

Session 1

Exercice 1 (Arithmétique Modulaire).

1. Donner les résultats des formules suivantes :
 - $12 \cdot 12 \bmod 11$
 - $5 - 7 \bmod 11$
 - $8 \cdot 5^{-1} \bmod 11$
2. Écrire les tables de multiplication dans $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.
3. Trouver l'inverse modulaire de $n + 1$ modulo n^2 , quand $n \in \mathbb{Z}_{\geq 1}$.
4. En utilisant l'algorithme d'Euclide étendu, calculez (s'il existe)
 - (a) L'inverse de 5 dans $\mathbb{Z}/26\mathbb{Z}$.
 - (b) L'inverse de 22 dans $\mathbb{Z}/79\mathbb{Z}$.
 - (c) L'inverse de 441 dans $\mathbb{Z}/777\mathbb{Z}$.

Exercice 2 (Restes Chinois).

Trouver le plus petit entier positif x tel que (à la fois) :

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Exercice 3 (Algebre Linéaire).

Rappelons quelques opérations d'algèbre linéaire:

- Produit d'un vecteur par un scalaire :

$$\text{Pour } a \in \mathbb{Z} \text{ et } \mathbf{b} \in \mathbb{Z}^n, a \cdot \mathbf{b} = \begin{bmatrix} ab_1 \\ \vdots \\ ab_n \end{bmatrix} \in \mathbb{Z}^n.$$

- Produit de deux vecteurs :
Pour $\mathbf{a} \in \mathbb{Z}^n$ et $\mathbf{b} \in \mathbb{Z}^n$, $\langle \mathbf{a}, \mathbf{b} \rangle = a_1b_1 + \cdots + a_nb_n \in \mathbb{Z}$.
- Produit de Hadamard :

$$\text{Pour } \mathbf{a} \in \mathbb{Z}^n \text{ et } \mathbf{b} \in \mathbb{Z}^n, \mathbf{a} \circ \mathbf{b} = \begin{bmatrix} a_1b_1 \\ \vdots \\ a_nb_n \end{bmatrix} \in \mathbb{Z}^n.$$

- Produit tensoriel :

$$\text{Pour } \mathbf{a} \in \mathbb{Z}^n \text{ et } \mathbf{b} \in \mathbb{Z}^m, \mathbf{a} \otimes \mathbf{b} = \begin{bmatrix} a_1 \cdot \mathbf{b} \\ \vdots \\ a_n \cdot \mathbf{b} \end{bmatrix} \in \mathbb{Z}^{nm}.$$

- Produit matrice-vecteur :

$$\text{Pour } \mathbf{A} \in \mathbb{Z}^{n \times m} \text{ et } \mathbf{b} \in \mathbb{Z}^m, \mathbf{A}\mathbf{b} = \begin{bmatrix} \sum_{i=1}^m a_{1,i}b_i \\ \vdots \\ \sum_{i=1}^m a_{n,i}b_i \end{bmatrix} \in \mathbb{Z}^n.$$

- Produit matrice-matrice :

$$\text{Pour } \mathbf{A} \in \mathbb{Z}^{n \times p} \text{ et } \mathbf{B} \in \mathbb{Z}^{p \times m}, \mathbf{A}\mathbf{B} = \begin{bmatrix} \sum_{i=1}^p a_{1,i}b_{i,1} & \cdots & \sum_{i=1}^p a_{1,i}b_{i,m} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^p a_{n,i}b_{i,1} & \cdots & \sum_{i=1}^p a_{n,i}b_{i,m} \end{bmatrix} \in \mathbb{Z}^{n \times m}.$$

1. Donner les résultats des formules suivantes :

$$\bullet \langle \mathbf{a}, \mathbf{b} \rangle \quad \bullet \mathbf{a} \circ \mathbf{b} \quad \bullet \mathbf{a} \otimes \mathbf{b} \quad \bullet \mathbf{A} \mathbf{b} \quad \bullet \mathbf{A} \mathbf{B}$$

$$\text{pour } \mathbf{a} = \begin{bmatrix} 4 \\ 9 \\ 2 \end{bmatrix}, \mathbf{b} = \begin{bmatrix} 5 \\ 1 \\ 0 \end{bmatrix}, \mathbf{A} = \begin{bmatrix} 1 & 5 & 7 \\ 1 & 8 & 2 \\ 2 & 7 & 3 \\ 9 & 3 & 3 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 2 & 3 \\ 6 & 7 \\ 9 & 7 \end{bmatrix}$$

2. Soit $\|\mathbf{v}\|_{\infty} \leq \beta$ et $\mathbf{v} \in \mathbb{Z}^n$, donner une borne supérieure de $\|\mathbf{v}\|_2$ où $\|\mathbf{v}\|_{\infty} = \max_i |v_i|$ et $\|\mathbf{v}\|_2 = \sqrt{\sum_{i=1}^n v_i^2}$.