Université PIERRE ET MARIE CURIE — 2006-2007
L2 Mathématiques — Module LM220

Correction de l'examen du 15 janvier 2007

Exercice 1

1) On a $187 = 11 \times 17$, donc 187 n'est pas premier.
2) Le nombre de générateurs d'un groupe cyclique d'ordre n est $\varphi(n)$, où $\varphi(n)$ est l'indicateur d'Euler de n. Par ailleurs, on a $1024 = 2^{10}$ et $\varphi(2^{10}) = 2^9 = 512$.
3) Si n est un entier naturel non nul et a un entier tels que $0 \leq a \leq n-1$, l'ordre de $\overline{a}$ dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ est $\frac{n}{\text{pgcd}(n,a)}$. L'ordre de $\overline{15}$ dans le groupe $(\mathbb{Z}/100\mathbb{Z}, +)$ est donc 20.
4) On a $129 = 3 \times 43$. Puisque 129 n'est pas une puissance d'un nombre premier, il n'existe pas de corps de cardinal 129.
5) Dans le corps $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ l'équation $x^2 = -1$ a comme solutions $x = \overline{2}$ et $x = \overline{3}$. L'ensemble cherché est donc formé des entiers congrus à 2 ou 3 modulo 5.

Exercice 2

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

	8	3	1	2	
15925	1925	525	350	175	0
1	0	1	-3	4	
0	1	−8	25	−33	

On en déduit que l'on a $d = 175$ et l'égalité $175 = 4 \times 15925 - 33 \times 1925$. Le couple $(u, v) = (4, -33)$ répond ainsi à la question. Signalons que l'on a

$$15925 = 5^2 \times 7^2 \times 13 \quad \text{et} \quad 1925 = 5^2 \times 7 \times 11,$$

ce qui conduit à $d = 5^2 \times 7 = 175$.

2) On détermine une relation de Bézout entre 19 et 23. Par exemple, en utilisant de nouveau l'algorithme d'Euclide, on obtient le tableau suivant :

	1	4	1	3	
23	19	4	3	1	0
1	0	1	-4	5	
0	1	−1	5	−6	

On en déduit l'égalité $5 \times 23 - 6 \times 19 = 1$, puis que

$$n_0 = 5 \times 23 - 2 \times (6 \times 19) = -113$$

vérifie les congruences $n_0 \equiv 1$ mod. 19 et $n_0 \equiv 2$ mod. 23. Il en résulte que l'ensemble des entiers relatifs n vérifiant les deux congruences de l'énoncé est

$$\Big\{ -113 + 437k \mid k \in \mathbb{Z} \Big\}.$$

L'entier naturel cherché est donc $-113 + 437 = 324$.

Exercice 3

1) Il s'agit de démontrer que P est irréductible dans $\mathbb{F}_2[X]$. On remarque d'abord que P n'a pas de racines dans $\mathbb{F}_2$. Par ailleurs, il existe un unique polynôme de $\mathbb{F}_2[X]$ irréductible de degré 2, qui est $1 + X + X^2$. Si P était réductible sur $\mathbb{F}_2$, il serait donc divisible par ce polynôme, ce qui n'est pas, vu l'égalité $P = (X^2+X+1)(X^2+X)+1$.
2) La caractéristique de K, qui est celle de $\mathbb{F}_2$, est 2. Son cardinal est $2^4 = 16$.
3) C'est une question de cours. If suffit de refaire la démonstration du théorème 5.9 du polycopié.
4) On a l'égalité $\alpha^4 = \alpha + 1$. On en déduit que l'on a

(1) $$\alpha^5 = \alpha^2 + \alpha, \quad \alpha^6 = \alpha^3 + \alpha^2 \quad \text{et} \quad \alpha^7 + 1 = \alpha^3 + \alpha.$$

Les coordonnées de $\alpha^7 + 1$ dans $\mathcal{B}$ sont donc $(0, 1, 0, 1)$.

5) Une méthode consiste par exemple à trouver une relation de Bézout entre P et X^3+X. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	X	$X+1$	X	$X+1$	
X^4+X+1	X^3+X	X^2+X+1	$X+1$	1	0
1	0	1	$X+1$	X^2+X+1	
0	1	X	X^2+X+1	X^3+X^2	

On en déduit l'égalité

$$(X^2 + X + 1)P + (X^3 + X)(X^3 + X^2) = 1.$$

Compte tenu de l'égalité $P(\alpha) = 0$, on a donc $(\alpha^3+\alpha)(\alpha^3+\alpha^2) = 1$, et l'inverse de α^7+1 est $\alpha^3 + \alpha^2$. Ses coordonnées dans $\mathcal{B}$ sont donc $(0, 0, 1, 1)$.

6) L'ordre du groupe K^* est 15. D'après le théorème de Lagrange, les ordres possibles de ses éléments sont $1, 3, 5$ et 15.

7) L'égalité $P(\alpha) = 0$ entraîne directement que α et α^3 sont distincts de 1. D'après (1), l'égalité $\alpha^5 = 1$ conduit à $\alpha^2 + \alpha = 1$, d'où $\alpha^4 = \alpha^2$, puis $\alpha^2 = 1$, $\alpha = 1$ et une contradiction. L'ordre de α est donc 15 i.e. α est un générateur de K^*. Par ailleurs, il y a $\varphi(15) = 8$ générateurs dans K^*.

8) D'après (1), on a $\alpha + \alpha^2 = \alpha^5$, qui d'après la question précédente, est d'ordre 3.

Exercice 4

1) Par exemple, le déterminant de la matrice extraite de G au moyen de ses lignes et de ses trois premières colonnes

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

vaut 1. Ainsi, le rang de G est ≥ 3. Il vaut donc 3, qui est le maximum possible.

2) La longueur de C est 5, sa dimension est 3 et son cardinal est $2^3 = 8$.

3) La matrice A étant inversible, C est systématique.

4) La matrice B s'obtient par une suite finie d'opérations élémentaires sur les lignes de G. Notons ℓ_i la i-ème ligne de G et par abus celle de tout autre matrice déduite de G par des opérations élémentaires. En remplaçant ℓ_3 par $\ell_3 + \ell_1$, on obtient la matrice

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

En remplaçant ℓ_3 par $\ell_3 + \ell_2$, on obtient

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

En remplaçant ℓ_2 par $\ell_2 + \ell_3$, puis ℓ_1 par $\ell_1 + \ell_3$, on obtient successivement les matrices

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Par suite, on a

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

5) Une matrice de contrôle de C est donc (cf. prop. 7.11 du polycopié)

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

6) La distance minimum d de C est le nombre minimum de colonnes de H qui, en tant que vecteurs de $\mathbb{F}_2^2$, sont linéairement dépendantes (prop. 7.13 du polycopié). Puisque les colonnes de H sont non nulles, et que la première et la troisième colonne sont égales, on a donc $d = 2$. La capacité de correction de C, qui est la partie entière de $(d-1)/2$, est nulle.

7) En notant n et k respectivement la longueur et la dimension de C, on a les égalités $n - k + 1 = 5 - 3 + 1 = 3$, qui est distinct de d. Ainsi, C n'est pas MDS.

8) Posons $x = (0, 0, 1, 0, 1)$. On a $H(x) = 0$, donc x appartient à C.
