

Devoir libre - AL2

L'objectif de ce devoir est de s'entraîner à rédiger soigneusement et de démontrer le théorème suivant :

Théorème 1. Soit p un nombre premier. On a l'isomorphisme de groupes :

$$((\mathbb{Z}/p\mathbb{Z})^\times, \times) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

On commence par démontrer un lemme.

Lemme 2. On note $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ l'indicatrice d'Euler, c'est-à-dire la fonction définie par

$$\varphi(n) = |\{k \in \llbracket 1, n \rrbracket, k \wedge n = 1\}|.$$

Alors pour tout entier $n \in \mathbb{N}^*$, on a

$$n = \sum_{d|n} \varphi(d).$$

Pour $n \in \mathbb{N}^*$ et d un diviseur de n , on note

$$Z_d := \{k \in \mathbb{Z}/n\mathbb{Z}, o(k) = d\}.$$

Soit G_d le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par l'élément $\frac{n}{d}$.

Question 1 - a : Montrer que $Z_d \subset G_d$.

Question 1 - b : En déduire que le cardinal de Z_d vaut $\varphi(d)$.

Question 1 - c : En déduire le lemme (*on pourra penser à utiliser le théorème de Lagrange*).

Question 2 : Soit p un nombre premier et d un diviseur de $p-1$. Soit $x \in ((\mathbb{Z}/(p\mathbb{Z}))^\times, \times)$ un élément d'ordre (multiplicatif) d . On note $H = \langle x \rangle$ le sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ engendré par x . Justifier soigneusement que tout élément d'ordre d appartient à H , puis que le groupe $(\mathbb{Z}/(p\mathbb{Z}))^\times$ admet exactement $\varphi(d)$ éléments d'ordre d .

Question 3 : Démontrer le théorème à l'aide des deux questions précédentes.

Remarque 3. Plus généralement, le résultat reste vrai pour n'importe quel corps fini :

$$\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z},$$

où q est de la forme p^n avec p premier. La démonstration est exactement la même.