www.freemaths.fr

Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 21

Correction

Partie A : Le chiffrement de Hill

Développons les différentes étapes telles qu'elles sont décrites dans l'énoncé afin de chiffrer le mot « HILL » :

Etape 1 : Divisons le mot « HILL » en deux blocs de deux lettres.

Les deux blocs sont « HI » et « LL »

Etape 2 : Associons à l'aide du tableau de correspondance qui nous est fourni une matrice-colonne de deux nombres aux deux lettres de chaque bloc.

Dans le tableau, les lettres H, I et L sont codées respectivement par les nombres 7, 8 et 11.

Au bloc « HI » nous associons la matrice-colonne : $X_{HI} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$

Au bloc « LL » nous associons la matrice-colonne : $X_{LL} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$

Etape 3 : Transformons la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y = A \times X$.

Nous effectuons pour cela les produits matriciels :

$$\begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \times \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 35 + 16 \\ 49 + 56 \end{pmatrix} = \begin{pmatrix} 51 \\ 105 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \times \begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 55 + 22 \\ 77 + 77 \end{pmatrix} = \begin{pmatrix} 771 \\ 154 \end{pmatrix}$$

Pour le bloc « HI » : $Y_{HI} = \begin{pmatrix} 51 \\ 105 \end{pmatrix}$

Pour le bloc « LL » : $Y_{LL} = \begin{pmatrix} 77 \\ 154 \end{pmatrix}$

Etape 4 : Transformons, pour chaque bloc, la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ des restes des divisions euclidiennes par 26 des nombres en jeu.

Pour cela, nous nous aidons des divisions euclidiennes suivantes :

$$51 = 1 \times 26 + 25 \quad ; \quad 105 = 4 \times 26 + 1$$

$$77 = 2 \times 26 + 25 \quad ; \quad 154 = 5 \times 26 + 24$$

Pour le bloc « HI » : $r_1 = 25$; $r_2 = 1$. Donc $R_{HI} = \begin{pmatrix} 25 \\ 1 \end{pmatrix}$

Pour le bloc « LL »: $r_1 = 25$; $r_2 = 2$. Donc $R_{LL} = \begin{pmatrix} 25 \\ 24 \end{pmatrix}$

Etape 5 : Associons aux entiers r_1 et r_2 en jeu les lettres lues dans le tableau de l'étape 2.

Dans le tableau, nous lisons que 1 est associé à la lettre B, 24 est associé à la lettre Y et 25 est associé à la lettre Z.

Nous codons le bloc « HI » par le bloc « ZB ».

Nous codons le bloc « LL » par le bloc « ZY ».

En conclusion, le mot « HILL » est chiffré par le mot « ZBZY »

Partie B : Quelques outils mathématiques nécessaires au déchiffrement

1. Montrons que, si un entier relatif *a* est premier avec 26, alors il existe un entier relatif *u* tel que $u \times a \equiv 1\ (26)$:

Si un entier relatif *a* est premier avec 26, alors les entiers *a* et 26 vérifient les hypothèses du théorème de Bézout, nous pouvons appliquer ce théorème.

Il existe deux entiers relatifs *u* et *v* tels que : $u \times a + v \times 26 = 1$.

Appliquons aux termes de cette égalité la congruence modulo 26 : $u \times a + v \times 26 \equiv 1\ (26)$.
Le nombre $v \times 26$ étant un multiple de 26, ce nombre est congru à 0 modulo 26 et en conséquence :

$$u \times a + v \times 26 \equiv u \times a\ (26).$$

La congruence modulo 26 étant une relation transitive, si deux entiers sont congrus à un même troisième, ils sont congrus entre eux.

Nous obtenons : $u \times a \equiv 1\ (26)$.

Nous avons bien trouvé un entier relatif *u* vérifiant la propriété demandée.

2.a. Reproduisons le tableau tout en le complétant :

u	0	1	2	3	4	5
r	0	21	16	11	6	1

L'arrêt de l'algorithme se produit lorsque $u = 5$.

2.b. Vérifions que $5 \times 21 \equiv 1 \ (26)$:

La produit 5×21 est égal à 105 et la division euclidienne de 105 par 21 s'écrit : $105 = 4 \times 26 + 1$.

Appliquons aux termes de cette égalité la congruence modulo 26 : $105 \equiv 1 \ (26)$.

Nous obtenons bien : $5 \times 21 \equiv 1 \ (26)$.

NB. Dans une congruence modulo *n*, nous pouvons toujours remplacer un nombre par le reste de sa division euclidienne par *n*. Le reste de la division euclidienne de 5×21 par 26 étant égal à 1, c'est pourquoi le nombre 5×21 est congru à 1 modulo 26.

Le résultat que nous obtenons est confirmé par l'arrêt pour la valeur 5 de l'algorithme décrit dans l'énoncé, rédigé ci-dessous avec Python :

```
>>> def hill(a):
        u=0
        r=0
        while r!=1:
            u=u+1
            r=a*u%26
        print ("la valeur de u est", u)


>>> hill(21)
la valeur de u est 5
```

NB. *Nous avons montré qu'il existe au moins un entier u vérifiant :* $u \times a \equiv 1 \ (26)$. *Puisque tel est le cas, le reste r de la division euclidienne de u par* 26 *vérifie lui aussi cette même propriété car :* $u \equiv r \ (26)$. *Parmi tous les entiers vérifiant* $u \times a \equiv 1 \ (26)$ *il en existe un qui est compris entre* 1 *et* 25 (*ce reste ne peut être* 0). *L'algorithme rédigé dans l'énoncé et que nous avons reproduit avec Python cherche cet entier.*

3.a. Calculons la matrice $12A$-A^2 :

D'une part $12A = \begin{pmatrix} 60 & 24 \\ 84 & 84 \end{pmatrix}$ et d'autre part $A^2 = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \times \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 39 & 24 \\ 84 & 63 \end{pmatrix}$

Donc : $12A - A^2 = \begin{pmatrix} 21 & 0 \\ 0 & 21 \end{pmatrix}$

3.b. Déduisons du 3.a la matrice *B* recherchée :

D'après le résultat de **3.a** : $12A - A^2 = 21 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 21I$

C'est-à-dire que : $(12I - A) \times A = 21I$

Effectuons le calcul : $12I - A = \begin{pmatrix} 12 & 0 \\ 0 & 12 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 12-5 & 0-2 \\ 0-7 & 12-7 \end{pmatrix}$

.

La matrice *B* telle que *BA* = 21*I* est la matrice : $B = 12I - A = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix}$

3.c. Montrons que si *AX=Y* alors 21*X*= *BY* :

Supposons que *AX=Y*.

Multiplions à gauche chaque membre de cette égalité par la matrice *B*.
Ecrivons ainsi que : *B*×(*AX*) = *B*×*Y*.

Regardons ce qu'il se passe au premier membre.
D'après la propriété d'associativité de la multiplication des matrices : *B*×(*AX*) = (*BA*)×*X*

D'après la propriété caractéristique de la matrice B vue au 3.b : $BA = 21I$

Donc $BY = B \times (AX) = (BA) \times X = (21I) \times X = 21(I \times X) = 21X$

Si *AX* = *Y*, alors nous obtenons bien : 21*X* = *B*×*Y*

Partie C : Déchiffrement

Déchiffrons le mot « VLUP » :

Lors de son chiffrement, le mot chiffré par « VLUP » a été découpé en deux blocs de deux lettres (étape 1) puis une matrice-colonne $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ constituée de deux entiers compris entre 0 et 25 a été associée à chacun de ces deux blocs (étape 2) comme l'indique l'énoncé.

Selon l'énoncé, la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ désigne la matrice *Y* = *A*×*X*.

1. Démontrons que $\begin{cases} \mathbf{21x_1 = 7y_1 - 2y_2} \\ \mathbf{21x_2 = -7y_1 + 5y_2} \end{cases}$ **:**

Pour chacun des deux blocs, l'étape 3 a transformé la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ telle que : $Y = A \times X$.

Mais si $Y = A \times X$, alors d'après la question B.3.c : $21X = B \times Y$. Autrement dit, vu que la matrice B est la matrice $= \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix}$, nous avons : $21\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$

Effectuons ces produits matriciels : $\begin{pmatrix} 21x_1 \\ 21y_2 \end{pmatrix} = \begin{pmatrix} 7y_1 - 2y_2 \\ -7y_1 + 5y_2 \end{pmatrix}$

Deux matrices sont égales si et seulement si leurs éléments homologues sont égaux.

Nous obtenons bien que : $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$

2. Etablissons que $\begin{cases} \mathbf{x_1 \equiv 9r_1 + 16r_2 \ (26)} \\ \mathbf{x_2 \equiv 17r_1 + 25r_2 \ (26)} \end{cases}$ **:**

Appliquons aux égalités précédentes la congruence modulo 26 : $\begin{cases} 21x_1 \equiv 7y_1 - 2y_2 \ (26) \\ 21x_2 \equiv -7y_1 + 5y_2 \ (26) \end{cases}$

Si r_1 et r_2 sont les restes des divisions euclidiennes de y_1 et de y_2 par 26, nous avons $y_1 \equiv r_1 \ (26)$ et $y_2 \equiv r_2 \ (26)$ donc : $\begin{cases} 21x_1 \equiv 7r_1 - 2r_2 \ (26) \\ 21x_2 \equiv -7r_1 + 5r_2 \ (26) \end{cases}$

Nous avons montré en B.2.b que : $5 \times 21 \equiv 1 \ (26)$. Multiplions par 5 les termes de ces deux congruences : $\begin{cases} 5 \times 21x_1 \equiv 5 \times (7r_1 - 2r_2) \ (26) \\ 5 \times 21x_2 \equiv 5 \times (-7r_1 + 5r_2) \ (26) \end{cases}$ soit : $\begin{cases} x_1 \equiv 35r_1 - 10r_2 \ (26) \\ x_2 \equiv -35r_1 + 25r_2 \ (26) \end{cases}$.

Or : $35 = 9 + 26$ donc $35 \equiv 9 \ (26)$ et $-10 = 16 - 26$ donc $-10 \equiv 16 \ (26)$.

Et aussi : $-35 = 17 - 52 = 17 - 2 \times 26$ donc : $-35 \equiv 17 \ (26)$.

Exploitons ces congruences dans les relations précédentes $\begin{cases} x_1 \equiv 35r_1 - 10r_2 \ (26) \\ x_2 \equiv -35r_1 + 25r_2 \ (26) \end{cases}$:

Nous obtenons bien : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \ (26) \\ x_2 \equiv 17r_1 + 25r_2 \ (26) \end{cases}$

3. Déchiffrons les « mots » associés aux matrices $\begin{pmatrix}21\\11\end{pmatrix}$ et $\begin{pmatrix}20\\15\end{pmatrix}$:

Selon le tableau de correspondance, les lettres V, L, U, P son associées respectivement aux nombres 21, 11, 20 et 15. Pour le premier bloc de deux lettres, nous avons $r_1 = 21$; $r_2 = 11$ et pour le deuxième bloc de deux lettres, nous avons $r_1 = 20$; $r_2 = 15$.

Déchiffrons le mot associé à la matrice $\begin{pmatrix}21\\11\end{pmatrix}$:

Dans ce cas, $9r_1 + 16r_2 = 9 \times 21 + 16 \times 11 = 365$ et : $17r_1 + 25r_2 = 17 \times 21 + 25 \times 11 = 632$.

Donc : $\begin{cases} x_1 \equiv 365 \ (26) \\ x_2 \equiv 632 \ (26) \end{cases}$. Puisque les entiers x_1 et x_2 sont compris entre 0 et 25, il s'agit des restes des divisions euclidiennes de 365 et de 632 par 26.

Effectuons les divisions euclidiennes de 365 et de 632 par 26 :
$365 = 14 \times 26 + 1$ et $632 = 24 \times 26 + 8$.

365 est congru à 1 modulo 26 et 632 est congru à 8 modulo 26. Il en résulte que : $\begin{cases} x_1 \equiv 1 \ (26) \\ x_2 \equiv 8 \ (26) \end{cases}$.

Selon le tableau de correspondance, 1 et 8 sont associés respectivement aux lettres B et I.

Le bloc « VL » chiffre le bloc « BI »

Déchiffrons le mot associé à la matrice $\begin{pmatrix}20\\15\end{pmatrix}$:

$9r_1 + 16r_2 = 9 \times 20 + 16 \times 15 = 420$ et : $17r_1 + 25r_2 = 17 \times 20 + 25 \times 15 = 715$.

Donc : $\begin{cases} x_1 \equiv 420 \ (26) \\ x_2 \equiv 715 \ (26) \end{cases}$

Effectuons les divisions euclidiennes de 420 et de 715 par 26 :

$420 = 16 \times 26 + 4$ et : $715 = 27 \times 26 + 13$

420 est congru à 4 modulo 26 et 715 est congru à 13 modulo 26.

Il en résulte que : $\begin{cases} x_1 \equiv 4 \ (26) \\ x_2 \equiv 13 \ (26) \end{cases}$.

Selon le tableau de correspondance, 4 et 13 sont associés respectivement aux lettres E et N.

Le bloc « UP » chiffre le bloc « EN »

En conclusion, le mot que nous devions déchiffrer est le mot « BIEN ».