

1. a. 109 est un nombre premier et 226 n'est pas un multiple de 109 donc :

$$\text{pgcd}(109, 226) = 1.$$

L'équation diophantienne (E) admet donc des couples solutions.

- b. • Vérifions que les couples de la forme $(141 + 226k, 68 + 109k)$ sont bien des solutions de (E) :
 $109 \times (141 + 226k) - 226 \times (68 + 109k) = 109 \times 141 - 226 \times 68 = 1.$
• Vérifions ensuite que ces couples sont les seules solutions de (E).

Notons $(x ; y)$ un couple solution quelconque (il y en a d'après la question 1a).

$$\text{On écrit le système : } \begin{cases} 109x - 226y = 1 \\ 109 \times 141 - 226 \times 68 = 1 \end{cases}$$

En retranchant membre à membre :

$$\begin{aligned} 109(x - 141) - 226(y - 68) &= 0 \\ 109(x - 141) &= 226(y - 68) \quad (*) \end{aligned}$$

On en déduit que 226 divise le produit $109(x - 141)$.

Mais, par ailleurs, $\text{pgcd}(226, 109) = 1$.

Donc, d'après le théorème de GAUSS, 226 divise $x - 141$.

Il existe donc un entier relatif k tel que :

$$\begin{aligned} x - 141 &= 226k \\ \Leftrightarrow x &= 141 + 226k. \end{aligned}$$

En remplaçant dans la relation (*), nous obtenons :

$$\begin{aligned} 109 \times 226k &= 226(y - 68) \\ \Leftrightarrow 109k &= (y - 68) \\ \Leftrightarrow y &= 109k + 68. \end{aligned}$$

Conclusion : les couples d'entiers $(x ; y)$ solutions de l'équation diophantienne $109x - 226y = 1$ sont de la forme $(x ; y) = (141 + 226k ; 109k + 68)$ où k est un élément de \mathbb{Z} .

Recherchons la valeur d de $x = 141 + 226k$ telle que :

$$\begin{aligned} 0 &\leq d \leq 226 \\ \Leftrightarrow 0 &\leq 141 + 226k \leq 226 \\ \Leftrightarrow -141 &\leq 226k \leq 85 \\ \Leftrightarrow -\frac{141}{226} &\leq k \leq \frac{85}{226}. \end{aligned}$$

Comme k est un entier, la seule possibilité est $k = 0$. D'où $d = 141$.

Et lorsque k vaut 0, la valeur e de y est alors égale à 68.

Ainsi, on a bien : $109d = 1 + 226e$ avec d inférieur ou égal à 226.

2. On teste si 227 est divisible par les nombres premiers inférieurs à $\sqrt{227}$:

227 n'est pas divisible par 2, par 3, par 5, par 7, par 11, ni par 13, donc 227 est un nombre premier.

3. a. $f(0)$ est le reste de la division euclidienne de 0^{109} par 227 donc $f(0) = 0$.

On a donc $g[f(0)] = g(0)$.

Or, $g(0)$ est le reste de la division euclidienne de 0^{141} par 227 donc $g(0) = 0$.

Finalement, $g[f(0)] = 0$.

- b. Soit a un élément non nul de A (A est l'ensemble des entiers naturels compris entre 0 et 226). Donc l'entier a n'est pas divisible par 227.

Comme 227 est premier (d'après la question 2), d'après le théorème de FERMAT, on a :

$$a^{226} \equiv 1 [227].$$

Ceci étant valable pour tout élément non nul a de A .

- c. On a modulo 227 : $g[f(a)] \equiv (f(a))^{141} \equiv a^{109 \times 141} [227]$.

Mais d'après la question 1b, on sait que $109 \times 141 = 1 + 226 \times 68$.

D'où :

$$g[f(a)] \equiv a^{109 \times 141} \equiv a a^{226 \times 68} [227].$$

Et, d'après la question 3b, on sait que $a^{226} \equiv 1 [227]$ donc :

$$g[f(a)] \equiv a [227].$$

Et comme $g[f(a)]$ et a sont tous deux inférieurs à 227, on peut écrire :

$$g[f(a)] = a.$$

Les fonctions f et g commutent ; en effet, pour tout entier a :

$$f[g(a)] \equiv (g(a))^{109} \equiv a^{109 \times 141} \equiv g[f(a)] [227].$$

On a donc également, pour tout entier a non nul de A :

$$f[g(a)] = a.$$