# Feuille de TD 2

## Résidus quadratiques

**Exercice 1 (Quelques applications de la loi de réciprocité quadratique).**
Soit $p$ un nombre premier.

(1) Calculer le symbole de Legendre $(\frac{754}{7})$.

(2) Calculer le symbole de Jacobi $(\frac{254}{1003})$.

(3) Supposons $p$ différent de 2 et 3. Montrer que 3 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \pmod{12}$.

(4) Montrer qu'un résidu quadratique modulo $p$ n'est pas un générateur de $\mathbb{F}_p^*$.

(5) Soit $a \in \mathbb{Z}$. Montrer que si $(\frac{a}{n}) = -1$, alors $a$ n'est pas un carré modulo $n$. Est-ce que la réciproque est vraie ?

(6) Supposons $p$ différent de 5. Trouver une condition nécessaire et suffisante portant sur le dernier chiffre décimal de $p$ pour que 5 soit un carré dans $\mathbb{F}_p$.

**Exercice 2.** Soit $p$ un nombre premier impair et soit $n$ le plus petit entier naturel non nul qui n'est pas un carré modulo $p$. Montrer qu'alors $n < 1 + \sqrt{p}$.

**Exercice 3 (Carrés dans $\mathbb{Z}/p^r\mathbb{Z}$).** Soit $p$ un premier impair et soit $r \in \mathbb{N}^*$.

(1) Soit $a$ un entier non divisible par $p$. Montrer que si $a$ est un résidu quadratique modulo $p^r$, alors $a$ l'est aussi modulo $p^{2r}$.

(2) Soit $a$ un entier non divisible par $p$. Montrer que le nombre de racines carrées de $a$ modulo $p^r$ est $1 + \left(\frac{a}{p}\right)$.

(3) Soit $a$ un entier impair. Pour $r \geqslant 3$, montrer que le nombre de racines carrées de $a$ modulo $2^r$ vaut 4 si $a \equiv 1 \mod 8$ et 0 sinon. Que vaut-il pour $r < 3$ ?

(4) Soit $n$ entier et soit $a$ premier avec $n$. Déduire des questions précédentes une condition nécessaire et suffisante pour que $a$ soit un carré modulo $n$. Donner une formule pour le nombre de racines carrées de $a$ modulo $n$.

**Exercice 4 (Détermination d'une racine carrée dans $\mathbb{F}_p$).** Soit $p$ un premier impair et soit $a$ un carré non nul modulo $p$. On chercher à calculer les racines carrées de $a$ dans $\mathbb{F}_p$.

(1) Justifier que $a$ admet exactement 2 racines carrées.

(2) Montrer que s'il existe un entier impair $k$ tel que $a^k \equiv 1 \mod p$, alors les racines carrées de $a$ sont données par $\pm a^{\frac{k+1}{2}}$.

(3) En déduire les racines carrées de $a$ pour $p \equiv 3 \mod 4$.
Supposons maintenant que $p \equiv 1 \mod 4$. On écrit $p = 1 + 2^e s$ avec $s$ impair et $e \geqslant 2$.

(4) Montrer que s'il existe $c$ tel que $c^2 a^s \equiv 1 \mod p$, alors les racines carrées de $a$ sont données par $\pm c a^{\frac{s+1}{2}}$.
On montre à présent l'existence d'un tel $c$. Pour cela, on considère la partie 2-primaire $G$ de $\mathbb{F}_p^*$, i.e. le sous-groupe formé des éléments d'ordre une puissance de 2. Ainsi $G$ est cyclique d'ordre $2^e$. Soit $z$ un générateur de $G$.

(5) Montrer que $a^s \in G$ et que $a^s$ est un carré dans $G$. En déduire une expression des racines carrées de $a$.

On cherche maintenant une méthode algorithmique pour déterminer un élément $c$ tel que $c^2 a^s \equiv 1 \mod p$. Soit $u$ un élément qui n'est *pas* un carré modulo $p$. Soit $\ell$ le plus petit entier positif tel que $(a^s)^{2^\ell} = 1 \mod p$ et supposons $\ell \geqslant 1$. Posons $v_1 = (u^s)^{2^{e-\ell-1}}$ et soit $\ell_1$ le plus entier positif tel que $(v^2 a^s)^{2^{\ell_1}} = 1$.

(6) Montrer qu'on a toujours $\ell_1 < \ell$. Que peut-on dire si $\ell_1 = 0$ ?

(7) Si $\ell_1 \neq 0$, trouver un élément $v_2$ tel que $((v_2 v_1)^2 a^s)^{2^{\ell_1 - 1}} \equiv 1 \mod p$.

(8) Plus généralement, donner un algorithme permettant de construire $c$ tel que $c^2 a^s \equiv 1 \mod p$.

(9) Utiliser cette méthode pour déterminer les racines carrées de 5 dans $\mathbb{Z}/41\mathbb{Z}$.

## Quelques algorithmes

**Exercice 5.** (1) Écrire l'algorithme d'Euclide étendu et prouver qu'il calcule bien une relation de Bézout.

(2) On considère la suite de Fibonacci donnée par $F_0 = 0, F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$. Soient $a$ et $b$ des entiers tels que $a \geqslant b > 0$. On note $n$ le nombre de pas dans l'algorithme d'Euclide, c'est-à-dire que si l'on note $(r_m)_{m \in \mathbb{N}}$ la suite des restes, avec $r_0 = a$ et $r_1 = b$, alors $r_n$ est le dernier reste non nul. Montrer que

$$a \geqslant (a \wedge b) F_{n+2} \qquad \text{et} \qquad b \geqslant (a \wedge b) F_{n+1}.$$

(3) En utilisant que $F_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n + \left( \frac{1-\sqrt{5}}{2} \right)^n \right)$, donner une borne sur le nombre $n$ de pas dans l'algorithme en termes des entrées $a$ et $b$. Est-elle optimale ?

(4) En supposant le coût des opérations élémentaires linéaire en la taille des entrées, donner la complexité de l'algorithme d'Euclide étendu.

**Exercice 6.** Implémenter les algorithmes de décomposition d'un rationnel en somme de fractions égyptiennes décrits dans la feuille de TD 1.

**Exercice 7.** Écrire et implémenter un algorithme calculant le symbole de Jacobi $\left(\frac{a}{n}\right)$, pour $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ impair, sans effectuer de décomposition en produits de facteurs premiers. Quelle est sa complexité ?