# Feuille d'exercices 4

*Avertissement* : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum*.

***Exercice 1.*** — ***(Cryptosystème de Massey-Omura)*** *Alice souhaite envoyer un message à Bob codé par un élément $m$ d'un groupe cyclique $G$ d'ordre $n$. Ils utilisent le cryptosystème (sans clé) suivant :*

1. *Alice choisit secrètement un entier $x_A$ tel que $1 < x_A < n$ et $x_A \wedge n = 1$, et elle envoie à Bob l'élément $a = m^{x_A}$.*
2. *Bob choisit secrètement un entier $x_B$ tel que $1 < x_B < n$ et $x_B \wedge n = 1$, et il renvoie à Alice l'élément $b = a^{x_B}$.*
3. *Alice calcule l'entier $y_A$ tel que $1 < y_A < n$ et $x_A y_A \equiv 1 \mod n$, et elle renvoie à Bob l'élément $c = b^{y_A}$.*
4. *Bob calcule l'entier $y_B$ tel que $1 < y_B < n$ et $x_B y_B \equiv 1 \mod n$, et détermine $c^{y_B}$.*
   (a) *Montrer que l'on a $m = c^{y_B}$.*
   (b) *On prend $G = \mathbb{F}_{19}^*$. Supposons qu'Alice choisisse l'entier $x_A = 5$ et qu'elle envoie à Bob $a = \overline{2}$. Trouver l'élément $m$ correspondant.*

***Exercice 2.*** — ***(Système RSA)*** *Soit $n$ un entier $\geq 1$. Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés par des éléments de $\mathbb{Z}/n\mathbb{Z}$. Soit $(e, n)$ sa clé publique.*

1. *Déterminer sa clé secrète dans chacun des cas suivants :*
$$(e, n) \in \Big\{(5, 35), (139, 265), (31, 3599)\Big\}.$$
2. *Avec $(e, n) = (31, 3599)$, elle reçoit le cryptogramme $2 + n\mathbb{Z}$. Quel est le message envoyé ? Soient $p$ et $q$ deux nombres premiers distincts congrus à 2 modulo 3. Posons*
$$n = pq \quad et \quad e = \frac{2(p-1)(q-1)+1}{3} \quad (e \text{ est un entier}).$$
3. *Montrer que $e$ est premier avec $\varphi(n)$ et calculer son inverse modulo $\varphi(n)$.*
4. *Alice choisit comme clé publique le couple $(e, n) = (107, 187)$. Elle reçoit le cryptogramme $9 + n\mathbb{Z}$. Quel est le message envoyé ?*

***Exercice 3.*** — ***(Protocole de Diffie-Hellman)*** *Alice et Bob décident d'utiliser ce protocole pour se fabriquer une clé secrète. Pour cela, ils rendent public le couple $(K, \alpha)$ où*
$$K = \mathbb{F}_3[X]/(X^3 + 2X + 1) \quad et \quad \alpha = X + (X^3 + 2X + 1).$$

1. *Vérifier que $K$ est un corps et que $\alpha$ est un générateur de $K^*$. Conformément à ce protocole, Alice choisit un entier $a$ compris entre 2 et 25, par exemple $a = 9$, et transmet $\alpha^9$ à Bob. Ce dernier choisit un entier $b$ compris entre 2 et 25 et lui renvoie l'élément $\alpha^b = 2 + \alpha + 2\alpha^2$.*
2. *Quelle est la clé secrète d'Alice et Bob ? On déterminera ses coordonnées dans la base $(1, \alpha, \alpha^2)$ de $K$ sur $\mathbb{F}_3$.*

***Exercice 4.*** — ***(Algorithme de El Gamal)*** *Alice souhaite se faire envoyer des messages confidentiellement en utilisant cet algorithme. Elle considère pour cela le corps*
$$K = \mathbb{F}_2[X]/(X^4 + X + 1).$$
*Soit $\alpha$ la classe de $X$ modulo $(X^4 + X + 1)$.*

1. *Justifier que $K$ est un corps et montrer que $\alpha$ est un générateur de $K^*$. Alice rend public le triplet $(K, \alpha, \alpha^2 + 1)$, et Bob envoie des messages à Alice en utilisant cette clé publique.*
2. *Bob veut coder le message $1 + \alpha$ pour l'envoyer à Alice. Conformément à l'algorithme, il choisit un entier $x$ compris entre 2 et 14, par exemple $x = 3$. Que transmet-il à Alice ?*
3. *Vous interceptez le message $(\alpha^3, \alpha^3 + \alpha^2 + \alpha)$. Quel était le message envoyé par Bob ?*

***Exercice 5***. — ***(Sac à dos)***

1. *Pour les suites d'entiers et* $\ll$ *volumes* $\gg$ $V$ *suivants, résoudre le problème du sac à dos correspondant :*
$$(2,3,7,20,35,69) \text{ et } V=45, \quad (1,2,5,9,20,49) \text{ et } V=73,$$
$$(1,3,7,12,22,45) \text{ et } V=67, \quad (4,5,10,30,50,101) \text{ et } V=186.$$
2. *Soit* $(v_i)_{i\geq 0}$ *une suite d'entiers positifs telle que l'on ait* $v_{i+1} > 2v_i$ *pour tout* $i$. *Montrer qu'elle est super croissante.*
3. *Montrer que la suite d'entiers strictement positifs super croissante dont chaque terme est le plus petit possible est la suite* $(2^i)_{i\geq 0}$.

***Exercice 6***. — ***(Sac à dos de Merkle-Hellman)*** *Alice et Bob utilisent le cryptosystème du sac à dos de Merkle-Hellman pour communiquer. L'alphabet utilisé est l'alphabet usuel, chaque lettre étant codée par un entier écrit en binaire avec cinq composantes* $(\varepsilon_4\varepsilon_3\varepsilon_2\varepsilon_1\varepsilon_0)_2$ *(on a* $A{=}(00000)_2$, $\cdots$, $Z{=}(11001)_2$*). Les unités de message sont des mots de trois lettres (ils ont donc quinze composantes). Les notations étant celles figurant dans le paragraphe 7 du chapitre IV du cours, Alice choisit la suite d'entiers* $(4,5,12,23,45)$, *ainsi que* $m=400$ *et* $a=381$.

1. *Vérifier que ces données sont conformes au principe d'utilisation de ce cryptosystème.*
2. *Déterminer la clé publique d'Alice.*
3. *Bob veut envoyer à Alice le message OUI. Indiquer le procédé qu'il doit suivre et comment Alice retrouve-t-elle le message.*

***Exercice 7***. — *Soit* $p$ *un nombre premier de Mersenne : on a* $p=2^\ell-1$ *où* $\ell$ *est premier. Posons*
$$K=\mathbb{F}_p[X]/(X^2+1).$$
*Notons* $i$ *la classe de* $X$ *modulo* $(X^2+1)$.

1. *Montrer que* $K$ *est* $\ll$ *le* $\gg$ *corps à* $p^2$ *éléments.*
2. *Soient* $a$ *et* $b$ *deux éléments de* $\mathbb{F}_p$ *tels que* $a^2+b^2$ *soit un générateur de* $\mathbb{F}_p^*$ *(cette hypothèse n'est pas restrictive car tout élément de* $\mathbb{F}_p$ *est somme de deux carrés). Montrer que* $a+ib$ *est un générateur de* $K^*$.
3. *En déduire que* $4+i$ *et* $3+2i$ *sont des générateurs du groupe* $\mathbb{F}_{31^2}^*$.
4. *Deux personnes Alice et Bob souhaitent se construire une clé de chiffrement commune en utilisant le protocole de Diffie-Hellman dans le groupe* $\mathbb{F}_{31^2}^*$, *avec le générateur* $4+i$.
   (a) *Alice choisit secrètement l'entier* 193 *et Bob envoie à Alice l'élément* $1+19i$. *Quelle est la clé commune de chiffrement ?*
   (b) *Quel élément de* $K^*$ *doit envoyer Alice à Bob pour qu'il connaisse la clé ?*

## 1. Solutions

**1** 1) On a les égalités

$$c^{y_B} = \big(b^{y_A}\big)^{y_B} = \big(a^{x_B y_A}\big)^{y_B} = \big(m^{x_A y_A}\big)^{x_B y_B}$$

Il existe deux entiers naturels $u$ et $v$ tels que l'on ait $x_A y_A = 1 + un$ et $x_B y_B = 1 + vn$. Soit $e$ l'élément neutre de $G$. Puisque $G$ est d'ordre $n$, on a $m^{un} = m^{vn} = e$. Par suite, on obtient

$$c^{y_B} = \big(m^{1+un}\big)^{1+vn} = m.$$

2) On a dans cet exemple $n = 18$. Supposons que Bob choisisse l'élément $x_B = 7$. Dans ce cas, il renvoie à Alice l'élément $b = \overline{2}^7 = 14 \mod 19$. On vérifie que l'on a $y_A = 11$ car on a $5 \times (-7) + 18 \times 2 = 1$. Alice renvoie ainsi à Bob l'élément $c = \overline{14}^{11}$. Par ailleurs, vu l'égalité $7 \times 13 - 5 \times 18 = 1$, on a $y_B = 13$. Ainsi Bob effectue l'opération $(14^{11})^{13}$ modulo 19. On a $11 \times 13 \equiv 17 \mod 18$. D'après le petit théorème de Fermat, on a donc

$$(14^{11})^{13} \equiv 14^{17} \mod 19.$$

On en déduit que l'on a $m = 14^{-1} \mod 19 = 15 \mod 19$ (on a $-4 \times 14 + 3 \times 19 = 1$) i.e. $m = \overline{15} \in \mathbb{F}_{19}^*$.

**2** 1) On a $35 = 5 \times 7$ et $\varphi(n) = 24$. Par ailleurs, on a $1 = 5 \times 5 - 24$, donc 5 est son propre inverse modulo 24. Dans ce cas, la clé secrète est donc $(5, 24)$.

On a $265 = 5 \times 53$ et $\varphi(n) = 208$. Il s'agit de déterminer l'inverse de 139 modulo 208. On peut utiliser pour cela l'algorithme d'Euclide, ce qui conduit à l'égalité $1 = 3 \times 139 - 2 \times 208$. La clé secrète est donc $(3, 208)$.

On a $3599 = 59 \times 61$, d'où $\varphi(n) = 3480$. En utilisant l'algorithme d'Euclide, on obtient directement l'égalité

$$4 \times 3480 - 449 \times 31 = 1,$$

de sorte que l'inverse de 31 modulo 3480 est 3031. La clé secrète est ainsi $(3031, 3480)$. 2) Le message $m$ envoyé est $(2 + n\mathbb{Z})^{3031}$. Afin de déterminer son représentant compris entre 1 et $n$, on procède comme suit. On remarque que l'on a $3031 = 7 \times 433$. On a $59 \equiv 3 \mod 8$, donc 2 n'est pas un carré modulo 59, d'où $2^{29} \equiv -1 \mod 59$ (critère d'Euler). On en déduit que l'on a

$$2^{433} \equiv 2^{27} = -4^{-1} \equiv 44 \mod 59 \quad \text{et} \quad \big(2^{433}\big)^7 \equiv 44^7 \equiv 23 \mod 59.$$

Par ailleurs, on a

$$2^{433} \equiv 2^{13} \equiv 18 \mod 61 \quad \text{et} \quad \big(2^{433}\big)^7 \equiv 18^7 \equiv -2 \mod 61.$$

On est donc amené à chercher l'entier $N$ tel que $1 \leq N \leq 3599$ vérifiant les congruences

$$N \equiv 23 \mod 59 \quad \text{et} \quad N \equiv -2 \mod 61. \tag{1}$$

On utilise pour cela l'algorithme donné par le théorème chinois. On a la relation de Bézout

$$30 \times 59 - 29 \times 61 = 1,$$

d'où l'on déduit que l'entier $-2\big(30 \times 59\big) - 23\big(29 \times 61\big) = -44227$ vérifie les congruences (1). Il en résulte que $N = 2560$. Le message $m$ envoyé est donc

$$m = 2560 + n\mathbb{Z}.$$

3) On a $\varphi(n) = (p-1)(q-1)$ i.e. on a $3e = 2\varphi(n) + 1$, donc $e$ est premier avec $\varphi(n)$ et 3 est l'inverse de $e$ modulo $\varphi(n)$. 4) On a $n = 11 \times 17$, $\varphi(n) = 160$. D'après la question 3, l'inverse de 107 modulo 160 est 3. Le message $m$ qui lui a été envoyé est donc

$$m = 9^3 \mod 187 = 168 \mod 187.$$

**3** 1) Le polynôme $X^3 + 2X + 1 \in \mathbb{F}_3[X]$ est irréductible sur $\mathbb{F}_3$ car il n'a pas de racines dans $\mathbb{F}_3$ et son degré est 3, donc $K$ est un corps de cardinal 27. Le groupe $K^*$ est d'ordre 26. Les ordres de ses éléments autres que l'élément neutre, sont donc 2, 13 ou 26. En fait, $-1$ est le seul élément d'ordre 2 de $K^*$, car par exemple $\pm 1$ sont les seules racines du polynôme $X^2 - 1 \in K[X]$. On a $\alpha^3 = \alpha - 1$, d'où $\alpha^9 = \alpha^3 - 1$ (car $K$ est de caractéristique 3) i.e. $\alpha^9 = \alpha + 1$, d'où $\alpha^{12} = \alpha^2 - 1$ puis $\alpha^{13} = -1$ et notre assertion. 2) On a $\alpha^4 = \alpha^2 - \alpha$ et $\alpha^5 = 2\alpha^2 + \alpha + 2$, d'où $b = 5$. La clé secrète d'Alice et Bob est donc $\big(\alpha^9\big)^5 = \alpha^{45}$. Déterminons ses coordonnées dans la base $(1, \alpha, \alpha^2)$ de $K$ sur $\mathbb{F}_3$. On a $\alpha^{26} = 1$, d'où $\alpha^{45} = \alpha^{19} = \alpha^{-7}$. Par ailleurs, on a $\alpha^6 = \alpha^2 + \alpha + 1$, d'où $\alpha^7 = \alpha^2 - \alpha - 1$. De l'égalité

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

on déduit alors que l'on a

$$\alpha^{45} = -(\alpha^2 + \alpha + 1).$$

**4** 1) Le polynôme $X^4 + X + 1 \in \mathbb{F}_2[X]$ n'a pas de racines dans $\mathbb{F}_2$ et n'est pas divisible par $X^2 + X = 1$ qui est le seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$, donc $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ et $K$ est un corps. Le groupe $K^*$ est d'ordre 15. On a $\alpha^4 = \alpha + 1$, d'où l'on déduit que $\alpha^3$ et $\alpha^5$ sont distincts de 1, ce qui entraîne que l'ordre de $\alpha$ dans $K^*$ est 15. 2) Il transmet le couple $\big(\alpha^3, (1+\alpha)(1+\alpha^2)^3\big)$ i.e. $\big(\alpha^3, \alpha^3 + \alpha^2 + 1\big)$. 3) On cherche l'entier $a$ tel que $1 \leq a \leq 14$ et que $1 + \alpha^2 = \alpha^a$. 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 $1 + \alpha^2 = \alpha^8$ i.e. on a $a = 8$. On a

$$\alpha^{xa} = \alpha^{24} = \alpha^9.$$

Par définition, si $m$ est le message envoyé par Bob, on a

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

L'inverse de $\alpha^{ax}$ i.e. de $\alpha^9$ est $\big(\alpha^9\big)^{14} = \alpha^{126} = \alpha^{8\times 15+6} = \alpha^6$, autrement dit, on a

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

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

**5** Soient $k$ un entier $\geq 1$ et $(v_i)_{0\leq i\leq k-1}$ une suite d'entiers super croissante. Rappelons que par définition on a

$$0 < v_0 < v_1 < \cdots < v_{k-1} \quad \text{et} \quad v_i > \sum_{j=0}^{i-1} v_j \quad \text{pour tout } i \text{ tel que } 0 \leq i \leq k-1. \tag{1}$$

Pour tout entier naturel $V$ (le volume), le problème du sac à dos relatif à $V$ et à une telle suite $(v_i)$ est facile à résoudre. Il s'agit de déterminer des entiers $a_i$ égaux à 0 ou 1, s'ils existent, tels que l'on ait

$$V = \sum_{i=0}^{k-1} a_i v_i.$$

Il existe au plus une solution. Pour résoudre ce problème, on utilise l'algorithme décrit dans l'alinéa 2 du paragraphe 6 du chapitre IV. 1) La suite $(2, 3, 7, 20, 35, 69)$ est super croissante et $n = (010110)_2$ est la solution (qui correspond à l'égalité $45 = 35 + 7 + 3$). Il en est de même de la suite $(1, 2, 5, 9, 20, 49)$. On constate qu'avec l'entier $V = 73$ le problème n'a pas de solution.
La suite $(1, 3, 7, 12, 22, 45)$ n'est pas super croissante. Dans ce cas, il y a exactement deux solutions $(110000)_2$ et $(101110)_2$.
La suite $(4, 5, 10, 30, 50, 101)$ est super croissante et l'on trouve la solution $(111010)_2$. 2) Il s'agit de démontrer que la suite (infinie) $(v_i)$ satisfait la condition (1). On a $v_1 > v_0$. Si pour $i \geq 1$, $v_i$ est plus grand que la somme des $i$ premiers termes, on a les inégalités

$$v_{i+1} > 2v_i > \sum_{j=0}^{i} v_j,$$

d'où le résultat par récurrence. 3) On vérifie d'abord que la suite $(2^i)_{i\geq 0}$ est super croissante. Par ailleurs, soit $(a_i)_{i\geq 0}$ la suite super croissante telle que pour tout $i$ le terme $a_i$ soit le plus petit possible. Remarquons que cette suite existe. En effet, on prend $a_0 = 1$ et pour tout $i \geq 1$, $a_i$ est le plus petit entier naturel vérifiant la condition

$$0 < a_0 < \cdots < a_{i-1} < a_i \quad \text{et} \quad a_i > \sum_{j=0}^{i-1} a_j.$$

Vérifions que l'on a $a_i = 2^i$. C'est vrai si $i = 0$. Soit $i$ un entier $\geq 0$. Supposons que l'on ait $a_j = 2^j$ pour tout $j$ tel que $0 \leq j \leq i$. On a alors

$$a_{i+1} > \sum_{j=0}^{i} 2^j = 2^{i+1} - 1.$$

Par suite, le plus petit entier $a_{i+1}$ possible est $2^{i+1}$, d'où l'assertion.

**6** Rappelons d'abord le principe de ce cryptosystème (paragraphe 7 du chapitre IV). Chaque utilisateur choisit une suite d'entiers super croissante $(v_0, v_1, \cdots, v_{k-1})$, un entier $m$ tel que

$$m > \sum_{i=0}^{k-1} v_i, \tag{1}$$

et un entier $a$ tel que $1 \leq a < m$ et $\text{pgcd}(a, m) = 1$. Il détermine ensuite l'entier $b$ tel que

$$1 \leq b < m \quad \text{et} \quad ab \equiv 1 \mod m,$$

et pour tout $i = 0, \cdots, k-1$, l'entier $w_i$ tel que

$$1 \leq w_i < m \quad \text{et} \quad w_i \equiv av_i \mod m. \tag{2}$$

Il garde secret les entiers $v_i$, $m$, $a$ et $b$. Sa clé publique est la suite $(w_0, \cdots, w_{k-1})$. Une personne souhaitant lui envoyer un message binaire $P = (\varepsilon_{k-1} \cdots \varepsilon_0)_2$, lui transmet l'entier

$$C = \sum_{i=0}^{k-1} \varepsilon_i w_i.$$

Afin de décrypter ce message, l'utilisateur calcule l'entier $V$ tel que

$$0 \leq V < m \quad \text{et} \quad V \equiv bC \mod m.$$

L'égalité

$$V = \sum_{i=0}^{k-1} \varepsilon_i v_i, \tag{3}$$

et l'algorithme du sac à dos super croissant, appliqué avec la suite $(v_0, v_1, \cdots, v_{k-1})$, lui permet alors de retrouver le message $P$.

1) On vérifie que la suite $(v_0, v_1, v_2, v_3, v_4) = (4, 5, 12, 23, 45)$ est super croissante, que l'on a $a = 381 = 3 \times 127$, puis

$$m = 400 > \sum_{i=0}^{4} v_i = 89 \quad \text{et} \quad \text{pgcd}(381, 400) = 1.$$

Les données proposées sont donc conformes au principe d'utilisation du cryptosystème. 2) On détermine l'entier $b$ tel que $1 \leq b < 400$ et $381b \equiv 1 \mod 400$. Ë l'aide de l'algorithme d'Euclide, on trouve que l'on a $b = 21$. Il s'agit ensuite de déterminer les entiers $w_i$ définis par l'égalité (2) ci-dessus. On vérifie alors que la clé publique d'Alice est

$$(w_0, w_1, w_2, w_3, w_4) = (324, 305, 172, 363, 345).$$

3) On vérifie que l'on a

$$O = (01110)_2, \quad U = (10100)_2, \quad I = (01000)_2.$$

Pour chacun des trois messages $(\varepsilon_4\varepsilon_3\varepsilon_2\varepsilon_1\varepsilon_0)_2$ ci-dessus à envoyer, Bob transmet donc à Alice successivement le message

$$\sum_{i=0}^{4} \varepsilon_i w_i.$$

Il transmet ainsi les messages cryptés

$$C_1 = 363 + 172 + 305 = 840, \quad C_2 = 345 + 172 = 517, \quad C_3 = 363.$$

Afin de retrouver le mot OUI, Alice calcule les trois entiers $V_i$ tels que

$$0 \leq V_i < 400 \quad \text{et} \quad V_i \equiv 21C_i \mod 400.$$

On trouve

$$V_1 = 40, \quad V_2 = 57, \quad V_3 = 23.$$

Les égalités (3) qui correspondent à chacun des $V_i$ sont respectivement

$$40 = 23 + 12 + 5, \quad 57 = 45 + 12, \quad 23 = 23,$$

et Alice peut alors retrouver le mot OUI.

**7** 1) On a $p \equiv 3 \mod 4$, donc $-1$ n'est pas un carré dans $\mathbb{F}_p$ i.e. $X^2+1$ est irréductible dans $\mathbb{F}_p[X]$. Il en résulte que $K$ est un corps à $p^2$ éléments (qui est unique à isomorphisme près). 2) Soit $m$ un entier $\geq 1$. Démontrons que l'on a l'implication

$$(a+ib)^m \in \mathbb{F}_p \Longrightarrow p+1 \text{ divise } m. \tag{1}$$

Soit $d$ le pgcd de $m$ et $p+1$. Il existe $u$ et $v \in \mathbb{Z}$ tels que $d = um + v(p+1)$. Puisque $K^*$ est d'ordre $p^2-1$, on a $\big((a+ib)^{p+1}\big)^{p-1} = 1$, donc $(a+ib)^{p+1}$ appartient $\mathbb{F}_p$. Il résulte que l'on a

$$\big((a+ib)^m\big)^u\big((a+ib)^{p+1}\big)^v = (a+ib)^d \in \mathbb{F}_p. \tag{2}$$

Vérifions alors que l'on a $d = p+1$. Supposons le contraire. Puisque $p+1$ est une puissance de 2, $d$ divise alors $\frac{p+1}{2}$. D'après (2), on en déduit que

$$(a+ib)^{\frac{p+1}{2}} \in \mathbb{F}_p.$$

Par ailleurs, le carré de cet élément est $a^2+b^2$. En effet, $p$ étant congru à 3 modulo 4, on a $i^p = -i$, et vu que l'on a $a^p = a$ et $b^p = b$, on obtient

$$(a+ib)^{p+1} = (a+ib)^p(a+ib) = (a^p + b^p i^p)(a+ib) = (a-ib)(a+ib) = a^2+b^2.$$

Cela conduit à une contradiction, car $a^2+b^2$ étant un générateur de $\mathbb{F}_p^*$, ce n'est pas un carré dans $\mathbb{F}_p$ (un carré est d'ordre divisant $\frac{p-1}{2}$). On a donc $d = p+1$, par suite $p+1$ divise $m$. Cela prouve l'implication (1). Considérons alors un entier $n \geq 1$ tel que

$$(a+ib)^n = 1.$$

D'après (1), $p+1$ divise $n$. Soit $r \in \mathbb{Z}$ tel que $n = (p+1)r$. L'égalité $(a+ib)^{p+1} = a^2+b^2$ entraîne alors

$$(a^2+b^2)^r = 1.$$

Puisque $a^2+b^2$ est un générateur de $\mathbb{F}_p^*$, $p-1$ divise $r$, donc $p^2-1$ divise $n$. Ainsi $a+ib$ est d'ordre $p^2-1$, d'où le résultat. 3) Il s'agit de démontrer que 13 et 17 sont des générateurs de $\mathbb{F}_{31}^*$. Démontrons que tel est bien le cas pour 13, l'argument pour 17 est analogue. On a (critère d'Euler)

$$13^{15} \equiv \Big(\frac{13}{31}\Big) \mod 31.$$

Par ailleurs, on a

$$\Big(\frac{13}{31}\Big) = \Big(\frac{31}{13}\Big) = \Big(\frac{5}{13}\Big) = \Big(\frac{13}{5}\Big) = \Big(\frac{3}{5}\Big) = -1,$$

d'où la congruence

$$13^{15} \equiv -1 \mod 31,$$

ce qui entraîne l'assertion (le fait que 13 ne soit pas d'ordre 6 ni d'ordre 10 modulo 31 résulte alors des congruences $13^2 \equiv 14 \mod 31$ et $13^3 \equiv -4 \mod 31$). 4.1) Conformément au protocole de Diffie-Hellman, la clé commune de chiffrement est

$$\alpha = (1+19i)^{193}.$$

On a $193 = 6 \times 31 + 7$, d'où les égalités

$$\alpha = (1-19i)^6(1+19i)^7 = 21^6(1+19i) = 2+7i.$$

4.2) Alice doit envoyer à Bob l'élément $\beta = (4+i)^{193}$. On obtient

$$\beta = (4-i)^6(4+i)^7 = 17^6(4+i) = 1+8i.$$