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

Examen du 14 décembre 2015

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.

Cet énoncé comporte 2 exercices. L'énoncé du deuxième exercice reprend une partie de l'énoncé du premier, mais il peut être traité indépendamment.

Exercice 1

1. Montrer que $X^2 + X + 1$ est le seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$.

Solution : Un polynôme de degré 2 est irréductible si et seulement s'il n'a pas de racine. Or ni 0 ni 1 ne sont racine de $X^2+X+1 \in \mathbb{F}_2[X]$ qui est donc irréductible. Les autres polynômes de degré 2 de $\mathbb{F}_2[X]$ sont X^2, $X^2+X = X(X+1)$ et $X^2+1 = (X+1)^2$ qui ne sont pas irréductibles.

2. Soit $P = X^4 + X + 1 \in \mathbb{F}_2[X]$. Montrer que P est irréductible.

Solution : Ni 0 ni 1 ne sont racines de P. Il en résulte que, si P n'est pas irréductible, alors il est le produit de 2 polynômes irréductibles de degré 2. Mais il n'y a qu'un seul polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$, à savoir $X^2 + X + 1$. On aurait donc $P = (X^2 + X + 1)^2$. Mais $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq P$, donc P est irréductible.

Soit $\mathbb{K} = \mathbb{F}_2[X]/P\mathbb{F}_2[X]$. On note x la classe de X dans $\mathbb{K}$.

3. Quelle est la valeur de $P(x) \in \mathbb{K}$?

Solution : Par définition $P(x) = x^4 + x + 1$ est la classe de P dans $\mathbb{F}_2[X]/P\mathbb{F}_2[X]$, donc $P(x) = 0$.

4. Montrer que tout élément a de $\mathbb{K}$ s'écrit de manière unique $a = a_3x^3 + a_2x^2 + a_1x + a_0$ où $(a_3, a_2, a_1, a_0) \in \mathbb{F}_2^4$.

Solution : Soit $a \in \mathbb{K}$. Il existe un polynôme $A \in \mathbb{F}_2[X]$ dont a est la classe, autrement dit $a = A(x)$. Effectuons la division euclidienne de A par P : il existe $Q, R \in \mathbb{F}_2[X]$ tels que $A = PQ + R$ et $\deg R < \deg P = 4$. On a alors $a = A(x) = P(x)Q(x) + R(x) = R(x)$. Mais $\deg R \leq 3$ donc il existe $(a_3, a_2, a_1, a_0) \in \mathbb{F}_2^4$ tels que $R = a_3X^3 + a_2X^2 + a_1X + a_0$ et on a alors $a = a_3x^3 + a_2x^2 + a_1x + a_0$. De plus, si $a = a_3x^3 + a_2x^2 + a_1x + a_0 = a'_3x^3 + a'_2x^2 + a'_1x + a'_0$ alors $(a_3 - a'_3)x^3 + (a_2 - a'_2)x^2 + (a_1 - a'_1)x + (a_0 - a'_0) = 0$ dans $\mathbb{K}$, donc le polynôme $S = (a_3 - a'_3)X^3 + (a_2 - a'_2)X^2 + (a_1 - a'_1)X + (a_0 - a'_0)$ est multiple de P. Or $\deg S < \deg P$ donc $S = 0$ d'où $(a_3, a_2, a_1, a_0) = (a'_3, a'_2, a'_1, a'_0)$.

5. Montrer que $\mathbb{K}$ est un corps.

Solution : P est irréductible, donc $\mathbb{K}$ est un corps.

6. Quel est l'inverse de x dans $\mathbb{K}$? Donner la réponse comme combinaison de x^3, x^2, x et 1.

Solution : On a $P(x) = x^4 + x + 1 = 0$ donc $x(x^3 + 1) = -1 = 1$ ($-1 = 1$ dans $\mathbb{K}$). Donc l'inverse de x est $x^3 + 1$.

7. Montrer que $P(X)^2 = P(X^2)$. En déduire que P a 4 racines distinctes dans $\mathbb{K}$ dont on donnera les valeurs. Exprimer chacune des racines comme combinaison de x^3, x^2, x et 1.

Solution : On a $P(X)^2 = (X^4+X+1)^2 = X^8+X^2+1+2X^5+2X^4+2X$. Or $2 = 0$ dans $\mathbb{K}$ donc $P(X)^2 = X^8+X^2+1 = P(X^2)$. On sait que $P(x) = 0$. On a donc $P(x^2) = P(x)^2 = 0$ et de même $P(x^4) = P(x^2)^2 = 0$, et $P(x^8) = P(x^4)^2 = 0$. Ainsi x, x^2, $x^4 = x+1$ et $x^8 = (x^4)^2 = (x+1)^2 = x^2+1$ sont 4 éléments distincts de $\mathbb{K}$, tous racines de P qui a degré 4. Ce sont donc toutes les racines de P dans $\mathbb{K}$. (On remarque que $x^{16} = (x^8)^2 = (x^2+1)^2 = x^4+1 = x$ qui est une racine déjà connue de P.)

Exercice 2

Introduction : un élément $b = b_3x^3+b_2x^2+b_1x+b_0$ du corps $\mathbb{K}$ défini dans l'exercice 1 est identifié par les coefficients $(b_3, b_2, b_1, b_0) \in \mathbb{F}_2^4$, c'est à dire par le nombre de 4 bits $b_3b_2b_1b_0$, ou encore par un chiffre dit « hexadécimal » entre 0 et F :

$\mathbb{K}$		BIN		HEX
0	$\longleftrightarrow$	0000	$\longleftrightarrow$	0
1	$\longleftrightarrow$	0001	$\longleftrightarrow$	1
x	$\longleftrightarrow$	0010	$\longleftrightarrow$	2
$x+1$	$\longleftrightarrow$	0011	$\longleftrightarrow$	3
x^2	$\longleftrightarrow$	0100	$\longleftrightarrow$	4
x^2+1	$\longleftrightarrow$	0101	$\longleftrightarrow$	5
x^2+x	$\longleftrightarrow$	0110	$\longleftrightarrow$	6
x^2+x+1	$\longleftrightarrow$	0111	$\longleftrightarrow$	7

$\mathbb{K}$		BIN		HEX
x^3	$\longleftrightarrow$	1000	$\longleftrightarrow$	8
x^3+1	$\longleftrightarrow$	1001	$\longleftrightarrow$	9
x^3+x	$\longleftrightarrow$	1010	$\longleftrightarrow$	A
x^3+x+1	$\longleftrightarrow$	1011	$\longleftrightarrow$	B
x^3+x^2	$\longleftrightarrow$	1100	$\longleftrightarrow$	C
x^3+x^2+1	$\longleftrightarrow$	1101	$\longleftrightarrow$	D
x^3+x^2+x	$\longleftrightarrow$	1110	$\longleftrightarrow$	E
x^3+x^2+x+1	$\longleftrightarrow$	1111	$\longleftrightarrow$	F

Les opérations en binaire sont données par les formules suivantes, qui résultent de la définition de $\mathbb{K}$:

$$(a_3, a_2, a_1, a_0) + (b_3, b_2, b_1, b_0) = (a_3 + b_3, a_2 + b_2, a_1 + b_1, a_0 + b_0)$$
$$(a_3, a_2, a_1, a_0) \times (b_3, b_2, b_1, b_0) = (c_6 + c_3, c_6 + c_5 + c_2, c_5 + c_4 + c_1, c_4 + c_0)$$

$$\text{avec} \begin{cases} c_6 = a_3b_3 & c_2 = a_2b_0 + a_1b_1 + a_0b_2 \\ c_5 = a_3b_2 + a_2b_3 & c_1 = a_1b_0 + a_0b_1 \\ c_4 = a_3b_1 + a_2b_2 + a_1b_3 & c_0 = a_0b_0 \\ c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 & \end{cases}$$

Les tables d'addition et de multiplication de $\mathbb{K}$ en notation hexadécimale sont données ci-dessous. L'élément neutre pour l'addition est 0 et l'élément neutre pour la multiplication est 1, mais ATTENTION : pour les éléments de 2 à 9, ces opérations ne correspondent pas aux opérations « standards ».

Table d'addition

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Table de multiplication

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

Pour tous les calculs, se reporter aux tables d'addition et de multiplication ci-dessus.

Questions :

1. Soit $a = 8 \in \mathbb{K}$. Déterminer a^2, a^3, a^4 et a^5. Se reporter à la table de multiplication ci-dessus.

Solution : $a^2 = \mathrm{C}$, $a^3 = \mathrm{A}$, $a^4 = \mathrm{F}$ et $a^5 = 1$.

2. Montrer que $1, a, a^2, a^3$ et a^4 sont les 5 racines dans $\mathbb{K}$ du polynôme $X^5 - 1$. Justifier la réponse.

Solution : On a $1^5 = 1$ et $a^5 = 1$ donc également $(a^2)^5 = 1$, $(a^3)^5 = 1$ et $(a^4)^5 = 1$. Donc $1, a, a^2, a^3$ et a^4 sont les 5 racines du polynôme $X^5 - 1$.

Soit $g = (X - 1)(X - a) \in \mathbb{K}[X]$.

3. Développer g dans $\mathbb{K}[X]$. Les calculs doivent figurer sur la copie.

Solution : $g = (X-1)(X-8) = X^2 - (1+8)X + 8 = X^2 - 9X + 8 = X^2 + 9X + 8$.

Soit $\mathscr{C}$ le code cyclique de longueur 5 de polynôme générateur g.

4. Quel est la dimension k de $\mathscr{C}$? Justifier la réponse.

Solution : $k = 5 - \deg g = 3$.

5. Donner une matrice génératrice G de $\mathscr{C}$. Justifier la réponse.

Solution : $G = \begin{pmatrix} 8 & 0 & 0 \\ 9 & 8 & 0 \\ 1 & 9 & 8 \\ 0 & 1 & 9 \\ 0 & 0 & 1 \end{pmatrix}$ qui est la matrice génératrice associée au polynôme générateur g.

6. Soit $m = \begin{pmatrix} 1 \\ 4 \\ 6 \end{pmatrix} \in \mathbb{K}^3$. Encoder m à l'aide de la matrice génératrice G. Les calculs doivent figurer sur la copie.

Solution : $G \times m = \begin{pmatrix} 8 \\ 9 + (8 \times 4) \\ 1 + (9 \times 4) + (8 \times 6) \\ 4 + (9 \times 6) \\ 6 \end{pmatrix} = \begin{pmatrix} 8 \\ 9 + 6 \\ 1 + 2 + 5 \\ 4 + 3 \\ 6 \end{pmatrix} = \begin{pmatrix} 8 \\ F \\ 6 \\ 7 \\ 6 \end{pmatrix}$

7. Déterminer le polynôme de contrôle h de $\mathscr{C}$. Les calculs doivent figurer sur la copie.

Solution : $X^5 - 1 = (X-1)(X-a)(x-a^2)(x-a^3)(X-a^4)$ et $g = (X-1)(X-a)$ donc $h = (x-a^2)(x-a^3)(X-a^4) = (X+\mathrm{C})(X+\mathrm{A})(X+\mathrm{F}) = (X^2+(\mathrm{C}+\mathrm{A})X+\mathrm{CA})(X+\mathrm{F}) = (X^2+6X+1)(X+\mathrm{F}) = X^3+(6+\mathrm{F})X^2+(6\mathrm{F}+1)X+\mathrm{F} = X^3 + 9X^2 + 5X + \mathrm{F}$.

8. Donner une matrice de contrôle H de $\mathscr{C}$. Justifier la réponse.

Solution : $H = \begin{pmatrix} 1 & 9 & 5 & \mathrm{F} & 0 \\ 0 & 1 & 9 & 5 & \mathrm{F} \end{pmatrix}$ qui est la matrice de contrôle associée au polynôme de contrôle h.

9. Déterminer la distance minimum d de $\mathscr{C}$, ainsi que sa capacité de correction t. Justifier la réponse.

Solution : La première colonne est indépendante de toutes les autres, de même que la dernière. De plus $9^2 \neq 5$, $9 \times 5 \neq \mathrm{F}$ et que $5^2 \neq \mathrm{F} \times 9$ donc la deuxième, la troisième et la quatrième colonne sont 2 à 2 indépendantes. On en déduit que $d \geq 3$. Or $d \leq n - k + 1 = 3$ donc $d = 3$ et $t = 1$.

10. Soit $\gamma = \begin{pmatrix} \mathrm{C} \\ 0 \\ \mathrm{A} \\ 0 \\ 1 \end{pmatrix} \in \mathbb{K}^5$.

(a) Calculer le syndrome de $S(\gamma)$. Les calculs doivent figurer sur la copie.

Solution : $S(\gamma) = H \times \gamma = \begin{pmatrix} \mathrm{C} + (5 \times \mathrm{A}) \\ (9 \times \mathrm{A}) + \mathrm{F} \end{pmatrix} = \begin{pmatrix} 8 \\ \mathrm{A} \end{pmatrix}$

(b) Déterminer la colonne de H dont $S(\gamma)$ est multiple et en déduire $c \in \mathscr{C}$ tel que $d(c, \gamma) \leq t$.

Solution : $\begin{pmatrix} 8 \\ \mathrm{A} \end{pmatrix} = 7 \begin{pmatrix} 5 \\ 9 \end{pmatrix}$ et $\begin{pmatrix} 5 \\ 9 \end{pmatrix}$ est la troisième colonne de H. On en déduit que $c = \gamma - \begin{pmatrix} 0 \\ 0 \\ 7 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathrm{C} \\ 0 \\ \mathrm{D} \\ 0 \\ 1 \end{pmatrix}$

(c) Sachant qu'un chiffre hexadécimal représente une séquence de 4 bits, donner la distance en nombre de bit entre γ et c. Justifier la réponse.

Solution : La distance en nombre de bit entre γ et c est égal la distance en nombre de bit entre A et D, c'est à dire 3, qui n'est autre que le nombre de bit non nul du chiffre hexadécimal $7 = \mathrm{A} - \mathrm{D}$.

(d) Déterminer le message $m \in \mathbb{K}^3$ associé à c. Justifier la réponse.

Solution : Si $m = \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$ alors $G \times m = \begin{pmatrix} 8m_1 \\ 9m_1 + 8m_2 \\ m_1 + 9m_2 + 8m_3 \\ m_2 + 9m_3 \\ m_3 \end{pmatrix} = \begin{pmatrix} \mathrm{C} \\ 0 \\ \mathrm{D} \\ 0 \\ 1 \end{pmatrix}$.

La dernière coordonnée donne $m_3 = 1$. L'avant dernière donne alors $m_2 = 9$. Enfin, la première ou la seconde coordonnée donnent directement $m_1 = 8$.

D'où $m = \begin{pmatrix} 8 \\ 9 \\ 1 \end{pmatrix}$