TS spé

Exercices sur les congruences

1 **Vrai ou faux ?**
Dire si les congruences suivantes sont vraies ou fausses.
$16 \equiv 30 \pmod 7$; $15 \equiv 26 \pmod 6$; $29 \equiv -121 \pmod 5$; $-623 \equiv 17 \pmod{10}$.

2 Démontrer que $901 \equiv 1 \pmod 3$; en déduire, sans calcul, le reste de la division euclidienne de 901^4 par 3.
Vérifier en calculant 901^4 avec la calculatrice (rubrique calculs ou Python).

3 Démontrer que $149 \equiv 9 \pmod{10}$ et $52 \equiv 2 \pmod{10}$; en déduire le reste de la division euclidienne de $N = 149 \times 52$ par 10 (sans calculer le produit).

4 Soit x et y deux entiers relatifs tels que $x \equiv 4 \pmod 7$ et $y \equiv 2 \pmod 7$.
Démontrer que le nombre $3x + y$ est divisible par 7.

5 Soit n un entier naturel quelconque.
Démontrer que $5^n + 19$ est divisible par 4 en utilisant les congruences.

6 Soit x et y deux entiers relatifs tels que $x \equiv 4 \pmod{13}$ et $y \equiv 5 \pmod{13}$.
En travaillant avec des relations de congruences, démontrer que $x^2 + 2y$ est divisible par 13.

7 Soit n un entier naturel quelconque.
Démontrer que $3^{2n} - 2^n$ est divisible par 7 en utilisant les congruences.

8 1°) Démontrer que $12 \equiv -1 \pmod{13}$.
2°) Déterminer suivant les valeurs de l'entier naturel n le plus petit entier relatif en valeur absolue auquel est congru 12^n modulo 13.

9 Soit n un entier naturel quelconque.
Démontrer à l'aide des congruences que $4^{3n} - 4^n$ est divisible par 5.

10 Soit n un entier relatif quelconque tel que $n \equiv 2 \pmod 5$.
Démontrer que $n^4 + n - 3$ est divisible par 5.

11 1°) Démontrer que $7 \equiv -1 \pmod 8$.
2°) Soit n un entier naturel quelconque. Démontrer que $7^{2n+1} + 1$ est divisible par 8.

12 Soit n un entier naturel quelconque.
Démontrer que $10^n - 1$ est divisible par 9.

13 1°) Démontrer que $10 \equiv -1 \pmod{11}$; $10^2 \equiv 1 \pmod{11}$; $10^3 \equiv -1 \pmod{11}$.
2°) En déduire le reste de la division euclidienne par 11 du nombre 5869.
Indication : Écrire la décomposition en base dix de 5869.

14 1°) Démontrer sans calculatrice que $3^2 \equiv 2 \pmod 7$; $3^4 \equiv 4 \pmod 7$; $3^6 \equiv 1 \pmod 7$.
2°) Effectuer la division euclidienne de 1000 par 6. En déduire le reste de la division euclidienne de 3^{1000} par 7.

15 Arthur et Wilson sont deux jumeaux qui ont l'habitude de communiquer à l'aide de messages codés.
Ils réalisent toujours leur cryptage de la façon suivante :
Chaque lettre de l'alphabet munie de son numéro d'ordre n est remplacée par la lettre de l'alphabet munie du numéro d'ordre p $(1 \leqslant p \leqslant 26)$ obtenu à l'aide de la formule : $p \equiv 3 \times n + 7 \pmod{26}$.

Par exemple la forme cryptée de L est Q car $3 \times 12 + 7 = 43$ et $43 \equiv 17 \pmod{26}$.

1°) Recopier et compléter la table de cryptage ci-dessous :

Lettre	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
n	1	2	3	4	5	6	7	8	9	10	11	12	13
p													
Forme cryptée													

Lettre	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
n	14	15	16	17	18	19	20	21	22	23	24	25	26
p													
Forme cryptée													

2°) Arthur a envoyé le message suivant à Wilson : MIJUZ CZRI OJ IVRLLHOV.
Retrouver la forme décryptée du message.
3°) Wilson désire lui répondre : MERCI.
Donner la forme cryptée de ce message.

16 Les codes secrets des cartes bancaires sont formés de quatre chiffres pris de 0 à 9.
Pierre n'a pas noté celui de sa carte bancaire dans son agenda, mais comme il a peur de l'oublier, il a quand même noté la forme « cryptée » de son code secret de façon que son code secret ne soit pas découvert si son agenda était perdu.
Pierre réalise toujours son cryptage de la façon suivante : il remplace chaque chiffre n de son code secret par le chiffre p, appelée forme cryptée de n, qu'il calcule à l'aide de la formule suivante $p \equiv 3n + 7 \pmod{10}$.
1°) Reproduire et compléter la table de cryptage ci-dessous correspondant à la formule de Pierre.

n	0	1	2	3	4	5	6	7	8	9
p										

2°) Pierre a inscrit 8503 dans son agenda qui est la forme cryptée de son code secret.
Quel est son véritable code secret ?

17 1°) On considère le tableau de congruences ci-dessous où n désigne un entier relatif.

Si $n \equiv \ldots$ (mod. 5)	0	1	2	3	4
Alors $3n \equiv \ldots$ (mod. 5)	…	…	…	…	…

Recopier et compléter les cases de la deuxième ligne de ce tableau en écrivant chaque fois le plus petit entier naturel. Il n'y a rien à compléter dans la première colonne.

2°) À l'aide du tableau de la question 1°), déterminer tous les entiers relatifs n tels que $3n \equiv 2$ (mod. 5).

Répondre par une phrase sur le modèle suivant à recopier et à compléter :

« D'après le tableau de congruences de la question 1°), les entiers relatifs n tels que $3n \equiv 2$ (mod. 5) sont les entiers relatifs congrus à … modulo 5. »

Vérifier en utilisant le site « dcode » partie « résolution des équations modulaires ».

3°) Retrouver les solutions de la congruence en utilisant un inverse de 3 modulo 5.

On utilisera une démarche par équivalences.

18 Le but de l'exercice est de démontrer l'implication suivante pour des entiers relatifs a, b, c.

« Si 7 divise $a^3+b^3+c^3$, alors 7 divise abc (produit des entiers a, b, c) ».

Réfléchir à une méthode lourde (pas forcément efficace) qui consiste à déterminer tous les triplets $(a\,;b\,;c)$ d'entiers relatifs tels que 7 divise $a^3+b^3+c^3$.

On pourra se ramener à la résolution de la congruence $a^3+b^3+c^3 \equiv 0$ (mod. 7).

Cette résolution pourra s'effectuer à l'aide du site dcode, rubrique équations modulaires, ou à l'aide d'un programme.

Dans la suite, on propose une méthode plus efficace.

1°) Dans le tableau ci-dessous, la première ligne représente les restes de la division euclidienne d'un entier relatif a par 7. Sur la deuxième ligne, figure un entier congru à a^3 modulo 7 (attention, ce n'est pas forcément le reste de la division euclidienne de a^3 par 7).

Si $a \equiv \ldots$ (mod. 7)	0	1	2	3	4	5	6
Alors $a^3 \equiv \ldots$ (mod. 7)	0	1	…	…	…	-1	-1

Recopier et compléter ce tableau (uniquement les cases de la deuxième ligne).

Dans les questions 2°) et 3°), on considère trois entiers relatifs a, b, c.

2°)Quels sont les restes possibles dans la division euclidienne par 7 de l'entier $a^3+b^3+c^3$?

Faire un arbre sur une page complète à la règle suivant les valeurs auxquelles sont congrus a^3, b^3, c^3.

3°) Démontrer que si 7 divise $a^3+b^3+c^3$, alors 7 divise abc (produit des entiers a, b, c).

19 1°) Recopier et compléter la deuxième ligne du tableau de congruences ci-dessous par des entiers entre 0 et 4 (x est un entier relatif) :

Si $x \equiv ...$ (mod. 5)	0	1	2	3	4
Alors $x^2 \equiv ...$ (mod. 5)					

2°) En déduire que l'équation $x^2 - 5y^2 = 3$ (E), avec x et y entiers, n'a pas de solution.

20 1°) Déterminer suivant les valeurs de l'entier naturel n le reste de la division euclidienne de 2^n par 7.
2°) En déduire le reste de la division euclidienne par 7 du nombre $\mathrm{N} = 247^{349}$.

21 Recopier et compléter la deuxième ligne du tableau de congruences suivant en écrivant chaque fois le plus petit entier naturel (n est un entier relatif) :

Si $n \equiv \ldots$ (mod. 3)	0	1	2
Alors $n^3 \equiv \ldots$ (mod. 3)	…	…	…

En déduire que, pour tout entier relatif n, $n^3 - n$ est divisible par 3.

22 Démontrer en reprenant la méthode de l'exercice précédent que pour tout entier relatif n, $n^5 - n$ est divisible par 5.

23 Déterminer les entiers relatifs n tels que l'entier $\mathrm{N} = n^2 - 3n + 7$ soit divisible par 5.
On pourra utiliser un tableau de congruences modulo 5.
Vérifier en utilisant le site « dcode », partie résolution modulaire.

24 Déterminer le chiffre x tel que l'entier $\overline{53x4}$ soit divisible par 9.

25 Déterminer les chiffres x et y tels que l'entier $\overline{3x2y}$ soit divisible par 4 et 3.

25 bis Soit N un entier naturel. On pose $\mathrm{N} = \overline{a_n a_{n-1} ... a_1 a_0}$ (écriture en base dix).
On a donc $\mathrm{N} = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$ (décomposition en base dix du nombre N).
Rappeler pourquoi $\mathrm{N} \equiv a_0 + a_1 + a_2 + ... + a_n$ (mod. 3).
Déterminer mentalement le reste de la division euclidienne du nombre 34442057 par 3.

26 Critère de divisibilité par 11

Soit N un entier naturel. On pose $N = \overline{a_n a_{n-1} ... a_1 a_0}$ (écriture en base dix).

On a donc $N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$ (décomposition en base dix du nombre N).

1°) Démontrer que $10 \equiv -1$ (mod. 11).

2°) Démontrer que $N \equiv a_0 - a_1 + a_2 - ...$ (mod. 11).

2 applications :

- reste de la division euclidienne d'un entier naturel par 11 (calcul mental)
- divisibilité par 11

Application :
Déterminer mentalement le reste de la division euclidienne d'un entier naturel par 11 du nombre 34442057.

3°) En déduire que N est divisible par 11 si et seulement si la somme alternée $a_0 - a_1 + a_2 - ...$ est divisible par 11.
On retiendra le critère de divisibilité par 11 sous la forme :
« Un entier naturel est divisible par 11 si et seulement si la différence de ses chiffres de rang pair et de ses chiffres de rang impair est divisible par 11 ».
4°) Appliquer le critère précédent pour déterminer sans calculatrice si les nombres 25 418 792 et 851 047 932 152 sont divisible par 11.

Pour le test de divisibilité par 11, peu importe si l'on part du chiffre le plus à gauche ou le plus à droite.

Dans les exercices **27** et **29**, on utilise les tableaux suivants qui font correspondre à chaque lettre de l'alphabet un entier naturel entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

27 On définit un système de codage affine selon le procédé suivant :
- à chaque lettre de l'alphabet, on associe l'entier x correspondant, on associe ensuite à x l'entier y qui est le reste de la division euclidienne de $15x + 7$ par 26,
- on associe à y la lettre correspondante.

Le but de l'exercice est de déterminer la procédure de décodage. Pour cela, on part de la relation
$y \equiv 15x + 7$ [mod. 26] (1).

1°) Justifier que 15 admet un inverse modulo 26 et déterminer un tel inverse.

Recopier et compléter alors l'équivalence : $(1) \Leftrightarrow x \equiv ...$ [mod. 26] (2).

2°) En déduire une description du système de décodage associé au système de codage considéré.
3°) Décoder le mot WHL.

Les exercices **28** et **29** portent sur les matrices d'entiers relatifs.
Ils seront donnés après le chapitre sur les matrices.
On commencera par lire l'encadré qui suit sur la notion de congruence pour des matrices formées d'entiers relatifs.

Dans les deux exercices, on veillera à ne travailler qu'avec des matrices d'entiers relatifs.

• **Définition et notation :**

Soit n un entier naturel supérieur ou égal à 2.
Soit P et Q sont deux matrices de mêmes dimensions dont les coefficients sont des entiers relatifs.

On dit qu'elles sont congrues modulo n et on note $P \equiv Q \pmod{n}$ pour parler de congruence coefficient par coefficient.

Par exemple, on peut écrire : $\begin{pmatrix} 15 \\ -3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 5 \end{pmatrix} \pmod{4}$ car $15 \equiv 3 \pmod{4}$ et $-3 \equiv 5 \pmod{4}$.

Pour démontrer que deux matrices P et Q de mêmes dimensions dont les coefficients sont des entiers relatifs sont congrues modulo n, il est possible de calculer leur différence et de démontrer que tous les coefficients sont divisibles par n.
Attention, on ne dit pas qu'une matrice est divisible par un entier (on doit dire que tous les coefficients de la matrice sont divisibles par cet entier).

• **Propriété :**

Les propriétés de comptabilité de la relation de congruence avec l'addition et la multiplication permettent d'écrire que, si A est une matrice carrée $p \times p$, et B et C sont deux matrices unicolonnes $p \times 1$, alors :

$B \equiv C \pmod{n} \Rightarrow AB \equiv AC \pmod{n}$.

Idée de la démonstration (dans le cas $p = 2$) :

Soit a, b, x, y, x' et y' des entiers relatifs.
On sait que si $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$, alors : $ax + by \equiv ax' + by' \pmod{n}$.

• **Définition :**

Soit M une matrice carrée d'ordre p dont tous les coefficients sont des entiers relatifs.
On dit qu'une matrice M' carrée d'ordre p à coefficients entiers relatifs est un inverse (pour le produit) de la matrice M modulo n lorsque $MM' \equiv I_p \pmod{n}$ et $MM' \equiv I_p \pmod{n}$.

Il n'y a pas de notation pour un inverse.
Nous admettrons que, dans cette définition, l'un des deux produits suffit.

• **Propriété :**

On prend $p = 2$.
On pose $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c, d sont des entiers relatifs.
M admet un inverse modulo n si et seulement si det M est premier avec n.
Dans ce cas, en notant u un inverse de det M modulo n, la matrice $M' = u\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est un inverse de M modulo n.

Démonstration :

Le premier point est admis.
Pour le deuxième point, on effectue un calcul.

Propriété (équivalence fondamentale :

Soit M une matrice carrée d'ordre p à coefficients entiers relatifs.
Soit X et Y sont deux matrices rectangulaires de taille $p \times q$ à coefficients entiers relatifs.
On suppose que M admet un inverse modulo n et on note M' un tel inverse.
On a $MX \equiv Y \pmod{n} \Leftrightarrow X \equiv M'Y \pmod{n}$. La démonstration est facile.

28 1°) Démontrer que la matrice $\mathrm{M}=\begin{pmatrix}3 & 1\\ 1 & -1\end{pmatrix}$ admet un inverse modulo 13 et déterminer un inverse M'.

2°) On considère le système $\begin{cases}3x+y\equiv 1 \pmod{13}\\ x-y\equiv 5 \pmod{13}\end{cases}$ d'inconnue $(x\,;y)\in\mathbb{Z}^2$.

Écrire matriciellement ce système avec les matrices M, $\mathrm{X}=\begin{pmatrix}x\\ y\end{pmatrix}$ et $\mathrm{Y}=\begin{pmatrix}1\\ 5\end{pmatrix}$.

Résoudre le système.

3°) Vérifier en utilisant « dcode », partie résolution des équations modulaires.

29 **Chiffrement de Hill**

On reprend l'exercice sur le chiffrement de Hill donné dans le chapitre précédent.

On veut coder un mot de deux lettres selon la procédure suivante.

Étape 1 :

Chaque lettre du mot est remplacée par un entier naturel compris entre 0 et 25 selon les tableaux précédents.

On obtient un couple d'entiers $(x_1\,;x_2)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 :

$(x_1\,;x_2)$ est transformé en $(y_1\,;y_2)$ tel que y_1 est le reste de la division euclidienne de $11x_1+3x_2$ par 26 et y_2 est le reste de la division euclidienne $7x_1+4x_2$ par 26.

Étape 3 :

$(y_1\,;y_2)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Le but de l'exercice est de déterminer la procédure de décodage. Pour cela, on va utiliser les matrices.

On pose $\mathrm{A}=\begin{pmatrix}11 & 3\\ 7 & 4\end{pmatrix}$ (matrice carrée d'ordre 2). Cette matrice est appelée la matrice de codage ou clef du chiffrage de Hill considéré dans l'exercice. Elle est connue seulement de l'émetteur et du destinataire.

• Le mot à coder est remplacé par la matrice colonne $\mathrm{X}=\begin{pmatrix}x_1\\ x_2\end{pmatrix}$, où x_1 est l'entier représentant la première lettre du mot et x_2 l'entier représentant la deuxième, selon le tableau de correspondance qui a été donné auparavant.

• La matrice X est transformée en la matrice colonne $\mathrm{Z}=\begin{pmatrix}z_1\\ z_2\end{pmatrix}$ telle que $\mathrm{Z}=\mathrm{AX}$.

• La matrice Z est transformée en la matrice $\mathrm{Y}=\begin{pmatrix}y_1\\ y_2\end{pmatrix}$, où y_1 est le reste de la division euclidienne de z_1 par 26 et y_2 le reste de la division euclidienne de z_2 par 26.

• Les entiers y_1 et y_2 donnent les lettres du mot codé, selon le tableau de correspondance qui a été donné.

1°) Justifier que A admet un inverse modulo 26 et déterminer l'inverse B de A modulo 26 dont tous les coefficients sont des entiers naturels les plus petits possibles.
/!\ On parle d'inverse de A modulo 26 (et pas d'inverse tout court). Cette matrice ne se note pas A^{-1}.
2°) Justifier que $Y \equiv AX \pmod{26}$ puis que $X \equiv BY \pmod{26}$.
En déduire que la matrice B est la matrice de décodage.
On dit aussi que A est la *matrice de cryptage* et que B est la *matrice de décryptage.*
3°) Décoder le mot YJ.

On pourra utiliser le site « dcode », rubrique sur le chiffrement de Hill (https://www.dcode.fr/chiffre-hill), pour vérifier le résultat.

Corrigé

Dans beaucoup d'exercices, on doit démontrer qu'une expression est divisible par un entier naturel n non nul.
En général, on n'est pas obligé de repasser chaque fois par zéro puisque l'on a la propriété

$a \equiv b \pmod{n}$ signifie $n \mid a - b$.

1 Vrai ou faux ?

Rappels

$a \equiv b \pmod{n}$ signifie $n \mid a - b$

$a \equiv b \pmod{n}$ se lit « a est congru à b modulo n ».

• $16 \equiv 30 \pmod{7}$

$16 - 30 = -14$
$7 \mid -14$
Donc $16 \equiv 30 \pmod{7}$ est vraie.

• $15 \equiv 26 \pmod{6}$

$15 - 26 = -11$
6 ne divise pas -11 (on peut noter $6 \nmid -11$).
Donc $15 \equiv 26 \pmod{6}$ est fausse.

• $29 \equiv -121 \pmod{5}$

$29 + 121 = 150$
$5 \mid 150$
Donc $29 \equiv -121 \pmod{5}$ est vraie.

• $-623 \equiv 17 \pmod{10}$

$-623 - 17 = -640$
$10 \mid -640$
Donc $-623 \equiv 17 \pmod{10}$ est vraie.

Lorsqu'un entier a ne divise pas un entier b, on peut écrire $a \nmid b$.

Par contre, on n'écrit pas : $a \not\equiv b \pmod{n}$.

2

Démontrons que $901 \equiv 1$ (mod. 3).

$901 - 1 = 900$

3 | 900

Donc **$901 \equiv 1$ (mod. 3)**.

Avec moins de calculs, on peut aussi dire qu'un entier naturel est congru à la somme de ses chiffres modulo 3.
On a $901 \equiv 10$ (mod. 3). Or $10 \equiv 1$ (mod. 3). Donc $901 \equiv 1$ (mod. 3).

Déduisons-en le reste de la division euclidienne de 901^4 par 3 sans calculatrice.

$901 \equiv 1$ (mod. 3) donc $901^4 \equiv 1^4$ (mod. 3) soit $901^4 \equiv 1$ (mod. 3).
Or $0 \leqslant 1 < 3$.
Donc **le reste de la division euclidienne de 901^4 par 3 est 1**.

On peut résumer ainsi :

$901^4 \equiv 1$ (mod. 3).
nombre à diviser — reste — diviseur

On peut calculer le reste de la division euclidienne de 901^4 par 3 dans la console Python (sinon, grâce à Python, on obtient $901^4 = 659020863601$).
On vérifie alors le résultat trouvé par les congruences.
On peut éventuellement utiliser la propriété de la somme des chiffres d'un entier naturel modulo 3.

3

Démontrons que $149 \equiv 9$ (mod. 10) et $52 \equiv 2$ (mod. 10).

On a : $149 - 9 = 140$.
10 | 140
Donc $149 \equiv 9$ (mod. 10)

On a : $52 - 2 = 50$ (mod. 10)
10 | 50
Donc $52 \equiv 2$ (mod. 10).

On peut aussi utiliser la propriété suivante :
« Tout entier naturel est congru à son chiffre des unités modulo l0. »

Déduisons-en le reste de la division euclidienne de $N = 149 \times 52$ par 10.

On a démontré que $149 \equiv 9$ (mod. 10) et $52 \equiv 2$ (mod. 10).

Donc $149 \times 52 \equiv 9 \times 2$ (mod. 10).

D'où $149 \times 52 \equiv 18$ (mod. 10).

On peut multiplier les deux congruences membre à membre car on a le « même modulo » (si on n'a pas le même modulo, on ne peut pas les multiplier membre à membre).

Or $18 \equiv 8$ (mod. 10).

Donc $149 \times 52 \equiv 8$ (mod. 10).

Comme $0 \leqslant 8 < 10$, on peut affirmer que $149 \times 52 \equiv 8$ (mod. 10).

Donc le reste de la division euclidienne de N par 10 est 8.

4

$(x\,;y) \in \mathbb{Z}^2$

$x \equiv 4$ (mod. 7) (1)

$y \equiv 2$ (mod. 7) (2)

Démontrons que le nombre $3x+y$ est divisible par 7.

On a : $x \equiv 4$ (mod. 7) donc $3x \equiv 12$ (mod. 7) (3).

D'après (2) et (3), on a : $3x+y \equiv 12 + 2$ (mod. 7) soit $3x+y \equiv 14$ (mod. 7).

Or $14 \equiv 0$ (mod. 7).

Donc $3x+y \equiv 0$ (mod. 7).

Par suite, $7 \mid 3x+y$.

5

$n \in \mathbb{N}$

Démontrons que 5^n+19 est divisible par 4 en utilisant les congruences.

On raisonne en congruence modulo 4.

1ère méthode :

On a : $5 \equiv 1$ (mod. 4)

On choisit 1 car 1 est le plus petit entier naturel congru à 5 modulo 4. C'est le reste de la division euclidienne de 5 par 4.
Ce choix du 1 plutôt qu'un autre nombre s'explique aussi par la suite où nous allons élever les deux membres à la puissance n. Nous obtenons 1^n qui est égal à 1.

1
Pourquoi 1 ?
Je prends le plus petit qui présente un avantage pour les puissances.

On peut donc élever les deux membres de la relation à l'exposant *n*.
On obtient : $5^n \equiv 1^n \pmod 4$ soit $5^n \equiv 1 \pmod 4$.

On ajoute ensuite 19 à chaque membre de cette dernière relation (propriété du cours).
On obtient $5^n + 19 \equiv 20 \pmod 4$.

Or $20 \equiv 0 \pmod 4$.

D'où $5^n + 19 \equiv 0 \pmod 4$.

Par suite, $4 \mid 5^n + 19$.

2e méthode (variante de la 1ère méthode) :

$5 \equiv 1 \pmod 4$ donc $5^n \equiv 1^n \pmod 4$ soit $5^n \equiv 1 \pmod 4$.

$19 \equiv 3 \pmod 4$ [on a le droit de créer une congruence qui n'est pas demandée dans l'énoncé]

Donc $5^n + 19 \equiv 1 + 3 \pmod 4$ soit $5^n + 19 \equiv 4 \pmod 4$.

Or $4 \equiv 0 \pmod 4$.

D'où $5^n + 19 \equiv 0 \pmod 4$.

Par suite, $4 \mid 5^n + 19$.

6

$(x\,;y) \in \mathbb{Z}^2$

$x \equiv 4 \pmod{13}$

$y \equiv 5 \pmod{13}$

Démontrons que $x^2 + 2y$ est divisible par 13.

Le lundi 28-11-2016

On ne remplace pas *x* par 4 et *y* par 5.
On travaille avec les congruences.

Question de Marine Dartois : « Monsieur, est-ce qu'il faut remplacer *x* par 4 et *y* par 5 ? »
Moi : Ne pas remplacer *x* par 4 et *y* par 5.

$x \equiv 4 \pmod{13}$ donc $x^2 \equiv 16 \pmod{13}$ (1).

$y \equiv 5 \pmod{13}$ donc $2y \equiv 10 \pmod{13}$ (2).

D'après (1) et (2), on a : $x^2 + 2y \equiv 26 \pmod{13}$.

D'où $x^2 + 2y \equiv 0 \pmod{13}$.

Donc $13 \mid x^2 + 2y$.

7

$n \in \mathbb{N}$

Démontrons que $3^{2n} - 2^n$ est divisible par 7 en utilisant les congruences.

On a : $3^2 \equiv 2 \pmod 7$.
Donc $3^{2n} \equiv 2^n \pmod 7$.
D'où $3^{2n} - 2^n \equiv 0 \pmod 7$.

Par suite, $7 \mid 3^{2n} - 2^n$.

On fera attention qu'il s'agit bien d'un raisonnement déductif avec les mots « donc », « d'où », « par suite ». Les raisonnements ne fonctionnent que dans un sens. Il n'y a pas d'équivalence.

8

1°) **Démontrons que $12 \equiv -1 \pmod{13}$.**

$12 - (-1) = 13$

$13 \mid 13$

Donc $12 \equiv -1 \pmod{13}$.

2°) **Déterminer suivant les valeurs de l'entier naturel *n* le plus petit entier relatif en valeur absolue auquel est congru 12^n modulo 13.**

On reprend le résultat du 1°).

Par élévation des deux membres de la congruence à l'exposant *n*.

On obtient : $12^n \equiv (-1)^n \pmod{13}$.

On distingue deux cas suivants la parité de *n*.

1er cas : *n* pair
Dans ce cas, $12^n \equiv 1 \pmod{13}$.

2e cas : *n* impair
Dans ce cas, $12^n \equiv -1 \pmod{13}$.

9

$n \in \mathbb{N}$

Démontrons que $4^{3n} - 4^n$ est divisible par 5.

On a : $4^3 = 64$.
Donc $4^3 \equiv 4 \pmod 5$ d'où $4^{3n} \equiv 4^n \pmod 5$.
D'où $4^{3n} - 4^n \equiv 0 \pmod 5$.
On en déduit que $5 \mid 4^{3n} - 4^n$.

On n'est pas obligé de passer par la ligne $4^{3n}-4^n \equiv 0 \pmod 5$ puisque la congruence $4^{3n} \equiv 4^n \pmod 5$ se traduit immédiatement par $5 \mid 4^{3n}-4^n$.

10

$n \in \mathbb{Z}$ tel que $n \equiv 2 \pmod 5$

Démontrons que n^4+n-3 est divisible par 5.

$n \equiv 2 \pmod 5$ donc $n^4 \equiv 16 \pmod 5$.
D'où $n^4+n-3 \equiv 16+2-3 \pmod 5$ soit $n^4+n-3 \equiv 15 \pmod 5$ ou encore $n^4+n-3 \equiv 0 \pmod 5$.

On en déduit que $5 \mid n^4+n-3$.

11

1°) **Démontrons que $7 \equiv -1 \pmod 8$.**

$7-(-1)=8$ donc $7 \equiv -1 \pmod 8$.

2°) $n \in \mathbb{N}$

Démontrons que $7^{2n+1}+1$ est divisible par 8.

$7 \equiv -1 \pmod 8$ donc $7^{2n+1} \equiv -1 \pmod 8$ (car, comme $2n+1$ est un entier impair, $(-1)^{2n+1}=-1$) d'où 8 divise $7^{2n+1}+1$.

12

$n \in \mathbb{N}$

Démontrons que 10^n-1 est divisible par 9.

On va raisonner en congruences modulo 9.
$10 \equiv 1 \pmod 9$ donc $10^n \equiv 1 \pmod 9$.
D'où $10^n-1 \equiv 0 \pmod 9$.
On en déduit que $9 \mid 10^n-1$.

13

1°) **Démontrons que $10 \equiv -1 \pmod{11}$; $10^2 \equiv 1 \pmod{11}$; $10^3 \equiv -1 \pmod{11}$.**

$10+1=11$
$11 \mid 11$ donc $10 \equiv -1 \pmod{11}$.

En élevant au carré les deux membres de la congruence, on obtient : $10^2 \equiv 1 \pmod{11}$.
De même en élevant au cube les deux membres de la congruence, on obtient : $10^3 \equiv (-1)^3 \pmod{11}$
soit $10^3 \equiv -1 \pmod{11}$.

2°) **Déduisons-en le reste de la division euclidienne de 5869 par 11.**

On commence par décomposer le nombre 5869 en base 10.

$5869 = 5\times10^3 + 8\times10^2 + 6\times10^1 + 9$

D'après la question précédente, $10^3 \equiv -1$ (mod. 11), $10^2 \equiv 1$ (mod. 11), $10 \equiv -1$ (mod. 11) donc d'après les propriétés des congruences, $5869 \equiv 5\times(-1) + 8\times1 + 6\times(-1) + 9$ (mod. 11) soit $5869 \equiv -5 + 8 - 6 + 9$ (mod. 11).
Donc $5869 \equiv 6$ (mod. 11).

Comme $0 \leqslant 6 < 11$, le reste de la division euclidienne de 5869 par 11 est 6.

On retiendra la méthode de calcul du reste de la division euclidienne d'un entier naturel par 11 en utilisant la décomposition en base 10.
Le résultat est généralisé dans l'exercice **26** .

14

1°) **Démontrons sans calculatrice que $3^2 \equiv 2$ (mod. 7) ; $3^4 \equiv 4$ (mod. 7) ; $3^6 \equiv 1$ (mod. 7).**

L'intérêt de ce type de question c'est de se résoudre sans calculatrice.

• Justifions que $3^2 \equiv 2$ (mod. 7).

On a : $3^2 - 2 = 7$. Or $7 \mid 7$.
Donc $3^2 \equiv 2$ (mod. 7).

• Justifions que $3^4 \equiv 4$ (mod. 7).

On a : $3^2 \equiv 2$ (mod. 7) donc $3^4 \equiv 2^2$ (mod. 7) soit $3^4 \equiv 4$ (mod. 7).

• Justifions que $3^6 \equiv 1$ (mod. 7).

1ère méthode :

On part de la congruence $3^4 \equiv 4$ (mod. 7).

En multipliant les deux membres de la congruence par 3^2, on obtient : $3^4 \times 3^2 \equiv 4\times3^2$ (mod. 7).
Soit $3^6 \equiv 36$ (mod. 7).
Or $36 \equiv 1$ (mod. 7). Donc par transitivité de la relation de congruence, on a : $3^6 \equiv 1$ (mod. 7).

2e méthode :

Cette méthode est légèrement meilleure que la 1ère méthode.

On part de la congruence $3^2 \equiv 2$ (mod. 7).
On a donc $\left(3^2\right)^3 \equiv 2^3$ (mod. 7) soit $3^6 \equiv 8$ (mod. 7).
Or $8 \equiv 1$ (mod. 7) donc par transitivité de la relation de congruence, $3^6 \equiv 1$ (mod. 7).

2°)

• **Effectuons la division euclidienne de 1000 par 6.**

L'égalité de la division euclidienne de 1000 par 6 s'écrit : $1000 = 166 \times 6 + 4$.

• **Déduisons-en le reste de la division euclidienne de 3^{1000} par 7.**

D'après la question 1°), on a $3^6 \equiv 1 \pmod 7$ donc $\left(3^6\right)^{166} \equiv 1 \pmod 7$. Par suite, $3^{166\times 6} \equiv 1 \pmod 7$.

En multipliant les deux membres de cette relation par 3^4, on obtient $3^{166\times 6} \times 3^4 \equiv 3^4 \pmod 7$.

D'où $3^{166\times 6+4} \equiv 3^4 \pmod 7$ soit $3^{1000} \equiv 3^4 \pmod 7$.

Or d'après la question 1°), on a : $3^4 \equiv 4 \pmod 7$.

Donc par transitivité de la relation de congruence, on a : $3^{1000} \equiv 4 \pmod 7$.

Comme $0 \leqslant 4 < 7$, on en déduit que le reste de 3^{1000} par 7 est 4.

15 **Un exemple de codage affine**

$$p \equiv 3 \times n + 7 \pmod{26}$$

$$1 \leqslant p \leqslant 26$$

1°) **Table de cryptage :**

Lettre	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
n	1	2	3	4	5	6	7	8	9	10	11	12	13
p	10	13	16	19	22	25	2	5	8	11	14	17	20
Forme cryptée	J	M	P	S	V	Y	B	E	H	K	N	Q	T

Lettre	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
n	14	15	16	17	18	19	20	21	22	23	24	25	26
p	23	26	3	6	9	12	15	18	21	24	1	4	7
Forme cryptée	W	Z	C	F	I	L	O	R	U	X	A	D	G

L'application de codage doit être « injective » (deux lettres distinctes doivent avoir des images distinctes).

Exemples :

Lettre A ($n=1$), on a : $p \equiv 3\times 1+7 \pmod{26}$ c'est-à-dire $p \equiv 10 \pmod{26}$. Or $1 \leqslant p \leqslant 26$ donc $p=10$.
Lettre B ($n=2$), on a : $p \equiv 3\times 2+7 \pmod{26}$ soit $p \equiv 13 \pmod{26}$. Or $1 \leqslant p \leqslant 26$ donc $p=13$.

Etc.

On peut observer que p est le reste de la division euclidienne de $3n+1$ lorsque $1 \leqslant p \leqslant 25$.
Il est ainsi possible d'utiliser la calculatrice pour obtenir directement le tableau de correspondance.

Astuce de Virgile Boué le 1-2-2022 pour remplir le tableau :

Lettre	**A**	**B**	**C**
n	1	2	3
p	10	13	16

On observe 10, 13, 16. On ajoute 3 à chaque fois. Cela fait gagner beaucoup de temps.
La ligne avec les valeurs de p se remplit en deux minutes.

2°)

Message : MIJUZ CZRI OJ IVRLLHOV.

Forme décryptée du message : **BRAVO POUR TA REUSSITE**.

3°)

Message : MERCI.

Forme cryptée du message : **TVIPH**.

16 Codage affine

$p \equiv 3n+7 \pmod{10}$

1°) **Table de cryptage :**

On rappelle qu'un chiffre est compris entre 0 et 9 au sens large.

n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
p	7	0	3	6	9	2	5	8	1	4

L'astuce de Virgile Boué le 1-2-2022 pour remplir le tableau reste valable pour cet exercice.

Exemples :

Pour $n=0$, on a : $p \equiv 3\times 0+7 \pmod{10}$ soit $p \equiv 7 \pmod{10}$. Or $0 \leqslant p \leqslant 9$ donc $p=7$.
Pour $n=1$, on a : $p \equiv 3\times 1+7 \pmod{10}$ soit $p \equiv 10 \pmod{10}$. Or $0 \leqslant p \leqslant 9$ donc $p=0$.

Etc.

- On peut dire que p est le reste de la division euclidienne de $3n+7$ par 10.

- On peut aussi dire que p est le chiffre des unités du nombre $3n+7$.

On peut donc utiliser la calculatrice pour remplir le tableau de cryptage.

2°)

La forme cryptée de son code secret est 8503.
Son véritable code secret est **7612**.

17 Équation et tableau de congruences

1°) **Tableau de congruences**

Si $n \equiv \ldots \pmod{5}$	0	1	2	3	4
Alors $3n \equiv \ldots \pmod{5}$	0	3	1	4	2

Explication :

- Si $n \equiv 0 \pmod{5}$, alors $3n \equiv 0 \pmod{5}$.

- Si $n \equiv 1 \pmod{5}$, alors $3n \equiv 3 \pmod{5}$.

- Si $n \equiv 2 \pmod{5}$, alors $3n \equiv 6 \pmod{5}$.
Or $6 \equiv 1 \pmod{5}$.
Donc $3n \equiv 1 \pmod{5}$.

2°) **Déterminons tous les entiers relatifs n tels que $3n \equiv 2 \pmod{5}$ (1).**

Il s'agit d'une équation de congruence.

On peut essayer de résoudre directement l'équation (1).

1ère piste :

$(1) \Leftrightarrow 5 \mid 3n-2$

On ne sait pas quoi faire après.

2e piste :

$(1) \Leftrightarrow 3n = 2+5k \quad (k \in \mathbb{Z})$

Cette dernière égalité est inexploitable. On ne sait pas isoler *n*.

On va utiliser le tableau de congruences établi à la question précédente.

Il faut observer que le tableau donne tous les cas de congruence de n modulo 5.

On résout par équivalences. On n'écrit pas les lignes surlignées en jaune.

$(1) \Leftrightarrow 3n \equiv 2 \pmod 5$

$(1) \Leftrightarrow$ le reste de la division euclidienne de $3n$ par 5 est égal à 2

$(1) \Leftrightarrow$ le reste de la division euclidienne de n par 5 est égal à 4 (on regarde dans le tableau de congruence du 1°))

$\Leftrightarrow n \equiv 4 \pmod 5$ [pour écrire cette ligne, on remonte à la première ligne du tableau de congruences]

Conclusion :

Il y a trois manières de conclure :

• Les entiers relatifs cherchés sont tous les nombres congrus à 4 modulo 5.

• Les entiers relatifs sont les entiers de la forme $5k+4$ avec $k \in \mathbb{Z}$.

• Les entiers relatifs cherchés sont les entiers relatifs dont le reste de la division euclidienne par 5 est égal à 4.

Remarques :

• On ne peut pas diviser les deux membres de la relation (1) par 3. Il n'est pas possible d'isoler *n* dans le membre de gauche.
En effet, il n'y a pas de règle qui permette de diviser les deux membres par 3 ($\frac{2}{3}$ n'est pas entier).

• On observera que l'on a déterminé les entiers *n* qui vérifient (1) en utilisant un raisonnement par équivalences (« chaîne d'équivalences »).

3°) 3 et 5 sont premiers entre eux donc, d'après une propriété du cours, 3 admet un inverse modulo 5 pour la multiplication.
On cherche un inverse de 3 modulo 5.
On observe que $2 \times 3 \equiv 1 \pmod 5$ donc 2 est un inverse de 3 modulo 5.

On cherche les entiers relatifs *n* tels que $3n \equiv 2 \pmod 5$ (1).

On peut appliquer l'équivalence fondamentale :

$(1) \Leftrightarrow n \equiv 2\times 2 \pmod 5$

$\Leftrightarrow n \equiv 4 \pmod 5$

On conclut de la même manière qu'au 2°).

Explication :

$3n \equiv 2 \pmod 5 \Leftrightarrow n \equiv 2\times \text{inv}(3) \pmod 5$

$\downarrow$

2

18

1°) **Tableau de congruence modulo 7 :**

Si $a \equiv \ldots \pmod 7$	0	1	2	3	4	5	6
Alors $a^3 \equiv \ldots \pmod 7$	0	1	1	– 1	1	– 1	– 1

Explication :

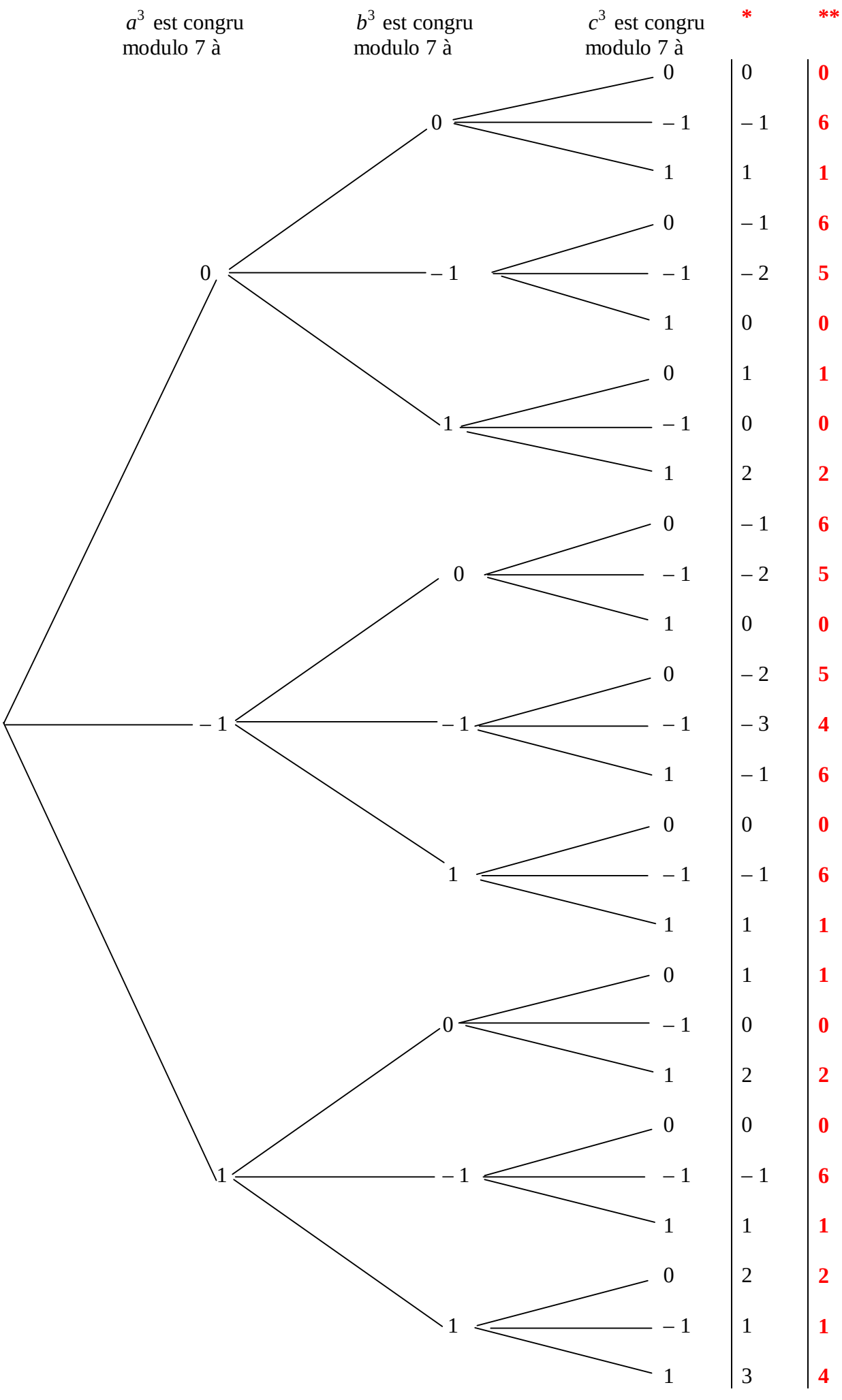
Pour $a \equiv 3 \pmod 7$, on a $a^3 \equiv 27 \pmod 7$. Or $27 \equiv 6 \pmod 7$ donc $a^3 \equiv 6 \pmod 7$.
On pourrait mettre 6 dans le tableau. J'ai décide de donner l'entier dont la valeur absolue est la plus petite possible.

2°) $(a, b, c) \in \mathbb{Z}^3$

Déterminons les restes possibles dans la division euclidienne par 7 de l'entier $a^3 + b^3 + c^3$.

On constate que le cube d'un entier relatif est congru soit à 1, soit à – 1, soit à 0.

Pour répondre à la question 2°), le plus judicieux est de procéder par un arbre : c'est un arbre ternaire.
On prend une page complète.
On fait toutes les branches à la règle.


a^3 est congru modulo 7 à
b^3 est congru modulo 7 à
c^3 est congru modulo 7 à
*
**
0
0
0
0
0
0
– 1
– 1
– 1
6
1
1
1
0
– 1
6
– 1
– 1
– 2
5
1
0
0
1
0
1
1
– 1
0
0
1
2
2
0
– 1
6
0
– 1
– 2
5
1
0
0
– 1
0
– 2
5
– 1
– 1
– 3
4
1
– 1
6
1
0
0
0
– 1
– 1
6
1
1
1
0
1
1
0
– 1
0
0
1
2
2
1
0
0
0
– 1
– 1
6
1
1
1
0
2
2
– 1
1
1
3
4

* $a^3+b^3+c^3$ est congru modulo 7 à :

** reste de la division euclidienne de $a^3+b^3+c^3$ par 7

$a \equiv .....$ (mod. n)

Souvent, on « congrue » le plus petit entier compris entre 0 et $n-1$ (au sens large)
On donne le plus entier naturel congru. Il s'agit dans ce cas du reste de la division euclidienne.

Mais il arrive aussi qu'on congrue avec un entier relatif dont la valeur absolue est inférieure ou égale à la partie entière de $\frac{n}{2}$ (de $-\mathrm{E}\left(\frac{n}{2}\right)$ à $\mathrm{E}\left(\frac{n}{2}\right)$).

3°) **Démontrons que si 7 divise $a^3+b^3+c^3$, alors 7 divise abc.**

- On utilise l'arbre réalisé à la question précédente.
- C'est la seule méthode pour répondre proprement à la question.

Il est possible de ne pas faire d'arbre. On cherche les possibilités d'écrire 0 avec 0, 1 et – 1.

On constate dans l'arbre que, lorsque la somme $a^3+b^3+c^3$ est congrue à 0 modulo 7, l'un au moins des trois entiers a^3, b^3, c^3 est congru à 0 modulo 7 (c'est-à-dire que l'on a $a^3+b^3+c^3 \equiv 0$ modulo 7, on a un 0 au moins une fois sur l'une des branches qui conduisent au résultat).

D'après le tableau de la première question, le cube d'un entier relatif est congru à 0 modulo 7 si et seulement si cet entier est congru à 0 modulo 7. Autrement dit, le cube d'un entier relatif est divisible par 7 si et seulement si cet entier est divisible par 7.

Donc si 7 divise $a^3+b^3+c^3$, alors 7 divise a ou 7 divise b ou 7 divise c.

Dans ce cas, 7 divise le produit abc.

La réciproque de cette propriété est fausse.
Par exemple, si on prend $a=0$, $b=0$, $c=1$, on a bien 7 qui divise le produit abc mais 7 ne divise pas $a^3+b^3+c^3$.

Autre méthode :

Il y a 7 cas qui donnent 0 comme reste de la division euclidienne de $a^3+b^3+c^3$ par 7.

Les triplets de $\left(a^3\,;b^3\,;c^3\right)$ correspondants sont :

$(0\,;0\,;0)$

$(0\,;-1\,;1)$

$(0\,;1\,;-1)$

$(-1\,;0\,;1)$

$(-1\,;1\,;0)$

$(1\,;0\,;-1)$

$(1\,;-1\,;0)$

Pour chacun de ces triplets, il y a au moins un 0, ce qui signifie que l'un des trois nombres a^3, b^3 ou c^3 est congru à 0 modulo 7.

On peut formuler le résultat avec les mots « condition nécessaire », « condition suffisante ».

• Une condition nécessaire et suffisante pour que « 7 divise $a^3+b^3+c^3$ » est « 7 divise abc ».

• Une condition suffisante pour que « 7 divise abc » est « 7 divise $a^3+b^3+c^3$ ».

Attention à ne pas faire le raisonnement suivant qui est faux :
« Si $a^3+b^3+c^3\equiv 0$ (mod. 7), alors $a\equiv 0$ (mod. 7) ou $b\equiv 0$ (mod. 7) ou $c\equiv 0$ (mod. 7) ».

19 Cet exercice est particulièrement important.

1°) **Déterminons selon les valeurs de l'entier relatif *x*, à quoi est congru x^2 modulo 5.**

Si $x\equiv\ldots$ [5]	0	1	2	3	4
Alors $x^2\equiv\ldots$ [5]	0	1	4	9 4	16 1

On raisonne par **disjonction de cas**.

Soit *x* un entier relatif.

On note *r* son reste dans la division euclidienne par 5.

$r\in\{0,1,2,3,4\}$

Il n'y a que cinq valeurs possibles du reste.

1er cas : $r=0$
Dans ce cas, $x\equiv 0$ (mod. 5).
On a alors : $x^2\equiv 0$ (mod. 5).

2e cas : $r = 1$

Dans ce cas, $x \equiv 1 \pmod 5$.

On a alors : $x^2 \equiv 1 \pmod 5$.

3e cas : $r = 2$

Dans ce cas, $x \equiv 2 \pmod 5$.

On a alors : $x^2 \equiv 4 \pmod 5$ (par élévation des deux membres au même exposant).

On pourrait aussi écrire : $x^2 \equiv -1 \pmod 5$ mais l'énoncé nous demande de donner le résultat sous la forme d'un entier compris entre 0 et 4.

4e cas : $r = 3$

Dans ce cas, $x \equiv 3 \pmod 5$.

On a alors : $x^2 \equiv 4 \pmod 5$ (car $9 \equiv 4 \pmod 5$).

5e cas : $r = 4$

Dans ce cas, $x \equiv 4 \pmod 5$.

On a alors : $x^2 \equiv 1 \pmod 5$ (car $16 \equiv 1 \pmod 5$).

On peut conclure la question de la manière suivante :

Pour tout entier relatif x, x^2 est congru à 0, 1 ou 4 modulo 5.

Autre manière de répondre (plus rapide) :

On dresse un tableau de congruences.

$x \equiv \ldots [5]$	0	1	2	3	4
$x^2 \equiv \ldots [5]$	0	1	4	4	1

2°) $x^2 - 5y^2 = 3$ (E) avec $(x\,;y) \in \mathbb{Z}^2$

Il s'agit d'une **équation diophantienne**.

Démontrons que l'équation (E) n'a pas de solution.

On va s'intéresser à la non existence de solutions entières de cette équation en utilisant les congruences.

On raisonne par l'absurde.

On suppose qu'il existe un couple (x_0, y_0) d'entiers relatifs solution de (E) [on peut aussi écrire $(x_0, y_0) \in \mathbb{Z}^2$].

On a alors $x_0^{\,2} - 5y_0^{\,2} = 3$ d'où $x_0^{\,2} = 3 + 5y_0^{\,2}$ (on a un raisonnement par déductions, pas d'équivalences).
Cette égalité peut s'interpréter de la manière suivante : le reste de la division euclidienne de $x_0^{\,2}$ par 5 est égal à 3.

Par conséquent, on peut dire aussi : $x_0^2 \equiv 3 \pmod 5$.

Ce point peut être démontré sans utiliser la division euclidienne.

1ère manière : utilisation des propriétés sur les congruences

En effet, $5 \equiv 0 \pmod 5$ donc $5y_0^2 \equiv 0 \pmod 5$.
D'où $3+5y_0^2 \equiv 3 \pmod 5$.
On en déduit que $x_0^2 \equiv 3 \pmod 5$.

En version plus courte, on peut dire que l'on « congrue » les deux membres de l'égalité $x_0^2 = 3+5y_0^2$ modulo 5.

2e manière : utilisation de la propriété : $a \equiv b \pmod n \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

On a $x_0^2 = 3+5\times y_0^2$ et $y_0^2 \in \mathbb{Z}$ donc $x_0^2 \equiv 3 \pmod 5$.

D'après le tableau de congruence précédent, nous observons que ce n'est pas possible.

Autre manière de répondre :

(E) implique que $x^2 \equiv 3$ [5] ce qui est impossible d'après le tableau de congruence de la question 1°).

On en déduit que (E) n'a donc pas de solution.

20

1°) **Déterminons suivant les valeurs de l'entier naturel *n*, le reste de la division euclidienne de 2^n par 7.**

Plutôt que de dire « suivant les valeurs de *n* » on devrait dire « suivant les valeurs du reste de l'entier *n* par … »

$2^0 \equiv 1 \pmod 7$
$2^1 \equiv 2 \pmod 7$
$2^2 \equiv 4 \pmod 7$
$2^3 \equiv 1 \pmod 7$
$2^4 \equiv 2 \pmod 7$
$2^5 \equiv 4 \pmod 7$

Il semble :
- que le reste de la division euclidienne de 2^n par 7 ne puisse rendre que 3 valeurs : 1, 2, 4.
- qu'il y ait une périodicité de « période » 3.

Le 3 n'a rien à voir avec le 7 du modulo. Il se réfère juste aux exposant de 2.

Soit *n* un entier naturel.

On sait que *n* est soit de la forme $3k$ avec $k \in \mathbb{N}$, soit de la forme $3k+1$ avec $k \in \mathbb{N}$, soit de la forme $3k+2$ avec $k \in \mathbb{N}$ ».
On distingue donc 3 cas.

1er cas : $n = 3k \quad (k \in \mathbb{N})$

On a alors $2^n = 2^{3k}$.
Or $2^3 \equiv 1 \pmod 7$ d'où $2^{3k} \equiv 1^k \pmod 7$ soit $2^n \equiv 1 \pmod 7$.
Par suite, le reste de la division euclidienne de 2^n par 7 est 1.

2e cas : $n = 3k + 1 \quad (k \in \mathbb{N})$

On a alors $2^n = 2^{3k+1}$.
Or $2^{3k} \equiv 1 \pmod 7$ d'où $2^{3k+1} \equiv 2 \pmod 7$.
Par suite, le reste de la division euclidienne de 2^n par 7 est 2.

3e cas : $n = 3k + 2 \quad (k \in \mathbb{N})$.
On a alors $2^n = 2^{3k+2}$.
Or $2^{3k+1} \equiv 2 \pmod 7$ d'où $2^{3k+2} \equiv 4 \pmod 7$.
Par suite, le reste de la division euclidienne de 2^n par 7 est 4.

Bilan :

- Si n est de la forme $3k$ avec $k \in \mathbb{N}$, alors le reste de la division euclidienne de 2^n par 7 est 1.
- Si n est de la forme $3k+1$ avec $k \in \mathbb{N}$, alors le reste de la division euclidienne de 2^n par 7 est 2.
- Si n est de la forme $3k+2$ avec $k \in \mathbb{N}$, alors le reste de la division euclidienne de 2^n par 7 est 4.

2°) **Déduisons-en le reste de la division euclidienne par 7 du nombre $N = 247^{349}$.**

On a $247 \equiv 2 \pmod 7$ donc $247^{349} \equiv 2^{349} \pmod 7$ [propriété des congruences] soit $N \equiv 2^{349} \pmod 7$.

On a $349 = 116 \times 3 + 1$ donc 349 est de la forme $3k+1$ avec $k \in \mathbb{N}$.

1ère façon pour conclure :

D'après la question 1°), le reste de la division euclidienne de 247^{349} par 7 est le même que celui de 2^{349} par 7 c'est-à-dire 2.

2e façon pour conclure :

D'après la question 1°), le reste de la division euclidienne de 2^{349} par 7 est égal à 2 donc $2^{349} \equiv 2 \pmod 7$.

Par transitivité de la relation de congruence, on obtient $N \equiv 2 \pmod 7$.

Or $0 \leqslant 2 < 7$.

On en déduit que le reste de la division euclidienne de N par 7 est 2.

21

Recopier et compléter la deuxième ligne du tableau de congruences suivant en écrivant chaque fois le plus petit entier naturel :

Si $n \equiv \dots$ (mod. 3)	0	1	2
Alors $n^3 \equiv \dots$ (mod. 3)	0	1	2

On effectue les calculs de tête.
Il s'agit chaque fois du reste de la division euclidienne de n^3 par 3.

En déduire que, pour tout entier relatif n, $n^3 - n$ est divisible par 3.

Dans les trois cas, on constate que $n^3 \equiv n$ (modulo 3).

On en déduit que : $\forall n \in \mathbb{Z} \quad 3 \mid n^3 - n$.

Commentaire : Nous verrons plus tard que cette propriété est un cas particulier du Petit théorème de Fermat.

22

Démontrons que pour tout entier relatif n, $n^5 - n$ est divisible par 5.

Méthode : On raisonne modulo 5.
On utilise un tableau de congruences.

Si $n \equiv \dots$ (mod. 5)	0	1	2	3	4
Alors $n^3 \equiv \dots$ (mod. 5)	0	1	2	3	4

Dans un contrôle, les calculs ne sont pas à détailler.
On fait directement le tableau en mettant les différents restes et en écrivant les valeurs de la 2e ligne.

Dans les cinq cas, on constate que $n^5 \equiv n$ (modulo 5).

On en déduit que : $\forall n \in \mathbb{Z} \quad 5 \mid n^5 - n$.

Commentaire : Comme dans l'exercice précédent, nous verrons plus tard que cette propriété est un cas particulier du « petit théorème de Fermat ».

23

Déterminons les entiers relatifs n tels que l'entier $N = n^2 - 3n + 7$ soit divisible par 5.

Méthode : On raisonne modulo 5.

On commence par retranscrire le problème « en modulo ».

On cherche les entiers relatifs n tels que $N \equiv 0 \pmod 5$ (1).

On dresse alors un tableau de congruences modulo 5.

Si $n \equiv \ldots \pmod 5$	0	1	2	3	4
Alors $N \equiv \ldots \pmod 5$	7 2	5 0	5 0	7 2	11 1

Les nombres écrits en rouge correspondent aux restes de la division euclidienne de N par 5.

D'après le tableau (on remonte à la 1ère ligne), on voit que $(1) \Leftrightarrow n \equiv 1 \pmod 5$ ou $n \equiv 2 \pmod 5$.

On conclut :

Les entiers cherchés sont les entiers congrus à 1 ou à 2 modulo 5.

24

Déterminons le chiffre x tel que l'entier $\overline{53x4}$ soit divisible par 9.

1ère méthode :

On teste tous les chiffres de 0 à 9. On pourrait éventuellement utiliser un programme Python.

2e méthode :

On applique le critère de divisibilité par 9.

La somme des chiffres est égale à $5+3+x+4=12+x$.

Or x est un chiffre donc compris entre 0 et 9. Par suite, $12+x$ est compris entre 12 et 21.

$\overline{53x4}$ est divisible par 9 $\Leftrightarrow$ $12+x$ est divisible par 9

$\Leftrightarrow x = 6$ (car le seul entier compris entre 12 et 21 divisible par 9 est 18)

3e méthode :

On utilise la propriété : « Tout entier naturel est congru à la somme des chiffres de son écriture en base dix ».

On pose $N = \overline{53x4}$.

On a donc $N \equiv x+12 \pmod 9$ d'où $N \equiv x+3 \pmod 9$.

On cherche le(s) chiffre(s) x tels que $x+3$ soit divisible par 9.

Une condition nécessaire et suffisante pour que $\overline{53x4}$ soit divisible par 9 est $x=6$.

Ancienne version :

$\overline{53x4}$ est divisible par 9 si et seulement si $5+3+x+4$ est divisible par 9
si et seulement si $12+x$ est divisible par 9
si et seulement si $x=6$ (on n'écrit pas tout le détail de la recherche)

Une condition nécessaire et suffisante pour que $\overline{53x4}$ soit divisible par 9 est $x=6$.

Autre rédaction :

Déterminer x tel que $9 \mid \overline{53x4}$ (1).

(1) $\Leftrightarrow 9 \mid 12+x$

$\Leftrightarrow 12+x=18$

$\Leftrightarrow x=6$ (car x est un chiffre donc $0 \leqslant x \leqslant 9$)

25

Déterminons les chiffres x et y tels que l'entier $\overline{3x2y}$ soit divisible par 4 et 3.

Version 9-2-2022

On pose $N=\overline{3x2y}$.

On cherche x et y tels que N soit divisible par 4 et 3.

1ère méthode : On teste toutes les valeurs de x et y. On peut éventuellement utiliser un programme Python.

2e méthode : On applique les critères de divisibilité.

N est divisible par 4 si et seulement si $\overline{2y}$ est divisible par 4

si et seulement si $y=0$ ou $y=4$ ou $y=8$

N est divisible par 3 si et seulement si $3+x+2+y=x+y+5$ est divisible par 3.

$\begin{cases} x=1 \\ y=0 \end{cases}$ $\begin{cases} x=4 \\ y=0 \end{cases}$ $\begin{cases} x=7 \\ y=0 \end{cases}$ $\begin{cases} x=0 \\ y=4 \end{cases}$ $\begin{cases} x=3 \\ y=4 \end{cases}$ $\begin{cases} x=6 \\ y=4 \end{cases}$ $\begin{cases} x=9 \\ y=4 \end{cases}$ $\begin{cases} x=2 \\ y=8 \end{cases}$ $\begin{cases} x=5 \\ y=8 \end{cases}$ $\begin{cases} x=8 \\ y=8 \end{cases}$

Version du 19 novembre 2019

$4 \mid \overline{2y} \Leftrightarrow \ldots$

divisibilité par 4

$\overline{2\ldots}$
$\uparrow$
$0 \leqslant y \leqslant 9$

$\overline{3x2y}$ est divisible par 4 et 3 si et seulement si $\overline{2y}$ est divisible par 4 et $3+x+2+y$ est divisible par 3.

On applique les critères de divisibilité par 4 et 3.

$\overline{2y}$ est divisible par 4 si et seulement $y=0$ ou $y=4$ ou $y=8$.

$3+x+2+y=x+y+5$

On donne la liste des possibilités pour lesquelles $\overline{3x2y}$ est divisible par 4 et 3 :

$\begin{cases} x=1 \\ y=0 \end{cases}$

$\begin{cases} x=4 \\ y=0 \end{cases}$

$\begin{cases} x=7 \\ y=0 \end{cases}$

$\begin{cases} x=0 \\ y=4 \end{cases}$

$\begin{cases} x=3 \\ y=4 \end{cases}$

$\begin{cases} x=6 \\ y=4 \end{cases}$

$\begin{cases} x=9 \\ y=4 \end{cases}$

$\begin{cases} x=2 \\ y=8 \end{cases}$

$\begin{cases} x=5 \\ y=8 \end{cases}$

$\begin{cases} x=8 \\ y=8 \end{cases}$

Autre solution :

$4 \mid \overline{3x2y} \Leftrightarrow 4 \mid \overline{2y}$ (critère de divisibilité par 4)

$\Leftrightarrow y = 0$ ou $y = 4$ ou $y = 8$

On rappelle que *y* est un entier compris entre 0 et 9 puisque c'est un chiffre. On cherche donc les entiers *y* compris entre 0 et 9 tels que $\overline{2y}$ soit divisible par 4.

$3 \mid \overline{3x2y} \Leftrightarrow 3 \mid 3+x+2+y$

$\Leftrightarrow 3 \mid x+y+5$

Pour $y = 0$, on doit avoir $3 \mid x+5$.
Les valeurs possibles de *x* sont (on évite le mot « solution ») 1 ; 4 ; 7.

Pour $y = 4$, on doit avoir $3 \mid x+9$.
Les valeurs possibles de *x* sont 0 ; 3 ; 6 ; 9.

Pour $y = 8$, on doit avoir $3 \mid x+13$.
Les valeurs possibles de *x* sont 2 ; 5 ; 8.

Les couples (*x* ; *y*) possibles pour que l'entier $\overline{3x2y}$ soit divisible par 3 et 4 sont :
(1 ; 0) ; (4 ; 0) ; (7 ; 0) ; (0 ; 4) ; (3 ; 4) ; (6 ; 4) ; (9 ; 4) ; (2 ; 8) ; (5 ; 8) ; (8 ; 8).

25 bis

On calcule la somme des chiffres : $S = 3+4+4+4+2+0+5+7$.
On effectue le calcul modulo 3.
3 est congru à 0 modulo 3.
$4+4+4 = 3\times 4$ est congru à 0 modulo 3.
$5+7 = 12$ est congru à 0 modulo 3.
On en déduit que S est congru à 2 modulo 3.
Le reste de la division euclidienne de 34442057 par 3 est donc égal à 2.
On peut vérifier le résultat à l'aide de la calculatrice.

26 Critère de divisibilité par 11 sera corrigé en clase

1°) Démontrons que $10 \equiv -1$ (mod. 11).

$10-(-1) = 11$
11 est divisible par 11.
On a donc $10 \equiv -1$ (mod. 11).

2°)

$N = \overline{a_n a_{n-1} \ldots a_0 a_1}$ (écriture en base dix)

On a donc : $N = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10 a_1 + a_0$ (décomposition en base dix du nombre N).

Par commodité, on utilise le symbole Σ (plus simple pour la démonstration).

On a $N = \sum_{k=0}^{k=n} a_k 10^k \quad (1)$.

Comme $10 \equiv -1 \pmod{11}$, $\forall k \in \mathbb{N} \quad 10^k \equiv (-1)^k \pmod{11}$.

Par passage aux congruences, en utilisant les propriétés, (1) entraîne $N \equiv \sum_{k=0}^{k=n} a_k \times (-1)^k \pmod{11}$ ou

On peut donc écrire $\boxed{N \equiv \sum_{k=0}^{k=n} (-1)^k a_k \pmod{11}}$.

↓

somme « alternée » des chiffres de l'écriture en base dix de N

$a_0 - a_1 + a_2 - \ldots$

Cette relation est fondamentale. On observera que l'on part du chiffre le plus à droite (chiffre des unités).

Ancienne version :
On a établi que $10 \equiv -1 \pmod{11}$.

Donc pour tout entier naturel *k*, on a :

$10^{2k} \equiv 1 \pmod{11}$
$10^{2k+1} \equiv -1 \pmod{11}$

On a : $10 \equiv -1 \pmod{11}$ donc $10a_1 \equiv -a_1 \pmod{11}$.

On a : $10^2 \equiv 1 \pmod{11}$ donc $10^2 a_2 \equiv a_2 \pmod{11}$.

On a : $10^3 \equiv -1 \pmod{11}$ donc $10^3 a_3 \equiv -a_3 \pmod{11}$.

On a : $N = a_0 + 10a_1 + 10^2 a_2 + \ldots$ donc d'après ce qui précède : $N \equiv a_0 - a_1 + a_2 - \ldots \pmod{11}$.

Remarque :

Application :

Le 13-1-2024

On calcule $S = 7 - 5 - 0 - 2 + 4 - 4 - 3 = 1$.
Le reste de la division euclidienne de 34442057 par 11est égal à 1.

3°) **Démontrons que N est divisible par 11 si et seulement si la somme alternée $a_0 - a_1 + a_2 - \ldots$ est divisible par 11.**

On reprend la relation : $N \equiv \sum_{k=0}^{k=n} (-1)^k a_k \pmod{11}$.

$11 \mid N \Leftrightarrow 11 \mid \sum_{k=0}^{k=n} (-1)^k a_k$ (propriété du cours)

Ancienne version :

Donc N est divisible par 11 si et seulement si $a_0 - a_1 + a_2 - \ldots \equiv 0 \pmod{11}$.

On peut écrire les équivalences :

$11 \mid N \Leftrightarrow N \equiv 0 \pmod{11}$

$11 \mid N \Leftrightarrow \sum_{k=0}^{k=n} (-1)^k a_k \equiv 0 \pmod{11}$ [par transitivité de la relation de congruence]

Énoncé du critère de divisibilité par 11 :

« Un entier naturel est divisible par 11 si et seulement si la différence de ses chiffres de rang pair et de ses chiffres de rang impair est divisible par 11 ».

4°) **Appliquons le critère précédent aux nombres 25 418 792 et 851 047 932 152.**

- **25 418 792**

On calcule : $2-9+7-8+1-4+5-2=-8$.

Le résultat n'est pas divisible par 11.

Donc 25 418 792 n'est pas divisible par 11.

- **851 047 932 152**

On calcule : $2-5+1-2+3-9+7-4+0-1+5-8=-11$.

Le résultat est divisible par 11.

Donc 851 047 932 152 est divisible par 11.

27

1°)

15 et 26 sont premiers entre eux donc 15 admet un inverse modulo 26.

Pour déterminer un inverse de 15 modulo 26, on peut essentiellement utiliser deux méthodes :
- par tâtonnement ;
- par la calculatrice en utilisant la fonction $Y1 = \text{reste}(15X, 26)$ (on cherche dans le tableau de valeurs une valeur de X pour laquelle le résultat est égal à 1).

On a $7\times15\equiv1$ (mod. 26) (car $7\times15=105$; $105-1=104=26\times4$).
On en déduit que 7 est un inverse de 15 modulo 26.

$y\equiv15x+7$ [26] (1)

$(1)\Leftrightarrow 15x\equiv y-7$ (mod. 26)

$\Leftrightarrow x\equiv7(y-7)$ (mod. 26)

$\Leftrightarrow x\equiv7y-49$ (mod. 26)

$\Leftrightarrow x\equiv7y+3$ (mod. 26) car $-49\equiv3$ (mod.26)

2°) **Déduisons-en le système de décodage.**

Les chiffres attribués aux lettres vont de 0 à 25 donc la relation (2) exprimer que x est le reste de la division euclidienne de $7y+3$ par 26.

lettre du message codé $\rightarrow y\rightarrow$ reste de la DE de $7y+3$ par 26 $\rightarrow$ lettre du message initial
3°) **Décodons le mot WHL.**

W $\rightarrow$ 22 $\rightarrow$ 1 $\rightarrow$ B
H $\rightarrow$ 7 $\rightarrow$ 0 $\rightarrow$ A
L $\rightarrow$ 11 $\rightarrow$ 2 $\rightarrow$ C

On observera que la fonction de codage est $f: x\mapsto$ reste de la division euclidienne de $15x+7$ par 26 et que la fonction de décodage est $g: x\mapsto$ reste de la division euclidienne de $7x+3$ par 26.

28

Version écrite le 30-5-2020 :

1°) On commence par calculer le déterminant de M.

$\det M=3\times(-1)-1\times1=-3-1=-4$

– 4 et 13 sont premiers entre eux donc M admet un inverse modulo 13.

On cherche un inverse de – 4 modulo 13 c'est-à-dire un entier relatif u tel que $-4\times u\equiv1$ (mod. 13).
On vérifie sans peine que 3 est un inverse de – 4 modulo 13 car $-4\times3=-12$ et $-12\equiv1$ (mod. 13)

On applique la formule. La matrice $M'=3\begin{pmatrix}-1&-1\\-1&3\end{pmatrix}$ est un inverse de M modulo 13.

On peut vérifier par le calcul que $M'M\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}$ (mod. 13) et $MM'\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}$ (mod. 13).

2°)

Il s'agit de résoudre un système de congruences.

Le système s'écrit matriciellement $MX \equiv A \pmod{13}$. On note (E) cette congruence.

(E) $\Leftrightarrow X \equiv M'Y \pmod{13}$

$\Leftrightarrow X \equiv \begin{pmatrix} -18 \\ 42 \end{pmatrix} \pmod{13}$

$\Leftrightarrow X \equiv \begin{pmatrix} 8 \\ 3 \end{pmatrix} \pmod{13}$

$\Leftrightarrow \begin{cases} x \equiv 8 \pmod{13} \\ y \equiv 3 \pmod{13} \end{cases}$

1ère manière de conclure :

Les solutions du système (S) sont les couples $(x\,;y)$ d'entiers relatifs tels que $x \equiv 8 \pmod{13}$ et $y \equiv 3 \pmod{13}$.

2e manière de conclure :
Les solutions du système (S) sont les couples de la forme $(8+13k\,;3+13k')$ où k et k' sont des entiers relatifs quelconque.

3°) On vérifie les solutions avec le site « dcode ».

29 Le chiffrement de Hill

Dans cet exercice, on travaille en congruences de matrices modulo 26.

$A = \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$

1°)

$\det A = 11\times 4 - 7\times 3 = 44 - 21 = 23$

23 et 26 sont premiers entre eux donc 23 admet un inverse modulo 26.

On trouve aisément que 17 est un inverse de modulo 26 (par exemple, calculatrice en utilisant la fonction x reste de la division euclidienne de $23x$ par 26 ou site dcode, rubrique inverse modulaire).

On applique la formule. La matrice $A' = 17\begin{pmatrix} 4 & -3 \\ -7 & 11 \end{pmatrix}$ est un inverse de A modulo 26.

En calculant les restes des divisions euclidiennes par 26 des coefficients de A', on démontre que $A' \equiv \begin{pmatrix} 16 & 1 \\ 11 & 5 \end{pmatrix} \pmod{26}$.

On en déduit que la matrice $B = \begin{pmatrix} 16 & 1 \\ 11 & 5 \end{pmatrix}$ est un inverse de A modulo 26.

2°) Justifier que $Y \equiv AX \pmod{26}$ puis que $X \equiv BY \pmod{26}$.
En déduire que la matrice B est la matrice de décodage.

On a $Z = AX$ et $Z \equiv Y \pmod{26}$ de manière évidente.
On en déduit que $Y \equiv AX \pmod{26}$.

Comme B est l'inverse de A modulo 26, on peut dire, d'après le résultat de l'encadré, la relation $Y \equiv AX \pmod{26}$ est équivalente à $X \equiv BY \pmod{26}$.

3°) Décodons le mot YJ.

$y_1 = 24$ et $y_2 = 9$
D'où $Y = \begin{pmatrix} 24 \\ 9 \end{pmatrix}$.
Or $X \equiv BY \pmod{26}$ qui donne $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv \begin{pmatrix} 16 & 1 \\ 11 & 5 \end{pmatrix}\begin{pmatrix} 24 \\ 9 \end{pmatrix} \pmod{26}$.
On obtient $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv \begin{pmatrix} 393 \\ 309 \end{pmatrix} \pmod{26}$.

On a donc $x_1 \equiv 393 \pmod{26}$ et $x_2 \equiv 309 \pmod{26}$.
Comme x_1 et x_2 sont des entiers compris entre 0 et 25, on en déduit que $x_1 = 3$ et $x_2 = 23$.
On en conclut que le mot « YJ » décodé donne « DX ».

Remarque :

Le codage DX est le nom donné à un élégant codage des films photographiques 35 mm argentiques au format 24×36. L'auteur de l'exercice a peut-être utilisé ce type de film il y a de ça des années avant l'avènement des appareils numériques. Mais peut-être s'agit-il seulement d'un « simple » hasard…