Exercice 1 Résoudre dans $\mathbb{Z}/2\mathbb{Z}$ le système linéaire

$$\begin{cases} x+2y+3z &= 0 \\ 4x+5y+6z &= 1 \\ 7x+8y+4z &= 2 \end{cases}$$

Même question dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

Exercice 2

1. La famille de vecteurs
$$\{v_1 = [1,2,3], v_2 = [-1,-1,1], v_3 = [2,1,1]\}$$
est-elle libre sur $K = \mathbb{Z}/2\mathbb{Z}$?
2. Si cette famille n'est pas libre, déterminez une combinaison linéaire non triviale.
3. Donner la dimension et le nombre d'éléments du sous-espace vectoriel de K^3 engendré par $\{v_1, v_2, v_3\}$.
4. Soit φ l'application linéaire de K^3 dans K^3 telle que les images des vecteurs de la base canonique $\{e_1, e_2, e_3\}$ soient $v_1 = \varphi(e_1), v_2 = \varphi(e_2), v_3 = \varphi(e_3)$. Déterminer le noyau et l'image de φ.

Mêmes questions sur $K = \mathbb{Z}/7Z$.

Exercice 3 Soit la matrice à coefficients dans $\mathbb{Z}/5\mathbb{Z}$ $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & -1 & 1 \\ 2 & 1 & 1 \end{pmatrix}$. Déterminez A^{12} en appliquant l'algorithme d'exponentiation rapide. Quel est le plus petit entier $n > 0$ tel que $A^n = I_3$? Exprimer A^{-1} comme une puissance entière positive de A.

Exercice 4 Calculez l'inverse de la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & -1 & 1 \\ 2 & 1 & 1 \end{pmatrix}$ dans $\mathbb{Z}/5\mathbb{Z}$ et dans $\mathbb{Z}/2\mathbb{Z}$. Vérifiez en effectuant le produit de A par son inverse !

Exercice 5 (cryptographie de Hill) On code les lettres de A à Z par les nombres de 1 à 26, l'espace par 0, , par 27 et . par 28. On groupe les caractères par paires et on utilise la matrice $A = \begin{pmatrix} 5 & 7 \\ 1 & 15 \end{pmatrix}$ (mod 29).

1. Coder le message suivant : "VIVE LES VACANCES"
2. A quelle condition sur la matrice A le destinataire du message codé pourra t'il le déchiffrer ?
3. Décoder : "IKYTYEH HSAHVRDAM "

Janvier 2021 : Cryptage matriciel à clef secrète (10 points)

Pour coder des messages pouvant contenir des caractères de diverses langues, on représente chaque caractère par un entier sur 16 bits (codage UTF16 par exemple). On décide ensuite de crypter le message par blocs de 2 caractères, en multipliant chaque vecteur v des 2 entiers représentant un bloc par une matrice carrée A de taille 2 modulo un entier p qui sera supposé premier dans les questions 1 à 6. La matrice A est tenue secrète, c'est la clef secrète du système de cryptage.

1. Dans quel intervalle se trouve un entier sur 16 bits ?
On suppose que p est un nombre premier qui permet de représenter de manière unique tous les entiers sur 16 bits par leur classe dans $\mathbb{Z}/p\mathbb{Z}$. Quel est le nombre minimal de bits de p ?
2. On admettra que $p = 65537$ est bien premier. On pose :
$$p = 65537, \quad A = \begin{pmatrix} 263 & 4122 \\ 1 & 1799 \end{pmatrix}$$
Crypter le vecteur v correspondant aux deux caractères "intégrale double" et "intégrale triple" représentés respectivement par les entiers 8748 et 8749, i.e. calculer $w = Av$ modulo p
3. Déterminer tous les vecteurs z à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ tels que $Az = Av$ modulo p pour $p = 65537$.
En déduire tous les vecteurs z à coefficients entiers qui vérifient $Az = Av$ modulo p.
Si on impose que les coordonnées de z sont dans l'intervalle du codage sur 16 bits, combien y-a-t-il de solutions ?

4. Que se passerait-il si on avait choisi la même matrice mais $p = 6551$?
5. Expliquer comment on peut décrypter, i.e. étant donné w quelconque, comment on trouve v tel que $Av = w$ modulo p.
6. Quel est le nombre de matrices A possibles pour $p = 65537$? Cela vous parait-il suffisant pour résister à une attaque de la clef secrète A par force brute ? Peut-on imaginer un autre type d'attaque ? Comment pourrait-on renforcer la sécurité ?
7. Dans cette question, on suppose que $p = 2^{16}$ et n'est donc pas premier. Peut-on appliquer l'algorithme du pivot de Gauss pour résoudre $Az = w = Av$ si on travaille modulo p bien que p ne soit alors pas premier ?
   En est-il de même pour la matrice
$$p = 65536, \quad A = \begin{pmatrix} 262 & 4122 \\ 1 & 1799 \end{pmatrix}$$
8. Quel(s) avantage(s) et inconvénient(s) y-a-t-il à travailler modulo 2^{16} par rapport à $p = 65537$?

Exercice 7 Parmi les octets suivants écrits en base 16 lesquels sont-ils de parité paire :
`0x7f`, `0x35`, `0x45`, `0xca`
Pour l'un de ces octets qui n'est pas de parité paire, déterminer les octets de parité paire qui ne différent que par un bit de cet octet.

Exercice 8 Parmi les parties suivantes de $\mathbb{Z}/2\mathbb{Z}^n$, lesquels sont des codes linéaires ? Si oui, en donner une matrice génératrice.

1. $n = 2, C = \{00, 10\}$.
2. $n = 4, C = \{0000, 1010, 0111, 1011, 0110\}$.
3. $n = 3, C = \{000, 100, 001, 111\}$.
4. $n = 4, C = \{0000, 0101, 1010, 1111\}$.
5. $n = 4, C = \{0000, 1011, 1000, 0011\}$.
6. $n = 4, C = \{0000, 1101, 1011, 1001\}$.

Exercice 9 On considère le code linéaire de matrice M sur $\mathbb{Z}/2\mathbb{Z}$ et le vecteur v :
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad v = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

1. Déterminer l'image w du vecteur v
2. Comment retrouve-t-on v à partir de son image $w = Mv$?
3. Déterminer la matrice de controle H ayant 3 lignes et 7 colonnes telle que l'ensemble des mots du code soit le noyau de H. Vérifiez que $Hw = 0$.
4. Montrez que tout vecteur dans l'image de M a au moins 2 composantes non nulles. Déterminer la distance de ce code.

Exercice 10

1. Créez une matrice M de taille 7,4 sur $\mathbb{Z}/2\mathbb{Z}$ telle que le code correspondant soit systématique et sa distance de Hamming 3.
2. Pour cette matrice, déterminer la matrice de controle H (3 lignes, 7 colonnes) telle que tout mot du code $w = Mv$ soit dans le noyau de H.
3. Calculer les entiers h_i dont l'écriture en base 2 est la i-ième colonne de H. En déduire comment corriger une erreur de transmission sur un vecteur $w \in K^7$ en utilisant la valeur de l'entier correspondant à Hw.
4. Peut-on réaliser un code linéaire de paramètres $n = 7, k = 4$ réalisant la borne de Singleton, i.e. une distance de 4 ?