TD6 – Théorie des nombres et hypothèses cryptographiques

Exercice 1. *Calculs dans $\mathbb{Z}/n\mathbb{Z}$*

1. On considère le groupe $((\mathbb{Z}/21\mathbb{Z})^\times, \times)$.
   - **i.** Quel est l'ordre du groupe ? Lister ses éléments.
   - **ii.** Calculer l'inverse de 11 dans le groupe.
   - **iii.** Calculer (à la main !) 2^{2403} dans le groupe. *Indication.* $x^{|G|} = 1$ *pour tout* $x \in G$.
   - **iv.** Calculer le sous-groupe G_7 engendré par 7.
2. On considère le groupe $((\mathbb{Z}/23\mathbb{Z})^\times, \times)$.
   - **i.** Quel est l'ordre du groupe ? Lister ses éléments.
   - **ii.** Calculer le sous-groupe G_2 engendré par 2.
   - **iii.** Calculer le sous-groupe G_5 engendré par 5. Que remarque-t-on ?

Exercice 2. *Groupes*

1. Soit G un groupe fini. Montrer que pour tout $x \in G$, $G_x = \{x^n : n \geq 0\}$ est un groupe.
2. Calculer $\varphi(p \times q \times r)$ où p, q et r sont des nombres premiers.
3. Calculer $\varphi(p^e)$ où p est un nombre premier.
4. Soit G un groupe abélien, noté multiplicativement.
   - **i.** Montrer qu'il n'existe qu'un seul neutre dans G. *Indication. Supposer qu'il existe deux neutres* e_1 *et* e_2*, écrire la définition de neutre, et en déduire que* $e_1 = e_2$.
   - **ii.** En déduire que pour tout x, il n'existe qu'un seul inverse y tel que $xy = 1$.

Exercice 3. *Test de puissances parfaites*

On souhaite tester si un entier N est une puissance parfaite, c'est-à-dire s'il s'écrit $N = n^e$ pour deux entiers n et $e \geq 2$. Ce test est l'étape initiale dans les algorithmes de tests de primalité.

1. Décrire un algorithme qui, étant donné N et e, détermine s'il existe un entier n tel que $n^e = N$. *Indication : chercher* n *par dichotomie.*
2. Montrer que si $N = n^e$, alors $e \leq \log_2(N)$.
3. En déduire un algorithme polynomial pour tester si N est une puissance parfaite et analyser sa complexité.