Exercice de spécialité Antilles-Guyane juin 2015

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 dans 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 la valeur de 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

À 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

$$x' \equiv px + q \quad [26] \quad \text{et} \quad 0 \leqslant x' \leqslant 25.$$

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 le 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 $x' \equiv 9x + 2 \quad [26]$ équivaut à $x \equiv 3x' + 20 \quad [26]$.
   d. Décoder la lettre R.
2. Dans cette question, on choisit $q = 2$ et p est inconnu. On sait que J 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 commentée

Partie A

1.a. Pour faire fonctionner un algorithme on note dans un tableau les différentes valeurs des variables à chaque tour de boucle (ici c'est la boucle Tant Que) :

Variables	Initialisation	Étape 1	Étape 2
a	26	9	8
b	9	8	1
c	8	1	0

Quand c=0 l'algorithme sort de la boucle Tant Que et exécute la ligne de sortie qui est d'afficher b, c'est à dire la dernière valeur stockée dans la variable b, soit ici 1.

2.b. L'algorithme met en pratique le lemme d'Euclide pour trouver le PGCD : $\text{PGCD}(a\,;b)=\text{PGCD}(b\,;r)$ avec r le reste de la division euclidienne de a par b.

la valeur de b affichée (la dernière valeur stockée dans b) donne le PGCD de a et b. Donc si le PGCD vaut 1 alors les nombres sont premiers entre eux.

Ainsi on modifie la sortie par :

```
Si b=1 Alors
        Afficher « les deux nombres sont premiers entre eux »
Sinon
        Afficher « les deux nombres ne sont pas premiers entre eux »
```

Partie B

1.a. D'après le tableau, V correspond au nombre 21, donc $x = 21$.

Ainsi $x' \equiv 9 \times 21 + 2 \ [26] \ \Leftrightarrow \ x' \equiv 191 \ [26]$

Or $191 = 7 \times 26 + 9$

donc $191 \equiv 9 \ [26]$ et donc $x' = 9$ car $0 \leqslant x' \leqslant 25$.

D'après le tableau, 9 correspond à la lettre J.

1.b. D'après la partie A, 26 et 9 sont premiers entre eux, donc d'après le théorème de Bézout, il existe 2 entiers relatifs u et v tel que $9u + 26v = 1$.

$9 \times 3 + 26 \times (-1) = 1$ donc le couple $(3\,;-1)$ est solution.

1.c. Attention à ne pas résoudre comme une équation avec égalité. Avec les congruences la division n'est pas permise. L'idée est donc de ne pas isoler x mais de faire apparaître $3x'$.

$x' \equiv 9x + 2 \ [26]$

$\Rightarrow \ 3x' \equiv 27x + 6 \ [26]$ (seule l'implication est possible car la réciproque nécessite une division)

$\Leftrightarrow \ 3x' \equiv 26x + x + 6 \ [26]$ (on décompose $27x$ pour faire apparaître x)

$\Leftrightarrow \ 3x' \equiv x + 6 \ [26]$ (car $26x$ est un multiple de 26)

$\Leftrightarrow \ x \equiv 3x' - 6 \ [26]$

$\Leftrightarrow \ x \equiv 3x' + 20 \ [26]$

De même « dans l'autre sens » :

$x \equiv 3x' + 20 \ [26]$

$\Rightarrow \ 9x \equiv 27x' + 180 \ [26]$

$\Leftrightarrow \ 9x \equiv x' + 180 \equiv x' - 2 \ [26]$

$\Leftrightarrow \ x' \equiv 9x + 2 \ [26]$

Ainsi : $x' \equiv 9x + 2 \ [26] \Leftrightarrow x \equiv 3x' + 20 \ [26]$

1.d. D'après le tableau la lettre R correspond au nombre 17, donc $x' = 17$.

On cherche donc x tel que $17 \equiv 9 \times x + 2 \ [26] \Leftrightarrow x \equiv 3 \times 17 + 20 \ [26]$ (d'après question 1.c.)

soit $x \equiv 71 \equiv 2 \times 26 + 19 \equiv 19 \ [26]$

D'après le tableau, 19 correspond à la lettre T. Donc le décodage de R donne T.

2. On sait que J est codé par D, ainsi $x = 9$ et $x' = 3$.

On a donc $3 \equiv 9p + 2 \ [26]$ soit $9p \equiv 1 \ [26]$

D'après la définition de la congruence, il existe k entier relatif, tel que $9p - 1 = 26k \Leftrightarrow 9p - 26k = 1$

D'après la question 1.b. on peut choisir $p = 3$ et $k = 1$.

Comme $0 \leqslant p \leqslant 25$ et p est unique donc la valeur de p recherchée est 3.

3. La lettre B correspond à $x = 1$.

Ainsi $x' \equiv 13 \times 1 + 2 \equiv 15 \ [26]$

15 correspond à P donc la lettre B est codée par P.

La lettre D correspond à $x = 3$.

Ainsi $x' \equiv 13 \times 3 + 2 \equiv 41 \equiv 26 + 15 \equiv 15 \ [26]$

15 correspond à P donc la lettre D est codée par P.

Ce codage ne permet pas de décodage unique puisque une lettre codée (P) donne au moins deux lettres décodées (B ou D).