www.freemaths.fr

Maths Expertes Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 36

Correction

Soit a et b deux entiers naturels fixés. Une fois pour toutes, nous allons noter $f_{a,b}$ l'application de l'ensemble $\Omega = \{0\,; 1; \dots; 25\}$ vers $\mathbb{N}$ qui, à chaque élément n de Ω, associe le nombre entier naturel $an + b$ et par $r_{a,b}$ l'application de l'ensemble $\Omega = \{0\,; 1; \dots; 25\}$ vers lui-même qui à chaque élément n de Ω associe le reste de la division euclidienne de $an + b$ par 26.

1. Disons quelque chose si $a = 0$:

Si $a = 0$, quel que soit b fixé, l'application $f_{0,b}$ est l'application constante qui, à tout élément n de Ω associe l'entier naturel b et $r_{a,b}$ est l'application constante qui, à tout élément n de Ω associe le reste de la division euclidienne de n par b.

Si $a = 0$, toutes les lettres de l'alphabet sont « codées » (sic) par une seule et même lettre.

On ne peut guère parler de « codage » dans ces conditions …

2. Montrons que, si on choisit $a = 13$, les lettres A et C sont codées par la même lettre :

Les lettres A et C sont associées aux éléments 0 et 2 de Ω.

Or, quel que soit l'entier naturel b fixé, $f_{13,b}(2) - f_{13,b}(0) = 26$.
Autrement dit, $f_{13,b}(2) \equiv f_{13,b}(0)\ (modulo\ 26)$. Ces deux nombres étant congrus modulo 26, les restes de leurs divisions euclidiennes par 26 sont égaux : $r_{13,b}(2) = r_{13,b}(0)$

Si $a = 13$, quel que soit b fixé, les lettres A et C sont « codées » (sic) par une seule et même lettre.

NB. Pour tout entier k tel que $0 \leq k \leq 12$, $f_{13,b}(2k) - f_{13,b}(0) = 26k$ donc $r_{13,b}(2k) = r_{13,b}(0)$
De même $f_{13,b}(2k+1) - f_{13,b}(1) = 26k$ donc $r_{13,b}(2k+1) = r_{13,b}(1)$.

Toutes les lettres de rang pair sont codées par une seule et même lettre et toutes les lettres de rang impair sont codées par une seule et même autre lettre. On ne peut pas non plus parler de « codage » dans ces conditions …

3. Remarquons surtout le choix du paramètre a : l'entier 5 est premier avec 26. En effet, 5 est un nombre premier donc il est premier avec tout nombre qu'il ne divise pas, en particulier avec 26. Ce choix d'un paramètre a premier avec 26 va s'avérer décisif.

3.a. Montrons que si $r_{5,2}(n) = r_{5,2}(p)$ alors $n - p$ est un multiple de 26 :

Soit n et p les deux éléments de Ω associés aux deux lettres mises en jeu et supposons que les restes des divisions euclidiennes par 26 de $(5n + 2)$ et de $(5p + 2)$ soient égaux.

Notons ici r ce reste commun aux deux divisions. Notons q_n et q_p les quotients respectifs des divisions. Ces divisions euclidiennes s'écrivent : $\begin{cases} 5n + 2 = 26q_n + r \\ 5p + 2 = 26q_p + r \end{cases}$

Par différence membre à membre de ces deux égalités, nous obtenons : $5(n - p) = 26(q_n - q_p)$.

Le nombre 26 divise le second membre donc il divise $5(n - p)$. Or, 26 est premier avec 5, nous pouvons appliquer le théorème de Gauss : L'entier 26 divise $n - p$.

Si $r_{5,2}(n) = r_{5,2}(p)$, alors $n - p$ est un multiple de 26.

NB. Il existe donc un entier relatif k tel que : $n - p = 26k$.

3.b. Déduisons-en que $n = p$:

Par hypothèse, n et p sont deux éléments de Ω, c'est-à-dire deux entiers compris, au sens large, entre 0 et 25. Par conséquent, la différence $n - p$ est comprise, au sens large, entre -25 et $+25$.

Nous avons montré que $n - p$ est un multiple de 26. Or, l'ensemble $\{-25, -24, \dots, 24, 25\}$ ne contient qu'un et un seul multiple de 26, l'entier 0. Nécessairement : $n - p = 0$

Si les restes des divisions euclidiennes par 26 de $(5n + 2)$ et de $(5p + 2)$ sont égaux, alors n et p sont égaux.

NB. Nous venons de montrer que l'application $r_{5,2}$ de l'ensemble $\Omega = \{0\,; 1; \dots; 25\}$ vers lui-même qui à chaque élément n de Ω associe le reste de la division euclidienne de $5n + 2$ par 26 est une application injective. En effet, deux images égales ayant nécessairement des antécédents égaux, deux éléments distincts ont nécessairement des images distinctes.

3.c. Codons le mot « AMI » :

	A	M	I
Associés numériques	0	12	8
Images par $f_{5,2}$	2	62	42
Images par $r_{5,2}$	2	10	16
Retour à l'alphabet	C	K	Q

Nous nous sommes aidés des deux divisions euclidiennes : $62 = 2 \times 26 + 10$ et $52 = 1 \times 26 + 16$.

Le mot « AMI » est codé par « CKQ ».

4.a. Interprétons mathématiquement le décodage de la lettre « E » :

Soit *n* l'associé numérique de la lettre codée par « E ».
Pour coder cette lettre, on a calculé $f_{5,2}(n) = 5n + 2$ puis effectué la division euclidienne de ce nombre par 26. Puisque cette lettre a été codée par « E », dont l'associé numérique est l'entier 4 (d'après le tableau de correspondance), on sait que le reste de cette division euclidienne est égal à 4.

Si nous désignons par *y* le quotient de la division euclidienne, cette dernière s'écrit :

$$5n + 2 = 26y + 4$$

Ou, ce qui revient au même, $5n - 26y = 2$

La question revient à déterminer quel est l'élément *n* de Ω tel que $5n - 26y = 2$.

4.b. Considérons l'équation $5n - 26y = 2$:

NB. Nous noterons **(E)** cette équation. Nous ne perdons pas de vue le fait que 5 et 26 sont des nombres premiers entre eux, propriété majeure dans la résolution.

4.b.i. Proposons une solution particulière :

Le couple $(-10\ ;\ -2)$ est une solution particulière.

En effet, $5 \times (-10) - 26 \times (-2) = -50 + 52 = 2$

4.b.ii. Résolvons l'équation :

Soit *a, b, c* trois entiers relatifs non nuls, les entiers *a* et *b* étant premiers entre eux, comme c'est le cas de 5 et 26.
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 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 $(x_0 = -10\ ;\ y_0 = -2)$.

Un couple $(x,\ y)$ est solution de l'équation **(E)** si et seulement si le couple $(X = x + 10,\ Y = y + 2)$ est solution de l'équation $5X - 26Y = 0$, équation qui a pour solutions les couples de la forme $(26k,\ \ 5k)$ où *k* est un entier relatif.

[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 $aX - bY = 0$.

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 $\begin{cases} x+10=26k \\ y+2=5k \end{cases}$.

Les couples solutions de l'équation **(E)** sont les couples de la forme $(-10+26k,\ -2+5k)$ où k est un entier relatif.

4.b.iii. Déterminons le(s) couple(s) solution(s) $(x\,;y)$ tel(s) que $0 \leq x \leq 25$:

Soit $(x=-10+26k,\ y=-2+5k)$ un couple solution de l'équation.

La double inégalité $0 \leq -10+26k \leq 25$ est équivalente à : $\frac{5}{13} \leq k \leq \frac{35}{26}$.

Un et un seul entier relatif vérifie cette double inégalité, c'est l'entier 1.

Il existe un seul couple $(x\,;y)$ solution de l'équation avec $0 \leq x \leq 25$, le couple $(16\,;3)$

4.c. Décodons la lettre « E » :

L'élément n de Ω tel que $5n-26y=2$, que nous cherchions dans la question 4.a est la première composante de l'unique couple $(x\,;y)$ solution de l'équation avec $0 \leq x \leq 25$.

Nous pouvons conclure que $n=16$, qui est l'associé numérique de la lettre « Q ».

La lettre qui est codée par la lettre « E » est la lettre « Q ».

NB. Ce sujet nous permet de nous interroger sur l'application $r_{a,b}$ de l'ensemble $\Omega=\{0\,;1;\ldots;25\}$ vers lui-même qui à chaque élément n de Ω associe le reste de la division euclidienne de $an+b$ par 26 Dans quels cas cette application réalise-t-elle un « codage » ?

On peut parler de « codage » si cette application réalise une permutation des éléments de Ω, ainsi deux lettres distinctes sont toujours codées par deux lettres distinctes et chaque lettre de l'alphabet est le codage d'une et d'une seule lettre. C'est le cas si $a=5$ mais ce n'est pas le cas si a est égal à 0 ou à 13.

Nous pourrions établir qu'une condition est que le paramètre <u>a soit un entier premier avec 26.</u> En suivant la démarche développée dans la **question 3**, nous pourrions montrer que l'application $r_{a,b}$ est alors une application injective de Ω vers lui-même. L'ensemble Ω étant fini, cette propriété suffit à justifier que $r_{a,b}$ réalise une permutation des éléments de Ω. Donc un « codage » (enfantin certes …).