Niveau : 1 **Jaune**

Éléments primitifs de Z/pZ (p premier)

1 Rappels sur $\mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier. Nous savons que l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est dans ce cas un corps. C'est-à-dire que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Rappelons que l'inverse se calcule facilement par l'algorithme d'Euclide étendu.

Théorème 1.1 *Soit n un entier ≥ 2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si p est premier.*

Rappelons aussi le petit théorème de Fermat :

Théorème 1.2 *Si a est premier avec p alors :*

$$a^{p-1} \equiv 1 \quad (p)$$

Si on décrit les classes de $\mathbb{Z}/p\mathbb{Z}$ par leur représentant appartenant à l'intervalle d'entiers :

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \cdots, p-1\}$$

alors on voit que tout élément non nul $a \in \mathbb{Z}/p\mathbb{Z}$ vérifie $a^{p-1} = 1$. Le petit théorème de Fermat implique la remarque suivante :

lorsqu'on travaille modulo p sur des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$, alors on travaille modulo $p-1$ sur leurs exposants

2 Le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$

2.1 Les éléments générateurs

Nous avons donc vu que lorsque p est premier, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est égal à $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Ce groupe est cyclique, plus précisément :

Théorème 2.1 *Soit p un nombre premier. Alors, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique. C'est-à-dire que ce groupe peut être engendré par un un élément générateur (dit aussi élément primitif) : il existe un élément α tel que*

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{p-2}\}.$$

Théorème 2.2 *Le nombre de générateurs de $\mathbb{Z}/p\mathbb{Z}^*$ est égal à $\Phi(p-1)$ où Φ est la fonction indicatrice d'Euler.*

2.2 Ordre d'un élément

Soit un élément $\beta \in \mathbb{Z}/p\mathbb{Z}^*$. L'ordre de β est le plus petit exposant $e > 0$ tel que $\beta^e = 1$. L'ordre d'un élément générateur est évidemment $p - 1$.

Théorème 2.3 *Pour que e soit l'ordre d'un élément il faut et il suffit que e divise $p - 1$.*

Théorème 2.4 *Si e divise $p - 1$ alors il y a exactement $\Phi(e)$ éléments d'ordre e.*

2.3 Construction d'un élément générateur

Dans un premier temps, il faudrait pouvoir tester si un élément est générateur (c'est-à-dire d'ordre $p-1$). Pour cela on ne connaît pas actuellement d'autre moyen que de faire intervenir la factorisation de $p - 1$ en nombres premiers :

$$p - 1 = \prod_{i=1}^{k} p_i^{n_i}.$$

Théorème 2.5 *L'élément α est générateur si et seulement si pour tout $1 \leq i \leq k$ on a :*

$$\alpha^{\frac{p-1}{p_i}} \neq 1.$$

Encore faut-il savoir factoriser $p - 1$. On voit donc que ceci ne permet pas de tester en pratique si un élément est générateur dans le cas où p **est grand**, à moins de connaître à priori la factorisation de $p - 1$. La construction d'un élément générateur lorsque p est grand ne se fait donc pas indépendamment de la construction du nombre premier p lui-même. Nous verrons dans la fiche "constructions de nombres premiers" comment procéder en pratique.