www.freemaths.fr

Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 28

Correction

Partie A. Préliminaires

1.a. Montrons que si $n^2 \equiv N-1 \ (modulo\ N)$ alors $n \times n^3 \equiv 1\ (modulo\ N)$:

Soit *n* et *N* deux entiers supérieurs ou égaux à 2 tels que $n^2 \equiv N-1 \ (modulo\ N)$.

Il est équivalent de dire que $n^2 \equiv -1 \ (modulo\ N)$

La relation de congruence étant compatible avec la multiplication, elle est compatible avec l'élévation au carré.

La congruence $n^2 \equiv -1 \ (modulo\ N)$ implique, en élevant au carré chacun de ses membres, la congruence $(n^2)^2 \equiv (-1)^2 \ (modulo\ N)$ soit $n^4 \equiv 1\ (modulo\ N)$, congruence qui s'écrit, si on le veut ainsi :

$$n \times n^3 \equiv 1\ (modulo\ N).$$

1.b. Déduisons-en un entier k_1 tel que $5k_1 \equiv 1 \ (modulo\ 26)$:

Par un sympathique hasard, le nombre 25 est le carré de 5 et est congru à -1 modulo 26. Nous pouvons appliquer la **question 1.a** avec $N = 26$; $n = 5$.

Nous obtenons : $5 \times 5^3 \equiv 1\ (modulo\ 26)$.

L'entier $k_1 = 5^3 = 125$ vérifie la congruence : $5k_1 \equiv 1 \ (modulo\ 26)$.

NB. L'écriture de la division euclidienne de 125 par 26, à savoir $125 = 4 \times 26 + 21$, montrerait que 21 est le reste de la division. L'entier $k = 21$ est donc l'unique entier compris au sens large entre 0 et 25 qui vérifie la même congruence modulo 26 que l'entier $k_1 = 125$. C'est ce que l'énoncé nous demande « d'admettre ».

2.a. Calculons la matrice $6A - A^2$:

La matrice A^2 est la matrice : $A^2 = \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix}$, nous laissons au lecteur le soin de le vérifier.

Nous obtenons : $6A - A^2 = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix} - \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

La notation *I* désignant la matrice-unité : $\boldsymbol{6A - A^2 = 5I.}$

2.b. Justifions l'inversibilité de la matrice *A* et déterminons sa matrice inverse :

De la relation $6A - A^2 = 5I$ nous pouvons déduire par factorisation :

$$A \times \left[\tfrac{1}{5}(6I - A)\right] = \left[\tfrac{1}{5}(6I - A)\right] \times A = I.$$

Il existe une matrice, en l'occurrence la matrice $\frac{1}{5}(6I - A)$, dont le produit à droite comme à gauche par la matrice *A* est égal à la matrice-unité. Par définition de l'inversibilité d'une matrice :

La matrice *A* est inversible et sa matrice inverse est la matrice $A^{-1} = \frac{1}{5}(6I - A) = \frac{6}{5}I - \frac{1}{5}A$.

Ainsi : $A^{-1} = \alpha I + \beta A$ avec $\alpha = \frac{6}{5}$; $\beta = -\frac{1}{5}$

2.c. Explicitons la matrice inverse de *A* :

$$A^{-1} = \frac{6}{5}I - \frac{1}{5}A = \begin{pmatrix} \frac{6}{5} & 0 \\ 0 & \frac{6}{5} \end{pmatrix} - \begin{pmatrix} \frac{4}{5} & \frac{1}{5} \\ \frac{3}{5} & \frac{2}{5} \end{pmatrix} = \begin{pmatrix} \frac{2}{5} & -\frac{1}{5} \\ -\frac{3}{5} & \frac{4}{5} \end{pmatrix}.$$

Vérifions son lien avec *B* :

$$5A^{-1} = 5 \times \begin{pmatrix} \frac{2}{5} & -\frac{1}{5} \\ -\frac{3}{5} & \frac{4}{5} \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = B.$$

2.d. Montrons que si *AX = Y* alors 5*X = BY* :

X est une matrice-colonne de deux lignes, *Y* est la matrice-colonne de deux lignes telle que $AX = Y$.

Multiplions les deux membres de cette dernière égalité par la matrice *B* : $B \times (AX) = BY$.

Par associativité du produit matriciel : $B \times (AX) = (BA) \times X = (5I) \times X = 5X$.

Si *AX = Y* alors 5*X = BY*.

Partie B. Procédure de codage

Codons le mot « ET » :

En quatre étapes…

E1. Associons à l'aide du tableau de correspondance qui nous est fourni la matrice-colonne des deux nombres associés aux deux lettres E et T :

Dans le tableau, les lettres E et T sont codées respectivement par les nombres 4 et 19.

Au mot « ST » nous associons la matrice-colonne : $X_{ET} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$

E2 : Transformons la matrice $X_{ET} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y_{ET} = A \times X_{ET}$:

Nous effectuons le produit matriciel : $\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} \times \begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 16+19 \\ 12+38 \end{pmatrix} = \begin{pmatrix} 35 \\ 50 \end{pmatrix}$

Ainsi : $Y_{ET} = \begin{pmatrix} 35 \\ 50 \end{pmatrix}$

E3 : Transformons la matrice $Y_{ET} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ en la matrice $R_{ET} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ des restes des divisions euclidiennes par 26 des nombres en jeu :

Nous nous aidons des divisions euclidiennes : $35 = 1 \times 26 + 9$; $50 = 1 \times 26 + 24$

Pour le mot « ST» : $r_1 = 9$; $r_2 = 24$. Donc $R_{ET} = \begin{pmatrix} 9 \\ 24 \end{pmatrix}$

E4 : Associons aux entiers r_1 et r_2 en jeu les lettres lues dans le tableau de correspondance.

Dans le tableau, nous lisons que 9 est associé à la lettre J et 24 est associé à la lettre Y.

Conclusion : Le mot « ET » est codé par le mot « JY »

Partie C. Procédure de décodage

X est la matrice-colonne $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et *Y = AX*

1. Montrons que $\begin{cases} \mathbf{5x_1 = 2y_1 - y_2} \\ \mathbf{5x_2 = -3y_1 + 4y_2} \end{cases}$ **:**

Nous avons vu dans la **question A.2.d** que, si *Y = AX*, alors 5*X = BY*. Explicitons cette dernière égalité.

$$5X = \begin{pmatrix} 5x_1 \\ 5x_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2y_1 - y_2 \\ -3y_1 + 4y_2 \end{pmatrix}$$

En identifiant terme à terme chacune des deux lignes des deux vecteurs-colonnes, nous obtenons effectivement :

$$\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$$

2. Etablissons que $\begin{cases} \boldsymbol{x_1 \equiv 16y_1 + 5y_2} \\ \boldsymbol{x_2 \equiv 15y_1 + 6y_2} \end{cases}$ $\boldsymbol{(modulo\ 26)}$ **:**

Dans la **question A.1.b** de l'exercice, nous avons vu un entier dont le produit avec 5 est congru à 1 modulo 26, à savoir le nombre 21 (résultat « admis » par l'énoncé).

Si nous multiplions par 21 chacun des membres de ces congruences, nous allons neutraliser le coefficient 5 figurant dans ces congruences.

Effectuons les calculs :

$$\begin{cases} 21 \times 5x_1 \equiv 21 \times (2y_1 - y_2) \\ 21 \times 5x_2 \equiv 21 \times (-3y_1 + 4y_2) \end{cases} (mod\ 26) \text{ soit : } \begin{cases} 21 \times 5x_1 \equiv 42y_1 - 21y_2 \\ 21 \times 5x_2 \equiv -63y_1 + 84y_2 \end{cases} (mod\ 26)$$

Exploitons la congruence $21 \times 5 \equiv 1\ (mod\ 26)$. En outre, les divisions euclidiennes $42 = 1 \times 26 + 16,\ -21 = (-1) \times 26 + 5,\ -63 = (-3) \times 26 + 15$ et $84 = 3 \times 26 + 6$ justifient les congruences $42 \equiv 16\ (mod\ 26)$, $-21 \equiv 5\ (mod\ 26)$, $-63 \equiv 15\ (mod\ 26)$ ainsi que $84 \equiv 6\ (mod\ 26)$.

Nous pouvons exploiter ces congruences dans l'écriture du système de congruences que nous avons trouvé.

Nous obtenons bien : $\begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_2 \equiv 15y_1 + 6y_2 \end{cases} (modulo\ 26)$.

Si (x_1, x_2) et (y_1, y_2) sont deux couples liés par les congruences modulo 26 du système de codage, ils sont aussi liés par les congruences du système $\begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_2 \equiv 15y_1 + 6y_2 \end{cases} (modulo\ 26)$.

Nous pouvons ainsi affirmer que ce système de congruences modulo 26 permet de décoder les mots codés par le système de codage.

3. Décodons le mot « QP » :

Selon le tableau de correspondance, les lettres Q et P sont associées respectivement aux nombres $y_1 = 16\,;\ y_2 = 15$

En appliquant au couple $(16, 15)$les formules de décodage nous obtiendrons modulo 26 son couple homologue (x_1, x_2).

En l'occurrence : $\begin{cases} x_1 \equiv 16 \times 16 + 5 \times 15 \\ x_2 \equiv 15 \times 16 + 6 \times 15 \end{cases} (mod\ 26)$ soit : $\begin{cases} x_1 \equiv 331 \\ x_2 \equiv 330 \end{cases} (mod\ 26)$

En écrivant les divisions euclidiennes de 331 et de 330 par 26 et en retenant les restes de ces divisions, nous obtenons le couple homologue recherché.

Des divisions euclidiennes : $331 = 12 \times 26 + 19$ et $330 = 12 \times 26 + 18$, nous déduisons : $(x_1, x_2) = (19,\ 18)$.

Les nombres 19 et 18 sont associés respectivement aux lettres Tet S.

Le mot « QP » code le mot « TS ».

NB. Il est possible de vérifier notre réponse en recodant le mot « TS » selon les formules de codage :

$\begin{cases} y_1 \equiv 4 \times 19 + 18 \\ y_2 \equiv 3 \times 19 + 2 \times 18 \end{cases} (mod\ 26)$ soit $\begin{cases} y_1 \equiv 94 \\ y_2 \equiv 93 \end{cases} (mod\ 26)$

Or : $94 = 3 \times 26 + 16$ et $93 = 3 \times 26 + 15$.

Nous retrouvons bien comme codage le couple prévu $(16, 15)$.