TD 6 – Morphismes (suite)

Exercice 1. *Anneau $\mathbb{Q}^{(m)}$*

Soit $m \in \mathbb{Z}_{>0}$ et $\mathbb{Q}^{(m)}$ l'ensemble des nombres rationnels a/b où $\text{PGCD}(b, m) = 1$.

1. Montrer que $\mathbb{Q}^{(m)}$ est un anneau, inclus dans $\mathbb{Q}$.
2. Caractériser les inversibles de $\mathbb{Q}^{(m)}$.
3. On définit $\Phi : \mathbb{Q}^{(m)} \to \mathbb{Z}/m\mathbb{Z}$ par $\Phi(a/b) = [a]_m[b]_m^{-1}$.
   - **i.** Montrer que Φ est bien définie, *c'est-à-dire que si $a/b = c/d$, alors* $[a]_m[b]_m^{-1} = [c]_m[d]_m^{-1}$.
   - **ii.** Montrer que Φ est un morphisme d'anneaux.
   - **iii.** Calculer l'image et le noyau de Φ.

Exercice 2. *Ordre d'éléments*

Soit G un groupe (multiplicatif) cyclique fini, $\alpha \in G$ et H le sous-groupe engendré par α. Soit $\rho : \mathbb{Z} \to H$ définie par $\rho(n) = \alpha^n$.

1. Montrer que ρ est un morphisme de groupes.
2. Montrer que ρ est surjective.
3. En déduire que $H \simeq \mathbb{Z}/n\mathbb{Z}$ où n est l'ordre de α.
4. Montrer que $\alpha^k = \alpha^\ell$ si et seulement si n divise $\ell - k$.

Exercice 3. *Aperçu de l'algorithme de Pollig & Hellman (1978)*

Soit G un groupe (multiplicatif) cyclique, généré par γ. Le *logarithme discret* de $\alpha \in G$ en base γ est l'unique entier $n \in \{0, \dots, \#G - 1\}$ tel que $\alpha = \gamma^n$. On le note (parfois) $n = \log_\gamma \alpha$.

1. Montrer qu'on peut calculer $\log_\gamma \alpha$ en $O(\#G)$ opérations dans G.

Remarque : on peut faire mieux, en $O(\sqrt{\#G})$ (cf. TP). L'algorithme de Pollig & Hellman permet lui de réduire ces coûts dans le cas où $\#G$ a de nombreux *petits* facteurs. On présente une partie de cet algorithme.

Dans la suite, on fixe $G = \mathbb{Z}/p\mathbb{Z}^\times$, γ un générateur de $\mathbb{Z}/p\mathbb{Z}^\times$ et $\alpha = \gamma^n$. Étant donné α et γ, on cherche à calculer n. Soit $p - 1 = \prod_{i=1}^k q_i^{e_i}$ la décomposition de $p - 1$ en facteurs premiers. On note, pour tout i, $\gamma_i = \gamma^{(p-1)/q_i^{e_i}}$ et $\alpha_i = \alpha^{(p-1)/q_i^{e_i}}$.

2. - **i.** Montrer que γ_i est d'ordre $q_i^{e_i}$ pour tout i.
   - **ii.** Montrer que α_i appartient au groupe engendré par γ_i.
   - **iii.** Soit $n_i = \log_{\gamma_i} \alpha_i$. Montrer que $0 \leq n_i < q_i^{e_i}$ et $n_i \equiv_{q_i^{e_i}} n$.
3. - **i.** Comment utiliser la question précédente pour concevoir un algorithme de calcul du logarithme discret, si on connaît la factorisation de $p - 1$?
   - **ii.** Estimer la complexité de cet algorithme.