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 "

Exercice 6 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 7 Soit $o_7, ..., o_0$ l'écriture en base 2 d'un octet o et $O(X) = o_7x^7 + ... + o_1x + o_0$. Déterminer le reste de la division euclidienne de $O(X)$ par $X+1$ dans $\mathbb{Z}/2\mathbb{Z}$ pour un octet de parité paire et pour un octet de parité impaire.
Soit b un entier compris entre 0 et 127, $b_6, ..., b_0$ son écriture en base 2 et $B(X) = b_6X^6 + ... + b_1X + b_0$ le polynôme associé dans $\mathbb{Z}/2\mathbb{Z}$.

1. Soit $P(X) = B(X)X$ et R le reste de la division euclidienne de P par $X+1$, montrer que $P+R$ correspond à un octet $\tilde{o}$ de parité paire.
2. Comment retrouve-t-on $b_6, ..., b_0$ à partir de $\tilde{o}_7, ..., \tilde{o}_0$?
3. Montrer que $O(X) = B(X)(X+1)$ correspond à un octet o de parité paire. Vérifiez avec $o =$`0x45`.
4. Comment retrouve-t-on $b_6, ..., b_0$ à partir de $o_7, ..., o_0$?
5. Écrire les matrices des 2 codages ci-dessus.

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 ?

Exercice 11 Code polynomial de polynome générateur $G(x) = x^4 + x + 1$ et paramètres $m = 4, n = 2^4 - 1 = 15, k = n - m = 11$.
On code 11 bits de données par un polynôme P ayant $k = 11$ coefficients dans $\mathbb{Z}/2\mathbb{Z}$ (donc de degré 10), on multiplie P par x^4 et on ajoute le reste de la division de Px^4 par G, le polynome obtenu Q a $n = 15$ coefficients.

1. Montrer que Q est divisible par G
   On transmet Q. Le destinataire vérifie alors que le polynôme reçu $\tilde{Q}$ est divisible par G, si oui il l'accepte, sinon il le corrige en tenant compte du reste R de la division de $\tilde{Q}$ par G.
2. Déterminer la liste des restes de division de x^0 à x^{14} par $x^4 + x + 1$ dans $\mathbb{Z}/2\mathbb{Z}[X]$, vérifiez qu'ils sont distincts 2 à 2. En déduire qu'un polynome multiple de G a au moins 3 coefficients non nuls (indication : considérer le reste par G de la somme de 2 monomes).
3. Comment peut-on corriger au plus proche une erreur de transmission sur un coefficient de $\tilde{Q}$?

Exercice 12 : algorithmes (bonus) Écrire et/ou programmer un ou plusieurs algorithmes réalisant les taches suivantes :

1. le calcul d'un octet de parité paire étant donné un entier compris entre 0 et 127, le test de parité d'un octet
2. le code de l'exercice 10 ou la création d'un code de Hamming binaire de paramètres $m = 7, n = 2^m - 1, k = 2^m - m - 1$ soit avec une matrice, soit en utilisant le polynôme $x^7 + x^3 + 1$, et la correction d'un mot au plus proche.
3. la réduction d'une matrice dans $\mathbb{Z}/2\mathbb{Z}$ par le pivot de Gauss, le calcul de l'inverse de matrice.