Université PIERRE ET MARIE CURIE
L2 Mathématiques

2006-2007
Module LM220

Correction de l'examen du 5 février 2007

Exercice 1

1) On a $19 \equiv -2$ mod. 7 et $23 \equiv 2$ mod. 7, d'où $19^{12} \times 23^{43} \equiv 2^{55}$ mod. 7. Par ailleurs, on a $2^3 \equiv 1$ mod. 7, d'où $2^{55} \equiv 2$ mod. 7. Le reste cherché est donc 2.

2) Les entiers naturels divisibles par 175 et 245 sont ceux divisibles par leur plus petit commun multiple m. On a $175 = 5^2 \times 7$ et $245 = 5 \times 7^2$, d'où $m = 5^2 \times 7^2 = 1225$. Par suite, les entiers cherchés sont

$$1225,\ 2450,\ 3675,\ 4900,\ 6125,\ 7350,\ 8575 \text{ et } 9800.$$

3) Soit a un entier naturel possédant la propriété de l'énoncé. Il existe $q \in \mathbb{N}$ tel que l'on ait $a = 64q + q^3$ avec $0 \leq q^3 < 64$. Vu que $64 = 4^3$, on a $0 \leq q < 4$. On en déduit que les entiers cherchés sont

$$0,\ 65,\ 136 \text{ et } 219.$$

4) On a les égalités $5757 = 5700 + 57 = 57 \times 100 + 57 = 57 \times 101$. La décomposition en facteurs premiers de 5757 est donc $3 \times 19 \times 101$. L'ordre du groupe est ainsi (φ étant la fonction indicatrice d'Euler),

$$\varphi(5757) = 2 \times 18 \times 100 = 3600.$$

5) On utilise l'algorithme d'Euclide. Conformément à cet algorithme, on obtient le tableau suivant :

	1	1	1	1	3	1	1	1	8	
553	337	216	121	95	26	17	9	8	1	0
1	0	1	−1	2	−3	11	−14	25	−39	
0	1	−1	2	−3	5	−18	23	−41	64	

On en déduit l'égalité $64 \times 337 - 39 \times 553 = 1$, d'où $\overline{337}^{-1} = \overline{64}$.

Exercice 2

1) Le polynôme P est irréductible sur $\mathbb{F}_5$, car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_5$. Par suite, K est un corps.

2) La caractéristique de K est 5 et son cardinal est $5^3 = 125$.

3) Le groupe K^* est d'ordre 124. On a $124 = 4 \times 31$. Les ordres possibles des éléments de K^* sont donc $1, 2, 4, 31, 62$ et 124.

4) On a $\alpha^3 = -1 - \alpha$. Par ailleurs, on a $\alpha^5 = 1 + \alpha - \alpha^2$. Puisque K est de caractéristique 5, il en résulte que l'on a

$$\alpha^{15} = -(1+\alpha)^5 = -1 - \alpha^5 = \alpha^2 - \alpha - 2.$$

On en déduit que

$$\alpha^{30} = (\alpha^2 - \alpha - 2)^2 = \alpha^2 + 1.$$

5) L'élément α n'est pas d'ordre $1, 2$ ni 4. D'après la question précédente, on a $\alpha^{31} = -1$. Ainsi, α est d'ordre 62. Par ailleurs, on constate directement que 2α n'est pas d'ordre $1, 2$ ni 4. On a $2^4 \equiv 1$ mod. 5 et $2^{31} \equiv 3$ mod. 5, d'où $(2\alpha)^{31} = 2$ et $(2\alpha)^{62} = -1$. Ainsi, 2α est d'ordre 124, autrement dit, 2α est un générateur de K^*.

6) Dans $\mathbb{F}_5[X]$, on obtient par division euclidienne l'égalité

$$P = (X+1)(X^2 - X + 2) - 1.$$

Vu que l'on a $P(\alpha) = 0$, on en déduit que $(\alpha+1)(\alpha^2 - \alpha + 2) = 1$ i.e. que l'inverse de $\alpha + 1$ est $\alpha^2 - \alpha + 2$, dont les coordonnées dans $\mathcal{B}$ sont $(2, -1, 1)$.

7) On a $P(\alpha) = 0$. Le corps K étant de caractéristique 5, cela entraîne $P(\alpha^5) = 0$. On peut aussi vérifier cette égalité directement. Par ailleurs, on a $\alpha^5 \neq \alpha$. Il en résulte que P a toutes ses racines dans K. Leur produit étant -1, la troisième racine de P est donc $-\alpha^{-6}$. On a $\alpha^6 = (\alpha+1)^2$. Compte tenu de la question précédente, on a ainsi $\alpha^{-6} = -\alpha^2 + 2\alpha + 1$, et les racines de P sont

$$\alpha, \quad -\alpha^2 + \alpha + 1 \quad \text{et} \quad \alpha^2 - 2\alpha - 1.$$

Exercice 3

1) Le déterminant de la matrice extraite de G au moyen de ses lignes et de ses deux premières colonnes vaut 1. Il en résulte que le rang de G est 2.

2) La longueur de C est 4, sa dimension est 2 et son cardinal est $3^2 = 9$.

3) La matrice $\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$ étant inversible, C est systématique.

4) Notons ℓ_i la i-ème ligne de G ainsi que celle de toute autre matrice déduite de G par des opérations élémentaires sur ses lignes. En remplaçant ℓ_2 par $\ell_2 - \ell_1$, on obtient la matrice

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

En remplaçant ℓ_1 par $\ell_1 + \ell_2$, on obtient

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Par suite, on a

$$B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

5) Une matrice de contrôle de C est donc

$$H = (-{}^tB \mid I_2) = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

6) La distance minimum d de C est le nombre minimum de colonnes de H qui, en tant que vecteurs de $\mathbb{F}_3^2$, sont linéairement dépendantes. Puisque les colonnes de H sont non nulles, on a $d \geq 1$, et l'on vérifie directement que deux colonnes quelconques de H sont indépendantes. On a donc $d = 3$. La capacité de correction de C, qui est la partie entière de $(d-1)/2$, vaut 1.

7) Conformément à l'algorithme de décodage des codes linéaires (p. 144 du polycopié), on détermine les syndromes $H(e) \in \mathbb{F}_3^2$ des éléments $e \in \mathbb{F}_3^4$ de poids au plus 1. Il y a neuf éléments de $\mathbb{F}_3^4$ de poids ≤ 1, qui sont

$$e_1 = (0,0,0,0),\ e_2 = (1,0,0,0),\ e_3 = (2,0,0,0),\ e_4 = (0,1,0,0),\ e_5 = (0,2,0,0),$$

$$e_6 = (0,0,1,0),\ e_7 = (0,0,2,0),\ e_8 = (0,0,0,1),\ e_9 = (0,0,0,2).$$

On vérifie que l'on a

$$H(e_1) = 0,\ H(e_2) = (2,1),\ H(e_3) = (1,2),\ H(e_4) = (2,2),\ H(e_5) = (1,1),$$

$$H(e_6) = (1,0),\ H(e_7) = (2,0),\ H(e_8) = (0,1),\ H(e_9) = (0,2).$$

Par ailleurs, on a $H(x) = (1,1)$, d'où $H(x) = H(e_5)$. Ainsi $x - e_5 = (1,1,2,0)$, qui est l'unique mot de C dans la boule de Hamming de centre x et de rayon 1, est le mot de C le plus proche de x.