Feuille d'exercices 1

1 Nombres premiers

Exercice 1. *Soient p et q des nombres premiers distincts.*

(a) Quel est le cardinal de $(\mathbb{Z}/pq\mathbb{Z})^*$? Combien y a-t-il d'éléments de $(\mathbb{Z}/pq\mathbb{Z})^*$ égaux à leur inverse ?

(b) Montrer la congruence :

$$\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}} \equiv 1 \bmod pq$$

(même méthode que pour le théorème de Wilson: $(p-1)! \equiv -1 \mod p$).

Exercice 2. *Montrer l'existence d'une infinité de nombres premiers p tels que*

(a) $p \equiv 3 \mod 4$;

(b) $p \equiv 1 \mod 4$;

(c) $p \equiv 1 \mod 8$;

(d) $p \equiv 5 \mod 6$.

(e) $p \equiv 5 \mod 8$.

(f) $p \equiv 1 \mod 6$;

(g) $p \equiv -1 \mod 12$.

Exercice 3. *Etude des premiers nombres de Fermat.*
On pose pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$; F_n est par définition le n-ième nombre de Fermat.

(a) Soit $m \in \mathbb{N}\backslash\{0\}$. En utilisant la factorisation

$$X^{2n+1} + 1 = (X+1)(X^{2n} - X^{2n-1} + \cdots + 1)$$

prouver que si $2^m + 1$ est premier alors m est une puissance de 2.

(b) Calculer F_n pour $n \leq 4$ et vérifiez qu'ils sont tous premiers.

(c) Montrer que tout diviseur premier de F_5 est de la forme $64k + 1$.

(d) Montrer que F_5 est divisible par $641 = 1 + 5.2^7 = 5^4 + 2^4$.

(e) Montrer que pour $n \neq m$, F_n et F_m sont premiers entre eux et en déduire l'existence d'une infinité de nombres premiers.

(f) Soit $p = F_n$ premier ; montrer qu'un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ est générateur si et seulement s' il n'est pas un carré. En utilisant la loi de réciprocité quadratique, montrer que $3, 5, 7$ sont des générateurs de $(\mathbb{Z}/p\mathbb{Z})^*$ pour $n \geq 2$. En déduire alors le critère de Pépin : $p = F_n$ est premier si et seulement si $3^{(p-1)/2} \equiv -1 \bmod p$.

Exercice 4. *Le but de cet exercice est d'étudier les nombres de Mersenne $M_p = 2^p - 1$ pour p premier. On veut en particulier montrer le test de primalité de Lucas-Lehmer: M_q est premier ($q \geq 3$ premier) si et seulement si $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$.*

(i) Montrez que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

(i) Montrez que l'anneau $A = \mathbb{Z}[\sqrt{3}]$ est euclidien et caractérisez les unités.

(ii) *Remarquez que pour q impair, $2^q - 1 \equiv 7 \mod 12$ et en déduire qu'il existe un premier $p \not\equiv \pm 1 \mod 12$ divisant $2^q - 1$ et remarquer que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. Montrez que si M_q vérifie la congruence ci-dessus, alors $p = M_q$.*

(iii) *En utilisant la loi de réciprocité quadratique, montrez que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \mod 12$. Pour $p > 3$ premier non congru à ± 1 modulo 12, montrez le petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$: $(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p$.*

On suppose désormais M_q premier. En remarquant que 2 est un carré modulo M_q, on définit dans $\mathbb{Z}[\sqrt{3}]/(M_q)$: $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. A partir des relations $\tau^2 = 2+\sqrt{3}$ et $\tau\bar{\tau} = -1$, en déduire la congruence de l'énoncé.

(iv) *Montrez le test de primalité suivant sur M_q pour $q \geq 3$ premier: soit $(L_i)_{i\geq 0}$ la suite de Lucas-Lehmer définie par $L_0 = 4$ et $L_{i+1} = L_i^2 - 2 \mod M_q$, alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \mod M_q$.*

Exercice 5. *Un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \mod n$.*

(a) *Montrez que $n = 105 = 3.5.7$ est pseudo-premier de base 13 mais qu'il ne l'est pas de base 2.*

(b) *Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p. Réciproquement un nombre n est dit de Carmichael s'il est pseudo-premier de base b pour tout b premier avec n, sans être premier. Montrez que $n = 561 = 3.11.17$ est un nombre de Carmichael.*

(c) *Un entier $n = 1 + 2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée:*

$$b^q \equiv 1 \mod n \qquad \exists 0 \leq j < k,\ b^{2^j q} \equiv -1 \mod n$$

(i) *Montrez que si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leq b < n$ et qui si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b.*

(ii) *Montrez que $n = 561$ n'est pas fortement pseudo-premier de base 2.*

(iii) *Pour n impair soit*

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ n \text{ est fortement pseudo-premier de base } x\}.$$

On veut montrez le théorème de Rabin: si n est non premier alors $\frac{|B_n|}{\phi(n)} \leq 1/4$ sauf pour $n = 9$. Sous une autre forme, si $|B_n| \geq \phi(n)/4$ alors n est premier.

(α) *Considérons $p_1 \equiv 3 \mod 4$ premier tel que $p_2 = 2p_1 - 1$ soit premier (exemple $p_1 = 40039, 41011, 42727$) Montrez alors que pour $n = p_1 p_2$, on a $4|B_n| = \phi(n)$.*

(β) *Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de $n = 1 + 2^k q$, q impair; on écrit $p_i = 1 + 2^{k_i} q_i$ avec q_i impair et $k_1 \leq \cdots \leq k_r$. Montrez alors que*

$$|B_n| = (q, q_1) \cdots (q, q_r)(1 + \sum_{j=0}^{k_1 - 1} 2^{jr})$$

En déduire que $\frac{|B_n|}{\phi(n)} \leq \frac{1+\frac{2^{k_1 r}-1}{2^r-1}}{2^{k_1 r}} K$, avec $K = \prod_{i=1}^r \frac{(q,q_i)}{q_i p_i^{\alpha_i - 1}}$. En outre si tous les k_i ne sont pas tous égaux, on peut améliorer l'inégalité précédente d'un facteur 2.

(γ) *Montrez le résultat dans le cas où n est une puissance d'un nombre premier, puis traitez le cas général.*

Remarque: Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier.

2 Corps finis

Exercice 1. *Montrer les isomorphismes suivant et donner un générateur du groupe des inversibles des corps en question :*

(i) $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/(X^2+X+1)$ *;*

(ii) $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/(X^3+X+1)$ *;*

(iii) $\mathbf{F}_{16} \simeq \mathbf{F}_2[X]/(X^4+X+1)$ *; donner dans cet isomorphisme l'image de* $\mathbf{F}_4 \subset \mathbf{F}_{16}$ *et en déduire* $\mathbf{F}_{16} \simeq \mathbf{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$.

(iv) $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2+X-1)$.

Exercice 2. *On dira d'une extension de corps* $k \subset \bar{k}$ *qu'elle est une clôture algébrique si:*
(a) tout élément $x \in \bar{k}$ *est algébrique sur* k*, i.e. il existe une polynôme* $P \in k[X]$ *tel que* $p(x)=0$*;*
(b) tout polynôme $P \in \bar{k}[X]$ *est totalement décomposé dans* $\bar{k}$.
Pour tout n *divisant* n' *on fixe une injection* $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^{n'}}$*. Montrez alors que* $\bar{\mathbb{F}}_p := \bigcup_{n>1} \mathbb{F}_{p^{n!}}$ *est une cloture algébrique de* $\mathbf{F}_p$.

Exercice 3. *(i) Donner tous les polynômes irréductibles de degré inférieur à* 4 *sur* $\mathbf{F}_2$.
(ii) Quelle est la factorisation sur $\mathbb{F}_4$ *d'un polynôme de* $\mathbb{F}_2[X]$ *irréductible de degré* 4*?*
(iii) Déduire des questions précédentes, le nombre de polynômes irréductibles de degré 2 *sur* $\mathbf{F}_4$.

Exercice 4. *Polynômes irréductibles sur* $\mathbb{F}_q$*. soient* $A(n,q)$ *l'ensemble des polynômes irréductibles unitaires de degré* n *sur* $\mathbb{F}_q$ *et* $I(n,q)$ *le cardinal de cet ensemble.*

(a) Montrer que si $d|n$ *alors si* $P \in A(d,q)$ *on a* P *qui divise* $X^{q^n}-X$.

(b) Montrer que si $P \in A(d,n)$ *divise* $X^{q^n}-X$ *alors* d *divise* n.

(c) En déduire la formule

$$\sum_{d|n} dI(d,q) = q^n,$$

puis en appliquant la formule d'inversion de Moebius

$$I(n,q) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})q^d.$$

(d) Montrer que pour tout $n \geq 1$*,* $I(n,q) \geq 1$ *et trouver un équivalent de* $I(n,q)$ *quand* n *tend vers* $+\infty$.

Exercice 5. *(1) Le nombre* 2 *est-il un carré dans* $\mathbf{F}_5$*? Montrer que* X^2+X+1 *est irréductible sur* $\mathbf{F}_5$.

(2) Soit $P(X) \in \mathbf{F}_5[X]$ *un polynôme unitaire irréductible de degré deux . Montrer que le quotient*

$$\frac{\mathbf{F}_5[X]}{(P(X))}$$

est isomorphe au corps $\mathbf{F}_{25}$ *et que* P *a deux racines dans* $\mathbf{F}_{25}$.

(3) On note α *une racine de* X^2+X+1 *dans* $\mathbf{F}_{25}$*. Montrer que tout* $\beta \in \mathbf{F}_{25}$ *peut s'écrire* $a\alpha+b$ *avec* a *et* b *dans* $\mathbf{F}_5$.

(4) Soit $P = X^5-X+1$*. Montrer que pour tout* $\beta \in \mathbf{F}_{25}$*, on a* $P(\beta) \neq 0$*. En déduire que* P *est irréductible sur* $\mathbf{F}_5$*.* P *est-il irréductible sur* $\mathbf{Q}$*?*

Exercice 6. *On considère le polynôme* $Q(X) = X^9-X+1$ *sur* $\mathbf{F}_3$.

(a) Montrer que le polynôme Q *n'a pas de racines dans* $\mathbb{F}_3, \mathbb{F}_9$.

(b) Montrer que $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3-X-1)}$.

(c) Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ *du polynôme* $X^3 - X - 1$ *est une racine du polynôme* Q.

(d) Déterminer toutes le racines de Q *dans* $\mathbb{F}_{27}$.

(e) Factoriser le polynôme Q *sur le corps* $\mathbb{F}_3$.

Exercice 7. *A quelle condition un polynôme* P *à coefficients dans* $\mathbf{F}_p$ *de degré* n *est-il irréductible sur* $\mathbf{F}_{p^m}$ *? Dans le cas où* P *est irréductible sur* $\mathbf{F}_p$*, on donnera des précisions sur les degrés des facteurs irréductibles de* P *sur* $\mathbf{F}_{p^m}$*. En particulier pour* $n = 5$*, donner* m *minimal tel que tout polynôme de degré* 5 *à coefficients dans* $\mathbf{F}_p$ *soit totalement décomposé (resp. possède une racine) sur* $\mathbf{F}_{p^m}$.

Exercice 8. *(i) Montrer que* X^4+1 *est irréductible sur* $\mathbb{Z}$ *et réductible modulo tout nombre premier* p*. (Indication : montrer que pour tout nombre premier impair* p*, le polynôme* $X^4 + 1$ *a une racine dans le corps* $\mathbb{F}_{p^2}$.

(ii) Soit n *un entier ne s'écrivant pas sous la forme* p^α *ou* $2p^\alpha$ *avec* p *premier impair. On sait que le* n*-ième polynôme cyclotomique* ψ_n *est irréductible sur* $\mathbb{Z}$*. Montrer en utilisant la question (ii) de l'exercice sur la théorie de Galois des corps finis, que* ψ_n *est réductible modulo tout nombre premier.*

Exercice 9. *Soit* $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$

(a) Décomposer P *en facteurs irréductibles modulo 2,3,5.*

(b) Montrer que P *est irréductible sur* $\mathbb{Q}$.

Exercice 10. *Soient* p *et* l *deux nombres premiers impairs. On suppose que* p *engendre* $(\mathbb{Z}/l\mathbb{Z})^*$ *et que* $l \equiv 2 \mod 3$*. On note* $P(X) = X^{l+1} - X + p$*. On veut montrer que* P *est irréductible sur* $\mathbb{Z}$.

(i) Montrer que P *n'a pas de racine rationnelle.*

(ii) On raisonne par l'absurde et on suppose $P = QR$ *avec* $Q, R \in \mathbb{Z}[X]$ *unitaire et de degré au moins* 2*. Montrer que* $\bar{P} = X(X-1)\bar{\Phi}_l$ *est la décomposition en polynômes irréductibles de* $\bar{P}$ *sur* $\mathbf{F}_p$ *; en déduire alors que* $\bar{Q} = \bar{\Phi}_l$ *et* $\bar{R} = X(X-1)$.

(iii) En passant modulo 2*, en déduire une contradiction. Comme exemple on propose le polynôme* $X^{72} - X + 47$.

Exercice 11. *Théorie de Galois des corps finis et version faible du théorème de Dirichlet: Soit* p *un nombre premier et* n *un entier premier avec* p*. On pose* $q = p^r$.

(1) Décrire le groupe de Galois de l'extension $\mathbb{F}_{q^n} : \mathbb{F}_q$ *et expliciter la théorie de Galois, i.e. montrer que l'application qui à un sous-groupe* H *de* $gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *associe le sous-corps de* $\mathbb{F}_{q^n}$ *des éléments fixés par tous les éléments de* H*, est une bijection entre les sous-groupes du groupe de Galois et les extensions intermédiaires* $\mathbb{F}_q \subset \mathbf{K} \subset \mathbb{F}_{q^n}$.

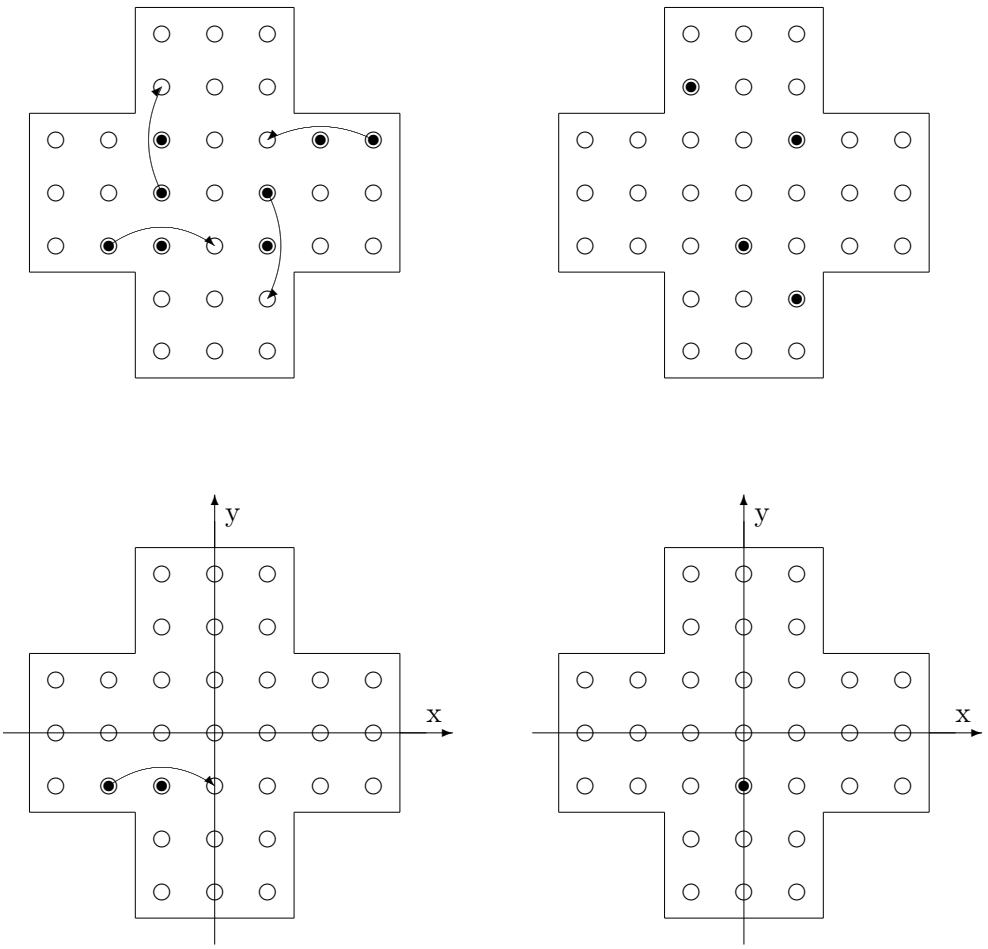
(2) Soit $L = Dec_{\mathbb{F}_p}(X^n - 1)$*. Montrer que* $\mathrm{Gal}(L/\mathbb{F}_p)$ *est isomorphe au sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$ *engendré par l'image de* p*. Montrer que le* n*-ième polynôme cyclotomique* $\Phi_n(X)$ *se décompose sur* $\mathbb{F}_p$ *en un produit de* $\phi(n)/k$ *facteurs irréductibles distincts, tous de degré* k*. Quel est cet entier* k*? En déduire une version faible du théorème de progression arithmétique, i.e. :*
pour tout entier n *il existe une infinité de nombres premiers* p *congrus à* 1 *modulo* n.

Exercice 12. *Le jeu du solitaire se joue sur un plateau disposant de* 33 *réceptacles (cercle vide) dans lesquels il peut y avoir des billes notés avec un cercle plein. A chaque étape on peut faire passer une bille au dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant soit vide, comme dans la figure suivante*

Soit alors O *placé au centre du plateau et un repère* (O, x, y) *comme dans la figure suivante et pour une configuration* $\mathcal{C}$ *quelconque de billes sur le plateau on introduit*

$$\alpha_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x+y} \in \mathbb{F}_4 \quad \beta_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x-y} \in \mathbb{F}_4$$

où j *est un générateur de* $\mathbb{F}_4^\times$.



(1) Montrer que (α, β) est un invariant du jeu.

(2) Habituellement le jeu consiste à partir d'une configuration où l'on place des billes dans tous les réceptacles sauf un seul disons (x_0, y_0) et à arriver à la configuration où tous les réceptacles sont vides sauf celui (x_0, y_0). Montrer qu'effectivement les deux configurations précédentes, possèdent les mêmes invariants (α, β).

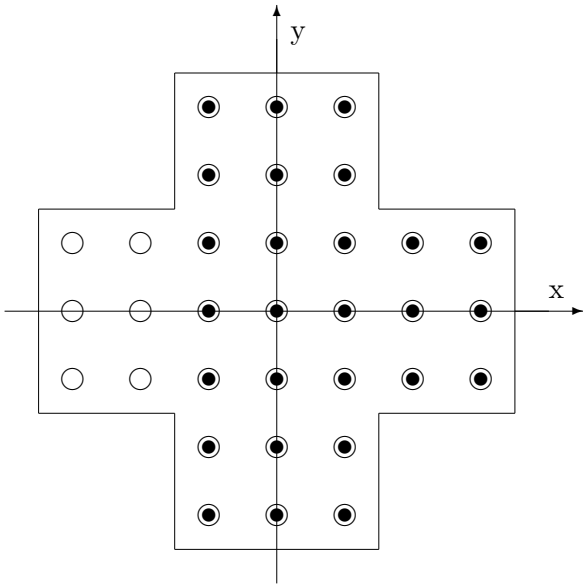
(3) Partant de la configuration suivante, montrer qu'il est impossible d'arriver à une configuration où il n'y aurait qu'une seule bille sur le plateau.

Exercice 13. ***Loi de réciprocité quadratique: DEVOIR A RENDRE*** *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

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

Exercice 14. *(i) Calculez $\left(\frac{713}{1009}\right)$.*

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

Exercice 15. *Soit n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer que n est un carré dans $\mathbb{N}$.*