

Arithmétique et applications, combinatoire et graphes

Devoir préparatoire No. 1, janvier 2018, corps finis, codes correcteurs

Aucun document n'est autorisé, usage de calculatrices interdit

1. (i) Factoriser le polynôme $x^4 + x + 3$ en polynômes irréductibles sur $\mathbf{Z}/7\mathbf{Z}$.

(ii) Montrer que le polynôme $x^3 + x^2 + 3$ est irréductible sur $\mathbf{Z}/7\mathbf{Z}$.

Soit \mathbb{K} le corps $\mathbb{K} = \frac{(\mathbf{Z}/7\mathbf{Z})[x]}{(x^3 + x^2 + 3)}$.

(iii) Combien d'éléments y a-t-il dans \mathbb{K} ?

(iv) Calculer l'inverse multiplicative de $2x^2 + 1$ dans \mathbb{K} .

(v) Est-ce-que le polynôme $x^2 + 4$ est primitif, vu comme un polynôme sur $\mathbf{Z}/7\mathbf{Z}$?

2. Soit C le code dans \mathbb{F}_2^9 dont les mots sont donnés par les lignes de la matrice :

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

Calculer la distance minimale $d = d(C)$ pour ce code. Pour quel t est ce code t -correcteur ? Est-ce-que ce code est linéaire ?

On reçoit les trois vecteurs :

$$r_1 = (111001000), \quad r_2 = (110100110), \quad r_3 = (000000110).$$

On adopte la stratégie de correction au plus proche voisin. Parmi ces vecteurs, lesquels sont corrigibles ? Dans le cas où le vecteur est corrigible, donner le corrigé.

FIN