## Exercice 4 — Candidats ayant suivi la spécialité — 5 points

*Les parties A et B peuvent être traitées de façon indépendante.*

**Partie A**

Pour deux entiers naturels non nuls a et b, on note r(a, b) le reste de la division euclidienne de a par b.
On considère l'algorithme suivant :

**Variables :** c est un entier naturel
a et b sont des entiers naturels non nuls
**Entrées :** Demander a
Demander b
**Traitement :** Affecter à c le nombre r(a, b)
Tant que $c \neq 0$
Affecter à a le nombre b
Affecter à b le nombre c
Affecter à c le nombre r($a$, $b$)
Fin Tant que
**Sortie :** Afficher b

**1.** Faire fonctionner cet algorithme avec a=26 et b=9 en indiquant les valeurs de a, b et c à chaque étape.

**2.** Cet algorithme donne en sortie le PGCD des entiers naturels non nuls a et b. Le modifier pour qu'il indique si deux entiers naturels non nuls a et b sont premiers entre eux ou non.

**Partie B**

A chaque lettre de l'alphabet on associe grâce au tableau ci-dessous un nombre entier compris entre 0 et 25.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

On définit un procédé de codage de la façon suivante :
**Étape 1 :** on choisit deux entiers naturels p et q compris entre 0 et 25.
**Étape 2 :** à la lettre que l'on veut coder on associe l'entier $x$ correspondant dans le tableau ci-dessus.
**Étape 3 :** on calcule l'entier $x'$ défini par les relations $x' \equiv px+q\,(26)$ et $0 \leqslant x' \leqslant 25$
**Étape 4 :** à l'entier $x'$ on associe la lettre correspondante dans le tableau.

**1.** Dans cette question, on choisit p=9 et q=2.
**a.** Démontrer que la lettre V est codée par la lettre J.
**b.** Citer un théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que $9u+26v=1$.
Donner sans justifier un couple (u, v) qui convient.
**c.** Démontrer que $x' \equiv 3x+2\,(26)$ équivaut à $x \equiv 3x'+20\,(26)$

**d.** Décoder la lettre R.

**2.** Dans cette question, on choisit q=2 et p inconnu. On sait que I est codé par D. Déterminer la valeur de p (on admettra que p est unique).

**3.** Dans cette question, on choisit p=13 et q=2. Coder les lettres B et D. Que peut-on dire de ce codage ?

**Correction :**

**Partie A**

**1.** a=26 et b=9
c=8 (car $26=2\times9+8$ )

$1^{ère}$ étape : a=9
b=8
c=1 (car $9=1\times8+1$ )

$2^{ème}$ étape : a = 8
b=1
c=0 (car $8=8\times1+0$ )

Sortie : **b = 1**

**2. Sortie :** **Si b=1 alors afficher « les nombres a et b sont premiers entre eux »**
**Sinon afficher « les nombres a et b ne sont premiers entre eux ».**

**Partie B**

**1.a.** On choisit p=9 et q=2
A la lettre V, on associe le nombre $x$=21
On détermine le nombre $x'$ tel que : $x'\equiv9\times21+2(26)$ et $0\leqslant x'\leqslant25$
Soit $x'\equiv191(26)$ et $0\leqslant x'\leqslant25$
$x'$ est **le reste de la division euclidienne de 191 par 26**
Or, $191=26\times7+9$
Donc, **x'=9**
Le tableau nous donne **la lettre J**.

**b.** 9 et 26 sont premiers entre eux ( on a démontré ce résultat dans la partie A).
**Le théorème de Bezout** nous permet d'affirmer qu'il existe un couple d'entiers relatifs $(u;v)$ tel que :
$9u+26v=1$ .
Le couple $(3;-1)$ est **une solution particulière** car $9\times3+26\times(-1)=27-26=1$ .
Remarque
$9\times3\equiv1(26)$

**c.** Si $x'\equiv9x+2(26)$ alors $3x'\equiv3\times9x+3\times2(26)$
soit $3x'\equiv27x+6(26)$
et $3x'\equiv x+6(26)$
et $x\equiv3x'-6(26)$
et $x\equiv3x'+20(26)$
car $-6\equiv-6+26(26)$ donc $-6\equiv20(26)$

**Réciproquement**
Si $x\equiv3x'+20(26)$ alors $9x\equiv9\times3x'+9\times20(26)$
soit $9x\equiv x'+180(26)$
or $180=6\times26+24$
donc $9x\equiv x'+24(26)$
et $x'\equiv9x-24(26)$
or $-24\equiv-24+26(26)$ donc $-24\equiv2(26)$
On obtient $x'\equiv9x+2(26)$
**Conclusion**
$x'\equiv9x+2(26)$ si et seulement si $x\equiv3x'+20(26)$

**d.** La lettre codée est R, le tableau nous donne $x'=17$ et $x\equiv 3x'+20(26)$ avec $0\leqslant x\leqslant 25$
$x\equiv 3\times 17+20(26)$
$x\equiv 71(26)$ $(26)$
Or, $71=2\times 26+19$
Donc, $x=19$ $(0\leqslant x\leqslant 25)$
La lettre que l'on a codée est **la lettre correspondante à 19** dans le tableau donc **T**.

**2.** q=2 et p inconnu $(0\leqslant p\leqslant 25)$ .
L'algorithme de codage : $x'\equiv px+2(26)$ et $0\leqslant x'\leqslant 25$
A la lettre J on associe $x$=9, donc $x'\equiv 9p+2(26)$
J est codée en D donc $x'$=3
Conséquence
$3\equiv 9p+2(26)$ soit $9p\equiv 1(26)$
Nous avons vu que $9\times 3\equiv 1(26)$ et $0\leqslant 3\leqslant 25$
Donc **p=3** (on admet l'unicité de p).

**3.** p=13 et q=2
$x'\equiv 13x+2(26)$ et $0\leqslant x'\leqslant 25$
A la lettre B on associe $x$=1 donc $x'\equiv 13\times 1+2(26)$
On obtient $x'$=15.
15 correspond à la lettre P.
La lettre B **est codée en P**.

A la lettre D on associe $x$=3 donc $x'\equiv 13\times 3+2(26)$ soit $x'\equiv 41(26)$
Or, $41=1\times 26+15$
On obtient $x'\equiv 15(26)$ et $0\leqslant 15\leqslant 25$
5 correspond **à la lettre P**.

Il **n'existe pas d'algorithme de décodage** car à la lettre P il y a au moins deux lettres correspondantes B et D.
Remarque
Les nombres 13 et 26 ne sont pas premiers entre eux.