Université Pierre et Marie Curie
2M120 – Éléments d'arithmétique

Examen du 3 janvier 2017 — Durée : 1 heure 30 minutes

Aucun document n'est autorisé. L'utilisation de tout appareil électronique (tel que calculatrices, téléphones portables, montres connectées, etc.) est interdite. Ceux-ci doivent être rangés dans les sacs et mis en position éteinte.

Les correcteurs tiendront compte de la qualité de la rédaction et de la précision des raisonnements.

Toute réponse doit être justifiée. Les calculs doivent figurer sur la copie.

Cet énoncé comporte deux exercices indépendants.

Exercice 1 Considérez le polynôme $P = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$, le quotient $\mathbb{K} = \mathbb{F}_2[X]/(P)$ ainsi que $x \in \mathbb{K}$ qui désigne la classe de X dans $\mathbb{K}$.

1. Les polynômes de degré 2 de $\mathbb{F}_2[X]$ sont : X^2, X^2+1, X^2+X, X^2+X+1. Dites lesquels d'entre eux sont irréductibles.
2. Effectuez la division euclidienne de P par X^2+X+1 dans $\mathbb{F}_2[X]$.
3. Montrez que P est irréductible.
4. Expliquez pourquoi $\mathbb{K}$ est un corps et pourquoi $\mathbb{K}$ possède 32 éléments.
5. Dans $\mathbb{K}$, exprimez sous la forme $c_4x^4+c_3x^3+c_2x^2+c_1x+c_0$ les puissances de x successives : x, x^2, $x^4 = \left(x^2\right)^2$, $x^8 = \left(x^4\right)^2$, $x^{16} = \left(x^8\right)^2$ et $x^{32} = \left(x^{16}\right)^2$.
6. (a) Montrez que $x^{31} = 1$.
   (b) Montrez alors que si $x^n = x^m$, où $(n,m) \in \mathbb{Z}^2$, alors $n-m$ est un multiple de 31.
   (c) Montrez enfin que pour tout $a \in \mathbb{K}^*$, il existe un unique entier n, tel que $0 \leq n < 31$ et $a = x^n$.

Considérez maintenant les applications $\exp_x : \mathbb{Z}/31\mathbb{Z} \to \mathbb{K}^*$, définie par $\exp_x\left(\overline{n}\right) = x^n$, et $\log_x : \mathbb{K}^* \to \mathbb{Z}/31\mathbb{Z}$ l'application réciproque de $\exp_x$. (Si $a = x^n$ on écrira $\log_x(a) = n \bmod 31$.)

7. Donnez les valeurs de $\log_x(1)$, $\log_x(x)$, $\log_x(x^2)$ et $\log_x(x^4)$.
8. Déduisez de vos calculs précédents les valeurs de $\log_x(x^3+x^2+1)$ et $\log_x(x^4+x^3+x+1)$.
9. Montrez que $\log_x(x^2+1) = 5 \bmod 31$.
10. Déterminez la valeur de $\log_x(x^4+1) \bmod 31$.
11. Calculez $(x^3+1)(x^2+1)$ est déduisez-en la valeur de $\log_x(x^3+1) \bmod 31$.
12. Déterminez la valeur de $\log_x(x+1) \bmod 31$.

Exercice 2

1. Vérifiez que 3 est un élément primitif de $\mathbb{F}_7$, c'est-à-dire : $(\mathbb{F}_7)^* = \{1, 3, 3^2, 3^3, 3^4, 3^5\}$ et $3^6 = 1$.
2. Montrez que $X^6 - 1 = (X-1)(X-3)(X-3^2)(X-3^3)(X-3^4)(X-3^5)$ dans $\mathbb{F}_7[X]$.

Considérez le polynôme $g = (X-1)(X-3)(X-3^2)(X-3^3)$ et le code cyclique C de polynôme générateur g.

3. Donnez la longueur n et la dimension k de C. Déterminez également le nombre d'éléments de C.
4. Montrez que la distance minimale d de C égale 5. Déduisez-en sa capacité de correction t.
5. Déterminez la matrice génératrice G de C associée au polynôme générateur g.
6. Déterminez le polynôme de contrôle h de C et la matrice de contrôle H associée.

Considérez désormais l'anneau quotient $\mathbb{F}_7[x] = \mathbb{F}_7[X]/(X^6-1)$ où x est la classe de X.

Rappelez-vous qu'un élément de $\mathbb{F}_7[x]$ s'écrit de manière unique sous la forme $c_0+c_1x+c_2x^2+c_3x^3+c_4x^4+c_5x^5$ où $(c_0,c_1,c_2,c_3,c_4,c_5) \in (\mathbb{F}_7)^6$ et que $x^6 = 1$. Le poids d'un élément $c_0+c_1x+c_2x^2+c_3x^3+c_4x^4+c_5x^5$ de $\mathbb{F}_7[x]$ est le nombre de c_k non nuls, $0 \leq k \leq 5$.

Considérez les polynômes $g_i = (X-3^i)(X-3^{i+1})(X-3^{i+2})(X-3^{i+3})$ et les codes cycliques C_i de polynômes générateurs g_i. (Remarquez que $g_0 = g$ et que $C_0 = C$ est le code introduit à la question précédente. Remarquez également que $g_{i+6} = g_i$ et que $C_{i+6} = C_i$.)

Rappelez-vous que les éléments de C_i sont les éléments de $\mathbb{F}_7[x]$ multiples de $g_i(x) = (x-3^i)(x-3^{i+1})(x-3^{i+2})(x-3^{i+3})$.

7. Montrez que si $P = c_0+c_1X+c_2X^2+c_3X^3+c_4X^4+c_5X^5$ est un polynôme et si $P(x) = c_0+c_1x+c_2x^2+c_3x^3+c_4x^4+c_5x^5 \in C_i$ alors $P(3x) = c_0+3c_1x+3^2c_2x^2+3^3c_3x^3+3^4c_4x^4+3^5c_5x^5 \in C_{i-1}$.
8. Montrez que les codes C_i sont tous en bijection avec $C_0 = C$.
9. Déterminez la longueur n_i de C_i, sa dimension k_i, sa distance minimale d_i et sa capacité de correction t_i.