

Correction des exercices - Chapitre VI

Exercice 1

- 1) Soit $f \in \mathbb{F}_3[X]$ un tel polynôme. Posons $f = X^2 + aX + b$. Notons Δ son discriminant. On a $\Delta = a^2 - 4b$. Les racines de f dans tout corps contenant \mathbb{F}_3 sont

$$\frac{-a \pm d}{2} \quad \text{où} \quad d^2 = \Delta.$$

Ce sont les formules de résolution des équations du second degré, valables pour tout corps de caractéristique différente de 2. Le fait que f n'ait pas de racines dans \mathbb{F}_3 signifie donc que Δ n'est pas un carré dans \mathbb{F}_3 , autrement dit que l'on a dans \mathbb{F}_3

$$a^2 - 4b = 2,$$

ce qui signifie que l'on a

$$(a, b) \in \{(0, 1), (1, 2), (2, 2)\}.$$

Il y a ainsi trois polynômes irréductibles unitaires de degré 2 sur \mathbb{F}_3 (ce que l'on savait déjà, voir le cours ou l'exercice 7 de la feuille du chapitre V), qui sont

$$X^2 + 1, \quad X^2 + X + 2, \quad X^2 + 2X + 2.$$

- 2) On a l'égalité

$$X^8 - X = \prod_f f,$$

où f parcourt l'ensemble des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré divisant 3 (th. 6.6). Ceux de degré 1 sont X et $X + 1$, et ceux de degré 3 sans racines dans \mathbb{F}_2 sont $X^3 + X + 1$ et $X^3 + X^2 + 1$, d'où la décomposition

$$X^8 - X = X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

- 3) Il s'agit d'expliciter un polynôme de degré 2 de $\mathbb{F}_5[X]$ (resp. $\mathbb{F}_7[X]$) irréductible sur \mathbb{F}_5 (resp. \mathbb{F}_7). Par exemple, les polynômes

$$f_1 = X^2 + 2 \in \mathbb{F}_5[X] \quad \text{et} \quad f_2 = X^2 + 1 \in \mathbb{F}_7[X]$$

conviennent, d'où à isomorphisme près,

$$\mathbb{F}_{25} = \mathbb{F}_5[X]/(f_1) \quad \text{et} \quad \mathbb{F}_{49} = \mathbb{F}_7[X]/(f_2).$$

- 4) L'ordre de 2 divise 18 qui l'ordre de \mathbb{F}_{19}^* . Il s'agit de vérifier que 2^6 et 2^9 sont distincts de 1 (prop. 2.9). On a $2^6 = 7$ et $2^9 = -1$, d'où l'assertion. En particulier, l'entier n tel que $0 \leq n \leq 17$ et $7 = 2^n$ est $n = 6$, c'est donc le logarithme discret de base 2 de 7.
- 5) Si $p = 2$, le seul générateur de \mathbb{F}_2^* est 1, d'où $\log_1(-1) = 0$. Supposons $p \geq 3$. On a

$$\left(g^{\frac{p-1}{2}}\right)^2 = g^{p-1} = 1.$$

Parce que g est un générateur de \mathbb{F}_p^* , on a donc

$$g^{\frac{p-1}{2}} = -1,$$

d'où $\log_g(-1) = \frac{p-1}{2}$.

Exercice 2

- 1) Soit x un élément de K^* . On a $x^{q-1} = 1$. Par hypothèse, $q-1$ divise n , on a donc $x^n = 1$. Puisque n est non nul, 0^n est nul. On obtient $S_n = q-1$. Par ailleurs, q est une puissance de la caractéristique de K , d'où $q = 0$, puis $S_n = -1$.
- 2) Si $n = 0$, pour tout $x \in K$ on a $x^n = 1$ (y compris si $x = 0$). On obtient $S_n = q = 0$. Supposons n non divisible par $q-1$. On a en particulier $n \geq 1$ et 0^n est nul. Soit g un générateur de K^* . On a ainsi

$$S_n = \sum_{j=0}^{q-2} (g^j)^n = \sum_{j=0}^{q-2} (g^n)^j.$$

D'après l'hypothèse faite sur n , on a $g^n \neq 1$, d'où

$$S_n = \frac{1 - (g^n)^{q-1}}{1 - g^n} = 0.$$

Exercice 3

Soit $f : K^* \rightarrow K^*$ l'homomorphisme de groupes défini pour tout $x \in K$ par $f(x) = x^2$.

- 1) Si $p = 2$, pour tout $x \in K$, on a $x^2 = 1$ si et seulement $(x-1)^2=0$ i.e. $x = 1$. Par suite, f est injectif, donc est surjectif car K est fini, d'où le résultat.
- 2) Le noyau de f est $\{\pm 1\}$. Il est d'ordre 2 car p est impair. Le groupe quotient $K^*/\text{Ker}(f)$ étant isomorphe à l'image de f (th. 2.7), le sous-groupe des carrés non nuls de K est donc d'ordre $\frac{q-1}{2}$, d'où $|K^2| = 1 + \frac{q-1}{2} = \frac{q+1}{2}$.

3) Considérons un élément $a \in K$. L'ensemble

$$S = \{a - x^2 \mid x \in K\}$$

est aussi de cardinal $(q+1)/2$. On en déduit que $S \cap K^2$ n'est pas vide. Il existe ainsi des éléments x et y de K tels que l'on ait $a - x^2 = y^2$, d'où l'assertion.

- 4.1) Le groupe K^* est cyclique d'ordre $q-1$. Il existe donc un unique sous-groupe de K^* d'ordre $\frac{q-1}{2}$ et il est formé des éléments $x \in K^*$ tel que $x^{\frac{q-1}{2}} = 1$ (th. 2.4). D'après la deuxième question, c'est donc le sous-groupe des carrés non nuls de K .
- 4.2) On en déduit que -1 est un carré dans K si et seulement si on a $(-1)^{\frac{q-1}{2}} = 1$, ce qui signifie que q est congru à 1 modulo 4.

Exercice 4

- 1) Posons $N = 2^{2k}(2k)!$. Comme indiqué dans l'énoncé, on a

$$N = \prod_{i=1}^{2k} (2i) = \prod_{i=1}^k (2i) \prod_{i=1}^k (2k+2i).$$

Par ailleurs, on a la congruence

$$\prod_{i=1}^k (2k+2i) \equiv (-1)^k \prod_{i=1}^k (2k+1-2i) \pmod{p}.$$

De l'égalité

$$\prod_{i=1}^k (2i) \prod_{i=1}^k (2k+1-2i) = (2k)!,$$

on déduit alors que $N \equiv (-1)^k (2k)! \pmod{p}$. On a $2k = \frac{p-1}{2}$, donc $(2k)!$ n'est pas divisible par p . Cela entraîne $2^{2k} \equiv (-1)^k \pmod{p}$, d'où la congruence annoncée.

- 2) Posons $M = 2^{2k+1}(2k+1)!$. On a

$$M = \prod_{i=1}^{2k+1} (2i) = \prod_{i=1}^k (2i) \prod_{i=1}^{k+1} (2k+2i),$$

$$\prod_{i=1}^{k+1} (2k+2i) \equiv (-1)^{k+1} \prod_{i=1}^{k+1} (2k+3-2i) \pmod{p}.$$

Comme ci-dessus, de l'égalité

$$\prod_{i=1}^k (2i) \prod_{i=1}^{k+1} (2k+3-2i) = (2k+1)!,$$

on déduit la congruence $M \equiv (-1)^{k+1}(2k+1)! \pmod{p}$. On a $2k+1 = \frac{p-1}{2}$, donc $(2k+1)!$ n'est pas divisible par p , d'où le résultat.

- 3) D'après l'exercice 3 (question 4.1), 2 est un carré dans \mathbb{F}_p si et seulement si on a $2^{\frac{p-1}{2}} = 1$. D'après ce qui précède, cela équivaut à $p \equiv \pm 1 \pmod{8}$.

Exercice 5 (Racines carrées dans \mathbb{F}_p)

- 1) On a les égalités

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a.$$

Parce que a est un carré non nul dans \mathbb{F}_p , on a $a^{\frac{p-1}{2}} = 1$ (exercice 3), d'où $\left(a^{\frac{p+1}{4}}\right)^2 = a$.

- 2.1) On a les égalités

$$\left(a^{\frac{p-1}{4}}\right)^2 = a^{\frac{p-1}{2}} = 1$$

ce qui entraîne l'assertion.

- 2.2) D'après l'hypothèse faite, on a

$$\left(a^{\frac{p+3}{8}}\right)^2 = a^{\frac{p+3}{4}} = a^{\frac{p-1}{4}} a = a.$$

- 2.3) On a dans ce cas

$$\left(2a(4a)^{\frac{p-5}{8}}\right)^2 = a^{\frac{p+3}{4}} 2^{\frac{p-5}{2}+2} = a^{\frac{p+3}{4}} 2^{\frac{p-1}{2}} = aa^{\frac{p-1}{4}} 2^{\frac{p-1}{2}}.$$

Parce que l'on a $p \equiv 5 \pmod{8}$, on a $2^{\frac{p-1}{2}} = -1$ (exercices 3 et 4), d'où l'égalité

$$\left(2a(4a)^{\frac{p-5}{8}}\right)^2 = a.$$

Exercice 6

Soient P et Q des polynômes de $K[X]$ dont les degrés sont $< q$. Les fonctions polynômes associées à P et Q sont égales si et seulement si $P = Q$. En effet, $P - Q$ est de degré $< q$, donc $P - Q$ ne peut avoir q racines que s'il est nul. Les fonctions polynômes associées aux polynômes de $K[X]$ de degré $< q$ forment donc un ensemble de q^q applications de K dans K . L'assertion en résulte vu que l'ensemble des applications de K dans K est aussi de cardinal q^q .

Exercice 7 (Théorème de Wolstenholme)

- 1) Il existe $u \in \mathbb{N}$ tel que $S = \frac{u}{(p-1)!}$. L'assertion en résulte car p ne divise pas $(p-1)!$.
 2) On a l'égalité

$$(1) \quad \frac{N}{D} = \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{1}{k} + \frac{1}{p-k} \right).$$

Les entiers D , k et $p - k$, pour $k = 1, \dots, \frac{p-1}{2}$ sont non nuls modulo p , i.e. sont inversibles modulo p . On déduit de (1) que l'on a dans \mathbb{F}_p

$$\frac{N}{D} \bmod p = 0$$

autrement dit, p divise N .

2) Posons $M = \frac{N}{p} \in \mathbb{Z}$. D'après (1), on a

$$\frac{N}{D} = p \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)}.$$

On a donc dans \mathbb{F}_p^* l'égalité

$$M \bmod p = -D \left(\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} \right) \bmod p.$$

Tout revient à vérifier que l'on a

$$\left(\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} \right) \bmod p = \sum_{x \in \mathbb{F}_p^*} x^2.$$

Considérons pour cela deux entiers i et j tels $i^2 \equiv j^2 \bmod p$ et $1 \leq i \leq j \leq \frac{p-1}{2}$. L'entier p divise $i - j$ ou $i + j$. Les inégalités $0 \leq j - i \leq j + i \leq p - 1$ entraînent alors $i = j$. Par ailleurs, il y a $(p-1)/2$ carrés dans \mathbb{F}_p^* , d'où notre assertion.

3) On a $p \geq 5$. D'après l'exercice 2 (question 2), la somme des carrés de \mathbb{F}_p^* est donc nulle. On obtient $M \bmod p = 0$, autrement dit, p divise M i.e. p^2 divise N .

Exercice 8

Posons $f = X^4 + X + 1$.

- 1) Il s'agit de démontrer que f est irréductible dans $\mathbb{F}_2[X]$. On remarque d'abord que f n'a pas de racines dans \mathbb{F}_2 . Par ailleurs, il existe un unique polynôme de $\mathbb{F}_2[X]$ irréductible de degré 2, qui est $1 + X + X^2$. Si f était réductible sur \mathbb{F}_2 , il serait donc divisible par ce polynôme, ce qui n'est pas, vu l'égalité $f = (X^2 + X + 1)(X^2 + X) + 1$.
- 2) La caractéristique de K , qui est celle de \mathbb{F}_2 , est 2. Son cardinal est $2^4 = 16$.
- 3) On a l'égalité $\alpha^4 = \alpha + 1$. On en déduit que l'on a

$$(1) \quad \alpha^5 = \alpha^2 + \alpha, \quad \alpha^6 = \alpha^3 + \alpha^2 \quad \text{et} \quad \alpha^7 + 1 = \alpha^3 + \alpha.$$

Les coordonnées de $\alpha^7 + 1$ dans \mathcal{B} sont donc $(0, 1, 0, 1)$.

- 4) Une méthode consiste par exemple à trouver une relation de Bézout entre f et $X^3 + X$. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	X	$X + 1$	X	$X + 1$	
$X^4 + X + 1$	$X^3 + X$	$X^2 + X + 1$	$X + 1$	1	0
1	0	1	$X + 1$	$X^2 + X + 1$	
0	1	X	$X^2 + X + 1$	$X^3 + X^2$	

On en déduit l'égalité

$$(X^2 + X + 1)f + (X^3 + X)(X^3 + X^2) = 1.$$

Compte tenu de l'égalité $f(\alpha) = 0$, on obtient $(\alpha^3 + \alpha)(\alpha^3 + \alpha^2) = 1$, et l'inverse de $\alpha^7 + 1$ est $\alpha^3 + \alpha^2$. Ses coordonnées dans \mathcal{B} sont $(0, 0, 1, 1)$.

- 5) L'ordre du groupe K^* est 15. D'après le théorème de Lagrange, les ordres possibles de ses éléments sont 1, 3, 5 et 15.
- 6) Parce que \mathcal{B} est une base de K , les éléments α et α^3 sont distincts de 1 et d'après (1) il en est de même de α^5 . Ainsi α est d'ordre 15 i.e. α est un générateur de K^* . Par ailleurs, il y a $\varphi(15) = 8$ générateurs dans K^* .
- 7) D'après (1), on a $\alpha + \alpha^2 = \alpha^5$, qui est d'ordre 3.
- 8) Supposons P réductible dans K . Il existe alors $\gamma \in K$ tel que $P(\gamma) = 0$. On a les égalités $P(\gamma^2) = P(\gamma^4) = 0$ (lemme 6.7, assertion 2) et l'on vérifie directement que γ , γ^2 et γ^4 sont distincts deux à deux. On a donc

$$P = (Y - \gamma)(Y - \gamma^2)(Y - \gamma^4).$$

On déduit que $\gamma^7 = 1$. On a $\gamma \neq 1$, donc γ est d'ordre 7 dans K^* , d'où une contradiction car K^* est d'ordre 15.

Le K -espace vectoriel $K[Y]/(P)$ est de dimension 3. Par suite, son cardinal est

$$|K|^3 = 2^{12} = 4096.$$

Exercice 9

Soit N le nombre cherché. On a l'égalité

$$X^{p^\ell} - X = \prod f,$$

où f parcourt l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré divisant ℓ (th. 6.6). Il y a p polynôme unitaires de degré 1. Puisque ℓ est premier, on a donc l'égalité $p^\ell = p + N\ell$, d'où

$$N = \frac{p^\ell - p}{\ell}.$$

Exercice 10

Si (1) ou (2) est satisfaite, la condition de l'énoncé est satisfaite car K^* est trivial (si $K = \mathbb{F}_2$) ou bien est un groupe d'ordre premier.

Inversement, supposons que tout élément de K^* , autre que 1, soit un générateur de K^* et que K ne soit pas \mathbb{F}_2 . Notons q le cardinal de K . Vérifions que $q - 1$ est premier. On a $q - 1 \geq 2$ car $K \neq \mathbb{F}_2$. Soit d un diviseur de $q - 1$, distinct de $q - 1$. Il existe $a \in K^*$ d'ordre d , car K^* est cyclique. L'élément a n'est pas un générateur de K^* . D'après l'hypothèse faite, on a donc $a = 1$, puis $d = 1$, d'où l'assertion. Par ailleurs, $q - 1 = p^n - 1$ est divisible par $p - 1$. On en déduit que l'on a

$$p - 1 = q - 1 \quad \text{ou bien} \quad p - 1 = 1.$$

Si $p - 1 = 1$, on a $p = 2$, donc $q - 1 = 2^n - 1$ est un nombre premier et la condition (2) est satisfaite. Supposons $p - 1 = q - 1$. Dans ce cas, on a $n = 1$. Les entiers p et $p - 1$ étant des nombres premiers, on obtient $p = 3$, puis $K = \mathbb{F}_3$, d'où le résultat.

Exercice 11

- 1) Le polynôme f est irréductible sur \mathbb{F}_5 , car il est de degré 3 et n'a pas de racines dans \mathbb{F}_5 . Par suite, K est un corps.
- 2) La caractéristique de K est 5 et son cardinal est $5^3 = 125$.
- 3) Le groupe K^* est d'ordre 124. On a $124 = 4 \times 31$. Les ordres possibles des éléments de K^* sont donc 1, 2, 4, 31, 62 et 124.
- 4) On a $\alpha^3 = -1 - \alpha$. Par ailleurs, on a $\alpha^5 = 1 + \alpha - \alpha^2$. Puisque K est de caractéristique 5, il en résulte que l'on a

$$\alpha^{15} = -(1 + \alpha)^5 = -1 - \alpha^5 = \alpha^2 - \alpha - 2.$$

On en déduit que

$$\alpha^{30} = (\alpha^2 - \alpha - 2)^2 = \alpha^2 + 1.$$

- 5) L'élément α n'est pas d'ordre 1, 2 ni 4. D'après la question précédente, on a

$$\alpha^{31} = -1.$$

Ainsi, α est d'ordre 62. Par ailleurs, on constate directement que 2α n'est pas d'ordre 1, 2 ni 4. On a $2^4 \equiv 1 \pmod{5}$ et $2^{31} \equiv 3 \pmod{5}$, d'où $(2\alpha)^{31} = 2$ puis

$$(2\alpha)^{62} = -1.$$

Il en résulte que 2α est d'ordre 124, autrement dit, 2α est un générateur de K^* .

6) Dans $\mathbb{F}_5[X]$, on obtient par division euclidienne l'égalité

$$f = (X + 1)(X^2 - X + 2) - 1.$$

Vu que l'on a $f(\alpha) = 0$, on en déduit que $(\alpha + 1)(\alpha^2 - \alpha + 2) = 1$ i.e. que l'inverse de $\alpha + 1$ est $\alpha^2 - \alpha + 2$, dont les coordonnées dans \mathcal{B} sont $(2, -1, 1)$.

7) On a $f(\alpha) = 0$. Le corps K étant de caractéristique 5, cela entraîne $f(\alpha^5) = 0$. Par ailleurs, on a $\alpha^5 \neq \alpha$. Il en résulte que f a toutes ses racines dans K . Leur produit étant -1 , la troisième racine de f est donc $-\alpha^{-6}$. On a $\alpha^6 = (\alpha + 1)^2$. D'après la question précédente, on a ainsi

$$\alpha^{-6} = (\alpha^2 - \alpha + 2)^2 = -\alpha^2 + 2\alpha + 1.$$

Les racines de f sont donc

$$\alpha, \quad -\alpha^2 + \alpha + 1 \quad \text{et} \quad \alpha^2 - 2\alpha - 1.$$

Exercice 12

1) Soit a un élément de \mathbb{F}_p . On a $a^p = a$. Par ailleurs, on a

$$(a + \alpha)^p - (a + \alpha) + u = a^p + \alpha^p - (a + \alpha) + u = \alpha^p - \alpha + u = 0.$$

2) Le degré de f est p , d'où l'assertion (question 1).

3.1) Notons n le degré de g . On a $n \geq 1$ et le coefficient de X^{n-1} de g est l'opposé de la somme des racines de g . Parce que g est à coefficients dans \mathbb{F}_p , la somme de ses racines est donc dans \mathbb{F}_p .

3.2) D'après la question 2, il existe des éléments $a_{i_1}, \dots, a_{i_n} \in \mathbb{F}_p$ tels que les racines de g soient les $\alpha + a_{i_k}$. La somme de ces éléments est dans \mathbb{F}_p (question précédente). On en déduit que $n\alpha$ l'est aussi. On a $n < p$, donc n est non nul modulo p . Il en résulte que α est dans \mathbb{F}_p . On obtient une contradiction car u étant non nul, on a $\alpha^p \neq \alpha$, d'où le résultat.

Exercice 13

1) Posons $f = X^6 + X + 1$. Ce polynôme n'a pas de racines dans \mathbb{F}_2 . Dans $\mathbb{F}_2[X]$, le seul polynôme irréductible de degré 2 est $X^2 + X + 1$, et les polynômes irréductibles de degré 3 sont

$$g = X^3 + X + 1 \quad \text{et} \quad h = X^3 + X^2 + 1.$$

On a

$$f = (1 + X^3)^2 + X = (1 + X)^2(1 + X + X^2)^2 + X,$$

donc f n'est pas divisible par $X^2 + X + 1$. Par ailleurs, f est distinct de g^2 , h^2 et gh . Il en résulte que f est irréductible sur \mathbb{F}_2 , donc K est un corps. Son cardinal est 64.

- 2) Le groupe K^* est d'ordre 63. On a $63 = 3^2 \times 7$. Il suffit alors de vérifier que l'on a (prop. 2.9)

$$\alpha^{\frac{63}{7}} = \alpha^9 \neq 1 \quad \text{et} \quad \alpha^{\frac{63}{3}} = \alpha^{21} \neq 1.$$

L'égalité $\alpha^6 = \alpha + 1$ implique

$$\alpha^9 = \alpha^4 + \alpha^3,$$

d'où $\alpha^9 \neq 1$, car $(1, \alpha, \dots, \alpha^5)$ est une base du \mathbb{F}_2 -espace vectoriel K . Par ailleurs, on a

$$\alpha^{18} = \alpha^8 + \alpha^6 = 1 + \alpha + \alpha^2 + \alpha^3,$$

d'où l'égalité

$$\alpha^{21} = 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^5.$$

On a donc $\alpha^{21} \neq 1$, d'où l'assertion.

- 3) On a $(1 + \alpha^3)^2 = 1 + \alpha^6 = \alpha$, donc α est un carré dans K .
 4) Comme indiqué dans l'énoncé, pour tout $x \in K$, on a $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Il s'agit ainsi de déterminer les racines cubiques de l'unité de K autres que 1. Pour tout $y \in K^*$, on a les égalités

$$y^{63} = (y^{21})^3 = 1.$$

Par suite, si l'on a $y^{21} \neq 1$, alors y^{21} est une solution de l'équation

$$(1) \quad 1 + x + x^2 = 0.$$

Il en résulte que α^{21} est une solution de (1). Par ailleurs, si $a \in K$ vérifie l'égalité (1), il en est de même de $1 + a$. Les racines de (1) sont donc

$$\alpha^{21} \quad \text{et} \quad 1 + \alpha^{21},$$

autrement dit,

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^5 \quad \text{et} \quad \alpha + \alpha^3 + \alpha^4 + \alpha^5.$$

Exercice 14 (Protocole de Diffie-Hellman)

- 1) Le polynôme $X^2 + 1 \in \mathbb{F}_3[X]$ est irréductible sur \mathbb{F}_3 , car il est de degré 2 et n'a pas de racines dans \mathbb{F}_3 . Par suite, K est un corps. Le cardinal de K est 9 et K^* est un groupe d'ordre 8. On a $1 + \alpha^2 = 0$ et les égalités

$$(1 + \alpha)^2 = 2\alpha \quad \text{et} \quad (1 + \alpha)^4 = (2\alpha)^2 = \alpha^2 = -1.$$

Il en résulte que $1 + \alpha$ est d'ordre 8 dans K^* i.e. que c'est un générateur de K^* .

- 2) Notons a et b les logarithmes discrets de base $1 + \alpha$ respectivement de α et $2 + \alpha$. Leur clé commune de chiffrement est $(1 + \alpha)^{ab}$. Déterminons a et b (il suffit en fait de déterminer a ou b). Pour cela, on vérifie que l'on a

$$(1 + \alpha)^3 = 1 + 2\alpha, \quad (1 + \alpha)^5 = 2 + 2\alpha, \quad (1 + \alpha)^6 = \alpha \quad \text{et} \quad (1 + \alpha)^7 = 2 + \alpha.$$

On obtient ainsi $a = 6$ et $b = 7$. Par ailleurs, on a $(1 + \alpha)^8 = 1$, d'où

$$(1 + \alpha)^{42} = (1 + \alpha)^2 = 2\alpha.$$

La clé cherchée est donc 2α . (On notera que l'on a $\alpha^7 = (2 + \alpha)^6 = 2\alpha$.)

Exercice 15 (Algorithme de El Gamal)

Déterminons a . On remarque pour cela que l'on a $(1 + \alpha^2)^2 = 1 + \alpha^4 = \alpha$. De l'égalité $(1 + \alpha^2)^{16} = 1 + \alpha^2$ (on a $x^{16} = x$ pour tout $x \in K$), on déduit alors que l'on a $1 + \alpha^2 = \alpha^8$, d'où $a = 8$. Par définition, si m est le message que Bob souhaite transmettre à Alice, on a

$$m\alpha^{3a} = \alpha + \alpha^2 + \alpha^3.$$

Par ailleurs, on a $\alpha^{15} = 1$, d'où l'on déduit que

$$\alpha^{3a} = \alpha^{24} = \alpha^9.$$

L'inverse de α^{3a} i.e. de α^9 est

$$(\alpha^9)^{14} = \alpha^{126} = \alpha^{8 \times 15 + 6} = \alpha^6,$$

autrement dit, on a

$$(\alpha^9)^{-1} = \alpha^2 + \alpha^3.$$

(De l'égalité $\alpha^{15} = 1$, on peut aussi déduire directement que l'inverse de α^9 est α^6 .)

On obtient $m = (\alpha + \alpha^2 + \alpha^3)(\alpha^2 + \alpha^3)$, d'où $m = \alpha^2$.
