1. Préliminaires

Soit p un nombre premier impair, et $y \in (\mathbf{Z}/p\mathbf{Z})^*$.

1.1 Considérons la permutation involutive $\varphi : x \mapsto y/x$ de $(\mathbf{Z}/p\mathbf{Z})^*$. Si l'on note $O(\varphi)$ l'ensemble de ses orbites, il vient, puisque $O(\varphi)$ est une partition de $(\mathbf{Z}/p\mathbf{Z})^*$:

$$\prod_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x = \prod_{X \in O(\varphi)} \prod_{x \in X} x$$

Chaque orbite de cette involution a un ou deux éléments. Si X est une orbite à deux éléments et $z \in X$, on a $X = \{z, y/z\}$, donc $\prod_{x \in X} x = y$. Il est donc facile d'évaluer le produit précédent si l'on connaît les points fixes de φ. Or x est point fixe de φ si et seulement si $x^2 = y$. Si y n'est pas un carré, toutes les oribites ont donc deux éléments, et il y en a en particulier $(p-1)/2$, d'où :

$$\prod_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x = \prod_{X \in O(\varphi)} y = y^{(p-1)/2}$$

Si maintenant y est un carré, l'équation $x^2 = y$ a au moins une solution z dans $(\mathbf{Z}/p\mathbf{Z})^*$, mais comme elle est de degré 2, elle en a au plus deux dans le corps $\mathbf{Z}/p\mathbf{Z}$. Or $-z$ est également solution, et $z - (-z) = 2z \neq 0$ puisque p est impair. φ a donc les deux points fixes z et $-z$, et par conséquent $(p-3)/2$ orbites à deux éléments, d'où :

$$\prod_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x = z \cdot (-z) \cdot y^{(p-3)/2} = -y^{(p-1)/2}$$

1.2 $1 = 1^2$ est un carré dans $(\mathbf{Z}/p\mathbf{Z})^*$, donc :

$$\prod_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x = -1^{(p-1)/2} = -1$$

Les calculs précédents montrent donc immédiatement que pour tout $y \in (\mathbf{Z}/p\mathbf{Z})^*$, $y^{(p-1)/2}$ vaut 1 si y est un carré et -1 sinon.

2. Généralités

2.1 Soit $\zeta \in \mathbf{C}$ quelconque. Supposons qu'il existe $P \in \mathbf{Q}[X]$ unitaire tel que $P(\zeta) = 0$. Alors le noyau de la surjection canonique $\mathbf{Q}[X] \to \mathbf{Q}[\zeta]$ contient l'idéal non nul (P). En particulier, ladite surjection se factorise par $\mathbf{Q}[X]/(P)$, qui est de dimension finie comme $\mathbf{Q}$-espace vectoriel. $\mathbf{Q}[\zeta]$ est donc a fortiori de dimension finie comme $\mathbf{Q}$-espace vectoriel. Or c'est une $\mathbf{Q}$-algèbre intègre, donc pour tout $x \in \mathbf{Q}[\zeta] - \{0\}$, l'endomorphisme $m_x : y \mapsto xy$ est injectif, donc surjectif, et x est donc inversible. $\mathbf{Q}[\zeta]$ est donc un corps de nombres.

Réciproquement, supposons que $\mathbf{Q}[\zeta]$ soit un corps de nombres, et soit alors n sa dimension. La famille de $n+1$ vecteurs $(1, \zeta, \ldots, \zeta^n)$ est donc liée. Soit $(a_0, \cdots, a_n) \in \mathbf{Q}^n - \{0\}$, tel que $\sum a_k \zeta^k = 0$, et soit et $Q = \sum a_k X^k$. Q est un polynôme non nul de $\mathbf{Q}[X]$ tel que $Q(\zeta) = 0$, donc le quotient P de Q par son coefficient dominant est un polynôme unitaire à coefficients rationnels annulant ζ.

2.2 Soit V un $\mathbf{Q}$ espace vectoriel de dimension finie et f un endomorphisme de V. On suppose qu'il existe un polynôme P unitaire à coefficients entiers annulant f. Écrivons $P = X^d - a_{d-1}X^{d-1} - \cdots - a_0$, et pour tout $x \in V$, notons :

$$M_x = \mathbf{Z}x + \mathbf{Z}f(x) + \cdots + \mathbf{Z}f^{d-1}(x)$$

On a alors pour $0 \leq k < d-1$, on a $f[f^k(x)] = f^{k+1}(x) \in M_x$, et d'autre part :

$$f[f^{d-1}(x)] = f^d(x) = a_0 x + a_1 f(x) + \cdots + a_{d-1} f^{d-1}(x) \in M_x$$

donc par $\mathbf{Z}$-linéarité, il vient que $f(M_x) \subset M_x$. Soit maintenant $(u_1, \cdots, u_k)$ est une famille génératrice de V. Comme f laisse stable chacun des M_{u_i}, il laisse stable le $\mathbf{Z}$-module :

$$M = M_{u_1} + \cdots + M_{u_k} = \mathbf{Z}u_1 + \cdots + \mathbf{Z}f^{d-1}(u_1) + \cdots + \mathbf{Z}u_k + \cdots + \mathbf{Z}f^{d-1}(u_k)$$

qu'ils engendrent. On a donc bien montré que si f est annulé par un polynôme unitaire à coefficients entiers, il laisse stable un sous-$\mathbf{Z}$-module de V de la forme $\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n$, avec $\mathrm{Vect}_{\mathbf{Q}}(v_i) = V$.

Pour obtenir la réciproque, on se propose de démontrer le lemme suivant : tout sous-$\mathbf{Z}$-module de type fini d'un $\mathbf{Q}$-espace vectoriel de dimension n est libre de rang au plus n. Pour $n = 0$ c'est immédiat. On traite à part le cas $n = 1$. Soit M un sous-$\mathbf{Z}$-module de type fini non nul de $\mathbf{Q}$. Il admet donc une famille génératrice de la forme $(a_1/q, \ldots, a_k/q)$ où les a_i sont des entiers non nuls, et q est dans $\mathbf{N}^*$. Il vient alors :

$$qM = \{qx \ / \ x \in M\} = a_1\mathbf{Z} + \cdots + a_k\mathbf{Z} = a\mathbf{Z} \quad \text{avec } a = \mathrm{pgcd}(a_1, \ldots, a_k)$$

Donc $M = \mathbf{Z}a/q$ est bien de rang 1.

On suppose maintenant le résultat vrai en toutes les dimensions inférieures à un certain $n \geq 1$, et l'on se place dans $V = \mathbf{Q}^{n+1}$. On se donne également une forme linéaire $p : V \to \mathbf{Q}$ non nulle, et l'on pose $H = \mathrm{Ker}\, p$. Soit alors M un sous-$\mathbf{Z}$-module de type fini de V, et $M' = M \cap H$. M' est de type fini, car $\mathbf{Z}$ est noethérien, donc M aussi. M' est donc un sous-$\mathbf{Z}$-module de type fini du $\mathbf{Q}$-espace vectoriel H, qui est de dimension n. Il est donc libre de rang $r \leq n$. Si $M = M'$, c'est donc terminé. Sinon, le sous-$\mathbf{Z}$-module de type fini $p(M)$ de $\mathbf{Q}$ est non nul. Il s'écrit donc $\mathbf{Z}e$ pour un certain $e \in \mathbf{Q}^*$. Soit alors une base de M', et $u \in M$ tel que $p(u) = e$. Notons que $p(mu) = 0$ si et seulement si $m = 0$, de sorte que $M' \cap \mathbf{Z}u = 0$. D'autre part, si x est un élément quelconque de M, et $p(x) = me$, on a $p(x - mu) = 0$, donc $x \in M' \oplus \mathbf{Z}u$. $M = M' \oplus \mathbf{Z}u$ est donc bien libre de rang $r + 1 \leq n + 1$.

Revenons alors à notre problème. On suppose que f laisse stable $M = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n$ pour une certaine famille $(v_1, \ldots, v_n)$ qui engendre V. On vient de voir que M était libre de rang $d \leq \dim V$. Soit $(e_1, \ldots, e_d)$ une base de M comme $\mathbf{Z}$-module. On a $\mathrm{Vect}_{\mathbf{Q}}(e_i)_{1 \leq i \leq d} = \mathrm{Vect}_{\mathbf{Q}}(v_i)_{1 \leq i \leq n} = V$, donc on a en fait $d = \dim V$, et $(e_1, \ldots, e_d)$ est une base de V. Le fait que f laisse stable M signifie par conséquent que la matrice A de f dans la base $(e_1, \ldots, e_d)$ est à coefficients entiers, donc il en est de même de son polynôme caractéristique : $P = \det(X - A) \in \mathbf{Z}[X]$, et P est unitaire. Le théorème de Cayley-Hamilton permet de conclure qu'il existe bien un polynôme unitaire à coefficients entiers qui annule f.

Remarquons que l'on a démontré au passage un résultat plus fort : un endomorphisme vérifie les conditions équivalentes qui précèdent (on dit qu'il est *entier*) si et seulement si son polynôme caractéristique est à coefficients entiers.

2.3 Soient f et g deux endomorphismes entiers de V qui commutent, et $P = X^p - a_{p-1}X^{p-1} - \cdots - a_0$ et $Q = X^q - b_{q-1}X^{q-1} - \cdots - b_0$ des polynômes unitaires à coefficients entiers qui annulent respectivement f et g. Pour tout $x \in V$, on pose alors :

$$M_x = \mathbf{Z}x_{0,0} + \cdots + \mathbf{Z}x_{0,q-1} + \cdots + \mathbf{Z}x_{p-1,0} + \cdots + \mathbf{Z}x_{p-1,q-1} \quad \text{avec } x_{i,j} = f^i g^j(x)$$

Pour tout (i, j), on a :

$$f(x_{i,j}) = f^{i+1}g^j(x) = \begin{cases} x_{i+1,j} & \text{si } i < p-1 \\ \sum_{k=0}^{p-1} a_k x_{k,j} & \text{si } i = p-1 \end{cases}$$

donc f laisse stable M_x. Comme f et g commutent, ils jouent le même rôle dans les définitions précédentes, et il vient donc de même que M_x est stable par g. Si $(u_1, \ldots, u_k)$ engendre V, f et g laissent donc stable le $\mathbf{Z}$-module de type fini $M = M_{u_1} + \cdots + M_{u_k}$ qui contient un système générateur de V. Par conséquent, $f + g$ et $f \circ g = g \circ f$ laissent également stable M, et sont donc entiers.

Ce résultat ne subsiste pas en général si l'on ne suppose plus que f et g commutent. Prenons par exemple $V = \mathbf{Q}^2$, et pour f et g les endomorphismes dont les matrices dans la base canonique sont respectivement :

$$A = \begin{bmatrix} 0 & 1/2 \\ 2 & 0 \end{bmatrix} \quad \text{et} \quad B = \begin{bmatrix} 1 & 1/3 \\ 0 & 1 \end{bmatrix}$$

f et g sont bien entiers, puisqu'ils ont pour polynômes caractéristiques respectifs $X^2 - 1$ et $X^2 - 2X + 1$. En revanche, on a :

$$A + B = \begin{bmatrix} 1 & 5/6 \\ 2 & 1 \end{bmatrix} \quad \text{et} \quad AB = \begin{bmatrix} 0 & 1/2 \\ 2 & 2/3 \end{bmatrix}$$

Par conséquent $\det(f+g) = -2/3 \notin \mathbf{Z}$, et $\operatorname{tr}(fg) = 2/3 \notin \mathbf{Z}$. Les endomorphismes $f+g$ et fg ont donc des polynômes caractéristiques à coefficients non tous entiers, donc ils ne sont pas entiers.

2.4 Soit K un corps de nombres et n sa dimension comme $\mathbf{Q}$-espace vectoriel. Pour tout $r \in \mathbf{Q}$, on a simplement $m_r = r\,\mathrm{id}$. En particulier, si $r \in \mathbf{Z}$, m_r est annulé par le polynôme unitaire à coefficients entiers $X - r$, donc $r \in \mathcal{O}_K$. Réciproquement, si $r \in \mathcal{O}_K \cap \mathbf{Q}$, on doit avoir $\det m_r = r^n \in \mathbf{Z}$, donc $r \in \mathbf{Z}$. Finalement, on a $\mathcal{O}_K \cap \mathbf{Q} = \mathbf{Z}$.

3. Entiers des corps quadratiques

Soit $D \in \mathbf{Q}$ qui n'est pas le carré d'un entier. On va considérer le corps $\mathbf{Q}[\sqrt{D}]$. On note σ l'automorphisme de ce corps défini par $\sigma(x + y\sqrt{D}) = x - y\sqrt{D}$.

3.1 Soit φ un automorphisme de corps de $\mathbf{Q}[\sqrt{D}]$. On a $\varphi(1) = 1$, donc $\varphi(m) = m$ pour tout $m \in \mathbf{Z}$, puis $\varphi(p/q) = p/q$ pour tout $p/q \in \mathbf{Q}$. En outre, $x = \varphi(\sqrt{D})$ vérifie $x^2 = D$, donc $x = \varepsilon\sqrt{D}$, avec $\varepsilon = \pm 1$. On a donc pour tout $a + b\sqrt{D} \in \mathbf{Q}[\sqrt{D}]$:

$$\varphi(a + b\sqrt{D}) = a + bx = a + \varepsilon b\sqrt{D}$$

Donc φ est l'identité ou σ selon le signe de ε.

3.2 Soit $D' \in \mathbf{Q}^*$ tel que $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{D'}]$. Alors en particulier, $\mathbf{Q}[\sqrt{D'}] \neq \mathbf{Q}$, donc D' n'est pas le carré d'un entier. Il existe de plus $(a, b) \in \mathbf{Q}^2$ tel que $\sqrt{D'} = a + b\sqrt{D}$. En élevant cette relation au carré, il vient :

$$D' = (a^2 + bD^2) + 2ab\sqrt{D}$$

donc en égalisant les composantes sur la base $(1, \sqrt{D})$, il vient $ab = 0$. Or si b était nul, on aurait $\sqrt{D'} = a$, ce qui, on l'a vu, est impossible. Donc $a = 0$, et $D/D' = (1/b)^2$ est bien le carré d'un rationnel.

Réciproquement, si $D' = k^2 D$ pour un certain $k \in \mathbf{Q}$, $\mathbf{Q}[\sqrt{D}]$ et $\mathbf{Q}[\sqrt{D'}]$ sont clairement égaux, puisque alors, pour tout $(a, b) \in \mathbf{Q}^2$, on a $a + b\sqrt{D} = a + kb\sqrt{D'}$.

3.3 Soit $D = \varepsilon p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ la décomposition de D en facteurs premiers (avec $\varepsilon = \pm 1$, les p_i des nombres premiers distincts, et les α_i dans $\mathbf{Z}$). On pose pour tout i, $\alpha_i = 2\beta_i + \eta_i$, avec $\eta_i \in \{0, 1\}$, $d = \varepsilon p_1^{\eta_1} \cdots p_n^{\eta_n}$, $r = p_1^{\beta_1} \cdots p_n^{\beta_n}$. d est alors un entier sans facteur carré, et l'on a $D = k^2 d$. En particulier, $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{d}]$.

Supposons que d' soit un entier sans facteur carré tel que $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{d'}]$. D'après ce qui précède, il existe donc $k \in \mathbf{Q}$ tel que $d' = k^2 d$. Si l'on écrit d sous forme de fraction irréductible p/q, il vient $q^2 d' = p^2 d$. En particulier, comme p^2 est premier à q^2 il divise d', qui est sans facteur carré, donc $p^2 = 1$. De même, q^2 divise d donc vaut 1, et l'on a $d = d'$. Par conséquent, il existe un et un seul entier d sans facteur carré vérifiant $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{d}]$.

3.4 Soit K un sous-corps de $\mathbf{C}$ de dimension 2 comme $\mathbf{Q}$-espace vectoriel, et soit $\alpha \in K - \mathbf{Q}$. $(1, \alpha)$ est alors une base du $\mathbf{Q}$-espace vectoriel K, et en particulier il existe $(u, v) \in \mathbf{Q}^2$ tel que $\alpha^2 + u\alpha + v = 0$. Posons $D = u^2 - 4v$. Il existe alors $\varepsilon \in \{-1, 1\}$ tel que $\alpha = [-u + \varepsilon\sqrt{D}]/2$. En particulier, comme α est irrationnel, D n'est pas le carré d'un rationnel. De plus, $\sqrt{D} = \varepsilon u + 2\varepsilon \cdot \alpha \in K$, d'où $\mathbf{Q}[\sqrt{D}] \subset K$. Or $\mathbf{Q}[\sqrt{D}]$ et K sont des $\mathbf{Q}$-espaces vectoriels de même dimension, d'où $K = \mathbf{Q}[\sqrt{D}]$. K est donc bien un corps quadratique.
On fixe alors $d \in \mathbf{Z}$ sans facteur carré tel que $K = \mathbf{Q}[\sqrt{d}]$.

3.5 Soit $x = a + b\sqrt{D} \in K$ quelconque. La matrice de m_x dans la base $(1, \sqrt{D})$ s'écrit :

$$\mathcal{M}(m_x) = \begin{bmatrix} a & Db \\ b & a \end{bmatrix}$$

donc le polynôme caractéristique de m_x est $X^2 - 2aX + (a^2 - Db^2)$. On a de plus :

$$x + \sigma(x) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a \quad \text{et} \quad x\sigma(x) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

Or $x \in \mathcal{O}_K$ si et seulement si le polynôme caractéristique de m_x est à coefficients entiers, ce qui donne bien le résultat.

3.6 Soit $\omega \in \mathcal{O}_K$ défini par :

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{sinon} \end{cases}$$

Comme $\mathcal{O}_K$ est un anneau contenant $\mathbf{Z}$, $\varphi : (x, y) \mapsto x + y\omega$ définit bien une application $\mathbf{Z}^2 \to \mathcal{O}_K$, qui est clairement un morphisme de groupes abéliens. Dans tous les cas, ω est irrationnel, donc il n'existe pas de $(x, y) \in \mathbf{Z}^2 - \{0\}$ tel que $x + y\omega = 0$, et φ est injectif. Montrons qu'il est surjectif. Soit $z \in \mathcal{O}_K$ quelconque. Comme $\omega \notin \mathbf{Q}$, $(1, \omega)$ est une base de K, il existe $(u, v) \in \mathbf{Q}^2$ tel que $z = u + v\omega$. Notons T et N les entiers $z + \sigma(z)$ et $z\sigma(z)$.
Si $d \not\equiv 1 \pmod 4$, on a $T = 2u$ et $N = u^2 - dv^2$, d'où $T^2 - 4N = 4dv^2 = (2v)^2 d \in \mathbf{Z}$. Comme d est sans facteur carré, il en résulte que $2v \in \mathbf{Z}$. Si $v \notin \mathbf{Q}$, $2v$ est impair, donc $(2v)^2 = 1$, et l'on a donc $d \equiv T^2 - 4N \equiv T^2 \pmod 4$. Puisque $d \not\equiv 1 \pmod 4$, T est donc pair, d'où $d \equiv 0 \pmod 4$, ce qui est impossible, puisque d est sans facteur carré. v est donc entier, et $u^2 = N + dv^2$ aussi, donc $(u, v) \in \mathbf{Z}$ et $z = \varphi(u, v)$.
Si maintenant $d \equiv 1 \pmod 4$, on a $T = 2u + v$ et $N = u^2 + uv + v^2 \cdot (1 - d)/4$. Alors $T^2 - 4N = dv^2 \in \mathbf{Z}$, d'où $v \in \mathbf{Z}$. Donc $2u = T - v \in \mathbf{Z}$, et :

$$0 \equiv 4N \equiv (2u)^2 + 4uv + v^2 \cdot (1 - d) \equiv (T - v)^2 + 2v(T - v) + 0 \equiv T^2 - 2v^2 \pmod 4$$

donc T est pair et $u = T/2 \in \mathbf{Z}$. D'où le résultat.

4. Un calcul analytique de τ_n

Soit $n \geq 1$ fixé. Pour $k = 0, \ldots, n-1$, on définit $f_k : [0, 1] \to \mathbf{C},\ t \mapsto \exp(2i\pi(t + k)^2/n)$, et l'on pose $f = f_0 + \cdots + f_{n-1}$.

4.1 On a :

$$f(0) = \sum_{k=0}^{n-1} \exp(2i\pi k^2/n) = \tau_n \quad \text{et} \quad f(1) = \sum_{k=0}^{n-1} \exp(2i\pi(k+1)^2/n) = \tau_n$$

En particulier, $f(0) = f(1)$, donc il existe une unique fonction $\tilde{f} : \mathbf{R} \to \mathbf{C}$ continue 1-périodique et telle que $\tilde{f}|_{[0,1]} = f$. $\tilde{f}$ est de plus C^1 par morceaux, donc elle est égale

à sa série de Fourier (au sens habituel de la convergence des séries de Fourier). On a autrement dit pour tout $x \in \mathbf{R}$:

$$\tilde{f}(x) = \lim_{k\to\infty} \sum_{m=-k}^{k} c_m(\tilde{f}) e^{2i\pi mx}$$

où l'on a posé :

$$c_m(\tilde{f}) = \int_0^1 \tilde{f}(t) e^{-2i\pi mt} dt = \int_0^1 f(t) \exp(-2i\pi mt) dt$$

Si l'on chosit en particulier $x = 0$, il vient que la suite de terme général :

$$u_k = \sum_{m=-k}^{k} c_m(\tilde{f}) = \sum_{m=-k}^{k} \int_0^1 f(t) \exp(-2i\pi mt) dt$$

converge vers $\tilde{f}(0) = f(0) = \tau_n$.

4.2 Soit $g : \mathbf{R} \to \mathbf{C}$ la fonction $x \mapsto \exp(2i\pi t^2/n)$. On a, pour tout $x \geq 1$:

$$\int_{-x}^{x} g(t)dt = \int_{-1}^{1} g(t)dt + 2\int_1^x g(t)dt$$

Or on peut effectuer une intégration par parties dans le dernière intégrale :

$$\begin{aligned}
\int_1^x g(t) &= \frac{n}{4i\pi} \int_1^x \frac{1}{t} \cdot \left[\frac{4i\pi t}{n} \exp\left(\frac{2i\pi t^2}{n} \right) \right] dt \\
\int_1^x g(t) &= \frac{n}{4i\pi} \left[\frac{1}{t} \exp\left(\frac{2i\pi t^2}{n} \right) \right]_1^x + \frac{n}{4i\pi} \int_1^x \frac{1}{t^2} \exp\left(\frac{2i\pi t^2}{n} \right) dt \\
\int_1^x g(t) &= -\frac{n}{4i\pi} g(1) + \frac{n}{4i\pi} \frac{g(x)}{x} + \frac{n}{4i\pi} \int_1^x \frac{g(t)}{t^2} dt
\end{aligned}$$

Comme $t \mapsto g(t)/t^2$ est intégrable sur $[1, +\infty[$, on voit donc que $x \mapsto \int_1^x g(t)dt$ a une limite dans $\mathbf{C}$ quand x tend vers $+\infty$. Il en est donc de même de $x \mapsto \int_{-x}^{x} g(t)dt$. On pose :

$$I_n = \lim_{x\to+\infty} \int_{-x}^{x} g(t)dt$$

Notons que I_n est dans $\mathbf{C}$, mais en fait pas dans $\mathbf{R}$, contrairement à ce que suggère l'énoncé.

4.3 En effectuant le changement de variable $u = t\sqrt{n}$, il vient pour tout $x \geq 0$

$$\int_{-x}^{x} \exp\left(\frac{2i\pi t^2}{n} \right) dt = \sqrt{n} \int_{-x\sqrt{n}}^{x\sqrt{n}} \exp(2i\pi u) du$$

d'où, en faisant tendre x vers $+\infty$:

$$I_n = \sqrt{n} I_1$$

4.4 Pour tout $m \in \mathbf{Z}$, on a :

$$\begin{aligned}
\int_0^1 f(t) \exp(-2i\pi mt) dt &= \sum_{j=0}^{n-1} \int_0^1 \exp\left(\frac{2i\pi(t+j)^2}{n} \right) \exp(-2i\pi mt) dt \\
\int_0^1 f(t) \exp(-2i\pi mt) dt &= \sum_{j=0}^{n-1} \int_j^{j+1} \exp\left(\frac{2i\pi u^2}{n} \right) \exp(-2i\pi m(u-j)) du \\
\int_0^1 f(t) \exp(-2i\pi mt) dt &= \int_0^n \exp\left(\frac{2i\pi t^2}{n} \right) \exp(-2i\pi mt) dt
\end{aligned}$$

Or, en faisant $t = u + mn/2$ dans la dernière intégrale, il vient :

$$\begin{aligned}\int_0^1 f(t)\exp(-2i\pi mt)dt &= \int_{-mn/2}^{n-mn/2} \exp\left(\frac{2i\pi u^2}{n} + 2i\pi mu + \frac{i\pi m^2 n}{2}\right) \\ &\quad \times \exp(-2i\pi mu - i\pi m^2 n)du \\ \int_0^1 f(t)\exp(-2i\pi mt)dt &= \int_{-mn/2}^{n-mn/2} (-i)^{m^2 n} g(t)dt\end{aligned}$$

On a par conséquent pour tout $k \in \mathbf{N}^*$:

$$u_{2k} = \sum_{m=-2k}^{2k} \int_{-mn/2}^{n-mn/2} (-i)^{m^2 n} g(t)dt$$

d'où, en séparant les termes correspondant à m pair et m impair il vient :

$$\begin{aligned}u_{2k} &= \sum_{p=-k}^{k} \int_{-(2p)n/2}^{n-(2p)n/2} (-i)^{4p^2 n} g(t)dt + \sum_{q=-k}^{k-1} \int_{-(2q+1)n/2}^{n-(2q+1)n/2} (-i)^{(4q^2+4q+1)n} g(t)dt \\ u_{2k} &= \sum_{p=-k}^{k} \int_{-pn}^{-(p-1)n} g(t)dt + \sum_{q=-k}^{k-1} \int_{-n/2-qn}^{-n/2-(q-1)n} g(t)dt \\ u_{2k} &= \int_{-kn}^{(k+1)n} g(t)dt + (-i)^n \int_{-(k-1/2)n}^{(k-1/2)n} g(t)dt \\ u_{2k} &= \int_{kn}^{(k+1)n} g(t)dt + \int_{-kn}^{kn} g(t)dt + (-i)^n \int_{-(k-1/2)n}^{(k-1/2)n} g(t)dt\end{aligned}$$

Comme $x \mapsto \int_1^x g(t)dt$ a une limite finie en $+\infty$, on a :

$$\lim_{k\to\infty} \int_{kn}^{kn+n} g(t)dt = 0$$

donc en faisant tendre k vers $+\infty$ dans l'expression obtenue pour u_{2k}, il vient :

$$\tau_n = (1 + (-i)^n)I_n = (1 + i^{-n})I_n$$

En particulier, $1 = \tau_1 = (1 + i^{-1})I_1 = (1 + i^{-1})I_n/\sqrt{n}$, donc :

$$\tau_n = \frac{1 + i^{-n}}{1 + i^{-1}}\sqrt{n}$$

4.5 Soit K un corps quadratique, et $d \in \mathbf{Z}$ tel que $K = \mathbf{Q}[\sqrt{d}]$. Si l'on note $\zeta = \exp(2i\pi/d)$, on a d'après ce qui précède :

$$\sqrt{d} = \frac{1 + i^{-1}}{1 + i^{-d}} \sum_{x\in(\mathbf{Z}/d\mathbf{Z})} \zeta^{x^2}$$

Considérons alors $\xi = \exp(i\pi/2d)$, racine primitive $4d$-ième de l'unité. On a $\zeta = \xi^4$, et $i = \xi^d$, donc :

$$\sqrt{d} = \frac{1 + \xi^{-d}}{1 + \xi^{-d^2}} \sum_{x\in(\mathbf{Z}/d\mathbf{Z})} \xi^{4x^2} \in \mathbf{Q}[\xi]$$

Il en résulte que ξ est une racine de l'unité telle que $K \subset \mathbf{Q}[\xi]$.

5. Un calcul algébrique de τ_n

Soit $n > 1$ un entier impair, et $\zeta = \exp(2i\pi/n)$. On note V le $\mathbf{C}$-espace vectoriel des fonctions de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{C}$, et φ l'endomorphisme de V qui à toute fonction $f \in V$ associe $\varphi(f) \in V$ définie par :

$$\varphi(f)(x) = \sum_{y \in \mathbf{Z}/n\mathbf{Z}} f(y)\zeta^{xy}$$

5.1 Soit $f \in V$. On a, pour tout $x \in \mathbf{Z}/n\mathbf{Z}$:

$$\begin{aligned}
\varphi \circ \varphi(f)(x) &= \sum_{y \in \mathbf{Z}/n\mathbf{Z}} \left[\sum_{z \in \mathbf{Z}/n\mathbf{Z}} f(z)\zeta^{yz} \right] \zeta^{xy} \\
\varphi \circ \varphi(f)(x) &= \sum_{(y,z) \in (\mathbf{Z}/n\mathbf{Z})^2} f(z)\zeta^{(x+z)y} \\
\varphi \circ \varphi(f)(x) &= \sum_{(a,y) \in (\mathbf{Z}/n\mathbf{Z})^2} f(a-x)\zeta^{ay} \\
\varphi \circ \varphi(f)(x) &= \sum_{a \in (\mathbf{Z}/n\mathbf{Z})^2} f(a-x) \sum_{y \in \mathbf{Z}/n\mathbf{Z}} (\zeta^a)^y
\end{aligned}$$

Soit $a \in \mathbf{Z}/n\mathbf{Z}$ non nul, et $d > 1$ l'ordre de ζ^a dans $\mathbf{C}^*$. On a alors :

$$\begin{aligned}
\sum_{y \in \mathbf{Z}/n\mathbf{Z}} (\zeta^a)^y &= \sum_{u \in \mathbf{Z}/d\mathbf{Z}} \sum_{\substack{y \in \mathbf{Z}/n\mathbf{Z} \\ y \equiv u \pmod d}} (\zeta^a)^u \\
\sum_{y \in \mathbf{Z}/n\mathbf{Z}} (\zeta^a)^y &= \frac{n}{d} \sum_{u \in \mathbf{Z}/d\mathbf{Z}} (\zeta^a)^u = 0
\end{aligned}$$

puisque $\sum_{u \in \mathbf{Z}/d\mathbf{Z}} (\zeta^a)^u$ n'est autre que la somme des racines d-ièmes de l'unité dans $\mathbf{C}$, qui est nulle (étant au signe près le coefficient de X^{d-1} dans le polynôme $X^d - 1$). Il en résulte que pour tout $x \in \mathbf{Z}/n\mathbf{Z}$:

$$\varphi \circ \varphi(f)(x) = f(0-x) \sum_{y \in \mathbf{Z}/n\mathbf{Z}} (\zeta^0)^y = nf(-x)$$

5.2 Il résulte en particulier de ce qui précède que $\varphi^4 = n^2 \,\mathrm{id}_V$, donc φ est annulée par le polynôme scindé à racines simples $X^4 - n^2$, et est donc diagonalisable. Par conséquent, φ^2 est diagonalisable, et ses valeurs propres sont contenues dans l'ensemble $\{-n, n\}$. Les vecteurs propres associées à la valeurs propres n (resp. $-n$) sont les $f \in V$ telles que pour tout x, $nf(x) = nf(-x)$ (resp. $-nf(x) = nf(-x)$), c'est-à-dire les fonctions paires (resp. impaires). Donc si l'on note P et I les sous-espaces supplémentaires de V formés par les fonctions paires et impaires, $\varphi \circ \varphi$ se décompose en $n \,\mathrm{id}_P \oplus (-n) \,\mathrm{id}_I$ sur la somme $P \oplus I$.

5.3 Si pour $x \in \mathbf{Z}/n\mathbf{Z}$ on note $f_x \in V$ la fonction valant 1 en x et 0 ailleurs, $(f_x)_{x \in \mathbf{Z}/n\mathbf{Z}}$ est une base de V, et dans cette base :

$$\varphi(f_x) = \sum_{z \in \mathbf{Z}/n\mathbf{Z}} \varphi(f_x)(z) f_z = \sum_{(y,z) \in (\mathbf{Z}/n\mathbf{Z})^2} f_x(y)\zeta^{zy} f_z = \sum_{z \in \mathbf{Z}/n\mathbf{Z}} \zeta^{xz} f_z$$

donc on a bien $\mathrm{tr}\,\varphi = \tau_n$.

Montrons que $|\tau_n| = \sqrt{n}$. En effet :

$$\begin{aligned}
\tau_n\overline{\tau_n} &= \left(\sum_{x\in\mathbf{Z}/n\mathbf{Z}} \zeta^{x^2}\right)\left(\sum_{y\in\mathbf{Z}/n\mathbf{Z}} \zeta^{-y^2}\right)\\
|\tau_n|^2 &= \sum_{(x,y)\in(\mathbf{Z}/n\mathbf{Z})^2} \zeta^{(x-y)(x+y)}\\
|\tau_n|^2 &= \sum_{(a,y)\in(\mathbf{Z}/n\mathbf{Z})^2} \zeta^{a(2y+a)}\\
|\tau_n|^2 &= \sum_{(a,z)\in(\mathbf{Z}/n\mathbf{Z})^2} \zeta^{az}
\end{aligned}$$

car, n étant impair, $y \mapsto 2y + u$ est une permutation de $\mathbf{Z}/n\mathbf{Z}$. Il vient alors finalement :

$$|\tau_n|^2 = n + \sum_{a\in(\mathbf{Z}/n\mathbf{Z})-\{0\}} \sum_{z\in\mathbf{Z}/n\mathbf{Z}} (\zeta^a)^z = n$$

5.4 Soient a, b, c, d les multiplicités respectives des valeurs propres $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$ et $-i\sqrt{n}$ de φ, et A, B, C, D les sous-espaces propres correspondants. On a donc $a = \dim A$, etc. Alors pour tout $f \in A \oplus B$, on a $\varphi^2(f) = (\pm\sqrt{n})^2 f = nf$, donc $A \oplus B \subset P$ et de même $C \oplus D \subset I$. Comme $P \oplus I = V = A \oplus B \oplus C \oplus D$, ces inclusions sont des égalités, d'où :

$$a + b = \dim P = \frac{n+1}{2} \quad \text{et} \quad c + d = \dim I = n - \dim P = \frac{n-1}{2}$$

En effet, une base de P est donnée par les $(n+1)/2$ fonctions (f_k+f_{-k}), $0 \le k \le (n-1)/2$. Par ailleurs, on a $\tau_n = \operatorname{tr}\varphi = a\sqrt{n}+b(-\sqrt{n})+c(i\sqrt{n})+d(-i\sqrt{n}) = [(a-b)+i(c-d)]\sqrt{n}$. En comparant les carrés des modules, il vient par conséquent :

$$(a-b)^2 + (c-d)^2 = 1$$

5.5 On a vu que la matrice de φ dans la base $(f_j)_{j\in\mathbf{Z}/n\mathbf{Z}}$ était simplement la matrice de Vandermonde $[\zeta^{ij}]_{(i,j)\in(\mathbf{Z}/n\mathbf{Z})^2}$. On a donc, en notant $\xi = \exp(i\pi/n)$:

$$\begin{aligned}
\det\varphi &= \prod_{0\le j<k\le n-1} (\zeta^k - \zeta^j)\\
\det\varphi &= \prod_{0\le j<k\le n-1} \xi^{k+j}(\xi^{k-j} - \xi^{j-k})\\
\det\varphi &= \prod_{0\le j<k\le n-1} \xi^{k+j}\left(2i\sin\frac{(k-j)i\pi}{n}\right)\\
\det\varphi &= i^{n(n-1)/2}\xi^m \prod_{0\le j<k\le n-1} \xi^{k+j}\left(2\sin\frac{(k-j)i\pi}{n}\right)
\end{aligned}$$

où l'on a posé :

$$m = \sum_{0\le j<k\le n-1} j+k = \sum_{k=1}^{n-1} \frac{k(k-1)}{2} + k^2 = \frac{1}{2}\left(\frac{3\cdot n(n-1)(2n-1}{6} - \frac{n(n-1)}{2}\right)$$

c'est-à-dire $m = n(n-1)^2/2$. Comme dans l'expression précédente de $\det\varphi$ chacun des sinus est positif, on a $\det\varphi = |\det\varphi|e^{i\theta}$ avec :

$$\theta = \frac{n(n-1)}{2}\frac{\pi}{2} + \frac{n(n-1)^2}{2}\frac{\pi}{n} = \frac{(n-1)(3n-2)}{2}\frac{\pi}{2}$$

Or $\det\varphi = \sqrt{n}^a(-\sqrt{n})^b(i\sqrt{n})^c(-i\sqrt{n})^d = i^{2b+c-d}\sqrt{n}^n$, d'où :

$$2b+c-d \equiv (n-1)(3n-2)/2 \pmod 2$$

Supposons $n = 4k+1$. Alors comme $a+b = (n+1)/2 = 2k+1$ est impair, on doit avoir $a \neq b$. L'équation $(a-b)^2+(c-d)^2 = 1$ impose donc $c = d$ et $a-b = \pm 1$. En particulier, on a $\{a,b\} = \{k, k+1\}$. Or :

$$2b \equiv 2b+c-d \equiv \frac{4k(12k+3-2)}{2} \equiv 2k(12k+1) \equiv 2k \pmod 4$$

donc b a la parité de k, d'où $b = k$ et $a = k+1$. D'autre part, comme $c+d = (n-1)/2$, on a $c = d = k$. On a finalement montré :

$$a = \frac{n+3}{4} \quad \text{et} \quad b = c = d = \frac{n-1}{4} \quad \text{quand } n \equiv 1 \pmod 4$$

Supposons maintenant $n = 4k+3$. Alors $c+d = (n-1)/2 = 2k+1$ est impair, donc $c \neq d$. Il vient donc cette fois $a = b = k+1$ et $\{c,d\} = \{k, k+1\}$. Or :

$$c-d \equiv \frac{(n-1)(3n-2)}{2} - 2b \equiv (2k+1)(12k+9-2) - 2k - 2 \equiv (-1)(2k+1) - 2k - 2 \equiv 1 \pmod 4$$

donc $c = k+1$ et $d = k$. Finalement :

$$a = b = c = \frac{n+1}{4} \quad \text{et} \quad d = \frac{n-3}{4} \quad \text{quand } n \equiv 3 \pmod 4$$

5.6 Il vient d'après ce qui précède :

$$\tau_n = [(a-b)+i(c-d)]\sqrt{n} = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 \pmod 4 \\ i\sqrt{n} & \text{si } n \equiv 3 \pmod 4 \end{cases}$$

Autrement dit, pour tout n, $\tau_n = \sqrt{(-1)^{(n-1)/2}n}$.

6. Réciprocité quadratique

On considère deux nombres premiers impairs p, q. On note L le corps de nombre $\mathbf{Q}[\zeta]$, $\zeta = \exp(2i\pi/p)$, et K le sous-corps quadratique $\mathbf{Q}[\tau_p]$. On note $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre.

6.1 Soit $x \in \mathcal{O}_L \cap K$ quelconque, et $P \in \mathbf{Z}[X]$ un polynôme unitaire annulateur de l'endomorphisme m_x de multiplication par x dans L. m_x laisse stable le sous-espace K de L, et l'endomorphise induit est la multiplication par x dans K. Or P annule encore cet endomorphisme, donc $x \in \mathcal{O}_K$. Réciproquement, soit $x \in \mathcal{O}_K$ quelconque, $P \in \mathbf{Z}[X]$ un polynôme unitaire annulateur de la multiplication par x dans K, $(\alpha_1, \ldots, \alpha_r)$ une base du K-espace vectoriel L, et m_x la multiplication par x dans L. Pour tout $u \in L$, si $u = \sum_{i=1}^r u_i\alpha_i$, il vient :

$$P(m_x)(u) = \sum_{i=1}^r P(m_x)(u_i)\alpha_i = 0$$

donc $x \in \mathcal{O}_L$. On a donc bien $\mathcal{O}_L \cap K = \mathcal{O}_K$.

6.2 On considère l'anneau quotient $A = \mathcal{O}_L/q\mathcal{O}_L$. Dans A, $q = 0$, donc pour tout $(x,y) \in A^2$, $(x+y)^q = x^q + y^q$. Par conséquent, $x \mapsto x^q$ est un endomorphisme de A. Notons en outre que, comme $\zeta^p - 1 = 0$, $\zeta \in \mathcal{O}_L$. Si l'on note $a \mapsto [a]$ la surjection canonique $\mathcal{O}_L \to A$, il vient donc :

$$[\tau_p^q] = \left(\sum_{x \in (\mathbf{Z}/p\mathbf{Z})} [\zeta]^{x^2}\right)^q = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})} [\zeta]^{qx^2}$$

$q \not\equiv 0 \pmod{p}$, donc si q est un carré modulo p, il existe $a \in (\mathbf{Z}/p\mathbf{Z})^*$ tel que $q = a^2$, et alors :

$$[\tau_p^q] = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})} [\zeta]^{(ax)^2} = [\tau_p] = \left[\left(\frac{q}{p}\right)\tau_p\right]$$

Sinon, soit C (resp. N) l'ensemble des carrés (resp. non-carrés) de $(\mathbf{Z}/p\mathbf{Z})^*$. $x \mapsto qx$ est alors une permutation de $(\mathbf{Z}/p\mathbf{Z})^*$ qui échange C et N. Or on a :

$$\tau_p = 1 + \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \zeta^{x^2} = 1 + 2\sum_{x \in C} \zeta^x$$

Il vient donc :

$$[\tau_p^q] = [1] + 2\sum_{x \in C} [\zeta]^{qx} = [1] + 2\sum_{x \in N} [\zeta]^x$$

Or $\sum_{x\in C} \zeta^x + \sum_{x \in N} \zeta^x = -1 + \sum_{x \in (\mathbf{Z}/p\mathbf{Z})} \zeta^x = -1$. Donc :

$$[\tau_p^q] = [1] + 2\left[-1 - \sum_{x \in C} \zeta^x\right] = [-\tau_p] = \left[\left(\frac{q}{p}\right)\tau_p\right]$$

Donc dans tous les cas, on a montré :

$$\left[\tau_p^q - \left(\frac{q}{p}\right)\tau_p\right] = 0 \quad \text{c'est-à-dire} \quad \tau_p^q - \left(\frac{q}{p}\right)\tau_p \in q\mathcal{O}_L$$

Comme en outre $\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in K$, il vient bien :

$$\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in q\mathcal{O}_L \cap K = q\mathcal{O}_K$$

6.3 Soit $\omega \in \mathcal{O}_K$ défini comme en 3.6, et $n \in \mathbf{Z}$ tel que $n\tau_p \in q\mathcal{O}_K$. On note $(a, b) \in \mathbf{Z}^2$ l'unique couple tel que $n\tau_p = q(a+b\omega)$. Si $p \equiv 1 \pmod 4$, on a $\tau_p = \sqrt{p}$ et $\omega = (1+\sqrt{p})/2$, donc il vient $n(-1+2\omega) = q(a+b\omega)$. Par conséquent, $n = -qa$ est divisible par q. Si maintenant $p \equiv 3 \pmod 4$, on a $\tau_p = \sqrt{-p}$ et $\omega = (1+\sqrt{-p})/2$, donc on a encore $n(-1+2\omega) = q(a+b\omega)$ et q divise n.

6.4 On a :

$$\tau_p^q = \left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^q = \left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^{2\frac{q-1}{2}}\tau_p = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}\tau_p$$

Donc on a $n\tau_p \in q\mathcal{O}_K$ où n est l'entier :

$$n = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)$$

D'après ce qui précède, il vient donc :

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod q$$

d'où :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod q$$

Comme $q > 2$, l'égalité est donc également vraie dans $\mathbf{Z}$, d'où le résultat.

6.5 Soit $\psi : \mathbf{Z}^2 \to \mathbf{Z}/pq\mathbf{Z}$ le morphisme de groupes défini par $\psi(x,y) = (xp+yq) \bmod pq$. Soit $(x,y) \in \operatorname{Ker}\psi$. Il existe $k \in \mathbf{Z}$ tel que $xp+yq = kpq$. On a alors $xp \equiv 0 \pmod q$ et $yq \equiv 0 \pmod p$, d'où $q|x$ et $p|y$. Réciproquement, pour tout $(x,y) \in q\mathbf{Z} \times p\mathbf{Z}$, on a clairement $\psi(x,y) = 0$. Par conséquent, il existe un morphisme injectif $\phi : \mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/pq\mathbf{Z}$ tel que pour tout $(x,y) \in \mathbf{Z}^2$:

$$\phi(x \bmod q, y \bmod p) = \psi(x,y) = (xp+yq) \bmod pq$$

Comme les groupes $\mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ et $\mathbf{Z}/pq\mathbf{Z}$, ϕ est un isomorphisme, et en particulier une bijection de la forme recherchée.
Une autre bijection $\phi' : \mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/pq\mathbf{Z}$ telle que $\phi'(x \bmod q, y \bmod p) = (xp+yq) \bmod pq$ coïncide avec ϕ en tout point de $\mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$, donc ϕ est bien unique.

6.6 Soit $\zeta_p = \exp(2i\pi/p)$, $\zeta_q = \exp(2i\pi/q)$ et $\zeta_{pq} = \exp(2i\pi/pq)$. On a :

$$\begin{aligned}
\tau_{pq} &= \sum_{z \in (\mathbf{Z}/pq\mathbf{Z})} \zeta_{pq}^{z^2} \\
\tau_{pq} &= \sum_{x \in (\mathbf{Z}/q\mathbf{Z})} \sum_{y \in (\mathbf{Z}/p\mathbf{Z})} \zeta_{pq}^{(xp+yq)^2} \\
\tau_{pq} &= \sum_{x \in (\mathbf{Z}/q\mathbf{Z})} \sum_{y \in (\mathbf{Z}/p\mathbf{Z})} \zeta_{pq}^{x^2p^2+2xypq+y^2q^2} \\
\tau_{pq} &= \sum_{x \in (\mathbf{Z}/q\mathbf{Z})} \sum_{y \in (\mathbf{Z}/p\mathbf{Z})} \zeta_q^{px^2} \cdot 1 \cdot \zeta_p^{py^2} \\
\tau_{pq} &= \left(\sum_{x \in (\mathbf{Z}/q\mathbf{Z})} \zeta_q^{px^2} \right) \left(\sum_{y \in (\mathbf{Z}/p\mathbf{Z})} \cdot \zeta_p^{py^2} \right) \\
\tau_{pq} &= \left(\frac{p}{q}\right) \tau_q \cdot \left(\frac{q}{p}\right) \tau_p
\end{aligned}$$

d'après l'évaluation de $\sum_{x \in (\mathbf{Z}/p\mathbf{Z})} \cdot \zeta_p^{px^2}$ obtenue au 6.2.

6.7 On a donc :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{\tau_{pq}}{\tau_p\tau_q} = \frac{u_{pq}}{u_p u_q}$$

où u_k vaut 1 ou i selon que k soit congru à 1 ou -1 modulo 4. Alors si $p \equiv 1 \pmod 4$, on a $u_p = 1$ et $u_{pq} = u_q$, donc $u_{pq}/u_pu_q = 1$, et de même si $q \equiv 1 \pmod 4$. Si maintenant $p \equiv q \equiv -1 \pmod 4$, il vient $u_{pq}/u_pu_q = 1/(-i)^2 = -1$. Tout cela revient donc effectivement à dire que :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

6.8 On se place maintenant dans $K = \mathbf{Q}[i]$. On a dans ce corps $(1+i)^2 = 2i$, donc :

$$(1+i)^q = (1+i)^{2\frac{q-1}{2}+1} = (2i)^{\frac{q-1}{2}}(1+i)$$

Par conséquent, si l'on note encore $a \mapsto [a]$ la surjection canonique $\mathcal{O}_K \to \mathcal{O}_K/q\mathcal{O}_K$, il vient :

$$[1+i^q] = [(1+i)^q] = \left[(2i)^{\frac{q-1}{2}}(1+i)\right] = \left[\left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i)\right]$$

Comme $\mathcal{O}_K = \mathbf{Z}[i]$, il existe donc $(a,b) \in \mathbf{Z}^2$ tel que :

$$\left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i) - 1 - i^q = q(a+bi)$$

Le module du membre de gauche est majoré par $|1+i|+|1+i^q| = 2\sqrt{2} < 3 \leq q$. Or, si $(a,b) \neq (0,0)$, on a $|q(a+bi)| = q\sqrt{a^2+b^2} \geq q$, ce qui est absurde. Par conséquent, $a = b = 0$, et :

$$\left(\frac{2}{q}\right) = i^{-\frac{q-1}{2}} \frac{1+i^q}{1+i} = \begin{cases} 1 & \text{si } q \equiv 1 \pmod 8 \\ -1 & \text{si } q \equiv 3 \pmod 8 \\ -1 & \text{si } q \equiv 5 \pmod 8 \\ 1 & \text{si } q \equiv 7 \pmod 8 \end{cases}$$

ce qui donne effectivement :

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$$

6.9 Soit n un entier qui n'est pas un carré. On veut montrer qu'il existe une infinité de nombres premiers modulo lesquels n est non carré. On peut supposer sans perte de généralité n non divisible par un carré. Si $n = \pm 2$ (resp. -1), alors on a $\left(\frac{n}{q}\right) = -1$ pour tout nombre premier q de la forme $8k+5$ (resp. $4k+3$), et il y a une infinité de tels nombres d'après le théorème de Dirichlet.
Si $n \notin \{2, -1, -2\}$, la décomposition de n en facteurs premiers s'écrit $n = (-1)^\alpha 2^\beta p_1 \cdots p_{r+1}$ avec $r \geq 0$ et où les p_i sont des nombres premiers impairs distincts. Soit $u \in (\mathbf{Z}/p_{r+1}\mathbf{Z})^*$ un élément qui n'est pas un carré. D'après le théorème chinois, il existe $b \in \mathbf{Z}$ tel que $b \equiv 1 \pmod{8p_1 \cdots p_r}$ et $b \equiv u \pmod{p_{r+1}}$. En particulier, b est premier à $a = 8p_1 \cdots p_r$, donc il existe une infinité de nombres premiers de la forme $ak+b$. Soit q un tel nombre premier. Comme $q \equiv 1 \pmod 8$, on a :

$$\left(\frac{-1}{q}\right) = \left(\frac{2}{q}\right) = 1 \quad \text{et pour tout nombre premier } p \neq q \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Par conséquent :

$$\left(\frac{n}{q}\right) = \left(\frac{-1}{q}\right)^\alpha \left(\frac{2}{q}\right)^\beta \left(\frac{p_1}{q}\right) \cdots \left(\frac{p_{r+1}}{q}\right) = \left(\frac{q}{p_1}\right) \cdots \left(\frac{q}{p_r}\right) \left(\frac{q}{p_{r+1}}\right)$$

et comme $q \equiv 1 \pmod{p_i}$ pour $1 \leq i \leq r$ et $q \equiv u \pmod{p_{r+1}}$, on a finalement :

$$\left(\frac{n}{q}\right) = \left(\frac{1}{p_1}\right) \cdots \left(\frac{1}{p_r}\right) \left(\frac{u}{p_{r+1}}\right) = -1$$

d'où le résultat.