Partie A Cours

Théorème de Bézout : $a \in \mathbb{N}*, b \in \mathbb{N}*, PGCD(a,b) = 1 \Longleftrightarrow \exists u \in \mathbb{Z}, \exists v \in \mathbb{Z} : au + bv = 1$
Théorème de Gauss : Soit des entiers $a > 0, b > 0, c > 0$; si a divise bc et $a \bigwedge b = 1$ alors a divise c

Partie B

1. $11 \times (-7) - 26 \times (-3) = -77 + 78 = 1$, donc le couple $(-7\ ;\ -3)$ **est solution de (E)**.

2. – Soit $(x;y)$ une solution de (E), alors $11x - 26y = 1$ or $11 \times (-7) - 26 \times (-3) = 1$ d'après la question **B.1.**
Donc $11x - 26y = 11 \times (-7) - 26 \times (-3)$. On en déduit que $11(x+7) = 26(y+3)$.
Ainsi 26 divise $11(x+7)$, or 26 et 11 sont premiers entre eux, donc d'après le théorème de Gauss :
26 divise $x+7$. Il existe donc un entier relatif k tel que $x+7 = 26k$, c'est-à-dire $x = -7 + 26k$.
On a alors $11 \times 26k = 26(y+3)$, d'où, en divisant par 26 : $11k = y+3$, d'où $y = -3 + 11k$.
Ainsi, si $(x;y)$ est solution de (E), il existe un entier k tel que $(x;y) = (-7+26k; -3+11k)$.
– Réciproquement, on vérifie que ces couples sont bien solutions de (E) ;
en effet : $11 \times (-7+26k) - 26 \times (-3+11k) = -77 + 286k + 78 - 286k = 1$.
– En conclusion, les solutions de (E) sont les couples de la forme $(-7+26k; -3+11k)$ où $k \in \mathbb{Z}$.

3. $(u;v)$ est solution de (E) avec $0 \leqslant u \leqslant 25$ si et seulement s'il existe un entier relatif k tel que :
$u = 26k - 7$, $v = 11k - 3$ et $0 \leqslant -7 + 26k \leqslant 25$. donc $7 \leqslant 26k \leqslant 32$.
$k = 1$ est la seule possibilité, donc l'unique couple répondant à la question est $(19;8)$: $11 * 19 - 26 * 8 = 1$.

Partie C

1. La lettre W est chiffrée par $x = 22$. Or $11 \times 22 + 8 \equiv 16$ (modulo 26), donc $y = 16$ qui correspond à la lettre Q.

2. – Soit x et z deux entiers relatifs tels que $11x \equiv z$ (modulo 26). Alors, $19 \times 11x \equiv 19z$ (modulo 26).
Or d'après **B.3.** $19 \times 11 = 26 \times 8 + 1$ soit $19 \times 11 \equiv 1$ (modulo 26), donc $x \equiv 19z$ (modulo 26).
– Réciproquement, si $x \equiv 19z$ (mod 26), alors, $11x \equiv 11 \times 19z$ (mod 26), or $19 \times 11 \equiv 1$ (modulo 26),
d'où $11x \equiv z$ (modulo 26). L'équivalence est ainsi démontrée.

3. Soit y un entier de $[0\ ;\ 25]$, on cherche un entier (unique) x de $[0\ ;\ 25]$ tel que : $11x + 8 \equiv y$ (modulo 26).
Or d'après la question **C.2.a.** : $11x \equiv y - 8$ (modulo 26), $\Leftrightarrow x \equiv 19(y-8)$ (modulo 26)
Or $19 \times (-8) \equiv 4$ (mod 26), donc $11x \equiv y - 8$ (modulo 26) $\Leftrightarrow x \equiv 19y + 4$ (modulo 26)
Ainsi "y est **le reste (unique)** de la division euclidienne de $11x + 8$ par 26"
équivaut à : "x est **le reste (unique)** de la division euclidienne de $19y + 4$ par 26"
Le décodage est donc possible par le procédé suivant :
– on chiffre la lettre à décoder par un nombre entier y compris entre 0 et 25 ;
– on calcule le reste x de la division euclidienne de $(19y + 4)$ par 26 ;
– on déchiffre alors x pour obtenir la lettre décodée.

4. W est chiffré par $y = 22$. Or $19 \times 22 + 4 \equiv 6$ (modulo 26), donc $x = 6$, ce qui correspond à la lettre G.