Université PIERRE ET MARIE CURIE — 2006-2007

L2 Mathématiques — Module LM220

# Examen du 15 janvier 2007

Durée 2 heures

**Les documents, calculatrices et téléphones portables sont interdits.**

**Toutes les réponses devront être soigneusement justifiées.**

## Exercice 1

1) L'entier 187 est-il premier ?
2) Quel est le nombre de générateurs d'un groupe cyclique d'ordre 1024 ?
3) Quel est l'ordre de la classe de 15 dans le groupe additif $(\mathbb{Z}/100\mathbb{Z}, +)$ ?
4) Existe-t-il un corps de cardinal 129 ?
5) Quel est l'ensemble des entiers relatifs $n$ tels que 5 divise $n^2 + 1$ ?

## Exercice 2

1) Posons $a = 15925$ et $b = 1925$. Quel est le plus grand commun diviseur $d$ de $a$ et $b$ ? Trouver deux entiers $u$ et $v$ tels que l'on ait $d = au + bv$.
2) Déterminer le plus petit entier naturel $n$ vérifiant les congruences

$$n \equiv 1 \text{ mod. } 19 \quad \text{et} \quad n \equiv 2 \text{ mod. } 23.$$

## Exercice 3

Soit $P$ le polynôme $X^4 + X + 1$ dans $\mathbb{F}_2[X]$. On considère l'anneau quotient

$$K = \mathbb{F}_2[X]/(P).$$

1) Montrer que $K$ est un corps.
2) Quelle est sa caractéristique ? Quel est son cardinal ?

Soit $\alpha$ la classe de $X$ modulo $(P)$.

3) Montrer que le système $\mathcal{B}= (1, \alpha, \alpha^2, \alpha^3)$ est une base du $\mathbb{F}_2$-espace vectoriel $K$.
4) Déterminer les coordonnées de $\alpha^7 + 1$ dans $\mathcal{B}$.

5) Déterminer les coordonnées de l'inverse de $\alpha^7 + 1$ dans $\mathcal{B}$.

6) Quels sont les ordres possibles des éléments du groupe $K^* = K - \{0\}$ ?

7) Montrer que $\alpha$ est un générateur de $K^*$. Combien y a-t-il de générateurs dans $K^*$ ?

8) Quel est l'ordre de $\alpha + \alpha^2$ dans $K^*$ ?

**Exercice 4**

Soit $G$ la matrice de taille $(3, 5)$ à coefficients dans $\mathbb{F}_2$ définie par

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

1) Quel est le rang de $G$ ?

Soit $C$ le code linéaire sur $\mathbb{F}_2$ de matrice génératrice $G$.

2) Déterminer sa longueur, sa dimension et son cardinal.

3) Montrer que $C$ est systématique.

4) Soit $I_3$ la matrice identité de taille $(3, 3)$. Trouver la matrice $B$ de taille $(3, 2)$ à coefficients dans $\mathbb{F}_2$ telle que $(I_3|B)$ soit une matrice génératrice de $C$.

5) Déterminer une matrice de contrôle de $C$.

6) Quelle est la distance minimum de $C$ ? Quelle est sa capacité de correction ?

7) Le code $C$ est-il MDS ?

8) L'élément $(0, 0, 1, 0, 1) \in \mathbb{F}_2^5$ est-il un mot de code ?