

Pondichéry 2012. Enseignement de spécialité

EXERCICE 4 (5 points)

Partie A Restitution organisée de connaissances

Puisque $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, il existe deux entiers relatifs k et k' tels que $b = a + kn$ et $d = c + k'n$.
Mais alors,

$$bd = (a + kn)(c + k'n) = ac + ak'n + ckn + kk'n^2 = ac + (ak' + ck + kk'n)n$$

Posons $K = ak' + ck + kk'n$. K est un entier relatif tel que $bd = ac + Kn$ et on a donc montré que $ac \equiv bd \pmod{n}$.

Partie B Inverse de 23 modulo 26

1) $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$. Donc le couple $(-9, -8)$ est solution de l'équation (E).

2) Posons $(x_0, y_0) = (-9, -8)$. Soient x et y deux entiers relatifs.

$$(x, y) \text{ solution de (E)} \Leftrightarrow 23x - 26y = 1 \Leftrightarrow 23x - 26y = 23x_0 - 26y_0 \Leftrightarrow 23(x - x_0) = 26(y - y_0).$$

Si (x, y) est solution de (E), alors l'entier 26 divise l'entier $26(y - y_0) = 23(x - x_0)$. D'autre part, la question précédente montre qu'il existe deux entiers relatifs u et v tels que $23u + 26v = 1$. Le théorème de BÉZOUT permet alors d'affirmer que les entiers 23 et 26 sont premiers entre eux.

Ainsi, 26 divise $23(x - x_0)$ et 26 est premier à 23. D'après le théorème de GAUSS, 26 divise $x - x_0$. Par suite, il existe un entier relatif k tel que $x - x_0 = 26k$ ou encore tel que $x = -9 + 26k$. De même, il existe un entier relatif k' tel que $y = -8 + 23k'$.

En résumé, si (x, y) est solution de (E), il existe deux entiers relatifs k et k' tels que $x = -9 + 26k$ et $y = -8 + 23k'$.

Réciproquement, soient k et k' deux entiers relatifs puis $x = -9 + 26k$ et $y = -8 + 23k'$.

$$(x, y) \text{ est solution de (E)} \Leftrightarrow 23(-9 + 26k) - 26(-8 + 23k') = 1 \Leftrightarrow 1 + 23 \times 26 \times (k - k') = 1 \Leftrightarrow k = k'.$$

Les solutions de (E) sont les couples d'entiers relatifs de la forme $(-9 + 26k, -8 + 23k)$, $k \in \mathbb{Z}$.

3) Soit a un entier relatif. $23a \equiv 1 \pmod{26}$ si et seulement si il existe un entier relatif y tel que $23a - 26y = 1$. D'après la question précédente, ceci impose l'existence d'un entier relatif k tel que $a = -9 + 26k$. Ensuite,

$$0 \leq a \leq 25 \Leftrightarrow 0 \leq -9 + 26k \leq 25 \Leftrightarrow 9 \leq 26k \leq 34 \Leftrightarrow \frac{9}{26} \leq k \leq \frac{34}{26} \Leftrightarrow k = 1.$$

Pour $k = 1$, on obtient $a = -9 + 26 = 17$. Réciproquement, puisque $17 \times 23 = 391 = 1 + 15 \times 26$, l'entier $a = 17$ est un entier tel que $0 \leq a \leq 25$ et $23a \equiv 1 \pmod{26}$.

$$\boxed{a = 17.}$$

Partie C Chiffrement de Hill

1) **Etape 1.** ST correspond à $(x_1, x_2) = (18, 19)$.

Etape 2. • $11x_1 + 3x_2 = 11 \times 18 + 3 \times 19 = 198 + 57 = 255$. y_1 est alors le reste de la division euclidienne de 255 par 26. Comme $255 = 21 + 234 = 21 + 9 \times 26$ et que $0 \leq 21 \leq 25$, on en déduit que $y_1 = 21$.

• $7x_1 + 4x_2 = 7 \times 18 + 4 \times 19 = 126 + 76 = 202$. Comme $202 = 20 + 182 = 20 + 7 \times 26$ et que $0 \leq 20 \leq 25$, on en déduit que $y_2 = 20$.

Etape 3. Le couple $(21, 20)$ correspond au mot VU et donc

$$\boxed{\text{le mot ST se code en VU.}}$$

2) a) Soient x_1, x_2, y_1 et y_2 quatre entiers.

$$\begin{aligned} \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} &\Rightarrow \begin{cases} 4y_1 + 23y_2 \equiv (4 \times 11 + 23 \times 7)x_1 + (4 \times 3 + 23 \times 4)x_2 \pmod{26} \\ 19y_1 + 11y_2 \equiv (19 \times 11 + 11 \times 7)x_1 + (19 \times 3 + 11 \times 4)x_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} 4y_1 + 23y_2 \equiv 205x_1 + 104x_2 \pmod{26} \\ 19y_1 + 11y_2 \equiv 286x_1 + 101x_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} 4y_1 + 23y_2 \equiv 23x_1 \pmod{26} \\ 19y_1 + 11y_2 \equiv 23x_2 \pmod{26} \end{cases} \end{aligned}$$

car $205 = 23 + 7 \times 26$, $104 = 4 \times 26$, $286 = 11 \times 26$ et $101 = 23 + 3 \times 26$ et donc

$$205 \equiv 23 \pmod{26}, 104 \equiv 0 \pmod{26}, 286 \equiv 0 \pmod{26} \text{ et } 101 \equiv 23 \pmod{26}.$$

b) On multiplie alors les deux membres de chaque congruence écrite par 17. D'après la question 3) de la partie B, on a $23 \times 17 \equiv 1 \pmod{26}$ et donc on obtient

$$\begin{aligned} \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases} &\Rightarrow \begin{cases} x_1 \equiv 4 \times 17y_1 + 23 \times 17y_2 \pmod{26} \\ x_2 \equiv 19 \times 17y_1 + 11 \times 17y_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} x_1 \equiv 68y_1 + 391y_2 \pmod{26} \\ x_2 \equiv 323y_1 + 187y_2 \pmod{26} \end{cases} \Rightarrow \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases} \end{aligned}$$

car $68 = 16 + 2 \times 26$, $391 = 1 + 15 \times 26$, $323 = 11 + 12 \times 26$ et $187 = 5 + 7 \times 26$ et donc

$$68 \equiv 16 \pmod{26}, 391 \equiv 1 \pmod{26}, 323 \equiv 11 \pmod{26} \text{ et } 187 \equiv 5 \pmod{26}.$$

c) Réciproquement,

$$\begin{aligned} \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases} &\Rightarrow \begin{cases} 11x_1 + 3x_2 \equiv 209y_1 + 26y_2 \pmod{26} \\ 7x_1 + 4x_2 \equiv 156y_1 + 27y_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \end{aligned}$$

car $209 = 1 + 8 \times 26$, $26 = 0 + 1 \times 26$, $156 = 0 + 6 \times 26$ et $27 = 1 + 1 \times 26$ et donc

$$209 \equiv 1 \pmod{26}, 26 \equiv 0 \pmod{26}, 156 \equiv 0 \pmod{26} \text{ et } 27 \equiv 1 \pmod{26}.$$

En résumé,

$$\boxed{\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}}$$

d) • Le mot **YJ** correspond au couple $(y_1, y_2) = (24, 9)$.

- $16y_1 + y_2 = 16 \times 24 + 9 = 393 = 3 + 15 \times 26$ et donc $x_1 = 3$.
- $11y_1 + 5y_2 = 11 \times 24 + 5 \times 9 = 309 = 23 + 11 \times 26$ et donc $x_2 = 23$.

Le couple $(3, 23)$ correspond au mot **DX** et donc

le mot YJ se décode en DX.