Les exercices étoilés (*) s'adressent aux seuls étudiants inscrits à l'unité MO12

Devoir 1

La loi de réciprocité quadratique:

Exercice 1. *Un entier a est dit un résidu quadratique modulo n si l'image $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ y est un carré.*

(i) Donnez les résidus quadratique modulo 6.

(ii) (*) Donnez un critère sur p premier pour que -1 soit un résidu quadratique modulo p.

(iii) ***Symbole de Legendre****: pour p premier et a non divisible par p, on définit $\left(\frac{a}{p}\right) \in \{\pm 1\} \subset \mathbb{R}$ comme étant égal à 1 si a est un résidu quadratique modulo p et -1 sinon. Montrez que le symbole de Legendre est multiplicatif, i.e.*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(iv) ***Symbole de Jacobi****: pour p premier et a divisible par p, on prolonge le symbole de Jacobi en posant $\left(\frac{a}{p}\right) = 0$ dans l'anneau commutatif $\mathbb{R}$. Pour $b = \prod_i p_i$ on pose*

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

Montrez que $\left(\frac{a}{b}\right) = 0$ si et seulement si a et b ne sont pas premiers entre eux.

(a) *Montrez que si a est un résidu quadratique modulo b alors $\left(\frac{a}{b}\right) = 1$. Donnez un contre exemple pour la réciproque.*

(b) *Montrez que le symbole de Jacobi est bi-multiplicatif (i.e. par rapport à la variable a et b).*

(v) On considère pour p premier impair, le morphisme de groupe multiplicatif $f : x \in (\mathbb{Z}/p\mathbb{Z})^\times \mapsto x^2 \in (\mathbb{Z}/p\mathbb{Z})^\times$. Donnez le cardinal de l'image ainsi que le nombre de carrés de $\mathbb{Z}/p\mathbb{Z}$. Montrez alors le critère d'Euler comme quoi x est un carré non nul de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x^{(p-1)/2} \equiv 1 \bmod p$.

(vi) (*) ***Lemme de Gauss****: pour p premier impair et $n \in \mathbb{Z}$, on appelle résidu minimal de n modulo p, l'unique entier $n' \in]-p/2, p/2[$ tel que $n \equiv n' \bmod p$. Soit $m \in \mathbb{N}$ non multiple de p; on note μ le nombre d'entiers de $\{m, 2m, \cdots, \frac{(p-1)}{2}m\}$ dont le résidu minimal est strictement négatif. Montrez que $\left(\frac{m}{p}\right) = (-1)^\mu$.*

(vii) Montrez, en utilisant le lemme de Gauss, que pour p premier impair, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, soit 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \bmod 8$.

(viii) Montrez que -3 est un résidu quadratique modulo p premier plus grand que 5, si et seulement si $p \equiv 1 \bmod 6$.

(ix) (*) ***Loi de réciprocité quadratique****: il s'agit de prouver que pour p et q premiers impairs*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$$

Enoncée la première fois par Euler en 1783, la première preuve est due à Gauss en 1798, qui en donnera 7 en tout. Aujourd'hui on en dénombre plus de 180! Nous proposons une preuve assez récente via le symbole de Zolotarev.

(a) *Pour m premier avec n, soit $\epsilon_n(m)$ le symbole de Zolotarev défini comme la signature de la permutation correspondant à la multiplication par m dans $\mathbb{Z}/n\mathbb{Z}$. Montrez que le symbole de Zolotarev est multiplicatif en la variable m, i.e. $\epsilon_n(mm') = \epsilon_n(m)\epsilon_n(m')$ et que pour n premier impair $\epsilon_n(m) \equiv m^{(n-1)/2} \bmod n$. Déduisez en que le symbole de Zolotarev pour n et m premiers distincts est égal au symbole de Legendre.*

(b) *On fixe n et m des premiers impairs distincts. Pour tout entier r positif, on note $\pi_r : \mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z}$ le morphisme de groupe qui à un entier associe sa classe. On note $I_r := \{0, \cdots, r-1\}$ et on considère b_r définie comme la restriction de π_r à I_r.*

On définit sur $I_n \times I_m$ l'ordre lexicographique $\leqslant_1$ ainsi que l'ordre lexicographique inverse $\leqslant_2$ dont on rappelle les définitions

$$(i,j) \leqslant_1 (i',j') \Leftrightarrow 0 \leqslant i < i' < n \text{ ou } i = i' \text{ et } 0 \leqslant j \leqslant j' < m$$

$$(i,j) \leqslant_2 (i',j') \Leftrightarrow 0 \leqslant j < j' < m \text{ ou } j = j' \text{ et } 0 \leqslant i \leqslant i' < n$$

On numérote alors par ordre croissant les éléments de $I_n \times I_m$ pour chacun de ces ordres et on note

$$c_0^1 = (0,0) <_1 c_1^1 <_1 \cdots <_1 c_{mn-1}^1 = (n-1, m-1)$$
$$c_0^2 = (0,0) <_2 c_1^2 <_2 \cdots <_2 c_{mn-1}^2 = (n-1, m-1)$$

(i) Montrez que pour tout $(i,j) \in I_n \times I_m$, $(i,j) = c^1_{mi+j} = c^2_{nj+i}$.

(ii) On considère les bijections $f_1, f_2 : I_n \times I_m \longrightarrow I_{mn}$ définie par $f_1(i,j) = mi + j$ et $f_2(i,j) = nj + i$. On définit alors la permutation λ de I_{mn} définie par $\lambda(f_1(i,j)) = f_2(i,j)$. Montrez que la signature $\epsilon(\lambda)$ est égale à $(-1)^{\frac{n(n-1)}{2}\frac{m(m-1)}{2}}$.

(iii) On considère σ (resp. τ) la permutation de $\mathbb{Z}/n\mathbb{Z} \times \{0, 1, \cdots m-1\}$ (resp. de $\{0, 1, \cdots, n-1\} \times \mathbb{Z}/m\mathbb{Z}$) définie par $(i,j) \mapsto (\pi_n(mb_n^{-1}(i)+j), j)$ (resp. $(i, \pi_m(nb_m^{-1}(j)+i))$). Montrez que $\epsilon(\sigma) = \epsilon_n(m)$, $e(\tau) = \epsilon_m(n)$.

(iv) On note $\tilde{\sigma}$ (resp. $\tilde{\tau}$) la permutation de $I_n \times I_m$ définie par $(b_n^{-1} \times Id) \circ \sigma \circ (b_n \times Id)$ (resp. $(Id \times b_m^{-1}) \circ \tau \circ (Id \times b_m)$). Soit ϕ la bijection $I_{nm} \longrightarrow I_n \times I_m$ donnée par le théorème chinois, soit $\phi = (b_n^{-1} \times b_m^{-1}) \circ \varphi \circ b_{mn}$. On note $\tilde{\lambda}$ la permutation de $I_n \times I_m$ définie par $\varphi \circ \lambda \circ \varphi^{-1}$. Montrez l'égalité

$$\tilde{\lambda} \circ \tilde{\sigma} = \tilde{\tau}.$$

(v) Montrez alors que pour n et m premiers entre eux, le symbole de Zolotarev vérifie l'égalité

$$\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4}\left(\frac{n}{m}\right)$$

En utilisant la loi de réciprocité quadratique *(à faire par tous)*

(x) Calculez $\left(\frac{713}{1009}\right)$.

(xi) Montrez que 5 *(resp.* 7*, resp.* 3*) est un résidu quadratique modulo* p *premier impair si et seulement si* $p \equiv \pm 1 \bmod 10$ *(resp.* $p \equiv \pm 1, \pm 3, \pm 9 \bmod 28$*, resp.* $p \equiv \pm 1 \bmod 12$*).*