Codes cycliques.

Exercice 1. Montrer que le polynôme $X^5 + X^4 + X + 1$ engendre un code cyclique binaire de longueur $n = 8$.

Exercice 2. Combien existe-t-il de codes cycliques binaires de longueur 4 ? Donner pour chacun une matrice génératrice et une matrice de contrôle.

Exercice 3. 1. Lesquels de ces polynômes engendrent-ils un code cyclique ternaire de longueur 9 ?

a) $X - 1$	*b*) $X^2 - 1$
c) $X^3 - 1$	*d*) $X^2 + X + 1$
e) $X^5 - 2X^4 + X^3 - X^2 + 2X - 1$	*f*) $X^6 + 1$

2. Soit C le code cyclique binaire de longueur 6 engendré par $g = 1 + X + X^2$. On note G la matrice génératrice de C associée de façon naturelle à g. Quel est le message qui, encodé par G, donne le mot (100011) ?

a) (1000)	*b*) (1100)
c) (0111)	*d*) (0101)
e) (1101)	*f*) (1011)

Exercice 4. Autre approche du code de Hamming binaire de longueur 7.
Soit $P = X^3 + X + 1 \in \mathbf{F}_2[X]$, et soit $\mathbf{K} = \mathbf{F}_2[X]/(P)$. On pose $\alpha = \mathrm{cl}(X) \in \mathbf{K}$.

1. a) Montrer que $\mathbf{K}$ est un corps ; calculer sa caractéristique et son cardinal.
b) Donner une base du $\mathbf{F}_2$-espace vectoriel $\mathbf{K}$. Lister toutes les racines primitives de l'unité de $\mathbf{K}$.

2. On considère le code binaire C de longueur 7 dont les mots $(c_0, c_1, \ldots, c_6) \in (\mathbf{F}_2)^7$ vérifient

$$\sum_{k=0}^{6} c_k \alpha^k = 0.$$

a) Montrer que C est un code cyclique.
b) Calculer la dimension de C.
c) Montrer qu'il n'existe pas de mots du code de poids 2.
d) Calculer la distance $d(C)$ de C. Donner un mot de poids $d(C)$.

3. a) Donner une matrice génératrice de C.
b) Déduire de la question précédente une matrice de contrôle de C. Retrouver $d(C)$ à partir de cette matrice de contrôle.
c) Montrer que le polynôme P engendre C.

Exercice 5. Généralisation : code de Hamming binaire de longueur $2^r - 1$.
Soit $\alpha \in \mathbf{F}_{2^r}^*$, on pose $n = 2^r - 1$. On considère l'application linéaire u de $(\mathbf{F}_2)^n$ dans $\mathbf{F}_{2^r}$ définie par

$$\forall (c_0, c_1, \ldots, c_{n-1}) \in (\mathbf{F}_2)^n,\ u(c_0, c_1, \ldots, c_{n-1}) = \sum_{k=0}^{n-1} c_k \alpha^k.$$

On note C le code binaire de longueur n défini par $C = ker(u)$.
1. Soit d la distance minimale de C. Montrer que $d \geq 3$ si et seulement si α est une racine primitive de l'unité de $\mathbf{F}_{2^r}$. On suppose dans la suite que $d \geq 3$.
2. Déterminer la dimension de C, montrer que C est un code parfait de distance 3.
3. En déduire que les colonnes d'une matrice de contrôle de C constituent tous les vecteurs non nuls de $\mathbf{F}_2^r$.
4. Soit P le polynôme défini par $P = \prod_{k=0}^{r-1} \left(X - \alpha^{2^k}\right)$. Montrer que $P \in \mathbf{F}_2[X]$, et que P divise $X^n - 1$ dans $\mathbf{F}_2[X]$.
5. Montrer que le code C est cylique engendré par P.

Exercice 6. 1. Montrer que le polynôme $g = (X-1)^5$ divise le polynôme $X^9 - 1$ dans $\mathbf{F}_3[X]$.
2. Soit C le code cyclique de longueur 9 sur $\mathbf{F}_3$, engendré par le polynôme g. Quelle est la dimension de C ? Quel est le nombre de mots de C ?
3. Développer le polynôme g dans $\mathbf{F}_3[X]$, en détaillant et justifiant les calculs.
4. Pourquoi la matrice

$$G = \begin{pmatrix} 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \end{pmatrix}$$

est-elle une matrice génératrice du code C ?
5. Montrer que C contient un mot de poids 3.
6. Montrer que le polynôme de contrôle de C est le polynôme $h = X^4 + 2X^3 + 2X + 1$.
7. Déterminer une matrice de contrôle de C.
8. Déterminer la distance minimum du code C et le nombre d'erreurs que C peut corriger.
9. Le mot $m = 121102210$ est reçu. Sous l'hypothèse d'au plus une erreur, quel est le mot de code émis ? Quel est le message envoyé, sachant qu'il est encodé par la matrice G ?