TD 2 – Résolution d'équations modulaires

Exercice 1. *Quelques équations*

1. Résoudre les équations $21z \equiv_{30} 12$ et $14z \equiv_{21} 5$.
2. Résoudre l'équation $z + 4 \equiv_{18} 16z + 13$.
3. Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$\begin{cases} z \equiv_7 1 \\ z \equiv_5 3 \end{cases}, \qquad \begin{cases} z \equiv_2 0 \\ z \equiv_3 1 \\ z \equiv_5 0 \end{cases}.$$

Exercice 2. *Quelques résultats généraux*

1. Soit $a_1, \ldots, a_k$, b et n des entiers, $n > 0$. Montrer que l'équation $a_1 z_1 + \cdots + a_k z_k \equiv_n b$ a une solution si et seulement si $\mathrm{PGCD}(a_1, \ldots, a_k, n)$ divise b.
2. Soit $a \in \mathbb{Z}_{\geq 0}$ et $n_1, \ldots, n_k > a$ des entiers premiers entre eux deux-à-deux. Résoudre le système suivant.

$$\begin{cases} z \equiv_{n_1} a \\ \vdots \\ z \equiv_{n_k} a \end{cases}$$

3. Soit $n_1, n_2 \in \mathbb{Z}_{>0}$, $d = \mathrm{PGCD}(n_1, n_2)$, et $a_1, a_2 \in \mathbb{Z}$. Montrer qu'il existe a tel que $a \equiv_{n_1} a_1$ et $a \equiv_{n_2} a_2$ si et seulement si $a_1 \equiv_d a_2$.

Exercice 3. *Théorème chinois*

Soit $n_1, \ldots, n_k$ des entiers positifs premiers deux-à-deux, et $N = \prod_{i=1}^{k} n_i$. On définit $\theta : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ par $\theta([a]_N) = ([a]_{n_1}, \ldots, [a]_{n_k})$. Pour α, $\beta \in \mathbb{Z}/N\mathbb{Z}$, on note $\theta(\alpha) = (\alpha_1, \ldots, \alpha_k)$ et $\theta(\beta) = (\beta_1, \ldots, \beta_k)$.

1. Montrer que θ est bien définie.
2. Montrer que $\theta(\alpha + \beta) = (\alpha_1 + \beta_1, \ldots, \alpha_k + \beta_k)$ et $\theta(\alpha\beta) = (\alpha_1\beta_1, \ldots, \alpha_k\beta_k)$.
3. Montrer que α est inversible si et seulement si α_i est inversible pour tout i, et que le cas échéant, $\theta(\alpha^{-1}) = (\alpha_1^{-1}, \ldots, \alpha_k^{-1})$.
4. Montrer que pour tout $m \geq 0$, $\theta(\alpha^m) = (\alpha_1^m, \ldots, \alpha_k^m)$.

Exercice 4. *Appliquer la définition*

1. Montrer que $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont des groupes additifs.
2. Montrer que $(\mathbb{R}^*, \times)$ et $(\mathbb{Q}^*, \times)$ sont des groupes multiplicatifs.
3. Montrer que $(\mathbb{N}, +)$, $(\mathbb{Z}, \times)$ et $(\mathbb{R}, \times)$ *ne sont pas* des groupes.
4. Montrer que les couples suivants sont des groupes, et préciser s'ils sont abéliens :
   - **i.** $(n\mathbb{Z}, +)$ où $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$;
   - **ii.** $(\{-1, 1\}, \times)$;
   - **iii.** $(\{0,1\}^n, \otimes)$ (ensemble des mots binaires de longueur n fixée, avec l'opération « ou exclusif bit-à-bit »);
   - **iv.** $(S_n, \circ)$ (ensemble des permutations de $\{1, \ldots, n\}$ avec l'opération de composition).
5. Le couple $(\{0,1\}^\star, \cdot)$ de l'ensemble des mots binaires avec l'opération de concaténation est-il un groupe ?