Références : R. Francinou, H. Gianella, S. Nicolas, Oraux X-ENS.
Leçons : 109 Anneaux Z/nZ. Applications. 110 Nombres premiers. Applications. 111 Anneaux principaux. Applications. 113 Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications. 116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Théorème de la progression arithmétique de Dirichlet (1838)
Pour tous les entiers naturels non nuls n et m premiers entre eux, il existe une infinité de nombres premiers de la forme $m + \lambda n$, où λ est un entier naturel non nul.
Il n'existe pas de démonstration élémentaire de ce théoréme. Toute démonstration utilise la théorie analytique des nombres.

DÉVELOPEMENT : Une preuve de la version faible du théorème de la progression arithmétique de Dirichlet :
Pour tout entier $n \geq 1$, il existe une infinité de nombres premiers de la forme $1 + \lambda n$, où λ est un entier strictément positif.

La preuve est divisée en deux parties :

PARTIE I : *Soit $n \geq 1$ un entier. Alors il existe un nombre premier p et un entier a tels que :*

1. *p divise $a^n - 1$;*
2. *pour tout diviseur d de n, $d \neq n$, p ne divise pas $a^d - 1$.*

Pour la preuve on utilise les propriétés suivantes des polynômes cyclotomiques $\Phi_m, m \in \mathbb{N}^*$, :

1. $X^n - 1 = \prod_{d|n} \Phi_d$, $\deg \Phi_n = \varphi(n)$ (fonction d'Euler).
2. $\Phi_n \in \mathbb{Z}[X]$.
3. Si $m \neq n$ alors Φ_m et Φ_n sont premiers entre eux dans $\mathbb{Q}[X]$.

Preuve de la partie I. : Notons $B(X) = \prod_{d|n, d\neq n} \Phi_d$

1. Montrer que Φ_n et B sont premiers entre eux (dans $\mathbb{Q}[X]$).
2. En déduire qu'il existe $U, V \in \mathbb{Z}[X]$ et un entier non nul a, tels que
$$a = U(X)\Phi_n(X) + V(X)B(X).$$
De plus, montrer qu'on peut choisir a tel que $\Phi_n(a) \neq 0$ et $\Phi_n(a) \neq \pm 1$.
3. Soit p un nombre premier divisant $\Phi_n(a)$. Montrer que p et a satisfont l'enoncé de la partie I.

PARTIE II :

1. Soit $n \geq 1$ un entier. Alors il existe un nombre premier p et un élément d'ordre n dans $(\mathbb{Z}p\mathbb{Z})^*$.
2. Soit $n \geq 1$ un entier. Montrer qu'il existe un nombre premier p de la forme $1+\lambda n$, $\lambda \in \mathbb{N}^*$.
3. Déduire de 2. (pour tout n) la version faible du théorème de la progression arithmétique de Dirichlet.

POLYNÔMES CYCLOTOMIQUES :

Définition :

$$\Phi_n(X) = \prod_{\zeta} (X - \zeta)$$

où ζ parcours les racines primitives n-ièmes de l'unité dans $\mathbb{C}$.

1. Calculer $\Phi_n(X)$ pour $n = 1, 2, 3, 4, 6, 8$.
2. Calculer $\Phi_p(X)$ pour p premier.
3. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$, et que $\deg \Phi_n = \varphi(n)$ (fonction d'Euler).
4. Montrer que $\Phi_n \in \mathbb{Z}[X]$.
   Indice : récurrence sur n.
5. Si $m \neq n$ alors Φ_m et Φ_n sont premiers entre eux dans $\mathbb{Q}[X]$.
6. Montrer que pour tout nombre premier p, $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.
   Indice : critère d'Eisenstein.

REMARQUE : Pour tout n, Φ_n est irréductible dans $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$). Pour la preuve, qui utilise la réduction modulo un nombre premier, voir X. Goudron Algèbre, ou M. Demazure Cours d'Algèbre.

QUESTION BONUS :
Les coefficients de Φ_n sont-ils toujours égaux à 0, 1 ou -1 ?