Maths Expertes
Terminale

La congruence

CORRIGÉ DE L'EXERCICE

La congruence

02

Correction

Soit *n* un entier non nul.

Rappelons une propriété de la congruence modulo *n*, sa compatibilité avec la multiplication : « On obtient une nouvelle congruence modulo *n* en multipliant membre à membre deux congruences modulo *n* ».

Compatibilité des congruences avec les puissances

1. Montrons par récurrence que si $a \equiv b \ [n]$ alors $a^p \equiv b^p \ [n]$ pour tout entier $p > 0$:

Soit *a* et *b* deux entiers relatifs tels que $a \equiv b \ [n]$.

Appelons « propriété $\wp_p$ » la propriété associée à l'entier *p* : « $a^p \equiv b^p \ [n]$ »

Initialisation :

Nous allons initialiser au rang 1, puisque nous devons montrer la propriété en jeu « pour tout entier $p > 0$ ».

Les « puissances 1 » de *a* et de *b* sont respectivement : $a^1 = a \ ; \ b^1 = b$

Nous avons bien $a^1 \equiv b^1 \ [n]$. La propriété $\wp_1$ est vraie.

Hérédité :

Supposons que, pour un certain entier *p* strictement positif, la propriété $\wp_p$ soit vraie, c'est-à-dire supposons que $a^p \equiv b^p \ [n]$.

Nous disposons des deux congruences $\begin{cases} a \equiv b \ [n] \\ a^p \equiv b^p \ [n] \end{cases}$. En vertu de la compatibilité de la relation de congruence modulo *n* avec la multiplication, nous obtenons une nouvelle congruence modulo *n* en multipliant membre à membre ces deux congruences.

Nous obtenons la congruence $a \times a^p \equiv b \times b^p \ [n]$ soit $a^{p+1} \equiv b^{p+1} \ [n]$. La propriété $\wp_{p+1}$ est vérifiée.

Si la propriété $\wp_p$ est vraie, alors la propriété $\wp_{p+1}$ est vraie elle aussi.

Nous avons démontré l'implication $\wp_p \ \Rightarrow \ \wp_{p+1}$, la « propriété $\wp_p$ » est héréditaire.

Conclusion :

Puisque la propriété $\wp_p$ est vraie lorsque $p = 1$ et qu'elle est héréditaire, elle est vraie pour tout entier $p \geq 1$.

Soit *a* et *b* deux entiers tels que $a \equiv b \ [n]$. Alors $a^p \equiv b^p \ [n]$ pour tout entier $p > 0$

NB. Notons que cette congruence est aussi vérifiée lorsque $p = 0$. En effet, quels que soient les entiers *a* et *b*, $a^0 = b^0 = 1$. Nous pouvons donc dire que « $a^p \equiv b^p \ [n]$ pour tout entier $p \geq 0$ ».

2. Montrons que $41^{183} \equiv 6 \ [7]$:

Nous avons : $41 - 6 = 35 = 5 \times 7$ donc $41 \equiv 6 \ [7]$.

Si nous appliquons à la lettre le résultat de la question 1 avec $a = 41, b = 6, p = 183, n = 7$, nous obtenons la congruence $41^{183} \equiv 6^{183} \ [7]$.

Il nous reste à étudier le comportement des puissances de 6 relativement à la congruence modulo 7.

Or : $6^2 = 36 = 1 + 35 = 1 + 5 \times 7$ donc : $6^2 \equiv 1 \ [7]$

Nous pouvons appliquer le résultat de la question 1 à cette congruence.

Pour tout entier naturel *p*, $(6^2)^p \equiv 1^p \ [7]$, soit aussi bien $6^{2p} \equiv 1 \ [7]$

Multiplions par 6 les deux membres de cette congruence : $6 \times 6^{2p} \equiv 6 \ [7]$ soit $6^{2p+1} \equiv 6 \ [7]$.

En résumé, les puissances paires de 6 sont toutes congrues à 1 modulo 7 et les puissances impaires de 6 sont toutes congrues à 6 modulo 7.

L'entier 183 étant un nombre impair, nous pouvons affirmer que $6^{183} \equiv 6 \ [7]$ et, par transitivité :

$$\begin{cases} 41^{183} \equiv 6^{183} \ [7] \\ 6^{183} \equiv 6 \ [7] \end{cases} \Rightarrow \ 41^{183} \equiv 6 \ [7]$$

Nous avons démontré que $41^{183} \equiv 6 \ [7]$

3.a. Vérifions :

$2^3 = 8$; $4^3 = 64$. Or : $64 - 8 = 56 = 8 \times 7$. La différence $4^3 - 2^3$ est un multiple de 7 donc nous pouvons affirmer que : $4^3 \equiv 2^3 \ [7]$

3.b. Etudions la réciproque de la propriété démontrée dans la question 1 :

Utilisons la question 3.a. Nous avons bien $4^3 \equiv 2^3\ [7]$ alors que les entiers 4 et 2 ne sont pas congrus modulo 7.

La question 3.a. nous fournit un contre-exemple d'entiers *a, b, p, n* tels que la congruence $a^p \equiv b^p\ [n]$ est vérifiée alors que la congruence $a \equiv b\ [n]$ ne l'est pas.

La propriété réciproque de celle de la question 2 est fausse.

Il se peut que $a^p \equiv b^p\ [n]$ sans que pour autant $a \equiv b\ [n]$

NB. Pour montrer qu'une propriété est fausse, il suffit de proposer un « contre-exemple », c'est-à-dire un exemple dans lequel la propriété en question est mise en défaut.

4.a. Vérifions :

$2^2 = 4$; $2^5 = 32$. Or : $32 - 4 = 28$. La différence $2^5 - 2^2$ n'est pas un multiple de 3.

Les entiers 2^5 et 2^2 ne sont pas congrus modulo 3.

4.b. Tirons-en une conséquence :

La question 4.a. nous fournit un contre-exemple d'entiers *a, b, p, n* tels que la congruence $a \equiv b\ [n]$ est vérifiée mais la congruence $p^a \equiv p^b\ [n]$ ne l'est pas.

La réponse est « Non !». Le « théorème » suggéré dans cette question est faux.

NB. Cette question quelque peu provocatrice montre qu'il faut se garder d'inventer sans contrôle des énoncés qui ont l'air à première vue sympathiques mais qui s'avèrent faux.

Retenons ici qu'on ne peut pas mélanger les vessies (des entiers) avec les lanternes (leurs exposants).