P) \geq \pi(\sqrt{Nn}-d)^2$. Comme $\text{vol}(P) = \frac{N\sqrt{|\delta_K|}}{2}$, on a $s(n,c) = \frac{2\pi}{\sqrt{|\delta_K|}w_k}n + O(\sqrt{n})$.

## 2.2 Le cas réel.

On note $K = \mathbb{Q}[\sqrt{d}]$ où $d$ est entier sans facteur carré.
La difficulté vient ici du fait que le groupe $\mathcal{O}_K^*$ est plus gros que dans le cas complexe.

**Théorème 2** *Il existe $\epsilon > 1$ tel que $\mathcal{O}_K^* = \{\pm\epsilon^n, n \in \mathbb{Z}\}$.*

Preuve : La première chose à faire est de montrer l'existence d'une unité de norme $> 1$. Pour cela nous utiliserons ce lemme :
**Lemme 3** *Soit $x$ un irrationnel. Il existe une infinité d'entiers naturels $p$ et $q$ tels que $\left|x - \frac{p}{q}\right| \leq \frac{1}{q^2}$.*
Preuve du lemme : Fixons un élément $N \in \mathbb{N}^*$ et considérons les $N+1$ éléments $nx - \text{E}(nx)$ pour $n$ variant entre 0 et $N$. Ces $N+1$ éléments sont tous dans l'intervalle $[0,1[$ que l'on peut découper en $N$ intervalles $[\frac{n}{N},\frac{n+1}{N}[$ avec $n$ variant entre 0 et $N-1$. Il existe donc deux de ces éléments dans le même sous-intervalle, disons pour les valeurs $a$ et $b$ de $n$, $a < b$. Ainsi $|(b-a)x-(\text{E}(bx)-\text{E}(ax))| \leq \frac{1}{N}$. En posant $q = b-a$ et $p = \text{E}(bx)-\text{E}(ax)$, on a $\left|x - \frac{p}{q}\right| < \frac{1}{qN} \leq \frac{1}{q^2}$.
Or comme $x$ est irrationnel, il existe un entier $N_1$ tel que $\frac{1}{N_1} < |qx - p|$. On obtient par la même méthode que précédemment $p_1$ et $q_1$ différents de $p$ et $q$ vu que $|q_1x - p_1| < \frac{1}{N_1} < |qx - p| < \frac{1}{N}$, en répétant cette construction on a une infinité de couples $(p,q)$.

On applique ce lemme en choisissant $x = \sqrt{d}$, il existe donc une infinité de couples $(p,q)$ vérifiant $|qx-p| < \frac{1}{q}$. Or un tel couple vérifie aussi $|qx+p| < \frac{1}{q} + 2qx$ d'où $|p^2 - xq^2| < 2x+1$. Le lemme nous dit donc qu'il existe une infinité de couples $(p,q)$ vérifiant $|p^2 - xq^2| < 2x+1$. On peut ainsi choisir deux tels couples $(x_1,y_1)$ et $(x_2,y_2)$ tels que $N(x_1 + xy_1) = N(x_2 + xy_2) = M \neq 0$, $x_1 \equiv x_2\,[M]$, $y_1 \equiv y_2\,[M]$ et $y_1 \neq y_2$. Posons alors $a+bx = (x_1+y_1x)(x_2-y_2x)$. $a = x_1x_2 - dy_1y_2$ et $b = x_1y_2 - x_2y_1$. Les propriétés de congruences imposées assurent que $M|b$ et $M|a$. Posons $a = Ma'$ et $b = Mb'$. Il est clair que $N(a+xb) = M^2$, donc $N(a'+xb') = 1$. De plus $|a'+xb'| \neq 1$, en effet comme $y_1 \neq y_2$, $x_2 - xy_2$ n'est pas l'inverse de $x_1 + xy_1$ et ce n'est pas l'opposé de son inverse non plus car $y_1 \neq -y_2$ vu que $y_1$ et $y_2$ sont entiers naturels. Quitte à prendre l'opposé ou l'inverse de $a' + xb'$ on a bien montré qu'il existe une unité $> 1$ dans $K$.
Il suffit maintenant pour conclure de prouver que les unités positives de $K$ forment un sous-groupe discret de $\mathbb{R}_+^*$. En effet si $M > 0$ et si $a + xb$ est une unité de $K$ comprise entre $\frac{1}{M}$ et $M$, alors comme $|a - xb| = \frac{1}{|a+xb|}$, il en est de même de son conjugué. Soit alors $P$ le polynôme minimal sur $\mathbb{Q}$ de $a + xb$. Ses coefficients sont alors des entiers bornés par $2M$ et $M^2$. Ainsi on ne peut construire qu'un nombre fini de tels polynômes et il n'y a qu'un nombre fini d'unités de $K$ dans $[\frac{1}{M},M]$, le groupe est donc discret et le théorème est démontré.

Remarque : Ce résultat est en fait un cas particulier d'un théorème plus général et plus difficile de Dirichlet.

**Théorème 3 (Dirichlet)** *Soit $K$ un corps de nombres de dimension $d$ sur $\mathbb{Q}$. Soit $r_1$ le nombres de morphismes de $K$ dans $\mathbb{R}$ et $r_2 = \frac{d-r_1}{2}$. Alors le groupe des unités $\mathcal{O}_K^*$ de $K$ est isomorphe à $U_K \times \mathbb{Z}^{r_1+r_2-1}$ où $U_K$ est le groupe (cyclique) des racines de l'unité présentes dans $K$.*

On appelle désormais dans la suite $\epsilon$ l'unité fondamentale du corps $K$. On fixe $(\alpha_1,\alpha_2)$ une $\mathbb{Z}$-base de $I_0$. On pose aussi pour $a + b\sqrt{d} \in K$, $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. On définit alors pour $x \in \mathcal{O}_K$, $v(x) = (x,\sigma(x)) \in \mathbb{R}^2$. $\mathcal{O}_K$ et $I_0$ s'identifient alors par $v$ à des réseaux de $\mathbb{R}^2$ de volumes élémentaires respecrifs $\sqrt{\delta_K}$ et $N\sqrt{\delta_K}$. Pour $(x,y) \in \mathbb{R}^{*2}$, on pose $l(x,y) = (\ln|x|, \ln|y|) \in \mathbb{R}^2$.

L'application $l$ est appelé plongement logarithmique, étudions ses propriétés. Notons $H$ l'hyperplan de $\mathbb{R}^2$ défini par $x + y = 0$. Il est clair que $x \in \mathcal{O}_K^*$ si et seulement si $l(x) \in H$. Comme de plus $\epsilon > 1$, $l(\epsilon)$ forme une base de $H$. Ainsi pour tout $x \in I_0\backslash\{0\}$, $l(x) = cW + c_1 l(\epsilon)$ où $W = (1,1)$ et $c$ et $c_1$ sont réels. Si $x \in I_0\backslash\{0\}$ il existe exactement deux $y$ associés à $x$ tels que $l(y) = cW + c_1 l(\epsilon)$ avec $c_1 \in [0,1[$.

Ainsi on a $2s(n,c) = |\{x \in I_0, |x\sigma(x)| \leq Nn, l(x) = cW + c_1 l(\epsilon), c_1 \in [0,1[\}$. Remarquons que $2c = \ln(|x\sigma(x)|)$. Ainsi $c_1 \in [0,1[$ si et seulement si $1 \leq \left|\frac{x}{\sigma(x)}\right| \leq \epsilon^2$. Posons donc $B(n) = \{(x,y) \in \mathbb{R}^2, |x||y| \leq n, |y| \leq |x| < \epsilon^2|y|\}$. D'après ce qui précède $2s(n,c) = |I_0 \cap v^{-1}B(Nn)|$. Pour conclure comme dans la partie précédente, il suffit maintenant de calculer le volume $\mathrm{vol}(B(n))$.

$$\begin{aligned}
\mathrm{vol}(B(n)) &= 4\int_0^{\frac{\sqrt{n}}{\epsilon}} \int_y^{\epsilon^2 y} dx\,dy + 4\int_{\frac{\sqrt{n}}{\epsilon}}^{\sqrt{n}} \int_y^{\frac{n}{y}} dx\,dy \\
&= 4\int_0^{\frac{\sqrt{n}}{\epsilon}} (\epsilon^2 - 1)y\,dy + 4\int_{\frac{\sqrt{n}}{\epsilon}}^{\sqrt{n}} (\frac{n}{y} - y)\,dy \\
&= 4n\ln(\epsilon)
\end{aligned}$$

Par un encadrement semblable à celui de la section précédente, on obtient :

$$s(n,c) = \frac{2\ln(\epsilon)}{N\sqrt{\delta_K}} Nn + O(\sqrt{n}) = \frac{4\ln(\epsilon)}{\sqrt{\delta_K} w_K} n + O(\sqrt{n})$$

vu que dans le cas réel $w_K = 2$.

## 2.3 Conclusion.

En fait $s(n,c)$ est asymptotiquement indépendant de $c$, on a donc montré le résultat suivant :
**Théorème 4** *La fonction $\zeta_K$ se prolonge en une fonction méromorphe sur $D(\frac{1}{2})$ et*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \begin{cases} \frac{4\ln(\epsilon)h_K}{\sqrt{\delta_K}w_K} & \textit{dans le cas réel} \\ \frac{2\pi h_K}{\sqrt{|\delta_K|}w_k} & \textit{dans le cas complexe} \end{cases}$$

Remarque : En fait il a été prouvé que $\zeta_K$ se prolonge en une fonction méromorphe sur $\mathbb{C}$ tout entier et qu'elle a un unique pôle simple en 1. On vient de voir que le résidu en ce pôle est très lié au nombre de classes $h_K$. Il est également vrai que $\zeta_K$ a une équation fonctionnelle proche de celle de la fonction $\zeta$ de Riemann.
Pour des corps de nombres de dimension supérieure, ces résultats restent vrais et le résidu en 1 vaut $\frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)h_K}{w_K\sqrt{|\delta_K|}}$ où $r_1$ et $r_2$ ont déjà été définis dans la remarque sur le théorème de Dirichlet et $\mathrm{reg}(K)$ est le volume élémentaire de $\mathcal{O}_K^*$ vu comme réseau de $H$ via le plongement logarithmique $l$.

# 3 La formule analytique du nombre de classes.

Rappelons quelques résultats sur la ramification dans un corps quadratique. Soit $p$ un nombre premier impair.

- Si $p$ divise $\delta_K$, $p$ est totalement ramifié dans $K$. Il existe donc un unique $\wp$ premier au-dessus de $p$ et $N\wp = p$.
- Si $\left(\frac{|\delta_K|}{p}\right) = 1$, $p$ est totalement décomposé, et il existe $\wp$ premier tel que $p = \wp\overline{\wp}$ et $N\wp = p$.
- Si $\left(\frac{|\delta_K|}{p}\right) = -1$, $(p)$ est un idéal premier de $\mathcal{O}_K^*$ et $N(p) = p^2$.

Étudions aussi le cas de 2, si $2|D$ alors 2 est totalement ramifié, sinon $d \equiv 1\,[4]$ et 2 est totalement décomposé si et seulement si $X^2 - X - \frac{d-1}{4}$ est réductible dans $\mathbb{F}_2$, c'est à dire si et seulement si $d \equiv 1\,[8]$.

On peut résumer ces résultats de cette façon : pour $p$ premier,

$$\prod_{\wp|p}\left(1 - \frac{1}{N\wp^s}\right) = \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{\chi(p)}{p^s}\right)$$

où $\chi(p) = \left(|\frac{\delta_K|}{p}\right)$ lorsque $p$ est un nombre premier impair et $\chi(2) = (-1)^{\frac{d-1}{4}}$ si et $d$ est congru à 1 modulo 4 et $\chi(2) = 0$ sinon. On étend alors $\chi$ à $\mathbb{N}^*$ par multiplicativité.

Nous allons maintenant introduire la notion de caractère de Dirichlet. Il est fondamental ici que l'application $\chi$ ainsi définie est un caractère de Dirichlet.
**Définition 2** *Soit $N \in \mathbb{N}^*$. On appelle caractère de Dirichlet modulo $N$ un morphisme $\chi$ de $\mathbb{Z}/NZ^*$ dans $\mathbb{C}^*$. On l'étend alors à $\mathbb{Z}/N\mathbb{Z}$ en posant $\chi(a) = 0$ lorsque $a$ n'est pas premier à $N$ puis à $\mathbb{Z}$ par $N$-périodicité. On notera alors également $\chi$ la nouvelle application ainsi définie.*

**Définition 3** *Un caractère de Dirichlet modulo $N$ est dit primitif s'il n'existe pas de diviseur $d$ de $N$, $1 \leq d < N$ tel que $\chi$ se factorise en un morphisme de $\mathbb{Z}/d\mathbb{Z}^*$ dans $\mathbb{C}^*$. Il revient au même de dire que pour tout diviseur strict $d$ de $N$ il existe un entier $a$ premier à $N$ et congru à 1 modulo $d$ tel que $\chi(a) \neq 1$.*

**Théorème 5** *L'application $\chi$ attachée au corps quadratique $K$ est un caractère de Dirichlet primitif modulo $D = |\delta_K|$. De plus $\chi(-1) = 1$ si et seulement si $K$ est réel.*

Nous ne démontrons pas ce théorème qui est fondamental pour ce qui va suivre. En effet nous pourrions le prouver de manière élémentaire (mais en disjoignant beaucoup de cas) au moyen de la loi de réciprocité quadratique. Cependant il est beaucoup plus agréable de le voir comme conséquence du plongement de $K$ dans le corps cyclotomique $\mathbb{Q}[\zeta_D]$, on peut alors conclure en caractérisant la ramification des différents premiers au moyen des Frobenius (et l'on retrouve au passage la loi de réciprocité quadratique). Ce résultat sera peut-être démontré dans un éventuel exposé sur la ramification.

Nous utilisons maintenant le caractère $\chi$ pour construire une fonction $L$.

**Définition 4** *La fonction L associée au caractère $\chi$ est la série de Dirichlet définie par $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$.*

La proposition 1 nous montre que si $\chi$ n'est pas le caractère valant 1 partout, $L(.,\chi)$ est convergente et analytique sur $D(0)$. Le fait que $\chi$ soit un caractère de Dirichlet nous permet d'écrire $L(s,\chi)$ comme un produit eulérien, la preuve est exactement la même que celle du théorème 1 :

**Théorème 6** *Pour $\Re(s) > 1$, on a*

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Les rappels sur la ramification et la décomposition de $\zeta_K$ et $L(.,\chi)$ en produit donnent alors $\zeta_K(s) = \zeta(s)L(s,\chi)$, pour $\Re(s) > 1$. La formule analytique du nombre de classes prend donc la forme suivante :

**Théorème 7**
- *Si $K$ est réel, $h_K = \frac{w_k\sqrt{\delta_K}}{4\ln(\epsilon)}L(1,\chi)$*
- *Si $K$ est complexe, $h_K = \frac{w_K\sqrt{|\delta_K|}}{2\pi}L(1,\chi)$*

# 4 Une formule explicite.

Il se trouve qu'en utilisant les sommes de Gauss on peut donner une expression relativement explicite de $L(1,\chi)$.

On note $D = |\delta_K|$. On pose $w = e^{\frac{2i\pi}{D}}$ et si $a \in \mathbb{Z}$, $g_a(\chi) = \sum_{k=1}^{D} \chi(k)w^{ak}$. C'est une somme de Gauss.

**Proposition 3** *Si PGCD$(a,D) = 1$, alors $\chi(a)g_a(\chi) = g_1(\chi)$, sinon $g_a(\chi) = 0$.*

Preuve : Soit PGCD$(a,D) = 1$. Alors $\chi(a)g_a(\chi) = \sum_{k=1}^{D} \chi(ak)\zeta^{ak}$ et la multiplication par $a$ est une permutation des classes de congruence modulo $D$, on obtient donc $g_1(\chi)$. Si maintenant PGCD$(a,D) \neq 1$, posons $d = \frac{D}{\text{PGCD}(a,D)}$. Comme $\chi$ est primitif, il existe $b \equiv 1\,[d]$ et premier à $D$ tel que $\chi(b) \neq 1$. On a alors $bl \equiv l\,[d]$ pour tout $l$ et donc $\chi(b)g_a(\chi) = \sum_{l=1}^{D} \chi(lb)w^{abl} = g_a(\chi)$. Ainsi $g_a(\chi) = 0$.

Nous allons maintenant donner une autre expression de $L(1,\chi)$. Posons $w = e^{\frac{2i\pi}{D}}$. Pour $\Re(s) > 1$, on a :

$$\begin{aligned} L(s,\chi) &= \sum_{l=1}^{D} \chi(l) \sum_{n \equiv l} \frac{1}{n^s} \\ &= \sum_{l=1}^{D} \chi(l) \sum_{n \geq 1} \frac{1}{D} \sum_{a=1}^{D} \frac{w^{(l-n)a}}{n^s} \\ &= \frac{1}{D} \sum_{a=1}^{D-1} g_a(\chi) \sum_{n \geq 1} \frac{w^{-an}}{n^s} \end{aligned}$$

Or les séries de Dirichlet qui appraissent à droite convergent et sont analytiques dans $D(0)$ et on a

$$\begin{aligned} L(1,\chi) &= -\frac{1}{D} \sum_{a=1}^{D-1} g_a(\chi) \log(1 - w^{-a}) \\ &= -\frac{g_1(\chi)}{D} \sum_{\mathrm{PGCD}(a,D)=1} \chi(a) \log(1 - w^{-a}) \end{aligned}$$

Or on a $\log(1 - w^{-a}) = \log(e^{-\frac{i\pi a}{D}} 2i \sin(\frac{\pi a}{D}))$. Ainsi

$$L(1,\chi) = -\frac{g_1(\chi)}{D} \left( \sum_{\mathrm{PGCD}(a,D)=1} \chi(a) \log(\sin(\frac{\pi a}{D})) - i\frac{\pi}{D} \sum_{\mathrm{PGCD}(a,D)} \chi(a) a \right)$$

## 4.1 $g_1(\chi)$.

Il se trouve que l'on connaît exactement le module de la somme de Gauss $g_1(\chi)$. En effet

$$\begin{aligned} g_1(\chi)^2 &= \sum_{a,b} \chi(a)\chi(b^{-1}) w^{a+b} \\ &= \sum_{c} \chi(c) \sum_{a} x^{(c+1)} \ avec\ c = ab^{-1} \\ &= \chi(-1) D \end{aligned}$$

Ainsi $|g_1(\chi)| = \sqrt{D}$.
Remarque : On a ainsi montré que si $K$ est réel, $g_1(\chi) = \pm\sqrt{D}$ et si $K$ est complexe, $g_1(\chi) = \pm i\sqrt{D}$. Il se trouve que Gauss a calculé exactement ces signes. C'est un résultat plus difficile que nous ne prouverons pas ici, mais nous verrons plus loin qu'il a une signification arithmétique. En fait $g_1(\chi) = \sqrt{D}$ dans le cas réel et $i\sqrt{D}$ dans le cas complexe.

## 4.2 Le cas réel.

Il correspond à $\chi(-1) = 1$.

Remarquons que $\sum_{\mathrm{PGCD}(a,D)=1} \chi(a)a = \sum_{\mathrm{PGCD}(a,D)=1} \chi(D-a)(D-a) = -\sum_{\mathrm{PGCD}(a,D)=1} \chi(a)a$. Ainsi $\sum_{\mathrm{PGCD}(a,D)=1} \chi(a)a = 0$. De plus comme $\log(\sin(\frac{a\pi}{D})) = \log(\sin(\frac{(D-a)\pi}{D}))$, on a

$$\sum_{\mathrm{PGCD}(a,D)=1} \chi(a) \log(\sin(\frac{a\pi}{D})) = 2 \sum_{0<a<\frac{D}{2}} \chi(a) \log(\sin(\frac{a\pi}{D}))$$

Remarquons qu'il n'y a pas de risque à mettre $<$ devant $\frac{D}{2}$, étant donné que soit $D$ est impair, soit il est divisible par 4 et dans ce cas $\chi(\frac{D}{2}) = 0$. Finalement on obtient :

$$h_K = \frac{1}{\ln(\epsilon)} \left| \sum_{0<a<\frac{D}{2}} \chi(a) \log(\sin(\frac{a\pi}{D})) \right|$$

## 4.3 Le cas complexe.

Il correspond cette fois à $\chi(-1) = -1$, c'est l'autre somme qui s'annule. En effet,

$$\sum_{\text{PGCD}(a,D)=1} \chi(a) \log(\sin(\frac{a\pi}{D})) = \sum_{\text{PGCD}(a,D)=1} \chi(D-a) \log(\sin(\frac{(D-a)\pi}{D})) = - \sum_{\text{PGCD}(a,D)=1} \chi(a) \log(\sin(\frac{a\pi}{D}))$$

. Ainsi $\sum_{\text{PGCD}(a,D)=1} \chi(a) \log(\sin(\frac{a\pi}{D})) = 0$. Cherchons maintenant à réécrire l'autre somme.
$1^{er}$ cas : $\chi(2) \neq 0$ ($D$ impair).

$$\begin{aligned} S = \sum_{0<a<D} \chi(a)a &= \sum_{0<a<\frac{D}{2}} \chi(a)a + \sum_{0<a<\frac{D}{2}} \chi(D-a)(D-a) \\ &= 2 \sum_{0<a<\frac{D}{2}} \chi(a)a - D \sum_{0<a<\frac{D}{2}} \chi(a) \end{aligned}$$

Mais on peut également séparer les entiers $a$ selon leur parité dans le calcul de $S$ :

$$\begin{aligned} S &= \sum_{0<a<\frac{D}{2}} \chi(2a)2a + \sum_{0<a<\frac{D}{2}} \chi(D-2a)(D-2a) \\ &= \sum_{0<a<\frac{D}{2}} 4\chi(2) \sum_{0<a<\frac{D}{2}} \chi(a)a - D\chi(2) \sum_{0<a<\frac{D}{2}} \chi(a) \end{aligned}$$

En combinant ces deux écritures on obtient

$$(2 - \chi(2))S = -D \sum_{0<a<\frac{D}{2}} \chi(a)$$

Rappelons que

$$h_K = \frac{ig_1(\chi)w_K\sqrt{D}}{2D^2} S$$

Ainsi ce qui précède nous donne

$$h_K = \frac{w_K}{2(2 - \chi(2))} \left| \sum_{0<a<\frac{D}{2}} \chi(a) \right|$$

$2^{eme}$ cas : $\chi(2) = 0$ ($D$ pair).
Dans ce cas, si $0 < a < D$ est pair, $\chi(a) = 0$. Si $a$ est impair alors $(1-a)\frac{D}{2}$ est divisible par $D$. Ainsi $\chi(\frac{D}{2} + a) = \chi((\frac{D}{2} + 1)a)$. Ainsi

$$S = \sum_{0<a<\frac{D}{2}} \chi(a)a + \chi(\frac{D}{2} + 1) \sum_{0<a<\frac{D}{2}} (\frac{D}{2} + a)\chi(a)$$

Or si $\chi(\frac{D}{2}+1)=1$, alors $\chi(\frac{D}{2}+a)=\chi(a)$ pour tout $0<a<\frac{D}{2}$ et $\chi$ peut se factoriser en un caractère modulo $\frac{D}{2}$, ce qui contredit le fait qu'il est primitif. Ainsi $\chi(\frac{D}{2}+1)=-1$ et $S=\frac{D}{2}\sum_{0<a<\frac{D}{2}}\chi(a)$. Comme $\chi(2)=0$, la formule démontrée dans le premier cas reste vraie. Donc dans tous les cas

$$S=-\frac{D}{2-\chi(2)}\sum_{0<a<\frac{D}{2}}\chi(a)$$

Rappelons que

$$h_K=\frac{ig_1(\chi)w_K\sqrt{D}}{2D^2}S$$

Le calcul de $S$ et de $|g_1(\chi)|$ nous donnent donc

**Théorème 8** *Si $K$ est un corps quadratique imaginaire,*

$$h_K=\frac{w_K}{2(2-\chi(2))}\left|\sum_{0<a<\frac{D}{2}}\chi(a)\right|$$

On voit ici que ce résultat est très explicite. Illustrons-le en calculant $h_K$ dans le cas du corps $K=\mathbb{Q}[\sqrt{-23}]$.

Tout d'abord déterminons $\chi$. 23 est un nombre premier congru à 3 modulo 4, le discriminant de $K$ est donc $-23$. Ainsi $\chi$ est un caractère non trivial modulo 3 à valeur dans $\{-1,1\}$. Comme $\mathbb{F}_{23}^*$ est cyclique d'ordre 22 il possède un unique sous-groupe d'indice 2 et donc un unique caractère non trivial à valeurs dans $\{-1,1\}$. Ainsi $\chi$ coïncide avec le symbole de Legendre $\left(\frac{\cdot}{23}\right)$.

Maintenant calculons en utilisant la loi de réciprocité quadratique :

- $23=16+7$ donc $16|(23^2-1)$ et $\chi(2)=1$
- $\chi(3)=-\left(\frac{23}{3}\right)=-\left(\frac{2}{3}\right)=1$
- $\chi(4)=1$
- $\chi(5)=\left(\frac{23}{5}\right)=\left(\frac{3}{5}\right)=-1$
- $\chi(6)=\chi(2)\chi(3)=1$
- $\chi(7)=-\left(\frac{23}{7}\right)=-\left(\frac{2}{7}\right)=-1$
- $\chi(8)=\chi(2)^3=1$
- $\chi(9)=1$
- $\chi(10)=\chi(2)\chi(5)=-1$
- $\chi(11)=-\left(\frac{23}{11}\right)=-1$

Comme $w_K=2$ l'application du théorème nous donne $h_K=7-4=3$.

Remarque : Regardons ce qui se passe si l'on tient compte des signes des sommes de Gauss. Dans le cas réel, $h_K\ln(\epsilon)=-\sum_{1<a<\frac{D}{2}}\chi(a)\log(\sin(\frac{a\pi}{D}))$. Ainsi

$$\epsilon^{h_K}=\frac{\prod_b\sin(\frac{\pi b}{D})}{\prod_a\sin(\frac{\pi a}{D})}$$

où $a$ parcourt les entiers entre 1 et $\frac{D}{2}$ tels que $\chi(a)=1$ et $b$ ceux tels que $\chi(b)=-1$. Supposons que $K=\mathbb{Q}[\sqrt{p}]$ où $p$ est un nombre premier congru à 1 modulo 4. Alors comme dans le calcul précédent, $\chi=\left(\frac{\cdot}{p}\right)$. Le fait que $\epsilon>1$ implique alors que le dénominateur du terme de droite est plus petit que le numérateur, ce qui peut encore s'interpréter comme la fait que les résidus

quadratiques sont plus nombreux près de 0 et $p$ qu'au centre près de $\frac{p}{2}$.
Dans le cas complexe, on a

$$h_K = \frac{w_K}{2(2-\chi(2))} \sum_{1<a<\frac{D}{2}} \chi(a)$$

Si $p$ est premier congru à 3 modulo 4, la même conclusion que précédemment s'obtient en considérant $K = \mathbb{Q}[\sqrt{-p}]$.
Ces résultats sont en fait équivalents aux assertions sur le signe des sommes de Gauss.

# Références


[1] Ireland et Rosen : *A classical introduction to modern number theory*, Springer

[2] Borevitch et Shavarevitch : *Number theory*

[3] Janusz : *Algebraic number fields*