Travaux Dirigés 2 : compléments d'algèbre

Exercice 1. Autour des symboles de Legendre et de Jacobi.

1. Calculer $\left(\frac{2}{3}\right), \left(\frac{2}{5}\right), \left(\frac{2}{7}\right), \left(\frac{3}{7}\right), \left(\frac{10}{11}\right)$ en utilisant seulement la définition.
2. Calculer le symbole de Jacobi $\left(\frac{3263}{1003}\right)$.
3. Soient p et q deux nombres premiers impairs distincts. Que vaut $\sum_{k=1}^{p} \left(\frac{k}{p}\right)$? Et $\sum_{k=1}^{pq} \left(\frac{k}{pq}\right)$?

Exercice 2. Racines carrées modulo p

On considère un nombre premier impair p, ainsi qu'un carré non nul a dans $\mathbb{Z}/p\mathbb{Z}$.

1. On suppose dans cette question p congru à 3 modulo 4. Montrer que $a^{\frac{p+1}{4}}$ est une racine carrée de a dans $\mathbb{Z}/p\mathbb{Z}$.

Dans le cas plus difficile où $p = 1 \bmod 4$, on note (s,t) l'unique couple d'entiers avec t impair tel que $p-1 = 2^s t$.

2. Justifier que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z}$.
3. Soit $y \in \mathbb{Z}/p\mathbb{Z}$ un élément qui n'est pas un carré, et $x = y^t$. Montrer que x engendre l'unique sous-groupe de cardinal 2^s de $(\mathbb{Z}/p\mathbb{Z})^\times$, puis qu'il existe un entier pair c tel que $a^t = x^c$.
4. Montrer finalement que $a^{\frac{t+1}{2}} x^{-\frac{c}{2}}$ est une racine carrée de a.
5. Le but de cette question est de calculer l'entier c de proche en proche. Pour cela, on écrit en base 2 : $c = 2c_1 + 4c_2 + \cdots + 2^{s-1}c_{s-1} = \sum_{k=1}^{s-1} c_k 2^k$ où $c_1, \ldots, c_{s-1}$ valent chacun 0 ou 1.
   (a) Justifier que $c_1 = 1$ si et seulement si $(a^t)^{2^{s-2}} = -1$.
   (b) On suppose $c_1, \ldots, c_i$ connus pour un certain $i \in [\![1, s-2]\!]$. Comment retrouver la valeur de c_{i+1} à partir du calcul de $\left(a^t x^{-2c_1 - \cdots - 2^i c_i}\right)^{2^{s-i-2}}$?
   (c) En déduire une méthode pour calculer c.
6. Calculer la racine carrée de 2 mod 97. On pourra remarquer que 5 n'est pas un carré modulo 97.

Exercice 3. Pile ou face à distance

Le problème de la résiduosité quadratique permet de construire un protocole de pile ou face à distance entre deux participants Alice et Bob :

— (Mise en place) Alice choisit un nombre impair $n = pq$, avec p, q deux nombres premiers distincts, et tel que $\left(\frac{-1}{n}\right) = 1$ et le transmet à Bob.
— Bob choisit $x \in \mathbb{Z}/n\mathbb{Z}$ et transmet $c = x^2$ à Alice.
— Alice doit deviner le symbole de Jacobi de x ; elle envoie $\epsilon = 1$ ou -1 à Bob.
— Bob dévoile x ; Alice vérifie que $x^2 = c$.
— Alice gagne si $\left(\frac{x}{n}\right) = \epsilon$ ou 0, et perd sinon.

On peut rejouer en recommençant à la deuxième étape.

Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$, on note a' l'unique élément de $\mathbb{Z}/n\mathbb{Z}$ tel que $a' = a \bmod p$ et $a' = -a \bmod q$.

1. Montrer que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, les seuls éléments de $\mathbb{Z}/n\mathbb{Z}$ dont le carré vaut x^2 sont x, x', $-x$ et $-x'$.
2. Montrer que si Bob connaît dans $\mathbb{Z}/n\mathbb{Z}$ deux éléments x_1 et x_2 tels que $x_1^2 = x_2^2 = c$ et $x_1 \neq \pm x_2$, alors il peut facilement trouver un facteur non trivial de n.

On suppose désormais que p et q sont deux grands nombres premiers, de telle sorte que l'entier n est impossible à factoriser en pratique.

3. Pourquoi faut-il que $\left(\frac{-1}{n}\right) = 1$?
4. Alice, elle, connaît la factorisation de n ; cela lui permet de calculer les quatre racines carrées de c dans $\mathbb{Z}/n\mathbb{Z}$.
   Montrer que cette information lui permet de gagner à tous les coups si $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = 1$.
5. En déduire qu'Alice ne peut pas tricher si p et q sont congrus à 3 mod 4.
6. Bob peut-il vérifier que cette condition est satisfaite ? Le cas échéant, proposer une modification du protocole permettant à Bob de s'assurer qu'Alice n'a pas triché dans le choix de n.