Arithmétique et applications, combinatoire et graphes

Contrôle No. 1, 6 fevrier 2017, corps finis, codes correcteurs

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

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

(ii) Montrer que le polynôme x^3+2x+1 est irréductible sur $\mathbf{Z}/3\mathbf{Z}$.

Soit $\mathbb{K}$ le corps $\mathbb{K} = \dfrac{(\mathbf{Z}/3\mathbf{Z})[x]}{(x^3+2x+1)}$.

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

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

(v) Est-ce-que le polynôme x^3+2x+1 est primitif ? (justifier)

(i) Soit $f(x) = x^4+1$, alors $f(0)=1$, $f(1)=2$, $f(2)=2$ (mod 3) donc pas de facteur linéaire.

Soit $x^4+1 = (x^2+ax+b)(x^2+cx+d)$ $(a,b,c,d \in \mathbb{F}_3)$

$\Rightarrow bd=1$, $ad+bc=0$, $b+d+ac=0$, $a+c=0$,

Soit $b=d=1$, soit $b=d=2$. En plus $c=-a=2a$

Cas $b=d=1$: $2+2a^2=0 \Rightarrow 1+a^2=0 \Rightarrow a^2=2$ impossible $(1^2=2^2=1)$

Cas $b=d=2$: $1+2a^2=0 \Rightarrow 2a^2=2 \Rightarrow a^2=1 \Rightarrow a=$ soit 1 soit 2.

D'où $x^4+1 = (x^2+x+2)(x^2+2x+2)$

(ii) Soit $f(x) = x^3+2x+1$, alors $f(0)=1$, $f(1)=1$, $f(2)=1$: pas de facteur linéaire, d'où $f(x)$ irréductible

(iii) $\mathbb{K}$ contient $3^3=27$ éléments.

(iv) $x^3+2x+1 = (x)(x^2+1)+x+1$

$x^2+1 = (x+2)(x+1)+2$

d'où $2 = x^2+1-(x+2)(x+1) = x^2+1-(x+2)\left(x^3+2x+1-x(x^2+1)\right)$

$= (x^2+1)(1+x(x+2)) - (x+2)(x^3+2x+1)$

$\times 2$

$\Rightarrow \cancel{2}\,1 = 2(x^2+2x+1)(x^2+1) - 2(x+2)(x^3+2x+1)$

$\Rightarrow$ Inverse mult : $2x^2+x+2$ (VÉRIF $(x^2+1)(2x^2+x+2) = 2x^4+x^3+x^2+x+2$
$= 2x(x+2)+x+2+x^2+x+2 = 1$)

(v) puissance de x doivent engendre $\mathbb{K}^*$, dont $|\mathbb{K}^*| = 26 = 2\times 13$. On $x^3 = x+2$ dans $\mathbb{K}$.

$x, x^2, x^3=x+2, x^2+2x, x^3+2x^2=2x^2+x+2, 2x^3+x^2+2x = x^2+x+1, x^3+x^2+x = x^2+2x+2,$ SUITE...

$x^3+2x^2+2x = 2x^2+2, 2x^3+2x = x+1, x^2+x, x^3+x^2 = x^2+x+2, x^3+x^2+2x = x^2+2,$

$x^3+2x=2, 2x, 2x^2, \dots$ On a évaluer >13 puissances. Puisque l'ordre divise 26, forcement l'ordre de x est 26 et le polynôme est primitif

2. Soit C le code dans $\mathbb{F}_2{}^{10}$ dont les mots sont donnés par les lignes de la matrice :

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

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

On reçoit les trois vecteurs :

$$r_1 = (0011010001), \quad r_2 = (0001101111), \quad r_3 = (1010101011)\,.$$

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.

Soit $\ell_1, \ell_2, \ell_3, \ell_4$ les lignes de la matrice. Puisque $\ell_4 = \ell_2 + \ell_3$, on voit que le code est linéaire.

Pour un code linéaire, la distance minimale est le poids minimal des mots de C, qui est achevé pour ℓ_3, dont son poids est 5, d'où $\underline{\underline{d = 5}}$

$d(\ell_1, r_1) = 7$, $d(\ell_2, r_1) = 7$, $d(\ell_3, r_1) = 3$, $d(\ell_4, r_1) = 6$, d'où r_1 est corrigible, on le corrige en $0111010100 = \ell_3$.

$d(\ell_1, r_2) = 6$, $d(\ell_2, r_2) = 5$, $d(\ell_3, r_2) = 7$, $d(\ell_4, r_2) = 2$, d'où r_2 est corrigible ; on le corrige en $\ell_4 = (1011101111)$

$d(\ell_1, r_3) = 6$, $d(\ell_2, r_3) = 3$, $d(\ell_3, r_3) = 9$, $d(\ell_4, r_3) = 2$, d'où r_3 est corrigible ; on le corrige en $\ell_4 = (1011101111)$