

Division euclidienne (b)

→ *Les commentaires en italique ne font pas partie de la rédaction des solutions !*

Exercice b.1 *L'exercice peut se résoudre uniquement avec la DE, comme dans la première solution ci-dessous. Si on dispose en plus de l'outil des congruences (qu'on a maintenant fait en cours) on peut aussi rédiger comme dans la deuxième solution.*

1^{ère} solution. Les DE de m et n par 17 sont $\left(\begin{array}{l} m = 17q + 8 \text{ avec } 0 \leq 8 < 17 \\ n = 17q' + 12 \text{ avec } 0 \leq 12 < 17 \end{array} \right)$ donc :

$$m + n = 17(q + q') + 20 = 17(q + q') + 17 + 3 = 17(q + q' + 1) + 3$$

(on utilise la DE : $20 = 17 + 3$). On reconnaît la DE de $m + n$ par 17 avec un reste égal à 3.

$$mn = (17q + 8)(17q' + 12) = 17(17qq' + 12q + 8q') + 8 \times 12 = 17(17qq' + 12q + 8q' + 5) + 11$$

(on utilise la DE : $96 = 5 \times 17 + 11$). On reconnaît la DE de mn par 17 avec un reste égal à 11.

$$m^2 = (17q + 8)^2 = 17^2q^2 + 2 \times 8 \times 17q + 64 = 17(17q^2 + 16q + 3) + 13$$

(on utilise la DE : $64 = 3 \times 17 + 13$). On reconnaît la DE de m^2 par 17 avec un reste égal à 13.

2^{ème} solution. Raisonnons modulo 17 ; pour simplifier on note $a \equiv b$ au lieu de $a \equiv b \pmod{17}$. Alors,

(1) $m \equiv 8$ et $n \equiv 12 \Rightarrow m + n \equiv 8 + 12 \equiv 3$. Le reste de la DE de $m + n$ par 17 est donc 3.

(2) $m \equiv 8$ et $n \equiv 12 \Rightarrow mn \equiv 8 \times 12 \equiv 11$. Le reste de la DE de mn par 17 est donc 11.

(3) $m \equiv 8 \Rightarrow m^2 \equiv 8^2 \equiv 13$. Le reste de la DE de m^2 par 17 est donc 13.

Exercice b.2 *Proposons deux solutions comme à l'exercice précédent.*

1^{ère} solution. Avec les premiers entiers n on a les DE : $10 = 6 + 4$, $100 = 6 \times 16 + 4$, $1000 = 6 \times 166 + 4$... On voit que le reste est 4. On le prouve par récurrence, en montrant que pour tout $n \geq 1$, $P(n)$: le reste de la DE de 10^n par 6 est 4. On a déjà montré que $P(1)$ est vraie. Supposant que $P(n)$ est vraie on a $10^n = 6q_n + 4$ et donc $10^{n+1} = 10 \times 10^n = 10(6q_n + 4) = 60q_n + 40 = 60q_n + 36 + 4 = 6(10q_n + 6) + 4$. On reconnaît la DE de 10^{n+1} par 6 avec un reste égal à 4. Donc $P(n)$ est vraie pour tout n .

2^{ème} solution. Raisonnons modulo 6 ; pour simplifier on note $a \equiv b$ au lieu de $a \equiv b \pmod{6}$. On montre par récurrence que $P(n)$: $10^n \equiv 4$. Comme $10 = 6 + 4$ la propriété $P(1)$ est vraie. Supposant $P(n)$ vraie on a $10^{n+1} \equiv 10 \times 10^n \equiv 10 \times 4 \equiv 40 \equiv 4$. Donc $P(n)$ est vraie pour tout n .

Exercice b.3 *Comme on l'avait dit en TD, on pourrait interpréter les questions 1 à 5 comme demandant de déterminer tous les cas pour lesquels les propriétés demandées sur les quotients sont vraies. En fait, dans le langage des mathématiciens, les questions posées reviennent à demander si on a «...» pour tous entiers a, b, h , et si non il faut simplement donner un contre-exemple.*

(1) Cela n'est pas vrai pour tous a, b, h car si h augmente, le quotient va augmenter. (En termes d'intervalles de longueur b , si on ajoute h au nombre a il peut sortir de son intervalle numéro q .) Un contre-exemple est le quotient de la DE de $a = 20$ par $b = 7$, qui vaut 2. En choisissant $h = 1$ le quotient de la DE de $a + h = 21$ par $b = 7$ est 3.

(2) Cela n'est pas vrai (pour tous a, b, h, \dots) car si h augmente, ici le quotient va diminuer. (En termes d'intervalles comme la longueur des intervalles augmente, le numéro de l'intervalle dans lequel se trouve a diminue.) Un contre-exemple est le quotient de la DE de $a = 20$ par $b = 7$, qui vaut 2. En choisissant $h = 5$ le quotient de la DE de $a = 20$ par $b + h = 12$ est 1.

(3) Cela n'est pas vrai car lorsque h devient très grand (si $h \rightarrow \infty$) alors le quotient s'approche de 1 (car la limite de $(a + h)/(b + h)$ est 1). Un contre-exemple est le quotient de la DE de $a = 20$ par $b = 7$, qui vaut 2. En choisissant $h = 100$ le quotient de la DE de $a + h = 120$ par $b + h = 107$ est 1.

(4) Cela n'est pas vrai car si on divise les intervalles de longueur b en sous-intervalles de longueur c , avec $b = nc$, alors on multiplie le nombre d'intervalles par n et donc le quotient sera multiplié à peu près par n . Un contre-exemple est le quotient de la DE de $a = 20$ par $b = 10$, qui vaut 2. En choisissant $c = 2$ le quotient de la DE de $a = 20$ par $c = 2$ est 10.

(5) Cela n'est pas vrai car le reste de la DE de a par b vérifie $0 \leq r < b$ mais il peut être plus grand que q (et donc il ne vérifiera pas $0 \leq r < q$). Un contre-exemple est le quotient de la DE de $a = 20$ par $b = 7$, qui vaut 2. Le quotient est $q = 2$ et le reste est 6. Le quotient de la DE de a par $q = 2$ est $10 \neq b$.

Exercice b.4 *C'est du calcul direct.*

(1) $n^2 + n + 1 = n(n + 1) + 1$ avec $0 \leq 1 < n + 1$. C'est donc la DE de $n^2 + n + 1$ par $n + 1$. Donc le quotient est $q = n$ et le reste est $r = 1$.

(2) *Comme le diviseur augmente, le quotient va diminuer un peu. En essayant un quotient égal à $n - 1$ on a $n^2 + n + 1 = (n - 1)(n + 2) + 3$. On doit vérifier que le reste vérifie l'inégalité fondamentale i.e. $0 \leq 3 < n + 2$. Ceci n'est vrai que pour $n \geq 2$. On répond donc :*

Si $n = 1$, il s'agit de la DE de 3 par 3, on a donc $q = 1$ et $r = 0$. Si $n \geq 2$ on a $n^2 + n + 1 = (n - 1)(n + 2) + 3$ avec $0 \leq 3 < n + 2$; donc, $q = n - 1$ et $r = 3$.

Exercice b.5 Si la DE de a par 125 est $a = 125q + 3$ avec $0 \leq 3 < 125$, alors on peut aussi écrire $a = 5 \times (25q) + 3$ avec $0 \leq 3 < 5$. Donc le reste de la DE de a par 5 est encore 3.

Si le reste de la DE de a par 5 est 13, i.e. $a = 125q + 13$ avec $0 \leq 13 < 125$, alors on a $a = 125q + 10 + 3 = 5 \times (25q + 2) + 3$ et $0 \leq 3 < 5$. Donc le reste est là aussi 3.

Enfin, supposons que la DE de b par 5 est $b = 5q + 3$. Écrivons la DE de b par 15 : $b = 15q' + r$ avec $0 \leq r < 15$. Écrivons ensuite la DE de r par 5 : $r = 5q'' + s$ avec $0 \leq s < 5$. On a donc $b = 15q' + 5q'' + s$ ce qui montre que s est le reste de la DE de b par 5, i.e. $s = 3$. Donc r est < 15 et congru à 3 modulo 5, les seules possibilités sont $r = 3, r = 8$ et $r = 13$.

Bases de numération (c)

Exercice c.1 *Cet exercice est un petit peu tordu. N'y prêtez pas trop attention.*

Pour écrire en base 423 il faut choisir 423 symboles. Pour éviter de le faire on prend les symboles $0, 1, 2, \dots, 422$ et on écrit les nombres en base 423 en mettant des points entre les symboles :

par exemple 946 s'écrit $\overline{2.100}_{(423)}$ car c'est $2 \times 423 + 100$. Pour le cas de 4498 on écrit les DE habituelles : $4498 = 10 \times 423 + 268$ avec $0 \leq 268 < 423$ (ici il n'y a qu'une DE à faire). Donc 4498 s'écrit $\overline{10.268}_{(423)}$.

Pour écrire 423 en base 4498 on prend la même convention d'écriture qu'au-dessus, avec les 4498 symboles $0, 1, 2, \dots, 4497$. Comme $423 < 4498$ il n'y a aucune DE à écrire et on obtient directement l'écriture de 423 : c'est $\overline{423}_{(4498)}$.

Exercice c.2 *Exercice de l'écrit du concours Prof des Écoles !*

Un nombre qui s'écrit abc en base 10 vaut $n = 10^2a + 10b + c$. Donc si $b = a + c$ on a : $n = 100a + 10(a + c) + c = 110a + 11c = 11(10a + c)$, qui est divisible par 11. Donc Olivier a raison.

Réciproquement, si le nombre abc est divisible par 11, on n'a pas forcément $b = a + c$ car la somme $a + c$ peut être supérieure ou égale à 10; or le nombre b est compris entre 0 et 9 car c'est un chiffre de l'écriture en base 10 de n . Voici un contre-exemple : le nombre $n = 616 = 11 \times 56$ est divisible par 11 mais $a + c = 12$.

Remarque: ce qui est toujours vrai c'est que $b \equiv a + c \pmod{11}$, voir exercice c.8(3) !

Exercice c.3 Les semaines, jours, heures, minutes sont des durées qui, exprimées en secondes, sont multiples de 60. Faisons la DE de 1494312 par 60 : $1494312 = 24905 \times 60 + 12$ et $0 \leq 12 < 60$. Donc 1494312 secondes valent 24905 minutes + 12 secondes.

Les semaines, jours, heures, exprimés en minutes sont des multiples de 60. La DE de 24905 par 60 est $24905 = 415 \times 60 + 5$ avec $0 \leq 5 < 60$. Donc 24905 minutes valent 415 heures + 5 minutes.

Les semaines et jours, exprimés en heures, sont des multiples de 24. La DE de 415 par 24 est $415 = 17 \times 24 + 7$ avec $0 \leq 7 < 24$. Donc 415 heures valent 17 jours et 7 heures.

Les semaines sont des multiples de 7 jours. On a $17 = 2 \times 7 + 3$ avec $0 \leq 3 < 7$.

Le résultat est que 1494312 secondes égalent 2 semaines, 3 jours, 7 heures, 5 minutes et 12 secondes. On a vu en faisant le calcul qu'on adapte la démonstration du cours en faisant des DE par des diviseurs qui varient **au lieu du même nombre de base b** : 60, 60, 24, 7. Le résultat s'exprime par l'égalité $1494312 = \mathbf{2} \times (7 \times 24 \times 60 \times) + \mathbf{3} \times (24 \times 60 \times) + \mathbf{7} \times (60 \times 60) + \mathbf{5} \times 60 + \mathbf{12}$. En d'autres termes 1494312 s'écrit $\overline{2.3.7.5.12}_{(\text{basevariable})}$. En référence au paragraphe 2.4 du cours on peut dire que le système utilisé pour les durées est un système de numération positionnel à base variable (positionnel car la place des chiffres est importante : 1 heure 10 minutes n'est pas la même chose que 10 heures 1 minute !).

Exercice c.4 126 s'écrit $\overline{1001}_{(\text{cinq})}$ et $\overline{7E}_{(\text{seize})}$, 221 s'écrit $\overline{1341}_{(\text{cinq})}$ et $\overline{DD}_{(\text{seize})}$, 1000 s'écrit $\overline{13000}_{(\text{cinq})}$ et $\overline{3E8}_{(\text{seize})}$.

Exercice c.5 En base 2 on a $S := \overline{1101} + \overline{1011} = \overline{11000}$ et $D := \overline{1101} - \overline{1011} = \overline{10}$.

Pour les produits : $\overline{110} \times \overline{11} = \overline{10010}$ et $(\overline{101})^2 = \overline{11001}$. Dans le dernier il y a une coquille : c'est $\overline{1001} \times \overline{101}$ qu'il fallait calculer et ça fait $\overline{101101}$.

Exercice c.6 Un nombre à 5 chiffres en binaire s'écrit $\overline{r_4r_3r_2r_1r_0}$ avec $r_4 = 1$ (sinon il aurait 4 chiffres !). Pour les chiffres de r_0 à r_3 on peut mettre des 0 ou des 1 au hasard, donc il y a $2 \times 2 \times 2 \times 2 = 16$ possibilités. Il y a donc 16 nombres à 5 chiffres en numération binaire.

En numération à base b , un nombre à n chiffres s'écrit $\overline{r_{n-1} \dots r_3r_2r_1r_0}_{(b)}$ avec $r_{n-1} \neq 0$. Donc il y a $b - 1$ choix possibles pour r_{n-1} , et b choix possibles pour chacun des autres chiffres. Au total il y a donc $(b - 1)b^{n-1}$ nombres à n chiffres en base b .

Le plus petit de ces nombres correspond à $r_{n-1} = 1$ et les autres chiffres nuls, c'est donc $\overline{100 \dots 0}_{(b)}$ avec $n - 1$ zéros. Il vaut b^{n-1} .

Le plus grand correspond à tous les chiffres égaux à $b-1$ (le plus grand parmi les chiffres en base b , qui sont $0, 1, \dots, b-1$). Il s'écrit $\overline{(b-1).(b-1).\dots.(b-1)}_{(b)}$ et est égal à $(b-1)b^{n-1} + (b-1)b^{n-2} + \dots + (b-1)b + (b-1) = (b-1)(b^{n-1} + b^{n-2} + \dots + b + 1) = b^n - 1$. Remarquons que le nombre suivant, qui est b^n , s'écrit en effet avec $n+1$ chiffres : $\overline{100\dots 0}_{(b)}$ avec n zéros.

Exemples : en base 2, il y a $(b-1)b^{n-1} = 1 \times 2^4 = 16$ nombres à 5 chiffres, comme on l'a calculé. En base 10, il y a $(b-1)b^{n-1} = 9 \times 10^3 = 9000$ nombres à 4 chiffres, ce sont les nombres de 1000 à 9999.

Exercice c.7 On écrit que $A = 2n^2 + n + 1$, $B = 3n^2 + n + 2$ et $C = n^5 + 3n^4 + 3n^3 + 3n + 2$.

(1) L'égalité $C = AB$ s'écrit $n^5 + 3n^4 + 3n^3 + 3n + 2 = (2n^2 + n + 1)(3n^2 + n + 2)$. Or

$$(2n^2 + n + 1)(3n^2 + n + 2) = 6n^4 + 5n^3 + 8n^2 + 3n + 2$$

donc $C = AB$ ssi $n^5 + 3n^4 + 3n^3 + 3n + 2 = 6n^4 + 5n^3 + 8n^2 + 3n + 2$ i.e. $n^5 - 3n^4 - 2n^3 - 8n^2 = 0$. Divisons par n^2 (qui est non nul) et on a : $n^3 - 3n^2 - 2n - 8 = 0$.

Ainsi $n(n^2 - 3n - 2) = 8$ donc n divise 8. En conséquence n vaut 2, 4 ou 8 (le nombre 1 est exclu car une base doit être ≥ 2). Il est clair que c'est $n = 4$ la seule solution de $n(n^2 - 3n - 2) = 8$.

(1) En base 10, on a $A = 2 \times 4^2 + 4 + 1 = 37$ et $B = 3 \times 4^2 + 4 + 2 = 54$ et $C = \dots = 1998$.

Exercice c.8 Je ne démontre que le critère de divisibilité par 11. Comme vous l'avez sans doute compris, le plus efficace est d'utiliser les congruences.

Raisonnons modulo 11 ; on note $a \equiv b$ au lieu de $a \equiv b \pmod{11}$. Une récurrence immédiate montre que pour tout $n \in \mathbb{N}$ on a $10^n \equiv (-1)^n$ (la démonstration est exactement la même que dans l'exercice b.2, 2^{ème} solution). Donc si on écrit a sous la forme $r_n r_{n-1} \dots r_0$ en base 10, on a $a = r_n 10^n + r_{n-1} 10^{n-1} + \dots + 10r_1 + r_0$. Alors, $a \equiv r_n (-1)^n + r_{n-1} (-1)^{n-1} + \dots - r_1 + r_0$. Multiplions par $(-1)^n$ (ce qui ne change pas le fait d'être divisible par 11), on voit que a est divisible par 11 ssi $r_n - r_{n-1} + \dots + (-1)^{n-1} r_1 + (-1)^n r_0$ est divisible par 11.

Exercice c.9 La première chose à écrire (là encore) est $n = 100x + 10y + z$. Il n'y a pas de critère de divisibilité par 7 (pour les nombres écrits en base 10), mais on sait que $10 \equiv 3 \pmod{7}$ et $100 \equiv 2 \pmod{7}$ (puisque $100 = 14 \times 7 + 2$). Donc on a $n \equiv 100x + 10y + z \equiv 2x + 3y + z \pmod{7}$. On reconnaît le nombre $2x + 3y + z$ parmi la liste proposée : si n est divisible par 7 alors $2x + 3y + z$ l'est aussi.

Aucun des autres nombres proposés n'est divisible par 7 à coup sûr : le nombre $n = 112$ est un contre-exemple pour tous les cas.

Divisibilité et congruences (d)

Exercice d.1 (1) On a $x^3 + 1 = x^3 - (-1)^3 = (x+1)(x^2 - x + 1)$ donc $x+1$ divise $x^3 + 1$.

(2) Soit pour $k \geq 1$ la propriété $P(k) : 3^k \mid 2^{3^k} + 1$. Clairement $P(1)$ est vraie car 3 divise $2^3 + 1 = 9$.

Soit $k \geq 1$ un entier tel que $P(k)$ est vraie : $3^k \mid 2^{3^k} + 1$. Utilisons la question (1) avec $x = x_k := 2^{3^k}$, en écrivant l'égalité

$$(x_k)^3 + 1 = (x_k + 1)((x_k)^2 - x_k + 1)$$

Par hypothèse de récurrence, $3^k \mid 2^{3^k} + 1 = x_k + 1$. Cela ne suffit pas pour montrer $P(k+1)$ car on veut montrer que 3^{k+1} divise $2^{3^{k+1}} + 1 = (x_k)^3 + 1$. Il manque juste un facteur 3 que l'on va trouver dans le 2^{ème} facteur $(x_k)^2 - x_k + 1$. Précisément, de l'hypothèse $3^k \mid x_k + 1$ on déduit que $x_k \equiv -1 \equiv 2 \pmod{3}$. Alors $(x_k)^2 - x_k + 1 \equiv 2^2 - 2 + 1 \equiv 0 \pmod{3}$ c'est-à-dire que 3 divise $(x_k)^2 - x_k + 1$.

Récapitulons : par hypothèse de récurrence il existe $q_k \in \mathbb{N}$ tel que $x_k + 1 = 3^k q_k$. D'après ce qu'on vient de montrer il existe $r_k \in \mathbb{N}$ tel que $(x_k)^2 - x_k + 1 = 3r_k$. En multipliant il vient

$$(x_k)^3 + 1 = (x_k + 1)((x_k)^2 - x_k + 1) = 3^{k+1} q_k r_k$$

Donc 3^{k+1} divise $(x_k)^3 + 1 = 2^{3^{k+1}} + 1$, i.e. $P(k+1)$ est vraie. Donc $P(k)$ est vraie pour tout $k \geq 1$.

Quelques remarques.

- (a) La factorisation $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$ est à connaître !
- (b) Dans cet exercice il faut se méfier : on ne peut pas vraiment raisonner avec des congruences car la « base » de la congruence est variable : on devrait raisonner modulo 3^k or k varie...
- (c) Pour démontrer (2), dans un premier essai on s'aperçoit qu'il ne suffit pas d'utiliser le résultat « $x + 1$ divise $x^3 + 1$ ». Qu'à cela ne tienne ! On finit par voir qu'il faut utiliser l'égalité $x^3 + 1 = (x + 1)(x^2 - x + 1)$, qui est plus forte.

Exercice d.2 Le reste de la DE de n par 5 vaut 0, 1, 2, 3 ou 4. C'est-à-dire, n est congru modulo 5 à l'un de ces 5 nombres.

$$\begin{aligned} \text{Si } n \equiv 0, & \quad n^5 - n \equiv 0. \\ \text{Si } n \equiv 1, & \quad n^5 - n \equiv 1^5 - 1 \equiv 0. \\ \text{Si } n \equiv 2, & \quad n^5 - n \equiv 2^5 - 2 \equiv 32 - 2 \equiv 30 \equiv 0. \\ \text{Si } n \equiv 3, & \quad n^5 - n \equiv 3^5 - 3 \equiv 243 - 3 \equiv 0. \\ \text{Si } n \equiv 4, & \quad n^5 - n \equiv 4^5 - 4 \equiv 1024 - 4 \equiv 0. \end{aligned}$$

Dans tous les cas, $n^5 - n \equiv 0 \pmod{5}$ i.e. il est divisible par 5.

On a déjà vu que $n^2 - n$ est toujours divisible par 2, $n^3 - n$ est toujours divisible par 3, $n^5 - n$ est toujours divisible par 5,... Les deux exercices suivants montrent que $n^p - n$ est toujours divisible par p si p est un nombre premier. Lorsque p n'est pas premier c'est faux : voir d.4(3).

Exercice d.3 On se rappelle un des premiers exercices du cours où on a montré que $iC_p^i = pC_{p-1}^{i-1}$ pour $0 < i < p$. Ainsi p divise iC_p^i , or comme p est premier avec i , par le lemme de Gauß p divise C_p^i .

Exercice d.4 (1) Il faut utiliser l'exercice précédent. On développe $(a+b)^p$ par la formule du binôme de Newton :

$$(a+b)^p = \sum_{k=0}^p C_p^k a^k b^{p-k} = a^p + C_p^1 a b^{p-1} + \dots + C_p^{p-1} a^{p-1} b + b^p$$

D'après l'exercice d.3, modulo p tous les coefficients binômiaux sont congrus à zéro (sauf pour les deux termes extrêmes), et donc $(a+b)^p \equiv a^p + b^p \pmod{p}$.

(2) Raisonnons modulo p ; on note $a \equiv b$ au lieu de $a \equiv b (p)$. On montre la propriété $P(n)$: $n^p - n \equiv 0$. Pour $n = 0$ c'est clair. Soit $n \geq 0$ tel que $P(n)$ soit vraie. Alors en utilisant la question précédente on a $(n+1)^p - (n+1) \equiv n^p + 1^p - (n+1) \equiv n^p - n \equiv 0$ d'après l'hypothèse de récurrence. Donc $P(n+1)$ est vraie. Par le principe de récurrence, $P(n)$ est vraie pour tout $n \geq 0$.

(3) Si p n'est pas premier ? Comme d'habitude, on expérimente pour se faire une idée. Le plus petit nombre non premier est 4. Le plus petit nombre n pour lequel $n^4 - n$ a une chance d'être non divisible par 4 est $n = 2$. On calcule : $n^4 - n = 2^4 - 2 = 14$ qui n'est pas divisible par 4 ! On a trouvé un contre-exemple. On répond ainsi :

Il n'est pas vrai que la propriété ait lieu pour tout entier p , car pour $p = 4$ et $n = 2$ on a $n^4 - n = 2^4 - 2 = 14$ qui n'est pas divisible par 4. C'est donc une propriété « magique » des nombres premiers.

Exercice d.6 (1) « Résoudre » veut dire « trouver toutes les solutions de ». Vous avez tous vu rapidement qu'on trouve des solutions de l'équation lorsque x est congru à 2 modulo 5, i.e. $x = 2 + 5n$ avec n entier. Le problème était ensuite de rédiger correctement la réponse : est-ce que j'ai là toutes les solutions ? Comment le montrer ? Que faut-il montrer ?

Pour cela je donne deux solutions. Dans la première on évite le recours aux congruences, qui gêne encore beaucoup d'entre vous. On observe (cf la table de multiplication des restes modulo 5 qu'on avait écrite au tableau) que lorsque $x = 2$ on a une solution. D'autres essais donnent $x = 7, x = 12 \dots$ En fait tous les $x \equiv 2 (5)$ marchent. Il reste à montrer que l'ensemble S des solutions et l'ensemble T des nombres qui sont congrus à 2 modulo 5 sont les mêmes. Pour cela une seule méthode : montrer que $S \subset T$, puis que $T \subset S$!

Dans la deuxième solution on calcule directement avec les congruences, ça va très vite !

1^{ère} solution. On va montrer que tout nombre x dont le reste dans la DE par 5 est 2 (càd x est congru à 2 modulo 5) est une solution. S'il y a un entier n tel que $x = 5n + 2$ alors $3x = 3(5n + 2) = 15n + 6 = 15n + 5 + 1$ qui est bien congru à 1 modulo 5. Donc c'est une solution.

Il faut maintenant montrer que ce sont là les seules solutions, c'est-à-dire qu'une solution de l'équation est congrue à 2 modulo 5. Écrivons la DE de x par 5 : $x = 5n + r$ avec $0 \leq r < 5$. On a $3x = 15n + 3r$, donc si x est une solution de l'équation on doit avoir $3x \equiv 1 \equiv 3r (5)$. Or $3r$ vaut 0, 3, 6, 9 ou 12 car $0 \leq r < 5$. Seul 6 est congru à 1 modulo 5, correspondant à $r = 2$. Donc $x = 5n + 2$.

On conclut que les solutions de l'équation sont les nombres congrus à 2 modulo 5, c'est-à-dire les nombres de la forme $x = 2 + 5k$ ($k \in \mathbb{Z}$).

2^{ème} solution. On raisonne modulo 5, on note $a \equiv b$ au lieu de $a \equiv b (5)$.

Le reste de la DE de x par 5 est l'un des nombres 0, 1, 2, 3 ou 4. On écrit les multiples de 3 :

x	$x \equiv 0$	$x \equiv 1$	$x \equiv 2$	$x \equiv 3$	$x \equiv 4$
$3x$	$3x \equiv 0$	$3x \equiv 3$	$3x \equiv 6 \equiv 1$	$3x \equiv 9 \equiv 4$	$3x \equiv 12 \equiv 2$

Donc si $x \equiv 2$, x est une solution de l'équation proposée. De plus si $x \not\equiv 2$ (i.e. si x est congru à 0, 1, 3 ou 4) alors $3x \not\equiv 1$ comme le montrent les calculs ci-dessus, c'est-à-dire que x n'est pas solution. En conclusion, l'ensemble des solutions est l'ensemble des entiers relatifs congrus à 2 modulo 5, c'est-à-dire les nombres de la forme $x = 2 + 5k$ ($k \in \mathbb{Z}$).

(2) L'équation est maintenant $5x \equiv 2 (7)$. On raisonne modulo 7, on note $a \equiv b$ au lieu de $a \equiv b (7)$. Le reste de la DE de x par 7 est l'un des nombres 0, 1, 2, 3, 4, 5, 6. On écrit les

multiples de 5 modulo 7 :

x	$x \equiv 0$	$x \equiv 1$	$x \equiv 2$	$x \equiv 3$	$x \equiv 4$	$x \equiv 5$	$x \equiv 6$
$5x$	$5x \equiv 0$	$5x \equiv 5$	$5x \equiv 10 \equiv 3$	$5x \equiv 15 \equiv 1$	$5x \equiv 20 \equiv 6$	$5x \equiv 25 \equiv 4$	$5x \equiv 30 \equiv 2$

Donc si $x \equiv 6$, x est une solution de l'équation proposée. De plus si $x \not\equiv 6$ alors $5x \not\equiv 2$ comme le montre le tableau, c'est-à-dire que x n'est pas solution. En conclusion, l'ensemble des solutions est l'ensemble des entiers relatifs congrus à 6 modulo 7, c'est-à-dire les nombres de la forme $x = 6 + 7k$ ($k \in \mathbb{Z}$).

(3) *Pour raisonner par congruence on est un peu coincé : il faut choisir modulo 5 ou modulo 7, on ne peut pas faire les deux ! Après quelques essais de calculs on voit que le nombre $5 \times 7 = 35$ semble jouer un grand rôle.*

On doit trouver les $x \in \mathbb{Z}$ tels que $3x \equiv 1$ (5) et $5x \equiv 2$ (7). Soit x une solution de ces deux équations, donc par ce qui précède, $x \equiv 2$ (5) et $x \equiv 6$ (7).

Soit la DE de x par 35 : $x = 35q + r$ avec $0 \leq r < 35$. Comme $x \equiv 2$ (5) on doit avoir $r \in \{2, 7, 12, 17, 22, 27, 32\}$. Comme $x \equiv 6$ (7) on doit avoir $r \in \{6, 13, 20, 27, 34\}$. Finalement, seul $r = 27$ convient. Donc, $x \equiv 27$ (35).

On a montré qu'une solution est congrue à 27 modulo 35. Réciproquement, soit un entier $x = 35q + 27$, $q \in \mathbb{Z}$. Il est clair que $x \equiv 2$ (5) et $x \equiv 6$ (7), donc x est solution des deux équations simultanément.

L'ensemble des solutions de (1) et (2) est l'ensemble des entiers relatifs congrus à 27 modulo 35.