# 1 Théorème de la progression arithmétique de Dirichlet

On va présenter dans cette sous-partie un cas particulier du théorème de Dirichlet.
Pour ce faire, on prouvera avant quelques propriétés des polynômes cyclotomiques.

## 1.1 Polynômes cyclotomiques

**Définition 1** *Pour $n \in \mathbb{N}^*$, on appelle* $n$-ième polynôme cyclotomique, *que l'on note* $\Phi_n$,

$$\Phi_n = \prod_{\substack{0\leq k\leq n \\ k\wedge n=1}} \left(X - e^{2ik\pi/n}\right) = \prod_{z\in\mathbb{C}^* \ / \ \omega(z)=n} (X-z).$$

**Proposition 1**

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

*Démonstration :*

$$X^n - 1 = \prod_{z\in\mathbb{C}^* \ / \ z^n=1} (X-z) = \prod_{d|n} \left( \prod_{z\in\mathbb{C}^* \ / \ \omega(z)=d} (X-z) \right) = \prod_{d|n} \Phi_d.$$

■

**Proposition 2** $\Phi_n \in \mathbb{Z}[X]$. *En particulier, le terme constant de* $\Phi_n$, *qui est le produit de ses racines, au signe près, vaut* $\pm 1$.

*Démonstration :* On raisonne par récurrence sur $n$.
$\underline{n=1}$ : c'est clair car $\Phi_1 = X - 1$.
$\underline{HR_{n-1} \Longrightarrow HR_n}$ : D'après la proposition précédente, on peut écrire $\Phi_n = \frac{X^n-1}{\prod_{d|n,\, d<n} \Phi_d}$. Il suffit alors de repenser au fait qu'une division euclidienne existe lorsque le diviseur est à coefficient dominant valant 1. ■

## 1.2 Un cas particulier du théorème de Dirichlet

Dans la suite, on choisit $n \geq 2$ et on note $\mathcal{P}_n = \{p \in \mathcal{P} \ / \ p \equiv 1\,[n]\}$. On cherche en fait à montrer que $\mathcal{P}_n$ est infini.

**Lemme 1** *Soient $p \in \mathcal{P}$ et $n \geq 2$ premier avec $p$. S'il existe $q \in \mathbb{Z}$ tel que $p \mid \Phi_n(q)$, alors $p \in \mathcal{P}_n$.*

*Démonstration :* Sachant que $X^n - 1 = \prod_{d|n} \Phi_d$, $\chi_p(q)$ est un élément de $\mathbb{F}_p^*$ d'ordre divisant $n$. Supposons cet ordre, noté $m$ strictement inférieur à $n$. Alors, comme $m$ divise $n$, d'après l'égalité précédente, on a $(X^m-1)\Phi_n \mid (X^n-1)$ ; cela voudrait dire que $X^n - 1$ a une racine double. Or, $p \wedge n = 1$ et donc $dP \neq 0$ ; c'est donc absurde. Donc l'ordre de $\chi_p(q)$ dans $(\mathbb{F}_p^*, \times)$ est $n$. Le théorème de Lagrange assure que $n \mid (p-1)$. ■

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

*Démonstration :* Raisonnons par l'absurde et supposons $\mathcal{P}_n$ fini. Posons $q = n \prod_{p\in\mathcal{P}_n} p \geq 2$. La factorisation de $\Phi_n$ sur $\mathbb{C}$ montre que $|\Phi_n(q)| > 1$. Soit alors $p_0$ un diviseur premier de $\Phi_n(q)$. Puisque le terme constant de $\Phi_n$ vaut $\pm 1$, on a $\Phi_n(q) \wedge q = 1$. Donc $p_0$ est premier avec $q$. Donc : $p_0 \notin \mathcal{P}_n$ et $p_0 \wedge n$. Le lemme précédent assure alors que $p_0 \in \mathcal{P}_n$. C'est absurde. ■