Exercice I

1. Au bout d'un an, puisque le bassin B contenait 100 poissons (car $b_0 = 100$), la vente de ces poissons permettra d'en acheter un nombre deux fois plus élevé à mettre dans le bassin A, soit 200. A cela, il faut ajouter les 200 poissons que le pisciculteur achète de toutes façons pour le bassin A. Cela confirme bien $a_1 = 200 + 200 = 400$.

   Pour le bassin B, on va commencer par y transférer les 200 poissons qui étaient dans le bassin A (car $a_0 = 200$), auxquels on ajoute les 100 poissons supplémentaires que le pisciculteur achète pour le bassin B, cela confirme bien : $b_1 = 200 + 100 = 300$.

   On aura ensuite $a_2 = 2 \times b_1 + 200 = 2 \times 300 + 200 = 800$ et, là encore de façon analogue $b_2 = a_1 + 100 = 400 + 100 = 500$.

2. **a.** On généralise le raisonnement établi à la question précédente : pour tout entier naturel n, on a :
   - $a_{n+1} = 2 \times b_n + 200$: le double du nombre de poissons dans le bassin B l'année précédente, auxquels on ajoute 200 poissons.
   - $b_{n+1} = a_n + 100$: les poissons transférés du bassin A l'année précédente, auxquels on ajoute 100 poissons.

   On calcule le produit matriciel AX_n :
   $$\begin{array}{cc} \times & \begin{pmatrix} a_n \\ b_n \end{pmatrix} \\ \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} & = \begin{pmatrix} 2b_n \\ a_n \end{pmatrix} \end{array}.$$

   On a donc la somme :
   $$AX_n + B = \begin{pmatrix} 2b_n \\ a_n \end{pmatrix} + \begin{pmatrix} 200 \\ 100 \end{pmatrix} = \begin{pmatrix} 2b_n + 200 \\ a_n + 100 \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = X_{n+1}.$$

   b. On a : $$\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix} + B \iff \begin{pmatrix} x \\ y \end{pmatrix} - A\begin{pmatrix} x \\ y \end{pmatrix} = B$$
   $$\iff (I_2 - A) \times \begin{pmatrix} x \\ y \end{pmatrix} = B$$

   Où la matrice I_2 est $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et donc $C = (I_2 - A) = \begin{pmatrix} 1 & -2 \\ -1 & 1 \end{pmatrix}$ est une matrice de déterminant non nul (le déterminant vaut -1), donc elle est inversible et $C^{-1} = \begin{pmatrix} -1 & -2 \\ -1 & -1 \end{pmatrix}$. On a donc :
   $$\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix} + B \iff C\begin{pmatrix} x \\ y \end{pmatrix} = B$$
   $$\iff \begin{pmatrix} x \\ y \end{pmatrix} = C^{-1} \times B$$

   Calculons le produit $C^{-1} \times B$:
   $$\begin{array}{cc} \times & \begin{pmatrix} 200 \\ 100 \end{pmatrix} \\ \begin{pmatrix} -1 & -2 \\ -1 & -1 \end{pmatrix} & = \begin{pmatrix} -200-200 \\ -200-100 \end{pmatrix} \end{array}$$

   On a donc $S = C^{-1} \times B = \begin{pmatrix} -400 \\ -300 \end{pmatrix}$, donc les nombres x et y sont respectivement -400 et -300.

   c. Pour tout entier naturel n, en posant $Y_n = \begin{pmatrix} a_n + 400 \\ b_n + 300 \end{pmatrix}$, on pose en fait $Y_n = X_n - S$, où S est la matrice déterminée à la question précédente, solution de l'équation $AX + B = X$, donc telle que $AS + B = S$, ou bien $AS = S - B$. On a donc, pour n entier naturel :

$$\begin{aligned} AY_n &= A \times (X_n - S) \\ &= AX_n - AS \\ &= AX_n - (S - B) && \text{car } S \text{ est solution de l'équation } AX + B = X. \\ &= AX_n + B - S \\ &= X_{n+1} - S && \text{d'après la relation de récurrence du } \textbf{2. a.} \\ &= Y_{n+1} && \text{d'après la définition de la matrice } Y_n. \end{aligned}$$

On a donc démontré que, pour tout entier naturel n, $Y_{n+1} = AY_n$.

3. **a.** Soit n un entier naturel. On a :

$Z_{n+1} = Y_{2\times(n+1)} = Y_{2n+2} = AY_{2n+1} = A \times (AY_{2n}) = A^2 Y_{2n} = A^2 Z_n$.

Or, on calcule A^2 :
$$\begin{array}{ccc} \times & & \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} & = & \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \end{array}$$

On a donc $A^2 = 2I_2$ et donc $Z_{n+1} = A^2 Z_n = 2I_2 Z_n = 2Z_n$, ce qu'il fallait démontrer.

b. On admet que pout tout entier n on a $Y_{2n} = 2^n Y_0$. En multipliant à gauche par la matrice A, cette égalité devient :

$AY_{2n} = 2^n AY_0$ et, en utilisant la relation de récurrence établie à la question **2. c.**, cela donne bien :

$Y_{2n+1} = 2^n Y_1$.

On en déduit donc, en utilisant $Y_{2n} = 2^n Y_0$, que pour tout entier n, on a :

$\begin{pmatrix} a_{2n} + 400 \\ b_{2n} + 300 \end{pmatrix} = 2^n \begin{pmatrix} a_0 + 400 \\ b_0 + 300 \end{pmatrix} = \begin{pmatrix} 600 \times 2^n \\ 400 \times 2^n \end{pmatrix}$, donc en particulier :

$a_{2n} + 400 = 600 \times 2^n$, soit $a_{2n} = 600 \times 2^n - 400$.

Puis, en utilisant $Y_{2n+1} = 2^n Y_1$, que pour tout entier n, on a :

$\begin{pmatrix} a_{2n+1} + 400 \\ b_{2n+1} + 300 \end{pmatrix} = 2^n \begin{pmatrix} a_1 + 400 \\ b_1 + 300 \end{pmatrix} = \begin{pmatrix} 800 \times 2^n \\ 600 \times 2^n \end{pmatrix}$, donc en particulier :

$a_{2n+1} + 400 = 800 \times 2^n$, soit $a_{2n} = 800 \times 2^n - 400$.

4. **a.** L'algorithme suivant demande un entier p à l'utilisateur, et renvoie dans la variable a qui sera affichée le nombre de poissons dans le bassin A au bout de p années. En effet :

— si p est un nombre pair, alors on affecte à n la valeur $\dfrac{p}{2}$, qui sera donc entière et on a $p = 2n$. On affecte à a la valeur qui est le résultat de la formule pour a_{2n}, c'est à dire a_p, formule établie à la question précédente. Donc si p est pair, à la fin de l'algorithme, a contient le nombre de poissons au bout de p années.

— si p est un nombre impair, alors $p - 1$ est pair et n est l'entier $\dfrac{p-1}{2}$ et donc $2n = p - 1$, soit $p = 2n + 1$. Et comme on affecte à a la valeur obtenue en appliquant la formule obtenue à la question précédente pour calculer a_{2n+1}, à nouveau, la valeur renvoyée sera a_p.

b. On peut modifier de façon assez basique l'algorithme présenté précédemment pour l'inclure dans une boucle :

```
Variables :        a, p et n sont des entiers naturels.
Initialisation :   Affecter à a la valeur 200
                   Affecter à p la valeur 0.
Traitement :       Tant que a ⩽ 10000 :
                      | Affecter à p la valeur p+1
                      | Si p est pair
                      |    | Affecter à n la valeur p/2
                      |    | Affecter à a la valeur 600 × 2^n − 400.
                      | Sinon
                      |    | Affecter à n la valeur (p−1)/2
                      |    | Affecter à a la valeur 800 × 2^n − 400.
                      | Fin de Si.
                   Fin de Tant que
                   Affecter à p la valeur p−1
Sortie :           Afficher p.
```

Cet algorithme initialise les variables a à a_0 et p à 0.

Après chaque itération de la boucle « Tant que », p aura été incrémenté de 1, et la variable a aura été recalculée de sorte qu'elle contient la valeur a_p, donc après n itérations, p contient la valeur n et a contient a_n.

On sort de la boucle « Tant que » dès que la valeur dans a est strictement supérieur à 10 000, c'est à dire le nombre de poissons pour la première année où le bassin A ne suffira plus, nombre d'années qui est contenu dans la variable p, donc le nombre d'années où le bassin A suffit est un de moins que ce qui est contenu dans la variable p, d'où la dernière affectation de p avant la sortie de l'algorithme.

On peut aussi proposer un algorithme un peu plus raffiné : chaque itération de la boucle « Tant que » nous fera passer deux ans au dessus :

```
Variables :        a, p et n sont des entiers naturels.
Initialisation :   Affecter à a la valeur 400
                   Affecter à p la valeur 1.
Traitement :       Tant que a ⩽ 10000 :
                      | Affecter à n la valeur (p+1)/2
                      | Affecter à a la valeur 600 × 2^n − 400.
                      | Si a ⩽ 10000 :
                      |    | Affecter à p la valeur p+1
                      |    | Affecter à n la valeur p/2
                      |    | Affecter à a la valeur 800 × 2^n − 400.
                      |    | Si a ⩽ 10000 :
                      |    |    | Affecter à p la valeur p+1
                      |    | Fin de Si
                      | Fin de Si
Tant que
Sortie :           Afficher p.
```

Ici, on initialise a avec la valeur a_1 et p avec 1. Du coup, on entre dans la boucle « Tant que » avec une valeur p impaire. On commence par calculer a_{p+1} avec la formule utilisée pour les indices pairs (p impair implique $p+1$ pair). a contient donc la valeur a_{p+1}. Si cette valeur reste inférieure à 10000 alors, cela veut dire que l'année $p+1$ reste valable pour le bassin A, donc on affecte cette valeur $p+1$ à la variable p, qui est maintenant paire. On a à ce moment là a qui contient la valeur a_p.

À ce moment, on va calculer a_{p+1} avec la formule utilisée pour les indices impairs (p pair implique $p+1$ pair). a contient donc la valeur a_{p+1}.

Si cette valeur reste inférieure à 10000 alors, cela veut dire que l'année $p+1$ reste valable pour le bassin A, donc on affecte cette valeur $p+1$ à la variable p, qui est redevient impaire. On a à ce moment là a qui contient la valeur a_p.

Exercice II

1. **a.** Traduire par une phrase la probabilité $P_{(X_n=1)}(X_{n+1}=1)$ puis déterminer les probabilités conditionnelles suivantes :

$$P_{(X_n=0)}(X_{n+1}=1), P_{(X_n=1)}(X_{n+1}=1) \text{ et } P_{(X_n=2)}(X_{n+1}=1).$$

> **Solution:** $P_{(X_n=1)}(X_{n+1}=1)$ est la probabilité qu'il y ait exactement une blanche dans l'urne U après le $(n+1)-$ième tirage sachant qu'il y en avait exactement une au $n-$ième tirage
>
> $P_{(X_n=1)}(X_{n+1}=1)=\frac{1}{2}$ car il s'agit de choisir une blanche dans chaque urne avec une probabilité $\frac{1}{4}$ ou de choisir une boule noire dans chaque urne avec une probabilité de $\frac{1}{4}$ pour que la situation reste inchangée.
>
> $P_{(X_n=0)}(X_{n+1}=1)=1$ car cela signifie que U ne contient que des boules noires et que l'on cherche la probabilité que l'urne V nous redonne une blanche (probabilité =1 car V ne contient que des blanches)
>
> $P_{(X_n=2)}(X_{n+1}=1)=1$ car cela signifie que U ne contient que des boules blanches et que l'on cherche la probabilité que l'urne V nous redonne une noire (probabilité =1 car V ne contient que des noires)

b. Exprimer $P(X_{n+1}=1)$ en fonction de $P(X_n=0)$, $P(X_n=1)$ et $P(X_n=2)$.

> **Solution:**
> $(X_n=0)$, $(X_n=1)$ et $(X_n=2)$ forment une partition de l'univers de départ du $(n+1)-$ième tirage on a donc
>
> $$P(X_{n+1}=1)=P\Big((X_{n+1}=1)\cap(X_n=0)\Big)+P\Big((X_{n+1}=1)\cap(X_n=1)\Big)+P\Big((X_{n+1}=1)\cap(X_n=2)\Big)$$
>
> $$=P_{(X_n=0)}(X_{n+1}=1)\times P(X_n=0)+P_{(X_n=1)}(X_{n+1}=1)\times P(X_n=1)+P_{(X_n=2)}(X_{n+1}=1)\times P(X_n=2)$$
>
> $$=P(X_n=0)+\frac{1}{2}P(X_n=1)+P(X_n=2)$$

2. Pour tout entier naturel n non nul, on note R_n la matrice ligne définie par :

$$R_n=\begin{pmatrix}P(X_n=0) & P(X_n=1) & P(X_n=2)\end{pmatrix}$$

et on considère M la matrice $\begin{pmatrix}0 & 1 & 0\\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4}\\ 0 & 1 & 0\end{pmatrix}$.

On note R_0 la matrice ligne $\begin{pmatrix}0 & 0 & 1\end{pmatrix}$.
On admettra par la suite que, pour tout entier naturel n, $R_{n+1}=R_n\times M$.
Déterminer R_1 et justifier que, pour tout entier naturel n, $R_n=R_0\times M^n$.

> **Solution:**
>
> $$R_1=R_0\times M=\begin{pmatrix}0 & 0 & 1\end{pmatrix}\times\begin{pmatrix}0 & 1 & 0\\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4}\\ 0 & 1 & 0\end{pmatrix}=\begin{pmatrix}0 & 1 & 0\end{pmatrix}$$

Démonstration par récurrence de $\forall n \in \mathbb{N}, R_n = R_0 \times M^n$

Initialisation : $M^0 = I_3$ et $R_0 \times I_3 = R_0$

hérédité : supposons que pour tout entier naturel k on ait $R_k = R_0 \times M^k$
Alors $R_{k+1} = R_k \times M = R_0 \times M^k \times M = R_0 \times M^{k+1}$
la propriété est donc héréditaire à partir du rang 0 et vraie au rang 0 donc on a bien d'après le principe de récurrence :
$\forall n \in \mathbb{N}, R_n = R_0 \times M^n$

Solution:
Initialisation: $M^0 = I_3$ et $P \times D^0 \times P^{-1} = P \times I_3 \times P = P \times P^{-1} = I_3$

Hérédité : supposons que pour tout entier naturel k, on ait $M^k = P \times D^k \times P^{-1}$
Alors $M^{k+1} = M^k \times M = R_k \times M = P \times D^k \times P^{-1} \times M = P \times D^k \times P^{-1} \times P \times D \times P^{-1} = P \times D^k \times D \times P^{-1} = P \times D^{k+1} \times P^{-1}$.
La propriété est donc héréditaire à partir du rang 0 et vraie au rang 0 donc on a bien d'après le principe de récurrence :
$\forall n \in \mathbb{N}, M^n = P \times D^n \times P^{-1}$

On admettra que, pour tout entier naturel n, $D^n = \begin{pmatrix} \left(-\frac{1}{2}\right)^n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

4. **a.** Calculer $D^n \times P^{-1}$ en fonction de n.

Solution:

$$D^n \times P^{-1} = \begin{pmatrix} \left(-\frac{1}{2}\right)^n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -2 & 1 \\ 1 & 0 & -1 \\ 1 & 4 & 1 \end{pmatrix} = \begin{pmatrix} \left(-\frac{1}{2}\right)^n & \left(-\frac{1}{2}\right)^{n-1} & \left(-\frac{1}{2}\right)^n \\ 0 & 0 & 0 \\ 1 & 4 & 1 \end{pmatrix}$$

b. Sachant que $R_0 P = \begin{pmatrix} \frac{1}{3} & -\frac{1}{2} & \frac{1}{6} \end{pmatrix}$, déterminer les coefficients de R_n en fonction de n.

Solution:

$$\forall n\in\mathbb{N}, R_n = R_0\times M^n = R_0\times P\times D^n\times P^{-1} = \begin{pmatrix}\frac{1}{3} & -\frac{1}{2} & \frac{1}{6}\end{pmatrix}\times\begin{pmatrix}\left(-\frac{1}{2}\right)^n & \left(-\frac{1}{2}\right)^{n-1} & \left(-\frac{1}{2}\right)^n\\ 0 & 0 & 0\\ 1 & 4 & 1\end{pmatrix}$$

On a donc $R_n = \begin{pmatrix}\frac{1}{3}\left(-\frac{1}{2}\right)^n+\frac{1}{6} & \frac{1}{3}\left(-\frac{1}{2}\right)^{n-1}+\frac{2}{3} & \frac{1}{3}\left(-\frac{1}{2}\right)^n+\frac{1}{6}\end{pmatrix}$

5. Déterminer $\lim\limits_{n\to+\infty} P(X_n=0)$, $\lim\limits_{n\to+\infty} P(X_n=1)$ et $\lim\limits_{n\to+\infty} P(X_n=2)$.
Interpréter ces résultats.

Solution: $\lim\limits_{n\to+\infty}\left(-\frac{1}{2}\right)^n = \lim\limits_{n\to+\infty}\left(-\frac{1}{2}\right)^{n+1} = 0$

Donc par produit et somme $\lim\limits_{n\to+\infty} P(X_n=0) = \lim\limits_{n\to+\infty} P(X_n=2) = \frac{1}{6}$ et $\lim\limits_{n\to+\infty} P(X_n=1) = \frac{2}{3}$

Cela signifie que la probabilité que les urnes se retrouvent dans la situation initiale se stabilise vers $\frac{1}{6}$ quand n devient grand

la probabilité que les urnes soient « monochrome » se stabilise vers $\frac{1}{3}$: $\left(\frac{1}{6}\text{ pour chaque couleur}\right)$

Exercice III

Partie A : quelques résultats

1. On considère l'équation (E) : $9d-26m=1$, où d et m désignent deux entiers relatifs.

a. Les nombres 9 et 26 sont premiers entre eux donc, d'après le théorème de BÉZOUT, l'équation (E) : $9d-26m=1$ admet des solutions entières.

$9\times3-26\times1=1$ donc le couple $(3\,;\,1)$ est solution de l'équation (E).

b. Le couple $(d\,;\,m)$ est solution de (E) si et seulement si $9d-26m=1$
si et seulement si $9d-26m=9\times3-26\times1$
si et seulement si $9(d-3)-26(m-1)=0$
si et seulement si $9(d-3)=26(m-1)$

c. $9(d-3)=26(m-1)$ donc 9 divise $26(m-1)$. Or 9 et 26 sont premiers entre eux donc, d'apèrs le théorème de GAUSS, 9 divise $m-1$. On peut donc écrire $m-1$ sous la forme $9k$ avec $k\in\mathbb{Z}$. Donc $m=9k+1$ avec $k\in\mathbb{Z}$.

$9(d-3)=26(m-1)$ et $m-1=9k$ donc $9(d-3)=26\times9k$ ce qui équivaut à $d-3=26k$ ou encore $d=26k+3$ avec $k\in\mathbb{Z}$.

Réciproquement, si $d=26k+3$ et $m=9k+1$ avec $k\in\mathbb{Z}$, alors
$9d-26m=9(26k+3)-26(9k+1)=9\times26k+27-26\times9k-26=1$ et donc le couple $(d\,;\,m)$ est solution de (E).

Les solutions de l'équation (E) sont donc les couples $(d\,;\,m)$ tels que

$$\begin{cases} d &=& 26k+3\\ m &=& 9k+1\end{cases}\text{, avec } k\in\mathbb{Z}.$$

2. a. Soit n un nombre entier.

$n=26k-1 \iff 26k-n=1 \iff 26k+n(-1)=1$

Il existe donc deux entiers relatifs k et -1 tels que $26k+n(-1)=1$ donc, d'après le théorème de BÉZOUT, les nombres n et 26 sont premiers entre eux.

b. Soit $n=9d-28$, avec $d=26k+3$ et $k\in\mathbb{Z}$.

$n=9d-28=9(26k+3)-28=9\times26k+27-28=26(9k)-1=26K-1$ où $K\in\mathbb{Z}$

D'après la question précédente, on peut déduire que $n=9d-28$ et 26 sont premiers entre eux.

Partie B : cryptage et décryptage

On considère la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$.

1. En cryptant par cette méthode le mot « PION », on obtient « LZWH » ; on veut crypter le mot « ESPION ».

   Les lettres ES correspondent à la matrice colonne $\begin{pmatrix} 4 \\ 18 \end{pmatrix}$; $\begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 36+72 \\ 28+54 \end{pmatrix} = \begin{pmatrix} 108 \\ 82 \end{pmatrix}$

   $\left.\begin{array}{l} 108 = 4 \times 26 + 4 \text{ donc } 108 \equiv 4 \text{ modulo } 26 \\ 82 = 3 \times 26 + 4 \text{ donc } 82 \equiv 4 \text{ modulo } 26 \end{array}\right\}$ donc $\begin{pmatrix} 108 \\ 82 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 4 \end{pmatrix}$ modulo 26 ce qui correspond à EE.

   Le mot ESPION se code donc en EELZWH.

2. **Méthode de décryptage**

   a. $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$; $\det(A) = 9 \times 3 - 4 \times 7 = -1 \neq 0$ donc la matrice A est inversible.

   On trouve son inverse à la calculatrice : $A^{-1} = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}$

   b. Au cryptage, une matrice colonne X correspondant à deux lettres, est d'abord transformée en la matrice Y telle que $AX = Y$. Puis on cherche la matrice Y' composée de nombres entiers entre 0 et 25 et telle que $Y' \equiv Y$ modulo 26.

   Au décryptage, on cherche la matrice colonne Y correspondant aux deux lettres à décrypter. Puis on détermine la matrice X telle que $AX = Y$, autrement dit telle que $X = A^{-1}Y$. Enfin on détermine la matrice colonne X' composée des restes des éléments de X modulo 26.

   Comme $X \equiv X'$ modulo 26, d'après le texte $AX \equiv AX'$ modulo 26 et donc AX et AX' correspondent à la même matrice colonne Y modulo 26 ; ce qui valide le processus de décryptage.

   Pour décrypter les lettres XQ, on cherche la matrice colonne correspondant à ces deux lettres : $\begin{pmatrix} 23 \\ 16 \end{pmatrix}$ puis on multiplie à gauche par la matrice A^{-1}

   $\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \times \begin{pmatrix} 23 \\ 16 \end{pmatrix} = \begin{pmatrix} -3 \times 23 + 4 \times 16 \\ 7 \times 23 - 9 \times 16 \end{pmatrix} = \begin{pmatrix} -5 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 17 \end{pmatrix}$ modulo 26 ce qui correspond à VR.

On fait de même avec GY représenté par $\begin{pmatrix} 6 \\ 24 \end{pmatrix}$:

$\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \times \begin{pmatrix} 6 \\ 24 \end{pmatrix} = \begin{pmatrix} -3 \times 6 + 4 \times 24 \\ 7 \times 6 - 9 \times 24 \end{pmatrix} = \begin{pmatrix} 78 \\ -174 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 8 \end{pmatrix}$ modulo 26 ce qui correspond à AI.

Le mot XQGY se décode en VRAI.