# Théorème de Dirichlet faible

## Leçons concernées

* **102 :** Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
* **120 :** Anneaux Z/nZ. Applications.
* **121 :** Nombres premiers. Applications.

Nous allons montrer le théorème suivant :

**Théorème.** *Soit $n \geq 2$. Alors il existe une infinité de nombres premiers congrus à 1 modulo $n$.*

Pour ce faire, nous allons utiliser les polynômes cyclotomiques. On appelle $n$-ème polynôme cyclotomique, noté $\phi_n$, le polynôme formé des racines $n$-èmes primitives de l'unité.
Commençons par un lemme sur les polynômes cyclotomiques :

**Lemme.** *On a l'égalité $X^n - 1 = \prod_{d|n} \phi_d(X)$. En conséquence, $\forall n \in \mathbb{N}, \phi_n \in \mathbb{Z}[X]$.*

*Démonstration.* Pour $P$ un polynôme, notons $\mathcal{R}(P)$ l'ensemble de ses racines complexes. On a alors l'égalité $\mathcal{R}(X^n - 1) = \mathcal{R}\left(\prod_{d|n} \phi_d\right)$.

En effet, le sens réciproque étant évident, attardons-nous sur le sens direct. Si $z$ est un complexe tel que $z^n - 1 = 0$, soit alors $d$ son ordre (qui existe et est fini) dans $\mathbb{C}^*$. Alors, puisque $d$ est l'ordre de $z$, on a $d|n$ et alors $z$ est une racine $d$-ème primitive de l'unité, ce qui prouve le sens direct. Or $X^n - 1$ et $\prod_{d|n} \phi_d$ sont des polynômes unitaires, et à racines simples. En effet, si $z$ est une racine commune à $\phi_d$ et $\phi_{d'}$, elle devrait être d'ordre $d$ et d'ordre $d'$ d'où $d = d'$. On a donc l'égalité recherchée.

Le corollaire se prouve par récurrence. Pour $n = 1$ c'est évident. Supposons la propriété vraie jusque $n$, et prouvons-là pour $n + 1$. On utilise la relation que nous venons de démontrer :

$$X^{n+1} - 1 = \left( \prod_{d|n+1, d \neq n+1} \phi_d(X) \right) \phi_{n+1}(X)$$

Le polynôme que nous avons mis entre parenthèse est, par hypothèse de récurrence, un polynôme à coefficients entiers relatifs. Notons $P$ ce polynôme, et réalisons, puisqu'il est unitaire, la division euclidienne de $X^{n+1} - 1$ par $P$ : il existe $Q$ et $R$ des polynômes de $\mathbb{Z}[X]$ tels que $X^{n+1} - 1 = QP + R$ avec $deg(R) < deg(P)$. Ceci donne en particulier l'égalité :

$$(Q - \phi_{n+1}(X)) \prod_{d|n+1, d\neq n+1} \phi_d(X) - R = 0$$

Si jamais $Q \neq \phi_{n+1}$, on aurait, par cette égalité, que $deg(R) \geq deg(P)$ ce qui est absurde par division euclidienne. Donc nécessairement $Q = \phi_{n+1}$ et en particulier, $\phi_{n+1}$ est un polynôme de $\mathbb{Z}[X]$.

□

Prouvons à présent un deuxième lemme utile pour trouver des nombres premiers congrus à $n$ aussi grand que nous voulons :

**Lemme.** *Soit $a$ un entier et soit $p$ un nombre premier diviseur de $\phi_n(a)$ et ne divisant pas les $\phi_d(a)$ pour $d|n$. Alors $p = 1[n]$.*

*Démonstration.* D'après la relation $a^n - 1 = \prod_{d|n} \phi_d(a)$, nous avons par hypothèse $a^n = 1[p]$. Soit alors $\omega$ l'ordre de $a$ dans $\mathbb{F}_p^*$. Si jamais $d < n$, on aurait :

$$a^\omega - 1 = 0 = \prod_{d|\omega} \phi_d(a)$$

Alors, puisque $\mathbb{F}_p$ est intègre, on aurait que l'un des $\phi_d(a)$ est divisible par $p$ ce qui est exclu car on a supposé $\omega < n$. Dans ce cas, nous avons alors $\omega = n$. L'ordre de $a$ dans $\mathbb{F}_p$ est alors $n$, dans un groupe d'ordre $p - 1$. Donc $n$ divise $p - 1$ soit $p = 1[n]$.

□

Prouvons à présent le théorème. Soit $N$ un entier que nous allons supposer $N > n$. Soit $a = 3N!$. On souhaite considérer les facteurs premiers de $\phi_n(a)$. Puisque $N$ et $a$ sont assez grands, une inégalité triangulaire inversée nous permet de voir immédiatement que $|\phi_n(a)| > 1$. Nous pouvons alors considérer $p$ un facteur irréductible de ce nombre.

Montrons que $p > N$. Si ce n'est pas le cas, on aurait $p|a$ puisqu'il apparaît alors dans le produit issue de la factorielle. Donc $p$ divise $\phi_n(a) - \phi_n(0)$, puisque, en soustrayant $\phi_n(0)$, on a tué le coefficient constant d'un polynôme en $a$. Mais $p$ divise aussi $\phi_n(a)$ par hypothèse. Donc au final $p$ divise $\phi_n(0)$ qui vaut 1 en valeur absolue, ce qui est manifestement absurde. Donc $p > N$.

Prouvons maintenant que $p = 1[n]$. Pour cela, on utilise notre lemme. Si jamais $p|\phi_d(a)$ pour $d|n$, $d \neq n$, alors, en écrivant $X^n - 1$, on se rendrait compte que $a$ est une racine double de $X^n - 1$ dans $\mathbb{F}_p$. Mais $X^n - 1$ est premier avec son polynôme dérivé $nX^{n-1}$ car $n$ est non nul dans $\mathbb{F}_p$, puisque $p > N > n$. C'est donc absurde. Donc, d'après le lemme, $p = 1[n]$ ce qu'il fallait démontrer.

**Remarque :** Le théorème de Dirichlet fort dit qu'il existe une infinité de nombres premiers $p$ tels que $p = a[n]$ dès que $a \wedge n = 1$, pour $a$ entier naturel non nul. Cependant, sa preuve est beaucoup plus difficile et longue (au point qu'elle soit quasiment impossible à faire en développement), et très différente de la preuve que nous venons de faire.