« Theorema aureum » de Gauss

Notations :

- Dans ce problème, la lettre p designera toujours un nombre premier impair. Alors que la lettre m sera réservée pour un entier naturel strictement supérieur à 2 (sans autre condition).
- Soient $a \in \mathbb{Z}$.
  On dit que a **est un résidu quadratique modulo** m s'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv a[m]$.
- Selon la notation `Python`, on notera $a\%m$, le reste de la division euclidienne de a par m.
  On admet que dans l'anneau $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$, les classes $\overline{a}$ et $\overline{a'}$ son égales si et seulement si $a\%m = a'\%m$.
  Puis, nous prendrons le nombre $r = a\%m$ comme représentant principal de cette classe, classe notée alors $\dot{r}$ (voire r directement à partir de la partie D).

Objectifs

Dans ce problème, on cherche les nombres entiers qui sont des carrés modulo un entier m ou p (premier). On démontre pour terminer le « théorème d'or » de Gauss, appelé aussi théorème de réciprocité quadratique qui fait le lien entre les questions : p est-il un carré modulo q et q est-il un carré modulo p ?
Dans les *difficiles* préliminaires, on généralise sur le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, le premier résultat vu en début d'année sur la factorisation des polynômes. Dans la partie A, on se concentre sur un cas numérique particulier $p = 17$. Les résultats numériques trouvés dans cette partie peut être mobilisés par la suite...
Dans la partie B, on étudie des fonctions arithmétiques, pseudo-indicatrices, qui étudie si -1, 2 sont des résidus quadratiques modulo p, ainsi qu'une application θ particulière. Les résultats de cette partie sont exploitée en partie E (et D).
Dans la partie C, on met en place le symbole de Legendre assez pratique pour répondre à nos questions. On démontre aussi un résultat important x est un carré modulo p si et seulement si $x^{\frac{p-1}{2}} \equiv 1[p]$, à l'aide du petit théorème de Fermat.
Dans la partie D, on démontre le théorème de réciprocité quadratique pour des nombres premiers, que l'on généralise dans la partie E avec le symbole de Jacobi.

1 Préliminaires

Soit $p \in \mathbb{Z}$, nombre premier.

▷ **1.1.**

1. Soit $t_n : x \mapsto \sum_{k=0}^{n} a_k x^k$, polynomiale à coefficients entiers ($\forall\, i \in [\![0, n]\!]$, $a_i \in \mathbb{Z}$) de degré n.
   On suppose qu'il existe $\alpha \in \mathbb{Z}$ tel que $t_n(\alpha) \equiv 0[p]$.
   Montrer qu'il existe t_{n-1}, polynomiale à coefficients entiers et de degré au plus $n-1$ telle que
   $$\forall\, x \in \mathbb{Z}, \quad t_n(x) \equiv (x-a)t_{n-1}(x)[p]$$
2. Soit $t_n : x \mapsto \sum_{k=0}^{n} a_k x^k$, une fonction polynôme à coefficients entiers de degré n.
   Montrer qu'il existe au plus n nombres distincts $\alpha_1, \dots \alpha_n$ de $[\![0, p-1]\!]$ tels que :
   pour tout $k \in \mathbb{N}_n$, $t_n(\alpha_k) \equiv 0[p]$

On a donc démontré :

> Si p est une fonction polynomiale de degré n dans un corps $\mathbb{K}$ (=$\mathbb{R}$, $\mathbb{C}$ ou $\frac{\mathbb{Z}}{p\mathbb{Z}}$)
> Alors p admet au plus n racines distinctes dans ce corps : $a_1, a_2 \dots a_r$ $(r \geqslant n)$
> et il existe un polynôme q à coefficients dans $\mathbb{K}$ tel que $\forall\, x \in \mathbb{K}$, $p(x) = q(x) \times \prod_{i=1}^{r}(x - a_i)$

2 Cas $p = 17$

▷ 2.1. Cas $p = 17$

1. Montrer que, pour tout $a \in \mathbb{Z}$, $a^2 \equiv (17 - a)^2[17]$.
2. Ecrire la table de tous les nombres a^2, pour a de 1 à 16, modulo 17.
   On attend, donc ici la liste $(a^2 \,\%17)_{a\in[\![1,16]\!]}$
3. Montrer alors qu'il existe exactement 8 résidus quadratiques modulo 17. Donner les racines de chacun de ces nombres
4. Pour tout $a \in [\![1, 16]\!]$, que vaut $a^{16} \,\%17$?
5. Donner l'ensemble des nombres a tel que $a^8 \equiv 1[17]$.
   Quelle relation entre cet ensemble, et l'ensemble des résidus quadratiques modulo 17 ?

3 Applications pseudo-indicatrices

On doit pouvoir récrire cette partie en action de groupes ou structure de groupes !
On considère de nouvelles applications définies sur $\mathbb{Z}$ ou $\mathbb{Z}^2$:

$$\epsilon : a \mapsto \begin{cases} 0 & \text{si } 2|a \\ 1 & \text{si } a \equiv 1[4] \\ -1 & \text{si } a \equiv 3[4] \end{cases}, \omega : a \mapsto \begin{cases} 0 & \text{si } 2|a \\ 1 & \text{si } a \equiv 1[8] \text{ ou } a \equiv 7[8] \\ -1 & \text{si } a \equiv 3[8] \text{ ou } a \equiv 5[8] \end{cases}, \theta : (a, a') \mapsto \begin{cases} 0 & \text{si } 2|a \text{ ou } 2|a' \\ -1 & \text{si } a \equiv 3[4] \text{ et } a' \equiv 3[4] \\ 1 & \text{sinon} \end{cases}$$

▷ 3.1. Etude de ϵ et ω.

1. Montrer que pour tout entier $\underline{a \text{ impair}}$, $\epsilon(a) = (-1)^{\frac{a-1}{2}}$ et $\omega(a) = (-1)^{\frac{a^2-1}{8}}$.
2. En déduire que pour tout $a, a' \in \mathbb{Z}$, $\epsilon(aa') = \epsilon(a)\epsilon(a')$ et $\omega(aa') = \omega(a)\omega(a')$

▷ 3.2. Etude de la fonction θ.

1. Calculer $\theta(1, 3)$, $\theta(5, 9)$, $\theta(1, 2)$.
2. Montrer que $\forall\, a, a' \in \mathbb{Z}$, $\theta(a, a') = \theta(a', a)$
3. Dans le cas où a et a' sont des entiers impairs, montrer que $\theta(a, a') = (-1)^{\frac{(a-1)(a'-1)}{4}}$.
4. Montrer que pour tout $a, b, a' \in \mathbb{Z}$: $\theta(ab, a') = \theta(a, a') \times \theta(b, a')$

4 Symbole de Legendre

On considère m, un nombre entier strictement supérieur à 2. On note $\left(\frac{Z}{m\mathbb{Z}}\right)^*$ l'ensemble des nombres inversibles de $\frac{\mathbb{Z}}{m\mathbb{Z}}$.
On rappelle la convention de l'énoncé, ces éléments (qui sont des classes d'équivalence) sont notées $\dot{r}$ où $r \in [\![0, m-1]\!]$

▷ 4.1. Image du produit

Montrer que pour tout $a, b \in \frac{\mathbb{Z}}{m\mathbb{Z}}$, $\overbrace{ab}^{\cdot} = \dot{a}\dot{\times}\dot{b}$.

Dans le cas où $m = p$ est un nombre premier, que pensez-vous de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$?

Pour la suite de cette partie, on suppose que $m = p$ est un nombre premier et on note $\mathbb{F}_p = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, qui est un groupe (associé à la multiplication $\dot{\times}$ simplifiée en $\times$).

▷ 4.2. Deux morphismes de groupes multiplicatifs

On note alors $\varphi_p : \mathbb{F}_p \to \mathbb{F}_p$, $\dot{x} \mapsto \overbrace{x^{\frac{p-1}{2}}}^{\cdot}$ et $\psi_p : \mathbb{F}_p \to \mathbb{F}_p$, $\dot{x} \mapsto \overbrace{x^2}^{\cdot}$

Pour les premières questions, on fera bien attention à différencier le nombre x de sa classe $\dot{x}$, *« nombre »* de $\mathbb{F}_p$.
Pour les questions suivantes, on pourra faire la confusion.

1. A l'aide de 1., montrer que ψ_p est un morphisme de groupes multiplicatifs.
   On admet que φ_p est également un morphisme de groupes multiplicatifs.
2. En exploitant le (petit) théorème de FERMAT montrer que $\psi_p \circ \varphi_p = \mathbf{1}_{\mathbb{F}_p}$.
   (où $\mathbf{1}_{\mathbb{F}_p} : \dot{x} \mapsto \dot{1}$)
3. Montrer que Ker $\psi_p = \{\dot{1}, \overbrace{p-1}^{\cdot}\}$
4. En déduire que Im $\varphi_p \subset \{\dot{1}, \overbrace{p-1}^{\cdot}\}$
5. En exploitant les fonctions polynomiales $t_1 : x \mapsto x^{\frac{p-1}{2}} - 1$ et $t_2 : x \mapsto x^{\frac{p-1}{2}} + 1$ *et le résultat démontré dans le préliminaire*, montrer que Im $\varphi_p = \{\dot{1}, \overbrace{p-1}^{\cdot}\}$ et plus précisément
$$\text{card}\left(\varphi_p^{-1}(\{\dot{1}\})\right) = \text{card}\left(\varphi_p^{-1}(\{\overbrace{p-1}^{\cdot}\})\right) = \frac{p-1}{2}$$
6. Donner une condition nécessaire et suffisante sur $p\%4$ pour que $\varphi_p(\dot{-1}) = \dot{1}$.

▷ 4.3. Symbole de Legendre

On note pour tout $a \in \mathbb{Z}$ (et p premier) :
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p|a \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p \\ 1 & \text{sinon} \end{cases}$$

1. Montrer que si $a \equiv a'[p]$, alors $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$
2. En exploitant la partie A, donner la liste des valeurs de $\left(\frac{a}{17}\right)$ pour $a \in [\![30, 40]\!]$.
3. Montrer également que $\left(\frac{a}{3}\right) \equiv a[3]$.
4. Montrer que :
$$\forall\, a \in \mathbb{Z}, \qquad \left(\frac{a}{p}\right) = \varphi_p(\overbrace{a\%p}^{\cdot})$$
   On complétera la définition de φ_p par : $\varphi_p(0) = 0^{\frac{p-1}{2}} = 0$. On rappelle que $\dot{-1} = \overbrace{p-1}^{\cdot}$.
5. En déduire la propriété de morphisme :
$$\forall\, a, a' \in \mathbb{Z}, \qquad \left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$$
6. Supposons que $a \wedge p = 1$. Comment se simplifie $\left(\frac{a^2 a'}{p}\right)$?
7. Montrer que $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$.

5 Somme de Gauss et réciprocité quadratique

On fixe un nombre premier $p > 2$ et considère $\xi = e^{2i\pi/p}$ et $\tau = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^k$.

▷ 5.1. Somme de Gauss.

1. Calculer $\sum_{k=0}^{p-1} \xi^k$.
2. Montrer que pour tout $k \in \mathbb{N}_p$, $h_k : \mathbb{F}_p \to \mathbb{F}_p$, $s \mapsto ks$ est bijectif.
   En déduire que : $\tau^2 = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \xi^k \times \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) \xi^h = \epsilon(p)p$
   On fera le changement de variable : $h \to s$ donné par la relation $h = ks$.
3. Soit q un nombre premier impair (différent de p).
   Montrer que : $\forall\ k \in [\![1, q-1]\!],\ q \left| \binom{q}{k} \right.$ puis par récurrence sur s

$$\forall\ a_1, \dots a_s \in \mathbb{Z}, \qquad \left(\sum_{k=1}^{s} a_k\right)^q \equiv \sum_{k=1}^{s} a_k^q\ [q]$$

4. Montrer que, pour $q(\neq p)$ premier impair : $\left(\frac{q}{p}\right) \tau^q \equiv \tau\ [q]$ avec q.
5. Montrer, par ailleurs, que $\tau^{q-1} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)\ [q]$

▷ 5.2. Réciprocité quadratique

1. Soient p et q deux nombres premiers impairs distincts. Montrer en exploitant 1.(d) et 1.(e) :

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

2. Application : Est-ce que 17 est un carré de $\frac{\mathbb{Z}}{41\mathbb{Z}}$?

6 Symbole de Jacobi et réciprocité quadratique généralisée

On note pour tout $a \in \mathbb{Z}$ et $n \geqslant 3$ <u>impair</u> tels que $n = \prod_{i=1}^{s} p_i^{\alpha_i}$, décomposition en facteurs premiers de n :

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

où $\left(\frac{a}{p_i}\right)$ est le symbole de Legendre

▷ 6.1. Symbole de Jacobi

1. Montrer que pour tout $a, a' \in \mathbb{Z}$, $m, m' \geqslant 3$, impairs tels que $m \wedge m' = 1$:

$$\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right) \qquad \text{et} \qquad \left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$$

2. Calculer $\left(\frac{14}{51}\right)$

▷ 6.2. Loi de réciprocité (généralisée)

Soient $n, m \in \mathbb{Z}$, impairs, positifs et premiers entre eux. Montrer que

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

▷ 6.3. Lois complémentaires

Montrer que pour tout n entier impair positif :

$$\left(\frac{-1}{n}\right) = \epsilon(n) = (-1)^{\frac{n-1}{2}} \qquad \text{et} \qquad \left(\frac{2}{n}\right) = \omega(n) = (-1)^{\frac{n^2-1}{8}}$$

Correction des exercices

▷ Corrigé de l'exercice 1.1

Préliminaires

Soit $p \in \mathbb{N}$, un nombre premier.

1. Soit $t_n : x \mapsto \sum_{k=0}^{n} a_k x^k$, polynomiale à coefficients entiers de degré n.
   On suppose qu'il existe $a \in \mathbb{Z}$ tel que $t_n(a) \equiv 0[p]$.
   Pour tout $x \in \mathbb{Z}$:

$$t_n(x) - t_n(a) = \sum_{k=1}^{n} a_k(x^k - a^k) + a_0 - a_0 = \sum_{k=1}^{n} \left((x-a) a_k \sum_{h=0}^{k-1} x^{k-1-h} a^h \right) = (x-a) \underbrace{\sum_{k=1}^{n} a_k \sum_{h=0}^{k-1} x^{k-1-h} a^h}_{p_{n-1}(x)}$$

   Soit $k \in [\![1, n-1]\!]$

   Comme pour tout $h \in [\![0, k-1]\!]$, $k-1-h \leqslant k-1$, alors $\deg \left(\sum_{h=0}^{k-1} x^{k-1-h} a^h \right) \leqslant k-1$.

   Donc $\deg t_{n-1} \leqslant \max\{k-1, k \in [\![1,n]\!]\} \leqslant n-1$.
   Enfin, comme $t_n(a) \equiv 0[p]$, on plonge la relation modulo p :

> il existe t_{n-1}, polynomiale à coefficients entiers et de degré au plus $n-1$ telle que
> $\forall\, x \in \mathbb{Z},\ t_n(x) \equiv (x-a) t_{n-1}(x)[p]$.

2. Soit $t_n : x \mapsto \sum_{k=0}^{n} a_k x^k$, polynomiale à coefficients entiers de degré n.
   On démontre par récurrence pour $k \leqslant n$:

$$\mathcal{P}_k : \quad \text{´ Si il existe } a_1, a_2, \dots a_k \text{ distincts de } [\![0, p-1]\!], \text{ tels que } t_n(a_k) \equiv 0[p]$$
$$\text{alors, il existe } t_{n-k} \text{ polynomiale de degré au plus } n-k \text{ telle que}$$
$$\forall\, x \in \mathbb{Z}, t_n(x) \equiv \prod_{i=1}^{k} (x - a_i) \times t_{n-k}(x)[p] \text{ ˇ}$$

   — $\mathcal{P}_0$ est vraie. avec $t_{n-0} = p_n$.
   — $\mathcal{P}_1$ est vraie d'après la question précédente (mais cela ne joue aucun rôle dans la démonstration de la récurrence).
   — Soit $k < n$. Supposons que $\mathcal{P}_k$ est vraie.
   Supposons, qu'il existe $k+1$ nombres (distincts) $a_1, \dots a_k, a_{k+1}$ de $[\![0, p-1]\!]$ tels que : $t_n(a_k) \equiv 0[p]$.
   On peut alors appliquer $\mathcal{P}_k$ pour les nombres $a_1, \dots a_k$.
   Donc il existe t_{n-k}, polynomiale de degré au plus $n-k$, tel que

$$\forall\, x \in \mathbb{Z},\ t_n(x) \equiv \prod_{i=1}^{k} (x - a_i) \times t_{n-k}(x)[p].$$

   Puis $t_n(a_{k+1}) \equiv 0[p]$, donc $\prod_{i=1}^{k} (a_{k+1} - a_i) \times t_{n-k}(a_{k+1}) \equiv 0[p]$
   Or p est premier donc divise l'un des termes.
   Mais pour tout $i \in \mathbb{N}_k$, $a_{k+1} - a_k \in [\![-p+1, p-1]\!] \setminus \{0\}$ car $a_{k+1} \neq a_i$.
   Donc $t_{n-k}(a_{k+1}) \equiv 0[p]$.
   Ainsi, d'après q.1 (en adaptant n), il existe t_{n-k-1} de degré inférieur à $\deg(t_{n-k}-1)$ tq
   pour tout $x \in \mathbb{Z}$, $t_{n-k}(x) \equiv (x - a_{k-1}) t_{n-k-1}(x)[p]$
   On ré-injecte dans la formule précédente, et on trouve que $\mathcal{P}_{k+1}$ est vraie.
   Supposons maintenant que t_n admette n racines distincts : $a_1, \dots a_n$ de $[\![0, p-1]\!]$
   alors il existe un polynôme t_0 de degré au plus 0 tel que
   $\forall\, x \in \mathbb{Z}$, $t_n(x) \equiv t_0(x) \prod_{i=1}^{n} (x - a_i)[p]$.

Comme t_0 est une constante, on a $t_n(x) \equiv 0[p]$ si et seulement si $\exists\, i \in \mathbb{N}_n$ tel que $p|x - a_i$.
Donc, si par ailleurs $x \in [\![0, p-1]\!]$, $x \in \{a_1, \dots a_n\}$.

> t_n ne peut admettre plus de racines que $a_1, \dots a_n$ dans $[\![0, p-1]\!]$ (modulo p)

▷ Corrigé de l'exercice 2.1

1. Soit $a \in \mathbb{Z}$.
$$(17-a)^2 = 17^2 - 2 \times 17 \times a + a^2 = a^2 + 17(17 + 2a)$$
> Donc, en déduisant modulo 17, pour tout $a \in \mathbb{Z}$, $a^2 \equiv (17-a)^2[17]$.

2. La question précédente nous signale la symétrie dans le calcul de a^2, modulo 17.

a	1	2	3	4	5	6	7	8
$17-a$	16	15	14	13	12	11	10	9
$a^2 = (17-a)^2$	1	4	9	$16(=-1)$	8	2	$15(=-2)$	$13(=-4)$

3. Un nombre est un résidu quadratique si et seulement si il est le carré d'un nombre a ; or on a fait la liste de tous les carrés possibles.

> Il y a exactement 8 résidus quadratiques modulo 17 : 1, 2, 4, 8, 9, 13, 15, 16
> et modulo 17 : $\sqrt{1} \in \{1, 16\}$, $\sqrt{2} \in \{6, 11\}$, $\sqrt{4} \in \{2, 15\}$, $\sqrt{8} \in \{5, 12\}$,
> $\sqrt{9} \in \{3, 14\}$, $\sqrt{13} \in \{8, 9\}$, $\sqrt{15} \in \{7, 10\}$ et $\sqrt{16} \in \{4, 13\}$

4. C'est le petit théorème de Fermat : $a^{p-1} \equiv 1[p]$, avec $p = 17$, nombre premier

> pour tout $a \in [\![1, 16]\!]$, $a^{16}\%17 = 1$.

5. On peut (re)faire un tableau, cette fois-ci on ne regarde que les nombres de 1 à 8 car comme $a^2 \equiv (17-a)^2[17]$, en élevant à la puissance 4 : $a^8 \equiv (17-a)^8[17]$.

a	1	2	3	4	5	6	7	8
a^2	1	4	-8	-1	8	2	-2	-4
a^4	1	-1	-4	1	-4	4	4	-1
a^8	1	1	-1	1	-1	-1	-1	1

> $\{a \in [\![1, 16]\!] \mid a^8 \equiv 1[17]\} = \{1, 2, 4, 8, 9, 13, 15, 16\} = \{a^2[17], a \in [\![1, 16]\!]\}$

▷ Corrigé de l'exercice 3.1

1. Supposons que a est impair, un et seul cas suivant se produit :
   - ou bien $a \equiv 1[4]$, alors $4|a-1$, donc $\dfrac{a-1}{2}$ est pair et donc $(-1)^{\frac{a-1}{2}} = 1 = \epsilon(a)$.
   - ou bien $a \equiv 3[4]$, alors $4|a-3$, donc $\dfrac{a-3}{2} = \dfrac{a-1}{2} - 1$ est pair et $\dfrac{a-1}{2} - 1$ est impair
     ainsi $(-1)^{\frac{a-1}{2}} = (-1) = \epsilon(a)$.

   Puis, également, un et seul cas suivant se produit :
   - ou bien $a \equiv 1[8]$, alors $8|a-1$ donc $\dfrac{a^2-1}{8} = \dfrac{a-1}{8}(a+1)$ est un pair car $a+1$ est pair.
     et donc $(-1)^{\frac{a^2-1}{8}} = 1 = \omega(a)$.
   - ou bien $a \equiv 7[8]$, alors $8|a+1$ donc $\dfrac{a^2-1}{8} = \dfrac{a+1}{8}(a-1)$ est un pair car $a-1$ est pair.
     et donc $(-1)^{\frac{a^2-1}{8}} = 1 = \omega(a)$.
   - ou bien $a \equiv 3[8]$, alors $a = 8k+3$, donc $a^2 - 1 = 8(8k^2+6k) + 9 - 1 = 8(2(4k^2+3k)+1)$

donc $\frac{a^2-1}{8} = 2(4k^2+3k)+1$ est un nombre impair et donc $(-1)^{\frac{a^2-1}{8}} = -1 = \omega(a)$.

- ou bien $a \equiv 5[8]$, alors $a = 8k+5$, donc $a^2-1 = 8(8k^2+10k)+25-1 = 8(2(4k^2+5k+1)+1)$
  donc $\frac{a^2-1}{8} = 2(4k^2+5k+1)+1$ est un nombre impair et donc $(-1)^{\frac{a^2-1}{8}} = -1 = \omega(a)$.

> Donc pour tout entier a impair, $\epsilon(a) = (-1)^{\frac{a-1}{2}}$ et $\omega(a) = (-1)^{\frac{a^2-1}{8}}$.

2. Si a ou a' est pair, alors $\epsilon(a) = 0$ ou $\epsilon(a') = 0$, d'où $\epsilon(a)\epsilon(a') = 0$
   Et par ailleurs, aa' est alors pair donc $\epsilon(aa') = 0$. Donc $\epsilon(aa') = \epsilon(a)\epsilon(a')$
   On a de même $\omega(aa') = 0 = \omega(a)\omega(a')$.
   Si a et a' sont impair, alors aa' aussi :
   $\epsilon(aa') = (-1)^{\frac{aa'-1}{2}} = (-1)^{\frac{aa'-1}{2}}$ et $\epsilon(a)\epsilon(a') = (-1)^{\frac{a-1}{2}}(-1)^{\frac{a'-1}{2}} = (-1)^{\frac{a+a'-2}{2}}$.
   Or $\frac{a+a'-2}{2} - \frac{aa'-1}{2} = \frac{a+a'-aa'-1}{2} = \frac{-(a-1)(a'-1)}{2}$ est un nombre pair (a et a' impaires).
   Donc $\frac{a+a'-2}{2}$ et $\frac{aa'-1}{2}$ ont même parité et donc $\epsilon(aa') = \epsilon(a)\epsilon(a')$
   De même on étudie la parité de $\frac{(a^2-1)+(a'^2-1)-((aa')^2-1)}{8} = \frac{a^2+a'^2-aa')^2-1}{8} = \frac{-(a^2-1)(a'^2-1)}{8}$
   Or $4|a^2-1$, car $a = 2k+1$ est impair donc $a^2-1 = 4(k^2+k)$. De même $4|a'^2-1$,
   donc $16|(a^2-1)(a'^2-1)$.
   Et donc $\frac{(a^2-1)+(a'^2-1)}{8}$ et $frac((aa')^2-1)8$ ont même parité : $\omega(aa') = \omega(a)\omega(a')$

> Pour tout $a, a' \in \mathbb{Z}$, $\epsilon(aa') = \epsilon(a)\epsilon(a')$ et $\omega(aa') = \omega(a)\omega(a')$.

▷ Corrigé de l'exercice 3.2

1. Comme $2|2$, $\theta(1,2) = 0$.
   Comme $1 \equiv 1[4]$ et 3 n'est pas divisible par 2 : $\theta(1,3) = 1$.
   Comme $5 \equiv 1[4]$ et 9 n'est pas divisible par 2 : $\theta(5,9) = 1$.

> $\theta(1,3) = 1 = \theta(5,9) \qquad \theta(1,2) = 0$

2. La définition de θ est parfaitement symétrique en a et a'.

> $\forall\ a, a' \in \mathbb{Z},\ \theta(a,a') = \theta(a',a)$

3. On suppose que a et a' sont des entiers impairs.
   Un et seul cas se produit :
   - $a \equiv 3[4]$ et $a' \equiv 3[4]$, alors il existe $k, k' \in \mathbb{Z}$ tels que $a = 4k+3$ et $a' = 4k'+3$.
     Donc $\frac{(a-1)(a'-1)}{4} = \frac{(4k-2)(4k'-2)}{4} = (4kk'-2k'-2k+1)$, impair.
     Dans ce cas : $(-1)^{\frac{(a-1)(a'-1)}{4}} = -1 = \theta(a,a')$.
   - $a \equiv 1[4]$ ou $a' \equiv 1[4]$. Par symétrie de $\theta(a,a')$, il suffit d'étudier un cas, sans perte de généralité.
     On suppose donc que $a = 4k+1$, donc $\frac{(a-1)(a'-1)}{4} = k(a'-1)$, pair car a est impair.
     Dans ce cas : $(-1)^{\frac{(a-1)(a'-1)}{4}} = 1 = \theta(a,a')$.

> Dans le cas où a et a' sont des entiers impairs, $\theta(a,a') = (-1)^{\frac{(a-1)(a'-1)}{4}}$.

4. Soient $a, b, a' \in \mathbb{Z}$,
   - Si a ou b est pair, ab l'est également et donc $\theta(ab,a') = 0 = \theta(a,a') \times \theta(b,a')$.
   - Si a' est pair alors $\theta(ab,a') = 0 = \theta(a,a')\theta(b,a')$.

• Il reste le cas où a, b et a' sont impairs.
Comme précédemment, on étudie simplement la parité de

$$\frac{(ab-1)(a'-1)}{4}-\frac{(a-1)(a'-1)}{4}-\frac{(b-1)(a'-1)}{4}=\frac{aba'-a'-ab+1-aa'+a+a'-1-ba'+b+a'-1}{4}$$

$$=\frac{aba'-ab-aa'-ba'+a+b+a'-1}{4}=\frac{(a-1)(b-1)(a'-1)}{4}$$

Or $a-1$, $b-1$ et $a'-1$ sont divisibles par 2, donc (produit) $8|(a-1)(b-1)(a'-1)$.
Ainsi $\dfrac{(ab-1)(a'-1)}{4}-\dfrac{(a-1)(a'-1)}{4}-\dfrac{(b-1)(a'-1)}{4}$ est pair.
Donc $\theta(ab,a')=\theta(a,a')\times\theta(b,a')$

Pour tout $a, b, a' \in \mathbb{Z}$, $\theta(ab,a')=\theta(a,a')\times\theta(b,a')$.

▷ Corrigé de l'exercice 4.1

Si $a \equiv a'[m]$ et $b \equiv b'[m]$.
alors $m|(a-a')$, $m|(b-b')$ Donc m divise $ab-a'b'=ab-ab'+ab'-a'b'=a(b-b')+b'(a-a')$, par stabilité de divisibilité sur les combinaisons linéaires.
Donc par indépendance du représentant, on peut affirmer :

pour tout $a, b \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$, $\dot{\overbrace{ab}} = \dot{a}\times\dot{b}$.

On raisonne directement par équivalence :

$$\dot{r}\in\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \iff \exists\ \dot{s}\in\frac{\mathbb{Z}}{m\mathbb{Z}} \text{ tel que } \dot{s}\dot{r}=\dot{r}\dot{s}=\dot{1} \iff \exists\ s\in\mathbb{Z} \text{ tel que } sr(\equiv rs)\equiv 1[m]$$
$$\iff \exists\ s\in\mathbb{Z}, k\in\mathbb{Z} \text{ tels que } sr=1+km \iff \exists\ s\in\mathbb{Z}, k'\in\mathbb{Z} \text{ tels que } sr+k'm=1$$
$$\iff r\wedge m=1$$

d'après l'identité de Bézout

$\dot{r}\in\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$ si et seulement si $r\wedge m=1$.

Dans le cas où $m=p$ est premier, tout les nombres de 1 à $p-1$ sont premiers avec p,

Donc $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^* = \{\dot{1}, \dot{2}, \dots \dot{p-1}\}$

▷ Corrigé de l'exercice 4.2

1. Pour tout $ab \in \mathbb{F}_p$ (on fait la confusion entre a et $\dot{a}$) :

$$\psi_p(ab)=\dot{\overbrace{(ab)}}=\dot{\overbrace{(a)}}\times\dot{\overbrace{(a)}} \underbrace{=}_{\text{d'après 1}} \dot{\overbrace{(ab)^2}} \underbrace{=}_{\text{commutativité dans } \mathbb{Z}} \dot{\overbrace{a^2b^2}} \underbrace{=}_{\text{d'après 1}} \dot{\overbrace{a^2}}\times\dot{\overbrace{b^2}}=\varphi_p(a)\varphi_p(b)$$

ψ_p est donc un morphisme de groupes

2. Soit $\dot{x}\in\mathbb{F}_p$, $\psi_p\circ\varphi_p(\dot{x})=(\dot{x})^{p-1}=\dot{\overbrace{x^{p-1}}}=\dot{1}$,
car d'après le petit théorème de Fermat, pour tout x tel que $x\wedge p=1$, on a $x^{p-1}\equiv 1[p]$.

$\psi_p\circ\varphi_p=\mathbf{1}_{\mathbb{F}_p}$

3. Soit $\dot{x} \in \text{Ker } \psi_p$, i.e. $x^2 \equiv 1[p]$.
   Donc $p|x^2 - 1 = (x-1)(x+1)$.
   Or p est un nombre premier donc $p|x-1$ ou $p|x+1$
   Ainsi $x \equiv 1[p]$ ou $x \equiv -1[p]$, i.e. $x \equiv p-1[p]$.
   Réciproquement, si $x = 1$, alors $\psi_p(\dot{x}) = \dot{1}^2 = 1^2 = \dot{1}$ et si $x = -p1$, $\psi_p(\dot{x}) = (\dot{-1})^2 = \dot{1}$.
   Par double inclusion :

$$\boxed{\text{Ker } \psi_p = \{\dot{1}, \overbrace{\dot{p-1}}^{\cdot}\}}$$

4. Soit $\dot{x} \in \text{Im } \varphi_p$.
   Donc il existe $\dot{a} \in \mathbb{F}_p$ tel que $\varphi_p(\dot{a}) = \dot{x}$.
   On a alors $\psi_p(\dot{x}) = (\psi_p \circ \varphi_p)(\dot{a}) = \mathbf{1}_{\mathbb{F}_p}(a) = 1$.
   Ainsi, $\dot{x} \in \text{Ker } \psi_p$.

$$\boxed{\text{Im } \varphi_p \subset \text{Ker } \psi_p = \{\dot{1}, \overbrace{\dot{p-1}}^{\cdot}\}}$$

5. On sait que $\text{Im } \varphi_p = \{\dot{1}, \overbrace{\dot{p-1}}^{\cdot}\}$.
   Donc $\mathbb{F}_p^* = \{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} \bigcup \{k \in \mathbb{F}_p \mid \varphi_p(k) = -1\}$. Cette réunion est disjointe.
   En prenant les cardinaux : $p - 1 = \text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} + \text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = -1\}$.
   Puis le polynôme $t_1 : x \mapsto x^{\frac{p-1}{2}} - 1$ admet au plus $\dfrac{p-1}{2}$ racines distinctes dans $[\![1, p-1]\!]$
   (0 n'est pas racine).
   Or $h \in \{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} \iff t_1(h) = 0$. Donc $\text{card}\big(\varphi_p^{-1}(\{\dot{1}\})\big) \leqslant \dfrac{p-1}{2}$.
   De même, le polynôme $t_2 : x \mapsto x^{\frac{p-1}{2}} + 1$ admet au plus $\dfrac{p-1}{2}$ racines distinctes dans $[\![1, p-1]\!]$
   (0 n'est pas racine).
   $h \in \{k \in \mathbb{F}_p \mid \varphi_p(k) \equiv -1 \equiv p-1[p]\} \iff t_2(h) = 0 : \text{card}\big(\varphi_p^{-1}(\{\overbrace{\dot{p-1}}^{\cdot}\})\big) \leqslant \dfrac{p-1}{2}$.
   Pour que la somme $\text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} + \text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = -1\}$ donne $p-1$, il faut et il suffit que

$$\boxed{\text{card}\big(\varphi_p^{-1}(\{\dot{1}\})\big) = \text{card}\big(\varphi_p^{-1}(\{\overbrace{\dot{p-1}}^{\cdot}\})\big) = \frac{p-1}{2}}$$

6. $\varphi_p(-1) = 1 \iff (-1)^{\frac{p-1}{2}} \equiv 1[p]$.
   Si $p \equiv 1[4]$, alors $\dfrac{p-1}{2}$ est un nombre pair et $(-1)^{\frac{p-1}{2}} = 1$, donc $(-1)^{\frac{p-1}{2}} \equiv 1[4]$.
   Si $p \equiv 3[4]$, alors $\dfrac{p-1}{2}$ est un nombre impair et $(-1)^{\frac{p-1}{2}} = -1$, donc $(-1)^{\frac{p-1}{2}} \equiv -1[4]$.

$$\boxed{\varphi_p(-1) = 1 \iff p \equiv 1[4]}$$

▷ Corrigé de l'exercice 4.3

1. Supposons que $a \equiv a'[p]$.
   - Si $p|a$ alors $p|a'$ et donc $\left(\dfrac{a}{p}\right) = \left(\dfrac{a'}{p}\right) = 0$
   - Si $\left(\dfrac{a}{p}\right) = 1$, alors $a \wedge p = 1$ et donc $a' \wedge p = 1$.

   Et il existe $b \in \mathbb{Z}$ tel que $a \equiv b^2[p]$ et donc $a' \equiv b^2[p]$ et donc $\left(\dfrac{a'}{p}\right) = 1 = \left(\dfrac{a}{p}\right)$
   - Si $\left(\dfrac{a}{p}\right) = -1$, alors $a \wedge p = 1$ et donc $a' \wedge p = 1$.

   Et $\forall\, b \in \mathbb{Z}$ tel que $a \not\equiv b^2[p]$ et donc $a' \not\equiv b^2[p]$ et donc $\left(\dfrac{a'}{p}\right) = -1 = \left(\dfrac{a}{p}\right)$

$$\boxed{\text{Si } a \equiv a'[p], \text{ alors } \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).}$$

2. Les résidu quadratique modulo 17 sont $1, 2, 4, 8, 9, 13, 15, 16$ et leur congruence modulo 17.
Or $30 \equiv 13[17]$, $32 \equiv 15[17]$, $33 \equiv 16[17]$, $35 \equiv 1[17]$, $36 \equiv 2[17]$, $38 \equiv 4[17]$.
On a donc la liste suivante :

a	30	31	32	33	34	35	36	37	38	39	40
$\left(\frac{a}{17}\right)$	1	-1	1	1	0	1	1	-1	1	-1	-1

3. Il suffit de se concentrer sur les nombres de $\{0, 1, 2\}$, on exploitera ensuite la congruence.
- si $a \equiv 0[3]$, alors $\left(\frac{a}{3}\right) = 0 \equiv a[3]$
- si $a \equiv 1[3]$, alors $a = 1^2$, donc $\left(\frac{a}{3}\right) = 1 \equiv a[3]$
- si $a \equiv 2[3]$, alors comme $1^2 \equiv 2^2 = 1[3]$, 2 n'est pas un résidu quadratique,
donc $\left(\frac{a}{3}\right) = -1 \equiv 2 \equiv a[3]$

Pour tout $a \in \mathbb{Z}$, $\left(\frac{a}{3}\right) \equiv a[3]$.

4. Soit $a \in \mathbb{Z}$, on sait d'après la question 5.(a) que $\left(\frac{a}{p}\right) = \left(\frac{a\%p}{p}\right)$.
- Si $p|a$, alors $a\%p = 0$ et donc $\left(\frac{a}{p}\right) = 0 = \varphi_p(a\%p)$.
- Si $p \wedge a = 1$, alors $a\%p \in \mathbb{N}_{p-1}$.

Si a est un résidu quadratique, il existe $b \in \mathbb{N}_{p-1}$ tel que $a = b^2$, donc $x^2 - a$ se factorise en $(x-b)(x+b)$ modulo p (cf. préliminaires).

Ainsi, a admet exactement deux racines carrées modulo p.
Par conséquent, il y a deux options :
— ou bien $x^2 - a$ admet deux racines l'une entre 1 et $\frac{p-1}{2}$ et l'autre entre $\frac{p+1}{2}$ et $p-1$,
— ou bien $x^2 - a$ n'admet aucune racine.

$$\text{card}\{(x^2)\%p; x \in \mathbb{Z}\} = \text{card}\{(x^2)\%p, x \in [\![1, \frac{p-1}{2}]\!]\} = \frac{p-1}{2}$$

Par ailleurs,
si a est un résidu quadratique, alors il existe $b \in \mathbb{Z}$ tel que $a\%p \equiv b^2[p]$ et donc $\varphi_p(a\%p) = \varphi_p(\psi_p(b)) = 1$
ainsi $a \in \text{Ker } \varphi_p = \{x \in \mathbb{F}_p \mid \varphi_p(x) = 1\}$.
On a donc l'inclusion : $\{(x^2)\%p; x \in \mathbb{Z}\} \subset \text{Ker } \varphi_p$.
Or on a démontré que $\text{card}\{(x^2)\%p; x \in \mathbb{Z}\} = \frac{p-1}{2}$ et en 4.(e) : $\text{card}\varphi_p^{-1}(\{1\}) = \frac{p-1}{2}$.
Ainsi, on exactement l'égalité des ensembles (inclusion + égalité des cardinaux) :

$$\{(x^2)\%p; x \in \mathbb{Z}\} = \varphi_p^{-1}(\{1\})$$

Et par passage au complémentaire :

$$\varphi_p^{-1}(\{-1\}) = \{a \in \mathbb{F}_p, a \text{ non résidu quadratique}\}$$

$$\forall\, a \in \mathbb{Z}, \quad \left(\frac{a}{p}\right) = \varphi_p(a\%p)$$

5. On exploite le fait que φ_p est un morphisme de groupe (pour a et a' non divisible par p).
Si p divise a ou a', donc l'un des termes est nul : $\left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$
alors que p divise aa' donc $\left(\frac{aa'}{p}\right) = 0$
Si p ne divise ni a ni a' :

$$\left(\frac{aa'}{p}\right) = \varphi_p\big((aa')\%\, p\big) = \varphi_p\big((a\%\, p) \times (a'\%\, p)\big) = \varphi_p\big(a\%\, p\big)\varphi_p\big(a'\%\, p\big) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$$

$$\forall\, a, a' \in \mathbb{Z}, \quad \left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$$

6. Supposons que $a \wedge p = 1$. On applique la propriété précédente, et comme a^2 est un carré :

$$\boxed{\left(\frac{a^2 a'}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{a'}{p}\right) = 1\left(\frac{a'}{p}\right)}$$

7. D'après 4.(e), il y a autant de racines quadratiques que de non racines quadratiques : $\dfrac{p-1}{2}$,

$$\boxed{\sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = \frac{p-1}{2} \times 1 + \frac{p-1}{2} \times (-1) = 0}$$

▷ Corrigé de l'exercice 5.1

1. Il s'agit d'une somme de p termes consécutifs d'une suite géométrique de raison $\xi \neq 1$.

$$\boxed{\sum_{k=0}^{p-1} \xi^k = \frac{1-\xi^p}{1-\xi} = \frac{1-e^{2i\pi}}{1-\xi} = 0}$$

2. On note $h_k : s \mapsto ks$.
   Comme p est premier, k est inversible modulo p (dans $\mathbb{F}_p$).
   On note k' tel que $kk' \equiv 1[p]$ (BÉZOUT).
   On a alors $h_k \circ h_{k'}(s) = kk's = s = k'ks = h_{k'} \circ h_k(s)$.

   Donc h_k est bijective.

   Puis, les sommes peuvent commencer à 1 car $\left(\dfrac{0}{p}\right) = 0$

$$\tau^2 = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\xi^k \times \sum_{h=1}^{p-1}\left(\frac{h}{p}\right)\xi^s = \sum_{k=1}^{p-1}\sum_{h=1}^{p-1}\left(\frac{kh}{p}\right)\xi^{k+h}$$

   Puis on fait le changement de variable : $h = h_k(s) = ks$ avec h_k bijective (de la variable h à la variable s) :

$$\tau^2 = \sum_{k=1}^{p-1}\sum_{s=1}^{p-1}\left(\frac{k^2 s}{p}\right)\xi^{k+ks} = \sum_{s=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{s}{p}\right)\xi^{k+ks}$$

   puisqu'on a vu que $\left(\dfrac{k^2 s}{p}\right) = \left(\dfrac{s}{p}\right)$. Donc

$$\tau^2 = \sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\sum_{k=1}^{p-1}\left(\xi^{1+s}\right)^k$$

   Comme : si $1+s \neq 0$, $\displaystyle\sum_{k=1}^{p-1}\left(\xi^{1+s}\right)^k = \sum_{k=0}^{p-1}\left(\xi^{1+s}\right)^k - 1 = \frac{(\xi^{1+s})^p - 1}{\xi^{1+s}-1} - 1 = -1.$

   et si $1+s = 0$, $\displaystyle\sum_{k=1}^{p-1}\left(\xi^{1+s}\right)^k = \sum_{k=1}^{p-1} 1 = p-1$, On trouve donc :

$$\tau^2 = \left(\frac{1}{p}\right)(p-1) - \sum_{s=2}^{p-1}\left(\frac{s}{p}\right)$$

   Or, on a vu en fin de partie précédente que $\displaystyle\sum_{s=1}^{p-1}\left(\frac{s}{p}\right) = 0$, donc $\displaystyle\sum_{s=2}^{p-1}\left(\frac{s}{p}\right) = -\left(\frac{1}{p}\right)$,

$$\boxed{\tau^2 = \left(\frac{1}{p}\right)p = \epsilon(p)p}$$

3. On considère q, un nombre premier impair et distinct de p.

   Pour tout entier $k \in [\![1, q-1]\!]$, $\binom{q}{k} = q \times (q-1)(q-2)\dots(q-k+1)k! \in \mathbb{Z}$

   Donc q divise $k! \times \binom{q}{k}$.

   Or pour tout $i \in [\![1, k]\!]$, $i \wedge q = 1$, donc d'après le lemme de Gauss :

$$\boxed{\forall\, k \in [\![1, q-1]\!],\ q | \binom{q}{k}}$$

   On démontre alors le résultat demandé par récurrence :

$$\left(\sum_{i=0}^{s} a_i\right)^q = \left(\underbrace{\sum_{i=0}^{s-1} a_i}_{=A} + a_s\right)^q = \sum_{k=0}^{q} \binom{k}{q} A^k a_s^{q-k}$$

   Or $q | \binom{k}{q}$, donc en plongeant modulo q :

$$\left(\sum_{i=0}^{s} a_i\right)^q \equiv A^0 a_s^{q-0} + A^q a_s^0 \equiv a_s^q + A^q \ [q]$$

   Puis, on applique le résultat à l'ordre $s-1$ pour calculer A^q :

$$\boxed{\left(\sum_{i=0}^{s} a_i\right)^q = \sum_{i=0}^{s} a_i^q \ [q]}$$

4. Avec le résultat précédent, on trouve (modulo q) :

$$\tau^q = \left(\sum_{k=1}^{p-1} a_k\right)^q \equiv \sum_{k=1}^{p-1} a_k^q \equiv \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)^q \xi^{qk} \ [q]$$

   Puis, comme q est un nombre impair et que $\left(\frac{k}{p}\right) = \pm 1$, on a $\left(\frac{k}{p}\right)^q = \left(\frac{k}{p}\right)$.

$$\boxed{\left(\frac{q}{p}\right)\tau^q \equiv \sum_{k=1}^{p-1} \left(\frac{q}{p}\right)\left(\frac{k}{p}\right)\xi^{qk} \equiv \sum_{s=1}^{p-1} \left(\frac{s}{p}\right)\xi^s \equiv \tau \ [q]}$$

   En exploitant toujours le changement de variable $k \to s$ avec $s = kq$.

5. Par ailleurs

$$\tau^{q-1} = \left(\tau^2\right)^{\frac{q-1}{2}} = (\epsilon(p)p)^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}}$$

   Or $p^{\frac{q-1}{2}}$ ressemble au calcul du symbole de Legendre :

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

$$\boxed{\tau^{q-1} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) \ [q]}$$

▷ Corrigé de l'exercice 5.2

1. Comme τ n'est pas nul, il est inversible dans $\mathbb{F}_q$, on a donc deux résultats concernant τ^{q-1} :

$$\tau^{q-1} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)^{-1} = \left(\frac{q}{p}\right) \ [q]$$

On a $\left(\frac{q}{p}\right)^{-1} = \left(\frac{q}{p}\right)$, car il s'agit d'un élément de $\{-1, 1\}$.
Enfin, ces deux nombres congruents modulo q sont deux nombres de $\{-1, 1\}$, donc leur équivalence modulo q signifie leur égalité.

> Pour p et q deux nombres premiers impairs distincts, $\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$

2. Il s'agit de calculer le symbole de Legendre $\left(\frac{17}{41}\right)$ en exploitant la réciprocité quadratique :

$$\left(\frac{17}{41}\right) = (-1)^{16\times 40/4} \left(\frac{41}{17}\right) = 1 \left(\frac{7}{17}\right) = -1$$

car $41 \equiv 7[17]$, et puisqu'on sait que 7 n'est pas un résidu quadratique modulo 17.

> 17 n'est pas un carré de $\dfrac{\mathbb{Z}}{41\mathbb{Z}}$

▷ Corrigé de l'exercice 6.1

1. Soient $a, a' \in \mathbb{Z}$, $m, m' \geqslant 3$, impairs tels que $m \wedge m' = 1$.
Supposons que $m = \prod_{i=1}^{s} p_i^{\alpha_i}$ et $m' = \prod_{j=1}^{r} {p'_j}^{\beta_j}$.
Comme $m \wedge m' = 1$, alors pour tout $i \in \mathbb{N}_s$ et $j \in \mathbb{N}_r$, $p_i \neq p'_j$.
On a alors

$$\left(\frac{aa'}{m}\right) = \prod_{i=1}^{s} \left(\frac{aa'}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{\alpha_i} \prod_{i=1}^{s} \left(\frac{a'}{p_i}\right)^{\alpha_i} = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right)$$

par multiplicativité du symbole de Legendre.
Puis :

$$\left(\frac{a}{mm'}\right) = \left(\frac{a}{\prod_{i=1}^{s} p_i^{\alpha_i} \prod_{j=1}^{r} {p'_j}^{\beta_j}}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{\alpha_i} \prod_{j=1}^{r} \left(\frac{a}{p'_j}\right)^{\beta_i} = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$$

> $\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right)$ et $\left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$

2. $51 = 3 \times 17$:

$$\left(\frac{14}{51}\right) = \left(\frac{14}{3}\right)\left(\frac{14}{17}\right) = \left(\frac{-1}{3}\right)\left(\frac{-3}{17}\right) = -1 \times -1 = 1$$

> $\left(\frac{14}{51}\right) = 1$

▷ Corrigé de l'exercice 6.2

Soient $n, m \in \mathbb{Z}$, impairs, positifs et premiers entre eux.
• si $n \wedge m \neq 1$, alors il existe un facteur premier commun noté p à n et m.

Dans ce cas, dans la décomposition $\prod_{p|n,\, p\in\mathcal{P}} \left(\frac{m}{p}\right)^{v_p(n)}$ se trouve un facteur nul.

De même pour $\prod_{p|m,\, p\in\mathcal{P}} \left(\frac{n}{p}\right)^{v_p(m)}$.

Et donc $\left(\frac{m}{n}\right) = 0 = \left(\frac{n}{m}\right)$.

•. Supposons que $m = \prod_{i=1}^{s} p_i^{\alpha_i}$ et $n = \prod_{j=1}^{r} {p'_j}^{\beta_j}$ avec $m \wedge n = 1$,

donc pour tout $i \in \mathbb{N}_s$ et $j \in \mathbb{N}_r$: $p_i \neq p'_j$.

Par multiplicativité, et comme $(-1)^{\frac{(p_i-1)(p'_j-1)}{4}} = \theta(p_i, p'_j)$:

$$\begin{aligned}\left(\frac{n}{m}\right) &= \prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{p'_j}{p_i}\right)^{\alpha_i\beta_j} = \prod_{i=1}^{s}\prod_{j=1}^{r}\left[(-1)^{\frac{(p_i-1)(p'_j-1)}{4}}\left(\frac{p_i}{p'_j}\right)\right]^{\alpha_i\beta_j} = \prod_{i=1}^{s}\prod_{j=1}^{r}\left[\theta(p_i,p'_j)\left(\frac{p_i}{p'_j}\right)\right]^{\alpha_i\beta_j} \\ &= \prod_{i=1}^{s}\left(\prod_{j=1}^{r}\theta(p_i,p'_j)^{\alpha_i\beta_j}\right) \times \prod_{i=1}^{s}\left(\prod_{j=1}^{r}\left(\frac{p_i}{p'_j}\right)^{\alpha_i\beta_j}\right) = \prod_{i=1}^{s}\theta(p_i, \prod_{j=1}^{r}{p'_j}^{\beta_j})^{\alpha_i} \times \left(\frac{m}{n}\right) \\ &= \prod_{i=1}^{s}\theta(p_i,n)^{\alpha_i} \times \left(\frac{m}{n}\right) = \theta(m,n)\left(\frac{m}{n}\right)\end{aligned}$$

Comme $\theta(m,n) = \theta(m,n)^{-1}$:

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

▷ Corrigé de l'exercice 6.3

Soit n un entier impair, on utilise les définitions et les propriétés multiplicatives de ϵ et ω :

$$\left(\frac{-1}{n}\right) = \prod_{j=1}^{r}\left(\frac{-1}{p'_j}\right)^{\beta_j} = \prod_{j=1}^{r}\epsilon(p_j)^{\beta_j} = \epsilon\left(\prod_{j=1}^{r}{p'_j}^{\beta_j}\right) = \epsilon(n)$$

Et

$$\left(\frac{2}{n}\right) = \prod_{j=1}^{r}\left(\frac{2}{p'_j}\right)^{\beta_j} = \prod_{j=1}^{r}\omega(p_j)^{\beta_j} = \omega\left(\prod_{j=1}^{r}{p'_j}^{\beta_j}\right) = \omega(n)$$

Puis par expression analytique de ϵ et ω :

$$\boxed{\text{Pour tout } n \text{ entier impair positif : } \left(\frac{-1}{n}\right) = \epsilon(n) = (-1)^{\frac{n-1}{2}} \text{ et } \left(\frac{2}{n}\right) = \omega(n) = (-1)^{\frac{n^2-1}{8}}}$$