Math 701 exercices – Arithmétique modulaire et corps finis

Nicolas Gast

28 octobre 2020

Exercise 1 Éléments inversibles

1. Quels éléments de $(\mathbb{Z}/8\mathbb{Z}, \times)$ sont inversibles ?
   a) Calculer l'inverse de tous les éléments inversibles de $(\mathbb{Z}/8\mathbb{Z}, \times)$.
   b) $(\mathbb{Z}/8\mathbb{Z}, +, \times)$ est-il un corps ?
2. Quels éléments de $(\mathbb{Z}/97\mathbb{Z}, \times)$ sont inversibles ?
   a) Calculer l'inverse de 8 dans $(\mathbb{Z}/97\mathbb{Z}, \times)$ (s'il existe).
   b) $(\mathbb{Z}/97\mathbb{Z}, +, \times)$ est-il un corps ?

Exercise 2 Retour sur `mod97-10`

Soit $x = x_{n-1} \dots x_0$ un mot de `mod97-10`. Soit x' un mot identique à x sauf pour le $k$ième chiffre (x_k en écriture décimale) a été changé en x'_k.

1. Est-ce que 10^k est inversible dans $\mathbb{Z}/97\mathbb{Z}$?
2. Montrer que $x - x' = (x_k - x'_k)10^k$ (modulo 97).
3. En déduire que x' n'est pas un mot valide.
4. Pourquoi peut-on en déduire que `mod97-10` détecte toutes les erreurs d'au plus un chiffre ?

Exercise 3 Corps

Parmis les anneaux, quels sont ceux qui sont des corps ? (sauf précision, à chaque fois, $+$ et $\times$ sont l'addition et la multiplication naturelle).

1. $(\mathbb{Q}, +, \times)$ où $\mathbb{Q}$ est l'ensemble des rationnels.
2. $(\mathbb{M}_2, +, \times)$ où $\mathbb{M}_2$ est l'ensemble des matrices réelles de taille 2×2, $+$ et $\times$ sont l'addition et la multiplication de matrices.
3. $(\mathbb{Z}/4\mathbb{Z}, +, \times)$.

Exercise 4 Corps finis

1. Pour quels valeurs de $n \in \{2, 3 \dots, 10\}$ existe-il un corps à n éléments ?
2. Constuire la table d'addition et de multiplication de $\mathbb{F}_4$.

Exercise 5 Espace vectoriel

Soit V l'espace vectoriel engendré par (v_1, v_2, v_3, v_4) où

$$v_1 = (0, 0, 1, 1, 1, 0, 0)$$
$$v_2 = (0, 1, 1, 1, 0, 1, 1)$$
$$v_3 = (1, 1, 1, 0, 1, 0, 0).$$
$$v_3 = (1, 0, 0, 1, 1, 1, 1).$$

1. Quelle est la dimension de V ?
2. Donner tous les éléments de V.
3. Trouver une base de V.

Exercise 6 Code de parité

Soit C le code de parité $(n, n-1)$. L'alphabet du code est $\mathbb{F}_2$, les mots du code sont tous les mots de n lettres tels que le nombre de bit à 1 soit pair.

1. C est-il un code linéaire ?
2. Donner une base de C.
3. Quelle est la distance minimale de C ?
4. Donner une matrice de contrôle de C.

Exercise 7

On considère le code linéaire correspondant à l'exercice 5.

1. Donner une matrice génératrice G du code V.
2. Donner une matrice de contrôle H du code V.
3. Supposons que nous recevons le mot $x = (1, 0, 1, 0, 1, 0, 1)$. Utiliser la matrice H pour calculer un syndrome. Le mot x est-il un mot valide ? x