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

Corrigé devoir 1

La loi de réciprocité quadratique

Définition 0.0.1. *Un entier $a \in \mathbb{Z}$ est dit un résidu quadratique modulo n si l'image $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ y est un carré.*

Ainsi pour connaître, par exemple, les résidus quadratique modulo 6, il suffit de faire la table des carrés dans $\mathbb{Z}/6\mathbb{Z}$:

$$\begin{array}{cccccccc} x & 0 & 1 & 2 & 3 & -2 & -1 \\ x^2 & 0 & 1 & -2 & 3 & -2 & 1 \end{array}$$

de sorte que a est un résidu quadratique modulo 6 si et seulement si $a \equiv 0, 1, 4, 3 \bmod 6$.

Lemme 0.0.2. *Pour p premier, -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1 mod 4$.*

Preuve : Supposons dans un premier temps que $p \equiv 1 \bmod 4$. On rappelle que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, soit alors x un générateur, $x^{p-1} \equiv 1 \bmod p$. On pose alors $p-1 = 4n$ et $y = x^n$ de sorte que la classe modulo p de y^2 est une racine carrée de 1 distincte de 1 dans le corps $\mathbb{Z}/p\mathbb{Z}$. Or dans un corps commutatif, il y a au plus deux racines carrées de 1, à savoir 1 et -1, ainsi -1 est le carré de y dans $\mathbb{Z}/p\mathbb{Z}$.

Réciproquement supposons qu'il existe y tel que $-1 \equiv y^2 \bmod p$, ce qui donne $y^4 \equiv 1 \bmod p$ et plus précisément la classe de y dans $\mathbb{Z}/p\mathbb{Z}$ est d'ordre 4. Or le petit théorème de Fermat donne $y^{p-1} \equiv 1 \bmod p$ de sorte que 4 divise $p-1$, d'où le résultat.

□

Proposition 0.0.3. *(critère d'Euler) Pour p premier impair, le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ est égal à $\frac{p+1}{2}$. Par ailleurs x est un résidu quadratique modulo p si et seulement si $x \equiv 0 \bmod p$ ou $x^{(p-1)/2} \equiv 1 \bmod p$.*

Preuve : On considère le morphisme de groupe multiplicatif $f : x \in (\mathbb{Z}/p\mathbb{Z})^\times \mapsto x^2 \in (\mathbb{Z}/p\mathbb{Z})^\times$ de sorte que l'image de f est l'ensemble des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$. Le premier p étant impair de sorte que $1 \neq -1$, le noyau de f est égal à $\{1, -1\}$ et donc de cardinal 2. Or $|\mathbb{Z}/p\mathbb{Z}| = |\operatorname{Ker} f||\operatorname{Im} f|$ soit $|\operatorname{Im} f| = \frac{p-1}{2}$. Si on rajoute 0 qui est visiblement un carré dans $\mathbb{Z}/p\mathbb{Z}$, l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ est égal à $\frac{p-1}{2} + 1 = \frac{p+1}{2}$.

En ce qui concerne le critère d'Euler, soit $x \in \mathbb{Z}/p\mathbb{Z}$ non nul tel qu'il existe y vérifiant $x = y^2$. Le petit théorème de Fermat donne $y^{p-1} = x^{(p-1)/2} = 1$ de sorte que tous les carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont solutions de l'équation $X^{(p-1)/2} - 1 = 0$ qui par ailleurs, $\mathbb{Z}/p\mathbb{Z}$ étant un corps commutatif, possède au plus $(p-1)/2$ solutions. On en déduit alors que l'ensemble des solutions dans $\mathbb{Z}/p\mathbb{Z}$ de $X^{(p-1)/2} = 1$ est l'ensemble des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$, d'où le résultat.

□

Définitions 0.0.4. - ***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.*

- ***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*

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

Lemme 0.0.5. *Le symbole de Legendre et est multiplicatif, i.e.*

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

de sorte que le symbole de Jacobi est bi-multiplicatif (i.e. par rapport aux variables a et b).

Preuve : La multiplicativité du symbole de Legendre découle directement du critère d'Euler donné à la proposition (0.0.3). En effet si x non nul dans $\mathbb{Z}/p\mathbb{Z}$ est un carré, on a $x^{(p-1)/2} = 1$ alors que dans le cas contraire on a $x^{(p-1)/2} = -1$. Ainsi si x et y sont des résidus quadratiques non nuls modulo p, on a $(xy)^{(p-1)/2} = x^{(p-1)/2}y^{(p-1)/2} \equiv 1 \bmod 2$, soit xy est un résidu quadratique modulo p. Si x est un résidu quadratique modulo p alors que y n'en n'est pas un, l'égalité précédente donne que xy n'est pas un résidu quadratique modulo p. Enfin si x et y ne sont pas des résidus quadratiques modulo p, l'égalité précédente donne $(xy)^{(p-1)/2} \equiv 1 \bmod p$ soit xy est un résidu quadratique modulo p, d'où la multiplicativité du symbole de Legendre et la bi-multiplicativité du symbole de Jacobi.

□

Lemme 0.0.6. *Le symbole de Jacobi $\left(\frac{a}{b}\right)$ est nul si et seulement si a et b ne sont pas premiers entre eux. Par ailleurs si a est un résidu quadratique modulo b alors $\left(\frac{a}{b}\right) = 1$.*

Preuve : Supposons qu'il existe p premier divisant $a \wedge b$; on en déduit alors que $a \equiv 0 \bmod p$ et donc $\left(\frac{a}{p}\right) = 0$, soit $\left(\frac{a}{b}\right) = 0$. Réciproquement si $\left(\frac{a}{b}\right) = 0$, on en déduit qu'il existe p divisant b tel que $\left(\frac{a}{p}\right) = 0$ soit $a \equiv 0 \bmod p$ et donc p divise $a \wedge b$.

En outre s'il existe c tel que $a \equiv c^2 \bmod b$, on en déduit que $a \equiv c^2 \bmod p$ pour tout p divisant b et donc $\left(\frac{a}{b}\right) = 1$.
Remarque: Soit $b = p^2$ et a qui n'est pas un carré modulo p. Par définition on a $\left(\frac{a}{b}\right) = 1$ alors que a n'est pas un carré modulo b car sinon il en serait un modulo p.

Proposition 0.0.7. ***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. On a alors $\left(\frac{m}{p}\right) = (-1)^\mu$.*

Preuve : Posons $\lambda = \frac{p-1}{2} - \mu$ et soit $r_1, \cdots, r_\lambda$ (resp. $s_1, \cdots, s_\mu$) les résidus minimaux positifs ou nuls (resp. strictement négatifs) de $\{m, 2m, \cdots, \frac{p-1}{2}m\}$. Notons tout d'abord que les r_i (resp. s_i) sont distincts deux à deux. Supposons qu'il existe un couple (i, j) tel que $r_i = s_j$ soit donc $am \equiv r_i \equiv s_j \equiv -bm \bmod p$ avec $1 \leqslant a, b \leqslant (p-1)/2$. On obtient alors $am + bm \equiv 0$ et comme m est premier avec p, $a + b$ est donc divisible par p ce qui ne se peut pas, d'où la contradiction. Ainsi on a

$$\{r_1, \cdots, r_\lambda, s_1, \cdots, s_\mu\} = \{1, 2, \cdots, (p-1)/2\}$$

En particulier on obtient

$$m.2m.\cdots.\frac{p-1}{2}m \equiv (-1)^{\mu} r_1 \cdots r_\lambda s_1 \cdots s_\mu = (-1)^{\mu}(\frac{p-1}{2})! \bmod p$$

Comme p ne divise pas $(\frac{p-1}{2})!$, il vient $m^{\frac{p-1}{2}} \equiv (-1)^{\mu} \bmod p$, d'où le résultat.

□

Corollaire 0.0.8. ***Le cas de*** 2*: 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* $p \equiv \pm 1 \bmod 8$*.*

Preuve : Il s'agit de calculer μ pour $m = 2$; on est donc ramené à compter les entiers l tels que $p/2 < 2l < p$. On vérifie aisément que si $p \equiv 1 \bmod 4$ (resp. $p \equiv 3 \bmod 4$) alors $\mu = \lambda = \frac{p-1}{4}$ (resp. $\lambda = \frac{p-3}{4}$ et $\mu = \frac{p+1}{4}$). On vérifie alors que $\frac{p^2-1}{4}$ a la même parité que μ, d'où le résultat.

□

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

Preuve : Il s'agit donc de calculer μ pour $m = -3$ et donc de compter les entiers l tels que $p/2 < -3l < p$. On vérifie alors que les l donnant un résidu minimal strictement négatifs sont

$$\{1, \cdots, \lfloor p/6 \rfloor, \lfloor p/3 \rfloor + 1, \cdots, \lfloor p/2 \rfloor\}$$

et donc $\mu = \lfloor p/6 \rfloor + \lfloor p/2 \rfloor - \lfloor p/3 \rfloor$. Ainsi si $p \equiv 1 \bmod 6$ (resp. $p \equiv 5 \bmod 6$), on obtient $\mu = n + 3n - 2n \equiv 0 \bmod 2$ (resp. $\mu = n + (3n+2) - (2n+1) \equiv 1 \bmod 2$); ainsi -3 est un carré modulo $p \neq 2, 3$ si et seulement si $p \equiv 1 \bmod 6$.

□

Théorème 0.0.9. ***Loi de réciprocité quadratique****: 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 163! Nous proposons une preuve assez récente via le symbole de Zolotarev.

Définition 0.0.10. *Pour* m *premier avec* n*, on définit le symbole de Zolotarev* $\epsilon_n(m)$ *comme la signature de la permutation (cf. le chapitre 3) correspondant à la multiplication par* m *dans* $\mathbb{Z}/n\mathbb{Z}$*. De manière générale, pour une permutation* τ*, on notera* $\epsilon(\tau)$ *sa signature.*

Proposition 0.0.11. *Pour* n *premier et* m *non divisible par* n*, le symbole de Zolotarev est égal au symbole de Legendre.*

Preuve : Le résultat découle directement du lemme suivant

Lemme 0.0.12. *Le symbole de Zolotarev est multiplicatif en la variable* m*, i.e.* $\epsilon_n(mm') = \epsilon_n(m)\epsilon_n(m')$*. En outre pour* n *premier impair* $\epsilon_n(m) \equiv m^{(n-1)/2} \bmod n$*.*

Preuve : 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

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

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 $m^{(n-1)/2} = (m^r)^{(n-1)/2r} \equiv 1 \bmod n$ d'où le résultat.

□

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

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

Lemme 0.0.13. *Pour tout $(i,j) \in I_n \times I_m$, $(i,j) = c^1_{mi+j} = c^2_{nj+i}$.*

Preuve : Par définition $(i',j') \leqslant_1 (i,j)$ si et seulement si $i < i'$ ou si $i = i'$ et $j \leqslant j'$ 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.

□

Lemme 0.0.14. *Soit m et n des premiers distincts. 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 $\lambda(f_1(i,j)) = f_2(i,j)$. La signature $\epsilon(\lambda)$ est alors égale à $(-1)^{\frac{n(n-1)}{2}\frac{m(m-1)}{2}}$.*

Preuve : 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 λ 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.

□

Lemme 0.0.15. *On fixe n et m des premiers impairs distincts. On considère alors 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. $(i, \pi_m(nb_m^{-1}(j)+i))$). On a alors $\epsilon(\sigma) = \epsilon_n(m)$, $e(\tau) = \epsilon_m(n)$.*

Preuve : 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 $\left(\frac{n}{m}\right)$.

□

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. $(Id \times b_m^{-1}) \circ \tau \circ (Id \times b_m)$).

Lemme 0.0.16. *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 $\phi \circ \lambda \circ \phi^{-1}$. On a alors l'égalité $\tilde{\lambda} \circ \tilde{\sigma} = \tilde{\tau}$.*

Preuve : Il suffit de suivre patiemment les diverses flèches:
- $\tilde{\sigma}(i, j) = (b_n^{-1}(\pi_n(mi + j)), j) \in I_n \times I_m$;
- $(b_n \times b_m)(b_n^{-1}(\pi_n(mi + j)), j) = (mi + j, j) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;
- $\varphi(mi + j, j) = mi + j \in \mathbb{Z}/mn\mathbb{Z}$;
- $b_{nm}^{-1}(mi + j) = mi + j \in I_{mn}$ car $0 \leqslant mi + j \leqslant mn - 1$;
- $\lambda(mi + j) = i + nj \in I_{mn}$;
- $b_{nm}(i + nj) = i + nj \in \mathbb{Z}/mn\mathbb{Z}$;
- $\varphi(i + nj) = (i, i + nj) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;
- $(b_n^{-1} \times b_m^{-1})(i, i + nj) = (i, b_m^{-1}(\pi_m(i + nj))) = \tilde{\tau}(i, j)$.

□

Preuve de la loi de réciprocité quadratique: en considérant les signatures dans l'égalité $\tilde{\lambda} \circ \tilde{\sigma} = \tilde{\tau}$, on obtient $(-1)^{(m-1)(n-1)/4}\epsilon_n(m) = \epsilon_m(n)$ soit d'après le lemme (0.0.12):

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

d'où le résultat.

□

Exemple: calcul de $\left(\frac{713}{1009}\right)$: en appliquant la loi de réciprocité quadratique, on a

$$(\begin{smallmatrix}713\\1009\end{smallmatrix}) = (\begin{smallmatrix}1009\\713\end{smallmatrix})(-1)^{\frac{1008.712}{4}} = (\begin{smallmatrix}296\\713\end{smallmatrix})(+1) = (\frac{8.37}{713}) = (\begin{smallmatrix}8\\713\end{smallmatrix})(\begin{smallmatrix}37\\713\end{smallmatrix})$$

Par ailleurs on a $(\begin{smallmatrix}8\\713\end{smallmatrix}) = (\begin{smallmatrix}2\\713\end{smallmatrix}) = 1$ car $713 \equiv 1 \bmod 8$. On calcule alors

$$(\begin{smallmatrix}37\\713\end{smallmatrix}) = (\begin{smallmatrix}5\\37\end{smallmatrix})(-1)^{\frac{712.36}{4}} = (\begin{smallmatrix}5\\37\end{smallmatrix})(+1) = (\begin{smallmatrix}2\\5\end{smallmatrix})(-1)^{\frac{4.36}{4}}$$

et $(\begin{smallmatrix}2\\5\end{smallmatrix}) = -1$ et finalement $(\begin{smallmatrix}713\\1009\end{smallmatrix}) = 1$ soit 713 est un carré modulo 1009.

Exercice 2. *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. $p \equiv \pm 1 \bmod 12$).*

Preuve : - On a $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{(p-1)(5-1)}{4}} = \left(\frac{p}{5}\right)$. Or les carrés modulo 5 sont 1 et 4. On obtient ainsi $p \equiv \pm 1 \bmod 5$. Si on impose de plus p impair, soit $p \equiv 1 \bmod 2$, on a donc $p \equiv \pm 1 \bmod 10$.

- De la même façon, on a $\left(\frac{7}{p}\right) = (-1)^{\frac{3(p-1)}{2}}\left(\frac{p}{7}\right)$. Or les carrés modulo 7 sont $1, 2, 4$. Ainsi 7 est un carré modulo p si et seulement si:

$$\begin{cases} p \equiv 1 \bmod 4 \text{ et } p \equiv 1, 2, 4 \bmod 7 \\ \text{ou} \\ p \equiv 3 \bmod 4 \text{ et } p \equiv 3, 5, 6 \bmod 7 \end{cases}$$

ce qui donne $p \equiv \pm 1, \pm 3, \pm 9 \bmod 28$.

- Pour 3, on rassemble les résultats obtenus pour -1 et -3 ce qui donne:

$$\begin{cases} p \equiv 1 \bmod 4 \text{ et } p \equiv 1 \bmod 6 \\ \text{ou} \\ p \equiv 3 \bmod 4 \text{ et } p \equiv 5 \bmod 6 \end{cases}$$

soit $p \equiv \pm 1 \bmod 12$.

□

Autre preuve via les sommes de Gauss (nécessite quelques connaissances sur les corps finis)

Exercice 3. *Soient p et q des nombres premiers impairs distincts. On considère un surcorps K de $\mathbb{Z}/p\mathbb{Z}$ contenant une racine primitive q-ième de l'unité que l'on note w, et on introduit $\tau := \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{x}{q}\right) w^x \in K$. On notera en particulier que la somme précédente à un sens car w^x ne dépend que de la classe de x modulo q.*

(a) En écrivant τ^2 sous la forme $\sum_{x,y \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{xy}{q}\right) w^{x+y}$ et en effectuant le changement de variable $y = xz$, montrer que $\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{\substack{z \in (\mathbb{Z}/q\mathbb{Z})^\times \\ z \neq -1}} -\left(\frac{z}{q}\right)$.

(b) En notant que dans $(\mathbb{Z}/q\mathbb{Z})^\times$, il y a autant de carrés que de non carrés en déduire que $\tau^2 = \left(\frac{-1}{q}\right) q$.

(c) En déduire que $\left(\frac{-1}{q}\right) q$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $\tau^p = \tau$.

(d) En utilisant le calcul de $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$ (cf. le lemme (0.0.2)), montrer alors la loi de réciprocité quadratique (cf. le théorème (0.0.9)), à savoir

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

Preuve : (a) On pose donc $y = xz$ de sorte que $\left(\frac{xy}{q}\right) = \left(\frac{x}{q}\right)^2\left(\frac{z}{q}\right) = \left(\frac{z}{q}\right)$. On obtient alors

$$\tau^2 = \sum_{z \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{z}{q}\right) \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^\times} w^{x(1+z)}$$

En outre on a $\sum_{x=1}^{q-1} w^x = 0$ de sorte que si $z \neq -1$, $\sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times} w^{x(1+z)} = -1$ ce qui permet d'écrire

$$\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{\substack{z\in(\mathbb{Z}/q\mathbb{Z})^\times \\ z\neq -1}} -\left(\frac{z}{q}\right)$$

(b) Comme il y a autant de carrés que de non carrés dans $(\mathbb{Z}/q\mathbb{Z})^\times$, on en déduit que $\sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times}\left(\frac{x}{q}\right) = 0$ d'où le résultat.

(c) Ainsi $\left(\frac{-1}{q}\right)q$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si τ appartient à $\mathbb{Z}/p\mathbb{Z}$, soit si et seulement si $\tau^p = \tau$. En effet on rappelle que $\mathbb{Z}/p\mathbb{Z} \subset K$ est l'ensemble des racines de l'équation $X^p - X$. On peut aussi utiliser la théorie de Galois en disant que $\tau \in K$ appartient à $\mathbb{Z}/p\mathbb{Z}$ si et seulement si il est invariant par tous les éléments du groupe de Galois de l'extension $K : \mathbb{Z}/p\mathbb{Z}$ la propriété découle alors du fait que ce groupe est cyclique engendré par le Frobenius $x \mapsto x^p$.

(d) On calcule alors

$$\begin{aligned}\tau^p &= \textstyle\sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times}\left(\frac{x}{q}\right)w^{px} \\ &= \left(\frac{p}{q}\right)^{-1}\textstyle\sum_{y\in(\mathbb{Z}/q\mathbb{Z})^\times}\left(\frac{y}{q}\right)w^y = \left(\frac{p}{q}\right)\tau\end{aligned}$$

Ainsi $\left(\frac{-1}{q}\right)q$ est un carré si et seulement si $\left(\frac{p}{q}\right) = 1$ i.e. p est un résidu quadratique modulo p. On a alors

$$\begin{aligned}\left(\frac{p}{q}\right) &= \left(\frac{\left(\frac{-1}{q}\right)q}{p}\right) = \left(\frac{(-1)^{(q-1)/2}}{p}\right)\left(\frac{q}{p}\right) \\ &= \left(\frac{-1}{q}\right)^{(q-1)/2}\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{2}}\end{aligned}$$

□