SUJETS D'ARITHMÉTIQUE

Printemps 2010

Vadim Schechtman

Zeittafel

Pierre de FERMAT (1601 - 1665)

Leonard EULER (1707 - 1783)

Adrien Marie LEGENDRE (1752 - 1833)

Carl Friedrich GAUSS (1777 - 1855)

Niels Henrik ABEL (1802 - 1829)

Carl Gustav Jacob JACOBI (1804 - 1851)

Eduard KUMMER (1810 - 1893)

Pafnuty Lvovich CHEBYSHEV (1821 - 1894)

Évariste GALOIS (1811 - 1832)

Gotthold EISENSTEIN (1823 - 1852)

Bernhard RIEMANN (1826 - 1866)

§4. Fonction Γ

4.1. On définit

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt = \int_0^\infty e^{-t}t^s\frac{dt}{t}, \quad \Re(s) > 0$$

Exercice. Montrer que $\Gamma(s+1) = s\Gamma(s)$ et $\Gamma(n) = (n-1)!$ si $n \in \mathbb{N}$.

A partir de l'équation fonctionelle (la première formule), définir le prolongement analytique de $\Gamma(s)$ à une fonction méromorphe sur le plan complexe avec les seuls pôles simples en $s = 0, -1, -2, \ldots$ Calculer les résidus en ces points.

La fonction Beta d'Euler est définie par

$$B(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx, \quad \Re(s), \Re(t) > 0$$

4.2. *Théorème.*

$$B(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$$

Exercice. Démontrer cette formule pour $s, t \in \mathbb{N}$.

Démonstration du théorème (Jacobi, cf. [J]). On a

$$\Gamma(a)\Gamma(b) = \int_0^\infty \int_0^\infty e^{-x-y}x^{a-1}y^{b-1}dxdy$$

On fait le changement de variables $x+y = r,\ x = rw$, donc $0 \leq r < \infty$, $0 \leq w \leq 1$ et $dxdy = rdwdr$, d'où

$$\Gamma(a)\Gamma(b) = \int_0^1 w^{a-1}(1-w)^{b-1}dw \int_0^\infty e^{-r}x^{a+b-1}dr = B(a,b)\Gamma(a+b)$$

4.3. *Exercice.* Rémarquons que

$$e^{-t} = \lim_{n\to\infty} \big(1 - \frac{t}{n}\big)^n,$$

d'où

$$\Gamma(s) = \lim_{n\to\infty} \int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1}dt \tag{4.3.1}$$

(pour une preuve, cf. 4.3.1 ci-dessous).

En déduire $\Gamma(s)$ comme une valeur limite de B.

En effet,

$$\int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1}dt =$$

$(u = t/n)$

$$= n^s \int_0^1 \big(1-u)^n u^{s-1} du$$

Pour $n \in \mathbb{N}$ on a

$$B(n+1,t) = \int_0^1 (1-v)^n v^{t-1} dv = \frac{n!}{t(t+1)\cdot \ldots \cdot (t+n)}$$

et cela est vrai pour tous $t \neq 0, -1, \ldots -n$ (prouver!)

Il en découle que

$$\Gamma(s) = \lim_{n\to\infty} n^s B(n+1,s) = \lim_{n\to\infty} n^s \frac{n!}{s(s+1)\cdot \ldots \cdot (s+n)} =$$

$$= \lim_{n\to\infty} n^s \frac{(n-1)!}{s(s+1)\cdot \ldots \cdot (s+n-1)} \tag{4.3.2}$$

(*formule d'Euler - Gauss*).

4.3.1. *Exercice.* Preuve de (4.3.1). C'est une conséquence du Théorème de convergence monotone.

En effet, posons

$$f_n(x) = (1 - \frac{x}{n}\Big)^n x^p \cdot 1_{[0,n]}$$

On affirme que $f_n(x) \leq f_{n+1}(x)$ pour tous x. C'est une conséquence du

Lemme. $f_n(x) \leq f_{n+1}(x)$ pour tout $0 < x < n$.

Preuve. Fixons un $x > 0$. Considérons la fonction $\phi(y) = (1 - x/y)^y$ définie pour $y > x$. Il suffit de montrer que

$$\psi(y) := \log \phi(y) = y(\log(y-x) - \log(y))$$

est croissante. On a

$$\psi'(y) = \log(y-x) - \log(y) - \frac{x}{y-x}$$

Le théorème des accroissements finis appliqué à la fonction $\log(y)$ sur l'intervale $[y-x, y]$ nous dit qu'il existe $c,\ y - x < c < y$ tel que

$$\log(y-x) - \log(y) = \frac{1}{c} \cdot x,$$

d'où $\psi'(y) > 0$. $\square$

4.4. *Exercice.* Calculer $\Gamma(1/2)$.

Solution. On a

$$\Gamma(1/2)^2 = \frac{\Gamma(1/2)\Gamma(1/2)}{\Gamma(1)} = B(1/2, 1/2)$$

Par définition,

$$B(1/2,1/2)=\int_0^1 x^{-1/2}(1-x)^{-1/2}dx=$$

$(x=u^2)$

$$=2\int_0^1 \frac{du}{\sqrt{1-u^2}}=2\arcsin\ 1=\pi,$$

d'où

$$\Gamma(1/2)=\int_0^\infty e^{-x}x^{-1/2}dx=\sqrt{\pi}$$

On rémarque que

$$\int_0^\infty e^{-x}x^{-1/2}dx=2\int_0^\infty e^{-u^2}du=\int_{-\infty}^\infty e^{-u^2}du,$$

donc

$$\int_{-\infty}^\infty e^{-u^2}du=\sqrt{\pi}$$

(l'intégrale de Poisson).

4.5. *Théorème.* On a

$$\Gamma(a)\Gamma(1-a)=\frac{\pi}{\sin\ \pi a}$$

Preuve. Supposons d'abord que $0<\Re(a)<1$. Par la formule d'Euler

$$\Gamma(a)\Gamma(1-a)=B(a,1-a)=\int_0^1 x^{a-1}(1-x)^{-a}dx=$$

$(x=u/(u+1))$

$$=\int_0^\infty \frac{u^{a-1}}{u+1}du=I$$

Nous calculons la dernière intégrale par la formule de Cauchy, cf. [WW], 6.24, Example 1. En effet, considérons intégrale

$$I(r,R)=\int_{C(r,R)} \frac{z^{a-1}}{z+1}dz,$$

où $C(r,R)$ est le contour

$$\begin{aligned}C(r,R)=\{r\leq z\leq R\}\cup\{z=Re^{i\theta},\ 0\leq\theta\leq 2\pi\}\cup\\ \cup\{R\geq z\geq r\}\cup\{z=re^{i\theta},\ 2\pi\geq\theta\geq 0\}=\\ =C_1\cup C_2(R)\cup C_3\cup C_4(r)\end{aligned}$$

Alors

$$I(R,r)=\int_{C_2}+\int_{C_4}+(1-e^{2\pi i(a-1)})\cdot\int_r^R \frac{u^{a-1}}{u+1}du=2\pi i\,\mathrm{Res}_{z=-1}\frac{z^{a-1}}{z+1}=2\pi i\cdot e^{\pi i(a-1)}$$

À la limite

$$\lim_{R\to\infty} \int_{C_2(R)} = \lim_{r\to 0} \int_{C_4(r)} = 0$$

grace à l'hypothèse $0 < \Re(a) < 1$, d'où

$$I = 2\pi i \cdot \frac{e^{\pi i(a-1)}}{1 - e^{2\pi i(a-1)}} = \frac{2\pi i}{e^{-\pi i(a-1)} - e^{\pi i(a-1)}} =$$

$$= \frac{2\pi i}{e^{\pi i a} - e^{-\pi i a}} = \frac{\pi}{\sin\ \pi a}$$

Ceci prouve 4.5 sous l'hypothèse $0 < \Re(a) < 1$; le cas général s'en suit, puisque les deux côtés sont des fonctions méromomorphes de a.

4.6. Soit

$$\omega = 4\int_0^1 \frac{dt}{\sqrt{1-t^4}}$$

Montrer que $\omega = \Gamma(1/4)^2/\sqrt{2\pi}$.

4.7. *Exercice: l'intégrale de Hankel.* Considérons l'intégrale

$$I(s) = \int_\infty^{(0+)} (-t)^{s-1} e^{-t} dt$$

Ici $\int_\infty^{(0+)} = \int_C$, où C désigne le chemin suivant:

$$C = \{\infty > t \geq \epsilon\} \cup \{t = \epsilon e^{i\theta},\ 0 \leq \theta \leq 2\pi\} \cup \{\epsilon \leq t < \infty\} =$$

$$= C_\epsilon^+ \cup C_\epsilon^0 \cup C_\epsilon^- \tag{4.7.1}$$

En plus,

$$(-t)^{s-1} = e^{(s-1)\log(-t)},$$

où $\log(-t)$ désigne la branche du logarithme qui prend les valeurs réels pour t réel négative.

(i) Montrer que

$$I(s) = -2i\sin\pi s \int_0^\infty t^{s-1}e^{-t}dt$$

si $\Re(s) > 0$. (Noter que $-t = te^{-i\pi}$ sur C_ϵ^+, $-t = te^{i\pi}$ sur C_ϵ^-).

Donc

$$\Gamma(s) = -\frac{1}{2i\sin\pi s}\int_\infty^{(0+)} (-t)^{s-1}e^{-t}dt$$

On note que $I(s)$ est bien définie pour tous $s \in \mathbb{C}$, c'est une fonction entière; donc on obtient (encore une fois) une définition de $\Gamma(s)$ comme une fonction méromorphe sur $\mathbb{C}$, avec les seules pôles simples en $s \in \mathbb{Z}_{\leq 0}$.

(ii) En déduire que

$$\frac{1}{\Gamma(s+1)} = -\frac{1}{2\pi i}\int_{\infty}^{(0+)} (-t)^{-s-1}e^{-t}dt$$

Prendre dans cette formule $s = n \in \mathbb{N}_+$, remplacer le contour $\int_{\infty}^{(0+)}$ par un cercle autour 0, et comparer avec le developpement taylorien de e^{-t}.

4.8. *Exercice:* formule de rédoublement (Legendre). En employant la formule d'Euler - Gauss (4.3.2), montrer que

$$\pi^{1/2}\Gamma(2s) = 2^{2s-1}\Gamma(s)\Gamma(s+1/2)$$

Idée. Considérons la fonction

$$\phi(s) = \frac{2^{2s-1}\Gamma(s)\Gamma(s+1/2)}{\Gamma(2s)}$$

Remplacez $\Gamma(s)$ et $\Gamma(s+1/2)$ par l'expression (4.3.2), et $\Gamma(2s)$ — par

$$\lim_{n\to\infty}(2n)^{2s}\frac{(2n-1)!}{2s(2s+1)\ldots(2s+2n-1)};$$

en déduisez que $\phi(s)$ ne depend pas de s. Faitez $s = 1/2$ pour conclure.

§5. Sommes de Gauss et de Jacobi

5.1. *Caractères.* Soit p un nombre premier. Un caractère (multiplicatif) de $\mathbb{F}_p$ est un homomorphisme $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$. Pour chaque $x \in \mathbb{F}_p$, $\chi(x)^{p-1} = \chi(x^{p-1}) = \chi(1) = 1$, donc $\chi(x)$ est une racine $(p-1)$-ième de l'unité. Il s'en suit que

$$\chi(x)^{-1} = \bar{\chi(x)}$$

On désigne par e le caractère trivial, $e(x) = 1$ pour chaque $x \in \mathbb{F}_p^*$.

On pose $\chi(0) = 0$ si $\chi \neq e$ et $e(0) = 1$.

Le groupe $\mathbb{F}_p^*$ étant cyclique d'ordre $p-1$, les caractères forment un groupe cyclique $X(\mathbb{F}_p^*)$ d'ordre $p-1$ (expliquer!).

Suivant l'usage, on dit que χ et d'ordre a si $\chi^a = e$ et $\chi^b \neq e$ pour $1 < b < a$. On a $a \mid (p-1)$.

5.1.1. *Exemple.* Le symbole de Legendre

$$\left(\frac{?}{p}\right) : \mathbb{F}_p^* \longrightarrow \{\pm 1\}$$

est un caractère d'ordre 2 ($p > 2$).

5.1.2. *Exercices.* (a) Pour chaque $x \in \mathbb{F}_p^*$, $x \neq 1$ il existe $\chi \in \mathbb{F}_p^*$ tel que $\chi(x) \neq 1$.

(b) $\sum_{x \in \mathbb{F}_p} \chi(x) = 0$ si $\chi \neq e$ et p si $\chi = e$.

(c) $\sum_{\chi \in X(\mathbb{F}_p^*)} \chi(x) = 0$ si $x \neq \mathbb{F}_p^* - \{1\}$ et $p-1$ si $x = 1$.

5.2. *Sommes de Gauss.* Soient $\zeta = e^{2\pi i/p}$, $a \in \mathbb{F}_p$, $\chi \in X(\mathbb{F}_p^*)$. On définit

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

Par définition, $g_a(\chi) \in \mathbb{Q}(\zeta_p, \zeta_{p-1})$.

5.2.1. *Exercice.* $g_a(\chi) = \chi(a)^{-1} g_1(\chi)$ si $\chi \neq e$ et $a \neq 0$. Si $a = 0$ et $\chi \neq e$ ou $a \neq 0$ et $\chi = e$, alors $g_a(\chi) = 0$. Enfin, $g_0(e) = p$.

On désignera $g(\chi) := g_1(\chi)$.

5.3. *Théorème.* Si $\chi \neq e$, alors $|g(\chi)| = \sqrt{p}$.

Considérons la somme $S = \sum_a |g_a(\chi)|^2$. Il est clair que $|g_a(\chi)|^2 = |g(\chi)|^2$ si $a \neq 0$; puisque $g_0(\chi) = 0$, on a $S = (p-1)|g(\chi)|^2$.

Par contre,

$$|g_a(\chi)|^2 = g_a(\chi)g_a\bar{(\chi)} = \sum_{x,y} \chi(x)\chi\bar{(y)}\ \zeta^{a(x-y)},$$

donc

$$S = \sum_{x,y} \chi(x)\chi\bar{(y)} \sum_a \zeta^{a(x-y)} = p \sum_{x,y} \chi(x)\chi\bar{(y)}\, \delta(x,y) = p \sum_x |\chi(x)|^2 = p(p-1),$$

d'où le théorème.

5.3.1. *Enoncé équivalente.* On a

$$g\bar{(\chi)} = \chi(-1)g(\bar{\chi})$$

(exercice). Donc le théorème nous dit que

$$g(\chi)g(\bar{\chi}) = \chi(-1)p$$

Par exemple, si χ est d'ordre 2, alors $\bar{\chi} = \chi$, donc $g(\chi)^2 = \chi(-1)p$; on a déjà vu cela.

5.4. *Sommes de Jacobi.* Soient $\chi, \chi' \in X(\mathbb{F}_p^*)$. On définit

$$J(\chi,\chi') = \sum_{a \in \mathbb{F}_p} \chi(a)\chi'(1-a) \in \mathbb{Q}(\zeta_{p-1})$$

Il est clair que $J(\chi,\chi') = J(\chi',\chi)$.

5.5. *Théorème.* (a) $J(e,e) = p$

(b) $J(e,\chi) = 0$ si $\chi \neq e$

(c) $J(\chi,\chi^{-1}) = -\chi(-1)$ si $\chi \neq e$

(d) Si $\chi, \chi', \chi\chi' \neq e$, alors

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

En particulier, $|J(\chi,\chi')| = \sqrt{p}$.

(a) est trivial; (b): exercice.

(c):

$$J(\chi,\chi^{-1}) = \sum_{a \neq 1} \chi(a(1-a)^{-1})$$

Quand a parcourt $\mathbb{F}_p - \{1\}$, $c = a(1-a)^{-1}$ parcourt $\mathbb{F}_p - \{-1\}$. Donc

$$J(\chi,\chi^{-1}) = \sum_{c \in \mathbb{F}_p - \{-1\}} \chi(c) = -\chi(-1)$$

(d): Calculons le produit

$$g(\chi)g(\chi') = (\sum_a \chi(a)\zeta^a)(\sum_b \chi'(b)\zeta^b) = \sum_c (\sum_{a+b=c} \chi(a)\chi'(b))\ \zeta^c$$

On a

$$\sum_{a+b=0} \chi(a)\chi'(b) = \sum_a \chi(a)\chi'(-a) = \chi'(-1) \sum_a (\chi\chi')(a) = 0$$

D'autre part, si $c \neq 0$,

$$\sum_{a+b=c} \chi(a)\chi'(b) = (\chi\chi')(c)\ J(\chi,\chi')$$

Il s'en suit que

$$g(\chi)g(\chi') = \sum_c (\chi\chi')(c)\ J(\chi,\chi')\ \zeta^c = g(\chi\chi')J(\chi,\chi'),$$

cqfd.

Sommes de deux carrés

5.9. On va travailler dans l'anneau de nombres gaussiens $R = \mathbb{Z}[i]$ qui est l'anneau d'entiers dans $L = \mathbb{Q}(i)$. La norme $N:\ L^* \longrightarrow \mathbb{Q}^*$ s'ecrit

$$N(a+bi) = |a+bi|^2 = a^2 + b^2$$

On a $N(x) \neq 0 \Leftrightarrow x \neq 0$.

5.10. *Lemme.* R est euclidien par rapport à N, donc principal.

En effet, on doit démontrer que, étant donnés $\alpha, \beta \in R,\ \beta \neq 0$, il existent $\gamma, r \in R$ tels que $\alpha = \gamma\beta + r$, avec $N(r) < N(\beta)$.

En divisant par y, il suffit de démontrer que, étant donné $x \in L$, il existe $\alpha \in R$ tel que $N(x-\alpha) < 1$. Or, il existe même un $\alpha \in R$ avec $N(x-\alpha) \leq 1/2$, ce qu'on voit tout de suite géométriquement.

5.11. *Exercice.* Montrer que les anneaux des entiers dans les corps suivants sont euclidiens par rapport à la norme: $\mathbb{Q}(\sqrt{d})$ où $d = -1, -2, -3, -7, -11$.

5.12. *Exercice.* Les unités dans R sont $\pm 1, \pm i$, autrement dit,

$$R^* = \mu_4 := \{x \in \mathbb{C}^* \mid x^4 = 1\} \tag{5.12.1}$$

En effet, un $\alpha \in R$ est inversible ssi $N(\alpha) = 1$.

5.13. *Théorème* (Fermat) Soit $p > 2$ premier.

(a) Si $p \mid (a^2 + b^2)$ avec $a, b \in \mathbb{Z},\ p \not| a$, alors $p \equiv 1 \pmod 4$.

(b) Chaque p premier de la forme $4k+1$ est représentable de la façon essentiellement unique sous une forme $p = a^2 + b^2$, $a, b \in \mathbb{Z}$.

"Essentiellement unique" signifie qu'on peut changer les signes de a et de b et permuter a avec b, ce qui donne 8 solutions.

Remarquons que $2 = (\pm 1)^2 + (\pm 1)^2$ (4 possibilités).

5.14. *Démonstration de* (a). Si $p \not| \, a$ alors $p \mid b$. On a $a^2 \equiv -b^2 \pmod{p}$, donc $(a/b)^2 = -1$ dans $\mathbb{F}_p$, donc $(-1/p) = 1$, d'où $p \equiv 1 \pmod 4$.

5.15. *Démonstration de* (b). Montrons que chaque p premier de la forme $4k+1$ est égale à $a^2 + b^2$, $a, b \in \mathbb{Z}$.

Choisissons un générateur $\lambda \in \mathbb{F}_p^*$. Alors

$$\chi(\lambda^a) = e^{2\pi i a k/(p-1)} = e^{\pi i a/2} \in \mu_4$$

est un caractére de $\mathbb{F}_p^*$ d'ordre 4. Il s'en suit que la somme de Jacobi $J(\chi, \chi) \in R = \mathbb{Z}[i]$, soit $J(\chi, \chi) = a + bi$.

Théorème 5.5 (d) montre alors que

$$a^2 + b^2 = |J(\chi, \chi)|^2 = p$$

Unicité. Posons $\pi = J(\chi, \chi)$, donc $p = \pi\bar{\pi}$.

Si $p = c^2 + d^2$ est une autre représentation, $\pi' = c + di$, alors $p = \pi'\bar{\pi}'$. Alors π' est necessairement premier dans R (prouver!).

L'anneau R étant principal, Il s'en suit que soit $\pi' = \epsilon\pi$, soit $\pi' = \epsilon\bar{\pi}$, avec $\epsilon \in R^*$. Ceci donne exactement 8 possibilités mentionnées ci-dessus.

5.17. *Exercice.* Soit $p = 5$. Écrivez explicitement un caractère $\chi : \mathbb{F}_5^* \longrightarrow \mathbb{C}^*$ d'ordre 4. Calculez $g(\chi), g(\chi^2)$ et $J(\chi, \chi)$ et leur valeur absolue; vérifiez la formule $J(\chi, \chi) = g(\chi)^2/g(\chi^2)$.

§5. Fonction ζ de Riemann

Cf. [R].

5.0. On pose

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},$$

la série converge normalement (donc uniformement et absolument) sur chaque compact $K\subset X=\{z\in\mathbb{C}|\ \Re(z)>1\}$, donc elle définit dans ce démi-plan une fonction holomorphe.

Montrez que

$$\zeta(s)=\prod_{p\ \text{premier}}\frac{1}{1-p^{-s}},\ \Re(s)>1$$

(*la formule de produit d'Euler*).

Pour démontrer la convergence du produit, utiliser le

Lemme. Le produit $\prod_{n=1}^{\infty}(1+a_n)$ converge dans $\mathbb{C}^*$ si et seulement si la série $\sum_{n=1}^{\infty}a_n$ converge.

Prouvez qu'il existe une infinité de nombres premiers (remarquez que la série $\sum n^{-1}$ diverge).

5.1. On a:

$$\Gamma(s)=\int_0^{\infty}e^{-x}x^s\frac{dx}{x}=\ (x=ty)\ =n^s\int_0^{\infty}e^{-ny}y^s\frac{dy}{y},$$

d'où

$$n^{-s}=\frac{1}{\Gamma(s)}\int_0^{\infty}e^{-ny}y^s\frac{dy}{y}$$

Il s'en suit:

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\frac{1}{\Gamma(s)}\sum_{n=1}^{\infty}\int_0^{\infty}e^{-ny}y^{s-1}dy=$$

$$=\frac{1}{\Gamma(s)}\int_0^{\infty}\sum_{n=1}^{\infty}e^{-ny}y^{s-1}dy=\frac{1}{\Gamma(s)}\int_0^{\infty}\frac{y^{s-1}}{e^y-1}dy,$$

$\Re(s)>1$. Pour justifier la permutation de la sommation et l'intégration, il suffit de montrer que: soit (a) $\int_0^{\infty}\sum_{n=1}^{\infty}|e^{-ny}y^{s-1}|dy<\infty$, soit (b) $\int_0^{\infty}\sum_{n=1}^{\infty}|e^{-ny}y^{s-1}|dy<\infty$. En effet, on voit facilement que les deux assertions soient vraies sous l'hypothèse $\Re(s)>1$.

5.2. *Intégral de Hankel.* Considérons l'intégral

$$I(s) = \int_{\infty}^{(0+)} \frac{(-x)^{s-1}}{e^x - 1} dx,$$

où $(-x)^{s-1} = e^{(s-1)\log(-x)}$, la branche de $\log(-x)$ étant choisie de telle façon que pour $x \in \mathbb{R}_{<0}$, $\log(-x)$ est réel.

Alors il est facile à voir que

$$\int_{\infty}^{(0+)} \frac{(-x)^{s-1}}{e^x - 1} dx = (e^{i\pi(s-1)} - e^{-i\pi(s-1)}) \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx = -2i \sin \pi s \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx$$

si $\Re(s) > 1$. Autrement dit,

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx = -\frac{I(s)}{2i \sin(\pi s)\Gamma(s)} =$$

(car $\Gamma(s)\Gamma(1-s) = \pi/\sin \pi s$)

$$= -\frac{\Gamma(1-s)}{2\pi i} \int_{\infty}^{(0+)} \frac{(-x)^{s-1}}{e^x - 1} dx \tag{5.2.1}$$

Par contre, l'intégrale $I(s)$ est une fonction entière sur le plan complexe $s \in \mathbb{C}$; donc $\zeta(s)$ est bien définie comme une fonction méromorphe avec les seuls pôles possibles en $s = 1, 2, 3, \ldots$. La définition de $\zeta(s)$ par la série montre qu'elle n'a pas de pôles en $s = 2, 3, 4, \ldots$.

Par contre, pour $s \to 1$, $\zeta(s) \to \infty$, donc $\zeta(s)$ a un pôle simple en $s = 1$ (car $\Gamma(1-s)$ a un pôle simple en $s = 1$).

5.3. *Nombres de Bernoulli* sont définis par une série génératrice:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n,$$

Exercice. Montrer que $B_{2n+1} = 0$ pour $n > 0$.

Voici quelques premières valeurs:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},$$

$$B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730}$$

5.4. *Polynômes de Bernoulli.* On définit les polynômes $B_n(t)$ $(n \geq 0)$ par la série génératrice:

$$\frac{xe^{tx}}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n(t)}{n!} \cdot x^n$$

Exercice. Montrez que: (i)

$$B_n(t) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} t^k$$

(ii) $B_n'(t) = nB_{n-1}(t)$

(iii) $B_n(t+1) - B_n(t) = nt^{n-1}$. En déduire que

$$\sum_{i=1}^{k} i^n = \frac{B_{n+1}(k+1) - B_{n+1}(0)}{n+1} \tag{5.4.1}$$

Considérez les cas $n = 1, 2$ explicitement.

(iv) $\sum_{m=0}^{n-1} \binom{n}{m} B_m = 0$ pour $n > 1$, ce qui permet de calculer les B_n par recurrence. (Utilisez (iii) avec $t = 0$).

5.5. *Valeurs en entiers negatifs.* Maintenant mettons $s = -n$ dans (5.2.1), $n \in \mathbb{N}$. Alors le contour $\int_{\infty}^{(+0)}$ se ferme, d'où

$$\zeta(-n) = (-1)^n \Gamma(n+1) \int_{|x|=\epsilon} \frac{x^{-n-1}}{e^x - 1} dx =$$

$$= (-1)^n n! \cdot \mathrm{res}_{x=0} \left(\frac{1}{x^{n+2}} \cdot \frac{x}{e^x - 1} \right) = (-1)^n n! \cdot \frac{B_{n+1}}{(n+1)!} = (-1)^n \cdot \frac{B_{n+1}}{n+1}, \tag{5.5.1}$$

cf. (5.4.1). Voici quelques exemples:

$$\zeta(0) = \sum_{n=1}^{\infty} 1 = -\frac{1}{2},\ \zeta(-1) = \sum_{n=1}^{\infty} n = -\frac{1}{12},\ \zeta(-3) = \sum_{n=1}^{\infty} n^3 = \frac{1}{120}$$

(une sommation de séries divergentes...). Par contre, $\zeta(-2n) = 0$ si $n > 0$.

5.6. *Equation fonctionelle.* Ce qui est plus populaire (dépuis Euler...), ce sont les expressions de $\zeta(2n)$ pour n positif en termes de nombres de Bernoulli. Par exemple, tous le monde sait que $\zeta(2) = \sum n^{-2} = \pi^2/6$. Dans l'approche de Riemann ils sont des conséquences de l'équation fonctionelle pour la fonction $\zeta(s)$.

Fixons un petit $\epsilon > 0$. Pour $m \in \mathbb{Z}, m \geq 1$, considérons le contour (cf. 4.7.1)):

$$C_m = \{R_m \geq x \geq \epsilon\} \cup \{x = \epsilon e^{i\theta},\ 0 \leq \theta \leq 2\pi\} \cup \{\epsilon \leq x \leq R_m\} \cup \{x = R_m e^{i\theta}, 2\pi \geq \theta \geq 0\} =$$

$$= C_m' \cup C_m'',\ C_m'' = \{x = R_m e^{i\theta}, 2\pi \geq \theta \geq 0\},$$

où $R_m = \pi(2m+1)$.

On considère l'intégrale (cf. (5.2.1)):

$$I(s; R_m) = -\frac{\Gamma(1-s)}{2\pi i} \int_{C_m} f(x,s) dx,\ f(x,s) = \frac{(-x)^{s-1}}{e^x - 1},$$

la branche de $f(x,s)$ étant fixée comme en 5.2. D'après (5.2.1),

$$\lim_{m\to\infty} -\frac{\Gamma(1-s)}{2\pi i}\int_{C'_m} f(x,s)dx = \zeta(s)$$

D'une autre part,

$$\left|\int_{C''_m} f(x,s)dx\right| \leq \int_{C''_m} \frac{|(-x)^{s-1}|}{|e^x-1|}dx \leq CR_m^\sigma \int_{C''_m} \frac{1}{|e^x-1|}dx$$

où $\sigma = \Re(s)$.

5.6.1. *Lemme.* Il existe une constante $\epsilon > 0$ telle que

$$|e^x - 1| > \epsilon$$

pour tous $x \in C''_m$ et tous m.

Preuve. L'application exponentielle e^x définit un homéomorphisme $p:\ \mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^*$. Choisissons $\delta > 0$ tel que

$$D_\delta + 2\pi i\mathbb{Z} \cap \left(\cup_{m=1}^\infty\ C''_m\right) = \emptyset,$$

où $D_\delta = \{z|\ |z| < \delta\}$. Alors $p(D_\delta)$ est un voisinage de 1, donc il existe $\epsilon > 0$ tel que $D_\epsilon \subset p(D_\delta)$.

On a $p^{-1}(D_\epsilon) \subset D_\delta + 2\pi i_B Z$, donc $p(C''_m) \subset \mathbb{C} - D_\epsilon$ pour tout m, i.e. pour tout m et tout $x \in C''_m$, on a $|e^x - 1| > \epsilon$, QED.

Corollaire. Si $\Re(s) < 0$, alors

$$\lim_{m\to\infty} -\frac{\Gamma(1-s)}{2\pi i}\int_{C''_m} f(x,s)dx = 0$$

D'autre part, on peut évaluer $I(s;R)$ par la formule des résidus de Cauchy: la fonction $f(x,s)$ a des pôles simples en $x = 2\pi in,\ n \in \mathbb{Z},\ n \neq 0$, avec les résidus

$$\mathrm{res}_{x=\pm 2\pi in}\frac{(-x)^{s-1}}{e^x-1} = (\pm 2\pi in)^{s-1} = (2\pi n)^{s-1}e^{\pm\pi i(s-1)/2},\ n \geq 1,$$

donc

$$I(s;R_m) = -\Gamma(1-s)\cdot\sum_{n=1}^m\{\mathrm{res}_{x=2\pi in}f(x;s) + \mathrm{res}_{x=-2\pi in}f(x;s)\} =$$

$$= (2\pi)^{s-1}\Gamma(1-s)2\sin(\pi s/2)\sum_{n=1}^m\ n^{s-1}$$

Il s'en suit que si $\Re(s) < 0$, alors

$$\lim_{m\to\infty} I(s;R_m) = 2^s\pi^{s-1}\Gamma(1-s)\sin(\pi s/2)\zeta(1-s)$$

On a démontré:

5.7. *Théorème* (Riemann). La fonction $\zeta(s)$ satisfait à l'eq́uation fonctionelle

$$\zeta(s) = 2^s\pi^{s-1}\Gamma(1-s)\sin(\pi s/2)\zeta(1-s)$$

En effet, on a montré tout-à-l'heure que cette équation est satisfaite pour $\Re(s) < 0$ donc pour tous s car les deux côtés sont des fonctions méromorphes.

Des cas particuliers de 5.7 ont été connus déjà à Euler, [E], (a).

En utilisant les propriétés standartes de la fonction Γ, on peut donner, avec Riemann, une réformulation plus symétrique de 5.7. Rappelons que l'on a:

$$\frac{\sin(\pi s/2)}{\pi} = \frac{1}{\Gamma(s/2)\Gamma(1-s/2)}$$

et d'un autre côté,

$$\pi^{1/2}\Gamma(1-s) = 2^{-s}\Gamma((1-s)/2)\Gamma(1-s/2),$$

cf. 4.8. Il s'en suit:

5.8. *Théorème.* Définissons

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$$

Alors

$$\xi(s) = \xi(1-s)$$

5.9. Si l'on met $s = 1-2n$ dans 5.7, et se rappelle (5.5.1), on obtient la formule celebre:

$$\zeta(2n) = (-1)^{n+1}\frac{2^{2n-1}B_{2n}}{(2n)!}\cdot\pi^{2n},$$

$n \geq 0$ (Euler).

Exercice. Montrer que

$$(-1)^{n-1}B_{2n} = 4n\int_0^\infty \frac{t^{2n-1}}{e^{2\pi t}-1}dt$$

pour $n \geq 1$ (utiliser 5.1).

5.9.1. *Zéros.* La formule de produit d'Euler implique que $\zeta(s)$ n'a pas de zéros dans le domaine $\Re(s) > 1$. Il s'en suit de l'équation fonctionelle que les seuls zéros dans le domaine symétrique $\Re(s) < 0$ sont $s = -2n$, $n \in \mathbb{N}^*$ (*les zéros triviaux*). *L'Hypothése de Riemann* prédit que tous les autres zéros se situent sur *la droite critique* $\Re(s) = 1/2$.

Formule sommatoire de Poisson

5.10. Considérons l'intégrale

$$\int_{C_N} \frac{e^{-\pi z^2 t}}{e^{2\pi i z} - 1} dz = \int_{C_N} \phi(z,t) dz$$

où C_N est le rectangle avec les sommets $\pm N + \frac{1}{2} \pm i$ orienté positivement, N étant un nombre entier, $N > 0$, t une variable complexe, $\Re(t) > 0$.

On a

$$\lim_{N\to\infty} \int_{C_N} \phi(z,t) dz = \left[\int_{-\infty-i}^{\infty-i} - \int_{-\infty+i}^{\infty+i} \right] \phi(z,t) dz =$$

par la formule de Cauchy

$$= \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} =: \psi(t)$$

5.11. D'une autre part, sur la droite $z = u - i,\ -\infty < u < \infty$

$$\phi(z,t) = \frac{e^{-\pi z^2 t}}{e^{2\pi i z} - 1} = e^{-2\pi i z} \frac{e^{-\pi z^2 t}}{1 - e^{-2\pi i z}} =$$

$$= e^{-\pi z^2 t} \sum_{n=1}^{\infty} e^{-2\pi i n z} = \sum_{n=1}^{\infty} e^{-\pi z^2 t - 2\pi i n z} =$$

$$= \sum_{n=1}^{\infty} e^{-\pi t[(z+in/t)^2 - n^2/t^2]},$$

la série convergeant uniformement. Il s'en suit

$$\int_{-\infty-i}^{\infty-i} \phi(z,t) dz = \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty-i}^{\infty-i} e^{-\pi t(z+in/t)^2} dz =$$

$$= \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty-i}^{\infty-i} e^{-\pi t z^2} dz = \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty}^{\infty} e^{-\pi t(u-i)^2} du =$$

$$= \sum_{n=1}^{\infty} e^{-\pi n^2/t} \int_{-\infty}^{\infty} e^{-\pi t u^2} du$$

Supposons que t et réel, $t > 0$. Alors (en posant $v = (\pi t)^{1/2} u$)

$$\int_{-\infty}^{\infty} e^{-\pi t u^2} du = (\pi t)^{-1/2} \int_{-\infty}^{\infty} e^{-v^2} dv = t^{-1/2},$$

donc ceci est vrai pout tous $t, \Re t > 0$. Donc

$$\int_{-\infty-i}^{\infty-i} \phi(z,t) dz = t^{-1/2} \sum_{n=1}^{\infty} e^{-\pi n^2/t}$$

De même,

$$\int_{-\infty+i}^{\infty+i} \phi(z,t)dz = -t^{-1/2}\sum_{n=0}^{\infty} e^{-\pi n^2/t};$$

on en déduit

$$\psi(t) = t^{-1/2}\sum_{n=-\infty}^{\infty} e^{-\pi n^2/t} = t^{-1/2}\psi(t^{-1})$$

5.12. Plus généralement, soit $f(z)$ une fonction entière qui satisfait à l'hypothèse suivante:

quelque soient $N \in \mathbb{Z}_{>0}$ et un sous-ensemble compact $K \subset \mathbb{R}$, en posant $z = x + iy$, on a: $\lim_{x\to\pm\infty} |x^N f(z)| = 0$ uniformement par rapport à $y \in K$.

Posons

$$\phi(z) = \frac{f(z)}{e^{2\pi iz}-1}$$

Alors

$$\left[\int_{-\infty-i}^{\infty-i} - \int_{-\infty+i}^{\infty+i}\right]\phi(z)dz = \lim_{N\to\infty}\int_{C_N}\phi(z)dz = \sum_{n=-\infty}^{\infty} f(n)$$

par la formule de Cauchy.

D'un autre côté,

$$\frac{f(z)}{e^{2\pi iz}-1} = e^{-2\pi iz}\frac{f(z)}{1-e^{-2\pi iz}} = \sum_{n=1}^{\infty} f(z)e^{-2\pi inz}$$

sur la droite $C_- = \{u - i,\ -\infty < u < \infty\}$, d'où

$$\int_{-\infty-i}^{\infty-i} \phi(z)dz = \sum_{n=1}^{\infty}\int_{-\infty}^{\infty} f(u)e^{-2\pi inu}du = \sum_{n=1}^{\infty} \hat{f}(-n),$$

où l'on pose

$$\hat{f}(t) := \int_{-\infty}^{\infty} f(u)e^{2\pi itu}du$$

De même,

$$\int_{-\infty+i}^{\infty+i} \phi(z)dz = -\sum_{n=0}^{\infty} \hat{f}(n)$$

Il s'en suit,

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n) \qquad (P)$$

("*formule sommatoire de Poisson*").

Exercice. Définissons une fonction périodique $g(x) := \sum_{n=-\infty}^{\infty} f(x+n)$. Developper cette fonction en série de Fourier et obtenir une autre démonstration de (P).

Deuxième preuve de Riemann de l'équation fonctionelle

5.13. On part de l'intégrale

$$\Gamma(s/2) = \int_0^\infty x^{s/2-1} e^{-x} dx =$$

$(x = \pi n^2 y)$

$$= \pi^{-s/2} n^s \int_0^\infty y^{s/2-1} e^{-\pi n^2 y} dy,$$

d'où:

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\sum_{n=1}^\infty n^{-s} = \int_0^\infty x^{s/2-1} \cdot \sum_{n=1}^\infty e^{-\pi n^2 x} dx = \int_0^\infty x^{s/2-1} \cdot \tilde{\psi}(x) dx, \tag{5.13.1}$$

où

$$\tilde{\psi}(x) = \sum_{n=1}^\infty e^{-\pi n^2 x},$$

donc

$$\psi(x) = \sum_{n=-\infty}^\infty e^{-\pi n^2 x} = 1 + 2\tilde{\psi}(x)$$

5.14. Maintenant on découpe l'intégrale (5.13.1) en deux:

$$\int_0^\infty x^{s/2-1} \cdot \tilde{\psi}(x) dx = \int_0^1 x^{s/2-1} \cdot \tilde{\psi}(x) dx + \int_1^\infty x^{s/2-1} \cdot \tilde{\psi}(x) dx,$$

où la première, après le changement de variable $x = 1/y$, deviendra:

$$\int_0^1 x^{s/2-1} \cdot \tilde{\psi}(x) dx = -\int_\infty^1 y^{-s/2-1} \tilde{\psi}(1/y) dy$$

Or, l'équation fonctionelle

$$x^{1/2}(1 + 2\tilde{\psi}(x)) = 1 + 2\tilde{\psi}(1/x)$$

fournit:

$$\tilde{\psi}(1/x) = x^{1/2}\tilde{\psi}(x) + \frac{x^{1/2}-1}{2},$$

d'où:

$$-\int_\infty^1 y^{-s/2-1}\tilde{\psi}(1/y) dy = \int_1^\infty y^{-s/2-1/2}\tilde{\psi}(y) dy + \frac{1}{2}\int_1^\infty \left(y^{-s/2-1/2} - y^{-s/2-1}\right) dy$$

Ici:

$$\frac{1}{2}\int_1^\infty \left(y^{-s/2-1/2} - y^{-s/2-1}\right)dy = \frac{1}{2}\left(\frac{y^{-s/2+1/2}}{-(s-1)/2} - \frac{y^{-s/2}}{-s/2}\right)\Bigg|_1^\infty = \frac{1}{s(s-1)}$$

si $\Re(s) > 1$.

Il s'en suit:

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = -\frac{1}{s(1-s)} + \int_1^\infty \left(x^{s/2-1} + x^{(1-s)/2-1}\right)\cdot\tilde{\psi}(x)dx, \tag{5.14.1}$$

si $\Re(s) > 1$. Par contre, l'intégrale à droite est une fonction entière sur tout le plan complexe, donc (5.14.1) est vrai pour tous s.

Or, l'expression à droite ne change pas si l'on remplace s par $1-s$, d'où

$$\xi(s) = \xi(1-s)$$

Fonction $\Xi(t)$

5.15. *Fonction* $\tilde{\xi}(s)$ *et deux intégrations par parties.* On pose

$$\tilde{\xi}(s) = \frac{s(s-1)}{2}\xi(s) = (s-1)\Gamma(s/2+1)\pi^{-s/2}\zeta(s)$$

L'expression intégrale (5.14.1) entraine:

$$\tilde{\xi}(s) = \frac{1}{2} + \frac{s(s-1)}{2}\int_1^\infty \left(x^{s/2-1} + x^{(1-s)/2-1}\right)\cdot\tilde{\psi}(x)dx$$

Faisons l'intégration par parties:

$$I := \int_1^\infty \left(x^{s/2-1} + x^{(1-s)/2-1}\right)\cdot\tilde{\psi}(x)dx = \tilde{\psi}(x)\cdot\left(\frac{x^{s/2}}{s/2} + \frac{x^{(1-s)/2}}{(1-s)/2}\right)\Bigg|_1^\infty -$$

$$-\int_1^\infty \tilde{\psi}'(x)\cdot\left(\frac{x^{s/2}}{s/2} + \frac{x^{(1-s)/2}}{(1-s)/2}\right)dx =$$

(puisque $\tilde{\psi}(\infty) = 0$)

$$= \frac{2\tilde{\psi}(1)}{s(s-1)} - \int_1^\infty \tilde{\psi}'(x)\cdot\left(\frac{x^{s/2}}{s/2} + \frac{x^{(1-s)/2}}{(1-s)/2}\right)dx,$$

d'où

$$\tilde{\xi}(s) = \frac{1}{2} + \frac{s(s-1)}{2}I = \frac{1}{2} + \tilde{\psi}(1) + \int_1^\infty \tilde{\psi}'(x)\cdot\left((1-s)x^{s/2} + sx^{(1-s)/2}\right)dx$$

Faisons encore une fois une intégration par parties:

$$I' := \int_1^\infty \tilde{\psi}'(x)\cdot\big((1-s)x^{s/2}+sx^{(1-s)/2}\big)dx = \int_1^\infty x^{3/2}\tilde{\psi}'(x)\cdot\big((1-s)x^{s/2-3/2}+sx^{-s/2-1}\big)dx =$$

$$-x^{3/2}\tilde{\psi}'(x)\cdot\left(2x^{s/2-1/2}+2x^{-s/2}\right)\Big|_1^\infty +$$

$$+\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}\cdot\left(2x^{s/2-1/2}+2x^{-s/2}\right)dx =$$

$$= 4\tilde{\psi}'(1)+2\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\left(x^{s/2-1/4}+x^{-s/2+1/4}\right)dx$$

Il s'en suit:

$$\tilde{\xi}(s) = \frac{1}{2}+\tilde{\psi}(1)+4\tilde{\psi}'(1)+2\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\left(x^{s/2-1/4}+x^{-s/2+1/4}\right)dx$$

5.16. *Exercice.* Montrer que $\frac{1}{2}+\tilde{\psi}(1)+4\tilde{\psi}'(1)=0$.

Il s'en suit que

$$\tilde{\xi}(s) = 2\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\left(x^{s/2-1/4}+x^{-s/2+1/4}\right)dx$$

5.17. *Droite critique.* Posons maintenant $s = 1/2+it$. Alors on aura:

$$x^{s/2-1/4}+x^{-s/2+1/4} = x^{it/2}+x^{-it/2} = 2\cos(t\log x/2),$$

d'où

$$\Xi(t) := \tilde{\xi}(\frac{1}{2}+it) = 4\int_1^\infty \frac{d(x^{3/2}\tilde{\psi}'(x))}{dx}x^{-1/4}\cdot\cos(t\log x/2)dx$$

5.18. *Exercice.* Considérons la fonction $h(x) = (x^{3/2}\tilde{\psi}'(x))'$. Montrer que $h(x^{-1}) = x^2h(x)$.

§??? Le théorème de la progression arithmétique

Le but de ce Chapitre est de démontrer le théorème suivant:

Théorème, (P.G. Lejuene-Dirichlet, [D]). Soient a, m deux entiers ≥ 1, premiers entre eux. Il existe une infinité de nombres premiers p tels que $p \equiv a \bmod m$.

pa.1. *Caractères.* Soit G un groupe abélien fini. *Un caractère* de G est un homomorphisme $\chi : \ G \longrightarrow \mathbb{C}^*$; ces valeurs sont des racines de l'unité. Les caractères forment un groupe abélien $\hat{G}$.

Exercices. (i) Soit $H \subset G$ un sous-groupe. Montrer que chaque caractère $\chi \in \hat{H}$ se prolonge en un caractère de G. En déduire la suite exacte

$$1 \longrightarrow (G/H)^\wedge \longrightarrow \hat{G} \longrightarrow \hat{H} \longrightarrow 1$$

Idée. Pour $x \in G \setminus H$ prolonger χ en un caractère de $H' =< H, x >$ en définissant $\chi(x)$ a partir de nombre n minimal tel que $x^n = y \in H$ et $\chi(y)$ connu.

(ii) Montrer que $\hat{G}$ est fini, $|\hat{G}| = |G|$ (utilisez (i)).

(iii) Montrer que pour $x \in G$, $x \neq 1$ il existe $\chi \in \hat{G}$ tel que $\chi(x) \neq 1$.

(iv) Un homomorphisme naturel $G \longrightarrow \hat{\hat{G}}$ est un isomorphisme.

(v) Pour $x \in G$, $x \neq 1$, on a $\sum_\chi \ \chi(x) = 0$.

Séries de Dirichlet

pa.2. Soit $\{\lambda_n\}$ une suite strictement croissante, $\lambda_n \geq 0$, $\lim_{n\to\infty} \lambda_n = \infty$. On va considérer les séries de la forme

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}, \ a_n, s \in \mathbb{C} \qquad (pa.2.1)$$

Exemple $\lambda_n = \log n$, $f(s) = \sum a_n n^{-s}$.

pa.2.1. *Théorème.* Si la série (pa.2.1) converge pour $s = s_0$, elle converge uniformement dans tout domaine de la forme $\Re s \geq \Re s_0$, $|\arg\, s| \leq \alpha$, avec $\alpha < \pi/2$.

pa.2.2. *Lemme* (Abel). Soient $\{a_n\}$, $\{b_n\}$ deux suites. Posons

$$A_{mn} = \sum_{p=m}^{n} a_p, \ S_{mn} = \sum_{p=m}^{n} a_p b_p$$

On a alors:

$$S_{mn} = \sum_{p=m}^{n-1} A_{mp}(b_p - b_{p+1}) + A_{mn}b_n$$

Preuve: exercice.

pa.2.3. *Lemme.* Soient $\beta > \alpha > 0$, $z = x + iy$, $x > 0$. Alors

$$|e^{-\alpha z} - e^{-\beta z}| \leq |z/x|(e^{-\alpha x} - e^{-\beta x})$$

Preuve.

$$e^{-\alpha z} - e^{-\beta z} = z \int_\alpha^\beta e^{-tz} dt,$$

d'où, en passant au valeurs absolues,

$$|e^{-\alpha z} - e^{-\beta z}| = |z| \int_\alpha^\beta e^{-tx} dt = |z/x|(e^{-\alpha x} - e^{-\beta x})$$

Preuve de pa.2.1. Quitte à effectuer une translation sur z, on peut supposer que $z_0 = 0$.

Il faut démontrer qu'il y a convergence uniforme dans tout domaine de la forme $x = \Re z \geq 0$, $|z/x| \leq k$. Puisque la série $\sum a_n$ converge, pour tout $\epsilon > 0$ il existe un N tel que $|A_{mn}| \leq \epsilon$ pour tous $m, n \geq N$. D'après le lemme d'Abel avec $b_n = e^{-\lambda_n z}$,

$$S_{mn} = \sum_{p=m}^{n-1} A_{mp}(e^{-\lambda_p z} - e^{-\lambda_{p+1} z}) + A_{mn}e^{-\lambda_n z},$$

d'où, en appliquant le lemme pa.2.3,

$$|S_{mn}| \leq \epsilon(1 + (|z|/x) \sum_{p=m}^{n-1} (e^{-\lambda_p x} - e^{-\lambda_{p+1} x})$$

$$= \epsilon(1 + (|z|/x)(e^{-\lambda_n x} - e^{-\lambda_m x}) \leq \epsilon(1 + k),$$

d'où le resultat. $\square$

pa.3. *Corollaire.* (a) Si $f(s)$ converge pour $s = s_0$, elle converge dans le domaine $\Re s > \Re s_0$ et définit dans ce domaine la fonction holomorphe.

(b) $f(s)$ ne peut être identiquement nulle que si tous les coefficients a_n sont nuls.

Démonstration. (b) Supposons que $f(s) \equiv 0$. Multiplions $f(s)$ par $e^{\lambda_1 s}$ et faisons tendre $s \to \infty$ en restant dans $\mathbb{R}$. Alors on aura

$$0 = \lim_{s\to\infty} e^{\lambda_1 s} f(s) = a_1$$

grace à convergence uniforme. En continuant, on obtient $a_2 = 0$, etc.

pa.4. *Théorème* (E. Landau). Soit $f(s) = \sum a_n e^{-\lambda_n s}$ comme dans pa.1, avec les coefficients $a_n \in \mathbb{R}_{\geq 0}$. Supposons que $f(s)$ converge pour $\Re s > \rho \in \mathbb{R}$ et puisse être prolongée en une fonction holomorphe au voisinage de $s = \rho$. Alors il existe $\epsilon > 0$ tel que $f(s)$ converge pour $s > \rho - \epsilon$.

Autrement dit, le demi-plan de convergence de $f(s)$ et borné par la droite verticale qui coupe la droite réelle en singularité de $f(s)$.

Démonstration. Quitte à remplacer s par $s-\rho$, on peut supposer que $\rho = 0$. Par hypothèse, il existe $\epsilon > 0$ tel que $f(s)$ est holomorphe dans le disque $|s-1| \leq 1+\epsilon$.

Grace à convergence uniforme (Thm. pa.2.1), on a

$$f^{(p)}(s) = \sum_n a_n(-\lambda_n)^p e^{-\lambda_n s}$$

pour $\Re(s) > 0$, donc

$$f^{(p)}(1) = (-1)^p \sum_n a_n \lambda_n^p e^{-\lambda_n}$$

La série de Taylor de $f(s)$ autour $s = 1$ s'écrit

$$f(s) = \sum_{p=0}^{\infty} \frac{(s-1)^p}{p!} f^{(p)}(1) \tag{$*$}$$

On va utiliser le

pa.4.1. *Lemme.* Si $f(s)$ est une fonction holomorphe dans un disque $|s-s_0| \leq R$ alors la série de Taylor $\sum_0^\infty f^{(p)}(s_0)(s-s_0)^p/p!$ converge dans ce disque vers $f(s)$.

(Autrement dit, le disque de convergence de la série de Taylor d'une fonction holomorphe est borné par une singularité de cette fonction.) □

Il s'en suit qu'on on peut poser $s = -\epsilon$ dans (*):

$$f(-\epsilon) = \sum_{p=0}^{\infty} \frac{(1+\epsilon)^p(-1)^p}{p!} f^{(p)}(1)$$

Or,

$$(-1)^p f^{(p)}(1) = \sum_n a_n \lambda_n^p e^{-\lambda_n}$$

est une série convergente à termes positifs. Il s'en suit que la série double à termes positifs

$$f(-\epsilon) = \sum_{p,n} \frac{a_n}{p!}(1+\epsilon)^p \lambda_n^p e^{-\lambda_n}$$

converge, donc on peut regrouper ses termes:

$$f(-\epsilon) = \sum_n a_n e^{-\lambda_n} \sum_p \frac{(1+\epsilon)^p \lambda_n^p}{p!} = \sum_n a_n e^{\lambda_n \epsilon}$$

En d'autres termes, la série de Dirichlet converge pour $s = -\epsilon$, donc pour $\Re(s) \geq \epsilon$. $\square$.

Dorénavant, on va considérer que les séries de la forme

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

pa.5. *Proposition.* (a) Si les a_n sont bornés, $f(s)$ converge absolument pour $\Re(s) > 1$.

(b) Si les sommes partielles $A_{mn} = \sum_{i=m}^{n} a_i$ sont bornées, $f(s)$ converge (pas nécessairement absolument) pour $\Re s > 0$.

Preuve. (a) est clair. Pour démontrer (b), appliquons le lemme d'Abel: si $|A_{mn}| \leq C$, on aura:

$$|S_{mm'}| \leq C\left(\sum_{n=m}^{m'} |n^{-s} - (n+1)^{-s}| + |m'^{-s}|\right)$$

D'après 2.1, on peut supposer que s est réel; il s'en suit que

$$|S_{mm'}| \leq Cm^{-s},$$

d'où la convergence pour $\Re(s) > 0$. $\square$

pa.6. *Produits Euleriens.* On note $\mathbb{P}$ l'ensemble des nombres premiers, $\mathbb{N} = \mathbb{Z}_{\geq 1}$.

pa.6.1. *Lemme.* Soit $f : \mathbb{N} \longrightarrow \mathbb{C}$ une fonction bornée et multiplicative, c'est à dire, $f(mn) = f(m)f(n)$ pour tout m, n. Alors

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_{p\in\mathbb{P}} (1 - f(p)p^{-s})^{-1},$$

deux termes convergent absolument pour $\Re s > 1$.

Fonctions $L(s, \chi)$

pa.7. *Caractères de Dirichlet.* Notations: $G(m)$ - le groupe des éléments inversibles de $\mathbb{Z}/m\mathbb{Z}$. *Un caractére modulo m* est un homomorphisme $\chi : G(m) \longrightarrow \mathbb{C}^*$. On va considérer χ comme une fonction $\mathbb{Z} \longrightarrow \mathbb{C}$ en posant $\chi(n) = 0$ si n n'est pas premier à m. $G(m)^*$: le groupe de tous caractères.

pa.8. Pour $\chi \in G(m)^*$ on pose

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

la série converge absolument pour $\Re(s) > 1$.

pa.8.1. *Proposition.* (a) Pour $\chi = 1$,

$$L(s,1) = \zeta(s) \prod_{p|m} (1 - p^{-s})$$

Par conséquence, $L(s,1)$ est prolongeable analytiquement pour $\Re s > 0$, et admèt $s = 1$ pour pôle simple.

(b) Si $\chi \neq 1$, la série $L(s,\chi)$ converge (resp. converge absolument) dans le demi-plan $\Re s > 0$ (resp. $\Re s > 1$), et

$$L(s,\chi) = \prod_{p\in\mathbb{P}} (1 - \chi(p)p^{-s})^{-1}, \ \Re(s) > 1$$

Démonstration. (a) est clair. (b). D'après pa.5 (b), il suffit de remarquer que les sommes $A_{mm'} = \sum_{n=m}^{m'} \chi(n)$ sont bornés pour $\chi \neq 1$. $\square$

pa.9. Fixons un entier $m \geq 1$. Pour un nombre premier $p \nmid m$ notons $\bar{p}$ son image dans $G(m)$, $f(p)$ son ordre dans $G(m)$ et posons $g(p) = \phi(m)/f(p)$.

On définit

$$\zeta_m(s) = \prod_{\chi\in G(m)^*} L(s,\chi)$$

Ici $G(m)^*$ désigne le groupe de tous les caractères de $G(m)$.

pa.10. *Proposition.* On a:

$$\zeta_m(s) = \prod_{p\nmid m} (1 - p^{-f(p)s})^{-g(p)}$$

C'est une série de Dirichlet à coefficients entiers ≥ 0, convergeant dans le demi-plan $\Re s > 1$.

Cette Proposition est une conséquence d'un

Exercice. Soit x une indeterminée. Alors pour $p \nmid m$,

$$\prod_{\chi\in G(m)^*} (1 - \chi(p)x) = (1 - x^{f(p)})^{g(p)}$$

(Utilisez l'identité $\prod_{w\in\mu_{f(p)}} (1 - wx) = 1 - x^{f(p)}$.)

pa.11. *Théorème.* (a) $\zeta_m(s)$ a un pôle simple pour $s = 1$.

(b) $L(1,\chi) \neq 0$ pour tout $\chi \neq 1$.

Preuve. (b) $\Rightarrow$ (a) puisque $L(s,1)$ ait un pôle simple pour $s = 1$. Si l'on avait $L(1,\chi) = 0$ pour un $\chi \neq 1$, $\zeta_m(s)$ serait holomorphe pour $\Re s > 0$, donc, d'après le théorème de Landau pa.4, la série de Dirichlet qui définit $\zeta_m(s)$ serait convergeant pour $\Re s > 0$.

Voyons que s'est absurde. En effet,

$$(1 - p^{-f(p)s})^{-g(p)} = (\sum_{i=0}^{\infty} p^{-if(p)s})^{g(p)} \geq \sum_{i=0}^{\infty} p^{-i\phi(m)s}$$

Il s'en suit que la série de Dirichlet de $\zeta_m(s)$ domine la série

$$\sum_{(n,m)=1} n^{-\phi(m)s}$$

laquelle diverge pour $s = 1/\phi(m)$ (expliquez pourquoi). $\square$

pa.12. *Lemme.* Lorsque $s \to 1+$, on a

$$\sum_{p\in\mathbb{P}} p^{-s} \sim \log 1/(s-1)$$

(On écrit $A(s) \sim B(s)$ si $A(s)/B(s) \to 1$.)

Preuve. On a

$$\log\zeta(s) = \sum_{p,k\geq 1} (kp^{ks})^{-1} = \sum_p p^{-s} + \sum_{p,k\geq 2} (kp^{ks})^{-1}$$

Or, si $s > 1$,

$$\sum_{p,k\geq 2} (kp^{ks})^{-1} \leq \sum_{p,k\geq 2} p^{-ks} = \sum_p 1/(p^s(p^s-1)) \leq \sum_p 1/(p(p-1)) \leq \sum_{n\geq 2} 1/(n(n-1)) = 1$$

Donc $\sum_p p^{-s} \sim \log\zeta(s) \sim \log 1/(s-1)$ lorsque $s \to 1+$. $\square$

pa. 13. *Définition.* Un sous-ensemble $A \subset \mathbb{P}$ *a pour densité* un nombre reél k, $0 \leq k \leq 1$, si

$$\sum_{p\in A} p^{-s} \sim k\log 1/(s-1)$$

lorsque $s \to 1+$.

pa.14. *Théorème* (Dirichlet). Soient $m, a \in \mathbb{Z}$, $m \geq 1$, $(a,m) = 1$. L'ensemble $\mathbb{P}_a$ de nombres premiers $p \equiv a \bmod m$ a pour densité $1/\phi(m)$.

pa.15. Soit χ un caractère de $G(m)$. Définissons

$$f_\chi(s) = \sum_{p\nmid m} \chi(p)p^{-s}$$

pa.15.1. *Lemme.* (a) Si $\chi = 1$, on a $f_\chi(s) \sim \log(1/(s-1))$ pour $s \to 1+$.

(b) Si $\chi \neq 1$, $f_\chi(s)$ reste borné lorsque $s \to 1+$.

Preuve. (a) $f_1(s)$ ne diffère de $\sum_p p^{-s}$ que par un nombre fini de termes.

(b) On a pour $s > 1$:

$$\log L(s,\chi) = \sum_p \log((1-\chi(p)p^{-s})^{-1}) = \sum_{p,k\geq 1} \chi(p)^k/(kp^{ks}) = f_\chi(s) + F_\chi(s),$$

où

$$F_\chi(s) = \sum_{p,k\geq 2} \chi(p)^k/(kp^{ks})$$

On a

$$|F(s)| \leq \sum_{p,k\geq 2} 1/(kp^{ks}) \leq 1$$

cf. la preuve de pa.12. Puisque $\log L(s,\chi)$ reste borné lorsque $s \to 1$, il en est de même de $f_\chi(s)$. □

pa.16. Considérons la fonction

$$g_a(s) = \sum_{p\in\mathbb{P}_a} \frac{1}{p^s}$$

pa.16.1. *Lemme* (transformation de Fourier).

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi\in\mathrm{Char}(G(m))} \chi(a)^{-1} f_\chi(s)$$

Exercice.

pa.17. *Fin de la preuve de* pa.14. Faisons tendre $s \to 1+$ dans pa.16.1; on obtient $g_a(s) \to (1/\phi(m)) \cdot \log 1/(s-1)$, d'où l'assertion. □

§??? Théorème de nombres premiers

tnp.1. Pour un réel x strictement positif, soit $\pi(x) :=$ le nombre de nombres premiers $p \leq x$. Le théorème de nombres premiers, ou *la loi asymptotique de la distribution de nombres premiers* est l'assertion suivante.

tnp.1.1. *Théorème* (J. Hadamard, Ch. de la Vallée-Poussin).

$$\lim_{x\to\infty} \pi(x)/(x/\log(x)) = 1$$

Cette assertion a été conjecturé par Gauss et démontrée par Jacques Hadamard et Charles de la Vallée-Poussin en 1896, simultanément et independemment, cf. [H], [VP].

Fonctions de Tchebychev $\psi(x)$ et $\vartheta(x)$ et fonction de von Mangoldt $\Lambda(x)$

tnp.2. Pour $x \in \mathbb{R},\ x > 0$ on pose

$$\vartheta(x) = \sum_{p \text{ premier},\ p\leq x} \log p$$

$$\psi(x) = \sum_{p \text{ premier},\ m\in\mathbb{Z}_{>0},\ p^m\leq x} \log p$$

Autrement dit, si $a_p(x) = [\log x/\log p]$ est la puissance maximale m telle que $p^m \leq x$ alors

$$\psi(x) = \sum_{p \textit{ premier}} a_p(x)\log p \qquad (tnp.2.1)$$

On a

$$\psi(x) = \sum_{n=1}^{\infty} \vartheta(x^{1/n}), \qquad (tnp.2.2)$$

la somme étant finie puisque $\vartheta(x) = 0$ si $x < 2$.

On introduit aussi une *fonction de von Mangoldt*

$$\Lambda(n) = \log p \text{ si } n = p^m,\ m > 0,\ 0 \text{ sinon}$$

Alors il est clair que

$$\psi(x) = \sum_{n\leq x} \Lambda(n)$$

tnp.3. *Théorème* (Tchebychev). Si l'une de trois limites

$$\lim_{x\to\infty} \vartheta(x)/x,\ \lim_{x\to\infty} \psi(x)/x,\ \lim_{x\to\infty} \pi(x)/(x/\log(x))$$

existe, alors deux autres existent aussi, et les trois limites coïncident.

Preuve. Le théorème est une conséquence immédiate du

tnp.3.1. *Lemme.* Posons

$$\ell_1 = \varliminf_{x\to\infty} \pi(x)/(x/\log x), L_1 = \varlimsup_{x\to\infty} \pi(x)/(x/\log x)$$

$$\ell_2 = \varliminf_{x\to\infty} \vartheta(x)/x, L_2 = \varlimsup_{x\to\infty} \vartheta(x)/x$$

$$\ell_3 = \varliminf_{x\to\infty} \psi(x)/x, L_3 = \varlimsup_{x\to\infty} \psi(x)/x$$

Alors $L_1 = L_2 = L_3$ et $\ell_1 = \ell_2 = \ell_3$.

Démonstration. On a $\vartheta(x) \leq \psi(x)$. D'un autre côté,

$$\psi(x) \leq \sum_{p\leq x} \frac{\log x}{\log p} \log p = \pi(x) \log x,$$

i.e.

$$\vartheta(x) \leq \psi(x) \leq \pi(x) \log x$$

En divisant par x et en passant aux limites, on obtient $L_2 \leq L_3 \leq L_1$, $\ell_2 \leq \ell_3 \leq \ell_1$.

Soit $\alpha \in \mathbb{R}$, $0 < \alpha < 1$ et $x > 1$. Alors

$$\vartheta(x) \geq \sum_{x^\alpha < p \leq x} \log p \geq$$

puisque $\log p > \log x^\alpha$

$$\geq \alpha \log x(\pi(x) - \pi(x^\alpha)) > \alpha \log x(\pi(x) - x^\alpha),$$

d'où

$$\frac{\vartheta(x)}{x} > \alpha\pi(x)\frac{\log x}{x} - \alpha\frac{\log x}{x^{1-\alpha}}$$

Or, $\log x/x^{1-\alpha} \to 0$ lorsque $x \to \infty$, d'où $L_2 \geq \alpha L_1$ et $\ell_2 \geq \alpha\ell_1$. Puisque $\alpha < 1$ est arbitraire, $L_2 \geq L_1$ et $\ell_2 \geq \ell_1$, d'où l'assertion du Lemme. □.

tnp.4. En prenant la dérivée logarithmique du produit d'Euler

$$\zeta(s) = \prod_{p \textit{ premier}} (1 - p^{-s})^{-1}, \ \Re s > 1$$

on obtient

$$-\zeta'(s)/\zeta(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

tnp.5. *Théorème.* Pour $s \in \mathbb{R}$, $s > 1$,

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(y)dy}{y^{s+1}}$$

En faisant $y = e^x$ on obtient comme corollaire:

$$-\frac{\zeta'(s)}{s\zeta(s)} = \int_0^\infty \psi(e^x)e^{-xs}dx,\ \Re(s) > 1 \qquad (tnp.5.1)$$

Pour la preuve du théorème on utilise

tnp.5.1. *Théorème* (Abel). Soient $0 \leq \lambda_1 \leq \lambda_2 \leq \ldots$, $\lim_{n\to\infty} \lambda_n = \infty$, $a_n \in \mathbb{C},\ n = 1, 2, \ldots$.

Posons

$$A(x) = \sum_{\lambda_n \leq x} a_n$$

Soit $\phi(x) \in \mathbb{C}$ une fonction, $x \geq 0$. Alors

(a)

$$\sum_{n=1}^{k} a_n\phi(\lambda_n) = A(\lambda_k)\phi(\lambda_k) - \sum_{n=1}^{k-1} A(\lambda_n)(\phi(\lambda_{n+1}) - \phi(\lambda_n))$$

(b) Si $\phi \in C^1(0, \infty)$ et $x \geq \lambda_1$,

$$\sum_{\lambda_n \leq x} a_n\phi(\lambda_n) = A(x)\phi(x) - \int_{\lambda_1}^{x} A(t)\phi'(t)dt$$

(c) Si de plus $\lim_{x\to\infty} A(x)\phi(x) = 0$,

$$\sum_{n=1}^{\infty} a_n\phi(\lambda_n) = -\int_{\lambda_1}^{\infty} A(t)\phi'(t)dt$$

Preuve: exercice.

Démonstration du Th. tnp.5. Prenons dans tnp.5.1 $\lambda_n = n,\ a_n = \Lambda(n)$ et $\phi(x) = x^{-s}$; alors $A(x) = \psi(x)$ Puisque $\psi(x) \leq \pi(x)\log x < x\log x$, $A(x)\phi(x) < x^{1-s}\log x \to 0$ si $x \to \infty$. On conclut que

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s\int_1^\infty \psi(x)x^{-s-1}dx,$$

cqfd. $\square$

tnp. 6. *Théorème* (J. Hadamard, Ch. de la Vallée Poussin). $\zeta(1 + it) \neq 0$ si $t \in \mathbb{R},\ t \neq 0$.

Preuve. Posons $s = \sigma + it$. Si $\sigma > 1$,

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

donc

$$\log \zeta(s) = \sum_{m\geq 1, p} \frac{1}{mp^s} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

où $c_n = m^{-1}$ si $n = p^m$, 0 sinon. De là,

$$\log |\zeta(s)| = \Re(\log(\zeta(s)) = \Re(\sum_n c_n n^{-s}) = \sum_{n=2}^{\infty} \frac{c_n}{n^\sigma} \cos(t \log n),$$

si $\sigma > 1$.

On a $c_n \geq 0$ et

$$3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2 \geq 0$$

pour tout $\theta \in \mathbb{R}$. Il s'en suit,

$$\log |\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| = \sum_n c_n(3 + 4\cos(t\log n) + \cos(2t\log n)) \geq 0$$

pour $\sigma > 0$, d'où

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \geq 1$$

donc

$$|(\sigma - 1)\zeta(\sigma)|^3 \left|\frac{\zeta(\sigma + it)}{\sigma - 1}\right|^4 |\zeta(\sigma + 2it)| \geq \frac{1}{\sigma - 1} \qquad (*)$$

Supposons que $\zeta(1 + it_0) = 0$, $t_0 \neq 0$. Posons dans (*) $t = t_0$ et faisons tendre $\sigma \to 1+$. Alors on aura ∞ à droite, tandis que à gauche viendra $|\zeta'(1 + it_0)|^4 |\zeta(\sigma + 2it_0)| < \infty$ puisque $\zeta(s)$ est analytique si $\sigma > 0, s \neq 1$. Contradiction. $\square$

Théorème de Wiener - Ikehara

tnp 7. *Théorème* (N. Wiener, [W]; S. Ikehara, [I]). Soit $A: \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}$ une fonction croissante (i.e. $x \leq y$ implique $A(x) \leq A(y)$). Supposons que l'intégrale

$$f(s) = \int_0^\infty A(x)e^{-xs}dx$$

converge pour $\Re(s) > 1$ et définit une fonction holomorphe en s qui se prolonge en une fonction holomorphe dans le demi-plan fermé $\{\Re(s) \geq 1\}$ sauf un pôle simple en $s = 1$ avec le résidu 1.

Alors $\lim_{x\to\infty} A(x)e^{-x} = 1$.

Preuve (cf. [Ch]). On pose $B(x) = e^{-x}A(x)$.

tnp.8. *Lemme.* Pour tous $\lambda > 0$

$$\lim_{y\to\infty}\int_{-\infty}^{\lambda y} B(y-v/\lambda)\frac{\sin^2 v}{v^2}dv = \pi \qquad (tnp.8.1)$$

Preuve. On a

$$\frac{1}{s-1} = \int_0^\infty e^{-(s-1)x}dx,$$

si $\Re(s) > 1$, d'où

$$g(s) := f(s) - \frac{1}{s-1} = \int_0^\infty (B(x)-1)e^{-(s-1)x}dx,$$

si $\Re(s) > 1$. Posons

$$g_\epsilon(t) = g(1+\epsilon+it)\ (\epsilon > 0, t \in \mathbb{R})$$

Pour chaque $\lambda > 0$ considérons l'intégrale

$$I(\epsilon) := \frac{1}{2}\int_{-2\lambda}^{2\lambda} g_\epsilon(t)(1-|t|/2\lambda)e^{iyt}dt =$$

$$= \frac{1}{2}\int_{-2\lambda}^{2\lambda} e^{iyt}(1-|t|/2\lambda)\left(\int_0^\infty (B(x)-1)e^{-(\epsilon+it)x}dx\right)dt \qquad (tnp.8.2)$$

tnp.8.1. *Sous-lemme.* Dans $I(\epsilon)$ on peut interchanger l'ordre d'intégration.

Preuve. $A(x)$ est croissante et positive, donc

$$f(s) = \int_0^\infty A(u)e^{-us}du \geq A(x)\int_x^\infty e^{-us}du = A(x)e^{-xs}/s$$

pour $s > 1, x > 0$, i.e. $A(x) \leq sf(s)e^{xs}$. Il s'en suit que $A(x) = O(e^{xs})$ quand $x \to \infty$ pour chaque $s > 1$, donc $A(x) = o(e^{xs})$ pour chaque $s > 1$. Il vient que $B(x)e^{-\delta x} = A(x)e^{-(1+\delta)x} = o(1)$ pour chaque $\delta > 0$. Il s'en suit que l'intégrale

$$\int_0^\infty (B(x)-1)e^{-(\epsilon+it)x}dx$$

converge uniformement pour $-2\lambda \leq t \leq 2\lambda$, donc on peut interchanger deux intégrales dans (tnp.8.2). $\square$

Il vient:

$$I(\epsilon) = \frac{1}{2}\int_0^\infty (B(x)-1)e^{-\epsilon x}\left(\int_{-2\lambda}^{2\lambda} e^{i(y-x)t}(1-|t|/2\lambda)dt\right)dx$$

tnp.8.2. *Sous-lemme.*

$$\frac{1}{2}\int_{-2\lambda}^{2\lambda} e^{iat}(1-|t|/2\lambda)dt = \frac{\sin^2(a\lambda)}{a^2\lambda}$$

Preuve: exercice.

Il s'en suit:

$$I(\epsilon) = \int_0^\infty (B(x)-1)e^{-\epsilon x}\frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx$$

Maintenant passons à la limite $\epsilon \to 0$: d'un côté par hypothèse $g_\epsilon(t) \to g(1+it)$ uniformément sur $[-2\lambda, 2\lambda]$, donc

$$\lim_{\epsilon\to 0} I_\epsilon = \frac{1}{2}\int_{-2\lambda}^{2\lambda} g(1+it)(1-|t|/2\lambda)e^{iyt}dt$$

De l'autre côté,

$$\lim_{\epsilon\to 0}\int_0^\infty e^{-\epsilon x}\frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx = \int_0^\infty \frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx > 0$$

par convergence monotone. Il s'en suit de (tnp.8.2) que la limite

$$\lim_{\epsilon\to 0}\int_0^\infty B(x)e^{-\epsilon x}\frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx$$

existe, et encore par convergence monotone elle est égale à

$$\int_0^\infty B(x)\frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx$$

Donc on obtient après passage à la limite $\epsilon \to 0$:

$$\frac{1}{2}\int_{-2\lambda}^{2\lambda} g(1+it)(1-|t|/2\lambda)e^{iyt}dt =$$

$$\int_0^\infty B(x)\frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx - \int_0^\infty \frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx \qquad (tnp.8.3)$$

Finalement, passons à la limite $y \to \infty$.

tnp.8.3. *Lemme de Riemann - Lebesgue.*

$$\lim_{y\to\infty}\int_{-a}^{a}\phi(t)e^{iyt}dt = 0$$

Donc le premier terme de (tnp.8.3) tend vers 0. Ensuite,

$$\lim_{y\to\infty}\int_0^\infty \frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda}dx = \lim_{y\to\infty}\int_{-\infty}^{\lambda y}\frac{\sin^2 v}{v^2}dx = \int_{-\infty}^{\infty}\frac{\sin^2 v}{v^2}dx$$

tnp.8.4. *Sous-lemme.*

$$\int_{-\infty}^{\infty}\frac{\sin^2 v}{v^2}dx = \pi$$

Preuve: exercice. Idée: par l'intégration par parties réduire l'intégrale à
$$\int_{-\infty}^{\infty} \frac{\sin v}{v} dx = \pi$$
Cette intégrale se calcule en appliquant la formule de résidus au contour $C_{r,R} = \{r \le z \le R\} \cup \{z = Re^{i\theta} | 0 \le \theta \le \pi\} \cup \{R \ge z \ge r\} \cup \{z = re^{i\theta} | \pi \le \theta \le 2\pi\}$ et en faisant tendre $r \to 0,\ R \to \infty$. $\square$

Le terme restant de (tnp.8.3) sera
$$\lim_{y\to\infty} \int_0^\infty B(x) \frac{\sin^2((y-x)\lambda)}{(y-x)^2\lambda} dx = \lim_{y\to\infty} \int_{-\infty}^{\lambda y} B(y - v/\lambda) \frac{\sin^2 v}{v^2} dx$$
Donc
$$\lim_{y\to\infty} \int_{-\infty}^{\lambda y} B(y - v/\lambda) \frac{\sin^2 v}{v^2} dx = \pi,$$
ce qui achève la démonstration du Lemme tnp.8. $\square$

tnp.9. Ici on va déduire du Lemme 8 que $\lim_{x\to\infty} B(x) = 1$, ce qui achevera la démonstration du Théorème de Wiener - Ikehara.

(i)
$$\overline{\lim_{y\to\infty}}\, B(y) \le 1 \qquad (tnp.9.1)$$

Preuve. Pour $a, \lambda > 0$ fixés et $y > a/\lambda$ variable on a d'après tnp.8:
$$\overline{\lim_{y\to\infty}} \int_{-a}^{a} B(y - v/\lambda) \frac{\sin^2 v}{v^2} dv \le \pi$$
car $B(x)$ est positive. La fonction $A(u) = B(u)e^u$ est croissante, donc
$$e^{y-a/\lambda} B(y - a/\lambda) \le e^{y-v/\lambda} B(y - v/\lambda)$$
si $-a \le v \le a$. Il s'en suit:
$$B(y - v/\lambda) \ge B(y - a/\lambda) e^{(v-a)/\lambda} \ge B(y - a/\lambda) e^{-2a/\lambda}$$
d'où
$$\pi = \overline{\lim_{y\to\infty}} \int_{-a}^{a} B(y - v/\lambda) \frac{\sin^2 v}{v^2} dv \ge \overline{\lim_{y\to\infty}} \int_{-a}^{a} B(y - a/\lambda) e^{-2a/\lambda} \frac{\sin^2 v}{v^2} dv =$$
$$\overline{\lim_{y\to\infty}}\, B(y - a/\lambda) e^{-2a/\lambda} \int_{-a}^{a} \frac{\sin^2 v}{v^2} dv = e^{-2a/\lambda}\, \overline{\lim_{y\to\infty}}\, B(y) \int_{-a}^{a} \frac{\sin^2 v}{v^2} dv$$
pour tout $a, \lambda > 0$. Maintenant faisons tendre $a, \lambda \to \infty$ de telle façon que $a/\lambda \to 0$; on obtient:
$$\overline{\lim_{y\to\infty}}\, B(y) \cdot \pi = \overline{\lim_{y\to\infty}}\, B(y) \int_{-\infty}^{\infty} \frac{\sin^2 v}{v^2} dv \le \pi,$$

d'où (tnp.9.1) $\square$

(ii)

$$\varliminf_{y\to\infty} B(y) \geq 1 \tag{tnp.9.2}$$

Preuve. (tnp.9.1) implique qu'il existe $c > 0$ tel que $B(x) \leq c$ pour tout $x \geq 0$. Il s'en suit que, étant donnés $a, \lambda > 0$, on a pour tout $y \geq a/\lambda$:

$$\int_{-\infty}^{\lambda y} B(y - v/\lambda)\frac{\sin^2 v}{v^2}dv \leq$$

$$\leq c\biggl(\int_{-\infty}^{-a} + \int_a^{\infty}\biggr)\frac{\sin^2 v}{v^2}dv + \int_{-a}^{a} B(y - v/\lambda)\frac{\sin^2 v}{v^2}dv$$

Comme tout-à l'heure,

$$B(y - v/\lambda) \leq B(y + a/\lambda)e^{2a/\lambda}$$

pour tout $-a \leq v \leq a$, d'où

$$\int_{-a}^{a} B(y - v/\lambda)\frac{\sin^2 v}{v^2}dv \leq B(y + a/\lambda)e^{2a/\lambda}\int_{-a}^{a}\frac{\sin^2 v}{v^2}dv$$

Il vient:

$$\pi = \lim_{y\to\infty}\int_{-\infty}^{\lambda y} B(y - v/\lambda)\frac{\sin^2 v}{v^2}dv \leq$$

$$\leq c\biggl(\int_{-\infty}^{-a} + \int_a^{\infty}\biggr)\frac{\sin^2 v}{v^2}dv + \varliminf_{y\to\infty} B(y + a/\lambda)e^{2a/\lambda}\int_{-a}^{a}\frac{\sin^2 v}{v^2}dv =$$

$$= c\biggl(\int_{-\infty}^{-a} + \int_a^{\infty}\biggr)\frac{\sin^2 v}{v^2}dv + \varliminf_{y\to\infty} B(y)e^{2a/\lambda}\int_{-a}^{a}\frac{\sin^2 v}{v^2}dv$$

Maintenant en faisant tendre $a, \lambda \to \infty$ de telle façon que $a/\lambda \to 0$, on obtient

$$\pi \leq \pi \varliminf_{y\to\infty} B(y),$$

d'où (tnp.9.2). (tnp.9.1) et (tnp.9.2) impliquent que $\lim_{y\to\infty} B(y) = 1$, ce qui achève la preuve du Théorème de Wiener - Ikehara. $\square$

tnp.10. *Preuve du Théorème de nombres premiers.* Considérons la fonction $A(x) = \psi(e^x)$, $x \geq 0$; c'est une fonction croissante. Sa transformation de Laplace

$$\int_0^{\infty} \psi(e^x)e^{-xs}dx = -\frac{\zeta'(s)}{s\zeta(s)}$$

(cf. tnp.5) converge si $\Re s > 1$ et se prolonge en une fonction analytique au voisinage de la droite $\Re s = 1$ sauf un pôle en $s = 1$ avec le résidu 1, en vertu du Théorème de Hadamard - de la Vallée-Poussin tnp.6. Donc les hypothèses du théorème de Wiener - Ikehara sont remplies, d'où $\psi(e^x) \sim e^x$, donc $\psi(x) \sim x$. D'après Tchebychev, tnp.3, cela entraine que $\pi(x) \sim x/\log(x)$. $\square$

§??? Formule explicite

fe.1. Pour $x \in \mathbb{R}$, $x > 0$, posons

$\pi(x) =$ le nombre de nombres premiers $p < x$ si x n'est pas un nombre premier et

$\pi(x) =$ (le nombre de nombres premiers $p < x$) $+ 1/2$ si x est un nombre premier.

Autrement dit,

$$\pi(x) = \frac{1}{2}\left(\sum_{p<x} 1 + \sum_{p\leq x} 1\right)$$

Donc partout $\pi(x) = (\pi(x-0) + \pi(x+0))/2$.

Ensuite on définit

$$J(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \ldots$$

Autrement dit,

$$J(x) = \frac{1}{2}\left(\sum_{p^n<x} \frac{1}{n} + \sum_{p^n\leq x} \frac{1}{n}\right)$$

Rappelons que la *fonction de Moebius* est définie par $\mu(n) = (-1)^k$ si n est le produit de k facteurs premiers distincts, $\mu(n) = 0$ si n contient un facteur carré.

fe.2. *Exercice.* Montrez que

$$\pi(x) = \sum_{n\geq 1} \frac{\mu(n)}{n} J(x^{1/n})$$

("formule d'inversion de Moebius").

fe.3. *Lemme.* Si $\Re(s) > 1$,

$$\frac{\log\zeta(s)}{s} = \int_0^\infty J(x)x^{-s-1}dx \tag{$fe.1$}$$

Preuve: exercice. Utilisez l'identité

$$p^{-ns} = s\int_{p^n}^\infty x^{-s-1}dx$$

Comparez avec les fonctions du chapitre precedente:

$$\psi(x) = \sum_{p,m>0,p^m\leq x} \log p$$

$$-\frac{\zeta'(s)}{s\zeta(s)} = \int_1^\infty \psi(x)x^{-s-1}dx$$

Notez la différence dans les limites d'intégration: dans la dernière formule on intègre sur "la moitié" $[1,\infty)$ de l'intérvale $[0,\infty)$.

fe.4. On veut maintenant inverser la formule (fe.1). Pour cela, on utilise l'inversion de Fourier:

(F) On a

$$g(y) = \int_{-\infty}^\infty f(x)e^{ixy}dx := Ff(y)$$

si et seulement si

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^\infty g(y)e^{-ixy}dy := F^{-1}g(x)$$

(sous les hypothèses convenables...).

Corollaire. Si $a > 1$,

$$J(x) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} \log\zeta(s)x^s\frac{ds}{s}$$

Preuve. Faisons dans (fe.1) un chagement de variables $x = e^y$:

$$\frac{\log\zeta(s)}{s} = \int_0^\infty J(x)x^{-s-1}dx = \int_{-\infty}^\infty J(e^y)e^{-sy}dy$$

Posons $s = a+bi,\ a > 1$:

$$\frac{\log\zeta(a+bi)}{a+bi} = \int_{-\infty}^\infty J(e^y)e^{-ay}e^{-iby}dy$$

Le deuxième terme est $F^{-1}\phi(b)$ où

$$\phi(y) = 2\pi J(e^y)e^{-ay}$$

Donc

$$2\pi J(e^y)e^{-ay} = \int_{-\infty}^\infty \frac{\log\zeta(a+bi)}{a+bi}e^{iby}db$$

$$J(e^y) = \frac{1}{2\pi}\int_{-\infty}^\infty \frac{\log\zeta(a+bi)}{a+bi}e^{(a+ib)y}db,$$

ou bien en revenant à $x = e^y$

$$J(x) = \frac{1}{2\pi}\int_{-\infty}^\infty \frac{\log\zeta(a+bi)}{a+bi}x^{a+ib}db = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{\log\zeta(s)}{s}x^s db,$$

$a > 1$.

fe.5. Les formules precedentes est un cas particulier de *transformation de Mellin* et son inverse:

(M) On a

$$\phi(s)=\int_0^{\infty} f(x)x^{s-1}dx := Mf(x)$$

si et seulement si

$$f(x)=\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} \phi(s)x^{-s}ds := M^{-1}\phi(x)$$

Exercice. Obtenir (M) à partir des formules de la transformation de Fourier.

fe.6. Rappelons la fonction

$$\tilde{\xi}(s)=\frac{s(s-1)}{2}\xi(s)=(s-1)\Gamma(s/2+1)\pi^{-s/2}\zeta(s)$$

cf. 5.15. Cette fonction est entière, satisfait à l'équation fonctionelle $\tilde{\xi}(s)=\tilde{\xi}(1-s)$ et n'a de zéros qu'à l'interieur de la bande critique $|\Re s-1/2|<1/2$.

Euler et Riemann utilise la notation $\Pi(s):=\Gamma(s+1)$, donc $\Pi(n)=n!$; alors la définition precedente se récrit

$$\tilde{\xi}(s)=(s-1)\Pi(s/2)\pi^{-s/2}\zeta(s)$$

Il s'en suit:

$$\log\zeta(s)=\log\xi(s)-\log\Pi(s/2)+(s\log\pi)/2-\log(s-1)$$

fe.7. *Théorème* (la formule de produit d'Hadamard).

$$\tilde{\xi}(s)=\tilde{\xi}(0)\prod_{\rho}\left(1-\frac{s}{\rho}\right)$$

le produit est pris sur toute les racines de $\tilde{\xi}(s)$, dans le produit on met ensemble les couples ρ avec $1-\rho$ ("produit d'Eisenstein").

Il s'en suit:

$$\log\zeta(s)=\log\xi(0)+\sum_{\rho}\log(1-s/\rho)-\log\Pi(s/2)+(s\log\pi)/2-\log(s-1)\quad (fe.3)$$

8. L'intégration par parties fournit

$$J(x)=-\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log\zeta(s)/s\big)x^s ds,\ a>1$$

Ici il faut plonger l'expression (fe.3) pour $\log\zeta(s)$ et on obtient une expression de $J(x)$ en fonction de 4 intégrales:

$$J(x)=\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(s-1)/s\big)x^s ds-$$

$$-\sum_\rho \frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(1-s/\rho)/s\big)x^s ds-$$
$$-\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(\tilde\xi(0))/s\big)x^s ds+$$
$$\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(\Pi(s/2))/s\big)x^s ds \qquad (fe.4)$$

Pour enoncer les valeurs de ces intégrales, on introduit une fonction importante du *logarithme intégrale*:

$$\mathrm{Li}(x)=\text{v.p.}\int_0^x\frac{dt}{\log t}:=\lim_{\epsilon\to 0}\Big(\int_0^{1-\epsilon}\frac{dt}{\log t}+\int_{1+\epsilon}^x\frac{dt}{\log t}\Big)$$

(ici "v.p." veut dire " la valeur principale au sens de Cauchy").

Exercice. Montrer que la limite dans la formule precedente existe.

fe.9. *Théorème.* Soit $a\in\mathbb{R}$, $a>1$. Alors:

(a)

$$I_a:=\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(\tilde\xi(0))/s\big)x^s ds=\log 2$$

(b)

$$I_b:=\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(\Pi(s/2))/s\big)x^s ds=\int_x^\infty\frac{dt}{t(t^2-1)\log t}$$

(c) Si $\Im\rho>0$,

$$I_c:=\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big((\log(1-s/\rho)+(\log(1-s/(1-\rho))/s\big)x^s ds=$$
$$=\mathrm{Li}(x^\rho)+\mathrm{Li}(x^{1-\rho})$$

(d)

$$I_d:=\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(\log(s-1)/s\big)x^s ds=\mathrm{Li}(x)$$

Pour faire le calcul, on va utiliser une transformation de Mellin inverse suivante (mais faitez attention, Riemann avait fait cela 40 ans avant Mellin).

fe.10. *Lemme.* Si $a>\Re\,\beta$,

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a-i\infty}\frac{y^s}{s-\beta}ds=y^\beta$$

si $y>1$, 0 si $y<1$.

Preuve. On a
$$\frac{1}{s-\beta} = \int_1^\infty x^{-s}x^{\beta-1}dx$$
$(\Re(s-\beta)>0)$, $x=e^\lambda$:
$$\frac{1}{a+ib-\beta} = \int_0^\infty e^{-ib\lambda}e^{\lambda(\beta-a)}d\lambda$$
$(a>\Re\beta)$, d'où, par l'inversion de Fourier
$$\int_{-\infty}^\infty \frac{e^{ibx}}{a+ib-\beta}db = 2\pi e^{x(\beta-a)}$$
si $x>0$, 0 si $x>0$, ce qui implique le lemme. □

fe.11. *Calcul de* (a). On a $\tilde{\xi}(0) = -\zeta(0) = 1/2$. D'un autre côté
$$\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\big(1/s\big)x^s ds = -\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{x^s}{s}ds = -1$$
d'après le lemme avec $\beta=0$, d'où (a).

fe.12. Toutes autres intégrales utilisent la fonction du logarithme intégrale $\mathrm{Li}(x)$. Étudions-la plus attentivement. Définissons deux fonctions
$$G_\pm(\beta,x) = \int_{C_\pm(x)}\frac{t^{\beta-1}}{\log t}dt$$
où $x\in\mathbb{R}$, $x>1$, $\Re\beta>0$,
$$C_-(x) = \{0\le z\le 1-\epsilon\}\cup\{z=1+\epsilon e^{i\theta},\ -\pi\le\theta\le 0\}\cup\{1+\epsilon\le z\le x\},$$
$$C_+(x) = \{0\le z\le 1-\epsilon\}\cup\{z=1+\epsilon e^{i\theta},\ \pi\ge\theta\ge 0\}\cup\{1+\epsilon\le z\le x\},$$

fe.12.1. *Lemme.* $\partial G_\pm(\beta,x)/\partial\beta = x^\beta/\beta.$

Preuve: exercice.

fe.12.2. *Lemme.* Si $\beta\in\mathbb{R}_{>0}$,
$$G_\pm(\beta,x) = \mathrm{Li}(x^\beta)\mp i\pi$$

fe.13. Ensuite, on introduit deux autres fonctions. Ici $x>1$:
$$F_+(\beta,x) = \frac{1}{2\pi i}\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\left\{\frac{\log(s/\beta-1)}{s}\right\}x^s ds,$$
$\beta\in\mathbb{C}\setminus\mathbb{R}_{\le 0}$, $a>\Re\beta$, $\log(s/\beta-1) = \log(s-\beta)-\log\beta$ et on prend la branche principale du logarithme;
$$F_-(\beta,x) = \frac{1}{2\pi i}\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\left\{\frac{\log(-s/\beta+1)}{s}\right\}x^s ds,$$

$\beta \in \mathbb{C} \setminus \mathbb{R}_{\geq 0}$, $a > \Re\beta$, $\log(s/\beta - 1) = \log(s-\beta) - \log(-\beta)$ et on prend la branche principale du logarithme.

Exercice. Montrez que les intégrales converge absolument.

fe.13.1. *Lemme.* $\partial F_{\pm}(\beta, x)/\partial\beta = x^\beta/\beta$.

Preuve. Considérons par exemple la fonction $F_+(\beta, x)$. On a

$$\frac{d}{d\beta}\left\{\frac{\log(s/\beta - 1)}{s}\right\} = \frac{1}{\beta(s-\beta)},$$

d'où

$$\frac{\partial F_+(\beta, x)}{\partial\beta} = \frac{1}{2\pi i}\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\left\{\frac{1}{\beta(s-\beta)}\right\}x^s ds =$$

par parties

$$= -\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{x^s}{\beta(s-\beta)}ds = \frac{x^\beta}{\beta}$$

d'aprèz fe.10, puisque $x > 1$. $\square$

fe.13.2. *Lemme.* (a) Si $\Im\beta > 0$,

$$F_+(x, \beta) - F_-(x, \beta) = i\pi$$

Si $\Re\beta > 0$, $F_+(x, \beta) = G_+(x, \beta) + i\pi$.

Donc si $\Im\beta > 0$, $\Re\beta > 0$ alors $F_-(x, \beta) = G_+(x, \beta)$.

(b) Si $\Im\beta < 0$, $\Re\beta > 0$ alors $F_-(x, \beta) = G_-(x, \beta)$.

Preuve de (a). $\Im\beta > 0$,

$$F_-(x, \beta) - F_+(x, \beta) = \frac{1}{2\pi i}\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\left\{\frac{\log\beta - \log(-\beta)}{s}\right\}x^s ds =$$

$$\frac{1}{2\pi i}\frac{1}{\log x}\int_{a-i\infty}^{a+i\infty}\frac{d}{ds}\left\{\frac{i\pi}{s}\right\}x^s ds = -\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{i\pi}{s}x^s ds = -i\pi,$$

d'aprèz fe.10 avec $\beta = 0$.

Corollaire. Si $\beta > 1$, $F_+(x, \beta) = \mathrm{Li}(x^\beta)$.

Pour $\beta = 1$, ceci donne la valeur de l'intégrale I_d du théorème fe.9.

L'assertion (c) du thérème s'en suit immédiatement aussi.

fe.14. Il reste à traiter l'intégrale (b). Rappelons la formule d'Euler - Gauss pour la fonction Γ:

$$\Pi(s) = \Gamma(s+1) = \lim_{N\to\infty}(N+1)^s\frac{N!}{(s+1)\cdot\ldots\cdot(s+N)}$$

qu'on peut reécrire sous une forme

$$\Pi(s) = \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right)^{-1} \left(1 + \frac{1}{n}\right)^{s},$$

$\Re(s) > -1$. En prenant le logarithme,

$$\log \Pi(s/2) = \sum_{n=1}^{\infty} \left\{ -\log(1 - s/2n) + \frac{s}{2}\log(1 + 1/n) \right\}$$

d'où, si l'on accepte qu'on peut interchanger l'intégration et la sommation,

$$I_b = -\sum_{n=1}^{\infty} \frac{1}{2\pi i} \frac{1}{\log x} \int_{a-i\infty}^{a+i\infty} \frac{d}{ds} \left\{ \frac{\log(1 + s/2n)}{s} \right\} x^s ds = -\sum_{n=1}^{\infty} F_{-}(-2n)$$

Pour calculer $F_{-}(-2n)$ ou, plus généralement, $F_{-}(\beta)$ pour $\Re\beta < 0$, considérons la fonction

$$E(x, \beta) = -\int_{x}^{\infty} \frac{t^{\beta-1}}{\log t} dt,$$

l'intégrale converge si $\Re\beta < 0$. Alors

$$\frac{\partial E(x, \beta)}{\partial \beta} = -\int_{x}^{\infty} t^{\beta-1} dt = x^{\beta}/\beta = \frac{\partial F_{\pm}(x, \beta)}{\partial \beta}$$

On peut montrer que $\lim_{\beta \to -\infty} E(x, \beta) = \lim_{\beta \to -\infty} F_{-}(x, \beta) = 0$, d'où $F_{-}(x, \beta) = E(x, \beta)$ si $\Re\beta < 0$.

Il s'en suit,

$$I_b = \sum_{n=1}^{\infty} \int_{x}^{\infty} \frac{t^{-2n-1}}{\log t} dt = \int_{x}^{\infty} \frac{\sum_{n=1}^{\infty} t^{-2n}}{t \log t} dt = \int_{x}^{\infty} \frac{dt}{t(t^2 - 1) \log t}$$

ce qui est la valeur cherchée.

En rassemblant les intégrales, on arrive au théorème ci-dessous, qui presente le résultat principal de l'article de Riemann.

fe.15. *Théorème* (la formule explicite de Riemann).

$$J(x) = \mathrm{Li}(x) - \sum_{\Im\rho > 0} \{\mathrm{Li}(x^{\rho}) + \mathrm{Li}(x^{1-\rho})\} + \int_{x}^{\infty} \frac{dt}{t(t^2 - 1) \log t} - \log 2$$

La sommation est prie sur les zéros ρ nontriviaux de $\zeta(s)$, dans l'ordre de croissance de $\Im\rho$.

Inversion de Möbius

(d) *Fonctions μ et ϕ*

1.14. Notation: $\mathbb{Z}_+ = \{n \in \mathbb{Z} \mid n > 0\}$. Un nombre $n \in \mathbb{Z},\ n > 1$, est dit *libre de carrés (square free)* si il est un produit de nombres premiers distincts.

On définit la *fonction de Moebius* $\mu : \ \mathbb{Z}_+ \longrightarrow \{-1, 0, 1\}$ par: $\mu(1) = 1$, pour $n > 1$ $\mu(n) = 0$ si n n'est pas libre de carrés et $\mu(n) = (-1)^r$ si $n = p_1 \cdot \ldots \cdot p_r$ avec p_i premiers et distincts.

1.15. *Exercice.* Montrer que

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

1.16. *Lemme.* Pour $n > 1$, on a $\sum_{d|n} \ \mu(d) = 0$.

En effet, si $n = \prod_{i=1}^{r} \ p_i^{a_i}$ alors

$$\sum_{d|n} \mu(d) = \sum_{(\epsilon_1,\ldots,\epsilon_r)\in\{0,1\}^r} \mu(p_1^{\epsilon_1} \cdot \ldots \cdot p_r^{\epsilon_r}) =$$

$$= \sum_{i=0}^{r} (-1)^i \binom{i}{r} = (1-1)^r = 0$$

1.17. Considérons l'ensemble $\mathbb{Z}_+^{\mathbb{C}} = \{f : \ \mathbb{Z}_+ \longrightarrow \mathbb{C}\}$. Introduisons sur cet ensemble une opération $\circ$ (*multiplication de Dirichlet*) par

$$f \circ g(n) = \sum_{d|n} f(d)g(n/d)$$

Elle est associative et commutative, avec l'unité $\underline{1}$, où $\underline{1}(1) = 1$, $\underline{1}(n) = 0$ pour $n > 1$ (vérifier!).

On définit $\nu : \ \mathbb{Z}_+ \longrightarrow \mathbb{C}$ par $\nu(n) = 1$ pour tous n. Évidemment,

$$f \circ \nu(n) = \sum_{d|n} f(d)$$

1.18. *Lemme.* $\mu \circ \nu = \underline{1}$

En effet, $\mu \circ \nu(1) = \mu(1)\nu(1) = 1$. D'autre part, pour $n > 1$

$$\mu \circ \nu(n) = \sum_{d|n} \mu(d) = 0,$$

d'après 1.16.

1.19. *Théorème* (formule d'inversion de Moebius) Pour $f \in \mathbb{Z}_+^{\mathbb{C}}$, soit $F(n) = \sum_{d|n} \ f(d)$. Alors

$$f(n) = \sum_{d|n} \mu(d)F(n/d)$$

Il s'agit de l'inversion d'une matrice triangulaire:

$$F(1) = f(1),$$

$$F(2) = f(1) + f(2),$$

$$F(3) = f(1) + f(3),$$

$$F(4) = f(1) + f(2) + f(4),$$

etc., d'où

$$f(1) = F(1),$$

$$f(2) = F(2) - F(1)$$

$$f(3) = F(3) - F(1),$$

$$f(4) = F(4) - F(2),$$

etc.

Démonstration du théorème: on a $F = f \circ \nu$, d'òu, par 1.18, $f = F \circ \mu$.

1.20. *Variante.* Soit $f : \mathbb{Z}_+ \longrightarrow G$ une application à valeurs dans un groupe abélien G, écrit multiplicativement. Si $F(n) = \prod_{d|n} f(d)$ alors

$$f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$$

Preuve: exercice.

1.21. *Rémarque.* Dans tout le précédent, on peut aussi remplacer $\mathbb{Z}_+$ par l'ensemble de tous diviseurs d'un nombre fixé $N \in \mathbb{Z}_+$.

Fonction d'Euler.

1.22. Pour $n \in \mathbb{Z}_+$, on définit $\Phi(n) = \{a \in \mathbb{Z},\ 1 \leq a \leq n \mid (a, n) = 1\}$; $\phi(n) := \mathrm{Card}(\Phi(n))$.

Par exemple, $\phi(1) = 1$, $\phi(p) = p - 1$ si p est premier.

On peut identifier $\Phi(n)$ avec l'ensemble de générateurs de $\mathbb{Z}/n\mathbb{Z}$.

1.23. *Lemme.* $n = \sum_{d|n} \phi(n)$.

En effet, pour chaque $d|n$ soit Φ_d l'ensemble d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ = l'ensemble de générateurs de $\mathbb{Z}/d\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$. Alors $\mathbb{Z}/n\mathbb{Z} = \coprod_{d|n} \Phi_d$.

1.24. *Corollaire.* $\phi(n) = \sum_{d|n} d\mu(n/d)$

1.25. *Exercice.* Montrer, en employant 1.25, que si $n = \prod_{i=1}^{r} p_i^{a_i}$ est la décomposition en facteurs premiers (tous p_i étant distincts), alors

$$\phi(n)/n = \prod_{i=1}^{r} (1 - p_i^{-1})$$

Solution. On a

$$\phi(n) = \sum_{d|n} d\mu(n/d) =$$

$$= n - \sum_{i} n/p_i + \sum_{i<j} n/p_i p_j - \ldots = n \prod_{i=1}^{r} (1 - p_i^{-1})$$

1.26. *Exercice.* Combien y a-t-il de racines primitives modulo 37?

1.27. *Lemme.* $x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x - i)\ (p)$.

En effet, par le petit Fermat on connait $p-1$ racines: $1, \ldots, p-1$ du polynôme dans $\mathbb{F}_p[x]$.

1.28. *Corollaire* (théorème de Wilson) $(p-1)! \equiv -1\ (p)$.

Poser $x = 0$ dans 1.27.

1.29. *Corollaire.* Si $d \mid (p-1)$ alors le polynome $x^d - 1$ a d racines dans $\mathbb{F}_p$.

En effet, si $d \mid (p-1)$ alors $(x^d - 1)|(x^{p-1} - 1)$ dans $\mathbb{F}_p$ (prouver!), i.e. $x^{p-1} - 1 = (x^d - 1)g(x)$. Nous savons que $x^{p-1} - 1$ a $p-1$ racines; mais si $x^d - 1$ avait moins que d racines alors $x^{p-1} - 1$ aurait moins que $p - 1$ racines car $g(x)$ a au plus $\deg(g(x)) = p - 1 - d$ racines.

1.30. *Théorème.* Le groupe $\mathbb{F}_p^*$ est cyclique.

Soit $\psi(d)$ le nombre d'éléments d'ordre d dans $\mathbb{F}_p^*$. D'après 1.29, on a $d = \sum_{c|d} \psi(c)$. D'après la formule d'inversion de Moebius,

$$\psi(d) = \sum_{c|d} c\mu(d/c) = \phi(d)$$

(par 1.23). En particulier, $\psi(p-1) = \phi(p-1) > 0$ si $p > 2$. Pour $p = 2$ l'assertion est triviale.

(d) *Identité cyclotomique de Gauss*

Cf. [G], (e), no. 343 - 347, pp. 220 - 222.

1.39. *Polynômes des colliers.* On définit, avec Gauss

$$M_n(x) = \frac{1}{n} \sum_{d|n} \mu(d) x^{n/d}$$

Un collier c est un anneau de n perles; supposons que chaque perle peut avoir m couleurs. Un collier de la forme $c = dc'$ pour $d|n$ est appelé décomposable. Un collier qui n'est pas décomposable est appelé *primitif.*

1.40. *Exercice.* Prouver le *théorème de Moreau* (1872, cf. [M]; C.Moreau était un capitaine d'artillerie français): le nombre de colliers primitifs à n perles et à m couleurs est égal à $M_n(m)$.

Faire d'abord le cas $n = p$ un nombre premier.

1.41. *Exercice.* Montrer que chaque série $f(t) \in \mathbb{Z}[[t]]$ avec $f(0) = 1$ se décompose uniquement en produit

$$f(t) = \prod_{n=1}^{\infty} (1 - t^n)^{a_n}, \ a_n \in \mathbb{Z}$$

Trouver les premiers a_n pour $f(t) = 1 + 2t$.

Réponse:

$$1 + 2t = (1-t)^{-2}(1-t^2)^3(1-t^3)^{-2}(1-t^4)^3(1-t^5)^{-6}\dots$$

1.42. *Théorème.* Pour tous $b \in \mathbb{C}$

$$1 - bt = \prod_{n=1}^{\infty} (1 - t^n)^{M_n(b)},$$

Preuve. On pose

$$1 - bt = \prod_{n=1}^{\infty} (1 - t^n)^{a_n}$$

et l'on prend $td \log /dt$ de deux côtés:

$$-\sum_{i=1}^{\infty} b^i t^i = -\sum_{n=1}^{\infty} a_n \sum_{j=1}^{\infty} n t^{nj} = -\sum_{i=1}^{\infty} \left(\sum_{n|i} n a_n \right) \cdot t^i,$$

d'où

$$b^i = \sum_{n|i} n a_n,$$

et l'on finit par application de l'inversion de Moebius.

1.43. *Exercice.* Soit $f(q) \in \mathbb{C}[q, q^{-1}]$. On définit:

$$M_n(f;q) := \frac{1}{n} \sum_{d|n} \mu(d) f(q^d)^{n/d}$$

Par exemple, si $f(q)$ est une constante c, alors $M_n(c;q) = M_n(c)$.

(i) Montrez que

$$1 - f(q)t = \prod_{n=1}^{\infty} \prod_{i=-\infty}^{\infty} (1 - q^i t^n)^{a_{in}}$$

où les exposants a_{in} sont définis par:

$$\sum_i a_{in} \cdot q^i = M_n(f;q)$$

(la somme est finie).

Solution. Prenons $-\log$ de deux côtés:

$$-\log(1 - f(q)t) = \sum_{m=1}^{\infty} \frac{f(q)^m t^m}{m}$$

et

$$-\log(\prod_{i,n} (1 - q^i t^n)^{a_{in}}) = \sum_i \sum_{n,k=1}^{\infty} a_{in} \frac{q^{ik} t^{nk}}{k} =$$

$$= \sum_{m=1}^{\infty} t^m \cdot \left(\sum_{n|m} \sum_i a_{in} \frac{q^{im/n}}{m/n} \right),$$

d'où

$$f(q)^m = \sum_{n|m} \sum_i n a_{in} q^{im/n}$$

pour chaque $m = 1, 2, \ldots$. On fait un changement de variable: $p = q^m$,

$$f(p^{1/m})^m = \sum_{n|m} \sum_i n a_{in} p^{i/n}$$

Maintenant on peut utiliser l'inversion de Moebius:

$$\sum_i n a_{in} p^{i/n} = \sum_{d|n} \mu(n/d) f(p^{1/d})^d,$$

et en faisant le retour: $q = p^{1/n}$, on obtient

$$\sum_i n a_{in} q^i = \sum_{d|n} \mu(n/d) f(q^{n/d})^d,$$

ce qui est la formule cherchée.

(ii) Faitez les cas: $f(q) = q^i$; $f(q) = -q$.

(e) *Fonction zeta de l'anneau* $\mathbb{F}_p[x]$

1.43. On pose $A := \mathbb{F}_p[x]$; cet anneau est tout à fait pareil à $\mathbb{Z}$.

Les idéaux non-nuls $I \subset A$ sont en bijection avec les polynômes unitares $f(x)$, $I = (f)$, et les idéaux premiers correspondent aux polynômes irréductibles. On pose

$$N(I) := \sharp(A/I) = p^{\deg f},$$

et l'on définit

$$\zeta(A; s) = \sum_{0 \neq I \subset A} N(I)^{-s} = \sum_{f \text{ unitaire}} p^{-s \deg f}$$

Il y a p^n polynômes unitaires de degré n, d'où

$$\zeta(A; s) = \sum_{n=1}^{\infty} p^n \cdot p^{-sn} = \frac{1}{1 - p \cdot p^{-s}} = \frac{1}{1 - pT}, \qquad (1.43.1)$$

où l'on pose $T := p^{-s}$.

Le produit d'Euler pour $\zeta(A; s)$ s'ecrit sous une forme

$$\zeta(A; s) = \prod_{f \text{ unitaire, irréductible}} \frac{1}{1 - p^{-\deg f \cdot s}} =$$

$$= \prod_{d=1}^{\infty} \prod_{f \text{ un., irr.,}\deg f = d} \frac{1}{1 - p^{-ds}} = \prod_{d=1}^{\infty} \frac{1}{(1 - T^d)^{N_d(p)}},$$

où $N_d(p)$ désigne le nombre de polynômes unitaires irréductibles de degré d dans A.

De l'autre côté, en appliquant l'identité cyclotomique à (1.33.1),

$$\zeta(A; s) = \frac{1}{1 - pT} = \frac{1}{\prod_{d=1}^{\infty} (1 - T^d)^{M_d(p)}},$$

et l'on a démontré

1.44. *Théorème* (Gauss). Le nombre de polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$ est égale à

$$N_d(p) = M_d(p) = \frac{1}{d} \sum_{l | d} \mu(l) p^{d/l}$$

1.45. *Corollaire.* Pour $d \geq 1$, $N_d(p) > 0$, i.e. pour chaque $d \geq 1$ il existe un polynôme irréductible de degré d.

En effet, l'ordre de croissance de $N_d(p)$ est exponentiel: $N_d(p) d^{-1} \sim p^d$ quand $d \to \infty$.

On a donc démontré en particulier encore une fois l'existence pour chaque $n \geq 1$ d'un corps fini à p^n éléments.

§2. Réciprocité quadratique

2.1. *Définition* (Gauss) Soient $m \in \mathbb{Z}_{>1}$, $a \in \mathbb{Z}$, $(a,m) = 1$. a est appelé *résidu quadratique* modulo m si il existe une solution de la congruence $x^2 \equiv a\ (m)$. Sinon, a est appelé *non-résidu quadratique.*

En d'autres termes, a est résidu quadratique modulo m ssi sa classe $\bar{a} := a\mathrm{mod}(m) \in \mathbb{Z}/m\mathbb{Z}$ appartient à $(\mathbb{Z}/m\mathbb{Z})^{*2}$.

Considérons le cas $m = p$ en nombre premier. Le cas $p = 2$ étant trivial, nous supposerons que $p > 2$. Le groupe $\mathbb{F}_p^*$ est cyclique. Soit $u \in \mathbb{F}_p^*$ un générateur (une racine primitive). Alors $a \in \mathbb{F}_p^{*2}$ ssi $a = u^n$ avec n pair.

Il s'en suit que $a^{(p-1)/2} \in \{-1, 1\}$ et $a \in \mathbb{F}_p^{*2}$ ssi $a^{(p-1)/2} = 1$.

2.2. *Symbole de Legendre.* Soient p un nombre premier impair, a un nombre entier qui n'est pas divisible par p (ou un élément de $\mathbb{F}_p^*$). On définit $(a/p) := a^{(p-1)/2}\mathrm{mod}(p) = \pm 1$.

Donc on a $(-1/p) = (-1)^{(p-1)/2}$. En d'autres termes, $(-1/p) = 1$ si $p \equiv 1\ (4)$ et $(-1/p) = -1$ si $p \equiv 3\ (4)$.

Pour un entier n impair, définissons

$$\epsilon(n) = \frac{n-1}{2}\ (\mathrm{mod}\ 2) \in \mathbb{Z}/2\mathbb{Z}$$

Considérons le groupe multiplicatif $(\mathbb{Z}/4\mathbb{Z})^*$; il est cyclique, avec un générateur 3. On peut considérer ϵ comme un homomorphisme $\epsilon :\ (\mathbb{Z}/4\mathbb{Z})^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$.

On a $(-1/p) = (-1)^{\epsilon(p)}$.

2.3. Considérons le groupe $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$. On a

$$(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{1, 7\} \times \{1, 3\}$$

Pour un nombre entier impair n, posons

$$\omega(n) = \frac{n^2-1}{8}\ (\mathrm{mod}\ 2) \in \mathbb{Z}/2\mathbb{Z}$$

Donc $\omega(n) = 0$ si $n \equiv \pm 1\ (\mathrm{mod}\ 8)$ et $\omega(n) = 1$ si $n \equiv \pm 3\ (\mathrm{mod}\ 8)$.

On peut considérer ω comme un homomorphisme $(\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$.

2.4. *Théorème.* $(2/p) = (-1)^{\omega(p)}$

Démonstration. Soit α une racine primitive 8-ième de l'unité dans une clôture algébrique $\Omega \supset \mathbb{F}_p$, c'est-à-dire, un élément $\alpha \in \Omega$ satisfaisant l'équation $\alpha^4 = -1$. Posons $y = \alpha + \alpha^{-1}$. Alors

$$y^2 = \alpha^2 + 2 + \alpha^{-2} = 2$$

Donc

$$\Big(\frac{2}{p}\Big) = 2^{(p-1)/2} = y^{p-1}$$

D'un autre côté,

$$y^p = \alpha^p + \alpha^{-p}$$

Il s'en suit que si $p \equiv \pm 1 \pmod 8$, alors $y^p = y$, donc $y^{p-1} = 1$.

Par contre, si $p \equiv \pm 3 \pmod 8$, alors (comme $\alpha^4 = -1$)

$$y^p = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -y,$$

donc $y^{p-1} = -1$, cqfd.

2.6. *Exercice.* Montrer qu'il existe un nombre infini de nombres premiers p de la forme $8n + 7$.

Solution. Soient $p_1, \ldots, p_m$ des nombres premiers de la forme $8n + 7$. Considérons le nombre $a = (4 \prod_{i=1}^{m} p_i)^2 - 2$. Si p est un nombre premier impair divisant a, alors 2 est résidu quadratique modulo p, donc $p \equiv \pm 1(8)$.

Par contre, $a/2 \equiv -1(8)$. Donc il existe un nombre premier p de la forme $8n + 7$ divisant a; évidemment, $p \notin \{p_1, \ldots, p_m\}$.

2.7. *Théorème* (Gauss) Soient p, q des nombres premiers impairs distincts. Alors

$$\Big(\frac{p}{q}\Big) = (-1)^{\epsilon(p)\epsilon(q)}\Big(\frac{q}{p}\Big)$$

Une démonstration d'Eisenstein

2.18. Soit p un nombre premier impair. Soit $S \subset \mathbb{F}_p^*$ un sous-ensemble tel que $\mathbb{F}_p^* = S \coprod (-S)$, par exemple, $S = \{1, \ldots, (p-1)/2\}$.

Pour $a \in \mathbb{F}_p^*,\ s \in S$, posons

$$as = e_s(a)s_a,\ \ e_s(a) = \pm 1,\ \ s_a \in S$$

On remarque que si $s \neq s'$ alors $s_a \neq s'_a$, car sinon, on aurait $s' = \pm s$, ce qui est impossible par hypothèse sur S. Donc $s \mapsto s_a$ est une bijection de S sur lui-même.

2.19. *Lemme* (Gauss) $(a/p) = \prod_{s\in S}\ e_s(a)$

En effet,

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

d'où

$$a^{(p-1)/2} = \prod_{s\in S} e_s(a),$$

ce qui entraîne le lemme.

2.20. *Exercice.* En déduire théorème 2.4.

Solution. Prenons $a = 2$, $S = \{1, \ldots, (p-1)/2\}$. On a $e_s(2) = 1$ si $2s \leq (p-1)/2$ et $e_s(2) = -1$ si $2s > (p-1)/2$. Donc $(2/p) = (-1)^{n(p)}$ où $n(p)$ est le nombre d'entiers s tels que $(p-1)/4 < s \leq (p-1)/2$. Il reste à montrer que $n(p) \equiv \omega(p)$ (mod2).

En effet, si $p = 4k+1$, la condition est $k < s \leq 2k$, d'où $n(p) = k$. De même, si $p = 4k-1$, $n(p) = k$ (vérifier!) Donc si $k = 2n$, c'est-à-dire, $p = 8n \pm 1$, alors $(2/p) = 1$.

Par contre, si $k = 2n+1$, i.e. $p = 8n+4\pm 1 = 8m \pm 3$, on a $(2/p) = -1$, cqfd.

Polynômes de Tchebycheff

2.21. *Lemme.* Soit m un nombre entier impair, $m \geq 1$. On a $\sin(mx) = f_m(\sin(x))$, où $f_m(t) \in \mathbb{Z}[t]$ est un polynôme de degré m, divisible par t, avec le terme supérieur égale à $(-4)^{(m-1)/2}$.

Démonstration par récurrence sur m. Le cas $m = 1$ est évident. Supposons que l'assertion est prouvée pour m. Nous avons

$$\sin(mx) = f_m(\sin(x)),$$

d'où, en faisant la dérivée,

$$m\cos(mx) = f'_m(\sin(x))\cos(x)$$

Donc

$$\sin((m+2)x) = \sin(mx)\cos(2x) + \cos(mx)\sin(2x) =$$

$$= f_m(\sin(x))(1-2\sin^2 x)) + 2m^{-1}f'_m(\sin(x))(1-\sin^2 x)\sin(x) = f_{m+2}(\sin(x)),$$

où

$$f_{m+2}(t) = f_m(t)(1-2t^2) + 2m^{-1}f'_m(t)t(1-t^2) \qquad (2.21.1)$$

Il s'en suit que $f_{m+2}(t) \in t\mathbb{Z}[t]$ et si $f_m(t) = a_m t^m + \ldots$, alors $f_{m+2}(t) = -4a_m t^{m+2} + \ldots$, ce qui implique le lemme.

Variante. On a

$$\sin((m-2)x) = \sin(mx)\cos(2x) - \cos(mx)\sin(2x),$$

donc

$$\sin((m+2)x) + \sin((m-2)x) = 2\sin(mx)(1-2\sin^2(x)),$$

d'où l'équation de récurrence

$$f_{m+2}(t) = 2f_m(t)(1-2t^2) - f_{m-2}(t) \qquad (2.21.2)$$

(On a $f_1(t) = t,\ f_{-1}(t) = -t$.)

2.22. *Lemme.* Soit m en entier impair ≥ 1. Alors

$$\frac{\sin(mx)}{\sin(x)} = (-4)^{(m-1)/2} \prod_{a=1}^{(m-1)/2} (\sin^2 x - \sin^2(2\pi a/m))$$

En effet, d'après le lemme précédent,

$$(-4)^{-(m-1)/2}\frac{\sin(mx)}{\sin(x)} = g_m(\sin(x)),$$

où $g(t)$ est un polynôme unitaire de degré pair $m-1$. Or, il est très facile d'exhiber les $m-1$ racines distinctes de $g_m(t)$: ils sont $\pm\sin(2\pi a/m)$, $a = 1, \ldots, (m-1)/2$ (on remarque que les nombres $\{\pm 2a \mid a = 1, \ldots, (m-1)/2\}$ décrivent tous les résidus possibles mod m sauf 0), d'où la formule désirée.

2.23. *Exercice* (Gauss, Eisenstein) (a) Montrer que $f_m(t)$ satisfait à l'équation différentielle

$$\frac{df_m(t)}{dt} = \frac{m\sqrt{1 - f_m(t)^2}}{\sqrt{1-t^2}}$$

(b) Montrer que $f_m(t)$ satisfait à l'équation différentielle

$$(1-t^2)f''_m(t) - tf'_m(t) + m^2 f_m(t) = 0$$

(c) En déduire que

$$f_m(t) = mt - \frac{m(m^2-1)}{3!}t^3 + \frac{m(m^2-1)(m^2-3^2)}{5!}t^5 - \ldots + (-1)^{(m-1)/2}2^{m-1}t^m =$$

$$= \sum_{j=0}^{(m-1)/2} (-1)^j \cdot \frac{m(m^2-1^2)(m^2-3^2)\ldots(m^2-(2j-1)^2)}{(2j+1)!} \cdot t^{2j+1}$$

[En effet, soit

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$$

une solution de (b). Alors:

$$0 = (1-t^2)\sum_{i=2}^{\infty} i(i-1)a_i t^{i-2} - t\sum_{i=1}^{\infty} ia_i t^{i-1} + m^2 \sum_{i=0}^{\infty} a_i t^i =$$

$$= \sum_{i=0}^{\infty} (i+2)(i+1)a_{i+2}t^i - \sum_{i=2}^{\infty} i(i-1)a_i t^i +$$

$$- \sum_{i=1}^{\infty} ia_i t^i + m^2 \sum_{i=0}^{\infty} a_i t^i =$$

$$= 2a_2 + m^2 a_0 + (6a_3 - a_1 + m^2 a_1)\cdot t +$$

$$+\sum_{i=2}^{\infty}\left\{(i+2)(i+1)a_{i+2}-i(i-1)a_i-ia_i+m^2a_i\right\}\cdot t^i,$$

d'où:

$$2a_2+m^2a_0=0,\ \text{i.e. } a_2=-m^2a_0/2;$$
$$6a_3+(m^2-1)a_1=0,\ \text{i.e. } a_3=-(m^2-1)a_1/6$$

et

$$(i+2)(i+1)a_{i+2}+\big(m^2-i^2\big)\big)a_i=0,$$

i.e.

$$a_{i+2}=-\frac{m^2-i^2}{(i+2)(i+1)}\cdot a_i,\ \ i\geq 2$$

Maintenant on rémarque que chez $f(t)=f_m(t)$, $a_0=f_m(0)=0$ et $a_1=f_m'(0)=m$, d'où la formule (c) est immédiate.]

(d) On note que si $m\in\mathbb{C}-\{0,\pm1,\pm3,\ldots\}$ alors on obtient comme $f_m(t)$ une série infinie:

$$f_m(t)==\sum_{j=0}^{\infty}(-1)^j\cdot\frac{m(m^2-1^2)(m^2-3^2)\ldots(m^2-(2j-1)^2)}{(2j+1)!}\cdot t^{2j+1}$$

Montrer que cette série converge absolument si $|t|<1$, uniformément sur chaque disque fermé $|t|\leq r<1$.

[Ceci est une conséquence immédiate du

Critère de d'Alembert. Si $\sum_{n=0}^{\infty}\ b_n$ est une série telle qu'il existent $r<1$ et n_0 tels que

$$\frac{|b_n|}{|b_{n+1}|}\leq r$$

pour $n\geq n_0$, alors cette série converge absolument.]

2.24. *Exercice.* Soit toujours m un entier impair, $m\geq 1$.

(a) Soit $\zeta=e^{2\pi i/m}$. Montrer que

$$u^m-v^m=\prod_{b=0}^{m-1}\ (\zeta^b u-\zeta^{-b}v)$$

(b) Soit $f(t)=e^{2\pi it}-e^{-2\pi it}$. Montrer que

$$f(mt)=f(t)\prod_{a=1}^{(m-1)/2}f(t-a/m)f(t+a/m)$$

(c) En déduire le lemme 2.22.

2.25. *Lemme.* Sous les hypothèses 2.18,

$$\left(\frac{a}{p}\right) = \prod_{s\in S} \frac{\sin(2\pi as/p)}{\sin(2\pi s/p)}$$

En effet, pour chaque $s \in S$, $as = e_s(a)s_a$, d'où

$$\sin(2\pi as/p) = e_s(a)\sin(2\pi s_a/p)$$

En faisant le produit sur $s \in S$, on a, par le lemme de Gauss,

$$\left(\frac{a}{p}\right) = \prod_{s\in S} e_s(a) = \prod_{s\in S} \frac{\sin(2\pi as/p)}{\sin(2\pi s/p)},$$

en tenant compte de ce que $s \mapsto s_a$ est une bijection, cqfd.

2.26. *Une démonstration de 2.7.* Soient ℓ, p deux nombres premiers distincts impairs. Prenons $S = \{1, \ldots, (p-1)/2\}$, $T = \{1, \ldots, (\ell-1)/2\}$. On a

$$\left(\frac{\ell}{p}\right) = \prod_{s\in S} \frac{\sin(2\pi\ell s/p)}{\sin(2\pi s/p)} =$$

$$= \prod_{s\in S} (-4)^{(\ell-1)/2} \prod_{t\in T} (\sin^2(2\pi s/p) - \sin^2(2\pi t/\ell)) =$$

$$= (-4)^{(\ell-1)(p-1)/4} \prod_{s,t} (\sin^2(2\pi s/p) - \sin^2(2\pi t/\ell))$$

En permutant les rôles de ℓ et p, on obtient

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

cqfd.

§6. Développements eulériens de sin et de cot

6.1. On suit Bourbaki, [B], Chapitre VI, §2.

Lemme. On a pour $n \in \mathbb{Z}$, $n > 0$:

$$\sin nz = 2^{n-1} \prod_{k=0}^{n-1} \sin(z + k\pi/n)$$

En effet,

$$\sin nz = \frac{1}{2i}(e^{inz} - e^{-inz}) = \frac{e^{-inz}}{2i}(e^{2inz} - 1) =$$

$$= \frac{e^{-inz}}{2i} \prod_{p=0}^{n-1}(e^{2iz} - e^{-2\pi ip/n}) = \frac{1}{2i} \prod_{p=0}^{n-1}(e^{iz} - e^{-iz-2\pi ip/n}) =$$

$$= (2i)^{n-1} \prod_{p=0}^{n-1} e^{-\pi ip/n} \prod_{p=0}^{n-1} \frac{e^{iz+\pi ip/n} - e^{-iz-\pi ip/n}}{2i}$$

Or,

$$(2i)^{n-1} \prod_{p=0}^{n-1} e^{-\pi ip/n} = (2i)^{n-1} e^{-\pi i/n \cdot \sum_{p=0}^{n-1} p} = (2i)^{n-1} e^{-\pi i(n-1)/2} = 2^{n-1},$$

d'où l'assertion.

6.2. En divisant par $\sin z$ et en faisant tendre z vers 0, on obtient:

$$\prod_{p=1}^{n-1} \sin(p\pi/n) = n2^{1-n}$$

6.3. Supposons que $n = 2m + 1$ est impair. Alors 6.1 peut s'écrire

$$\sin nz = (-1)^m 2^{n-1} \prod_{p=-m}^{m} \sin(z - p\pi/n) =$$

$$= (-1)^m 2^{n-1} \sin z \prod_{p=1}^{m} \sin(z - p\pi/n) \sin(z + p\pi/n)$$

Or, on vérifie aisément la formule suivante:

$$\sin^2(a + b) - \sin^2(a - b) = \sin 2a \sin 2b,$$

d'où

$$\sin a \sin b = \sin^2((a + b)/2) - \sin^2((a - b)/2)$$

Il s'en suit,

$$\sin(z - p\pi/n)\sin(z + p\pi/n) = \sin^2 z - \sin^2(p\pi/n),$$

d'où

$$\sin nz = 2^{n-1}\sin z\prod_{p=1}^{m}(\sin^2(p\pi/n) - \sin^2 z)$$

Or, d'après 6.2,

$$\prod_{p=1}^{m}\sin^2(p\pi/n) = \frac{n}{2^{n-1}},$$

d'où

$$\sin nz = n\sin z\prod_{p=1}^{m}(1 - (\sin^2 z/\sin^2(p\pi/n)))$$

En remplaçant z par z/n, on arrive au

6.4 *Théorème.* Si $n = 2m + 1$ est impair alors

$$\sin z = n\sin(z/n)\prod_{k=1}^{m}\left(1 - \frac{\sin^2(z/n)}{\sin^2(k\pi/n)}\right)$$

Maintenant si l'on fait m tendre vers l'infini, on obtient

6.5. *Théorème.*

$$\sin z = z\cdot\prod_{k=1}^{\infty}\left(1 - \frac{z^2}{k^2\pi^2}\right)$$

(Convergence uniforme dans des sous-ensembles compacts.)

Preuve (cf. *op. cit.*). On réecrit 6.4 sous une forme

$$\sin z = n\sin(z/n)\prod_{k=1}^{\infty}(1 - w_k(n, z)) \tag{6.5.1}$$

où $w_k(n, z) = \sin^2(z/n)/\sin^2(k\pi/n)$ si $1 \le k \le m$ et $w_k(n, z) = 0$ si $k > m$.

Lemme. Pour tout z contenu dans une partie compacte $K \subset \mathbb{C}$ et pour tous n impaire, la série $\sum_{k=1}^{\infty} w_k(n, z)$ est *normalement convergente* (uniformément par rapport à n et z).

Démonstration. On a

$$\lim_{n\to\infty} n\sin(z/n) = z$$

uniformement dans K, donc il existe $M > 0$ tel que $|n\sin(z/n)| \le M$ pour tout n et tout $z \in K$.

Sous-lemme. Pour $1 \le k \le m$ on a $n\sin(k\pi/n) \ge k\pi/2$.

En effet, pour $4 \geq x \geq 0$ on a $(\sin x)/x \geq 1 - x^2/6$, donc pour $0 \leq x \leq \pi/2$ on a $(\sin x)/x \geq 1/2$, d'où l'assertion de sous-lemme.

Il s'en suit de sous-lemme que $|w_k(n,z)| \leq 4M^2/k^2\pi^2$ pour tous k et $z \in K$, d'où le lemme en découle.

Le lemme implique qu'on peut faire tendre $n \longrightarrow \infty$ dans (6.5.1); comme pour k fixé, $w_k(n,z)$ tend (uniformément dans K) vers $z^2/k^2\pi^2$, on obtient l'assertion du théorème.

6.6. Prenons la dérivée logarithmique:

$$\cot z = \frac{1}{z} + \sum_{p=1}^{\infty} \frac{2z}{z^2 - p^2\pi^2} = \frac{1}{z} + \sum_{p=1}^{\infty} \left(\frac{1}{z - p\pi} + \frac{1}{z + p\pi} \right)$$

l'égalité est vraie pour tout $z \in \mathbb{C}$ dinstinct d'un multiple entier de π, la série étant normalement convergente dans tout ensemble compact $K \subset \mathbb{C} - \mathbb{Z}\pi$.

Application aux nombres de Bernoulli

6.7. *Exercice.* Montrer que

$$\frac{z}{e^z - 1} = -\frac{z}{2} + \frac{iz}{2}\cot(iz/2)$$

On rappelle que le nombres de Bernoulli sont définis par:

$$\frac{z}{e^z - 1} = 1 - \frac{z}{2} + \sum_{n=1}^{\infty} B_{2n} \frac{z^{2n}}{(2n)!}$$

6.8. Le développement de cot nous dit:

$$\cot\ z - \frac{1}{z} = \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2\pi^2}$$

Maintenant:

$$\frac{2z}{z^2 - n^2\pi^2} = -\frac{2z}{n^2\pi^2} \cdot \frac{1}{1 - z^2/n^2\pi^2} = -\frac{2z}{n^2\pi^2} \cdot \sum_{k=0}^{\infty} \frac{z^{2k}}{n^{2k}\pi^{2k}} =$$
$$= -2 \sum_{k=1}^{\infty} \frac{z^{2k-1}}{n^{2k}\pi^{2k}}$$

$(|z| < \pi)$.

Lemme. La série double

$$\sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{-2z^{2k-1}}{n^{2k}\pi^{2k}} \tag{6.8.1}$$

est absolument convergente dans le disque ouvert $D = \{|z| < \pi\}$ normalement convergente dans tout compact $K \subset D$, et a pour somme $\cot\ z - 1/z$.

En effet, pour $|z| \le a < \pi$, on a

$$\left|\frac{-2z^{2k-1}}{n^{2k}\pi^{2k}}\right| \le \frac{2a^{2k-1}}{n^{2k}\pi^{2k}}$$

et la somme d'un nombre fini quelconque de termes à droite est $\le \sum_{n=1}^{\infty} 2a/(n^2\pi^2 - a^2) < \infty$, d'où la convergeance normale. Pour trouver la somme, on fait d'abord la sommation par rapport à k, puis par rapport à n, et l'on trouve

$$\sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2\pi^2} = \cot\ z - \frac{1}{z}$$

En échangeant l'ordre de sommations, il s'en suit:

$$\cot z = \frac{1}{z} - 2\sum_{k=1}^{\infty} \frac{\zeta(2k)}{\pi^{2k}} z^{2k-1},$$

où

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$$

Donc

$$\frac{z}{e^z - 1} = -\frac{z}{2} + \frac{iz}{2} \cdot \left(\frac{2}{iz} + 2\sum_{k=1}^{\infty} \frac{\zeta(2k)}{\pi^{2k}}(-1)^k i \frac{z^{2k-1}}{2^{2k-1}}\right) =$$

$$= 1 - \frac{z}{2} + \sum_{k=1}^{\infty} (-1)^{k-1} \frac{\zeta(2k)}{2^{2k-1}\pi^{2k}} z^{2k}$$

6.9. En comparaisant avec 6.7,

$$B_{2n} = (-1)^{n-1}(2n)!\frac{2\zeta(2n)}{(2\pi)^{2n}},$$

ou

$$\zeta(2n) = (-1)^{n-1}\frac{(2\pi)^{2n}}{2(2n)!}B_{2n},$$

$n \ge 1$.

Bibliographie

[Ch] K. Chandrasekharan, Introduction to analytic number theory, *Die Grundlehren der mathematischen Wissenschaften*, Band **148**, Springer, 1968.

[D] P.G. Lejeune-Dirichlet, Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viele Primzahlen enthält, *Abh. Akad. Berlin* (1837).

[G] C.F.Gauss (a) Disquisitiones arithmeticae, 1801, Werke, Bd. I. Traduction française: Recherches arithmétiques, Jacques Gabay, 1989. (b) Theoria residuorum biquadraticorum, Commentatio prima, Comm. soc. reg. sci. Gott. 6(1828) = Werke, Bd. II, pp. 65 - 92. (c) Theoria residuorum biquadraticorum, Commentatio secunda, Comm. soc. reg. sci. Gott. 7(1832) = Werke, Bd. II, pp. 93 - 148. (d) Summatio quarumdam serierum singularium, Werke, Bd. II, p. 9. (e) Disquisitiones generales de congruentis, Analysis residuorum Caput octavum, Werke, Bd. II, 212 - 242.

[E] H.M. Edwards, Riemann's zeta function, Dover, Mineola, NY, 2001.

[H] J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, *Bull. Soc. Math. France*, **24** (1896), 199 - 220.

[I] S. Ikehara, *J. Math. Phys. MIT*, **10** (1931), 1 - 12.

[M] C. Moreau, Sur les permutations circulaires distinctes, *Nouv. Ann. Math.*, **11** (1872), 309 - 314.

[VP] Ch. de la Vallée Poussin, Recherches analytiques sur la théorie de nombres premiers, *Ann. Soc. Sci. Bruxelles* **20** (1896), 183 - 256, 281 - 297.

[W] N. Wiener, *Annals of Math.* **33** (1932), 1 - 100.