TD2. Arithmétique modulaire

Exercice 1
Résoudre dans $\mathbb{Z}/13\mathbb{Z}$ l'équation $z^2 + z + \overline{7} = \overline{0}$.

Exercice 2
(a) Ecrire les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ (on notera $\overline{n}$ la classe d'un entier n).
(b) En déduire que le groupe additif $(\mathbb{Z}/5\mathbb{Z}, +)$ est *engendré* par chacun de ses éléments non nuls, c'est-à-dire : si $\overline{x} \neq 0$, $\{k\overline{x},\ k \in \mathbb{Z}\} = \mathbb{Z}/5\mathbb{Z}$.
(c) Quels sont les éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$? Trouver l'inverse de chacun d'eux.
(d) Faire la liste des puissances de $\overline{3}$. En déduire que le groupe multiplicatif $((\mathbb{Z}/5\mathbb{Z})^\times, \times)$ est engendré par $\overline{3}$. Que dire de ses autres éléments ?

Exercice 3
Démontrer la proposition du cours : $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier ou $n = 0$.

Exercice 4 (Petit théorème de Fermat)
Soit p un premier. On rappelle que les éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ sont les $\overline{n}$ pour $n \in \mathbb{Z}$ premier à p. On note $(\mathbb{Z}/p\mathbb{Z})^\times$ l'ensemble des éléments inversibles.
(a) Montrer que $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ est un groupe d'ordre (cardinal) $p - 1$.
(b) Sachant que l'ordre d'un élément $\overline{n}$ (plus petit entier s tel que $\overline{n}^s = \overline{1}$) divise l'ordre du groupe (théorème de Lagrange), en déduire, pour $n \in \mathbb{Z}$ premier à p :
$$n^{p-1} \equiv 1 \pmod{p} \ .$$
(c) En déduire que $n^p \equiv n \pmod{p}$ pour tout entier n.
(d) Application : déterminer le reste modulo 11 de 102^{102}.

Exercice 5
(a) Démontrer que la relation binaire $\mathcal{R}$ définie sur $E = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ par
$$(a, b)\,\mathcal{R}(c, d) \iff ad = bc$$
est une relation d'équivalence.
(b) Justifier que l'on note $\frac{a}{b}$ la classe de $(a, b) \in E$.
(c) Montrer que les opérations + et × définies dans l'exercice 7 du TD1 permettent de définir des opérations dans $E/\mathcal{R}$. En déduire les règles d'addition et de multiplication des fractions.
(d) Montrer que les lois + et × ainsi définies font de $E/\mathcal{R}$ un anneau commutatif unitaire intègre.
(e) Montrer que tout élément non nul de $E/\mathcal{R}$ est inversible, ce qui entraîne que $E/\mathcal{R}$ est un corps. Quel est ce corps ?
On peut faire la même construction en remplaçant $\mathbb{Z}$ par n'importe quel anneau intègre A. L'ensemble quotient obtenu s'appelle le *corps des fractions* de A.