Session 2

Exercice 1 (Algebre Abstrait).

1. Rappeler les définitions d'un groupe, un groupe abélien, un anneau et un corps.
2. Combien y a-t-il d'éléments dans l'anneau $\mathcal{R}_{13} = \mathbb{Z}_{13}[X]/(X^4+1)$?
3. Étant donnée $a = 1 + 3X^2 + X^3$ et $b = 9 + 2X + 5X^2 + 6X^3$ dans $\mathcal{R}_{13}$, calculer $a + b$ et $a \cdot b$.
4. Considérer l'anneau $\mathcal{R}_3 = \mathbb{Z}_3[X]/(X^2+1)$. Est-ce un corps ? Justifier la réponse.
5. Considérer l'anneau $\mathcal{R}_3 = \mathbb{Z}_3[X]/(X^2+X+1)$. Est-ce un corps ? Justifier la réponse.
6. Soit l'ensemble des réels qui s'écrivent de la forme $a + b\sqrt{2}$ avec $(a, b) \in \mathbb{Q}^2$. Montrer que cet ensemble forme un corps, noté $\mathbb{Q}(\sqrt{2})$.

Exercice 2 (Algorithme de Shor).
Rappelons l'algorithme de Shor pour le problème de factorisation :

Algorithme 1 : Algorithme de Shor pour FACT

Require: N
Ensure: p, un facteur non trivial de N
1. $a \leftarrow \mathbb{Z}_N$
if $\text{pgcd}(a, N) \neq 1$ **then**
  return $\text{pgcd}(a, N)$
end if
Calcul quantique de la période r de $\text{F}_a(x) = a^x \bmod N$.
if r n'est pas pair ou si $a^{\frac{r}{2}} \equiv -1 \bmod N$ **then**
  GOTO 1.
end if
return $\text{pgcd}(a^{\frac{r}{2}} + 1, N)$

1. Factoriser $N = 21$ avec l'algorithme de Shor, en prenant pour valeurs successives de a : 2, 3 et 5.
2. Le calcul quantique de l'ordre de $a \bmod N$ s'effectue de la façon suivante. Soit $\mathcal{O}_{\text{F}_a}$ l'oracle quantique associé à la fonction F_a, *i.e.*, le circuit quantique de $(k, 1) \mapsto (k, a^k \bmod N)$. Calculer la fonction $\mathcal{O}_{\text{F}_2}$ pour $N = 15$.

Exercice 3 (DLWE $\leq$ SIS).
Montrer que SIS est plus difficile que DLWE, c'est-à-dire DLWE $\leq$ SIS.