Université Pierre et Marie Curie LICENCE A Année 2005-2006

Devoir 1

Exercice 1. ***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 $\epsilon_n(m) \equiv m^{(n-1)/2} \mod n$. 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 $\leq_1$ ainsi que l'ordre lexicographique inverse $\leq_2$ dont on rappelle les définitions

$$(i,j) \leq_1 (i',j') \Leftrightarrow 0 \leq i < i' < n \text{ ou } i = i' \text{ et } 0 \leq j \leq j' < m$$

$$(i,j) \leq_2 (i',j') \Leftrightarrow 0 \leq j < j' < m \text{ ou } j = j' \text{ et } 0 \leq i \leq i' < n$$

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 l de I_{mn} définie par $l(f_1(i,j)) = f_2(i,j)$. Montrez que la signature $\epsilon(l)$ 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 $\phi = (b_n^{-1} \times b_m^{-1}) \circ \psi \circ b_{mn}$. On note $\tilde{l}$ la permutation de $I_n \times I_m$ définie par $\psi \circ l \circ \psi^{-1}$. Montrez l'égalité

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

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

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

Preuve :

(a) La multiplicativité du symbole de Zolotarev en la variable m provient du fait que la composition de la multiplication par m avec la multiplication par m' correspond à la multiplication par mm' et que la signature d'une composée est le produit des signatures.

Soit r l'ordre de m dans $(\mathbb{Z}/n\mathbb{Z})^\times$ qui est cyclique si n est premier; ce groupe se décompose alors sous l'action de m en $(n-1)/r$ orbites chacune de longueur r et sur ces orbites la multiplication par m y induit un cycle de longueur r. On en déduit alors que le symbole de Zolotarev est $(-1)^{(r-1)(n-1)/r}$. Ainsi

- si r est pair on a

$$m^{(n-1)/2} = (m^{r/2})^{(n-1)/r} \equiv (-1)^{(n-1)/r} \mod n$$

car m étant d'ordre r, $m^{r/2}$ est une racine carrée de 1 dans le corps $\mathbb{Z}/n\mathbb{Z}$ distincte de 1 donc égale à -1;

- si r est impair, $n-1$ est alors divisible par $2r$ et donc $m^{(n-1)/2} = (m^r)^{(n-1)/2r} \equiv 1 \mod n$ d'où le résultat.

Autre preuve: on utilise la formule

$$\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i-j}$$

ce qui donne $\epsilon(\sigma) \equiv m^{n(n-1)/2} \equiv m^{(n-1)/2} \mod p$, car $m^n \equiv m \mod n$ pour $m \not\equiv 0 \mod p$.

(b) (i) Par définition $(i',j') \leq_1 (i,j)$ si et seulement si $i < i'$ ou si $i = i'$ et $j \leq j'$ de sorte que l'ensemble de ces éléments est de cardinal $mi+j$, d'où le résultat. L'ordre lexicographique inverse se traite exactement de la même manière.

(ii) D'après ce qui précède on a donc $(i,j) = c^1_{f_1(i,j)} = c^2_{f_2(i,j)}$. On rappelle que la signature de l est égale à $(-1)^k$ où k est le cardinal de l'ensemble des $f_1(i,j) < f_1(i',j')$ tels que $f_2(i,j) > f_2(i',j')$, soit par définition à l'ensemble des $(i,j) <_1 (i',j')$ tels que $(i',j') <_2 (i,j)$. On remarque alors que l'égalité $i = i'$ impose $j < j'$ et $j' < j$, d'où une contradiction, ce qui donne alors $i < i'$ et $j' < j$ et donc un cardinal égal à $\frac{n(n-1)}{2}\frac{m(m-1)}{2}$ d'où le résultat.

(iii) La signature de σ restreint à $\mathbb{Z}/n\mathbb{Z} \times \{j\}$, comme composée de la multiplication par m et de la translation par j sur la première composante, est donc de signature $\left(\frac{m}{n}\right)$ car la translation en question est de signature $(-1)^{(n-1)j} = 1$. En outre j décrit m valeurs de sorte que la signature de σ est $\left(\frac{m}{n}\right)^m = \left(\frac{m}{n}\right)$. Par symétrie τ est donc de signature $\left(\frac{n}{m}\right)$.

(iv) Il suffit de suivre patiemment les diverses flèches:

- $\tilde{\sigma}(i,j) = (b_n^{-1}(\pi_n(mi+j)), j) \in I_n \times I_m$;
- $(b_n \times b_m)(b_n^{-1}(\pi_n(mi+j)), j) = (mi+j, j) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;
- $\psi(mi+j, j) = mi+j \in \mathbb{Z}/mn\mathbb{Z}$;
- $b_{nm}^{-1}(mi+j) = mi+j \in I_{mn}$ car $0 \leq mi+j \leq mn-1$;
- $l(mi+j) = i+nj \in I_{mn}$;
- $b_{nm}(i+nj) = i+nj \in \mathbb{Z}/mn\mathbb{Z}$;
- $\psi(i+nj) = (i, i+nj) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;
- $(b_n^{-1} \times b_m^{-1})(i, i+nj) = (i, b_m^{-1}(\pi_m(i+nj))) = \tilde{\tau}(i,j)$.

(v) En considérant les signatures dans l'égalité $\tilde{l} \circ \tilde{\sigma} = \tilde{\tau}$, on obtient $(-1)^{(m-1)(n-1)/4}\epsilon_n(m) = \epsilon_m(n)$ soit:

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

d'où le résultat.