TD 6 : Symbole de Legendre et réciprocité quadratique

Exercice 1. [Cas $p = 2$ de la réciprocité quadratique]

Soit p un nombre premier impair, on va montrer ici avec les lois de réciprocité que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(a) En posant $p^* = (-1)^{\frac{p-1}{2}}p$, montrer que $p^* \equiv 1 \mod 4$ et que $\mathbb{Q}(\sqrt{p^*})$ est l'unique sous-corps quadratique de $\mathbb{Q}(\zeta_p)$.

(b) Montrer que 2 est décomposé dans $\mathbb{Q}(\sqrt{p^*})$ si et seulement si $p^* \equiv 1 \mod 8$.

(c) En déduire la formule grâce aux lois de réciprocité.

Exercice 2. [Symbole de Jacobi et applications]

(a) Rappeler les propriétés du symbole de Jacobi.

(b) Calculer les symboles de Jacobi et $\left(\frac{122}{237}\right)$ et $\left(\frac{2411}{5031}\right)$.

(c) Pour $K = \mathbb{Q}(\sqrt{15})$, rappeler brièvement à quelles conditions un nombre premier p est ramifié, inerte ou totalement décomposé dans K.

(d) Grâce au symbole de Jacobi, décrire la forme de la décomposition de p dans $\mathcal{O}_K$ en fonction des classes de congruence de p modulo 60.

Exercice 3. [Test de primalité de Lucas-Lehmer]

On considère la suite $(s_n)_{n\in\mathbb{N}}$ définie par récurrence par $s_0 = 4$ et $s_{i+1} = s_i^2 - 2$ pour tout i. Le but de cet exercice est de démontrer le théorème de Lucas-Lehmer : si p est un nombre premier, le nombre de Mersenne $M_p = 2^p - 1$ est premier si et seulement si il divise s_{p-2}.

(a) Discuter de la complexité de ce test de primalité en fonction des données.

(b) On pose $\omega = 2 + \sqrt{3}$ et $\omega' = 2 - \sqrt{3}$. Montrer par récurrence que pour tout $n \in \mathbb{N}$,

$$s_n = \omega^{2^n} + (\omega')^{2^n}.$$

(c) Supposons que M_p divise s_{p-2}. Montrer qu'il existe un entier k tel que

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1.$$

(d) On suppose par l'absurde que M_p n'est pas premier. On fixe q son plus petit facteur premier, et on fixe $\mathfrak{Q}$ un idéal premier de $\mathbb{Z}[\sqrt{3}]$ au-dessus de q, montrer que ω est d'ordre exactement 2^p modulo $\mathfrak{Q}$.

(e) En déduire que $2^p < q^2$, et une contradiction. On a donc montré que M_p est premier s'il divise s_{p-2}.

(f) Supposons maintenant que M_p est premier. Montrer que $2^p - 1$ est congru à 7 modulo 12, et en déduire que 3 n'est pas carré modulo M_p alors que 2 l'est.

(g) On pose $\sigma = 2\sqrt{3}$ et $\mathfrak{P}$ un idéal premier de $\mathbb{Z}[\sqrt{3}]$ au-dessus de M_p. Montrer que

$$(6+\sigma)^{M_p} = 6 - \sigma \mod \mathfrak{Q}.$$

(h) En utilisant que $\omega = (6+\sigma)^2/24$, en déduire que $\omega^{(M_p+1)/2} = -1 \mod \mathfrak{Q}$.

(i) Prouver finalement que $s_{p-2} = 0 \mod \mathfrak{Q}$ et conclure.

Exercice 4. [Signe des sommes de Gauss]

Dans cet exercice, p est un nombre premier impair, $\zeta = e^{2i\pi/p}$ et

$$G_p = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

On rappelle que $G_p^2 = (-1)^{(p-1)/2}p$, donc $G_p = \pm\sqrt{p}$ si $p \equiv 1 \mod 4$, et $G_p = \pm i\sqrt{p}$ si $p \equiv 3 \mod 4$. Le but de cet exercice est de déterminer complètement G_p, pas seulement au signe près.

(a) Montrer que $p = \prod_{r=1}^{p-1}(1-\zeta^r)$.

(b) Montrer que les $\pm 4k-2$ où $k = 1, \cdots, (p-1)/2$ forment un système de représentants de $(\mathbb{Z}/p\mathbb{Z})^*$.

(c) En déduire que $(-1)^{(p-1)/2}p = \prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-2k+1})^2$.

(d) Prouver que $\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-2k+1})$ vaut $\sqrt{p}$ si $p \equiv 1 \mod 4$ et $i\sqrt{p}$ si $p \equiv 3 \mod 4$.

On a donc $G_p = \varepsilon \prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-2k+1})$ avec $\varepsilon = \pm 1$ qu'il suffit de déterminer.

(e) Soit le polynôme $P(X) = \sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) X^k - \varepsilon \prod_{k=1}^{(p-1)/2}(X^{2k-1} - X^{p-2k+1})$.

Montrer que $X^p - 1$ divise P, soit Q tel que $P(X) = (X^p-1)Q(X)$. On écrit formellement $X = e^z$ d'où une égalité de séries entières $P(e^z) = (e^{pz}-1)Q(e^z)$.

(f) Montrer que le coefficient en $z^{(p-1)/2}$ du terme de gauche est

$$\frac{1}{((p-1)/2)!} \sum_{j=1}^{(p-1)/2} \left(\frac{j}{p}\right) j^{(p-1)/2} - \varepsilon \prod_{k=1}^{(p-1)/2} (4k-p-2).$$

(g) Montrer que le coefficient en $z^{(p-1)/2}$ du terme de droite est de la forme pa/b avec a, b entiers et p ne divisant pas b.

(h) En déduire que

$$\sum_{j=1}^{(p-1)/2} \left(\frac{j}{p}\right) j^{(p-1)/2} \equiv \varepsilon((p-1)/2)! \prod_{k=1}^{(p-1)/2} (4k-2) \mod p$$

(i) En utilisant le théorème de Wilson, en déduire que

$$\sum_{j=1}^{(p-1)/2} \left(\frac{j}{p}\right) j^{(p-1)/2} \equiv -\varepsilon \mod p$$

(j) Conclure que $\varepsilon = 1$.