Contrôle Continu - Corrigé

20/10/26

Exercice 1.

(a) À l'aide de l'algorithme d'Euclide étendu, calculer le pgcd entre 83 et 57, et une identité de Bézout.

(b) En déduire deux entiers $u, v \in \mathbb{Z}$ tels que

$$\frac{1}{4731} = \frac{u}{57} + \frac{v}{83}. \tag{1}$$

(On remarquera que $4731 = 57 \times 83$.)

(c) Existe-t-il des entiers u, v tels que $\frac{1}{24} = \frac{u}{4} + \frac{v}{6}$? Justifier.

(d) Soient $m, n \geq 2$ et $k \in \mathbb{Z}$. Montrer qu'il existe $u, v \in \mathbb{Z}$ tels que

$$\frac{k}{mn} = \frac{u}{m} + \frac{v}{n}$$

si et seulement si $\text{pgcd}(m, n)$ divise k.

Solution

(a) [2 points] *On applique l'algorithme d'Euclide étendu pour déterminer le pgcd de 83 et 57 et une identité de Bézout :*

$$\begin{aligned} 83 &= 1 \cdot 57 + 26 \\ 57 &= 2 \cdot 26 + 5 \\ 26 &= 5 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Donc $\text{pgcd}(83, 57) = 1$. *En remontant les égalités on obtient :*

$$\begin{aligned} 1 &= 26 - 5 \cdot 5 \\ &= 26 - 5 \cdot (57 - 2 \cdot 26) \\ &= 11 \cdot 26 - 5 \cdot 57 \\ &= 11 \cdot (83 - 57) - 5 \cdot 57 \\ &= 11 \cdot 83 + (-16) \cdot 57. \end{aligned}$$

Donc une identité de Bézout est :

$$1 = 11 \cdot 83 + (-16) \cdot 57.$$

(b) [1 point] *En divisant les deux membres de l'identité de Bézout obtenue en (a) par* $4731 = 57 \cdot 83$*, on obtient*

$$\frac{1}{4731} = \frac{11 \cdot 83}{57 \cdot 83} + \frac{(-16) \cdot 57}{57 \cdot 83} = \frac{11}{57} + \frac{-16}{83}.$$

Donc $u = 11$ *et* $v = -16$ *vérifient (1).*

(c) [1 point] *Supposons qu'il existe* $u, v \in \mathbb{Z}$ *tels que* $\frac{1}{24} = \frac{u}{4} + \frac{v}{6}$*. En multipliant les deux membres par* 24*, on obtient*

$$1 = 6u + 4v = 2(3u + 2v),$$

donc $2 \mid 1$*, ce qui est absurde. Il n'existe donc pas de tels entiers.*

(d) [2 points] *Soient* $m, n \geq 2$*,* $k \in \mathbb{Z}$ *et notons* $d = \operatorname{pgcd}(m, n)$*. En multipliant par* mn*, on remarque d'abord que*

$$\frac{k}{mn} = \frac{u}{m} + \frac{v}{n} \quad \Longleftrightarrow \quad k = un + vm$$

L'énoncé est donc équivalent à montrer qu'il existe $u, v \in \mathbb{Z}$ *tels que* $k = un + vm$*. si et seulement si* $d|k$*.*

(⇒) *Supposons qu'il existe* $u, v \in \mathbb{Z}$ *tels que* $k = un + vm$*. Comme* $d \mid m$ *et* $d \mid n$*, on a* $d \mid un + vm$*, c'est-à-dire* $d \mid k$*.*

(⇐) *Réciproquement, supposons que* $d \mid k$*, et soit* $k' \in \mathbb{Z}$ *tel que* $k = dk'$*. D'après l'identité de Bézout, il existe* $\alpha, \beta \in \mathbb{Z}$ *tels que* $d = \alpha m + \beta n$*. En multipliant par* k'*, on obtient*

$$k = (\beta k')\, n + (\alpha k')\, m.$$

Donc $u = \beta k'$ *et* $v = \alpha k'$ *vérifient* $k = un + vm$*, c'est-à-dire* $\frac{k}{mn} = \frac{u}{m} + \frac{v}{n}$*.*

Exercice 2. Soit $N \in \mathbb{Z}_{>0}$ un entier dont l'écriture en base 10 est

$$N = \sum_{i=0}^{k} c_i 10^i, \text{ avec } c_i \in \{0, \ldots, 9\}.$$

(a) Montrer que $N \equiv \sum_{i=0}^{k} c_i \pmod 9$. En déduire un critère de divisibilité par 9.

(b) Établir un critère de divisibilité par 11.

(c) Les entiers 123456789 et 20266202 sont-ils divisibles par 9 ? par 11 ?

(d) On dit que N est un *palindrome* si $c_i = c_{k-i}$ pour tout i. Montrer que tout palindrome ayant un nombre pair de chiffres est divisible par 11. Est-ce encore vrai pour un nombre impair de chiffres ?

Solution

(a) [1,5 point] *On a* $10 \equiv 1 \pmod 9$, *donc pour tout* $i \geq 0$, $10^i \equiv 1^i = 1 \pmod 9$. *On en déduit*

$$N = \sum_{i=0}^{k} c_i 10^i \equiv \sum_{i=0}^{k} c_i \pmod 9.$$

En particulier, $N \equiv 0 \pmod 9$ *si et seulement si* $\sum_{i=0}^{k} c_i \equiv 0 \pmod 9$, *c'est-à-dire :* N est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

(b) [1,5 point] *On a* $10 \equiv -1 \pmod{11}$, *donc pour tout* $i \geq 0$, $10^i \equiv (-1)^i \pmod{11}$. *On en déduit*

$$N = \sum_{i=0}^{k} c_i 10^i \equiv \sum_{i=0}^{k} (-1)^i c_i \pmod{11}.$$

Ainsi : N est divisible par 11 si et seulement si la somme alternée de ses chiffres $c_0 - c_1 + c_2 - \cdots + (-1)^k c_k$ (en partant du chiffre des unités) est divisible par 11.

(c) [1,5 points] *Pour* $N = 123456789$ *:*

- *la somme des chiffres est* $1+2+3+4+5+6+7+8+9 = 45 = 9 \cdot 5$, *donc* 123456789 *est divisible par* 9 *;*
- *la somme alternée des chiffres est* $9-8+7-6+5-4+3-2+1 = 5$, *qui n'est pas divisible par* 11, *donc* 123456789 *n'est pas divisible par* 11.

Pour $N = 20266202$ *:*

- *la somme des chiffres est* $2+0+2+6+6+2+0+2 = 20 \equiv 2 \pmod 9$, *donc* 20266202 *n'est pas divisible par* 9 *;*
- *la somme alternée des chiffres est* $2-0+2-6+6-2+0-2 = 0$, *donc* 20266202 *est divisible par* 11.

(d) [1,5 points] *Supposons que N est un palindrome ayant un nombre pair de chiffres. Comme N a $k+1$ chiffres, k est impair. Cela implique que 2 divise $(k-1)$ et $i \neq k-i$, pour tout $i \in \{0,\dots,k\}$. De plus, pour tout $i \in \{0,\dots,k\}$, on a $(-1)^{k-i} = (-1)^k(-1)^i = -(-1)^i$.*
Donc, en regroupant les termes d'indices i et $k-i$ dans la somme alternée des chiffres, et en utilisant $c_{k-i} = c_i$, on obtient

$$\sum_{i=0}^{k}(-1)^i c_i = \sum_{i=0}^{\frac{k-1}{2}}\left((-1)^i c_i + (-1)^{k-i}c_{k-i}\right) = \sum_{i=0}^{\frac{k-1}{2}} c_i\left((-1)^i - (-1)^i\right) = 0.$$

D'après le critère de (b), N est divisible par 11.
Ce n'est plus vrai pour un nombre impair de chiffres : par exemple, 101 est un palindrome à 3 chiffres, mais la somme alternée de ses chiffres vaut $1-0+1=2$, donc 101 n'est pas divisible par 11.

Exercice 3. Pour $a, b \in \frac{\mathbb{Z}}{26\mathbb{Z}}$, on considère l'application

$$\begin{array}{rccc} f_{a,b}\colon & \frac{\mathbb{Z}}{26\mathbb{Z}} & \to & \frac{\mathbb{Z}}{26\mathbb{Z}} \\ & x & \mapsto & ax+b. \end{array}$$

(a) Déterminer les éléments inversibles de $\frac{\mathbb{Z}}{26\mathbb{Z}}$ et l'inverse de 7 modulo 26.

(b) Montrer que $f_{a,b}$ est bijective si et seulement si $\mathrm{pgcd}(a,26) = 1$. Combien y a-t-il de couples (a,b) pour lesquels $f_{a,b}$ est bijective ?

(c) On suppose a inversible dans $\frac{\mathbb{Z}}{26\mathbb{Z}}$ et on note a^{-1} son inverse. Montrer que la réciproque $f_{a,b}^{-1}$ est encore de la forme $f_{a',b'}$, et exprimer a' et b' en fonction de a et b.

Application au chiffrement affine. On identifie maintenant les lettres A, B, …, Z aux éléments $0, 1, \dots, 25$ de $\frac{\mathbb{Z}}{26\mathbb{Z}}$.

Soient $a, b \in \mathbb{Z}$ tels que $\mathrm{pgcd}(a,26) = 1$. Le *chiffrement affine* de clé (a,b) remplace chaque lettre x par la lettre $f_{a,b}(x)$. La *fonction de déchiffrement* correspondante est la fonction $f_{a,b}^{-1}$.

Exemple. Prenons la clé $(a,b) = (15,2)$, qui est valable car $\mathrm{pgcd}(15,26) = 1$. Pour chiffrer la lettre C, on remplace C par son numéro $x = 2$, on calcule $f_{15,2}(2) = 15\times 2+2 = 32 \equiv 6 \pmod{26}$. On revient aux lettres : 6 correspond à G. La lettre C est donc chiffrée en G. En procédant de même pour chaque lettre, le mot `CIAO` est chiffré en `GSCE`.

(d) Pour la clé $(a,b) = (7,3)$, chiffrer le message `HELLO`.

(e) Le message `KSDUX` a été chiffré avec la clé $(7,3)$. Après avoir déterminé la fonction de déchiffrement $f_{7,3}^{-1}$, le déchiffrer.

(f) On intercepte un message chiffré avec une clé inconnue, et on sait que les lettres E et S ont été chiffrées respectivement en B et en T. Retrouver la clé.

(g) Pour essayer de renforcer la sécurité, on chiffre un message avec la clé $(7, 3)$, puis on chiffre le résultat avec la clé $(5, 7)$. Montrer que l'on obtient le même résultat qu'avec un unique chiffrement affine, dont on donnera la clé. Ce double chiffrement est-il plus sûr ?

Solution

(a) [2 points] *Un élément* $a \in \frac{\mathbb{Z}}{26\mathbb{Z}}$ *est inversible si et seulement si* $\text{pgcd}(a, 26) = 1$. *Comme* $26 = 2 \cdot 13$, *cela équivaut à dire que* a *n'est divisible ni par* 2 *ni par* 13. *Donc*

$$\left(\frac{\mathbb{Z}}{26\mathbb{Z}}\right)^{\times} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\},$$

qui contient 12 *éléments. Pour calculer l'inverse de* 7 *modulo* 26, *on applique l'algorithme d'Euclide étendu :*

$$\begin{aligned} 26 &= 3 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

En remontant les égalités on obtient :

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 26 + (-11) \cdot 7. \end{aligned}$$

Donc $7 \cdot (-11) \equiv 1 \pmod{26}$ *et l'inverse de* 7 *modulo* 26 *est* $-11 \equiv 15 \pmod{26}$.

(b) [2 points] *Supposons que* $\text{pgcd}(a, 26) = 1$. *Alors* a *est inversible dans* $\frac{\mathbb{Z}}{26\mathbb{Z}}$. *Soient* $x, y \in \frac{\mathbb{Z}}{26\mathbb{Z}}$ *tels que* $f_{a,b}(x) = f_{a,b}(y)$. *Alors* $ax + b = ay + b$, *donc* $a(x - y) = 0$ *et, en multipliant les deux membres par* a^{-1}, *on obtient* $x = y$. *Donc* $f_{a,b}$ *est injective. Comme* $f_{a,b}$ *est une application injective de l'ensemble fini* $\frac{\mathbb{Z}}{26\mathbb{Z}}$ *dans lui-même, elle est aussi surjective,*

donc bijective.
Réciproquement, supposons que $f_{a,b}$ est bijective. Donc, en particulier, $f_{a,b}$ est surjective. Cela implique que pour tout $y \in \frac{\mathbb{Z}}{26\mathbb{Z}}$ il existe $x \in \frac{\mathbb{Z}}{26\mathbb{Z}}$ tel que $y = ax + b$. En particulier, pour $y = b + 1$, il existe $x \in \frac{\mathbb{Z}}{26\mathbb{Z}}$ tel que $b + 1 = ax + b$, c'est à dire $1 = ax$. Donc a est inversible, ce qui est équivalent à $\text{pgcd}(a, 26) = 1$.
Ainsi $f_{a,b}$ est bijective si et seulement si a est l'un des 12 éléments inversibles déterminés en (a), b étant quelconque parmi les 26 éléments de $\frac{\mathbb{Z}}{26\mathbb{Z}}$. Il y a donc $12 \cdot 26 = 312$ couples (a, b) pour lesquels $f_{a,b}$ est bijective.

(c) [1 point] *Soient $x, y \in \frac{\mathbb{Z}}{26\mathbb{Z}}$. On a*

$$y = f_{a,b}(x) \iff ax = y - b \iff x = a^{-1}(y - b) = a^{-1}y - a^{-1}b.$$

Donc $f_{a,b}^{-1}(y) = a^{-1}y - a^{-1}b$ pour tout y, c'est-à-dire

$$f_{a,b}^{-1} = f_{a',b'}, \quad \text{où } a' = a^{-1},\ b' = -a^{-1}b.$$

(d) [1 point] *Pour la clé $(7, 3)$, on a $f_{7,3}(x) = 7x + 3$:*

lettre	*H*	*E*	*L*	*L*	*O*
x	7	4	11	11	14
$7x + 3$	52	31	80	80	101
$7x + 3 \bmod 26$	0	5	2	2	23
lettre chiffrée	*A*	*F*	*C*	*C*	*X*

Le message **`HELLO`** *est donc chiffré en* **`AFCCX`**.

(e) [1,5 points] *D'après (a), $7^{-1} = 15$ dans $\frac{\mathbb{Z}}{26\mathbb{Z}}$, et d'après (c),*

$$f_{7,3}^{-1} = f_{15,\,-15\cdot 3} = f_{15,-45} = f_{15,7}.$$

La fonction de déchiffrement est donc $y \mapsto 15y + 7$. On l'applique au message **`KSDUX`** *:*

lettre chiffrée	*K*	*S*	*D*	*U*	*X*
y	10	18	3	20	23
$15y + 7$	157	277	52	307	352
$15y + 7 \bmod 26$	1	17	0	21	14
lettre	*B*	*R*	*A*	*V*	*O*

Le message déchiffré est **`BRAVO`**.

(f) [1,5 points] *Notons* (a, b) *la clé inconnue. Comme E, S, B et T correspondent respectivement à* 4, 18, 1 *et* 19*, on a* $f_{a,b}(4) = 1$ *et* $f_{a,b}(18) = 19$*, c'est-à-dire*

$$\begin{cases} 4a + b \equiv 1 \pmod{26} \\ 18a + b \equiv 19 \pmod{26} \end{cases}$$

En soustrayant la première équation à la seconde, on obtient $14a \equiv 18 \pmod{26}$*. Comme* $\text{pgcd}(14, 26) = 2$ *divise* 18*, cette congruence admet des solutions modulo 26, et en simplifiant par* 2 *elle équivaut à*

$$7a \equiv 9 \pmod{13} \Leftrightarrow a \equiv 5 \pmod{13},$$

c'est-à-dire $a \equiv 5$ *ou* $a \equiv 18 \pmod{26}$*. Or la clé doit être valable, donc* $\text{pgcd}(a, 26) = 1$*, ce qui exclut* $a = 18$ *(qui est pair). On a donc* $a = 5$*, puis*

$$b = 1 - 4a = 1 - 20 = -19 = 7 \equiv 7 \pmod{26}.$$

La clé est $(5, 7)$*.*

(g) [1 point] *Chiffrer avec la clé* $(7, 3)$ *puis avec la clé* $(5, 7)$ *revient à appliquer* $f_{5,7} \circ f_{7,3}$*. Pour tout* $x \in \frac{\mathbb{Z}}{26\mathbb{Z}}$*, on a*

$$f_{5,7} \circ f_{7,3}(x) = 5(7x + 3) + 7 = 35x + 22 = 9x + 22 = f_{9,22}(x).$$

Le double chiffrement est donc le chiffrement affine de clé $(9, 22)$*, qui est bien une clé valable car* $\text{pgcd}(9, 26) = 1$*. Il n'est pas plus sûr : un attaquant n'a pas besoin de retrouver les deux clés* $(7, 3)$ *et* $(5, 7)$*, il lui suffit de retrouver la clé* $(9, 22)$*, qui est l'une des* 312 *clés affines possibles.*