Corrigé de l'exercice de spécialité maths du galop d'essai, janvier 2016.

Exercice n° 4 — CORRIGÉ *5 points*

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

Partie A. Dans cette partie, on choisit $p = 9$ et $q = 2$.

1. Dans le tableau V correspond à 21, or $9 \times 21 + 2 = 189 + 2 = 191$ et $191 = 26 \times 7 + 9$; donc $y \equiv 9$ [26].
Dans le tableau 9 correspond à la lettre J, donc V se code en J.

2. $9 \times 3 = 27 = 26 + 1$ donc $u = 3$ convient (mais ce n'est pas le seul à vérifier $9u \equiv 1$ [26]).

3. On démontre les deux sens séparement, car si on peut multiplier les deux membres d'une congruence par un même entier, on ne peut pas diviser (ici par 3 ou 9).

$y \equiv 9x + 2$ [26]	$x \equiv 3y + 20$ [26]
$\implies 3y \equiv 3 \times (9x + 2)$ [26]	$\implies 9x \equiv 9 \times (3y + 20)$ [26]
$\implies 3y \equiv 27x + 6$ [26]	$\implies 9x \equiv 27y + 180$ [26]
$\implies 3y - 6 \equiv x$ [26]	$\implies 9x - (26 \times 7 - 2) \equiv y$ [26]
$\implies x \equiv 3y + 20$ [26]	$\implies y \equiv 9x + 2$ [26]

Ainsi on a bien : $y \equiv 9x + 2$ [26] $\iff x \equiv 3y + 20$ [26] ce qui donne une méthode pour décoder.

4. R correspond à $y = 17$, donc $3y + 20 = 51 + 20 = 71$ et $71 = 26 \times 2 + 19$, soit $71 \equiv 19$ [26].
On a donc $x = 19$ qui correspond à la lettre T. Donc R se décode par T.

5. Il suffit de rentrer en B2 la formule `=MOD(3*B1+20;26)` puisque d'après les questions précédentes pour décoder y on calcule le reste de $3y + 20$ divisé par 26.

Partie B. Dans cette partie on étudie divers cas selon les valeurs de p et q.

1. Dans cette question, on choisit $q = 2$ et p est inconnu. On sait que J est codé par D.
J correspond à $x = 9$ et D correspond à $y = 3$. On a donc :
$3 \equiv 9p + 2$ [26] soit $9p \equiv 1$ [26]. En multipliant par 3 on a donc $27p \equiv 3$ [26] donc $p \equiv 3$ [26] Si on choisit p compris entre 0 et 25, on a donc $p = 3$.

2. Dans cette question, on choisit $p = 13$ et $q = 2$.

a. B correspond à $x = 1$, d'où $y = 13x + 2 \equiv 15$ [26] et 15 correspond à la lettre P.
D correspond à $x = 3$, d'où $y \equiv 13 \times 3 + 2$ [26] donc $y \equiv 41$ [26] et $41 \equiv 15$ [26] et 15 correspond à la lettre P.
Conclusion : deux lettres différentes sont codées par la même lettre. Ce codage n'est pas bon puisque le décryptage de P donnera plusieurs solutions possibles.

b. Si $x = 2k$ (où $k \in \mathbb{N}$) alors $y \equiv 13 \times 2k + 2$ [26] soit $y \equiv 2$ [26] et comme $0 \leqslant y \leqslant 25$ on a bien $y = 2$.

c. Si x est impair, il est de la forme $x = 2k + 1$ pour un $k \in \mathbb{N}$ et alors :
$y \equiv 13 \times (2k + 1) + 2$ [26] soit $y \equiv 26k + 15$ [26] et donc $y = 15$.
Soit x est pair et alors d'après le 2b. il sera codé par $y = 2$ soit la lettre C,
soit x est impair et alors il sera codé par $y = 15$ soit la lettre P.
Ainsi un message codé ne comportera que les lettres C et P.