université de BORDEAUX	**ANNÉE UNIVERSITAIRE 2017-2018** **Examen - Session 1 d'Automne** **Parcours :** Master CSI **UE :** 4TCY703U **Épreuve :** Arithmétique **Date :** 20 Décembre 2017 **Heure :** 14h30 **Durée :** 3h Documents : aucun document autorisé Épreuve de M. Cerri	**Collège Sciences et Technologies**

L'usage de la calculatrice est autorisé, mais non indispensable.
La qualité de l'argumentation et de la rédaction sera un facteur d'appréciation.
Barème indicatif : 10/40, 8/40, 10/40, 12/40.

Exercice 1 – Soit $P(X) = X^3 + X^2 - X + 1 \in \mathbb{F}_5[X]$.

1) Montrer que $K = \mathbb{F}_5[X]/\langle P(X)\rangle$ est un corps. Quel est son cardinal ?
On note α la classe de X dans K.

2) Calculer α^{31} et en déduire l'ordre de α dans $K^\times$.

3) Le polynôme $P(X)$ est-il irréductible primitif dans $\mathbb{F}_5[X]$?

4) Combien y a-t-il de polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_5[X]$?

5) Parmi ces polynômes, combien sont primitifs ?

6) Montrer que $\alpha + 1$ est un élément primitif de K.

7) En déduire un polynôme unitaire, irréductible et primitif de degré 3 dans $\mathbb{F}_5[X]$.

8) Montrer que dans $\mathbb{F}_5[X]$ le polynôme $\sum_{i=0}^{30} X^i$ est le produit de 10 polynômes unitaires irréductibles de degré 3 et qu'aucun de ces polynômes n'est primitif.

9) Le polynôme $P(X)$ fait-il partie de ces 10 polynômes ?

Exercice 2 – Soit $P(X) = X^5 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$.

1) Montrer que $P(X)$ est irréductible et primitif dans $\mathbb{F}_2[X]$.
On identifie $\mathbb{F}_2[X]/\langle P(X)\rangle$ et $\mathbb{F}_{2^5}$ et on note α la classe de X dans $\mathbb{F}_{2^5}$.

2) On considère la suite $(s_i)_{i\geqslant 0} \in \mathbb{F}_2^{\mathbb{N}}$ définie par $(s_0, s_1, s_2, s_3, s_4) = (1, 0, 0, 0, 0)$ et par la relation $s_{i+5} = s_{i+3} + s_{i+2} + s_{i+1} + s_i$ pour tout $i \geqslant 0$. Rappeler pourquoi $(s_i)_{i\geqslant 0}$ est périodique et déterminer sa période r sans calcul.

3) On note Tr la fonction trace dans $\mathbb{F}_{2^5}$. Calculer $\mathrm{Tr}(\alpha^i)$ pour $0 \leqslant i \leqslant 4$.

4) Montrer qu'il existe un unique $0 \leqslant k \leqslant r-1$ tel que $s_i = \mathrm{Tr}(\alpha^{i+k})$. Déterminer k en calculant les premiers termes de $(s_i)_{i\geqslant 0}$.
On admettra dans la suite que $Q(X) = X^{12} + X^3 + 1$ est irréductible dans $\mathbb{F}_2[X]$. On identifie $\mathbb{F}_2[X]/\langle Q(X)\rangle$ et $\mathbb{F}_{2^{12}}$ et on note β la classe de X dans $\mathbb{F}_{2^{12}}$.

5) Calculer β^{48}.

6) En déduire l'ordre de β dans $\mathbb{F}_{2^{12}}^\times$.

7) Dresser la liste des sous-corps de $\mathbb{F}_{2^{12}}$ et établir le schéma des inclusions.

8) Montrer que $\mathbb{F}_2(\beta^3)$ est un sous-corps strict de $\mathbb{F}_{2^{12}}$ que l'on identifiera dans la liste précédente.

9) On considère la suite $(t_i)_{i\geqslant 0} \in \mathbb{F}_2^{\mathbb{N}}$ définie par $(t_0, t_1, t_2, \ldots, t_{11}) = (1, 0, 0, \ldots, 0)$ et par la relation $t_{i+12} = t_{i+3} + t_i$ pour tout $i \geqslant 0$. Rappeler pourquoi $(t_i)_{i\geqslant 0}$ est périodique. Quelle est sa période ?

Exercice 3 – Soient un entier $m \geqslant 2$ et $n = 2^m - 1$. On considère un code de Hamming cyclique $\mathcal{H}$ de longueur n et de dimension $n-m$, de polynôme générateur $g(X)$ de degré m, irréductible et primitif dans $\mathbb{F}_2[X]$. On note $\mathcal{C}$ le dual de $\mathcal{H}$.

1) Soit G une matrice génératrice de $\mathcal{C}$.

a) Montrer que G ne peut pas contenir une colonne nulle.

b) Montrer que G ne peut pas contenir deux colonnes identiques.

c) En déduire que les n colonnes de G sont exactement les n vecteurs non nuls de $\mathbb{F}_2^m$.

2) Soit $y = (y_1, y_2, \ldots, y_m) \in \mathbb{F}_2^m \setminus \{0\}$.

a) Combien de y a-t-il de $x = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_2^m \setminus \{0\}$ tels que $\sum_{i=1}^{m} x_i y_i = 0$?

b) Combien y a-t-il de $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^m \setminus \{0\}$ tels que $\sum_{i=1}^{m} x_i y_i = 1$?

3) En déduire que le poids de tout mot non nul de $\mathcal{C}$ est 2^{m-1}.

4) Quels sont la distance minimale de $\mathcal{C}$ et l'ordre de la condition de décodage vérifiée par $\mathcal{C}$?

5) On considère le polynôme $g(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$. On rappelle que $g(X)$ est irréductible et primitif dans $\mathbb{F}_2[X]$. Soit $\mathcal{H}$ le code de Hamming de longueur 15, de dimension 11, de polynôme générateur $g(X)$, et soit $\mathcal{C}$ son code dual.

a) Quels sont les paramètres de $\mathcal{C}$? Que vaut e, l'ordre de la condition de décodage vérifiée par $\mathcal{C}$?

b) Quel est le polynôme générateur de $\mathcal{C}$?

c) On suppose qu'un mot $c \in \mathcal{C}$ a été envoyé et a subi au plus e erreurs lors de la transmission. Le mot reçu est $r = (0,0,1,1,0,0,1,0,0,1,1,0,1,0,1)$. Retrouver c.

Exercice 4 – Soit $P(X) = X^2 + X - 1 \in \mathbb{F}_3[X]$.

1) Montrer que $P(X)$ est irréductible et primitif dans $\mathbb{F}_3[X]$.
On identifie $\mathbb{F}_9$ et $\mathbb{F}_3[X]/\langle P(X) \rangle$ et on note α la classe de X dans $\mathbb{F}_9$. Soit $M \in \mathcal{M}_{4,8}(\mathbb{F}_9)$ définie par

$$M = \begin{pmatrix} \alpha-1 & \alpha & 1 & \alpha-1 & 1 & 0 & 0 & 0 \\ 0 & \alpha-1 & \alpha & 1 & \alpha-1 & 1 & 0 & 0 \\ 0 & 0 & \alpha-1 & \alpha & 1 & \alpha-1 & 1 & 0 \\ 0 & 0 & 0 & \alpha-1 & \alpha & 1 & \alpha-1 & 1 \end{pmatrix}.$$

2) Montrer que les lignes de M sont linéairement indépendantes sur $\mathbb{F}_9$.
On note $\mathcal{C}$ le code linéaire inclus dans $\mathbb{F}_9^8$ de matrice génératrice M.

3) Quel est le cardinal de $\mathcal{C}$?

4) Montrer que $(1,0,0,0,\alpha-1,\alpha,1,\alpha-1) \in \mathcal{C}$.

5) En déduire que $\mathcal{C}$ est cyclique.

6) Quel est le polynôme générateur $g(X)$ de $\mathcal{C}$?

7) Vérifier que $g(X) = (X-1)(X-\alpha)(X-\alpha^2)(X-\alpha^3)$ et que $g(X)$ divise bien $X^8 - 1$ dans $\mathbb{F}_9[X]$.

8) En déduire que tout $Q(X) \in \mathcal{C}$ vérifie $Q(1) = Q(\alpha) = Q(\alpha^2) = Q(\alpha^3) = 0$, et que si $Q(X) \neq 0$, le poids de $Q(X)$ est > 4.

9) Quels sont la distance minimale de $\mathcal{C}$ et l'ordre de la condition de décodage vérifiée par $\mathcal{C}$?

10) Le code $\mathcal{C}$ est-il MDS ?

11) Soit $\mathcal{C}^\perp$ le code dual de $\mathcal{C}$. Quel est son polynôme générateur et quelles sont ses racines dans $\mathbb{F}_9$?

12) Quels sont les paramètres de $\mathcal{C}^\perp$?