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.

Solution : X^2, $X^2+1 = (X+1)^2$ et $X^2+X = X(X+1)$ ne sont pas irréductibles dans $\mathbb{F}_2[X]$.
X^2+X+1 est irréductible dans $\mathbb{F}_2[X]$ car il est de degré 2 et n'a pas de racine dans $\mathbb{F}_2$.

2. Effectuez la division euclidienne de P par X^2+X+1 dans $\mathbb{F}_2[X]$.

Solution :

$$\begin{array}{rl|l} X^5 + X^2 + 1 & & X^2+X+1 \\ \cline{3-3} -(X^5 + X^4 + X^3) & & X^3 + X^2 \\ \cline{1-1} X^4 + X^3 + X^2 + 1 & & \\ -(X^4 + X^3 + X^2) & & \\ \cline{1-1} 1 & & \end{array}$$

Le quotient est $Q = X^3 + X^2$. Le reste est $R = 1$.

3. Montrez que P est irréductible.

Solution : P n'a pas de racine dans $\mathbb{F}_2$ car $P(0) = P(1) = 1 \neq 0$. Si P n'était pas irréductible, il serait alors produit d'un polynôme irréductible de degré 2 et d'un polynôme irréductible de degré 3. Donc P serait multiple de X^2+X+1 qui est le seul polynôme irréductible de degré 2. Mais $P = (X^2+X+1)Q + R$ avec $Q = X^3+X^2$ et $R = 1$, donc P n'est pas multiple de X^2+X+1 et donc P est irréductible.

4. Expliquez pourquoi $\mathbb{K}$ est un corps et pourquoi $\mathbb{K}$ possède 32 éléments.

Solution : Le quotient $\mathbb{F}_2[X]/(P)$ est un corps si et seulement si P est irréductible, ce qui est bien le cas ici, donc $\mathbb{K}$ est un corps. Il possède $32 = 2^5$ éléments car $\deg P = 5$.

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 $x^{32} = \left(x^{16}\right)^2$.

Solution : Pour les premières puissances, x, x^2 et x^4 il n'y a aucun calcul à faire.
On a : $x^8 = x^3 \times x^5 = x^3(x^2+1) = x^5 + x^3 = x^3 + x^2 + 1$.
On a : $x^{16} = (x^3+x^2+1)^2 = x^6 + x^4 + 1 = x \times x^5 + x^4 + 1 = x(x^2+1) + x^4 + 1 = x^4 + x^3 + x + 1$.
Enfin, on a : $x^{32} = (x^4+x^3+x+1)^2 = x^8 + x^6 + x^2 + 1 = (x^3+x^2+1) + (x^3+x) + x^2 + 1 = x$.

6. (a) Montrez que $x^{31} = 1$.

Solution : $x^{32} = x$ donc $x^{31} = 1$.

(b) Montrez alors que si $x^n = x^m$, où $(n, m) \in \mathbb{Z}^2$, alors $n - m$ est un multiple de 31.

Solution : Si $x^n = x^m$ alors $x^{n-m} = 1$, mais on sait déjà que $x^{31} = 1$, or 31 est premier, donc $n-m$ est multiple de 31. (On peut montrer cela de la façon suivante : on effectue la division euclidienne de $n-m$ par 31 : $n - m = 31q + r$ avec $0 \leq r < 31$. On a alors $x^r = x^{n-m} \times \left(x^{31}\right)^{-q} = x^{n-m} \times 1^{-q} = 1$. Si $r \neq 0$ alors r et 31 sont premiers entre eux, car 31 est un nombre premier et $1 \leq r < 31$. Mais alors il existe deux entiers u et v tels que $ru + 31v = 1$. On a alors $x = x^{ru+31v} = \left(x^r\right)^u \times \left(x^{31}\right)^v = 1$ ce qui est faux. Conclusion : $r = 0$ ce qui signifie bien que $n-m$ est 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 $a = x^n$.

Solution : On déduit de la question précédente que les puissances de x : $1 = x^0$, $x = x^1$, x^2, ..., x^{29} et x^{30} sont des éléments de $\mathbb{K}^*$ 2 à 2 distincts. Mais ces puissances sont au nombre de 31. Ce sont donc tous les éléments de $\mathbb{K}^*$.

Considérez maintenant les applications $\exp_x : \mathbb{Z}/31\mathbb{Z} \to \mathbb{K}^*$, définie par $\exp_x(\overline{n}) = x^n$, 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 $\log_x(x^4)$.

Solution : $\log_x(1) = 0 \bmod 31$, $\log_x(x) = 1 \bmod 31$, $\log_x(x^2) = 2 \bmod 31$ et $\log_x(x^4) = 4 \bmod 31$.

8. Déduisez de vos calculs précédents les valeurs de $\log_x(x^3 + x^2 + 1)$ et $\log_x(x^4 + x^3 + x + 1)$.

Solution : On a montré que $x^8 = x^3 + x^2 + 1$ donc $\log_x(x^3 + x^2 + 1) = 8 \bmod 31$. On a également montré que $x^4 + x^3 + x + 1 = x^{16}$ donc $\log_x(x^4 + x^3 + x + 1) = 16 \bmod 31$.

9. Montrez que $\log_x(x^2 + 1) = 5 \bmod 31$.

Solution : $x^2 + 1 = x^5$ donc $\log_x(x^2 + 1) = 5 \bmod 31$.

10. Déterminez la valeur de $\log_x(x^4 + 1) \bmod 31$.

Solution : $x^4 + 1 = (x^2 + 1)^2 = x^{10}$ donc $\log_x(x^4 + 1) = 10 \bmod 31$.

11. Calculez $(x^3 + 1)(x^2 + 1)$ est déduisez-en la valeur de $\log_x(x^3 + 1) \bmod 31$.

Solution : $(x^3 + 1)(x^2 + 1) = x^5 + x^3 + x^2 + 1 = x^3$ donc $\log_x(x^3 + 1) + \log_x(x^2 + 1) = 3 \bmod 31$ d'où $\log_x(x^3 + 1) = 3 - 5 = 29 \bmod 31$.

12. Déterminez la valeur de $\log_x(x + 1) \bmod 31$.

Solution : $(x + 1)^2 = x^2 + 1$ donc $2 \log_x(x + 1) = 5 \bmod 31$ d'où $\log_x(x + 1) = 18 \bmod 31$.

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 $3^6 = 1$.

Solution : Dans $\mathbb{F}_7$: $3^2 = 9 = 2$, $3^3 = 2 \times 3 = 6$, $3^4 = 6 \times 3 = 18 = 4$, $3^5 = 4 \times 3 = 12 = 5$ et $3^6 = 5 \times 3 = 15 = 1$, donc $(\mathbb{F}_7)^* = \{1, 3, 3^2, 3^3, 3^4, 3^5\}$ 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 $\mathbb{F}_7[X]$.

Solution : Le polynôme $X^6 - 1$ a évidemment 1 comme racine. De plus, comme $3^6 = 1$ dans $\mathbb{F}_7$, on en déduit que 3, 3^2, 3^3, 3^4 et 3^5 (qui sont tous distincts) sont également racines du polynôme $X^6 - 1$ dans $\mathbb{F}_7$. Comme $X^6 - 1$ est de degré 6, il en résulte que $X^6 - 1 = (X - 1)(X - 3)(X - 3^2)(X - 3^3)(X - 3^4)(X - 3^5)$ dans $\mathbb{F}_7[X]$.
On peut également développer le polynôme $(X-1)(X-3)(X-3^2)(X-3^3)(X-3^4)(X-3^5) = (X-1)(X-3)(X-2) \times (X - 6)(X - 4)(X - 5)$ et constater qu'il est égal à $X^6 - 1$.

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.

Solution : La longueur de C est $n = \deg X^6 - 1 = 6$. La dimension de C est $k = n - \deg g = 2$. Le nombre d'éléments de C est $7^k = 49$.

4. Montrez que la distance minimale d de C égale 5. Déduisez-en sa capacité de correction t.

Solution : Par construction, C est un code de Reed-Solomon de dimension 2 sur $\mathbb{F}_7$, donc sa distance minimale est $d = 7 - 2 = 5$, et sa capacité de correction est $t = \left\lfloor \frac{5-1}{2} \right\rfloor = 2$.

5. Déterminez la matrice génératrice G de C associée au polynôme générateur g.

Solution : $g = (X-1)(X-3)(X-2)(X-6) = X^4 + 2X^3 + 5X^2 + 5X + 1$ donc $G = \begin{pmatrix} 1 & 0 \\ 5 & 1 \\ 5 & 5 \\ 2 & 5 \\ 1 & 2 \\ 0 & 1 \end{pmatrix}$.

6. Déterminez le polynôme de contrôle h de C et la matrice de contrôle H associée.

Solution : $h_1 = (X-4)(X-5) = X^2 + 5X + 6$ donc $H_1 = \begin{pmatrix} 1 & 5 & 6 & 0 & 0 & 0 \\ 0 & 1 & 5 & 6 & 0 & 0 \\ 0 & 0 & 1 & 5 & 6 & 0 \\ 0 & 0 & 0 & 1 & 5 & 6 \end{pmatrix}$

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 $P(3x) = c_0 + 3c_1x + 3^2c_2x^2 + 3^3c_3x^3 + 3^4c_4x^4 + 3^5c_5x^5 \in C_{i-1}$.

Solution : Si $P(x) \in C_i$ alors il existe un polynôme Q tel que $P(x) = Q(x) \times (x-3^i)(x-3^{i+1})(x-3^{i+2})(x-3^{i+3})$. On a alors $P(3x) = Q(3x) \times (3x-3^i)(3x-3^{i+1})(3x-3^{i+2})(3x-3^{i+3}) = Q(3x) \times 3^4 \times (x-3^{i-1})(x-3^i)(x-3^{i+1})(x-3^{i+2})$ qui est un multiple de g_{i-1} donc un élément de C_{i-1}.

8. Montrez que les codes C_i sont tous en bijection avec $C_0 = C$.

Solution : La question précédente nous donne, pour $1 \leq i \leq 5$, deux applications : la première est $\varphi_i : C_i \to C_0$ définie par $\varphi_i\big(P(x)\big) = P(3^ix)$ et la seconde est $\psi_i : C_0 = C_6 \to C_i$ définie par $\psi_i\big(Q(x)\big) = Q(3^{6-i}x)$.
On a : $\varphi_i \circ \psi_i\big(Q(x)\big) = \varphi_i\big(Q(3^{6-i}x)\big) = Q(3^i3^{6-i}x) = Q(x)$ et $\psi_i \circ \varphi_i\big(P(x)\big) = \psi_i\big(P(3^ix)\big) = P(3^{6-i}3^ix) = P(x)$, ce qui montre que φ_i et ψ_i sont des bijections réciproques entre C_i et C_0.

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.

Solution : La longueur de C_i est $n_i = \deg X^6 - 1 = 6$. La dimension de C_i est $k_i = n_i - \deg g_i = 2$.
D'après les questions précédentes, si $P(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + c_5x^5 \in C_i$ est de poids w, alors $P(3^ix) = c_0 + 3^ic_1x + 3^{2i}c_2x^2 + 3^{3i}c_3x^3 + 3^{4i}c_4x^4 + 3^{5i}c_5x^5 \in C_0$ est également de poids w. Or la distance minimale de C_0 est 5, donc $w \geq 5$, ce qui montre que $d_i \geq 5$.
De même, si $Q(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + c_5x^5 \in C_0$ est de poids 5, alors $P(3^{6-i}x) = c_0 + 3^{6-i}c_1x + 3^{2(6-i)}c_2x^2 + 3^{3(6-i)}c_3x^3 + 3^{4(6-i)}c_4x^4 + 3^{5(6-i)}c_5x^5 \in C_i$ est également de poids 5, donc $d_i \leq 5$.
Conclusion : la distance minimale de C_i est $d_i = 5$ et sa capacité de correction est $t_i = \left\lfloor \frac{5-1}{2} \right\rfloor = 2$.