TD 7 - Arithmétique dans $\mathbb{Z}/n\mathbb{Z}$

Prérequis

- ☐ Réviser les notions de *relation d'équivalence* et de *partition*.
- ☐ Revoir les notions de *classe d'équivalence* et d'*ensemble quotient*.
- ☐ Connaître la définition de la relation de congruence modulo n et savoir montrer que c'est une relation d'équivalence.
- ☐ Réviser les règles de calculs modulaires exprimées comme relation de congruence et comme égalités entre classes d'équivalence.

Objectifs

- ☐ Savoir faire le lien entre une équation modulaire et une équation dans $\mathbb{Z}$.
- ☐ Savoir simplifier des expressions modulaires.
- ☐ Savoir résoudre un système de congruence lorsque les modules sont premiers entre eux.
- ☐ Savoir identifier si un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible (ou non), et le cas échéant, savoir calculer son inverse multiplicatif.

1 Avant le TD

Échauffement 1.

1. Décrire la classe d'équivalence de -3 modulo 7.
2. Les égalités suivantes sont-elles vraies ou fausses ?

$$6 \equiv 4 \bmod 2 \qquad 5 \equiv -5 \bmod 12 \qquad 11 \equiv -2 \bmod 13 \qquad 24 \equiv 0 \bmod 12$$

3. Simplifier l'expression $1234 \bmod 7$.
4. Le cas particulier de $n = 2$. Montrer que pour tout $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2 \iff 2 \mid (a + b)$.

2 Propriétés de la congruence et calcul modulaire

Exercice 1 (Congruence et division euclidienne)**.** Soit $a \in \mathbb{Z}, b \in \mathbb{N}^*$ Montrer les propositions suivantes :

1. Soit $a = bq + r$ la division euclidienne de a par b. Alors $a \equiv r \bmod b$ et $a \equiv r \bmod q$.
2. Soit t un entier vérifiant $a \equiv t \bmod b$ et tel que $0 \leq t < b$. Alors t est le reste de la division euclidienne de a par b.

Exercice 2 (Calcul modulaire)**.** Simplifier les expressions modulaires suivantes.

1. $2025 \bmod 13$ **2.** $10! \bmod 17$ **3.** $5^{10} \bmod 11$ **4.** $2005^{2006} \bmod 7$

Exercice 3.

1. Montrer que $10^6 \equiv 1 \bmod 7$
2. Quel est le chiffre des unités de 3^{12} ?
3. Montrer que pour tout $n \in \mathbb{N}, \quad 7 \mid 2^{4^n} + 5$.

Exercice 4 (Critères de divisibilités)**.** Soit $n = (a_m \dots a_0)_{10}$.

1. Montrer que $2 \mid n$ si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$.
2. Montrer que $3 \mid n$ si et seulement si $3 \mid a_0 + \dots + a_m$.
3. Montrer que $5 \mid n$ si et seulement si $a_0 \in \{0, 5\}$.

3 Systèmes d'équations modulaires

Exercice 5 (Un premier système d'équations modulaires)**.** On considère le système suivant :

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}.$$

1. En supposant qu'il existe une solution $x \in \mathbb{Z}$, décrire quelle forme x doit avoir.
2. En déduire l'ensemble des solutions du système.

Exercice 6 (Le théorème de Sun Zi (dit des « restes chinois »))**.** L'objectif de cet exercice est de prouver le théorème suivant.

Théorème de Sun Zi. Soit n, m deux entiers premiers entre eux. Soit $a, b \in \mathbb{Z}$. Considérons le système suivant :

$$\begin{cases} x \equiv a \bmod n \\ x \equiv b \bmod m \end{cases}$$

Alors :

— le système $(\triangle)$ admet une infinité de solutions dans $\mathbb{Z}$, et

— l'ensemble de solutions S forme une classe d'équivalence modulo nm.

Autrement, un tel système admet une unique solution modulo nm.

1. (Forme de l'ensemble des solutions). Supposons qu'il existe $x_0, x_1 \in \mathbb{Z}$ deux solutions du système.
   - **a.** Montrer que ces solutions sont égales modulo nm.
   - **b.** En déduire la forme de l'ensemble des solutions en fonction d'une solution particulière (si elle existe).
2. (Existence et construction d'une solution).
   - **a.** À l'aide d'une identité de Bézout, identifier deux entiers $e, f \in \mathbb{Z}$ tels que :

$$\begin{cases} e \equiv 1 \bmod n \\ e \equiv 0 \bmod m \end{cases} \quad \text{et} \quad \begin{cases} f \equiv 0 \bmod n \\ f \equiv 1 \bmod m \end{cases}$$

b. En déduire deux entiers $e', f' \in \mathbb{Z}$ tels que :

$$\begin{cases} e \equiv a \bmod n \\ e \equiv 0 \bmod m \end{cases} \quad \text{et} \quad \begin{cases} f \equiv 0 \bmod n \\ f \equiv b \bmod m \end{cases}$$

c. En déduire une solution particulière du système.

3. Conclure la preuve du théorème.

4. Résoudre dans $\mathbb{Z}$ le système suivant :

$$\begin{cases} x \equiv 9 \bmod 17 \\ x \equiv 3 \bmod 10 \end{cases}.$$

Exercice 7 (Inverses et équations modulaires)**.**

1. 5 est-il inversible modulo 15 ? modulo 13 ? Si oui quel est son inverse ?

2. 110 est-il inversible modulo 63 ? modulo 32 ? Si oui quel est son inverse ?

3. Résoudre dans $\mathbb{Z}/13\mathbb{Z}$ l'équation $5x = 1$. En déduire les solutions dans $\mathbb{Z}$ de l'équation $5x \equiv 1 \bmod 13$.

4 Après le TD

Exercice 8. Soit $n = (a_m \dots a_0)_{10}$. Montrer que $9 \mid n$ si et seulement si $9 \mid a_0 + \cdots + a_m$.

Exercice 9. **1.** On considère le système suivant :

$$\begin{cases} 2x \equiv 4 \bmod 6 \\ x \equiv 1 \bmod 5 \end{cases}.$$

En supposant qu'il existe une solution $x \in \mathbb{Z}$, décrire quelle forme x doit avoir.

2. En déduire l'ensemble des solutions du système.

Exercice 10 (Système à 3 équations)**.** On considère le système d'équations suivant :

$$\begin{cases} x \equiv 3 \bmod 17 \\ x \equiv 4 \bmod 11 \\ x \equiv 5 \bmod 6 \end{cases}$$

1. En observant que les modules sont 2 à 2 premiers entre eux, trouver une solution particulière $x_0 \in \mathbb{Z}$ du système.

2. Soit $x \in \mathbb{Z}$. Montrer que si x est une solution du système alors, $x \in x_0 + 17 \cdot 11 \cdot 6\mathbb{Z}$.

3. Montrer que l'ensemble des solutions entières du système est exactement $x_0 + 17 \cdot 11 \cdot 6\mathbb{Z}$.