COURS 1 (17 janvier 2024)

Chapitre 1 : Les nombres premiers

* Un nombre entier $n \geq 2$ est premier si les seuls diviseurs de n sont 1 et n. Autrement, on note p les nbs premiers et $\mathcal{P}$ l'ensemble qu'ils forment.

* Si n n'est pas premier, alors n est divisible par un nbre premier $p \leq \sqrt{n}$.

* Crible d'Eratosthène :

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

$\Longrightarrow \mathcal{P} \cap \{1, \dots, 19\} = \{2, 3, 5, 7, 11, 13, 17, 19\}$

(en fait pour calculer $\mathcal{P} \cap \{1, \dots, N\}$, il suffit de rayer les multiples de $p \leq \sqrt{N}$).

* Lemme d'Euclide :

Lemme : Soient a et b des nbres entiers et soit p un nbre premier qui divise ab. Alors p divise a ou p divise b.

Démonstration : Supposons que p ne divise pas a.
Soit $n = \min\{m > 1 \mid p \text{ divise } am\}$. On a

$$1 < n \leq p.$$

Soit $p = nq + r$ la division euclidienne. $0 \leq r < n$
On a alors

$$ar = ap - anq = ap - (an)q \Rightarrow p \mid ar$$

d'où $r = 0$ par minimalité de n. Donc,
$p = nq \Rightarrow \boxed{n = p}$ car p est premier.
D'un autre côté, p divise ab par hypothèse,
d'où $p = n \leq b$. Soit $b = pn + s$ la
division euclidienne. Alors :

$$as = ab - apn = (ab) - (an)p \Rightarrow p \mid as$$

s est multiple de p, d'où $s = 0$ comme avant

$\Rightarrow p$ divise b ∎

(Avec un peu plus de théorie)

$$G = \{n \in \mathbb{Z} \mid p \text{ divise } an\} \subseteq \mathbb{Z}$$

est un sous-groupe, on revient à la
car il contient p, donc $G = n\mathbb{Z}$ pour
le même n qu'avant.

Si p ne divise pas a, alors $n > 1$. Comme $p \in n\mathbb{Z}$, $p = n$. Par hypothèse, $b \in G$, donc $n = p$ divise b

* Variante : Soient a, b des entiers pas tous deux nuls. Alors

$$\langle a, b \rangle = \{ an + bm \mid n, m \in \mathbb{Z} \} \subset \mathbb{Z}$$

$$= \underbrace{pgcd(a,b)}_{\text{le plus petit élément } \geq 1 \text{ de } \langle a,b \rangle} \cdot \mathbb{Z}$$

$a, b \in \langle a, b \rangle$
$\Rightarrow pgcd(a,b) \mid a$
$pgcd(a,b) \mid b$
et c'est le plus grand avec cette propriété

En particulier, pour $d = pgcd(a,b)$, on a une relation

$$d = au + bv \qquad \text{(Bézout)}$$

Si $d = 1$, on dit que a et b sont premiers entre eux.

Proposition : Soit n un entier ≥ 2.

① Soit a un nombre entier. Alors :

a et n sont premiers entre eux

$\Leftrightarrow$ a mod n est inversible dans $\mathbb{Z}/n\mathbb{Z}$

② n est un nbre premier

$\Leftrightarrow$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps

$\Leftrightarrow$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre

(c'est-à-dire, ne contient pas de diviseur de zéro)

$\boxed{\Rightarrow}$

Démonstration : ① Si a et n sont premiers entre eux, alors $1 = au + nv$, (Bézout) d'où

$1 = \bar{1} \equiv \bar{a}\bar{u} \pmod{n}$,

c'est-à-dire $\bar{a}$ est inversible.

$\boxed{\Leftarrow}$ Si $\bar{a}$ est inversible, alors il existe $b \in \mathbb{Z}$ tel que $1 \equiv \bar{a}.\bar{b} \pmod{n}$. On a donc $1 = ab + nv$, ce qui entraîne que a et n sont premiers entre eux

② Si n est premier, n est premier avec tout $1 \leq a < n$, donc tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible par ①.

On a toujours corps $\Rightarrow$ intègre.

Si n n'est pas premier, alors $n = ab$ pour $1 < a, b < n$, donc $0 \equiv \bar{a}.\bar{b} \pmod{n}$ ($\bar{a} \neq 0$, $\bar{b} \neq 0$)

donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. ∎

Notation :

$$\varphi(n) = \left| \{ a \mid 1 \leq a \leq n \text{ premiers avec } n \} \right|$$

$$= \left| (\mathbb{Z}/n\mathbb{Z})^\times \right|$$

indicatrice d'Euler

Lemme chinois : Soient m et n des entiers premiers entre eux. Alors

$$f : \mathbb{Z}/mn \xrightarrow{\sim} \mathbb{Z}/m \times \mathbb{Z}/n$$

$$a \longmapsto (a \bmod m,\ a \bmod n)$$

f : surjective d'ensemble

d'où : $(\mathbb{Z}/mn)^\times \simeq (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$

et en particulier $\varphi(mn) = \varphi(m)\varphi(n)$

(c'est une fonction multiplicative).

Démonstration : * Il suffit de montrer que f est surjective. Soient $x \bmod m$, $y \bmod n$.

Comme n et m sont premiers entre eux, $1 = nu + mv$ et on pose

$$z = nxu + myv$$

Alors : $z \bmod m = nxu = x(1-mv) \equiv x \bmod m$

$z \bmod n = myv = y(1-nu) \equiv y \bmod n$

* Si $f : A \to B$ est un isomorphisme d'anneaux, alors $f_{|A^\times} : A^\times \to B^\times$ est un isomorphisme de groupes et $(B \times C)^\times \simeq B^\times \times C^\times$ □

Généralisation à plusieurs entiers

$$\mathbb{Z}/m_1 \dots m_\ell \mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_\ell \mathbb{Z}$$

Si $m_1, \dots, m_\ell$ deux à deux premiers entre eux.
et de même pour les inversibles

* Factorisation

Théorème : Pour tout entier $n \geq 1$, il existe des nombres premiers p_i et des exposants $q_i \geq 1$ tels que

$$n = p_1^{q_1} \dots p_2^{q_2}$$

et cette "factorisation" est unique à l'ordre des facteurs près.

Démonstration : par récurrence sur n.

Pour $n=1$, produit vide / supposons le résultat vrai pour les entiers $< n$. On écrit :

$$n = p\,n' \qquad 1 \leq n' < n$$

$$= p\,p_1^{a_1} \cdots p_2^{a_2} \quad \text{par récurrence}$$

Unicité de la factorisation :

$$n = p_1^{a_1} \cdots p_2^{a_2} = q_1^{b_1} \cdots q_s^{b_s}$$

Chaque p_i divise le produit $q_1^{b_1} \cdots q_s^{b_s}$, donc par le lemme d'Euclide divise un des facteurs, donc $p_i = q_j$ pour un certain j. De même, $q_i = p_j$ pour un certain j. Donc $r = s$ et $\{p_1, \ldots, p_2\} = \{q_1, \ldots, q_s\}$, puis $a_i = b_i$ en appliquant encore Euclide. □

Plus généralement, n'importe quel $x \in \mathbb{Q}^\times$ s'écrit de manière unique comme

$$x = \varepsilon \prod_{p \in \mathcal{P}} p^{a_p} \qquad \varepsilon \in \{\pm 1\}$$

$(a_p)_{p \in \mathcal{P}}$ presque tous nuls $a_i \in \mathbb{Z}$

Définition : $a_p = \mathrm{ord}_p(x)$ valuation p-adique

$\mathrm{ord}_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ $\quad \mathrm{ord}_p(0) = \infty$

satisfait à

$$\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$$

$$\mathrm{ord}_p(x+y) \geq \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))$$

avec égalité si $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$.

* $x \in \mathbb{Q}$ est dans $\mathbb{Z} \iff \mathrm{ord}_p(x) \geq 0$ pour tout p

* L'ensemble des nbs premiers est infini.

En effet, autrement $\mathcal{P} = \{p_1, \dots, p_m\}$. Alors $N = p_1 \cdots p_m + 1 > 1$ est multiple d'un nbre premier, mais aucun des p_i divise N $\lightning$

Buts de la première moitié du cours

- Théorème des nbs premiers (Hadamard, de la Vallée-Poussin, 1896)

Pour $X > 0$ réel, posons

$$\pi(X) = \{p \leq X \mid p \text{ premier}\}$$

Alors, $\pi(X) \sim \dfrac{X}{\log X}$ lorsque $X \to \infty$.

(i.e. $\lim\limits_{X \to \infty} \pi(X) \dfrac{\log X}{X} = 1$)

• Théorème de la progression arithétique (Dirichlet) 1837

Soient a et n des entiers premiers entre eux. Alors il existe une infinité de nbs premiers de la forme $a + kn$ (c'est-à-dire congrus à a modulo n)

② Critères de primalité et de non-primalité

Comment savoir si un nbre donné n est premier ou pas ? La méthode de essayer tous les premiers $\leq \sqrt{n}$ est en pratique impraticable.

→ Critère de Fermat. Soit p un nbre premier. Pour tout entier a qui n'est pas multiple de p, on a $a^{p-1} \equiv 1 \mod p$. (« petit théorème de Fermat »)

Démonstration : Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe de cardinal $p-1$. Donc $a^{p-1} = 1$ pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ □

Application : S'il existe $a \in \{1, \dots, n-1\}$ tel que $a^{n-1} \not\equiv 1 \mod n$, alors n n'est pas premier.

⚠ ce n'est pas un critère de primalité :
il existe des nbres, tels que $561 = 3 \times 11 \times 17$,
avec la propriété $a^{n-1} \equiv 1 \pmod n$ pour
tout $1 \leq a < n$ premier à n.
(nbres de Carmichael)

→ Test de Miller-Rabin

Proposition : Soit $p \geq 3$ premier. Écrivons
$p-1 = 2^s m$. Soit a un nbre entier non
multiple de p. Soit $s \geq 0$ le plus petit
tel que $a^{2^s m} \equiv 1 \pmod p$. Si $s > 0$,
alors $a^{m 2^{s-1}} \equiv -1 \pmod p$.

Démonstration : Si $s > 0$, $a^{2^s m} = \left(a^{2^{s-1} m}\right)^2$.
Si p est premier et $b^2 \equiv 1 \pmod p$, alors
$p \mid b^2 - 1 = (b-1)(b+1)$, donc par le
lemme d'Euclide $p \mid b-1 \iff b \equiv 1 \pmod p$
ou $p \mid b+1 \iff b \equiv -1 \pmod p$

Comme $a^{2^{s-1} m} \equiv 1 \pmod p$ contredit la minimalité
de s, on a $a^{2^{s-1} m} \equiv -1 \pmod p$ □

(test de non-primalité)

→ Critère de Lucas :

Quelques propriétés des groupes finis :

Lemme : G groupe abélien fini

$g, h \in G$ d'ordres m, n

Si m et n sont premiers entre eux, alors gh est d'ordre mn.

Démonstration : $\langle g \rangle \cap \langle h \rangle = \{e\}$ dans G car si $x \in \langle g \rangle \cap \langle h \rangle$, l'ordre de x divise m et divise n, donc est égal à 1

Si $(gh)^N = 1$, alors $g^N = h^{-N}$ car G est commutatif. On a donc $g^N = h^{-N} = 1$, ce qui entraîne $n \mid N$, $m \mid N$, donc $mn \mid N$. D'autre part,

$$(gh)^{mn} = g^{mn} h^{mn} = (g^n)^m (h^m)^n = 1$$

□

Proposition : G groupe abélien fini, $S \subset G$ sous ensemble. Il existe un élément de G d'ordre le ppcm(ordres des éléments de S)

Démonstration : Il suffit de voir que si G possède g d'ordre m et h d'ordre n, alors il possède un élément d'ordre $\mathrm{ppcm}(m,n)$. On écrit :

$m = m' m''$ si $\mathrm{ord}_p(m) \geq \mathrm{ord}_p(n)$ $\Rightarrow$
$n = n' n''$

si $\mathrm{ord}_p(m) < \mathrm{ord}_p(n)$

m et p dans m'', n''

$g^{m''}$ d'ordre m' ⟵ premiers entre eux
$h^{n'}$ d'ordre n'' ⟵

$m' n'' = \mathrm{ppcm}(m,n)$

$\Longrightarrow$ l'ordre de $g^{m''} h^{n'}$ est $\mathrm{ppcm}(m,n)$ □

Lemme

Théorème : Soit $n \geq 2$ un entier. Supposons que pour tout $p \mid n-1$, il existe un entier a tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$. Alors n est un nombre premier.

Démonstration : Si $a^{n-1} \equiv 1 \bmod n$, alors a et n sont premiers entre eux. (a est inversible) Pour tout $p \mid n-1$, il existe $a_p \in (\mathbb{Z}/n\mathbb{Z})^\times$ dont l'ordre divise $n-1$ mais pas $\frac{n-1}{p}$. Le ppcm de ces ordres est égale à $n-1$. Par la proposition, il existe un élément d'ordre $n-1$. Donc

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = n-1 \Rightarrow n \text{ est premier} \quad \square$$

Remarque : Nous avons donc démontré que, sous les hypothèses du théorème, $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. C'est toujours le cas pour n premier, ce qui montre que le théorème est mieux si et seulement si.

Théorème : Soit F un corps et soit $G \subset F^\times$ un sous-groupe fini. Alors G est cyclique.

Démonstration 1 : Soit $g \in G$ un élément d'ordre multiple de tous les éléments de G (autrement dit avec $S = G$). Posons $n = \mathrm{ord}(g)$. Alors

$$x^n = 1 \quad \text{pour tout } x \in G$$

L'équation $x^n = 1$ a au plus n solutions (car F est un corps). Comme

$$1, g, g^2, \dots, g^{n-1}$$

sont solutions, on a $G = \langle g \rangle$ □

Démonstration 2 : Soit $n = |G|$. D'après le lemme, il suffit de trouver $g_p \in G$ d'ordre $p^{\mathrm{val}_p(n)}$ (= 2) pour tout $p \mid n$.

L'équation $x^{n/p} = 1$ a au plus $\frac{n}{p} < n$ solutions, donc il existe $x \in G$ tel que $x^{n/p} \neq 1$.

Posons $y = x^{n/p^2}$. On a $y^{p^2} = 1$, $y^{p^{2-1}} = x^{n/p} \neq 1$.

Donc l'ordre de y divise p^2 mais pas p^{2-1},

donc $g_p = y$ convient □

Exemple : calcul d'un générateur de $(\mathbb{Z}/71\mathbb{Z})^\times$

$71 - 1 = 70 = 2 \times 5 \times 7$

on cherche des éléments d'ordre 2, 5, 7

ordre 2 : $-1 = g_2$

ordre 5 : on cherche $x^{14} \neq 1 \mod 71$

$2^{14} \equiv 4^7 \equiv 4 \cdot (16)^3 \equiv 4 \cdot 16 \cdot 256$

$\equiv \underbrace{4 \cdot 16}_{64} \cdot 43 \equiv (-7) \cdot 43 \equiv -301 \equiv -17$

$\Rightarrow g_5 = -17$

ordre 7 : on cherche $x^{10} \neq 1 \mod 71$

$2^{10} \equiv 16 \cdot 64 \equiv 16 \cdot (-7) \equiv -112 \equiv 30$

$\Rightarrow g_7 = 30$

$g_2 g_5 g_7 = (-1) \cdot (-17) \cdot 30 \equiv 510 \equiv 13$

donc $(\mathbb{Z}/71\mathbb{Z})^\times = \langle 13 \rangle$.

COURS 3 (24 janvier 2024)

③ La loi de réciprocité quadratique

Soit p un nombre premier. Notons

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

(c'est un corps à p éléments). Dans cette
↑ car p est premier

section on admettra le résultat qu'il existe un corps $\Omega \supset \mathbb{F}_p$ tel que tout polynôme $P \in \mathbb{F}_p[T]$ de degré ≥ 1 a une racine dans Ω. Un tel Ω s'appelle une clôture algébrique de $\mathbb{F}_p$. et tous les éléments de Ω sont racine d'un polynôme $P \in \mathbb{F}_p[T]$

Question générale : Étant donné $x \in \mathbb{F}_p$, comment décider si x est un carré, c'est-à-dire s'il existe $y \in \mathbb{F}_p$ tel que $y^2 = x$?

* Si $p = 2$, tous les éléments de $\mathbb{F}_2$ sont des carrés. En effet, $0 = 0^2$ et $1 = 1^2$.

Proposition. Soit $p \geq 3$ un nombre premier. Les carrés forment un sous-groupe d'indice 2 d'éléments non nuls de $\mathbb{F}_p$

de $\mathbb{F}_p^\times$, qui est le noyau de l'homomorphisme

$$\begin{aligned} \mathbb{F}_p^\times &\longrightarrow \{\pm 1\} \\ x &\longmapsto x^{\frac{p-1}{2}} \end{aligned}$$

$\leftarrow$ puisque $x^{p-1} = 1$ par le petit théorème de Fermat

Preuve : Pour $x \in \mathbb{F}_p^\times$, soit $y \in \Omega$ un élément de la clôture algébrique tel que $y^2 = x$. On a alors :

$$y^{p-1} = x^{\frac{p-1}{2}} \in \{\pm 1\}$$

On en déduit :

$$x \text{ est un carré} \iff y \in \mathbb{F}_p^\times$$

$\Leftarrow$ évident

$\Rightarrow$ si $x = z^2$, alors $y^{p-1} = z^{p-1} = 1$, donc $y \in \mathbb{F}_p^\times$ car l'équation $y^{p-1} = 1$ a $\leq p-1$ solutions dans le corps Ω et elle en a déjà $p-1$ dans $\mathbb{F}_p^\times$.

Par conséquent :

$$(\mathbb{F}_p^\times)^2 = \ker\left(x \longmapsto x^{\frac{p-1}{2}}\right)$$

Par ailleurs, $\mathbb{F}_p^\times$ est cyclique d'ordre $p-1$.

Si x est un générateur, alors $x^{\frac{p-1}{2}} \neq 1$.
L'application $x \mapsto x^{\frac{p-1}{2}}$ est donc surjective,
d'où : $\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \simeq \{\pm 1\}$ □

Définition : Soit $p \geq 3$ un nombre premier. Le symbole de Legendre de $x \in \mathbb{F}_p^\times$ est l'entier

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{\pm 1\}$$

$$= \begin{cases} 1 & \text{si } x \text{ est un carré} \\ -1 & \text{sinon} \end{cases}$$

On étend le symbole de Legendre à $\mathbb{F}_p$ en posant $\left(\frac{0}{p}\right) = 0$. Si $x \in \mathbb{Z}$, on définit

$$\left(\frac{x}{p}\right) = \left(\frac{x \bmod p}{p}\right) = \begin{cases} 0 & \text{si } p \mid x \\ 1 & \text{si } x \text{ est un carré mod } p \\ -1 & \text{si } x \text{ n'est pas un carré mod } p \end{cases}$$

Le symbole de Legendre est multiplicatif :

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$$

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

c'est-à-dire

-1 est un carré mod $p \iff p \equiv 1 \bmod 4$

Proposition :

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

c'est-à-dire 2 est un carré mod $p \iff$

$p \equiv 1$ ou $p \equiv -1 \bmod 8$

Preuve : Soit $\alpha \in \Omega$ une racine de T^4+1.

L'élément $y = \alpha + \frac{1}{\alpha}$ satisfait alors à

$$y^2 = \left(\alpha + \frac{1}{\alpha}\right)^2 = \alpha^2 + 2 + \frac{1}{\alpha^2} = 2$$

puisque $\alpha^4 = -1$ implique $\alpha^2 = -\frac{1}{\alpha^2}$.

$\therefore$ 2 est un carré mod $p \iff y \in \mathbb{F}_p$

Pour cela on calcule

$$y^p = \left(\alpha + \frac{1}{\alpha}\right)^p = \alpha^p + \frac{1}{\alpha^p}$$

Si $p \equiv 1$ ou $p \equiv -1 \bmod 8$, alors $\alpha^p = \alpha$

car $\alpha^8 = 1$. Donc $y^p = y$, d'où $y \in \mathbb{F}_p$.

Si $p \equiv 5$ ou $p \equiv -5 \bmod 8$, alors $\alpha^p = -\alpha$

car $\alpha = -1$. Donc $y^p = -y$, d'où $y \notin \mathbb{F}_p$ □

Théorème (loi de réciprocité quadratique)

Soient ℓ et p deux premiers impairs distincts.
Alors on a l'égalité

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

Très utile pour calculer !

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right)(-1)^{\cdot 21} = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right)$$

$$= (-1)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right)(-1)^{3.14} = -\left(\frac{1}{7}\right)$$

$29 \equiv 5 \mod 8$

$$= -1$$

$\Rightarrow$ 29 n'est pas un carré mod 43

Démonstration de la loi de réciprocité

Notation : $\varepsilon(n) = \frac{n-1}{2}$ pour n impair

Soit $\alpha \in \Omega$ une racine primitive ℓ ième de l'unité, c'est-à-dire une racine de

$$T^{\ell-1} + T^{\ell-2} + \dots + T + 1.$$

Considérons la somme de Gauss

$$y = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \alpha^x$$

↑ bien défini puisque $\alpha^\ell = 1$

Lemme : (1) $y^2 = (-1)^{\frac{\ell-1}{2}} \ell$

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

Voyons comment conclure en supposant le lemme déjà démontré.

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

Mais, d'autre part,

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

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

Preuve du lemme (1)

$$y^2 = \sum_{x,z \in \mathbb{F}_\ell} \left(\frac{xz}{\ell}\right) \alpha^{x+z} = \sum_{u \in \mathbb{F}_\ell} S(u) \alpha^u$$

avec $S(u) = \sum_{x+z=u} \left(\frac{xz}{\ell}\right) = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x(u-x)}{\ell}\right)$

Si $u = 0$,

$$S(0) = \sum_{x \in \mathbb{F}_\ell} \left(\frac{-x^2}{\ell}\right) = \underbrace{\left(\frac{-1}{\ell}\right)}_{(-1)^{\varepsilon(\ell)}} (\ell - 1)$$

Si $u \neq 0$,

$$S(u) = \sum_{x \in \mathbb{F}_\ell^\times} \left(\underbrace{\frac{x(u-x)}{\ell}}_{\frac{-x^2(1-ux^{-1})}{\ell}}\right)$$

$$= (-1)^{\varepsilon(\ell)} \sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{1-ux^{-1}}{\ell}\right)$$

et $1 - ux^{-1}$ parcourt tous les éléments de $\mathbb{F}_\ell$ sauf 1. Donc

$$\sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{1-ux^{-1}}{\ell}\right) = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) - 1$$

$$= -1$$

↑ autant de carrés que de non carrés dans $\mathbb{F}_\ell^\times$!

Mettant tout ensemble :

$$y^2 = \sum_{u \in \mathbb{F}_\ell} S(u)\, \alpha^u = \underbrace{\left(\frac{-1}{\ell}\right)}_{u=0}\Big[(\ell-1) - \underbrace{\sum_{u=1}^{p-1} \alpha^u}_{-1}\Big]$$

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

$$= (-1)^{\varepsilon(\ell)}\ell$$

Preuve du lemme (2)

$$y^p = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right)^p \alpha^{px} = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \alpha^{px}$$

↑ p impair et $\left(\frac{x}{\ell}\right) \in \{-1, 0, 1\}$

$$\underset{t = px}{=} \sum_{t \in \mathbb{F}_\ell} \left(\frac{t p^{-1}}{\ell}\right) \alpha^t = \left(\frac{p^{-1}}{\ell}\right) y$$

$$\underset{\nearrow}{=} \left(\frac{p}{\ell}\right) y,$$

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

donc $y^{p-1} = \left(\frac{p}{\ell}\right)$ □

Chapitre 2 : le théorème des nombres premiers

① Caractères des groupes abéliens finis

Soit G un groupe abélien fini.

Définition. Un caractère de G est un morphisme de groupes $\chi : G \to \mathbb{C}^\times$.
On note $\hat{G}$ l'ensemble des caractères de G.

* Si G est d'ordre n, alors $g^n = e$ pour tout $g \in G$, d'où $\chi(g)^n = \chi(g^n) = \chi(e) = 1$. Un caractère prend donc ses valeurs dans les racines de l'unité.

* $\hat{G}$ est un groupe, d'élément neutre le caractère trivial $\chi(g) = 1$ pour tout g. Comme

$$1 = |\chi(g)| = \chi(g)\,\overline{\chi(g)}$$

l'inverse d'un caractère est son conjugué $\overline{\chi}$.

Exemple : Si G est cyclique d'ordre n, alors $\hat{G}$ est isomorphe à $\mu_n(\mathbb{C}) = \{\xi \in \mathbb{C} \mid \xi^n = 1\}$.

En effet, comme tout élément de G est de la forme g^a, un caractère χ est déterminé par $\chi(g)$, qui est une racine n-ième de l'unité.

Réciproquement, si $\zeta \in \mu_n(\mathbb{C})$, alors

$$G \longrightarrow \mathbb{C}^\times \quad \text{pour } 0 \le a < n$$
$$g^a \longmapsto \zeta^a$$

est un caractère de G.

$\Rightarrow |\hat{G}| = |G|$ et ils sont même isomorphes.

En général :

Proposition : Soit G un groupe abélien fini. Alors $\hat{G}$ a le même cardinal que G.

(G et $\hat{G}$ sont en fait des groupes isomorphes)

La démonstration repose sur le lemme suivant :

Lemme : Soit H un sous-groupe de G. Pour tout caractère χ_1 de H, il existe un caractère χ de G tel que $\chi_{|H} = \chi_1$.

Preuve : Par récurrence sur l'indice $\frac{|G|}{|H|} = (G:H)$.

* Si $(G:H) = 1$, rien à démontrer.
* Sinon, soit $g \in G \setminus H$ et soit m le plus petit entier tel que $g^m \in H$. Soit

$$H \subset H' = \{ g^a h \mid 0 \le a < m, \ h \in H \} \subset G$$
$$\geq 2$$

C'est un sous-groupe car G est abélien. Si

$$g^a h = g^b h' \Rightarrow g^{b-a} = h h' \in H$$
$$0 \le a \le b < m$$
$$h, h' \in H$$

$\Rightarrow b = a$, $h = h'$ par minimalité de m.

∴ Tout élément de H' s'écrit de même sorte comme $g^q h$.

Soit $\xi \in \mathbb{C}$ tel que $\xi^m = \chi_1(g^m)$ ($g^m \in H$). Pour $x = g^a h$, posons $\chi'(x) = \xi^a \chi_1(h)$

c'est un caractère :

$$\chi'(xy) = \chi'(g^{a+b} hh')$$

($x = g^a h$, $y = g^b h'$)

Si $a+b < m$, $= \xi^{a+b} \chi_1(h)\chi_1(h')$

$$= \chi'(x)\chi'(y)$$

Si $a+b \geq m$, alors $a+b < 2m$,

$$= \chi'(g^{a+b-m} \underbrace{g^m hh'}_{\in H})$$

$$= \xi^{a+b-m} \underbrace{\chi_1(g^m)}_{\xi^m} \chi_1(h)\chi_1(h')$$

$$= \chi'(x)\chi'(y)$$

On a donc étendu le caractère à H', et

$$(G:H') = \frac{(G:H)}{m} < (G:H)$$

Par récurrence, il existe χ caractère de G tel que $\chi_{|H'} = \chi'$, donc $\chi_{|H} = \chi_1$ ▨

Preuve de la proposition : OK pour G cyclique.

Récurrence sur l'ordre $|G|$. Cas $|G| = 1, 2, 3$ OK.

* Soit $h \in G \setminus \{e\}$, $H = \langle h \rangle \subset G$ le sous-groupe cyclique qu'il engendre, $n = |H|$. On a $n > 1$.

* H cyclique $\Rightarrow$ pour toute racine $\zeta \in \mu_n(\mathbb{C})$, il existe un unique caractère $\tilde{\chi}_\zeta$ de H avec $\tilde{\chi}_\zeta(h) = \zeta$.

* Par le lemme, on peut les prolonger en des caractères χ_ζ de G.

* G/H est d'ordre $k = \frac{|G|}{n} < |G|$ Par récurrence, $\bar{\theta}_1, \dots, \bar{\theta}_k$ caractères distincts de G/H

$\theta_i : G \longrightarrow G/H \xrightarrow{\bar{\theta}_i} \mathbb{C}^\times$

satisfaisant à $\theta_i|_H = 1$.

* Introduisons

$$\chi_\zeta \theta_i : G \longrightarrow \mathbb{C}^\times \qquad i = 1, \dots, k \quad \zeta \in \mu_n(\mathbb{C})$$

Ils sont deux à deux distincts :

$\chi_\zeta \theta_i = \chi_{\zeta'} \theta_j$ donne $\zeta = \zeta'$ par restriction à H, puis $\theta_i = \theta_j$

$\therefore$ $k n = |G|$ caractères distincts

Réciproquement, si χ est un caractère de G, $\chi_{|H}$ est de la forme $\tilde{\chi}_\xi$ pour $\xi \in \mu_m(\mathbb{C})$.

Alors $\chi \chi_\xi^{-1}$ vaut 1 sur H, donc donne lieu à un caractère de G/H, donc il est égal à θ_i pour un $i = 1, \dots, k$.

$$\Rightarrow \chi = \chi_\xi \theta_i$$

et on a trouvé tous les caractères □

Remarque : Dans la preuve, on a vu que si h est un élément d'un groupe abélien fini G et $h \neq e$, alors il existe un caractère χ de G tel que $\chi(h) \neq 1$. (« les caractères séparent les points »)

Proposition : Soit G abélien fini.

(1) Pour tout caractère χ de G,

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{si } \chi \neq 1 \\ |G| & \text{si } \chi = 1 \end{cases}$$

(2) Pour tout élément $g \in G$,

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} 0 & \text{si } g \neq e \\ |G| & \text{si } g = e \end{cases}$$

Preuve : ① le cas $\chi = 1$ est évident.

Si $\chi \neq 1$, soit h tel que $\chi(h) \neq 1$. Alors :

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \chi(h) \sum_{g \in G} \chi(g)$$

□

donc $\sum_{g \in G} \chi(g) = 0$

② Si $g \neq e$, il existe $\Psi \in \hat{G}$ tel que $\Psi(g) \neq 1$.

Alors

$$\sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\Psi\chi)(g) = \Psi(g) \sum_{\chi \in \hat{G}} \chi(g)$$

d'où $\sum_{\chi \in \hat{G}} \chi(g) = 0$. Dans le cas $g = e$,

$$\sum_{\chi \in \hat{G}} \chi(g) = |\hat{G}| = |G|$$

par la proposition

□

② Caractères modulaires

Soit $N \geq 1$ un entier. On considère

$G = (\mathbb{Z}/N\mathbb{Z})^\times$ groupe abélien fini à $\varphi(N)$ éléments

Définition : Un caractère de Dirichet modulo N est un caractère de $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e.

un homomorphisme de groupes $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

On peut le voir comme une fonction

$$\chi : \mathbb{Z} \to \mathbb{C}$$

en définissant

$$\chi(a) = \begin{cases} 0 & \text{si } a \text{ et } N \text{ ne sont pas premiers entre eux} \\ \chi(a \bmod N) & \text{si } a \text{ et } N \text{ sont premiers entre eux} \end{cases}$$

Cette fonction satisfait à

$$\chi(ab) = \chi(a)\chi(b)$$

pour tous $a, b \in \mathbb{Z}$

Exemple : Si $N = p$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$, donc le groupe de caractères aussi. Si $p \geq 3$, il existe un unique caractère $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ d'ordre 2 (qui prend donc des valeurs dans $\{\pm 1\}$) : c'est le caractère de Legendre

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$$
$$a \longmapsto \left(\frac{a}{p}\right)$$

Il est non trivial car il prend (autant de fois que la valeur 1) la valeur -1.

Lemme : Soit a un entier non nul sans facteur carré (c'est-à-dire $v_p(a) \in \{0,1\}$ pour tout nombre premier p). Soit $N = 4|a|$. Il existe un unique caractère χ_a modulo n tel que $\chi_a(p) = \left(\frac{a}{p}\right)$ pour tout p qui ne divise pas a. Il vérifie $\chi_a^2 = 1$ et $\chi_a \neq 1$ si $a \neq 1$.

Preuve : Comme tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont des produits de premiers qui ne divisent pas n, s'il existe χ_a est unique et satisfait $\chi_a^2 = 1$.

Existence : si $a = \ell_1 \dots \ell_k$, où les ℓ_i sont des premiers impairs distincts, on pose

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \left(\frac{x}{\ell_1}\right) \cdots \left(\frac{x}{\ell_k}\right)$$

Si p est différent de 2 et des ℓ_i, alors

$$\chi_a(p) = (-1)^{\varepsilon(p)\varepsilon(a)} \left(\frac{p}{\ell_1}\right) \cdots \left(\frac{p}{\ell_k}\right)$$

$$= (-1)^{\varepsilon(p)\varepsilon(a)} (-1)^{\varepsilon(p)(\varepsilon(\ell_1)+\cdots+\varepsilon(\ell_k))} \left(\frac{\ell_1}{p}\right) \cdots \left(\frac{\ell_k}{p}\right)$$

loi de réciprocité quadratique

$$= \left(\frac{a}{p}\right)$$

car $\varepsilon(a) = \varepsilon(\ell_1) + \cdots + \varepsilon(\ell_k) \bmod 2$. En effet, la fonction est donnée par

$$\varepsilon(m) \equiv \begin{cases} 0 & m \equiv 1 \bmod 4 \\ 1 & m \equiv -1 \bmod 4 \end{cases} \bmod 2.$$

On a $\chi_a \neq 1$ car si on choisit x de sorte que $\left(\frac{x}{\ell_1}\right) = -1$ et $x \equiv 1 \bmod 4\ell_2 \cdots \ell_k$, alors on a $\chi_a(x) = -1$.

Si a est de la forme (avec b comme avant)

$-b$ $\quad \chi_b \cdot (-1)^{\varepsilon(x)}$

$2b$ $\quad \chi_b \cdot (-1)^{w(x)}$

$-2b$ $\quad \chi_b (-1)^{\varepsilon(x)+w(x)}$

avec $w(m) = \dfrac{m^2-1}{8} \bmod 2 = \begin{cases} 0 & m \equiv \pm 1 \\ 1 & m \equiv \pm 5 \end{cases} \bmod 8$

et on fait le même type de vérifications. □

Un tel x existe par le lemme chinois

$$(\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/\ell_1\mathbb{Z})^\times \times (\mathbb{Z}/4\ell_2 \cdots \ell_2)^\times$$

et on prend une préimage de $(y, 1)$ avec y non carré modulo ℓ_1.

COURS 5 (31 janvier 2024)

③ Fonction zêta et fonctions L de Dirichlet

Soit $f : \mathbb{N}^* \longrightarrow \mathbb{C}$ une fonction.

(Notation : $\mathbb{N}^* = \{1, 2, 3, \dots\}$)

Définition : On dit que f est **multiplicative** si $f(1) = 1$ et $f(mn) = f(m)f(n)$ pour tous m et n premiers entre eux.

On dit que f est **complètement multiplicative** si $f(1) = 1$ et $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{N}^*$.

Remarque : f multiplicative est déterminée par les valeurs $f(p^k)$, p premier, $k \geq 1$

f complètement multiplicative est déterminée par les valeurs $f(p)$, p premier.

Exemples : $f = 1$ fonction constante

$\chi : \mathbb{N}^* \longrightarrow \mathbb{C}$ caractère de Dirichlet modulo N sont des fonctions complètement multiplicatives.

Soit $(a_p)_p$ une suite de nbres complexes indexée par les nbres premiers. Si la suite

$$\left(\prod_{p \leq n} a_p \right)_n$$

converge, on note $\prod_{p \in \mathcal{P}} a_p$ sa limite, et on l'appelle le produit eulérien des a_p.

Théorème : Soit $f : \mathbb{N}^* \to \mathbb{C}$ une fonction telle que la série $\sum_{n=1}^{\infty} f(n)$ converge absolument (i.e. $\sum_{n=1}^{\infty} |f(n)|$ converge).

Si f est multiplicative, alors

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \left(\sum_{k \geq 0} f(p^k) \right)$$

Si f est complètement multiplicative, alors $|f(p)| < 1$ pour tout nbre premier p et

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \frac{1}{1 - f(p)}$$

Démonstration : Soit $N \geq 1$ un entier, et soit $p_1, \dots, p_r$ les nbres premiers $\leq N$.

$$\prod_{p\le N}\left(\sum_{k=0}^{\infty} f(p^k)\right) = \sum_{n_1,\dots,n_2\in\mathbb{N}} \prod_{i=1}^{2} f(p_i^{n_i})$$

somme car $(f(n))_{n\ge 1}$ l'est par hypothèse

$$= \sum_{n_1,\dots n_2\in\mathbb{N}} f\left(\prod_{i=1}^{2} p_i^{n_i}\right)$$

Si f est multiplicative. Si $A_N \subset \mathbb{N}^*$ désigne l'ensemble des entiers dont les diviseurs premiers sont $\le N$, on a

$$\prod_{p\le N}\left(\sum_{k=0}^{\infty} f(p^k)\right) = \sum_{n\in A_N} f(n)$$

par l'unicité de la décomposition en facteurs premiers. Comme $\mathbb{N}^* = \bigcup_N A_N$ et que $\sum_{n=1}^{\infty} f(n)$ converge absolument, on en déduit

$$\prod_{p}\left(\sum_{k=0}^{\infty} f(p^k)\right) = \sum_{n=1}^{\infty} f(n)$$

Supposons maintenant que f soit complètement multiplicative. On a alors $f(p^k) = f(p)^k$ pour p premier et $k\ge 1$, donc $\sum f(p^k)$ converge implique $|f(p)|<1$. On peut alors développer en série géométrique

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

pour enfin obtenir

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathcal{P}} \frac{1}{1-f(p)} \qquad \square$$

Les exemples qui nous intéressent ne satisfont pas aux hypothèses du théorème. Par contre, pour tout $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$, si f est bornée ($|f(n)| \leq C$ pour tout n), alors la série de Dirichlet

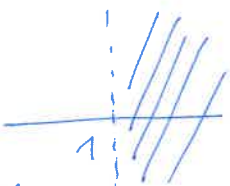
$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

converge absolument, puisque $\left|\frac{f(n)}{n^s}\right| \leq \frac{C}{n^{\mathrm{Re}(s)}}$ et que la série $\sum_{n=1}^{\infty} \frac{1}{n^\alpha}$ converge pour $\alpha > 1$.

En appliquant ce qui précède, on obtient

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

pour tout $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$



Définition : La fonction zêta de Riemann est la série de Dirichlet

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}}$$

Si χ est un caractère de Dirich... modulo N, on appelle fonction L de Dirichlet de χ

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

Remarque : Pour $\chi = 1\!\!1$, le caractère trivial, on trouve

$$L(\chi, s) = \prod_{p \mid N} (1-p^{-s})\ \zeta(s)$$

{ car dans $L(\chi, s)$ seulement les termes premiers à N contribuent

et donc l'étude de la fonction L se réduit à celui de la fonction zêta de Riemann $\zeta(s)$

Théorème : La fonction ζ de Riemann est holomorphe et non nulle sur $\mathrm{Re}(s) > 1$. Elle se prolonge en une fonction méromorphe sur $\mathrm{Re}(s) > 0$ avec un unique pôle en $s = 1$, simple de résidu égal à 1.

Preuve : La série $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converge uniformément sur chaque demi-plan $\mathrm{Re}(s) > a$ avec $a > 1$ et une limite de fonctions holomorphes qui converge uniformément est holomorphe.

pour tout $\varepsilon > 0$, il existe n_0 tel que $|f_n(x) - f(x)| < \varepsilon$ pour tout $n \geq n_0$ et tout x

Pour le prolongement :

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

$$\int_1^{\infty} x^{-s}\,dx = \left[\frac{x^{1-s}}{1-s}\right]_1^{\infty}$$

$$= \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s}\right) dx$$

Par intégration par parties :

$$f_n(s) = \int_n^{n+1} \underbrace{\left(\frac{1}{n^s} - \frac{1}{x^s}\right)}_{u} \underbrace{dx}_{d(x-n-1)} = \left[\left(\frac{1}{n^s} - \frac{1}{x^s}\right)(x-n-1)\right]_n^{n+1}$$

$$+ s \int_n^{n+1} (n+1-x)\, x^{-s-1}\, dx$$

$\int d(uv) = \int du\, v + \int u\, dv$

$$= s \int_n^{n+1} (n+1-x)\, x^{-s-1}\, dx$$

$$\Rightarrow |f_n(s)| \leq \frac{|s|}{n^{\mathrm{Re}(s)+1}}$$

converge normale $\Rightarrow$ converge uniformément

La fonction f_n est holomorphe sur $\mathrm{Re}(s) > 0$ et la série $\sum f_n(s)$ converge uniformément sur $\mathrm{Re}(s) > a$ pour tout $a > 0$, donc f est holomorphe sur $\mathrm{Re}(s) > 0$, et on a

$$\zeta(s) = \frac{1}{s-1} + f(s)$$

Pour la non-annulation on utilise :

Lemme : Si $\sum_{n=1}^{\infty} |u_n| < \infty$, le produit $\prod_{n=1}^{\infty} (1+u_n)$ converge. Il converge vers 0 $\Leftrightarrow$ un des facteurs est nul.

Dans notre situation :

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \prod_p \left(1 + \underbrace{\frac{1}{p^s} + \cdots}_{u_n}\right)$$

et la somme $\sum_p \left|\frac{1}{p^s}+\cdots\right| \leq \sum_n \left|\frac{1}{n^s}\right|$

converge pour $\mathrm{Re}(s)>1$. □

Théorème. Soit χ un caractère de Dirichlet modulo N. Si $\chi \neq \mathbb{1}$, la fonction

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

se prolonge en une fonction holomorphe sur $\{\mathrm{Re}(s)>0\}$.

Démonstration : Soit $F(n) = \sum_{m=1}^{n} \chi(m)$.

Pour $\mathrm{Re}(s)>1$, on a :

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

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

La fonction $F(n)$ est bornée :

$$F(n) = \sum_{\substack{m=1 \\ m \bmod N}}^{n} \chi(m), \quad \text{d'où : } |F(n)| \leq \varphi(N)$$

$$\uparrow$$

$$\sum_{m=1}^{N} \chi(m) = 0$$

Par ailleurs, lorsque n tend vers l'infini

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

$$= O\left(\frac{1}{n^{s+1}}\right)$$

Par conséquent, la série

$$\sum F(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)$$

converge absolument pour $\mathrm{Re}(s) > 0$, uniformément dans $\mathrm{Re}(s) > a$ pour $a > 0$. Sa somme est une fonction holomorphe qui prolonge $L(\chi, s)$ □

Preuve du lemme sur les produits infinis

Comme $\sum |a_n|$ converge, $|u_n| \to 0$ quand $n \to \infty$, et en particulier $|u_n| < \frac{1}{2}$ pour n assez grand. Quitte à "enlever" un nombre fini de termes, on peut supposer $|u_n| < \frac{1}{2}$ pour tout n. On définit alors

$$\log(1+u_n) = \sum_{m=1}^{\infty} (-1)^{m+1} \frac{u_n^m}{m}$$

et cette quantité satisfait $1 + u_n = e^{\log(1+u_n)}$.

On a alors :

$$\prod_{n=1}^{N}(1+u_n) = \prod_{n=1}^{N} e^{\log(1+u_n)} = e^{\sum_{n=1}^{N}\log(1+u_n)}$$

Comme

$$|\log(1+z)| \leq 2|z| \quad \text{si } |z| < \frac{1}{2}$$

(en effet, $|\log(1+z)| \leq \sum_{n=1}^{\infty} \frac{|z|^n}{n} \leq |z| \underbrace{\sum_{n=1}^{\infty} \frac{1}{2^{n-1}}}_{2}$)

la série $\sum_{n=1}^{N} \log(1+u_n)$ converge par comparaison avec $\sum_{n=1}^{\infty} |u_n|$. Notons C sa limite, on a

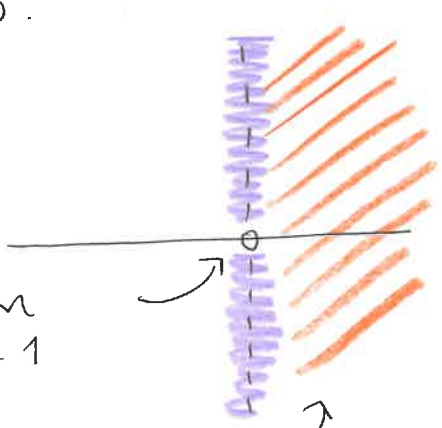
$$\prod_{n=1}^{N}(1+u_n) \xrightarrow[N\to\infty]{} e^{C} \neq 0$$

□

COURS 6 (2 février 2024)

4) Non-annulation sur la droite $\mathrm{Re}(s)=1$

Théorème : Pour tout nombre complexe $s \in \mathbb{C}\setminus\{1\}$ tel que $\mathrm{Re}(s)=1$, on a $\zeta(s)\neq 0$.



Démonstration : Si $\mathrm{Re}(s)>1$,

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

et $\zeta(s)\neq 0$. Prenons la dérivée logarithmique

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \underbrace{\log(1-p^{-s})'}_{\frac{-(p^{-s})'}{1-p^{-s}} = \frac{p^{-s}\log p}{1-p^{-s}}} = \sum_p \frac{\log p}{p^s-1}$$

$$= \sum_p \frac{\log p}{p^s} + \sum_p \frac{\log p}{p^s(p^s-1)}$$

$$\frac{1}{p^s-1} = \frac{1}{p^s} + \frac{1}{p^s(p^s-1)}$$

Comme $\log p = O(p^\varepsilon)$ pour tout $\varepsilon>0$, les séries $\sum_p \frac{\log p}{p^s}$ et $\sum_p \frac{\log p}{p^s(p^s-1)}$ convergent

uniformément dans $\{Re(s) > a\}$ pour $a > 1$ et $\{Re(s) > b\}$ pour $b > \frac{1}{2}$ respectivement, et définissent donc des fonctions holomorphes sur $\{Re(s) > 1\}$ et $\{Re(s) > \frac{1}{2}\}$.

On a :

$$\underbrace{\sum_p \frac{\log p}{p^s}}_{\Phi(s)} = -\frac{\zeta'(s)}{\zeta(s)} - \underbrace{\sum_p \frac{\log p}{p^s(p^s-1)}}_{\Psi(s)}$$

et donc $\Phi(s)$ se prolonge en une fonction méromorphe sur $\{Re(s) > \frac{1}{2}\}$.

↳ pôles proviennent du pôle simple de ζ en $s=1$ (pôle simple de résidu 1 car

$$\zeta(s) = \frac{1}{s-1} + f(s)$$

$$\Rightarrow \frac{\zeta'(s)}{\zeta(s)} = \frac{-\frac{1}{(s-1)^2} + f'(s)}{\frac{1}{s-1} + f(s)} = \frac{-\frac{1}{s-1} + (s-1)f'(s)}{1 + (s-1)f(s)}$$

donc $\lim_{s \to 1} (s-1)\frac{\zeta'(s)}{\zeta(s)} = 1$)

et des zéros de ζ dans le demi plan $\{Re(s) > \frac{1}{2}\}$ avec résidu $-$ ordre du zéro

(par un calcul similaire). En particulier,

$$\lim_{\sigma \to 1} (\sigma - 1)\, \Phi(\sigma) = 1$$

$$\lim_{\sigma \to 1} (\sigma - 1)\, \Phi(\sigma + it) = -m$$

si ζ s'annule à l'ordre m en $s = \sigma + it$.

Supposons que ζ a un zéro d'ordre m en $s = 1 + it$ et que ζ a aussi un zéro d'ordre n en $s = 1 + 2it$. Comme

$$\zeta(\bar{s}) = \overline{\zeta(s)}$$

car c'est vrai sur la droite réelle > 1 (+ fonction holomorphe)

cela entraîne que

$\zeta(s)$ a un zéro d'ordre m en $1 - it$

n en $1 - 2it$

Soit σ un nombre réel $>$. Alors:

$$F(\sigma) = \Phi(\sigma - 2it) + 4\Phi(\sigma - it) + 6\Phi(\sigma) + 4\Phi(\sigma + it) + \Phi(\sigma + 2it)$$

$$= \sum_p \frac{\log p}{p^\sigma} \underbrace{\left(p^{2it} + 4p^{it} + 6 + 4p^{-it} + p^{-2it}\right)}_{\left(p^{\frac{it}{2}} + p^{-\frac{it}{2}}\right)^4}$$

$$= \sum_p \sum_{m \geq 1} \frac{\log p}{p^{m\sigma}} \underbrace{\left(2\cos\left(\tfrac{t}{2}\log p\right)\right)^4}_{p^{i\frac{t}{2}} + p^{-i\frac{t}{2}} = e^{i\frac{t}{2}\log p} + e^{-i\frac{t}{2}\log p}} \geq 0$$

Par conséquent, cette fonction

$$\lim_{\sigma \to 1^+} (\sigma - 1) F(s) \geq 0$$

mais le côté gauche est aussi égal à

$$-n - 4m + 6 - 4m - n \geq 0$$

$$\Leftrightarrow \boxed{8m + 2n \leq 6}$$

qui a une solution en $m \geq 0$ seulement pour $m = 0$.

$\therefore$ $\zeta(s)$ ne s'annule pas en $s = \sigma + it$. $\square$

Théorème : Soit χ un caractère de Dirichlet modulo N.

(1) Si $\chi \neq \mathbb{1}$, alors $L(\chi, s) \neq 0$ pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) \geq 1$.

(2) Si $\chi = \mathbb{1}$, alors $L(\chi, s) \neq 0$ pour tout $s \in \mathbb{C} \setminus \{1\}$ avec $\mathrm{Re}(s) \geq 1$.

Proposition. Si $\chi \neq 1$ est réel (c'est-à-dire $\chi = \bar{\chi}$), alors $L(\chi, 1) \neq 0$.

Démonstration : Pour $t \in [0, 1)$, soit

$$f(t) = \sum_{d=1}^{\infty} \chi(d) \frac{t^d}{1-t^d}$$

Cette série converge normalement sur chaque intervalle $[0, a]$ avec $a < 1$, puisque

$$\left| \chi(d) \frac{t^d}{1-t^d} \right| \leq \frac{a^d}{1-a^d}$$

Écrivons

$$f(t) = \sum_{d=1}^{\infty} \chi(d) \sum_{m=1}^{\infty} t^{dm} = \sum_{n=1}^{\infty} t^n \sum_{d \mid n} \chi(d)$$

en regroupant les termes de même valeur $n = dm$.

Soit $c_n = \sum_{d \mid n} \chi(d)$. Si $n = p^a$, alors

$$c_{p^a} = 1 + \chi(p) + \chi(p)^2 + \ldots + \chi(p)^a$$

$$= \begin{cases} 1 & \text{si } p \mid N \\ a+1 & \text{si } \chi(p) = 1 \\ 1 & \text{si } \chi(p) = -1 \quad a \text{ pair} \\ 0 & \text{si } \chi(p) = -1 \quad a \text{ impair} \end{cases}$$

Dans tous les cas, $c_{p^q} \geq 0$. En général :

$n = \prod p_i^{q_i}$ donne

$$c_n = \sum_{m_1=0}^{q_1} \cdots \sum_{m_2=0}^{q_2} \underbrace{\chi(p_1^{m_1} \cdots p_2^{m_2})}_{\chi(p_1^{m_1}) \cdots \chi(p_2^{m_2})}$$

$$= \prod_{i=1}^{2} c_{p_i^{q_i}} \geq 0$$

On a $\sum_{n=1}^{\infty} c_n = +\infty$ car $c_n = 1$ pour tous les puissances de p divisant N et $c_n \geq 0$ pour tout n.

$$\Rightarrow \lim_{t \to 1^-} f(t) = +\infty.$$

Soit $b_n = (1-t)\left(\frac{t^n}{1-t^n} - \frac{1}{n(1-t)}\right)$

Logique : $\frac{t^n}{1-t^n} \sim \frac{1}{n(1-t)}$ si $t \to 1$

$$= \frac{t^n}{1+t+\cdots+t^{n-1}} - \frac{1}{n}$$

La suite (b_n) est croissante. En effet,

$$b_n - b_{n+1} = \frac{t^n}{(1+t+\cdots+t^{n-1})(1+t+\cdots+t^n)} - \frac{1}{n(n+1)}$$

Par ailleurs,

$$1+t+\cdots+t^{n-1} \geq n\, t^{\frac{n-1}{2}}$$

$$1+t+\dots+t^n \geq (n+1)\,t^{\frac{n}{2}} \geq (n+1)\,t^{\frac{n+1}{2}}$$

$t<1$

(inégalité arithmético-géométrique)

ce qui donne

$$b_n - b_{n+1} \leq \frac{t^n}{n(n+1)\,t^n} - \frac{1}{n(n+1)} = 0$$

$$\Rightarrow \quad b_n \leq b_{n+1}$$

Supposons par l'absurde que $\sum_{n=1}^{\infty} \frac{\chi(n)}{n} = L(\chi,1)$ s'annule. Alors :

$$f(t) = \sum_{n=1}^{\infty} \chi(n)\,\frac{t^n}{1-t^n}$$

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

$$= \frac{1}{1-t} \sum_{n=1}^{\infty} b_n\,\chi(n)$$

Puisque χ est périodique de période N et que $\sum_{n=1}^{N} \chi(n) = 0$, on a $\left|\sum_{d=1}^{n} \chi(d)\right| \leq N$

quelque soit l'entier n. Mais alors :

$$\left|\sum_{n=1}^{\infty} b_n\,\chi(n)\right| = \left|\sum_{d=1}^{\infty} \left(\sum_{n=1}^{d} \chi(n)\right)(b_d - b_{d+1})\right|$$

$$\leq N \sum_{d=1}^{\infty} (b_{d+1} - b_d) = N(1-t)$$

$\uparrow$ $b_1 = t-1$

On a donc $|f(t)| \leq N$ pour tout $t \in [0,1)$, en contradiction avec le fait que $f(t) \to \infty$ pour $t \to 1$ □

Démonstration du théorème : L'énoncé de non-annulation pour $\mathrm{Re}(s) \geq 1$ a déjà été traité avec le produit eulérien.

Posons

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

↑ produit sur tous les caractères de Dirichlet modulo N

et calculons la dérivée logarithmique pour $\mathrm{Re}(s) > 1$:

$$-\frac{Z'(s)}{Z(s)} = \sum_{\chi} \sum_{p} \log(1-\chi(p)p^{-s})'$$

$$= \sum_{\chi} \sum_{p} \frac{\chi(p)\log p}{p^s - \chi(p)}$$

$$= \sum_p \left(\sum_\chi \chi(p) \right) \frac{\log p}{p^s} + \sum_\chi \sum_p \frac{\chi(p)^2 \log p}{p^s (p^s - \chi(p))}$$

$$\frac{\chi(p)}{p^s - \chi(p)} = \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^s - \chi(p)}$$

Posons $\Phi(s) = \sum_p \left(\sum_\chi \chi(p) \right) \frac{\log p}{p^s}$

$$= \varphi(N) \sum_{p \equiv 1 \bmod N} \frac{\log p}{p^s}$$

$$\sum_\chi \chi(p) = \begin{cases} 0 & p \not\equiv 1 \\ |(\mathbb{Z}/N\mathbb{Z})^\times| = \varphi(N) & \text{si } p \equiv 1 \end{cases}$$

Soit $t > 0$ un nombre réel. Posons

$$q = \operatorname{ord}_{s=1} Z(s) = \sum_\chi \text{ ordre du zéro/pôle de } L(\chi, s) \text{ en } s = 1$$

$$m = \operatorname{ord}_{s=1+ti} Z(s)$$

$$n = \operatorname{ord}_{s=1+2ti} Z(s)$$

On sait déjà que $\zeta(s)$, et donc $L(\mathbb{1}, s)$, a un pôle simple en $s = 1$ et que les autres

fonctions L n'ont pas de pôle dans $\{\mathrm{Re}\, s > 0\}$.

Donc : $q \geq -1$, $m, n \geq 0$.

Comme $\overline{L(\chi, s)} = L(\bar{\chi}, \bar{s})$, et que $Z(s)$ est le produit sur tous les caractères, on a aussi

$$m = \mathrm{ord}_{s=1-ti} Z(s)$$

$$n = \mathrm{ord}_{s=1-2ti} Z(s)$$

Avec la même méthode déjà utilisée pour les fonctions zêta,

$$\sum_{k=-2}^{2} \binom{4}{2+k} \Phi(\sigma + tki) = \sum_{\substack{p \equiv 1 \\ \mathrm{mod}\, N}} \frac{\log p}{p^\sigma} \left(2\cos(t \log p)\right)^4 \geq 0$$

ce qui en multipliant par $(\sigma - 1)$ et faisant $\sigma \to 1$ donne

$$-n - 4m - 6q - 4m - n \geq 0$$

$$\Longrightarrow \quad -6q \geq 8m + 2n$$

et les seuls situations possibles sont

$q = -1 \Longrightarrow m = 0$, ce qui veut dire

$q = 0$

Dans le cas $q = 0$, il existe un (seul !) caractère χ modulo N tel que

$L(\chi, s)$ a un zéro simple en $s = 1$

(pour comprendre le pôle simple de $\zeta(s)$)

Mais $L(\overline{\chi}, 1) = \overline{L(\chi, 1)} = 0$, et comme il y a un seul caractère $\chi = \overline{\chi}$, c'est-à-dire χ est à valeurs réelles. Mais on a déjà vu $L(\chi, 1) \neq 0$ dans ce cas $\square$

COURS 7 (9 février 2024)

⑤ Le théorème de la progression arithmétique

Théorème (Dirichlet, 1837)

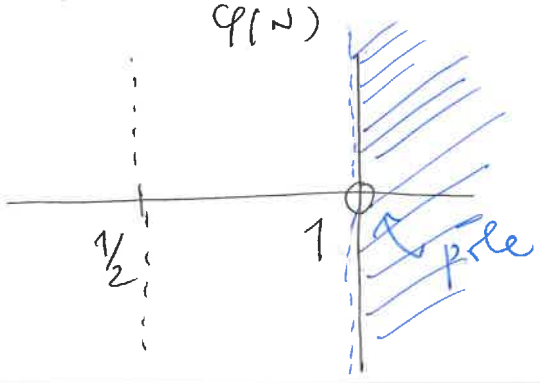
Soient a et N des entiers premiers entre eux. Alors il existe une infinité de nombres premiers de la forme $p \equiv a \bmod N$.

Pour $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$, posons

$$\Phi(s; a) = \sum_{\substack{p \equiv a \\ \bmod N}} \frac{\log p}{p^s}$$

qui est une fonction holomorphe d'après ce qu'on a déjà vu. sur $\mathrm{Re}(s) > 1$

Proposition. $\Phi(s; a)$ se prolonge en une fonction méromorphe dans $\{\mathrm{Re}\, s > \frac{1}{2}\}$ qui n'a pas de pôle dans un voisinage de $\{\mathrm{Re}\, s \geq 1\}$, sauf un pôle simple de résidu $\frac{1}{\varphi(N)}$ en $s = 1$.



Preuve : Soit χ un caractère de Dirichlet modulo N et $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$. Alors :

$$-\frac{L'(\chi,s)}{L(\chi,s)} = \sum_p \chi(p) \frac{\log p}{p^s} + \underbrace{\sum_p \chi(p)^2 \frac{\log p}{p^s(p^s - \chi(p))}}_{\Psi(\chi,s)}$$

fonction définie dans $\{\mathrm{Re}(s) > 0\}$ qui,

* pour $\chi \neq \mathbb{1}$ n'a pas de pôle dans un voisinage ouvert de $\{\mathrm{Re}(s) \geq 1\}$

(en effet, $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 0,\ L(\chi,s) \neq 0\}$ est un ouvert contenant $\{\mathrm{Re}(s) \geq 1\}$)

* pour $\chi = \mathbb{1}$, pôle simple de résidu égal à 1.

$$\sum_p \chi(p) \frac{\log p}{p^s} = -\frac{L'(\chi,s)}{L(\chi,s)} - \Psi(\chi,s)$$

$\Psi(\chi,s)$: holomorphe sur $\mathrm{Re}(s) > \frac{1}{2}$

$\therefore \sum_p \chi(p) \frac{\log p}{p^s}$ définit une fonction méromorphe dans $\{\mathrm{Re}(s) > \frac{1}{2}\}$, sans pôle au voisinage de $\{\mathrm{Re}(s) \geq 1\}$ sauf en $s = 1$ si $\chi = \mathbb{1}$.

Comme a et N sont premiers entre eux, $\chi(a) \neq 0$, et on peut donc écrire :

$$-\sum_{\chi} \frac{L'(\chi,s)}{L(\chi,s)} \chi(a)^{-1} = \sum_{p} \left(\sum_{\chi} \chi(p) \chi(a)^{-1} \right) \frac{\log p}{p^s}$$

$$+ \sum_{\chi} \Psi(\chi,s) \chi(a)^{-1}$$

somme sur tous les caractères de Dirichlet modulo N

D'ailleurs,

$$\sum_{\chi} \chi(p) \chi(a)^{-1} = \sum_{\chi} \chi(pb) = \begin{cases} 0 & pb \not\equiv 1 \\ \varphi(N) & pb \equiv 1 \end{cases}$$

b inverse de a modulo N

et comme $pb \equiv 1 \bmod N$ équivaut à $p \equiv a \bmod N$,

$$-\sum_{\chi} \frac{L'(\chi,s)}{L(\chi,s)} \chi(a)^{-1} = \varphi(N) \Phi(s;a) + \sum_{\chi} \Psi(\chi,s) \chi(a)^{-1}$$

Par conséquent,

$$\Phi(s;a) = \frac{1}{\varphi(N)} \left(-\sum_{\chi} \frac{L'(\chi,s)}{L(\chi,s)} \chi(a)^{-1} - \cdots \right)$$

s'étend en une fonction méromorphe dans le demi-plan $\{Re(s) > \frac{1}{2}\}$, sans pôle au voisinage de $\{Re(s) \geq 1\}$ sauf en $s=1$ où elle a un pôle simple de résidu $\frac{1}{\varphi(N)}$ (comptant au caractère $\chi = 1$, qui vaut 1 sur a) □

Démonstration du théorème : Comme $\Phi(s;a)$ a un pôle en $s=1$, $\lim_{s \to 1} \Phi(s;a) = +\infty$, ce qui serait en contradiction avec la formule de la somme $\sum_{1 \equiv a \bmod N} \frac{\log p}{p^s}$.

⑥ Le théorème des nombres premiers

Théorème (Hadamard, de la Vallée-Poussin, 1876)

$$\text{Lorsque } X \to +\infty, \quad \pi(X) \sim \frac{X}{\log X}$$

Pour tout nombre réel $X > 0$, posons

$$\theta(X) = \sum_{p \leq X} \log p.$$

Lemme : Si $\theta(x) \sim X$ lorsque $X \to +\infty$, alors

$$\pi(X) \sim \frac{X}{\log X} \text{ lorsque } X \to +\infty.$$

Preuve : Par définition,

$$\theta(X) = \sum_{p \leq X} \log p \leq \sum_{p \leq X} \log X = \pi(X) \log X,$$

d'où : $$\frac{\theta(X)}{X} \leq \frac{\pi(X)}{X/\log X}.$$

Pour tout $0 < \varepsilon < 1$,

$$\theta(X) \geq \sum_{X^{1-\varepsilon} \leq p \leq X} \log p$$

$$\geq (1-\varepsilon) \log X \left(\pi(X) - \pi(X^{1-\varepsilon})\right)$$

$$\geq (1-\varepsilon) \log X \left(\pi(X) - X^{1-\varepsilon}\right),$$

d'où : $$\pi(X) \leq \frac{\theta(X)}{(1-\varepsilon)\log X} + X^{1-\varepsilon}$$

mettant les deux estimés ensemble :

$$\frac{\theta(X)}{X} \leq \frac{\pi(X)}{X/\log X} \leq \frac{\theta(X)}{(1-\varepsilon)X} + \frac{\log X}{X^{\varepsilon}}$$

$X \to +\infty$ ↓

$$1 \leq \liminf_{X \to \infty} \frac{\pi(X)}{X/\log X} \leq \frac{1}{1-\varepsilon}$$

puis $\varepsilon \to 0$: 0 □

Lemme : Supposons que l'intégrale

$$\int_1^{\infty} \frac{\theta(t)-t}{t^2}\,dt$$

converge. Alors $\theta(x) \sim x$ lorsque $x \to +\infty$.

Preuve : Soit λ un nombre réel tel que $\theta(x) > \lambda x$ avec $\lambda > 1$. Alors :

$$\int_x^{\lambda x} \frac{\theta(t)-t}{t^2}\,dt \geq \int_x^{\lambda x} \frac{\theta(x)-t}{t^2}\,dt$$

θ est croissante

$$\geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\,dt$$

$t = xu$, $dt = x\,du$

$$\int_1^{\lambda} \frac{\lambda - u}{u^2}\,du > 0$$

$$\frac{\lambda x - xu}{x^2 u^2} x\,d$$

Si l'intégrale converge, alors pour tout $\varepsilon > 0$, il existe $\eta \geq 1$ tel que

$$\left| \int_a^b \frac{\theta(t)-t}{t^2}\,dt \right| < \varepsilon \quad \text{pour tout } b \geq a \geq \eta.$$

(critère de Cauchy). Donc, pour X assez grand, on ne peut pas avoir $\theta(X) > \lambda X$ avec $\lambda > 1$.

* De même, supposons que $\theta(X) < \lambda X$ pour X réel avec $\lambda < 1$. Alors:

$$\int_{\lambda X}^{X} \frac{\theta(t)-t}{t^2}\,dt \leq \int_{\lambda X}^{X} \frac{\theta(x)-t}{t^2} \leq \int_{\lambda X}^{X} \frac{\lambda X - t}{t^2}\,dt$$

$$\| \int_{\lambda}^{1} \frac{\lambda - u}{u^2}\,du < 0,$$

donc par le même argument on ne peut pas avoir de tels X arbitrairement grands:

$$\therefore \boxed{\lim_{X \to \infty} \frac{\theta(X)}{X} = 1} \qquad \square$$

Lemme: Il existe un nombre réel $C > 0$ tel que $\theta(X) \leq CX$ pour tout $X \geq 2$.

Preuve: Pour $n \geq 1$ entier, on a:

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} \geq \binom{2n}{n}$$

Au vu de la formule

$$\binom{2n}{n} = \frac{(2n)!}{n!\,n!} = \frac{2n\,(2n+1)\cdots(n+1)}{1\cdot 2\cdots n}$$

tout nbre premier p tel que $n < p < 2n$ divise (exactement une fois) $\binom{2n}{n}$, d'où :

$$\binom{2n}{n} \geq \prod_{n<p<2n} p$$

$$\Rightarrow \quad \prod_{n<p<2n} p \leq \binom{2n}{n} \leq 2^{2n}$$

et on prend les logarithmes

$$\theta(2n) - \theta(n) \leq 2n \log 2$$

Soit X un nbre réel et $n = \lceil X/2 \rceil$, de sorte que $n-1 < X/2 \leq n$. On en déduit :

$$2n-2 < X \leq 2n$$

$$\theta(X) - \theta(X/2) \leq \theta(2n) - \theta(n-1)$$

$$\theta(2n) - \theta(n) + \theta(n) - \theta(n-1)$$

$$\leq 2n \log 2 + \theta(n) - \theta(n-1)$$

$$\leq \log n \leq n$$

$$\leq n(2\log 2 + 1) \leq X(2\log 2 + 1)$$

$$n < 1 + X/2 \leq X \text{ si } X \geq 2$$

(l'égalité est aussi trivialement satisfaite pour $0 < X < 2$ car $\theta(X) = 0$ dans ce cas).

Pour $X > 1$

$$\theta(X) \leq \sum_{n=0}^{\infty} \left(\theta\left(\frac{X}{2^n}\right) - \theta\left(\frac{X}{2^{n+1}}\right) \right)$$

$$\leq (1 + 2\log 2) \sum_{n=0}^{\infty} \frac{X}{2^n}$$

$$\leq 2(1 + 2\log 2) X$$

□

COURS 10 (16 février 2024)

⑦ le théorème de Newman

Rappel : la dernière fois nous avons vu la démonstration du théorème des nombres premiers à

$$\underbrace{\frac{\Phi(s)}{s} - \frac{1}{s-1}}_{\text{fonction holomorphe au voisinage de } \{\mathrm{Re}(s) \geq 1\}} = \int_1^\infty \frac{\theta(x) - x}{x^{s+1}}\, dx$$

et pour conclure il fallait savoir que

$$\lim_{s \to 1} \int_1^\infty \frac{\theta(x) - x}{x^{s+1}}\, dx = \int_1^\infty \frac{\theta(x) - x}{x^2}\, dx$$

En remplaçant s par $s+1$ pour regarder la situation en $s=0$ et faisant le changement de variable $x = e^t$, on trouve :

$$\lim_{s \to 0} \int_0^\infty \frac{\theta(e^t) - e^t}{e^{(s+2)t}}\, e^t\, dt$$

$$= \lim_{s \to 0} \int_0^\infty f(t)\, e^{-st}\, dt$$

avec $f(t) = \theta(e^t) e^{-t} - 1$. Cette fonction est bornée, car on a vu que $\theta(X) \leq CX$ pour tout nombre réel $X > 0$, d'où

$$-1 \leq f(t) \leq C - 1$$

Théorème (Newman) Soit $f : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{C}$ une fonction mesurable bornée telle que

$$g(s) = \int_0^\infty f(t) e^{-st} \, dt \qquad \mathrm{Re}(s) > 0$$

converge et définit une fonction holomorphe sur $\{\mathrm{Re}(s) > 0\}$ qui se prolonge en une fonction holomorphe sur un voisinage de $\{\mathrm{Re}(s) \geq 0\}$.

Alors $\int_0^\infty f(t) \, dt$ existe et vaut $\boxed{g(0)}$.

Démonstration du théorème : Pour chaque $T > 0$, posons

$$g_T(s) = \int_0^T f(t) e^{-st} \, dt$$

qui est une fonction holomorphe sur $\mathbb{C}$.

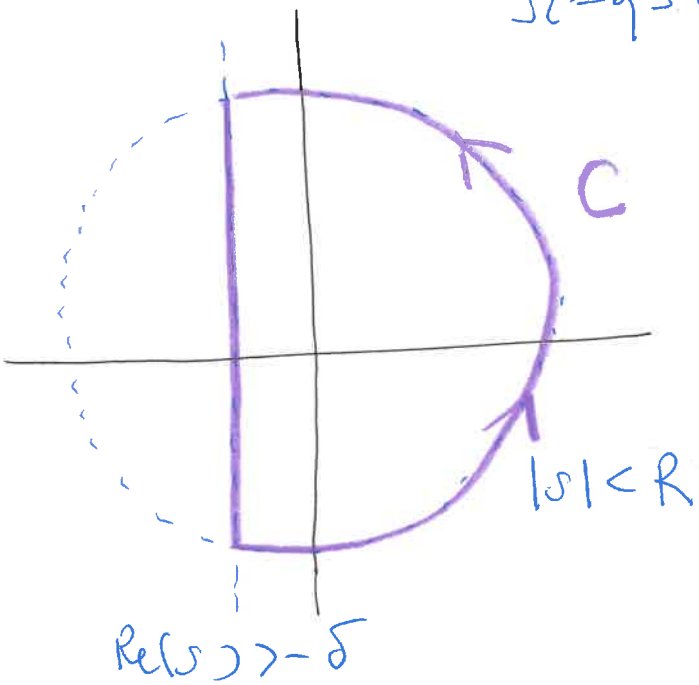
Notre but : $g(0) = \lim_{T \to \infty} g_T(0)$

Comme f est par hypothèse bornée,

$$B = \max_{t \in \mathbb{R}_{\geq 0}} |f(t)|$$

est bien défini. Considérons l'ouvert

$$\Omega = \{ s \in \mathbb{C} \mid |s| < R \text{ et } \mathrm{Re}(s) > -\delta \}$$



pour $R > 0$ "grand" et $\delta > 0$ "petit". Par hypothèse, $g(s)$ est holomorphe sur un voisinage de $\{\mathrm{Re}(s) \geq 0\}$ et donc sur un tel Ω.

Notons $\boxed{C = \partial\overline{\Omega}}$.

Par le théorème des résidus de Cauchy,

$$h(0) = \frac{1}{2\pi i} \int_C h(s) \frac{ds}{s}$$

pour toute fonction holomorphe h sur un

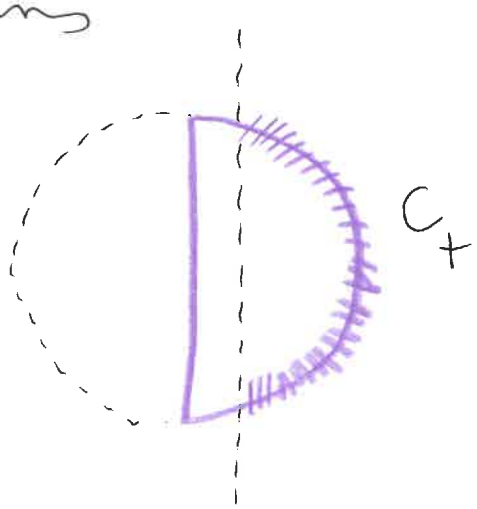
voisinage de C. Appliquons cela à

$$h(z) = (g(s) - g_T(s))\, e^{sT}\left(1 + \frac{s^2}{R^2}\right)$$

dont la valeur en $s=0$ est

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_C (g(s) - g_T(s))\, e^{sT}\left(1 + \frac{s^2}{R^2}\right)\frac{ds}{s}$$

Décomposons



et commençons par estimer l'intégrale lorsque $\mathrm{Re}(s) > 0$. On a :

$$|g(s) - g_T(s)| = \left| \int_T^\infty f(t)\, e^{-st}\, dt \right|$$

$$\leq B \int_T^\infty e^{-\mathrm{Re}(s)t}\, dt$$

$$= B \left[\frac{e^{-\mathrm{Re}(s)t}}{\mathrm{Re}(s)} \right]_T^\infty$$

$$= B\, \frac{e^{-\mathrm{Re}(s)T}}{\mathrm{Re}(s)}$$

Par ailleurs, toujours pour $\mathrm{Re}(s) > 0$ et $|s| = R$,

$$\left| e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{1}{s} \right| = \frac{1}{R}\, e^{\mathrm{Re}(s)\,T} \left| 1+\frac{s^2}{R^2} \right|$$

Or $|s| = R$, on a

$$\left| 1+\frac{s^2}{R^2} \right| = \left| \frac{s}{R} + \frac{R}{s} \right| = 2\,\frac{\mathrm{Re}(s)}{R}$$

Si $s = Re^{i\theta}$, alors

$$\left|\frac{s}{R} + \frac{R}{s}\right| = |2\cos\theta| = 2\cos\theta$$
$$= 2\,\frac{\mathrm{Re}(s)}{R}$$

donc $$\left| e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{1}{s} \right| = 2\,\frac{\mathrm{Re}(s)\, e^{\mathrm{Re}(s)T}}{R^2}$$

On peut donc majorer la contribution de l'intégrale sur C_+ par :

$$\left| \frac{1}{2\pi i} \int_{C_+} \left(g(s) - g_T(s)\right) e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{ds}{s} \right|$$

$$\leq B\, \frac{e^{-\mathrm{Re}(s)T}}{\mathrm{Re}(s)}\, \frac{2\,\mathrm{Re}(s)\, e^{\mathrm{Re}(s)T}}{R^2}\, \frac{1}{2\pi} \int_{C_+} ds$$

C_+ : πR

$$= \frac{B}{R}$$

Soit maintenant C_- la partie [du lacet.

on considère les extensions de $g_T(s)$ et $g(s)$ séparément. Donc

$$0 = \frac{1}{2\pi i} \int_{\text{(semi-cercle)}} g_T(s)\, e^{sT} \left(1 + \frac{s}{R^2}\right) \frac{ds}{s},$$

l'intégrale que l'on voudrait calculer vaut :

$$\frac{1}{2\pi i} \int_{C_-} g_T(s) e^{sT} \left(1 + \frac{s}{R^2}\right) \frac{ds}{s}$$

$$= \frac{1}{2\pi i} \int_{C \cap \{\mathrm{Re}(s) < 0\}} g_T(s) e^{sT} \left(1 + \frac{s}{R^2}\right) \frac{ds}{s}$$

On a dans cette région :

$$|g_T(s)| = \left| \int_0^T f(t) e^{-st}\, dt \right| \leq B \int_0^T e^{-\mathrm{Re}(s)t}\, dt$$

$$\leq B \left[\frac{e^{-\mathrm{Re}(s)t}}{-\mathrm{Re}(s)} \right]_0^T$$

$$\leq B \frac{e^{-\mathrm{Re}(s)T}}{\mathrm{Re}(s)}$$

Sur cette région, l'égalité

$$\left| e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{1}{s}\right| = \frac{2|\mathrm{Re}(s)|}{R^2}\, e^{\mathrm{Re}(s)T}$$

on en déduit :

$$\left|\frac{1}{2\pi i}\int_{C_-} g_T(s)\, e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{ds}{s}\right|$$

$$\leq B\, \frac{e^{-\mathrm{Re}(s)T}}{\mathrm{Re}(s)}\, \frac{2\,\mathrm{Re}(s)}{R^2}\, e^{\mathrm{Re}(s)T}\, \frac{R}{2}$$

$$= \frac{B}{R}$$

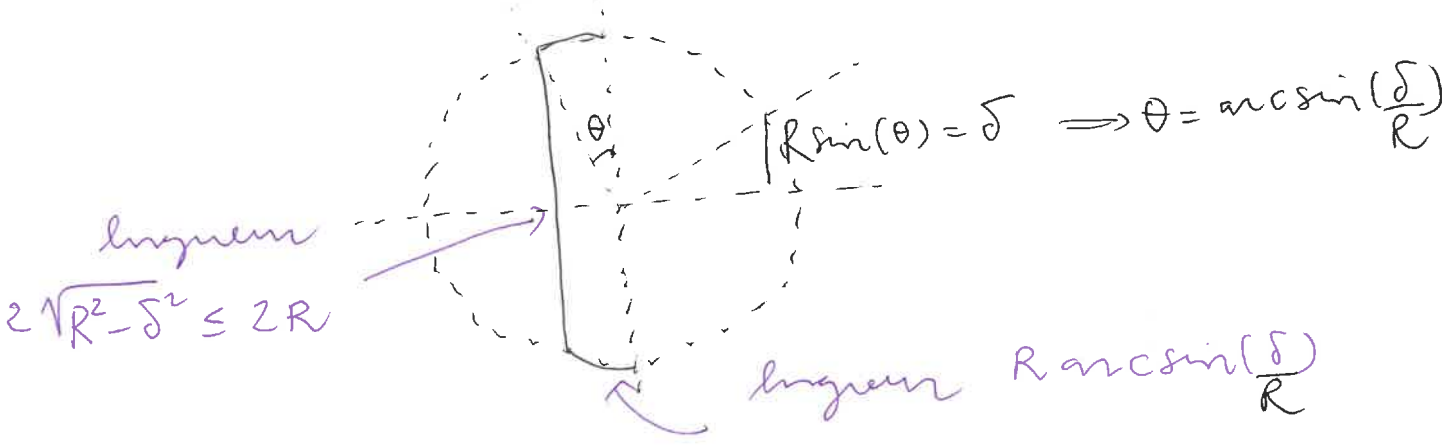
Il reste à majorer l'intégrale

$$\frac{1}{2\pi i}\int_{C_-} g(s)\, e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{ds}{s}$$

Pour ce faire, posons

$$B' = \max_{s\in C_-} \left| g(s)\left(1+\frac{s^2}{R^2}\right)\frac{1}{s}\right|$$

le domaine d'intégration C_- consiste en



et on trouve donc la majoration

$$\left| \frac{1}{2\pi i} \int_C g(s) e^{sT} \left(1 + \frac{s}{R^2}\right) \frac{ds}{s} \right|$$

$$\leq \frac{B' 2R e^{-\delta T}}{2\pi} + B' \frac{2R \arccos(\delta)}{2\pi R}$$

$$\leq \frac{B' R}{\pi} \left(e^{-\delta T} + 2\delta \right)$$

pour δ assez petit

$e^{\mathrm{Re}(s)T} \leq 1$ sur les arcs de cercle

En bout de compte, on trouve :

$$|g(0) - g_T(0)| \leq \frac{B}{R} + \frac{B}{R} + B' \frac{R}{\pi} \left(2\delta + e^{-\delta T}\right)$$

Soit $\varepsilon > 0$. Prenons $R = \frac{2B}{\varepsilon}$ et soit $\delta > 0$ assez petit pour que $\frac{2R\delta B'}{\pi} \leq \varepsilon$. Comme $e^{-\delta T} \longrightarrow 0$ lorsque $T \to +\infty$ et que la fonction $e^{-\delta T}$ est décroissante, il existe T_0 tel que $\frac{RB'}{\pi} e^{-\delta T} < \varepsilon$ pour tout $T \geq T_0$. On a alors :

$$|g(0) - g_T(0)| \leq \varepsilon + \varepsilon + \varepsilon = 3\varepsilon,$$

c'est-à-dire $\lim_{T \to \infty} g_T(0) = g(0)$ □

Remarque : Avec des modifications minimales, la même preuve donne le théorème de la progression arithétique dans sa version la plus forte, c'est-à-dire : la fonction

$$\pi(X;a) = \left\{ p \leq X \;\middle|\; \begin{array}{l} p \text{ premier} \\ p \equiv a \bmod N \end{array} \right\}$$

satisfait à $\pi(X;a) \sim \dfrac{1}{\varphi(N)} \dfrac{X}{\log X}$

lorsque $X \to +\infty$. En effet,

* on introduit $\theta(X;a) = \displaystyle\sum_{\substack{p \leq X \\ p \equiv a}} \log p$

et on montre que

$$\theta(X;a) \sim \frac{X}{\varphi(N)} \Rightarrow \pi(X;a) \sim \frac{1}{\varphi(N)} \frac{X}{\log X}$$

* on montre qu'il suffit d'avoir la convergence de l'intégrale

$$\int_1^\infty \left(\frac{\theta(t;a)}{t^2} - \frac{1}{\varphi(N) t} \right) dt$$

* on déduit la convergence de l'intégrale du théorème de Newman appliqué à

$$\frac{\Phi(s;a)}{s} - \frac{1}{\varphi(N)} \frac{1}{s-1} = \int_1^\infty \left(\theta(t;a) - \frac{1}{\varphi(N) t} \right) \frac{dt}{t^{s+1}}$$

Chapitre 3 : Équirépartition

① Équirépartition modulo 1

Soit $(x_n)_{n\geq 1}$ une suite d'éléments de $[0,1]$.
On dit que $(x_n)_{n\geq 1}$ est équirépartie quand $n\to\infty$ si, pour tout $0\leq a\leq b\leq 1$,

$$\lim_{n\to\infty} \frac{\left|\{k \mid \substack{1\leq k\leq n \\ k\in[a,b]}\}\right|}{n} = b-a.$$

Définition. On dit qu'une suite de nombres réels $(x_n)_{n\geq 1}$ est équirépartie modulo 1 si la suite des parties fractionnaires

$$\{x_n\} = x_n - [x_n] \in [0,1)$$

est équirépartie.

Remarque : Une suite équirépartie est dense.
En effet, pour tout $c\in[0,1]$, soit U_c un intervalle ouvert de longueur $\varepsilon>0$. Alors

$$\lim_{n\to\infty} \frac{\left|\{k \mid \substack{1\leq k\leq n \\ x_k\in U_c}\}\right|}{n} = \varepsilon > 0$$

et donc pour n assez grand il existe $x_n\in U_c$.
La réciproque n'est pas vraie !

Proposition : La suite $(x_n)_{n\geq 1}$ est équirépartie dans $[0,1]$ si et seulement si

$$(*) \quad \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(x_k) = \int_0^1 f(x)\,dx$$

pour toute fonction continue $f : [0,1] \longrightarrow \mathbb{R}$.

Démonstration :

$\boxed{\Rightarrow}$ Soit $f = \mathbb{1}_{[a,b]}$ la fonction indicatrice d'un intervalle $[a,b] \subset [0,1]$. Alors :

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(x_k) = \lim_{n\to\infty} \frac{\left|\left\{k \;\middle|\; \begin{array}{c} 1\leq k\leq n \\ x_k \in [a,b] \end{array}\right\}\right|}{n}$$

$$\int_0^1 f(x)\,dx = b-a$$

donc l'égalité (*) est vraie dans ce cas, ainsi que pour toute combinaison linéaire de fonctions $\mathbb{1}_{[a,b]}$, c'est-à-dire pour les fonctions en escalier.

Soit maintenant $f : [0,1] \longrightarrow \mathbb{R}$ une fonction continue. Pour tout $\varepsilon > 0$, il existe une fonction en escalier g telle que

$$\|f - g\|_\infty \leq \varepsilon.$$

On a alors :

$$\left| \frac{1}{n} \sum_{k=1}^{n} f(x_k) - \int_0^1 f(x)\,dx \right|$$

$$\leq \frac{1}{n} \sum_{k=1}^{n} |f(x_k) - g(x_k)| + \left| \frac{1}{n} \sum g(x_k) - \int_0^1 g\,dx \right|$$

$$+ \int_0^1 |g(x) - f(x)|\,dx$$

$$\leq 3\varepsilon$$

pour n assez grand.

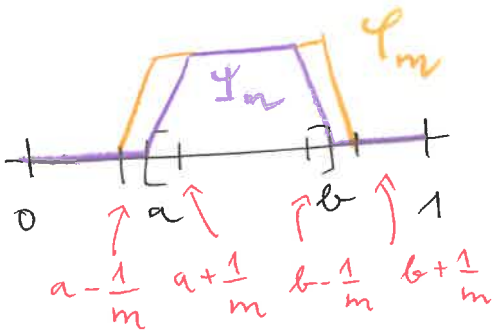
$\Leftarrow$ Soit $[a,b] \subset [0,1]$. On construit des fonctions continues

$$\psi_m \leq \mathbb{1}_{[a,b]} \leq \varphi_m ,$$

de sorte que

$$\frac{1}{n} \sum_{k=1}^{n} \psi_m(x_k) \leq \frac{\#\{k \mid 1 \leq k \leq n,\ x_k \in [a,b]\}}{n}$$

$$\leq \frac{1}{n} \sum_{k=1}^{n} \varphi_m(x_k)$$



et en passant à la limite d'abord quand $n \to \infty$, puis quand $m \to \infty$, on obtient que la suite $(x_n)_{n \geq 1}$ est équirépartie.

□

Remarque: Soit X un espace topologique compact. Plus généralement, on dit qu'une suite $(x_n)_{n\geq 1}$ est équirépartie selon une mesure μ sur X si

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(x_k) = \int_X f \, d\mu$$

pour toute fonction continue $f : X \to \mathbb{C}$. Le cas qu'on regarde est celui de la mesure de Lebesgue et s'appelle parfois équirépartition uniforme.

② Le critère de Weyl

Théorème (Critère de Weyl)

Une suite $(x_n)_{n\geq 1}$ est équirépartie dans $[0,1]$ si et seulement si, pour tout entier z non nul,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2\pi i z x_k} = 0$$

Démonstration

$\boxed{\Longrightarrow}$ Comme $e^{2\pi i z x_k} = \cos(2\pi z x_k) + i \sin(2\pi z x_k)$,

il suffit de démontrer

équirépartition

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \cos(2\pi 2 x_k) \overset{\downarrow}{=} \int_0^1 \cos(2\pi 2x)\, dx$$

$$= \left[\frac{\sin(2\pi 2x)}{2\pi 2} \right]_0^1 = 0$$

et de même pour le sinus.

$\boxed{\Leftarrow}$ La propriété (*) est vraie pour la fonction constante égale à 1 et pour $\cos(2\pi 2x)$ et $\sin(2\pi 2x)$, donc pour tout polynôme trigonométrique

$$q(x) = a_0 + (a_1 \cos(2\pi x) + b_1 \sin(2\pi x)) + \dots + (a_2 \cos(2\pi 2x) + b_2 \sin(2\pi 2x))$$

Or, on sait que toute fonction continue $f : [0,1] \to \mathbb{R}$ est limite uniforme de polynômes trigonométriques et on conclut comme dans la preuve de la proposition. □

Remarque : Dans la situation d'équirépartition plus générale, on voit qu'il suffit de tester l'équirépartition pour une famille de fonctions dont les combinaisons linéaires sont denses

dans les fonctions continues $\mathcal{C}^0(X;\mathbb{C})$.

③ Exemples

Exemple 1 : Soit $\theta \in \mathbb{R}$ un nombre irrationnel. Alors la suite $(n\theta)_{n\geq 1}$ est équirépartie modulo 1. On commence par remarquer que $e^{2\pi i 2n\theta} = e^{2\pi i 2 n\theta}$ et on peut donc travailler avec $n\theta$. Comme θ est irrationnel, 2θ n'est pas un entier, c'est-à-dire $1-e^{2\pi i 2\theta}$ n'est pas nul. Alors :

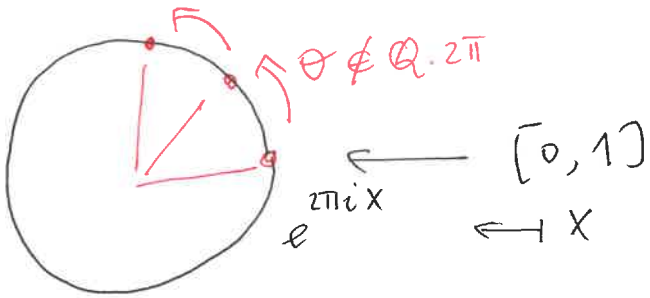
$$\frac{1}{n}\sum_{k=1}^{n} e^{2\pi i 2k\theta} = \frac{1}{n}\sum_{k=1}^{n}\left(e^{2\pi i 2\theta}\right)^k$$

$$= \frac{1}{n}\,\frac{e^{2\pi i 2\theta} - e^{2\pi i 2(n+1)\theta}}{1-e^{2\pi i 2\theta}}$$

d'où

$$\left|\frac{1}{n}\sum_{k=1}^{n} e^{2\pi i 2k\theta}\right| \leq \frac{2}{n}\,\frac{1}{|1-e^{2\pi i 2\theta}|}$$

$\longrightarrow 0$ quand $n\to\infty$



Exemple 2 : La suite $(\{\ln n\})_{n\geq 1}$ est dense dans $[0,1]$ mais non équirépartie.

* Densité : Soit $[a,b] \subset [0,1]$ avec $b > a$. Pour tout s assez grand il existe n avec

$$e^{a+s} \leq n \leq e^{b+s}$$

d'où $a+s \leq \ln n \leq b+s$, c'est-à-dire $\{\ln n\}$ appartient à $[a,b]$.

* Non-équirépartition : On utilise la formule d'Euler-Maclaurin

$$\frac{1}{n}\sum_{k=1}^{n} F(k) = \frac{1}{n}\int_1^n F(t)\,dt + \frac{1}{n}\int_1^n \left(\{t\}-\frac{1}{2}\right)F'(t)\,dt + \frac{F(1)+F(n)}{2n}$$

pour une fonction $F : \mathbb{R} \to \mathbb{C}$ de classe $\mathcal{C}^1$.

(Démonstration :

$$\int_1^n \left(\{t\}-\frac{1}{2}\right)F'(t)\,dt = \sum_{k=1}^{n-1}\int_k^{k+1}\left(t-k-\frac{1}{2}\right)F'(t)\,dt$$

$$= \sum_{k=1}^{n-1} \left((1-\tfrac{1}{2}) F(k+1) - (-\tfrac{1}{2}) F(k) - \int_k^{k+1} F(t)\,dt \right)$$

$u = t-k-\frac{1}{2}$
$v = F(t)$

$$= \frac{1}{2} \sum_{k=1}^{n-1} (F(k)+F(k+1)) - \int_1^n F(t)\,dt$$

$$= \sum_{k=1}^{n-1} F(k) + \frac{F(1)+F(n)}{2} - \int_1^n F(t)\,dt \Big)$$

Appliquons cette formule à $\boxed{F(t) = e^{2\pi i \log(t)}}$

on trouve alors :

$$\frac{1}{n} \sum_{k=1}^{n} e^{2\pi i \log(k)} = \frac{1}{n} \int_1^n e^{2\pi i \log(t)}\,dt + \frac{1+e^{2\pi i \log(n)}}{2n}$$

$$+ \frac{1}{n} \int \left(\{t\} - \frac{1}{2}\right) \frac{2\pi i}{t} e^{2\pi i \log(t)}\,dt$$

$(F'(t) = 2\pi i F(t))$

la dernière terme $\longrightarrow 0$ lorsque $n \to +\infty$.

le troisième terme est majoré par

$$\frac{2\pi}{n} \int_1^n \frac{1}{2} \frac{dt}{t} = \pi \frac{\log(n)}{n} \longrightarrow 0 \quad (n \to +\infty)$$

Par contre, le premier terme vaut

$$\frac{1}{n}\int_1^n e^{2\pi i \log(t)}\,dt = \frac{1}{n}\left[\frac{e^{(2\pi i+1)\log(t)}}{2\pi i+1}\right]_1^n$$

$$= \frac{e^{2\pi i \log(n)} - 1/n}{2\pi i + 1}$$

qui ne tend pas vers 0 lorsque $n \to +\infty$. Le critère de Weyl est donc non défini pour $x=1$.

(4) Équirépartition des angles des premiers de Gauss

Théorème (Fermat) Tout nombre premier p tel que $p \equiv 1 \bmod 4$ est somme de deux carrés. De plus, la représentation

$$p = a^2 + b^2$$

est unique si $a > b > 0$.

On en déduit que le nombre complexe $a+bi$ s'écrit de manière unique comme

$$a+bi = \sqrt{p}\, e^{i\theta_p} \quad \text{avec } \theta_p \in (0, \tfrac{\pi}{4}).$$

Théorème (Hecke) La suite $(\theta_p)_p$ est équirépartie : si p_n désigne le n-ième nombre premier tel que $p_n \equiv 1 \bmod 4$, alors

$$\lim_{n\to\infty} \frac{1}{n} \left| \{ k \le n \mid \theta_{p_k} \in [a,b] \} \right| = \frac{4}{\pi}(b-a)$$

pour tout $[a,b] \subset [0, \tfrac{\pi}{4}]$.