TD ∗ ALGÈBRE MODULAIRE

1 CNS pour que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ soit cyclique

Soient $a, b \in \mathbb{N}^*$.
Montrer que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique si et seulement si $a \wedge b = 1$.

2 Mines

Soit $n \in \mathbb{N}^*$.

1. Soit H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$. Montrer qu'il existe a divisant n vérifiant $H = \langle \overline{a} \rangle$.
2. Observer que si $d \mid n$, il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d.
3. Justifier que si $d \mid n$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ possède exactement $\varphi(d)$ éléments d'ordre d (avec φ la fonction indicatrice d'Euler).
4. Montrer
$$\sum_{d|n} \varphi(d) = n$$

3 Centrale – X-ENS : polynômes cyclotomiques et version faible du théorème de Dirichlet

Soit $n \in \mathbb{N}^*$, $\varphi(n)$ l'indicatrice d'Euler de n, $\mathbb{U}_n$ l'ensemble des racines n^{e} de l'unité et $\mathbb{U}_n^*$ l'ensemble des racines de l'unité d'ordre exactement n. Enfin, pour $d \in \mathbb{N}^*$, on pose
$$\Phi_d = \prod_{z \in \mathbb{U}_d^*} (X - z)$$

1. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$.
2. Justifier que $\sum_{d|n} \varphi(d) = n$.
3. Montrer que Φ_n est un polynôme à coefficients entiers.
4. **Application**
   (a) Que peut-on dire d'un nombre premier p qui divise $\Phi_n(a)$ où $a \in \mathbb{Z}$, mais aucun des $\Phi_d(a)$ pour d diviseur strict de n ?
   (b) En déduire que pour $n \geqslant 1$ fixé, il existe une infinité de nombres premiers de la forme $kn+1$ avec $k \in \mathbb{N}$.

4 Cyclicité du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$

Soit p un nombre premier.

1. Soit q un nombre premier qui divise $p-1$.
   Établir l'existence d'un élément de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre multiplicatif q.
   On pourra s'intéresser au polynôme $X^{\frac{p-1}{q}} - 1 \in \mathbb{F}_p[X]$.
2. Soit q un nombre premier et $\alpha \in \mathbb{N}^*$ tel que q^α divise $p-1$.
   Montrer l'existence d'un élément de $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ d'ordre q^α.
3. En déduire que $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique.