Niveau : 1 **Jaune**

La fonction d'Euler

1 Définition de la Fonction indicatrice d'Euler

Soit n un entier > 1. On sait que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier. Dans ce cas, tout élément sauf 0 est inversible, c'est-à-dire que si on note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversible (qui est un groupe multiplicatif), on a :

$$(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}.$$

Pour un n général, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont représentés par les entiers $1 \leq k < n$ tels que k et n soient premiers entre eux.

Notons $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Nous noterons $\Phi(n)$ le nombre des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$. On posera en outre $\Phi(1) = 1$. La fonction Φ est appelée **fonction indicatrice d'Euler**.

2 Les propriétés de la fonction d'Euler

Voici quelques propriétés importantes de la fonction d'Euler, dont les démonstrations sont laissées en exercice.

Lemme 2.1 *Si p est un nombre premier alors :*

$$\Phi(p) = p - 1.$$

Lemme 2.2 *Si p est un nombre premier et α un entier ≥ 1 alors :*

$$\Phi(p^\alpha) = (p-1)p^{\alpha-1}.$$

Lemme 2.3 *Si m et n sont premiers entre eux alors :*

$$\Phi(mn) = \Phi(m)\Phi(n).$$

Théorème 2.4 *Pour tout $n > 1$ la fonction $\phi(n)$ s'exprime sous la forme :*

$$\Phi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right),$$

où les p_i sont les facteurs premiers de n.

Théorème 2.5 *Soit a un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ (c'est-à-dire a premier avec n) alors :*

$$a^{\Phi(n)} \equiv 1 \quad (n).$$

Théorème 2.6 *Pour tout entier $n \geq 1$ on peut écrire n sous la forme suivante :*

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

Preuve. On note :

$$D = \left\{ \frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n} \right\},$$

et pour tout d divisant n on définit :

$$D_d = \left\{ \frac{k}{d} \mid \text{pgcd}(k, d) = 1 \; et \; 1 \leq k \leq d \right\}.$$

De l'existence et l'unicité de l'écriture d'un nombre rationnel sous forme d'une fraction irréductible on déduit que les D_d forment une partition de D. La formule souhaitée découle alors des égalités :

$$\sharp D = \sum_{d|n} \sharp D_d \quad \text{et} \quad \sharp D_d = \Phi(d).$$

□