Feuille Exercice - Résidus quadratiques et anneaux

1 Résidus quadratiques

Etant donné un groupe G, un élément $y \in G$ est un *résidu quadratique* si il existe $x \in G$ tel que $x^2 = y$. Dans ce cas, on appelle x la *racine carrée* de y.
Dans le cas spécifique de $\mathbb{Z}_p^\times$ où $p \geq 2$ est premier, un élément y est un résidu quadratique s'il existe x tel que $x^2 = y \bmod p$. On appelle $\mathcal{QR}_p$ l'ensemble des résidus quadratiques modulo p, et $\mathcal{QNR}_p$ l'ensemble des éléments qui ne sont pas des résidus quadratiques modulo p.
Soit $x \in \mathbb{Z}_p^\times$, on définit $\mathcal{J}_p(x)$, le *symbole de Jacobi de x modulo p* de la manière suivante :

$$\mathcal{J}_p(x) = \begin{cases} +1 \text{ if } x \text{ est un residu quadratique modulo } p, \\ -1 \text{ if } x \text{ n'est pas un résidu quadratique modulo } p. \end{cases}$$

Exercise 1.
Pour tout l'exercice, on considérera que $p \geq 3$ est un nombre premier.

1. Montrer que $\mathcal{QR}_p$ est un sous-groupe de $(\mathbb{Z}_p^\times, \times)$.
2. Calculer les racines carrées de 3 dans $\mathbb{Z}_{13}^\times$.
3. Montrez que tout résidu quadratique de $\mathbb{Z}_p^\times$ a exactement deux racines.
4. Déterminez l'ensemble des résidus quadratiques de $\mathbb{Z}_{13}^\times$.
5. Combien d'éléments de $\mathbb{Z}_p^\times$ sont des résidus quadratiques ? Combien n'en sont pas ?

On rappelle que $\mathbb{Z}_p^\times$ est un groupe cyclique d'ordre $p-1$, soit g un de ses générateurs, on peut écrire :

$$\mathbb{Z}_p^\times = \{g^0, g^1, g^2, \ldots, g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, g^{\frac{p-1}{2}+1}, \ldots, g^{p-2}\}.$$

Si on met chacun de ces éléments au carré, on obtient :

$$\mathcal{QR}_p = \{g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^2, \ldots, g^{p-3}\},$$

où chaque élément apparaît deux fois.
Les résidus quadratiques s'écrivent donc g^i pour $i \in \{0, 2, \ldots, p-2\}$ pair.

6. Montrez que pour tout $x \in \mathbb{Z}_p^\times$, on a $\mathcal{J}_p(x) = x^{\frac{p-1}{2}} \bmod p$. En déduire un algorithme polynomial pour tester si un élément $x \in \mathbb{Z}_p^\times$ est un résidu quadratique ou non.
7. Montrer que pour tout $x, y \in$, $\mathcal{J}_p(xy) = \mathcal{J}_p(x)\mathcal{J}_p(y)$.
   En déduire que si $x, x' \in \mathcal{QR}_p$ et $y, y' \in \mathcal{QNR}_p$ alors :
   — $xx' \bmod p \in \mathcal{QR}_p$
   — $yy' \bmod p \in \mathcal{QR}_p$
   — $xy' \bmod p \in \mathcal{QNR}_p$

Exercise 2.
Soit $N = pq$ avec p et q deux nombres premiers distincts. On rappelle que $\mathbb{Z}_N^\times$ est isomorphe à $\mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$ et on appelle f l'isomorphisme correspondant, pour tout $y \in \mathbb{Z}_N^\times$, $f(y) = (y_p, y_q)$ tel que $y_p = y \bmod p$ et $y_q = y \bmod q$.
On étend la définition du symbole de Jacobi dans le cas où $N = pq$, pour tout x qui est premier avec N :

$$\mathcal{J}_N(x) = \mathcal{J}_p(x) \cdot \mathcal{J}_q(x).$$

1. Soit $y \in \mathbb{Z}_N^\times$ et $(y_p, y_q) = f(y)$. Montrer que y est un résidu quadratique modulo N si et seulement si y_p est un résidu quadratique modulo p et y_q est un résidu quadratique modulo q.
2. Combien d'éléments de $\mathbb{Z}_N^\times$ sont des résidus quadratiques ?
3. Montrer que si x est un résidu quadratique modulo N, alors $\mathcal{J}_N(x) = +1$. Montrer que l'inverse n'est pas vrai.
4. Soit $\mathcal{J}_N^{+1}$ les éléments de $\mathbb{Z}_N^\times$ dont le symbole de Jacobi est égal à 1. Montrez que :
   — La moitié des éléments de $\mathbb{Z}_N^\times$ sont dans $\mathcal{J}_N^{+1}$.
   — $\mathcal{QR}_N \subseteq \mathcal{J}_N^{+1}$.
   — Exactement la moitié des éléments de $\mathcal{J}_N^{+1}$ sont dans $\mathcal{QR}_N$.

2 Exercices complémentaires sur les anneaux

Exercise 3.

1. Soient A un anneau intègre et $a \in A$ non nul. Montrer que l'application $f_a \colon A \to A$ définie par $f_a(x) = ax$ est injective.
2. En déduire que si A est intègre et de cardinal fini, alors A est un corps (il suffit de trouver un inverse à l'élément a).

Exercise 4.
Soit $(G, +)$ un groupe commutatif. On note $End(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : G \to G, x \mapsto f(x) + g(x)$. Démontrer que $(End(G), +, \circ)$ est un anneau.

Exercise 5.
Résoudre l'équation $x^2 - 4x + 3 = 0$ dans l'anneau $\mathbb{Z}_{21}$ à l'aide du théorème des restes chinois.