Maths Expertes
Terminale

La congruence

CORRIGÉ DE L'EXERCICE

La congruence

15

Correction

NB. Voici un exercice portant sur « l'inversion modulaire ».
Pour obtenir un « inverse modulo *n* » d'un entier relatif donné *x*, le jeu consiste à trouver un entier *y* tel que $x \times y \equiv 1 \ [n]$.
Pour cela, on cherche un entier *y* tel que le produit $x \times y$ soit de la forme $1 + kn$ où *k* est un entier relatif.
Voir sur le même sujet l'exercice numéro 23.

1 et 2 (traitées ensemble). Cherchons des inverses modulo 5 des nombres 2, 3 et 4 :

Soit $x = 2$ ou 3 ou 4. Il s'agit dans chaque cas de trouver un entier *y* tel que le produit $x \times y$ soit de la forme $1 + 5k$ où *k* est un entier relatif.

Ainsi par exemple, un produit égal à 6, 11, 16 ou 21 fera parfaitement l'affaire.

Nous observons que $2 \times 3 = 6 = 1 + 5$ et que $4 \times 4 = 16 = 1 + 3 \times 5$.

En conséquence : $2 \times 3 \equiv 1 \ [5]$ et $4 \times 4 \equiv 1 \ [5]$.

- Un inverse modulo 5 de 2 est l'entier 3.
- Un inverse modulo 5 de 3 est l'entier 2.
- Un inverse modulo 5 de 4 est l'entier 4 lui-même.

NB. L'énoncé nous demande « un inverse » car il n'y a pas unicité. Pour tout entier relatif *p* :
Tout entier *y* tel que $y \equiv 3 \ [5]$ est un inverse modulo 5 de 2. Il en est ainsi des entiers $-2, 3, 8, \ldots$
Tout entier *y* tel que $y \equiv 2 \ [5]$ est un inverse modulo 5 de 3. Il en est ainsi des entiers $-3, 2, 7, \ldots$
Tout entier *y* tel que $y \equiv 4 \ [5]$ est un inverse modulo 5 de 4. Il en est ainsi des entiers $-1, 4, 9, \ldots$

3. L'entier 0 admet-il un inverse ?

La réponse est non, car quel que soit l'entier relatif *y*, le produit $0 \times y$ est égal à 0, entier qui n'est pas de la forme «$1 + 5k$ ». On ne peut donc trouver aucun entier relatif y vérifiant $0 \times y \equiv 1\ [5]$.

4. Un « tableau de congruence » :

Il s'agit plutôt d'une « table de multiplication modulaire ».

Pour la construire, nous confectionnons un tableau à 5 lignes et 5 colonnes dont chaque case contient non pas le produit « ligne-colonne » mais le reste de la division euclidienne de ce produit par 5. Voici la table attendue. En rouge, la zone « intéressante », concernant les multiplications d'entiers non congrus à 0 modulo 5 :

×	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Chaque fois que nous obtenons « 1 » dans une case, nous pouvons dire que les nombres « ligne » et « colonne » sont inverses modulo 5 l'un de l'autre. Nous retrouvons les résultats précédents, la table ne nous apprend rien de nouveau.

Les entiers 1 et 4 sont leur propre inverse modulo 5, tandis que 2 et 3 sont inverses modulo 5 l'un de l'autre.

5. Résolvons « à l'aide du tableau » les congruences proposées :

5.a. Résolvons ainsi la congruence $2x \equiv 3\ [5]$:

Pour ce faire, nous repérons sur la ligne « 2 » du tableau la case (ou les cases …) dans laquelle est inscrit « 3 » et nous retenons le nombre-colonne. Ainsi, 3 est inscrit uniquement dans la colonne « 4 », donc l'entier 4 est l'unique nombre-colonne solution. Tout entier congru à 4 est solution et sont solution seulement ces entiers.

$2x \equiv 3\ [5]$ si et seulement si $x \equiv 4\ [5]$

5.b. Résolvons ainsi la congruence $9x \equiv 1\ [5]$:

Cette congruence est équivalente à la congruence $4x \equiv 1\ [5]$. Résoudre cette dernière revient à chercher les inverses modulo 5 de 4, ce qui a été vu. Nous repérons d'ailleurs dans le tableau que « 1 » figure une fois et une seule sur la ligne « 4 » (dans la colonne « 4 »).

$9x \equiv 1\ [5]$ si et seulement si $x \equiv 4\ [5]$

NB. La question 5 aborde la résolution de congruences du type $ax \equiv b\ [n]$. Nous relevons ici deux pistes de résolution de telles congruences :

- La confection d'un « tableau de congruence » puis la lecture directe du tableau (ce qui n'est envisageable pratiquement que si l'entier *n* n'est « pas trop grand »).
- La recherche puis l'utilisation (s'il en existe …) d'un inverse modulo *n* de *a* (voir méthode développée dans l'exercice 23). Le lecteur aura certainement l'occasion de se confronter à des conditions d'existence de tels inverses, conditions qui sont en lien avec le thème « nombres premiers entre eux ».