www.freemaths.fr

Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 25

Correction

Partie A.

Soit *a, b, c* et *d* des entiers relatifs et soit *n* un entier naturel non nul.

Montrons que, si $a \equiv b \pmod{n}$ et si $c \equiv d \pmod{n}$, alors $a \times c \equiv b \times d \pmod{n}$:

- Si $a \equiv b \pmod{n}$, alors il existe un entier relatif *k* tel que : $a = b + kn$.
- Si $c \equiv d \pmod{n}$, alors il existe un entier relatif *k'* tel que : $c = d + k'n$.

Supposons ces deux congruences simultanément vérifiées.

Des deux relations $\begin{cases} a = b + kn \\ c = d + k'n \end{cases}$ nous pouvons déduire par multiplication membre à membre la relation : $a \times c = (b + kn) \times (d + k'n)$.

Développons l'expression figurant au second membre : $ac = bd + (kn)d + b(k'n) + (kn)(k'n)$.

Nous pouvons factoriser *n* dans trois des termes figurant au second membre :
$ac = bd + (kd + k'b + kk'n)n$.

Le nombre $K = kd + k'b + kk'n$ est un nombre entier relatif en tant que cocktail (additions et multiplications uniquement) d'entiers relatifs. Il existe donc un entier relatif *K* tel que $ac = bd + Kn$.
Compte tenu de cette existence, par définition de la congruence modulo *n* :

$$ac \equiv bd \pmod{n}$$

Si $a \equiv b \pmod{n}$ et si $c \equiv d \pmod{n}$, alors $ac \equiv bd \pmod{n}$

Nous venons de démontrer que la relation de congruence modulo *n* dans l'ensemble des entiers relatifs est compatible avec la multiplication des entiers relatifs.

Partie B. Inverse de 23 modulo 26.

L'équation (E) dont il est question est l'équation $23x - 26y = 1$ dans l'ensemble $\mathbb{Z} \times \mathbb{Z}$. On note que 23 et 26 sont des entiers premiers entre eux. Résoudre cette équation revient à rechercher quels sont les entiers *x* et *y* satisfaisant, à l'égard de 23 et 26, l'égalité de Bézout.

1. Vérifions que le couple $(-9\ ;\ -8)$ est solution de l'équation (E) :

$23 \times (-9) - 26 \times (-8) = -217 + 218 = 1$

Le couple $(-9\ ;\ -8)$ est bien solution de l'équation (E).

2. Résolvons l'équation (E) :

NB. Soit *a, b, c* trois entiers relatifs non nuls, les entiers *a* et *b* étant premiers entre eux.
La méthode générale de résolution dans l'ensemble $\mathbb{Z} \times \mathbb{Z}$ de l'équation $ax - by = c$ **(E)** quand on en connaît déjà un couple solution $(x_0,\ y_0)$ particulier est la suivante :

- Un couple $(x,\ y)$ est solution de **(E)** si et seulement si le couple $(x - x_0,\ y - y_0)$ est solution de l'équation $aX - bY = 0$ **(H)**, équation dite « homogène » ou « sans second membre » qui a pour solutions les couples de la forme $(kb,\ ka)$ *k* est un entier relatif[1].
- Les couples solutions de **(E)** sont les couples de la forme : $(x_0 + kb,\ y_0 + ka)$ où *k* est un entier relatif.

En l'occurrence, nous disposons du couple solution particulier $(x_0 = -9\ ;\ y_0 = -8)$.

Un couple $(x,\ y)$ est solution de l'équation **(E)** si et seulement si le couple $(X = x + 9,\ Y = y + 8)$ est solution de l'équation $23X - 26Y = 0$, équation qui a pour solutions les couples de la forme $(26k,\ 23k)$ où *k* est un entier relatif.

Un couple d'entiers relatifs $(x,\ y)$ est solution de l'équation **(E)** si et seulement s'il existe un entier relatif *k* tel que $\begin{cases} x + 9 = 26k \\ y + 8 = 23k \end{cases}$.

Les couples solutions de l'équation **(E)** sont les couples de la forme $(-9 + 26k,\ -8 + 23k)$ où *k* est un entier relatif.

3. Déduisons-en un entier *a* compris entre 0 et 25 tel que $23a \equiv 1\ (mod\ 26)$:

Pour cela, distinguons parmi les couples $(x_k = -9 + 26k,\ y_k = -8 + 23k)$ solutions de (E) celui (il y en a un et un seul) où le nombre x_k est compris entre 0 et 25.
Il s'agit du couple $(x_1 = -9 + 26 = 17,\ y_1 = -8 + 23 = 15)$.

Ce couple vérifie, en raison de son statut de solution de (E) : $23 \times 17 - 26 \times 15 = 1$.

Appliquons à cette égalité la congruence modulo 26 : $23 \times 17 \equiv 1\ (mod\ 26)$

L'entier $a = 17$ est compris entre 0 et 25 et vérifie la congruence : $23 \times 17 \equiv 1\ (mod\ 26)$

[1] **Pour mémoire, résolution de l'équation homogène $aX - bY = 0$.** Soit (*X, Y*) un couple solution. L'entier *a* divise *bY* et est premier avec *b*, donc il divise *Y* (théorème de Gauss). Il existe un entier relatif *k* tel que $Y = ka$. De ce fait : $aX = b \times (ka)$ d'où on déduit, puisque *a* est non nul, $X = kb$. Le couple (X, Y) est nécessairement de la forme (ka, kb) où *k* est un entier relatif. Réciproquement, on vérifie sans peine qu'un couple de cette forme est solution de l'équation $aX - bY = 0$.

NB. Nous pouvons vérifier que notre réponse est correcte : $23 \times 17 = 391 = 15 \times 26 + 1$, le reste de la division euclidienne de 391 par 26 est bien égal à 1. Cet entier 17 est « l'inverse de 23 modulo 26 », selon les termes de l'énoncé.

Partie C. Le chiffrement de Hill.

1. Codons le mot de deux lettres « ST » :

Pour cette question, nous allons utiliser une méthode matricielle pour effectuer certaines des étapes du codage. À cet effet, remarquons que les formules $\begin{cases} y_1 = 11x_1 + 3x_2 \\ y_2 = 7x_1 + 4x_2 \end{cases}$ peuvent être représentées matriciellement par l'action, modulo 26, de la matrice $A = \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$ sur la matrice-colonne $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Nous avons ici : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

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

Dans le tableau, les lettres S et T sont codées respectivement par les nombres 18 et 19.

Au mot « ST » nous associons la matrice-colonne : $X_{ST} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 18 \\ 19 \end{pmatrix}$

E2 : Transformons la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y = A \times X$:

Nous effectuons le produit matriciel : $\begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix} \times \begin{pmatrix} 18 \\ 19 \end{pmatrix} = \begin{pmatrix} 198 + 57 \\ 126 + 76 \end{pmatrix} = \begin{pmatrix} 255 \\ 202 \end{pmatrix}$

Ainsi : $Y_{ST} = \begin{pmatrix} 255 \\ 202 \end{pmatrix}$

E3 : Transformons 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 :

Nous nous aidons des divisions euclidiennes : $255 = 9 \times 26 + 21$; $202 = 7 \times 26 + 2$.

Pour le mot « ST» : $r_1 = 21$; $r_2 = 20$. Donc $R_{ST} = \begin{pmatrix} 21 \\ 20 \end{pmatrix}$

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 21 est associé à la lettre V et 20 est associé à la lettre U.

Conclusion : Le mot « ST » est codé par le mot « VU ».

2.a. Montrons que tout couple vérifiant les équations de (S_1) vérifie les équations de (S_2) :

Soit (x_1, x_2) et (y_1, y_2) deux couples liés par les congruences modulo 26 du système (S_1), c'est-à-dire les deux congruences $\begin{cases} y_1 \equiv 11x_1 + 3x_2 \\ y_2 \equiv 7x_1 + 4x_2 \end{cases} (mod\ 26)$

Alors : $\begin{cases} 4y_1 + 23y_2 \equiv 4 \times (11x_1 + 3x_2) + 23 \times (7x_1 + 4x_2) \\ 19y_1 + 11y_2 \equiv 19 \times (11x_1 + 3x_2) + 11 \times (7x_1 + 4x_2) \end{cases} (mod\ 26).$

Effectuons les opérations : $\begin{cases} 4y_1 + 23y_2 \equiv 205x_1 + 104x_2 \\ 19y_1 + 11y_2 \equiv 286x_1 + 101x_2 \end{cases} (mod\ 26)$

Or, 104 et 286 sont deux multiples de 26 tandis que $101 = 3 \times 26 + 23$ et $205 = 7 \times 26 + 23$.

En conséquence : $\begin{cases} 4y_1 + 23y_2 \equiv 23x_1 \\ 19y_1 + 11y_2 \equiv 23x_2 \end{cases} (mod\ 26)$. Nous reconnaissons le système (S_2).

Si (x_1, x_2) et (y_1, y_2) sont deux couples liés par les congruences modulo 26 du système (S_1), alors ils sont aussi liés par les congruences modulo 26 du système (S_2).

2.b. Montrons que tout couple vérifiant les équations de (S_2) vérifie les équations de (S_3) :

Soit (x_1, x_2) et (y_1, y_2) deux couples liés par les congruences modulo 26 du système (S_2), c'est-à-dire les deux congruences $\begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \\ 23x_2 \equiv 19y_1 + 11y_2 \end{cases} (mod\ 26)$

Dans la **partie B** de l'exercice, nous avons déterminé « l'inverse modulo 26 de 23 », à savoir le nombre 17. Si nous multiplions par 17 chacun des membres de ces congruences, nous allons neutraliser le coefficient 23 figurant dans ces congruences.

Effectuons les calculs relatifs à la multiplication par 17 des deux congruences :

$\begin{cases} 17 \times 23x_1 \equiv 17 \times (4y_1 + 23y_2) \\ 17 \times 23x_2 \equiv 17 \times (19y_1 + 11y_2) \end{cases} (mod\ 26)$ soit : $\begin{cases} 17 \times 23x_1 \equiv 68y_1 + 17 \times 23y_2 \\ 17 \times 23x_2 \equiv 323y_1 + 187y_2 \end{cases} (mod\ 26)$

Nous savons que $17 \times 23 \equiv 1\ (mod\ 26)$.
De plus, les divisions euclidiennes $68 = 2 \times 26 + 16,\ 323 = 12 \times 26 + 11$ et $187 = 7 \times 26 + 5$ justifient les congruences $68 \equiv 16\ (mod\ 26)$, $323 \equiv 11\ (mod\ 26)$ et $187 \equiv 5\ (mod\ 26)$.

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

Nous obtenons : $\begin{cases} x_1 \equiv 16y_1 + y_2 \\ x_2 \equiv 11y_1 + 5y_2 \end{cases} (mod\ 26)$. Il s'agit bien du système (S_3).

Si (x_1, x_2) et (y_1, y_2) sont deux couples liés par les congruences modulo 26 du système (S_2), alors ils sont aussi liés par les congruences modulo 26 du système (S_3).

En conclusion des questions 2.a et 2.b, si (y_1, y_2) est un couple qui s'exprime en fonction de (x_1, x_2) à l'aide des équations du système (S_1), alors le couple (x_1, x_2) s'exprime en fonction de (y_1, y_2) à l'aide des équations du système (S_3).

2.c. Montrons que tout couple vérifiant les équations de (S_3) vérifie les équations de (S_1) :

Soit (x_1, x_2) et (y_1, y_2) deux couples liés par les congruences modulo 26 du système (S_3), c'est-à-dire les deux congruences : $\begin{cases} x_1 \equiv 16y_1 + y_2 \\ x_2 \equiv 11y_1 + 5y_2 \end{cases} (mod\ 26)$

Appliquons au couple (x_1, x_2) en jeu les formules décrites par le système (S_1).

$\begin{cases} 11x_1 + 3x_2 \equiv 11(16y_1 + y_2) + 3(11y_1 + 5y_2) \\ 7x_1 + 4x_2 \equiv 7(16y_1 + y_2) + 4(11y_1 + 5y_2) \end{cases} (mod\ 26)$ soit

$\begin{cases} 11x_1 + 3x_2 \equiv 209y_1 + 26y_2 \\ 7x_1 + 4x_2 \equiv 156y_1 + 27y_2 \end{cases} (mod\ 26).$

Or, 26 et 156 sont des multiples de 26 tandis que 27 et 209 sont congrus à 1 modulo 26.

Nous obtenons $\begin{cases} 11x_1 + 3x_2 \equiv y_1 \\ 7x_1 + 4x_2 \equiv y_2 \end{cases} (mod\ 26)$, il s'agit bien du système (S_1).

Si réciproquement (x_1, x_2) et (y_1, y_2) sont deux couples liés par les congruences modulo 26 du système (S_3), ils sont aussi liés par les congruences modulo 26 du système (S_1).

Nous pouvons ainsi affirmer que les congruences modulo 26 du système (S_3) décodent les mots codés par celles du système (S_1) et seulement ceux-là.

2.d. Décodons le mot « YJ » :

Selon le tableau de correspondance, les lettres Y et N sont associées respectivement aux nombres $y_1 = 24$; $y_2 = 9$. En appliquant au couple $(24, 9)$ les formules décrites par le système (S_3), nous obtenons modulo 26 son couple homologue (x_1, x_2).

En l'occurrence : $\begin{cases} x_1 \equiv 16 \times 24 + 9 \\ x_2 \equiv 11 \times 24 + 5 \times 9 \end{cases} (mod\ 26)$ soit : $\begin{cases} x_1 \equiv 393 \\ x_2 \equiv 309 \end{cases} (mod\ 26)$

En écrivant les divisions euclidiennes de 393 et de 309 par 26 et en retenant les restes de ces divisions, nous obtenons le couple homologue recherché.
Des divisions euclidiennes : $393 = 15 \times 26 + 3$ et $309 = 11 \times 26 + 23$, nous déduisons :
$(x_1, x_2) = (3,\ 23)$.
Les nombres 23 et 3 sont associés respectivement aux lettres D et X.

Le mot « YN » chiffre le mot « DX ».

NB. Nous nous attendions à un mot qui ait un sens dans la langue française, ce n'est pas le cas. Par acquis de conscience, il est possible de vérifier notre réponse en recodant le mot « DX » :

$\begin{cases} y_1 \equiv 11 \times 3 + 3 \times 23 \\ y_2 \equiv 7 \times 3 + 4 \times 23 \end{cases} (mod\ 26)$ soit $\begin{cases} y_1 \equiv 102 \\ y_2 \equiv 113 \end{cases} (mod\ 26)$

Or : $102 = 3 \times 26 + 24$ et $113 = 4 \times 26 + 9$.

Nous retrouvons bien comme codage numérique du couple $(3, 23)$ le couple prévu $(24, 9)$.