Université de Saint Etienne **Arithmétique**
L1 MISPIC **Année 2024/2025**

TD 3 : Arithmétique modulaire $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 (F)

1. *Etablir la table de multiplication de* $\mathbb{Z}/5\mathbb{Z}$. *En déduire que* $\mathbb{Z}/5\mathbb{Z}$ *est un corps commutatif.*
2. *Trouver l'opposé de* $\bar{3}$ *dans* $\mathbb{Z}/5\mathbb{Z}$.
3. *Trouver l'inverse de* $\bar{3}$ *dans* $\mathbb{Z}/5\mathbb{Z}$.
4. *Résoudre dans* $\mathbb{Z}/5\mathbb{Z}$ *l'équation* $x^2 + x + \bar{1} = \bar{0}$.

Exercice 2 (F)

1. *Donner la table de multiplication de* $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.
2. *Déterminer les éléments inversibles de* $\mathbb{Z}/6\mathbb{Z}$ *et donner leur inverse.*

Exercice 3 (F) *On travaille dans* $A = \mathbb{Z}/43\mathbb{Z}$

1. *Est-ce que* A *est un corps ?*
2. *Trouver une relation de Bézout entre* 43 *et* 30.
3. *En déduire l'inverse de* 30 *dans* A.

Exercice 4 (F)

1. *Résoudre les équations suivantes :*

$$(a)\ \ n^2 + n + 3 = 0 \text{ dans } \mathbb{Z}/5\mathbb{Z}, \qquad (b)\ \ n^2 - n = 2 \text{ dans } \mathbb{Z}/3\mathbb{Z}$$

2. *Résoudre les congruences suivantes dans* $\mathbb{Z}$ *:*

$$(a)\ \ n^2 + n + 3 \equiv 0 \quad [5], \qquad (b)\ \ n^2 - n \equiv 2 \quad [3]$$

Exercice 5 (F) *Montrer que pour tout* $n \in \mathbb{N}$, $2^{3n} \equiv (-1)^n \bmod 9$

Exercice 6 (*) *Les questions suivantes sont indépendantes.*

1. *Quel est le reste dans la division euclidienne de* 6^{537} *par 7 ?*
2. *Quel est le reste dans la division euclidienne de* 5^{2024} *par 7 ?*
3. *Quel est le reste dans la division euclidienne de* 793^{123} *par 7 ?*
4. *Quels sont les entiers naturels* n *tels que* $2^n - 1$ *est divisible par 9 ?*
5. *Démontrer que 13 divise* $3^{126} + 5^{126}$.
6. *Démontrer que* $2^{4n+1} + 3^{4n+1}$ *est divisible par 5 quel que soit l'entier naturel* n.

Exercice 7 (*)

1. *Etablir la table de multiplication de* $\mathbb{Z}/8\mathbb{Z}$.
2. *Enumérer les couples* $(a, b) \in (\mathbb{Z}/8\mathbb{Z})^2$ *tels que* $a \times b = \bar{0}$.
3. *Résoudre dans* $\mathbb{Z}/8\mathbb{Z}$ *les équations* $x^2 + x + \bar{1} = \bar{0}$, $x^2 + x = \bar{0}$ *et* $x^2 + x + \bar{4} = \bar{0}$.

Exercice 8 (F) *On considère l'équation* $x^5 - x = 0$. *Résoudre cette équation dans*

$$(a)\ \mathbb{Z}/5\mathbb{Z}, \qquad (b)\ \mathbb{Z}/4\mathbb{Z}.$$

Exercice 9 (F) *Résoudre le système* $\begin{cases} x+y=\bar{2} \\ x-y=\bar{3} \end{cases}$ *dans*

$$(a)\ \mathbb{Z}/5\mathbb{Z}, \qquad (b)\ \mathbb{Z}/6\mathbb{Z}.$$

Exercice 10 (*)

1. *Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{N}^*$.*
   Montrer que si a et n sont premiers entre eux alors $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. (Indication : Utiliser Bézout).
2. *La réciproque est-elle vraie ?*
3. *Calculer l'inverse de $\overline{18}$ dans $\mathbb{Z}/35\mathbb{Z}$.*
4. *Calculer l'inverse de $\overline{21}$ dans $\mathbb{Z}/32\mathbb{Z}$.*

Exercice 11 (F) *Déterminer l'ensemble des x dans $\mathbb{Z}$ tels que*

$$(a)\ \begin{cases} x \equiv 0 \quad [3] \\ x \equiv 1 \quad [6] \end{cases} \qquad (b)\ \begin{cases} x \equiv 1 \quad [13] \\ x \equiv 4 \quad [6] \end{cases} \qquad (c)\ \begin{cases} x \equiv 12 \quad [150] \\ x \equiv 7 \quad [41] \end{cases} \qquad (d)\ \begin{cases} x \equiv 3 \quad [91] \\ x \equiv 4 \quad [17] \end{cases}$$

Exercice 12 (*) *Un enfant dispose d'un nombre n de briques de construction. Lorsque qu'il fait un mur de 4 briques de large, il lui reste 3 briques non-utilisées. Lorsqu'il fait un mur de 5 (resp. 7, resp. 9) briques de large, il lui reste 1 (resp. 3, resp. 2) briques non-utilisées. Déterminer les valeurs possibles pour n, ainsi que la plus petite d'entre elles.*

Exercice 13 *Le but de l'exercice est de déterminer tous les couples d'entiers $(m\,;n) \in \mathbb{N}^2$ tels que $2^m - 3^n = 1$.*

1. **(*)** *Déterminer, pour tout entier naturel n, le reste dans la division euclidienne de 3^n par 8.*
2. **(**)** *En déduire que si $(m\,;n)$ est solution de $2^m - 3^n = 1$, alors $m \leqslant 2$.*
3. **(*)** *Conclure en donnant les solutions de l'équation.*

Exercice 14 *Soit p un nombre premier et soit $G = ((\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}, \times)$.*

1. **(*)** *Montrer que G est un groupe commutatif.*
2. **(**)** *Soit $a \in G$, Montrer que $a^{p-1} = \bar{1}$.*
3. **(*)** *Montrer que $\forall a \in \mathbb{Z}$, $a^p \equiv a \bmod p$ (“*Petit théorème de Fermat*”)*
4. **(*)** *Soit $p = 5$. Montrer qu'il existe un morphisme de groupe bijectif entre G et $(\mathbb{Z}/4\mathbb{Z}, +)$*
5. **(***)** *Soit p arbitraire. Montrer qu'il existe un morphisme de groupe bijectif entre G et $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$*

Exercice 15 *Soit $n \in \mathbb{N}$ fixé. On s'intéresse à l'équation $a^n + b^n = c^n$ avec $a, b, c \in \mathbb{N}$.*

1. **(**)** *Soit $n = 2$*
   (a) Montrer que $\forall x \in \mathbb{Z}$, $x^2 \not\equiv 2 \bmod 3$.
   (b) Soit a, b, c une solution de l'équation, montrer que a ou b est un multiple de 3.
   (c) Montrer que si c est un multiple de 3 alors a et b sont des multiples de 3.
   (d) Montrer que a ou b est multiple de 4 et que a, b ou c est multiple de 5
2. **(***...*)** *Soit $n \geqslant 3$. Montrer qu'il n'existe aucun triplet d'entiers a, b, c tous non-nuls tels que $a^n + b^n = c^n$ (“*Grand Théorème de Fermat*”)*