Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 30

Correction

L'application g est définie sur l'ensemble $E = \{0, 1, \dots, 26\}$. Elle associe à tout élément *x* de E le reste de la division euclidienne du nombre $4x + 3$ par 27. Etant un reste dans une division euclidienne par 27, le nombre $g(x)$ est lui-même élément de E.

1. Déterminons tous les éléments de *E* invariants par *g* :

Un entier *x* élément de *E* est invariant par *g* si et seulement s'il est lui-même le reste de la division euclidienne de $4x + 3$ par 27, c'est-à-dire si et seulement si : $4x + 3 \equiv x \pmod{27}$ avec la double inégalité $0 \leq x \leq 26$.

Vu la compatibilité de la relation de congruence modulo 27 avec l'addition, cette congruence est équivalente à la congruence $3x + 3 \equiv 0 \pmod{27}$.

Cette congruence s'écrit aussi bien : $3 \times (x + 1) \equiv 0 \pmod{27}$. Elle est vérifiée si et seulement s'il existe un entier relatif *k* tel que : $3(x + 1) = 27k$, c'est-à-dire tel que $x = 9k - 1$. Un tel entier *x* appartient à *E* si et seulement si $0 \leq 9k - 1 \leq 26$ soit $\frac{1}{9} \leq k \leq 3$. Trois valeurs de *k*, et trois seulement, vérifient cette double inégalité, les valeurs 1, 2 et 3.

Il existe exactement trois éléments de E qui conviennent, les entiers 8, 17 et 26 et eux seuls.

Les éléments de E invariants par *g* sont les entiers 8, 17 et 26.

2. Déduisons-en les caractères invariants dans le codage :

Il s'agit des caractères dont les associés numériques sont 8, 17 et 26.

Dans ce codage, les lettres « i » et « r » sont invariantes de même que le séparateur « * ».

En particulier, le séparateur étant invariant, une phrase composée de plusieurs mots sera codée par une phrase composée d'autant de mots s'écrivant avec autant de lettres.

3. Vérifions que pour tout *x* et *y* de E, si $y \equiv 4x+3 \ \ (mod\ 27)$ alors $x \equiv 7y+6\ (mod\ 27)$:

Il s'agit d'une « vérification » plutôt que d'une « démonstration » puisque le résultat est donné par l'énoncé.

Supposons que *x* et *y* soient deux entiers relatifs tels que $y \equiv 4x+3 \ \ (mod\ 27)$. Compte tenu de la compatibilité de la relation de congruence modulo 27 avec la multiplication et avec l'addition, nous obtenons une nouvelle congruence si nous multiplions chacun des deux membres par 7 et si nous ajoutons 6. La congruence $y \equiv 4x+3 \ \ (mod\ 27)$ implique : $7y+6 \equiv 7 \times (4x+3)+6 \ \ (mod\ 27)$ soit aussi bien : $7y+6 \equiv 28x+27 \ \ (mod\ 27)$.
Or, $28 \equiv 1 \ \ (mod\ 27)$ et $27 \equiv 0 \ \ (mod\ 27)$.

Nous obtenons, comme prévu : $7y+6 \equiv x \ \ (mod\ 27)$.

Si *x* et *y* vérifient $y \equiv 4x+3 \ \ (mod\ 27)$ alors ils vérifient $x \equiv 7y+6\ (mod\ 27)$

NB. L'hypothèse « *x* et *y* appartiennent à E » est inerte dans cette vérification. L'implication est vraie quels que soient les entiers relatifs *x* et *y*, pourvu qu'ils vérifient $y \equiv 4x+3 \ \ (mod\ 27)$.

4. Démontrons que deux caractères distincts sont codés par deux caractères distincts :

Nous allons procéder par contraposition, c'est-à-dire que nous allons démontrer que, si deux caractères sont codés par des caractères égaux, alors ils sont égaux.

Soit *x* et *x'* deux éléments de *E* qui sont codés par un même caractère. C'est-à-dire qu'il existe un même élément *y* de *E* : $\begin{cases} y \equiv 4x+3 \ \ (mod\ 27) \\ y \equiv 4x'+3 \ \ (mod\ 27) \end{cases}$.

D'après le résultat de la question 3, nous avons dans ce cas : $\begin{cases} x \equiv 7y+6 \ \ (mod\ 27) \\ x' \equiv 7y+6 \ \ (mod\ 27) \end{cases}$

Par transitivité de la relation de congruence modulo 27, nous en déduisons : $x \equiv x'\ (mod\ 27)$.

Puisqu'ils sont congrus modulo 27, *x* et *x'* diffèrent d'un multiple de 27. Mais ces deux entiers appartiennent à *E*, ils sont tous les deux compris entre 0 et 26 au sens large. L'entier dont ils diffèrent est nécessairement nul. La congruence : $x \equiv x'\ (mod\ 27)$ couplée avec l'appartenance des deux entiers à *E* implique leur égalité : $x = x'$.

Deux caractères codés par des caractères égaux sont égaux. Par contraposition, deux caractères distincts sont codés par des caractères distincts.

5. Proposons une méthode de décodage :

Reprenons les phases décrites dans l'énoncé en remplaçant *g* par l'application *h* qui associe à tout élément *x* de *E* le reste de la division euclidienne de $7x+6$ par 27. Les **questions 3 et 4** montrent que cette application *h* n'est autre que l'application réciproque de *g*.

En effet, pour tout élément *x* de *E* : $x \xrightarrow{g} g(x) \xrightarrow{h} h\big(g(x)\big) = x$

Donc, cette méthode appliquée avec *h* décode ce que *g* a permis de coder.

On peut décoder une lettre d'associé numérique *x* en cherchant le reste de la division euclidienne de $7x + 6$ par 27.

6. Décodons le mot « VFV » :

Pour cela, il nous faut décoder les deux lettres « F » et « V ». Appliquons le protocole de décodage décrit dans la **question 5**.

	F	V
Associons des nombres *x* aux caractères	5	21
Calculons $h(x) = 7x + 6$	41	153
Divisions euclidiennes	$41 = 1 \times 27 + 14$	$153 = 5 \times 27 + 18$
Les restes des divisions euclidiennes	14	18
Associons des caractères aux nombres	O	S

Le mot « VFV » code le mot « SOS ».