Correction de la feuille d'exercices n° 6
Calculs dans $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 :

1. Construire les tables d'addition et de multiplication dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.
2. Pour chaque élément de ces 2 ensembles, citer l'opposé et l'inverse s'il existe. Citer les diviseurs de zéro.

Solution :

Dressons la table d'addition dans $\mathbb{Z}/5\mathbb{Z} = \{\dot{0}, \dot{1}, \dots, \dot{4}\}$:

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

On a :
$-\dot{0} = \dot{0}$
$-\dot{1} = \dot{4}$
$-\dot{2} = \dot{3}$
$-\dot{3} = \dot{2}$
$-\dot{4} = \dot{1}$

Dressons la table de multiplication dans $\mathbb{Z}/5\mathbb{Z} = \{\dot{0}, \dot{1}, \dots, \dot{4}\}$:

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Les éléments inversibles sont $\dot{1}$, $\dot{2}$, $\dot{3}$ et $\dot{4}$.
De plus $\dot{1}^{-1} = \dot{1}$, $\dot{2}^{-1} = \dot{3}$, $\dot{3}^{-1} = \dot{2}$ et $\dot{4}^{-1} = \dot{4}$ d'après la table ci-contre.
Seule la classe $\dot{0}$ est un diviseur de zéro car $\dot{0} \times \dot{1} = \dot{0}$ (par exemple).

Remarque : 5 est premier donc, d'après le corollaire 2.6 du cours, toute classe non nulle de $\mathbb{Z}/5\mathbb{Z}$ est inversible, ce que nous avons trouvé d'après la table de multiplication. Mais ce corollaire ne nous donne pas les inverses des classes inversibles.

Dressons la table d'addition dans $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dots, \dot{5}\}$:

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

On a :
$-\dot{0} = \dot{0}$
$-\dot{1} = \dot{5}$
$-\dot{2} = \dot{4}$
$-\dot{3} = \dot{3}$
$-\dot{4} = \dot{2}$
$-\dot{5} = \dot{1}$

Dressons la table de multiplication dans $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \dot{5}\}$:

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Les éléments inversibles sont $\dot{1}$ et $\dot{5}$.
De plus $\dot{1}^{-1} = \dot{1}$ et $\dot{5}^{-1} = \dot{5}$ d'après la table ci-contre.
Les classes $\dot{0}, \dot{2}, \dot{3}$ et $\dot{4}$ sont les diviseurs de zéro car $\dot{0} \times \dot{1} = \dot{0}$, $\dot{2} \times \dot{3} = \dot{0}$, et $\dot{4} \times \dot{3} = \dot{0}$.

Remarque : D'après le théorème 2.5 du cours, $\dot{a} \in \mathbb{Z}/6\mathbb{Z}$ est inversible si et seulement si a et 6 sont premiers entre eux, c'est-à-dire si et seulement si $PGCD(a, 6) = 1$.

On retrouve que les classes inversibles sont $\dot{1}$ et $\dot{5}$, puisque $PGCD(1, 6) = 1$ et $PGCD(5, 6) = 1$. Tandis que $PGCD(2, 6) = 2$, $PGCD(3, 6) = 3$ et $PGCD(4, 6) = 2$.

Exercice 2 :

1. *Résoudre dans* $\mathbb{Z}/7\mathbb{Z}$ *:* $\dot{x}^2 + \dot{x} + \dot{1} = \dot{0}$.

$\dot{x}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{x}^2 + \dot{x} + \dot{1}$	$\dot{1}$	$\dot{3}$	$\dot{0}$	$\dot{6}$	$\dot{0}$	$\dot{3}$	$\dot{1}$

Alors $\mathcal{S} = \{\dot{2}, \dot{4}\}$.

2. *Résoudre dans* $\mathbb{Z}/6\mathbb{Z}$ *:* $\dot{x}^2 + \dot{x} + \dot{1} = \dot{0}$.

$\dot{x}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{x}^2 + \dot{x} + \dot{1}$	$\dot{1}$	$\dot{3}$	$\dot{1}$	$\dot{1}$	$\dot{3}$	$\dot{1}$

Alors $\mathcal{S} = \emptyset$.

3. *Résoudre dans* $\mathbb{Z}/7\mathbb{Z}$ *:* $\left\{ \begin{array}{rcl} \dot{x} + \dot{y} & = & \dot{3} \\ \dot{x} - \dot{y} & = & \dot{5} \end{array} \right.$

$$\left\{ \begin{array}{rcll} \dot{x} + \dot{y} & = & \dot{3} & L_1 \\ \dot{x} - \dot{y} & = & \dot{5} & L_2 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcll} \dot{x} + \dot{y} & = & \dot{3} & L_1 \\ \dot{2}\dot{x} & = & \dot{1} & L_2 \leftarrow L_2 + L_1 \end{array} \right.$$

Dans $\mathbb{Z}/7\mathbb{Z}$, $\dot{2}$ est inversible et $\dot{2}^{-1} = \dot{4}$ donc $\dot{2}\dot{x} = \dot{1} \Leftrightarrow \dot{x} = \dot{1} \times \dot{2}^{-1} = \dot{1} \times \dot{4} = \dot{4}$.
Alors $\dot{y} = \dot{3} - \dot{4} = \dot{6}$. Ainsi $\mathcal{S} = \{(\dot{4}, \dot{6})\}$.

Exercice 3 : *Déterminer les entiers relatifs* n *tels que* $n^2 - 3n + 6 \equiv 0 \ (mod\ 5)$. *(Travailler dans* $\mathbb{Z}/5\mathbb{Z}$*)*

$$\begin{aligned} n^2 - 3n + 6 \equiv 0 \ (mod\ 5) &\Leftrightarrow \dot{n}^2 + \dot{2}\dot{n} + \dot{1} = \dot{0} \text{ dans } \mathbb{Z}/5\mathbb{Z} \\ &\Leftrightarrow (\dot{n} + \dot{1})^2 = \dot{0} \text{ dans } \mathbb{Z}/5\mathbb{Z}. \end{aligned}$$

$\dot{n}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$(\dot{n} + \dot{1})^2$	$\dot{1}$	$\dot{4}$	$\dot{4}$	$\dot{1}$	$\dot{0}$

$(\dot{n} + \dot{1})^2 = \dot{0} \Leftrightarrow \dot{n} = \dot{4} \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $n = 4 + 5k$.

Alors $\mathcal{S} = \{4 + 5k, \ k \in \mathbb{Z}\}$.

Exercice 4 : *Résoudre dans* $\mathbb{Z}/7\mathbb{Z}$ *:* $\left\{ \begin{array}{rcl} \dot{3}\dot{x} + \dot{2}\dot{y} & = & \dot{1} \\ \dot{5}\dot{x} + \dot{4}\dot{y} & = & \dot{3} \end{array} \right.$

Solution : On échelonne le système par la méthode du pivot comme en algèbre linéaire :

$$\left\{ \begin{array}{rcrcll} \dot{3}\dot{x} & + \dot{2}\dot{y} & = & \dot{1} & L_1 \\ \dot{5}\dot{x} & + \dot{4}\dot{y} & = & \dot{3} & L_2 \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{rcrcll} \dot{3}\dot{x} & + \dot{2}\dot{y} & = & \dot{1} & L_1 \\ & \dot{2}\dot{y} & = & \dot{4} & L_2 \leftarrow \dot{3}L_2 - \dot{5}L_1 \end{array} \right.$$

L'équivalence entre les deux systèmes est rendue possible par le fait que $\dot{3}$ (coefficient de L_2) est *inversible* dans $\mathbb{Z}/7\mathbb{Z}$. Le système étant échelonné, on résout la seconde équation pour déterminer $\dot{y}$. Puisque $\text{pgcd}(2,7) = 1$, l'élément $\dot{2}$ est inversible dans $\mathbb{Z}/7\mathbb{Z}$; un bref calcul des valeurs successives de $\dot{2}\dot{z}$ pour $\dot{z} = \dot{0}, \dot{1}, \ldots$ donne $\dot{2}^{-1} = \dot{4}$ (en effet $\dot{2} \times \dot{4} = \dot{8} = \dot{1}$ dans $\mathbb{Z}/7\mathbb{Z}$), ainsi

$$\dot{2}\dot{y} = \dot{4} \qquad \Longleftrightarrow \qquad \dot{y} = \dot{2}^{-1} \times \dot{4} = \dot{4} \times \dot{4} = \dot{16} = \dot{2}.$$

En remplaçant $\dot{y}$ par $\dot{2}$ dans L_1, on obtient $\dot{3}\dot{x} = \dot{1} - \dot{2}\dot{y} = -\dot{3} = \dot{4}$. Mais $\dot{3}$ est inversible dans $\mathbb{Z}/7\mathbb{Z}$ et $\dot{3}^{-1} = \dot{5}$ (en effet $\dot{3} \times \dot{5} = \dot{15} = \dot{1}$), par conséquent

$$\dot{3}\dot{x} = \dot{4} \qquad \Longleftrightarrow \qquad \dot{x} = \dot{3}^{-1} \times \dot{4} = \dot{5} \times \dot{4} = \dot{20} = \dot{6}.$$

En conclusion, l'ensemble des solutions du système est

$$\mathcal{S} = \left\{(\dot{6}, \dot{2})\right\}.$$

Exercice 5 : Résoudre dans $\mathbb{Z}/n\mathbb{Z}$ les congruences suivantes :

1. $3x \equiv 7\ mod 16$
2. $4x \equiv 9\ mod 13$

Solution :

1. $3x \equiv 7\ mod\ 16 \iff \dot{3}\dot{x} = \dot{7}$ dans $\mathbb{Z}/_{16\mathbb{Z}}$.
   $16 = 2^4$ donc $PGCD(16,3) = 1$. $\dot{3}$ est inversible donc $\dot{3}\dot{x} = \dot{7} \iff \dot{x} = \dot{3}^{-1}\dot{7}$.
   Cherchons l'inverse de $\dot{3}$, qui appartient aussi à $(\mathbb{Z}/_{16\mathbb{Z}})^*$. 16 étant une puissance de 2 seules les classes représentées par un entier impair sont inversibles.

$\dot{x} \in (\mathbb{Z}/_{16\mathbb{Z}})^*$	$\dot{1}$	$\dot{3}$	$\dot{5}$	$\dot{7}$	$\dot{9}$	$\dot{11}$	$\dot{13}$	$\dot{15}$
$\dot{3}\dot{x}$	$\dot{3}$	$\dot{9}$	$\dot{15}$	$\dot{5}$	$\dot{11}$	$\dot{1}$		

   Alors $\dot{3}^{-1} = \dot{11}$ et $\dot{x} = \dot{3}^{-1} \times \dot{7} \iff \dot{x} = \dot{7} \times \dot{11} = \dot{77} = \dot{13}$
   $\iff \exists k \in \mathbb{Z}$ tel que $x = 13 + 16k$
   Alors l'ensemble des solutions de la congruence $3x \equiv 7\ mod\ 16$ est $\mathcal{S} = \{13 + 16k / k \in \mathbb{Z}\}$.
2. $4x \equiv 9\ mod\ 13 \iff \dot{4}\dot{x} = \dot{9}$ dans $\mathbb{Z}/_{13\mathbb{Z}}$.
   13 est premier danc toutes les classes non nulles sont inversibles.
   $\dot{4}$ est inversible donc $\dot{4}\dot{x} = \dot{9} \iff \dot{x} = \dot{4}^{-1}\dot{9}$.
   Cherchons l'inverse de $\dot{4}$, qui appartient aussi à $(\mathbb{Z}/_{13\mathbb{Z}})^*$.

$\dot{x} \in (\mathbb{Z}/_{13\mathbb{Z}})^*$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	$\dot{11}$	$\dot{12}$
$\dot{4}\dot{x}$	$\dot{4}$	$\dot{8}$	$\dot{12}$	$\dot{3}$	$\dot{7}$	$\dot{11}$	$\dot{2}$	$\dot{6}$	$\dot{10}$	$\dot{1}$		

   Alors $\dot{4}^{-1} = \dot{10}$ et $\dot{x} = \dot{4}^{-1} \times \dot{9} \iff \dot{x} = \dot{10} \times \dot{9} = \dot{90} = \dot{12}$
   $\iff \exists k \in \mathbb{Z}$ tel que $x = 12 + 13k$
   Alors l'ensemble des solutions de la congruence $4x \equiv 9\ mod\ 13$ est $\mathcal{S} = \{12 + 13k / k \in \mathbb{Z}\}$.