Problème. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel $n \geqslant 2$.

1) -a- Soit $(x, x') \in \mathbb{Z}^2$.

$\Rightarrow$ Supposons $x \equiv x'\ [n]$.
Alors

$$\begin{aligned} \overline{x} &= \{y \in \mathbb{Z} \,/\, x \equiv y\ [n]\} \\ &= \{y \in \mathbb{Z} \,/\, x' \equiv y\ [n]\} \text{ car } x \equiv x'\ [n] \text{ et par transitivité de } \equiv \\ &= \overline{x'}. \end{aligned}$$

$\Leftarrow$ Supposons $\overline{x} = \overline{x'}$. Comme $x \in \overline{x}$ alors $x \in \overline{x'}$ donc $x \equiv x'\ [n]$.

On a donc bien : $\boxed{x \equiv x'\ [n] \Leftrightarrow \overline{x} = \overline{x'}}$.

-b- Montrons que $\{\overline{x} \,/\, x \in \mathbb{Z}\} = \{\overline{x} \,/\, x \in [\![0, n-1]\!]\}$.
L'inclusion $\supset$ est évidente.
Inversement, soit $x \in \mathbb{Z}$. Et posons r le reste de la division euclidienne de x par n, alors $r \in [\![0, n-1]\!]$.
Puis comme $x \equiv r\ [n]$ alors d'après 1)-a-, $\overline{x} = \overline{k}$.
La deuxième inclusion est donc prouvée.
Enfin, les classes d'équivalence $\overline{x}$ où $x \in [\![0, n-1]\!]\}$ sont deux à deux distinctes. En effet si $\overline{x} = \overline{y}$ alors d'après 1)-a-, $x \equiv y\ [n]$ donc $n | x - y$. Or $x - y \in [\![-(n-1), n-1]\!]$ donc $x - y = 0$ c'est-à-dire $x = y$.
Par conséquent, $\boxed{\{\overline{x} \,/\, x \in \mathbb{Z}\} \text{ est fini et contient } n \text{ éléments.}}$

2) Prenons deux classes équivalences $\overline{x}$ et $\overline{y}$. Et choisissons un autre représentant x' et y' pour chacune d'entre elles. On a donc :

$$\overline{x} = \overline{x'} \qquad\qquad \overline{y} = \overline{y'}$$

et donc d'après 1)-a-

$$x \equiv x'\ [n] \qquad\qquad y \equiv y'\ [n] \quad (*).$$

Pour la somme, on a par définition

$$\overline{x} + \overline{y} = \overline{x+y} \qquad\qquad \overline{x'} + \overline{y'} = \overline{x'+y'}.$$

Il s'agit de prouver que l'on obtient le même résultatn à savoir, $\overline{x+y} = \overline{x'+y'}$.
Ce qui est bien le cas car en sommant les deux congruences $(*)$ et en utilisant 1)-a-, on obtient $\overline{x+y} = \overline{x'+y'}$.
Même raisonnement pour le produit.
$\boxed{\text{Ces opérations sont donc bien définies}}$.

3) Tout d'abord d'après la définion $+$ et $\times$ son bien des lois de composition interne.
Soit $(\overline{x}, \overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2$, alors

$$\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x} \qquad \text{(on a utilisé la commutativité de } + \text{ dans } \mathbb{Z}).$$

Puis

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{x}.$$

L'autre sens est obtenu par comutativité de $+$. Donc $+$ admet un neutre : $\overline{0}$.
Enfin

$$\overline{x} + \overline{-x} = \overline{x + (-x)} = \overline{0}.$$

L'autre sens est obtenu par commutativité de $+$. Donc $\overline{x}$ admet un opposé : $\overline{-x}$.
Reste à démontrer : l'associativité de $+$, de $\times$, l'existence d'un neutre pour $\times$ $(\overline{1})$, la distributivité de $\times$ par rapport à $+$.

4) -a-

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

-b- $\mathbb{Z}/3\mathbb{Z}$ est intègre (aucun produit nul sans que l'un des facteurs ne le soit) et est un corps (c'est un anneau et les éléments non nuls $\overline{1}$ et $\overline{2}$ sont inversibles d'inverse $\overline{2}$ et $\overline{1}$).
$\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre ($\overline{22} = \overline{0}$) et n'est pas un corps ($\overline{2}$ n'a pas d'inverse).

5) On pose $\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{U}_n \\ & \overline{x} & \mapsto & \mathrm{e}^{\frac{2\,\mathrm{i}\,x\pi}{n}} \end{array}$.

- f est bien définie. Pour $x \in \mathbb{Z}$, $f(\overline{x})$ est bien définie car ne dépend pas du représentant choisi. En effet si x' est un autre représentant alors $x \equiv x'\ [n]$ donc $x' = x + kn$ où $k \in \mathbb{Z}$. Alors

$$f(\overline{x'}) = \mathrm{e}^{\frac{2\,\mathrm{i}\,x'\pi}{n}} = \mathrm{e}^{\frac{2\,\mathrm{i}(x+kn)\pi}{n}} = \mathrm{e}^{\frac{2\,\mathrm{i}\,x'\pi}{n}}\mathrm{e}^{2\,\mathrm{i}\,k\pi} = \mathrm{e}^{\frac{2\,\mathrm{i}\,x'\pi}{n}} = f(\overline{x}).$$

- Surjectivité. Soit $z \in\in \mathbb{U}_n$, $z = \mathrm{e}^{\frac{2\,\mathrm{i}\,x\pi}{n}}$ où $x \in \mathbb{Z}$ alors immédiatement, $f(\overline{x}) = z$.
- Injectivité. Soit $(\overline{x}, \overline{x'}) \in (\mathbb{Z}/n\mathbb{Z})^2$ tel que $f(\overline{x}) = f(\overline{x'})$ alors

$$\mathrm{e}^{\frac{2\,\mathrm{i}\,x\pi}{n}} = \mathrm{e}^{\frac{2\,\mathrm{i}\,x'\pi}{n}} \quad \text{donc} \quad \frac{2x\pi}{n} \equiv \frac{2x'\pi}{n}\ [2\pi] \quad \text{donc} \quad x \equiv x'\ [n] \quad \text{donc} \quad \overline{x} = \overline{x'}.$$

- Morphisme. Soit $(\overline{x}, \overline{x'}) \in (\mathbb{Z}/n\mathbb{Z})^2$,

$$f(\overline{x} + \overline{x'}) = f(\overline{x + x'}) = \mathrm{e}^{\frac{2\,\mathrm{i}(x+x')\pi}{n}} = \mathrm{e}^{\frac{2\,\mathrm{i}\,x\pi}{n}}\mathrm{e}^{\frac{2\,\mathrm{i}\,x'\pi}{n}} = f(\overline{x})f(\overline{x'}).$$

Conclusion : f est un isomorphisme et donc $\boxed{(\mathbb{Z}/n\mathbb{Z}, +) \text{ et } (\mathbb{U}_n, \times) \text{ sont isomorphes}}$.

6) -a- Supposons n non premier, alors $n = ab$ où a et b sont deux entiers $2 \leqslant a \leqslant n-1$ et $2 \leqslant b \leqslant n-1$.
Alors $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$ avec $\overline{a}$ et $\overline{b}$ non nuls.
Donc $\boxed{\mathbb{Z}/n\mathbb{Z} \text{ n'est pas intègre}}$.

-b- Soit $a \in \mathbb{Z}$.

$$\begin{aligned} \overline{a} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists \overline{a'} \in \mathbb{Z}/n\mathbb{Z} \ / \ \overline{a}\overline{a'} = \overline{1} \quad (\overline{a}\overline{a'} = \overline{a'}\overline{a} \text{ par commutativité }) \\ &\Leftrightarrow \exists a' \in \mathbb{Z} \ / \ \overline{aa'} = \overline{1} \\ &\Leftrightarrow \exists a' \in \mathbb{Z} \ / \ aa' \equiv 1\ [n] \quad \text{(d'après 1)-a-)} \\ &\Leftrightarrow \exists (a', k) \in \mathbb{Z}^2 \ / \ aa' - kn = 1 \end{aligned}$$

$$\boxed{\overline{a} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \Leftrightarrow a \wedge n = 1} \quad \text{(théorème de Bezout)}$$

D'après le DM10 et la définition de l'indicatrice d'Euler, $\boxed{\text{le nombre d'éléments de } (\mathbb{Z}/n\mathbb{Z})^* \text{ est } \varphi(n)}$.

-c- On a $4 \times 34 - 9 \times 15 = 1$ donc $-9 \times 15 \equiv 1[34]$ donc $\overline{-915} = \overline{1}$. $\boxed{\text{L'inverse de } \overline{15} \text{ est donc } \overline{-9} = \overline{6}}$.

-d- $\Rightarrow$ Par contraposée, si n n'est pas premier alors d'après 6)-a-, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre donc n'est pas un corps.
$\Leftarrow$ Supposons p premier. Soit $\overline{x}$ un élément non nul de $\mathbb{Z}/n\mathbb{Z}$ alors x n'est pas divisible par p. Comme p est premier alors $p \wedge n = 1$ et donc d'après 6)-b-, $\overline{x}$ est inversible. Donc $\mathbb{Z}/n\mathbb{Z}$ est un anneau où tout élément non nul est iversible. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps

7) -a- Soit $x \in \mathbb{Z}$,

$$\overline{x}^2 = \overline{1} \Leftrightarrow (\overline{x} - \overline{1})((\overline{x} + \overline{1})) = \overline{0}$$
$$\Leftrightarrow \overline{x} - \overline{1} = \overline{0} \quad \text{ou} \quad \overline{x} + \overline{1} = \overline{0}$$
$$\boxed{\overline{x}^2 = \overline{1} \Leftrightarrow \overline{x} = \overline{1} \quad \text{ou} \quad \overline{x} = -\overline{1} = \overline{p-1}}.$$

-b- $\boxed{\text{On déduit immédiatement de 7)-a- que les seuls éléments qui sont leur propres inverse sont } \overline{1} \text{ et } \overline{p-1}}$.

8) Le but de cette question est de prouver le théorème de Wilson :

$$p \text{ premier } \Leftrightarrow (p-1)! \equiv -1\ [p].$$

-a- Si $p = 2$ alors $(p-1)! = 1 \equiv -1\ [2]$. Donc l'implication directe est prouvée.

-b- Soit $p \geqslant 3$. Dans le produit $\prod_{k=1}^{p-1} \overline{k}$ on regroupe les éléments de $k = 2$ à $p-2$ par paire (élément,son inverse); cela est possible d'après 7)-b- car seuls les éléments extrêmes de la somme sont égaux à leur propre inverse. Le produit se simplifie alors en ne laissant que les deux termes extrêmes

$$\prod_{k=1}^{p-1} \overline{k} = \overline{1} \times \overline{p-1} = \overline{1} \times \overline{-1} = \overline{p-1}.$$

-c- $\Rightarrow$ Supposons p premier. Si $p = 2$ d'après 8)-a-, l'implication est prouvée.

Si $p \geqslant 3$ alors d'après 8)-b-, $\overline{\prod_{k=1}^{p-1} k} = \overline{p-1}$ c'est-à-dire $\overline{(p-1)!} = \overline{p-1}$ donc d'après 1)-a-, $(p-1)! \equiv -1\ [p]$.

$\Leftarrow$ Supposons $(p-1)! \equiv -1\ [p]$.
Par l'absurde si p n'est pas premier alors $\mathbb{Z}/p\mathbb{Z}$ n'est pas intègre, donc il existe un produit $\overline{a}\overline{b} = \overline{o}$ sans que $\overline{a}$ et $\overline{b}$ ne le soient.

Ce produit fait partie de $\prod_{k=1}^{p-1} \overline{k}$ donc $\prod_{k=1}^{p-1} \overline{k} = \overline{0}$ donc $(p-1)! \equiv 0\ [p]$, ce qui est absurde.

On a donc bien : $\boxed{p \text{ premier } \Leftrightarrow (p-1)! \equiv -1\ [p].}$