TD 6 : Résidus quadratiques et réciprocité

Exercice 1. [Symbole de Jacobi]

Pour $a \in \mathbb{Z}$ et $b = \prod_i p_i^{r_i}$ impair premiers entre eux, on définit le symbole de Jacobi de a modulo b par

$$\left(\frac{a}{b}\right) := \prod_i \left(\frac{a}{p_i}\right)^{r_i}$$

(a) Montrer que $\left(\frac{a}{b}\right)$ peut être égal à 1 sans que a ne soit un carré modulo b.

(b) Montrer que $\left(\frac{a}{b}\right)$ ne dépend que de a modulo b, et est multiplicatif en a et en b.

(c) Calculer $\left(\frac{-1}{b}\right)$ et $\left(\frac{2}{b}\right)$ en fonction des congruences de b modulo 4 et 8.

(d) Démontrer que pour tous a, b premiers entre eux, impairs et avec $a > 0$, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ si a ou b est congru à 1 modulo 4, et $-\left(\frac{b}{a}\right)$ sinon.

(e) En déduire un algorithme de calcul du symbole de Legendre.

(f) Calculer les symboles de Jacobi $\left(\frac{7}{15}\right), \left(\frac{12}{43}\right), \left(\frac{13}{53}\right), \left(\frac{10}{99}\right)$.

Exercice 2. [Décomposition en idéaux premiers]

On fixe $d \in \mathbb{Z}$ sans facteur carré, différent de 0 et 1, $K = \mathbb{Q}(\sqrt{d})$ et p un nombre premier.

(a) Rappeler le comportement de $p\mathcal{O}_K$ en fonction de d modulo p.

(b) Pour d premier, en déduire le comportement de $p\mathcal{O}_K$ en fonction de p modulo d. Avec quelle fréquence est-il inerte ? Totalement décomposé ?

(c) Détailler ce comportement pour $d = -7, -2, 2, 5$.

Exercice 3.

(a) Pour p un nombre premier impair, soit n le plus petit entier positif qui n'est pas un carré modulo p. En considérant m le plus petit entier tel que $mn > p$, montrer que $n < \sqrt{p} + 1$.

(b) Soit $n \in \mathbb{N}^*$ et $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Si $p = F_n$ est premier, montrer que a engendre $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $\left(\frac{a}{p}\right) = -1$.

(c) Montrer que 3 est alors un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

(d) Montrer que p est premier si et seulement si

$$3^{\frac{p-1}{2}} = -1 \mod p$$

(critère de Pépin).

Exercice 4. [Preuve d'Eisenstein de la réciprocité quadratique]

Soient p et q des nombres premiers impairs distincts.

(a) Soit A_p l'ensemble des entiers pairs de 2 à $p-1$, et pour tout $a \in A_p$, r_a le reste de la division euclidienne de qa par p. Montrer que modulo p, $A_p = \{(-1)^{r_a} r_a, a \in A_p\}$.

(b) En déduire que $\left(\frac{q}{p}\right) = (-1)^{\sum_{a\in A_p} r_a}$ puis que $\left(\frac{q}{p}\right) = (-1)^{\sum_{a\in A_p} \lfloor \frac{qa}{p} \rfloor}$.

(c) On note $O = (0,0), P = (p,0), Q = (0,q), R = (p,q), S = (p/2,0), T = (0,q/2)$ et $M = (p/2,q/2)$ (faire un dessin). Montrer que $\left(\frac{q}{p}\right)$ est égal à $(-1)^\mu$ avec μ le nombre de points de $\mathbb{Z}^2$ compris dans l'intérieur du domaine délimité par le triangle OSM.

(d) En déduire la réciprocité quadratique par symétrie du raisonnement.