EXAMEN DU 21 JANVIER 2005

Durée 2 heures

Les documents, calculatrices et téléphones portables sont interdits.

Toutes les réponses devront être soigneusement justifiées.

⋆ ⋆ ⋆⋆

Question de cours

Sachant que dans un corps $\mathbb{K}$ de caractéristique p, on a la relation

$$\forall a \in \mathbb{K},\ \forall b \in \mathbb{K}, \quad (a+b)^p = a^p + b^p,$$

démontrer le théorème suivant :

Théorème *Soit $\mathbb{K}$ un corps fini de caractéristique p, et soit $Q \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$. On a l'équivalence*

$$\Big(Q \in \mathbb{F}_p[X]\Big) \Longleftrightarrow \Big(\ (Q(X))^p = Q(X^p)\ \Big).$$

⋆ ⋆ ⋆⋆

Problème

Partie I Soit $P \in \mathbb{F}_2[X]$ le polynôme défini par $P = X^4 + X + 1$.

1. Montrer que l'anneau quotient $\mathbb{K} = \mathbb{F}_2[X]/\langle P\rangle$ est un corps.
2. Déterminer
   (a) la caractéristique du corps $\mathbb{K}$,
   (b) une base du $\mathbb{F}_2$-espace vectoriel $\mathbb{K}$ et la dimension de cet espace vectoriel,
   (c) le nombre d'éléments de $\mathbb{K}$.
3. Soit $\alpha = \overline{X}$ la classe du polynôme X dans $\mathbb{K}$, montrer que α est un élément primitif du corps $\mathbb{K}$.

Partie II : Étude d'un code de Hamming de longueur 15

Dans ce qui suit, P désigne toujours le polynôme X^4+X+1, $\mathbb{K}$ désigne le corps défini dans la question 1 de la partie I, et α l'élément primitif de $\mathbb{K}$ défini dans la question 3 de la partie I.
On considère l'application $\mathbb{F}_2$-linéaire u de $(\mathbb{F}_2)^{15}$ dans $\mathbb{K}$ définie par

$$\forall (c_0, c_1, \ldots, c_{14}) \in (\mathbb{F}_2)^{15}, \qquad u(c_0, c_1, \ldots, c_{14}) = \sum_{k=0}^{14} c_k\, \alpha^k,$$

et on désigne par C le code binaire de longueur 15 défini par $C = \ker(u) \subset (\mathbb{F}_2)^{15}$.
Chaque vecteur $(c_0, c_1, \ldots, c_{14}) \in (\mathbb{F}_2)^{15}$ est identifié au mot $c_0c_1\ldots c_{14}$ de longueur 15. On appelle mots de code les éléments de C.

1. Montrer qu'il n'existe pas de mot de code de poids 1.
2. Montrer qu'il n'existe pas de mot de code de poids 2.
3. Déterminer un mot de code de poids 3.

4. En déduire la distance minimale d du code C et sa capacité de correction.
5. Montrer que $\mathrm{Im}\,(u) = \mathbb{K}$. En déduire
   (a) la dimension du code C,
   (b) le nombre d'éléments de C.
6. Montrer que le code C est parfait.
7. Montrer que le code C est cyclique.
8. Montrer que que le polynôme P divise le polynôme $X^{15} - 1$ dans dans $\mathbb{F}_2[X]$.
9. Montrer que P est le polynôme générateur du code cyclique C.
10. Combien de lignes et de colonnes possède une matrice génératrice G de C? Justifier.
11. Déterminer une première ligne possible d'une matrice génératrice de C.
12. Déterminer le polynôme de contrôle h du code cyclique C.
13. Combien de lignes et de colonnes possède une matrice de contrôle H de C? Justifier.
14. Déduire de la question 12 une matrice de contrôle H de C.
15. Calculer le syndrome du mot reçu 110000000000000 puis corriger ce mot sous l'hypothèse de l'existence d'au plus une erreur.

Université Pierre & Marie Curie — 2004/05

L2 MATHÉMATIQUES — MODULE LM 220

CORRIGÉ DE L'EXAMEN DU 21 JANVIER 2005

Partie I

1. Le polynôme P est irréductible dans $\mathbb{F}_2[X]$ car il n'est divisible ni par X^2+X+1, seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$, ni par un polynôme de degré 1 puisque P n'a pas de racine dans $\mathbb{F}_2$. L'anneau quotient $\mathbb{K}$ est donc un corps.
2. $\mathbb{K}$ est de caractéristique 2 puisque $\mathbb{F}_2 \subset \mathbb{K}$.
   Le système $\{1, \alpha, \alpha^2, \alpha^3\}$ est une base de $\mathbb{K}$, qui est donc de dimension 4 sur $\mathbb{F}_2$.
   Il en résulte que $\mathbb{K}$ possède $2^4 = 16$ éléments.
3. Le groupe multiplicatif $\mathbb{K}^*$ est d'ordre 15, l'ordre de α dans $\mathbb{K}^*$ est donc un diviseur de 15.
   Comme le système $\{1, \alpha, \alpha^2, \alpha^3\}$ est une base de $\mathbb{K}$, on ne peut avoir ni $\alpha = 1$ ni $\alpha^3 = 1$. De plus, comme $\alpha^4 = \alpha + 1$, on a $\alpha^5 = \alpha\,\alpha^4 = \alpha(\alpha+1) = \alpha^2 + \alpha$, et $\alpha^2 + \alpha \neq 1$ pour la même raison. On en déduit que α est d'ordre 15, c'est-à-dire est un élément primitif de $\mathbb{K}$.

Partie II

1. S'il existait un mot de poids 1, il existerait, par définition de u, un entier $k \in \{0, 1, \ldots, 14\}$ tel que $\alpha^k = 0$, ce qui est impossible.
2. S'il existait un mot de poids 2, il existerait deux entiers i et j vérifiant $0 \leq i < j \leq 14$ et $\alpha^j = \alpha^i$, on en déduirait $\alpha^{j-i} = 1$, avec $0 < j - i \leq 14$, et α ne serait pas primitif.
3. Comme $1 + \alpha + \alpha^4 = 0$, le mot $m_0 = 110010000000000$ vérifie $u(m_0) = 1 + \alpha + \alpha^4 = 0$, c'est donc un mot de code, il est de poids 3.
4. $d = 3$ et $t = \left\lfloor \dfrac{3-1}{2} \right\rfloor = 1$.
5. Soit $\{e_1, e_2, \ldots, e_{15}\}$ la base canonique de $(\mathbb{F}_2)^{15}$. Pour chaque entier $k = 1, 2, \ldots, 15$, on a
   $$\alpha^{k-1} = u(e_k) \in \mathrm{Im}\,(u), \text{ donc } \mathbb{K}^* \subset \mathrm{Im}\,(u).$$
   D'autre part $u(0) = 0 \in \mathrm{Im}\,(u)$, donc $\mathbb{K} \subset \mathrm{Im}\,(u)$ d'où $\mathrm{Im}\,(u) = \mathbb{K}$.
   Comme $\mathbb{K}$ est un $\mathbb{F}_2$-espace vectoriel de dimension 4, le théorème du rang appliqué à u s'écrit
   $$\dim(\ker(u)) + \dim(\mathrm{Im}\,(u)) = \dim(\ker(u)) + 4 = 15,$$
   c'est-à-dire que $C = \ker(u)$ est de dimension $15 - 4 = 11$, et possède donc $2^{11} = 2048$ éléments.
6. Dans $(\mathbb{F}_2)^{15}$, une boule de Hamming de rayon 1 possède 16 éléments. Comme $d = 3$, deux telles boules centrées en deux mots de code distincts ont une intersection vide. On en déduit que la réunion des boules de Hamming de rayon 1 centrées en les 2^{11} mots de code possède
   $$2^{11} \times 16 = 2^{11} \times 2^4 = 2^{15} \text{ éléments,}$$
   donc est égale à $(\mathbb{F}_2)^{15}$, ce qui signifie que le code C est parfait.
7. Soit $m = c_0 c_1 \ldots c_{14} \in C$, et soit $m' = c_{14} c_0 c_1 \ldots c_{13}$ le mot obtenu à partir de m par décalage à droite, on a
   $$u(m') = c_{14} + \sum_{k=0}^{13} c_k\,\alpha^{k+1} = \alpha\left[c_0\alpha^{14} + \sum_{k=0}^{13} c_k\,\alpha^k\right] = \alpha\,u(m) = 0, \quad \text{donc } m' \in C.$$
8. La division suivant les puissances décroissantes du polynôme $X^{15} - 1$ par le polynôme P est rapide à effectuer, elle s'écrit
   $$X^{15} - 1 = (X^4 + X + 1)(X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1).$$
9. Le polynôme P est unitaire, de degré $4 = 15 - 11$, il divise le polynôme $X^{15} - 1$, et le mot $m_0 = 110010000000000$ associé à P est un mot de code. Le code engendré par P est donc égal à C.

10. Par définition d'une matrice génératrice du code C, les lignes de G constituent une base de l'espace vectoriel C, lequel est un sous-espace vectoriel de dimension 11 de $(\mathbb{F}_2)^{15}$, c'est-à-dire que G possède 11 lignes et 15 colonnes.
11. Première ligne possible de G : $l_1 = m_0 = 110010000000000$.
12. Il résulte de la question 8 que $h = X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1$.
13. Par définition, une matrice de contrôle H est la matrice (par rapport aux bases canoniques) d'une application linéaire S de $(\mathbb{F}_2)^{15}$ sur $(\mathbb{F}_2)^4$ (dont le noyau $\ker(S)$ est égal à C). On en déduit que H possède 4 lignes et 15 colonnes.
14. Il résulte de la question 12 que
    $$H = \begin{pmatrix} 1&0&0&1&1&0&1&0&1&1&1&1&0&0&0 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \end{pmatrix}.$$
15. Le syndrome du mot 110000000000000 est 1100, 5eme colonne de H. Sous l'hypothèse d'au plus une erreur, le mot émis est donc 110010000000000.

UNIVERSITÉ PIERRE ET MARIE CURIE 9 juin 2005

Examen de Mathématiques LM 220 (durée 2 heures)

Les six exercices sont indépendants. Les documents et calculatrices ne sont pas autorisés.

1. *a*) Quel est le pgcd de 5141 et 2491 ?
   b) Décomposer ces deux nombres en facteurs premiers.
   c) Quel est leur ppcm ?

2. *a*) Trouver des entiers relatifs u et v tels que $35u + 29v = 1$.
   b) Déterminer un entier n tel que $n \equiv 3 \bmod 35$ et $n \equiv 5 \bmod 29$.
   c) Quel est le plus petit entier $n \geq 10000$ satisfaisant ces conditions ?

3. On considère les polynômes $\mathrm{X}^4 - 4$ et $\mathrm{X}^4 + \mathrm{X} - 2$ de $\mathbf{F}_5[\mathrm{X}]$.
   a) Déterminer leurs racines dans $\mathbf{F}_5$.
   b) Quelles sont leurs multiplicités ?
   c) Décomposer ces polynômes en facteurs irréductibles dans $\mathbf{F}_5[\mathrm{X}]$.

4. Posons $\mathrm{K} = \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^4 + \mathrm{X} + 1)$ et notons a la classe de X dans K.
   a) Démontrer que K est un corps. Quelle est sa caractéristique ? Son cardinal ? Expliciter une base de K sur son sous-corps premier.
   b) Soit $\mathrm{F} : x \mapsto x^2$ l'automorphisme de Frobenius de K. Calculer $\mathrm{F}^m(a)$ pour tout $m \geq 1$.
   c) L'élément a engendre-t-il $\mathrm{K}^\times$? Calculer $\log_a(a+1)$.

5. Alice veut envoyer à Bob un message crypté en se servant de l'algorithme RSA. La clé publique de Bob est $(n, e) = (391, 9)$. Le message que veut envoyer Alice est 28.
   a) Quel calcul doit effectuer Alice pour encrypter ce message ?
   b) Effectuer ce calcul.
   c) Quels nombres premiers Bob a-t-il utilisé pour fabriquer sa clé ? Quel est sa clé secrète ?

6. Considérons le code linéaire ayant pour alphabet $\mathbf{F}_5$ et pour matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix}.$$

   a) Quelle est le mot-code correspondant au mot-source 321 ?
   b) Expliciter une matrice de contrôle de ce code. Déterminer la distance minimum et la capacité de correction du code. Le code est-il MDS (Maximum Distance Separable) ?
   c) On reçoit le message 14030. Vérifier qu'il est entaché d'erreurs. En supposant qu'il comporte un seul chiffre erroné, le corriger et retrouver le mot-source dont il provient.

UNIVERSITÉ PIERRE ET MARIE CURIE 9 juin 2005

Corrigé de l'examen de Mathématiques LM 220

1. *a*) L'algorithme d'Euclide donne les restes successifs de divisions euclidiennes

$$5141 \quad 2491 \quad 159 \quad 106 \quad 53$$

(puis 0 car 106 est multiple de 53). Le pgcd de 5141 et 2491 est donc 53.

b) Comme les nombres 53, $\frac{5141}{53} = 97$ et $\frac{2491}{53} = 47$ sont tous premiers, 53×97 et 47×53 sont les décompositions en facteurs premiers de 5141 et 2491.

c) Le ppcm de 5141 et 2491 est $\frac{5141 \times 2491}{53} = 5141 \times 47 = 241627$.

2. *a*) L'algorithme d'Euclide étendu :

(q_n) :		1	4	1	
(d_n) :	35	29	6	5	1
(u_n) :	1	0	1	-4	5
(v_n) :	0	1	-1	5	-6

conduit à $u = 5$, $v = -6$. (Vérification : $5 \times 35 - 6 \times 29 = 175 - 174 = 1$.)

b) On peut prendre $n = 3 \times (-6) \times 29 + 5 \times 5 \times 35 = -522 + 875 = 353$.

c) Les autres entiers n satisfaisant ces conditions sont ceux de la forme $353 + 1015k$. Le plus petit qui soit ≥ 10000 est $353 + 1015 \times 10 = 10503$.

3. *a*) On a $0^4 = 0$ et $x^4 = 1$ pour $x \neq 0$ dans $\mathbf{F}_5$. Le polynôme $X^4 - 4$ n'a donc pas de racine dans $\mathbf{F}_5$, et le polynôme $X^4 + X - 2$ en a une seule, à savoir 1.

b) On a $X^4 + X - 2 = (X-1)(X^3 + X^2 + X + 2) = (X-1)^2(X^2 + 2X + 3)$ dans $\mathbf{F}_5[X]$ et 1 n'est pas racine de $X^2 + 2X + 3$ dans $\mathbf{F}_5$. Donc 1 est racine double de $X^4 + X - 2$.

c) On a $X^4 - 4 = (X^2 - 2)(X^2 + 2)$ et $X^4 + X - 2 = (X-1)^2(X^2 + 2X + 3)$. Ce sont des décompositions en facteurs irréductibles : en effet les facteurs de degré 2 intervenant dans ces expressions n'ont pas de racines dans $\mathbf{F}_5$.

4. *a*) Tout polynôme irréductible de degré ≤ 2 de $\mathbf{F}_2[X]$ divise $X^4 - X$, *i.e.* $X^4 + X$, donc ne divise pas $X^4 + X + 1$. Par suite $X^4 + X + 1$ est irréductible dans $\mathbf{F}_2[X]$ et K est un corps. Sa caractéristique est 2. Son cardinal est $2^4 = 16$. Une base de K sur $\mathbf{F}_2$ est $1, a, a^2, a^3$.

b) On a $F(a) = a^2$, $F^2(a) = a^4 = a + 1$, $F^3(a) = a^2 + 1$, $F^4(a) = a^4 + 1 = a$. Par suite, $F^m(a)$ est égal à a, a^2, $a + 1$, $a^2 + 1$ suivant que m est congru à 0, 1, 2 ou 3 modulo 4.

c) Le groupe $K^\times$ est d'ordre $16 - 1 = 15$. On a $a^3 \neq 1$ et $a^5 = a^2 + a \neq 1$, donc a engendre $K^\times$. Comme $a + 1 = a^4$, $\log_a(a + 1)$ est la classe de 4 modulo 15.

5. *a*) Alice doit calculer le reste de la division euclidienne de 28^9 par 391.

b) Dans $\mathbf{Z}/391\mathbf{Z}$, on a $\overline{28}^2 = \overline{784} = \overline{2}$, $\overline{28}^4 = \overline{4}$, $\overline{28}^8 = \overline{16}$, $\overline{28}^9 = \overline{28} \times \overline{16} = \overline{448} = \overline{57}$. Le message encrypté est donc 57.

c) Les nombres premiers utilisés par Bob sont 17 et 23 car $391 = 17 \times 23$. On a $\varphi(391) = 16 \times 22 = 352$. La clé secrète d de Bob est l'inverse de 9 modulo 352. Comme $352 = 9 \times 39 + 1$, d est l'opposé de 39 modulo 352, c'est-à-dire 313.

6. *a*) Le mot-code correspondant au mot-source 321 est 32110 car

$$(3 \quad 2 \quad 1) \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix} = (3 \quad 2 \quad 1 \quad 1 \quad 0).$$

b) Une matrice de contrôle du code est $H = \begin{pmatrix} -1 & -1 \\ -1 & -2 \\ -1 & -3 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 4 \\ 4 & 3 \\ 4 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Les lignes de cette matrice sont deux à deux non proportionnelles ; par contre trois quelconques d'entre elles sont linéairement dépendantes. La distance minimum du code est donc $d = 3$. La capacité de correction du code est $t = [\frac{d-1}{2}] = 1$. La dimension du code est $k = 3$ et sa longueur est $n = 5$. On a $d + k = n + 1$, donc le code est MDS.

c) On a $(1 \quad 4 \quad 0 \quad 3 \quad 0)H = (3 \quad 1) \neq (0 \quad 0)$, donc le message est entaché d'erreurs. Le symptôme de l'erreur est $(3 \quad 1)$, qui est le double de la deuxième ligne de H. L'erreur commise est donc 02000, le message corrigé est 12030 et le mot-source dont il provient 120.

Université Pierre et Marie Curie — Jeudi 15 septembre 2005

Examen de Mathématiques LM220

(durée 2 heures)

Les documents et calculatrices ne sont pas autorisés. Les téléphones portables doivent être maintenus éteints.

Les exercices sont indépendants. Les réponses doivent être soigneusement justifiées.

1. On considère le code linéaire sur $\mathbb{F}_2$ ayant pour matrice de génératrice :

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

   (a) Quelle est la longueur du code ? Quelle est sa dimension ?

   (b) Donner une matrice de contrôle du code. Quelle est sa distance minimale et sa capacité de correction ?

   (c) Le code est-il MDS (Minimum Distance Separable) ? Le code est-il parfait ?

   (d) Encoder le mot source 1001.

   (e) Vérifier que le mot 1111000 n'est pas un mot de code. Trouver le mot de code le plus proche. Quel est le mot source ?

2. Soit $P = X^7 + X + 1 \in \mathbb{F}_2[X]$, $A = \mathbb{F}_2[X]/(P)$ et α la classe de X dans A.

   (a) Expliciter une base de A sur $\mathbb{F}_2$. Quel est le cardinal de A ?

   (b) Montrer que α est un élément inversible de A. Quel est son inverse ?

   (c) Soit $F : A \to A$ tel que $F(x) = x^2$. Exprimer $F^m(\alpha)$, pour $1 \leq m \leq 6$, comme combinaison linéaire de $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. Montrer que $F^7(\alpha) = \alpha$.

   (d) Quel est le plus petit entier $n \geq 1$ tel que $\alpha^n = 1$?

   (e) Montrer que A est un corps. Que peut-on en déduire sur le polynôme P ?

   (f) Montrer que α et $\alpha + 1$ sont des générateurs de A^*. Quels sont les plus petits entier $d \geq 0$ et $e \geq 0$ tels que $\alpha + 1 = \alpha^d$ et $\alpha = (\alpha + 1)^e$.

3. Bob reçoit d'Alice un message qu'elle a encrypté en se servant de l'algorithme RSA. La clef publique de Bob est $(n, e) = (667, 493)$. Le message crypté qu'il reçoit est 24.

   (a) Quels nombres premiers Bob a-t-il utilisé pour fabriquer sa clef ? Quelle est sa clef secrète ?

   (b) Quel calcul doit effectuer Bob pour décrypter le message ?

   (c) Effectuer ce calcul. Quel est le message qu'Alice a envoyé ?

Université Pierre et Marie Curie — Jeudi 15 septembre 2005

Corrigé de l'examen de Mathématiques LM220

1. On considère le code linéaire sur $\mathbb{F}_2$ ayant pour matrice de génératrice :

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

   (a) Quelle est la longueur du code ? Quelle est sa dimension ?
   Réponse : Longueur : $n = 7$. Dimension : $k = 4$.

   (b) Donner une matrice de contrôle du code. Quelle est sa distance minimale et sa capacité de correction ?
   Réponse : Matrice de contrôle : $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$
   Distance minimale : $d = 3$. Capacité de correction : $t = 1$.

   (c) Le code est-il MDS (Minimum Distance Separable) ? Le code est-il parfait ?
   Réponse : On a $n - k + 1 = 4 \neq d$ donc le code n'est pas MDS. Les boules de rayon t ont pour cardinal $1 + C_7^1 = 8 = 2^{n-k}$ donc le code est parfait.

   (d) Encoder le mot source 1001.
   Réponse : $1001 \times G = 1001001$.

   (e) Vérifier que le mot 1111000 n'est pas un mot de code. Trouver le mot de code le plus proche. Quel est le mot source ?
   Réponse : $H \times \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \neq 0$ donc 1111000 n'est pas un mot de code.
   Son syndrôme est la première colonne de H. Il est donc a distance 1 du mot de code 0111000 (qui est l'unique mot le plus proche car $t = 1$). Le mot source est 0111.

2. Soit $P = X^7 + X + 1 \in \mathbb{F}_2[X]$, $A = \mathbb{F}_2[X]/(P)$ et α la classe de X dans A.

   (a) Expliciter une base de A sur $\mathbb{F}_2$. Quel est le cardinal de A ?
   Réponse : $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$ est une base de A sur $\mathbb{F}_2$. $|A| = 2^7 = 128$.

   (b) Montrer que α est un élément inversible de A. Quel est son inverse ?
   Réponse : On a $\alpha(\alpha^6 + 1) = 1$ donc α est inversible et son inverse est $\alpha^6 + 1$.

   (c) Soit $F : A \to A$ tel que $F(x) = x^2$. Exprimer $F^m(\alpha)$, pour $1 \leq m \leq 6$, comme combinaison linéaire de $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. Montrer que $F^7(\alpha) = \alpha$.
   Réponse : $F(\alpha) = \alpha^2$, $F^2(\alpha) = \alpha^4$, $F^3(\alpha) = \alpha^8 = \alpha^2 + \alpha$,
   $F^4(\alpha) = (\alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2$, $F^5(\alpha) = (\alpha^4 + \alpha^2)^2 = \alpha^8 + \alpha^4 = \alpha^4 + \alpha^2 + \alpha$,
   $F^6(\alpha) = (\alpha^4 + \alpha^2 + \alpha)^2 = \alpha^8 + \alpha^4 + \alpha^2 = \alpha^4 + \alpha$, $F^7(\alpha) = (\alpha^4 + \alpha)^2 = \alpha^8 + \alpha^2 = \alpha$.

   (d) Quel est le plus petit entier $n \geq 1$ tel que $\alpha^n = 1$?
   Réponse : De la question précédente on déduit que $\alpha^{128} = \alpha$, or α est inversible donc $\alpha^{127} = 1$. On en déduit que n est un diviseur de 127 qui est un nombre premier. De plus $n \neq 1$ car $\alpha \neq 1$ donc $n = 127$.

   (e) Montrer que A est un corps. Que peut-on en déduire sur le polynôme P ?
   Réponse : De la question précédente on déduit que $1, \alpha, \alpha^2, \ldots, \alpha^{126}$ sont tous distincts (sinon on aurait $n < 127$). Il y a donc au moins 127 éléments inversibles dans A, donc tous les éléments non nuls de A sont inversibles. A est donc un corps. On en déduit que P est irréductible.

   (f) Montrer que α et $\alpha + 1$ sont des générateurs de A^*. Quels sont les plus petits entier $d \geq 0$ et $e \geq 0$ tels que $\alpha + 1 = \alpha^d$ et $\alpha = (\alpha + 1)^e$.
   Réponse : 127 est premier donc tous les éléments de $K^* \setminus \{1\}$ sont d'ordre 127, donc sont des générateurs de K^*. Il en est donc ainsi de α et $\alpha + 1$.
   On a $\alpha + 1 = \alpha^7$ donc $d \leq 7$. De plus $\alpha^{7-d} = 1$ et $0 \leq 7 - d < 127$ donc $7 - d = 0$ car α est d'ordre 127, d'où $d = 7$.
   On a $127 = 7 \times 18 + 1$ donc l'inverse de 7 modulo 127 est $-18 \equiv 109 \pmod{127}$.
   On en déduit que $(\alpha + 1)^{109} = \alpha^{7 \times 109} = \alpha^{-7 \times 18} = \alpha^{127 - 7 \times 18} = \alpha$ (car $\alpha^{127} = 1$).
   D'où $e \leq 109$. De plus $(\alpha + 1)^{109-e} = 1$ et $0 \leq 109 - e < 127$ donc $109 - e = 0$ car $\alpha + 1$ est d'ordre 127, d'où $e = 109$.

3. Bob reçoit d'Alice un message qu'elle a encrypté en se servant de l'algorithme RSA. La clef publique de Bob est $(n, e) = (667, 493)$. Le message crypté qu'il reçoit est 24.

   (a) Quels nombres premiers Bob a-t-il utilisé pour fabriquer sa clef ? Quelle est sa clef secrète ?
   Réponse : $667 = 23 \times 29$. Les nombres premiers sont $p = 23$ et $q = 29$. La clef secrète de Bob est (pq, d) où d est l'inverse de e modulo $(p - 1)(q - 1)$. On écrit l'algorithme d'Euclide étendu, pour les entiers $(p - 1)(q - 1) = 616$ et $e = 493$; on obtient le tableau suivant dans lequel on a $r_{i-1} = q_i r_i + r_{i+1}$ (division euclidienne) et $v_{i+1} = v_{i-1} - q_i v_i$:

r_i	616	493	123	1
q_i	–	1	4	–
v_i	0	1	-1	5

   On en déduit que l'inverse de 493 modulo 616 est 5.
   La clef secrète de Bob est donc $(667, 5)$.

   (b) Quel calcul doit effectuer Bob pour décrypter le message ?
   Réponse : Le message d'Alice est $24^5 \pmod{667}$.

   (c) Effectuer ce calcul. Quel est le message qu'Alice a envoyé ?
   Réponse : On a : $24^2 = 676 \equiv 9 \pmod{667}$,
   $24^4 \equiv 9^2 \equiv 81 \pmod{667}$,
   $24^5 \equiv 81 \times 24 \equiv 1944 \equiv 610 \pmod{667}$.
   Le message qu'Alice a envoyé est 610.