Dans ce problème les questions : 1), 3), 4) et 6) sont obligatoires. Le reste est facultatif.

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

Soit n un entier naturel $n \geqslant 2$. Le but de ce problème est d'introduire l'anneau $\mathbb{Z}/n\mathbb{Z}$.

On rappelle que la relation de congruence "modulo n" est une relation d'équivalence sur $\mathbb{Z}$. Pour tout entier relatif x, on note $\overline{x}$ la classe d'équivalence de x pour la relation de congruence "modulo n",

$$\overline{x} = \{y \in \mathbb{Z} \,/\, x \equiv y\,[n]\}.$$

1) -a- Soit $(x, x') \in \mathbb{Z}^2$. Montrer que : $x \equiv x'\,[n] \Leftrightarrow \overline{x} = \overline{x'}$.

   -b- Montrer que $\{\overline{x} \,/\, x \in \mathbb{Z}\}$ est fini et contient n élément.
   Cet ensemble est noté $\mathbb{Z}/n\mathbb{Z}$.

2) On définit les lois d'addition de multiplication sur $\mathbb{Z}/n\mathbb{Z}$:

$$\forall(\overline{x}, \overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2, \qquad \overline{x} + \overline{y} = \overline{x+y} \qquad\qquad \overline{x} \cdot \overline{y} = \overline{xy}.$$

   Montrer que ces opérations sont bien définies (il s'agit de prouver que la définition ne dépend pas des représentants choisis x et y pour les classes d'équivalence $\overline{x}$ et $\overline{y}$).

3) Montrer que muni de ces deux lois, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif. On ne rédigera que la démonstration de la commutativité de $+$, de l'existence d'un neutre pour $+$ et de l'existence d'un opposé de $\overline{x}$ pour la loi $+$.
   Quelles sont les autres propriétés qui restent à démontrer?

4) -a- Ecrire les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

   -b- Lesquels de ces deux anneaux sont intègres? sont des corps?

5) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes.

6) -a- Montrer que si n n'est pas premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

   -b- Soit $a \in \mathbb{Z}$. Montrer que $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.
   On rappelle que $(\mathbb{Z}/n\mathbb{Z})^*$ est l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
   Quel est le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$? (penser au DM10).

   -c- Déterminer l'inverse de $\overline{15}$ dans $\mathbb{Z}/34\mathbb{Z}$.

   -d- Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

7) Dans cette question p désigne un nombre premier.

   -a- Résoudre dans $\mathbb{Z}/p\mathbb{Z}$ l'équation $\overline{x}^2 = \overline{1}$.

   -b- En déduire que les seuls éléments qui sont leur propres inverse sont $\overline{1}$ 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- Montrer l'application directe lorsque $p = 2$.

   -b- Soit $p \geqslant 3$. Montrer que $\displaystyle\prod_{k=1}^{p-1} \overline{k} = \overline{p-1}$. *On pourra utiliser 7)-b-.*

   -c- En déduire le théorème de Wilson.