

Feuille 4. L'anneau $\mathbb{Z}/n\mathbb{Z}$ **Exercice 1.**

1. Ecrire l'ensemble des multiples de \bar{x} dans $\mathbb{Z}/5\mathbb{Z}$ pour $x = 0, \dots, 4$.
2. Ecrire l'ensemble des multiples de \bar{x} dans $\mathbb{Z}/6\mathbb{Z}$ pour $x = 0, \dots, 5$.
3. Soient n et x deux entiers naturels. Démontrer que les trois propositions suivantes sont équivalentes.
 - (a) \bar{x} admet un inverse pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.
 - (b) x et n sont premiers entre eux.
 - (c) tout élément de $\mathbb{Z}/n\mathbb{Z}$ est multiple de \bar{x} dans $\mathbb{Z}/n\mathbb{Z}$.
4. Calculer l'inverse de $\bar{4}$ dans $\mathbb{Z}/9\mathbb{Z}$.
5. Calculer l'inverse de $\bar{8}$ dans $\mathbb{Z}/15\mathbb{Z}$.

Exercice 2. Résoudre les équations suivantes dans $\mathbb{Z}/37\mathbb{Z}$:

1.
$$\begin{cases} \bar{3}x + \bar{7}y = \bar{3} \\ \bar{6}x - \bar{7}y = \bar{0} \end{cases}$$
2. $x^2 - \bar{31}x + \bar{18} = \bar{0}$
Indication : $\bar{6}^2 = -\bar{1}$.

Exercice 3.

1. Justifier que l'anneau $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
2. Observer que si $u \in \mathbb{Z}/2\mathbb{Z}$ alors $u^2 = u$, et si $u \in \mathbb{Z}/3\mathbb{Z}$ alors $u^3 = u$. En déduire que si $x \in \mathbb{Z}/6\mathbb{Z}$ alors $x^3 = x$.
3. Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les équations suivantes :
 - (a) $x^5 - \bar{1} = \bar{0}$.
 - (b) $x^5 - \bar{2} = \bar{0}$.
 - (c) $x^4 + x^3 + \bar{2} = \bar{0}$.

Exercice 4. Trouver les entiers relatifs n tels que
$$\begin{cases} n \equiv 3 \pmod{17} \\ n \equiv 4 \pmod{11} \end{cases}.$$
Exercice 5. Résoudre dans \mathbb{Z} le système
$$\begin{cases} x \equiv 1 \pmod{27} \\ x \equiv 13 \pmod{17} \end{cases}.$$
Exercice 6. On veut résoudre dans $\mathbb{Z}/33\mathbb{Z}$ l'équation $x^2 + \bar{2} = \bar{0}$.

1. Montrer que $n \in \mathbb{Z}$ vérifie $n^2 + 2 \equiv 0 \pmod{33}$ si et seulement si :

$$n^2 + 2 \equiv 0 \pmod{3} \text{ et } n^2 + 2 \equiv 0 \pmod{11}.$$

2. Observer que si $n \in \mathbb{Z}$, alors $n^2 \equiv 0 \pmod{3}$ si $n \in 3\mathbb{Z}$, et $n^2 \equiv 1 \pmod{3}$ sinon.
3. Observer que $3^2 \equiv -2 \pmod{11}$, et en déduire que dans $\mathbb{Z}/11\mathbb{Z}$ on a

$$x^2 + \bar{2} = (x - \bar{3})(x + \bar{3}).$$

4. Donner toutes les solutions de l'équation $x^2 + \bar{2} = \bar{0}$ dans $\mathbb{Z}/33\mathbb{Z}$.

Exercice 7. Trouver tous les entiers naturels $n \in \mathbb{N}$ tels que $1 \leq n \leq 105$ et les restes des divisions euclidiennes de n par 3, 5, 7 sont respectivement 1, 2, 3.

Exercice 8.

1. Dresser la liste des cubes de $\mathbb{Z}/13\mathbb{Z}$.
2. Soient $(x, y, z) \in \mathbb{Z}^3$ tels que $5x^3 + 11y^3 + 13z^3 = 0$. Montrer que 13 divise x , y et z .
3. L'équation $5x^3 + 11y^3 + 13z^3 = 0$ a-t-elle des solutions entières non nulles ?

Exercice 9.

1. Déterminer l'inverse de $\bar{17}$ dans $\mathbb{Z}/25\mathbb{Z}$ et l'inverse de $\bar{25}$ dans $\mathbb{Z}/17\mathbb{Z}$.
2. Déterminer les solutions entières de l'équation $17x + 25y = 13$.

Exercice 10.

1. Soit n un entier naturel non premier, $n \geq 5$. Montrer qu'il existe deux éléments de $\mathbb{Z}/n\mathbb{Z}$, différents de $\bar{0}$, dont le produit est $\bar{0}$. En déduire que $(n-1)!$ est divisible par n .
2. Soit p un nombre premier ≥ 5 . Montrer que pour tout entier $x = 2, \dots, p-2$, il existe un entier $y = 2, \dots, p-2$ différent de x , tel que le produit xy soit congru à 1 modulo p . En déduire que si p est un nombre premier, alors $(p-1)! + 1$ est divisible par p . (C'est le théorème de Wilson).

Exercice 11. Montrez que tous les facteurs premiers impairs de $n^2 + 1$, où $n \in \mathbb{Z}$, sont de la forme $4k + 1$. Pour cela, on évaluera de deux manières le carré de $n^{\frac{p-1}{2}}$ modulo p .

Exercice 12. Soient p et q deux entiers premiers entre eux. Démontrer que $(\mathbb{Z}/pq\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$.

Exercice 13. Soit $n = 561 = 3 \times 11 \times 17$. Montrer grâce au théorème chinois que si a est premier avec n , alors $a^{n-1} \equiv 1 \pmod{n}$.

Exercice 14. Soient p et q deux nombres premiers distincts, $n = pq$ et t un entier tel que $t \equiv 1 \pmod{\varphi(n)}$ où φ est l'indicatrice d'Euler.

1. Montrer que $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $x^t = x$ en distinguant les quatre cas possibles pour $d = \text{pgcd}(x, pq)$.
2. On considère u un entier premier avec $\varphi(n)$ et v son inverse dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Montrer que les fonctions ψ_u et ψ_v de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ définies par $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $\psi_u(x) = x^u$ et $\psi_v(x) = x^v$ sont des fonctions réciproques l'une de l'autre et sont donc bijectives.