Théorème de Dirichlet faible

Léo Gayral

2017-2018

ref : FGN – Oraux X-ENS, Algèbre 1 – p.135

Définition 1. On définit le polynôme cyclotomique Φ_n dont les racines dans $\mathbb{C}[X]$ sont exactement les racines primitives n-ièmes de l'unité. Autrement dit :

$$\Phi_n(X) = \prod_{\substack{1\leq k\leq n\\ k\wedge n=1}} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

On peut vérifier que $\Phi_n \in \mathbb{Z}[X]$, et que $X^n - 1 = \prod_{d/n} \Phi_d$.

Lemme 1. Soient $a \in \mathbb{N}$ et p premier, tels que $p \wedge \Phi_n(a) = p$ mais que $p \wedge \Phi_d(a) = 1$ pour tout diviseur strict d de n. Alors $p \equiv 1[n]$.

Démonstration.
On a $a^n - 1 = \Phi_n(a) \times \prod_{\substack{d/n\\ d\neq n}} \Phi_d(a) \equiv 0[p]$, donc $\overline{a} \in \mathbb{F}_p^*$ inversible ; on pose ω l'exposant de cet élément.

Si d/n est un diviseur strict, alors $\nu_p\left(a^d - 1\right) = \prod_{\substack{d/n\\ d\neq n}} \nu_p\left(\Phi_d(a)\right) = 1$ donc $a^d \not\equiv 1[p]$ et $\omega \neq d$.

On en déduit $\omega = n$. En conséquence, par le théorème de Lagrange sur $\mathbb{F}_p^*$, on en déduit $n/(p-1)$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $p = kn+1 \equiv 1[n]$, d'où le résultat. □

Théorème 1. Soit $n \geq 2$ entier. L'ensemble $P = \{p \text{ premier}, p \equiv 1[n]\}$ est infini.

Démonstration.
Considérons $p_1 \neq \cdots \neq p_r \in P$, et posons $N = n \times \prod_{i=1}^{r} p_i$. Supposons qu'on a q tel que $q \equiv 1[N]$. Dans ce cas, $q \in P$ et $q \notin \{p_1, \ldots, p_r\}$. Par récurrence sur r, P est infini.

Soit $R = \frac{X^N - 1}{\Phi_N}$. Par définition des polynômes cyclotomiques, R et Φ_N n'ont aucune racine complexe en commun. Ces polynômes sont donc premiers entre eux. Par identité de Bezout dans $\mathbb{Q}[X]$, on en déduit $U, V \in \mathbb{Q}[X]$ tels que $UR + V\Phi_N = 1$.

Pour tout polynôme non constant de $\mathbb{C}[X]$, on a $|P(x)| \underset{|x|\to\infty}{\longrightarrow} \infty$. En particulier, comme Φ_N est non constant, on a $|\Phi_N(a)| \geq 2$ pour tout $a \geq a_0 \in N$; $\Phi_n(a)$ admet toujours un facteur premier q. On peut en particulier choisir a de sorte $aU, aV \in \mathbb{Z}[X]$. Dans ce cas, on a $aU(a) \times R(a) + aV(a) \times \Phi_N(a) = a$.

Comme $\Phi_N(a) \equiv 0[q]$, c'est a fortiori vrai pour $X^N - 1$ d'où $a^N \equiv 1[q]$, $a \wedge q = 1$. Il en découle $aU(a) \times R(a) \equiv a[q]$, d'où $R(a) \wedge q = 1$. En particulier, pour tout diviseur strict d de N, on a $\Phi_d(a) \wedge q = 1$.

Par le lemme préliminaire, on en déduit $q \equiv 1[N]$, le résultat voulu. □

Remarque 1. Par d'obscurs arguments de théorie analytique des nombres, on peut montrer le résultat d'équipartition suivant pour $m \wedge n = 1$:

$$\frac{\#\{p \in [\![1, k]\!], p \text{ premier}, p \equiv m[n]\}}{\#\{p \in [\![1, k]\!], p \text{ premier}\}} \underset{k\to\infty}{\longrightarrow} \frac{1}{\varphi(n)}.$$