

COURS 7 (9 février 2024)

⑤ Le théorème de la progression arithmétique

Théorème (Dirichlet, 1837)

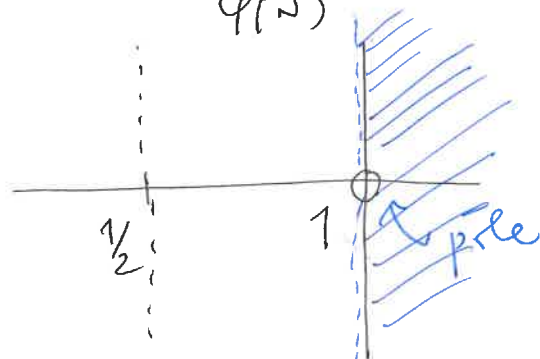
Sont a et N des entiers premiers entre eux. Alors il existe une infinité de nombres premiers de la forme $p \equiv a \pmod{N}$.

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

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

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

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



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

$$\underbrace{-\frac{L'(X, s)}{L(X, s)}}_{\text{fonction n\u00e9gative}} = \sum_p X(p) \frac{\log p}{p^s} + \underbrace{\sum_p X(p)^2 \frac{\log p}{p^s(p^s - X(p))}}_{\Psi(X, s)}$$

* pour $X \neq \mathbb{1}$ n'a pas de p\u00e2le dans un voisinage ouvert de $\{\operatorname{Re}(s) \geq 1\}$ | * pour $X = \mathbb{1}$, p\u00e2le simple de r\u00e9sidu \u00e9gal \u00e0 1.

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

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

$\uparrow$
 simple
 sur $\operatorname{Re}(s) > \frac{1}{2}$

$\therefore \sum_p X(p) \frac{\log p}{p^s}$ d\u00e9finit une fonction n\u00e9gative dans $\{\operatorname{Re}(s) > \frac{1}{2}\}$, sans p\u00e2le au voisinage de $\{\operatorname{Re}(s) \geq 1\}$ sauf en $s=1$ si $X = \mathbb{1}$.

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

$$- \sum_x \frac{L'(x, s)}{L(x, s)} X(a)^{-1} = \sum_p \left(\sum_x \frac{X(p) X(a)^{-1}}{p^s} \right) + \sum_x \Psi(x, s) X(a)^{-1}$$

→ somme sur tous les caractères de Dirichlet modulo N

D'ailleurs,

$$\sum_x X(p) X(a)^{-1} = \sum_x X(p^b) = \begin{cases} 0 & p^b \not\equiv 1 \\ \varphi(N) & p^b \equiv 1 \end{cases}$$

↑ inverse de a modulo N

et comme $p^b \equiv 1 \pmod{N}$ équivaut à $p \equiv a \pmod{N}$,

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

Par conséquent,

$$\Phi(s; a) = \frac{1}{\varphi(N)} \left(- \sum_x \frac{L'(x, s)}{L(x, s)} X(a)^{-1} - \dots \right)$$

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

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

⑥ le théorème des nombres premiers

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

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

Pour tout nombre réel $X > 0$, posons

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

lemme: Si $\theta(X) \sim X$ large $X \rightarrow +\infty$, alors

$$\pi(X) \sim \frac{X}{\log X} \text{ large } X \rightarrow +\infty.$$

(3)

Preuve: Par définition,

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

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

Pour tout $0 < \varepsilon < 1$,

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

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

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

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

mettant les deux estimées ensemble:

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

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

$\downarrow X \rightarrow +\infty$
 0

pour $\varepsilon \rightarrow 0$ □

lemme: Supposons que l'intégrale

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

converge. Alors $\theta(X) \sim X$ lorsque $X \rightarrow +\infty$.

preuve: Soit X 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

$$\geq \int_X^{\lambda X} \frac{\lambda X - t}{t^2} dt$$

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

$$\begin{aligned} t &= Xu \\ dt &= X du \\ \frac{\lambda X - Xu}{X^2 u^2} X du & \end{aligned}$$

Si l'intégrale converge, alors pour tout $\varepsilon > 0$,

il existe $\eta \geq 1$ tel que

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

④

(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 :

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

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

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

$$\therefore \lim_{X \rightarrow \infty} \frac{\theta(X)}{X} = 1$$

□

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 :

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

À partir de la formule

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

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

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

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

et en prend les logarithmes

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

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

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

$$\begin{aligned} \theta(X) - \theta(X/2) &\leq \underbrace{\theta(2n) - \theta(n-1)}_{\theta(2n) - \theta(n) + \theta(n) - \theta(n-1)} \\ &\leq 2n \log 2 + \underbrace{\theta(n) - \theta(n-1)}_{\leq \log n \leq n} \\ &\leq n(2 \log 2 + 1) \leq X(2 \log 2 + 1) \end{aligned}$$

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

(l'égalité est aussi triviale satisfaite pour $0 < X < 2$ car $\theta(X) = 0$ dans ce cas). ⑤

pour $X > 1$

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

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

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

□

