N.B. : les énoncés ci-dessous utilisent les conventions usuelles de l'algèbre linéaire, i.e. on utilise des vecteurs colonnes pour représenter des éléments de K^n et on effectue le produit Mv pour calculer l'image de v par l'application linéaire de matrice M. Les conventions transposées sont souvent utilisées dans le domaine du codage.

TD Exercice 1 Déterminer le code linéaire dont la matrice de contrôle est

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Compléter le code en ajoutant un 8ème bit pour réaliser une parité paire. Le code complété est-il auto-orthogonal ? Quelle est sa distance de Hamming ?

TD Exercice 2 Construire la matrice d'un code de Hamming binaire en écrivant en colonnes les entiers de 1 à 7 en base 2 et en permutant les colonnes de l'identité en fin de matrice. Coder un exemple de quartet (=4 bits). Comment corrige-t-on une erreur de transmission ?

TD Exercice 3 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 $\tilde{Q}$?

TD Exercice 4 Soit un code polynomial de polynome générateur un polynome irréductible primitif P de $\mathbb{Z}/2\mathbb{Z}[X]$. Montrer que la distance du code ne peut pas être 1 ou 2. À quelle condition a-t-on un code de Hamming binaire ? Comment peut-on corriger une erreur en utilisant les puissances d'un générateur de $\mathbb{Z}/2\mathbb{Z}[X]/P$?

TD Exercice 5 On se donne un générateur a de F_q^* et le polynôme $g(x) = (x - a)...(x - a^{2t})$ (donc $n - k = 2t$). Montrer que la distance du code polynomial de générateur g est $2t + 1$.

TD Exercice 6 On travaille sur le corps $\mathbb{Z}/5$, on pose $x_1 = 2, x_2 = -1, x_3 = -2, x_4 = 1$. On code un couple y_1, y_2 en déterminant la droite passant par (x_1, y_1) et x_2, y_2, et on complète y_1, y_2 par y_3 et y_4 les ordonnées des points d'abscisses x_3, x_4 de cette droite. Coder un exemple non trivial ($y_1 \neq y_2$). Modifier un des y_i, puis décoder le message modifié en cherchant deux polynômes Q_0, Q_1 non nuls de degrés au plus 2 et 1 tels que $Q_0(x_i) = y_i Q_1(x_i)$ (système linéaire homogène de 4 équations en les 5 coefficients de Q_0 et Q_1). Puis poser $P = Q_0/Q_1$ et en déduire y_1 et y_2.

TP Exercice 1 Écrire un programme permettant de rajouter un bit de parité à une liste composée de 7 bits. Puis un programme de vérification qui accepte un octet selon sa parité. On représentera l'octet par une liste de bits ou par un polynôme (le délimiteur ouvrant `poly1[` permet d'effectuer des opérations arithmétiques polynomiales), et on effectuera la vérification de deux manières, en comptant le nombre de 1 ou avec l'instruction de reste de division euclidienne polynomiale (`rem`).

TP Exercice 2 Créez une matrice M de taille 7,4 injective sur le corps $\mathbb{Z}/2$. Puis un programme qui teste si un vecteur est un mot de code et en extrait alors la partie avant codage. Vérifiez votre programme avec un vecteur Mv, on doit obtenir un mot de code.
Instructions utiles : `idn` (matrice identité), `ker` (noyau d'une application linéaire), `rank` (rang), `tran` (tranposée), `[op(A),op(B)]` (concaténation de matrice), `blockmatrix`.
Comparez avec le cas où M est une matrice de code systématique.
Quelle est la distance de votre code systématique ?
Si votre code linéaire n'est pas de distance 3, modifiez les 3 dernières lignes pour réaliser un code de distance 3. Peut-on réaliser la borne de Singleton ? Votre code est-il 1-correcteur parfait ?
Écrire un programme corrigeant une erreur éventuelle.

TP Exercice 3 Écrire un programme de codage polynomial utilisant $g = X^7 + X^3 + 1$
N.B. on obtient le polynôme X^{n-k} sous forme de polynome-liste dans Xcas par `poly1[1,0$(n-k)]`.

TP Exercice 4 Créer un code de Hamming binaire (15,11) (syndrome, fonction de codage, fonction de décodage avec correction)

TP Exercice 5 Programmer un code de Hamming binaire (7,4) ou/et (15,11) en utilisant un code polynomial de polynôme générateur irréductible primitif de degré 3 ou 4 sur $\mathbb{Z}/2$.

TP Exercice 6 Programmer le codage d'un code de Reed-Solomon i.e. obtenu en ajoutant $P(x_{k+1}), ..., P(x_n)$ où P est le polynôme d'interpolation du message $y_1, .., y_k$ en $x_1, ..., x_k$. Puis le décodage avec correction d'erreur.