**Arithmétique et applications, graphes et combinatoire**

**Exercices d'entrainement**

**Corps finis** :

**1.** Soit $A = \mathbf{Z}/3\mathbf{Z}[x]$ et soit $f(x) = x^2 + 1 \in A$. Montrer que $f$ est irréductible mais pas primitive. Montrer que $g(x) = x^2 + x + 2$ est primitive dans $A$.

**2.** Montrer que $f(x) = x^2 + x + 2$ est primitive dans $\mathbf{Z}/5\mathbf{Z}[x]$ mais pas dans $\mathbf{Z}/11\mathbf{Z}[x]$ (pour ce dernier il suffit de montrer que $f$ est réductible).

**3.** Soient $a$ et $b$ les deux éléments de $\mathbb{F}_2[x]$ donnés par $a = x^5 + x^4 + x^3 + x^2$ et $b = x^4 + x^3 + x + 1$. Calculer $c = \text{pgcd}(a, b)$ et trouver deux polynômes $u, v \in \mathbb{F}_2[x]$ tels que $ua + vb = c$.

**4.** Soient $f(x) = x^4+x^3+x^2+x+1, g(x) = x^4+x^3+x^2+1, h(x) = x^4+x^3+1 \in \mathbb{F}_2[x]$. Parmi ces polynômes, un est primitif, un est irréductible et pas primitif et un est réductible. Préciser lesquels. Pour le polynôme qui est irréductible mais pas primtif, trouver l'ordre de $x$ dans la corps quotient corréspondant.

**5.** (a) Soit $p$ un nombre premier. Montrer que le polynôme $f(x) = x^2+1$ est irréductible sur $\mathbb{F}_p$ si et seulement si $p$ est congru à 3 mod 4.

(b) Déduire de la question précédente que, si $p$ est congru à 3 mod 4, $\mathbb{F}_p[x]/(x^2+1)$ est un corps à $p^2$ éléments.

**Codes correcteurs** : On écrit "un $[n, k]$-code linéaire" pour un code de dimension $k$ dans ${\mathbb{F}_2}^n$.

**6.** (a) Construire un code pour lequel les mots sont de longueur 15, la distance minimale est 8 contenant 16 mots. Quel est le nombre maximal d'erreurs corrigibles dans ce code?

(b) Construire un code pour lequel les mots sont de longueur 8, la distance minimale est 4 contenant 16 mots. Quel est le nombre maximal d'erreurs corrigibles dans ce code?

**7.** Est-t-il possible de construire un $[6, 2]$-code linéaire qui est 2 correcteur ?

**8.** Soit $C$ le $[7, 4]$-code de Hamming.

(a) Construire les mots de $C$.

(b) Corriger les vecteurs reçus : $r_1 = (0011101)$ et $r_2 = (0100101)$.

(c) Construire une liste des "coset leaders" et leurs syndromes.

**9.** (a) Construire le $[7,3]$-code $C$ avec matrice génératrice :

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

(b) Calculer la matrice de contrôle $H$ pour $C$.

(c) Pour quel $t$ est ce code $t$-correcteur ?

(d) Calculer les syndromes associés aux erreurs de poids $\leq t$.

(e) Parmi les vecteurs reçus $r_1 = (1100111), r_2 = (1111110), r_3 = (0111101)$, lesquels sont corrigibles par la méthode des syndromes ?

**Codes BCH** :

**10.** (a) Utiliser le polynôme primitif $p(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ afin de construire le polynôme générateur d'un code BCH 2-correcteur. Quels sont le paramètres $[n, k]$ pour ce code ?

(b) Utiliser le polynôme primitif $p(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ afin de construire le polynôme générateur d'un code BCH 3-correcteur. Quels sont le paramètres $[n, k]$ pour ce code ?

(c) Utiliser le polynôme primitif $p(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ afin de construire le polynôme générateur d'un $[15, 7]$-code BCH. Combine de mots sont dans ce code et combien d'erreurs sont corrigibles ?

**11.** Les facteurs irréductibles du polynôme $f(x) = x^{31} - 1 \in \mathbb{F}_2[x]$ sont $x + 1$ et six polynômes primitives de degré 5. Afin de construire un code BCH $t$-correcteur avec mots de longueur 31, on commence avec un polynômes primitif $p(x) \in \mathbb{F}_2[x]$ de degré 5 et un nombre à préciser de puissances de $a = \overline{x}$ dans le corps d'ordre 32 qui en résulte de $p(x)$. Cette procédure va déterminer un polynôme générateur $g(x)$, le nombre d'éléments d'une base et le nombre de mots dans ce code. Compléter le tableau suivant :

| $t$-corr., $t =$ | $a, a^2, \ldots a^s$, $s = ?$ | degré $g(x)$ | cardinal d'une base | nombre de mots |
|---|---|---|---|---|
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |

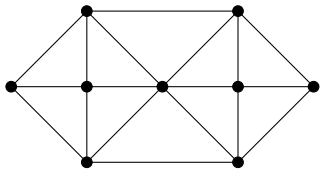
**Graphes** :

**12.** (a) Montrer qu'un graphe simple a un nombre pair de sommets de degré impair.

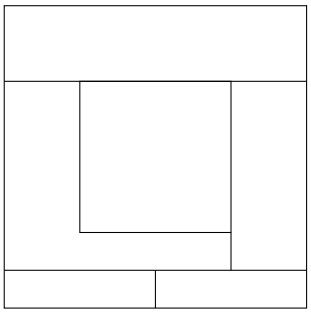
(b) Est-il possible de relier 15 ordinateurs de sorte que chaque appareil soit relié avec exactement trois autres ?

(c) Expliciter un graphe qui représente un ensemble de 6 ordinateurs dont chaque appareil soit relié avec exactement trois autres.

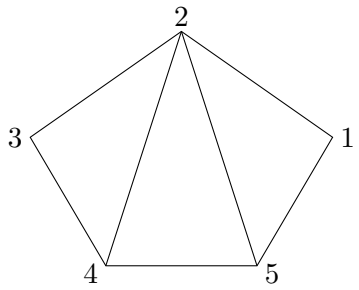
**13.** Est-ce-que le graphe suivant contient un chemin eulérien ? Si oui, construisez-le.



**14.** On considère la décomposition du carré en régions comme indiqué. Pour chaque région on associe un sommet et on connecte deux sommets par une arête si les régions corréspondantes sont adjacentes. Dessiner le graphe qui se déduit. Combien de couleurs faut-il pour colorier ce graphe ? Calculer le polynôme chromatique associé à ce graphe.



**15.** Calculer la matrice d'adjacence du graphe suivant :




Déterminer le nombre de chemins de longueur 4 allant de 1 à 3.

**16.** Existe-t-il un graphe simple sont la suite de degrés est $(7, 7, 5, 3, 3, 3, 2, 2)$. Si oui, construisez-le.

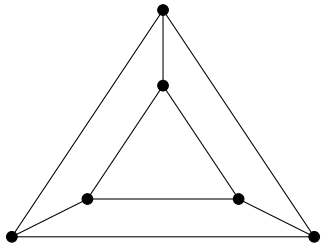
**17.** (a) Trouver une coloration des arêtes du graphe complet $K_5$ en deux couleurs, rouge et bleue, telle qu'il n'y aurait pas de triangle rouge ni de triangle bleu.

(b) Montrer que, quelle que soit une coloration des arêtes du graphe complet $K_6$, il existe toujours soit un triangle rouge, soit un triangle bleu (soit les deux).

**18.** Le graphe $L(G)$ des arêtes du graphe $G$ a pour sommets les arêtes de $G$ et une arête entre deux sommets si les arêtes correspondantes ont une extrémité commune.

(a) Tracer $L(K_3), L(K_{1,3}), L(C_5), L(E_5)$ et $L(K_4)$ (où $E_n$ corréspond à une étoile à $n$ sommets, c'est à dire un sommet interne connecté à $n-1$ sommets externes sans autres connexions). En déduire la forme des graphes $L(C_n), L(E_n)$ et $L(L_n)$, où $L_n$ est le graphe linéaire à $n$ sommets.

(b) Déterminer, s'il existe, le graphe $G$ dont le graphe $L(G)$ associé est le graphe ci-dessous :



(c) Si $G$ eulérien, le graphe $L(G)$ est-il eulérien ? Est-il hamiltonien ?

(d) Si $G$ hamiltonien, le graphe $L(G)$ est-il eulérien ?

**19.** En considérant le graphe suivant, montrer que $R(3,4) > 8$, puis que $R(3,4) = 9$.