# Arithmétique partie I

**D ensemble des entiers naturels, ensembles des entiers relatifs**

• $\mathbb{N} = \{0; 1; 2; \dots\}$, $\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1; 2; \dots\}$

• $\mathbb{Z} = \{\dots; -2; -1; 0; 1; 2; \dots\}$, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\} = \{\dots; -2; -1; 1; 2; \dots\}$

**P • à propose de $\mathbb{N}$**

– la somme et le produit de deux entiers naturels sont des entiers naturels : on dit que $\mathbb{N}$ est stable pour l'addition et la multiplication

– $\mathbb{N}$ n'est pas stable par soustraction

– il est interdit d'effectuer un division décimales dans $\mathbb{N}$ : il n'y a pas de « fraction » dans $\mathbb{N}$

**• à propos de $\mathbb{Z}$**

– $\mathbb{Z}$ est stable par addition, multiplication et soustraction

– il est interdit d'effectuer une division décimale dans $\mathbb{Z}$ : il n'y a pas de « fraction » dans $\mathbb{Z}$

**• quelques rappels**

– l'affirmation « si $A$ est vraie alors $B$ est vraie » se note aussi « $A \Rightarrow B$ »

– démontrer l'affirmation « $A \Rightarrow B$ » revient à démontrer sa forme contraposée « $non\ B \Rightarrow non\ A$ » (attention à l'ordre … )

– pour démontrer que l'affirmation $A$ est vraie on peut effectuer un raisonnement par l'absurde : on suppose que $A$ est fausse, on en déduit un ensemble d'affirmations contenant une contradiction ce qui permet de rejeter l'hypothèse que l'affirmation $A$ est fausse, donc d'en déduire que l'affirmation $A$ est vraie

– « $A \Leftrightarrow B$ » signifie « $A \Rightarrow B$ et $B \Rightarrow A$ » (simultanément).

Le symbole « $\Leftrightarrow$ » peut être remplacé par « cela revient à dire que ».

i Dans ce chapitre, sauf indication contraire on travaille **dans $\mathbb{Z}$**.

D Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

▶ **$a$ divise $b$** (on écrit $a|b$) $\overset{déf}{\Leftrightarrow}$ il existe $k \in \mathbb{Z}$ tel que : $b = k \times a$

Lorsque $a|b$ ont dit aussi que **$a$ est un diviseur de $b$** ou encore que **$b$ est un multiple de $a$**.

*On peut utiliser la calculatrice pour « tester » si un entier relatif non nul est ou non un diviseur d'un autre entier relatif mais cela n'a pas valeur de preuve.*

**A01** • justifier que : $5 \mid (-15)$, que $(-8) \mid (-32)$

• on sait que $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ et $x = 7y$ : quelles affirmations peut-on en déduire parmi $x|y$ , $y|x$, $x|7$, $7|x$, $7|y$ et $y|7$ ?

• un élève affirme : « $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}$, on a : $a + b | a^2 - b^2$ » ; démontrer cette affirmation ou bien en donner un contre-exemple

P ▶Pour tout a $\in \mathbb{Z}$, on a : $\mathbf{1}|a$, $(-\mathbf{1})|a$, $a|a$ et $(-a)|a$.

**A02** Justifier les quatre affirmations de la propriété précédente.

P **Le cas particulier de 0**

• tout entier relatif divise 0 : $\forall a \in \mathbb{Z}$, $a|\mathbf{0}$, en particulier : $\mathbf{0}|\mathbf{0}$.

• 0 ne divise aucun entier relatif non nul, autrement dit pour tout $a \in \mathbb{Z}$ on a l'implication : ▶ $a \neq 0 \Rightarrow non(\mathbf{0}|a)$

**A03** Démontrer la propriété précédente.

P Soit $a \in \mathbb{Z}$.

Alors, pour tout $b \in \mathbb{Z}$ on a l'équivalence : ▶ $b|a \Leftrightarrow (-b)|a$.

**A04** Démontrer la propriété précédente.

**A01** • **justifier que : $5 \mid (-15)$, que $(-8) \mid (-32)$.**
**• on sait que $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ et $x = 7y$, quelles affirmations peut-on en déduire parmi : $x|y$ , $y|x$, $x|7$, $7|x$, $7|y$, $y|7$ ?**
**• un élève affirme : « $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}$, on a : $a + b|a^2 - b^2$ »**
**si cette affirmation est vraie la démontrer, sinon donner un contre-exemple.**

• $-15 = (-3) \times 5$ : il existe $k \in \mathbb{Z}$ tel que $-15 = k \times 5$, à savoir $k = -3$, donc $5 \mid (-15)$
$-32 = 4 \times (-8)$ : il existe $k' \in \mathbb{Z}$ tel que $-32 = k' \times (-8)$, à savoir $k' = 4$, donc $(-8) \mid (-32)$
• on sait que $x = 7y$, on peut en déduire : $y|x$ et $7|x$
• $a^2 - b^2 = (a + b)(a - b) = k \times (a + b)$ avec $k = a - b$
Il existe $k \in \mathbb{Z}$ tel que $a^2 - b^2 = k \times (a + b)$ donc $(a + b)|a^2 - b^2$

$P$ Pour tout $a \in \mathbb{Z}$, on a : $\mathbf{1}|a$, $(-\mathbf{1})|a$, $a|a$ et $(-a)|a$.

**A02** Démontrer la propriété précédente.

$a = 1 \times a$ montre que $1|a$ et que $a|a$
$a = (-1) \times (-a)$ montre que $(-1)|a$ et $(-a)|a$

$P$ **Le cas particulier de $0$**
• tout entier relatif divise $0$ : $\forall a \in \mathbb{Z}$, $a|0$, en particulier : $0|0$.
• $0$ ne divise aucun entier relatif non nul. Autrement dit, pour tout $a \in \mathbb{Z}$, on a l'implication : $a \neq 0 \Rightarrow non(0|a)$.

**A03** **Démontrer la propriété précédente.**

• pour tout $a \in \mathbb{Z}$, $0 = 0 \times a$ montre que $a$ est un diviseur de $0$
• soit $a$ un entier relatif admettant $0$ pour diviseur, alors il existe $k \in \mathbb{Z}$ tel que $a = k \times 0$ donc $a = 0$.
On a montré que : $0$ est un diviseur de $a \Rightarrow a = 0$.
En prenant la contraposée : non $(a = 0) \Rightarrow$ non $(0|a)$ ce qui s'écrit aussi : $a \neq 0 \Rightarrow 0$ n'est pas un diviseur de $a$.

$P$ Soit $a \in \mathbb{Z}$.
Alors, pour tout $b \in \mathbb{Z}$ on a l'équivalence : ▶ $b|a \Leftrightarrow (-b)|a$.

**A04** **Démontrer la propriété précédente.**
Soient $a \in \mathbb{Z}$.
**• montrons que : $\forall b \in \mathbb{Z}$, si $b|a$ alors $(-b)|a$.**
Soit $b \in \mathbb{Z}$ tel que $b|a$. Il existe $k \in \mathbb{Z}$ tel que : $a = k \times b$, ce qui s'écrit aussi : $a = (-k) \times (-b)$.
Il existe $k' \in \mathbb{Z}$ tel que : $a = k' \times (-b)$, à savoir $k' = -k$, donc $(-b)$ est un diviseur de $a$.
**• montrons que : $\forall b \in \mathbb{Z}$, si $(-b)|a$ alors $b|a$.**
Soit $b \in \mathbb{Z}$ tel que $(-b)|a$ : d'après le point précédent on a : $-(-b)|a$ autrement dit : $b|a$.

Conclusion
Il résulte des deux points précédents que : $b|a \Leftrightarrow (-b)|a$.

**Quelques rappels sur la valeur absolue et des compléments**

Pour tout $x \in \mathbb{R}$, $|x| \overset{\text{def}}{=} \sqrt{x^2}$.

$P$ Soient $x$ et $y$ deux réels, on a :

- $|x| \geqslant 0$
- $|0| = 0$ et $|1| = 1$
- si $x \geqslant 0$ alors $|x| = x$ , et si $x < 0$ alors $|x| = -x$
- $|x \times y| = |x| \times |y|$
- $|x| = 0 \Leftrightarrow x = 0$

**A05** Démontrer chacun des points de la propriété précédente.

$P$ Soit $a$ un entier relatif non nul et $d$ un diviseur positif de $a$, alors $d$ est compris au sens large entre 1 et $|a|$ : $1 \leqslant d \leqslant |a|$,

autrement dit on a l'implication : $\begin{cases} \boldsymbol{a \in \mathbb{Z} \setminus \{0\}} \\ \boldsymbol{d \in \mathbb{N}} \textbf{ et } \boldsymbol{d|a} \end{cases} \Rightarrow \boldsymbol{1 \leqslant d \leqslant |a|}$.

**A06** Démontrer la propriété précédente.

**A07** Un élève affirme « si $a \in \mathbb{Z}$, $d \in \mathbb{N}$ et $d|a$, alors $1 \leqslant d \leqslant |a|$ ».
Montrer que cet élève se trompe.

**A08** Donner sans justification les diviseurs positifs de $(-15)$ puis donner sans justification tous les diviseurs de $(-15)$.

$i$ Pour $a \in \mathbb{Z} \setminus \{0\}$, la commande **`ListeDiviseurs`**$(a)$ dans GeoGebra donne la liste des diviseurs positifs de $a$.

**A09** Démontrer que $\forall (a,b) \in \mathbb{Z}^2$, on a : $4|(a+b)^2 - (a-b)^2$.

**A10** Démontrer que : $\forall n \in \mathbb{N}$, on a : $3|(2^n + 2^{n+1})$.

$D$ Des **entiers consécutifs** sont des entiers dont la différence est 1.

**A11** Que penser de l'affirmation d'**u**n élève « la somme de trois entiers relatifs consécutifs est divisible par 3 » ?

$P$ ▶ **transitivité de la divisibilité**

Pour tout $(a,b,c) \in \mathbb{Z}^3$ on a l'implication : $\boldsymbol{a|b}$ **et** $\boldsymbol{b|c} \Rightarrow \boldsymbol{a|c}$

**A12** Démontrer la propriété « transitivité de la divisibilité ».

$P$ ▶ **divisibilité et combinaison linéaire**

Pour tout $(a,b,c) \in \mathbb{Z}^3$, on a l'**implication** :

$$\boldsymbol{a|b} \textbf{ et } \boldsymbol{a|c} \Rightarrow \forall (\boldsymbol{m},\boldsymbol{n}) \in \mathbb{Z}^2, \boldsymbol{a}|(\boldsymbol{mb}+\boldsymbol{nc})$$

Autrement dit : si un entier qui divise deux nombres alors il divise toute combinaison linéaire de ces deux nombres.

**A13** Démontrer la propriété « divisibilité et combinaison linéaire ».

$P$ Pour tout $(a,b,c) \in \mathbb{Z}^3$, on a les implications :

$$\boldsymbol{a|b} \textbf{ et } \boldsymbol{a|c} \Rightarrow \boldsymbol{a|b+c}$$
$$\boldsymbol{a|b} \textbf{ et } \boldsymbol{a|c} \Rightarrow \boldsymbol{a|b-c}$$

▶ Si un entier divise deux nombres, alors il divise la somme et la différence de ces deux nombres.

**A14** Justifier la propriété précédente.

**A15** Un élève affirme que : « pour tous entiers relatifs $a$, $b$, $c$, $d$ on a l'implication : $a|b$ et $c|d \Rightarrow a+c|b+d$ et $a-c|b-d$ ».
Montrer qu'il se trompe.

On **ne peut pas** ajouter ou soustraire « membre à membre » des relations de divisibilité.

**A16 Un programme Python**

Rappel

Pour $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, dire que $b$ est un diviseur de $a$ revient à dire que le reste de la division euclidienne de $a$ par $b$ est nul.

Écrire un programme Python qui demande d'entrer un entier naturel non nul puis affiche ses diviseurs positifs sous forme de liste.

**A17** Déterminer tous les entiers naturels $n$ tels que : $n-3|7$.

**Quelques rappels sur la valeur absolue et des compléments**

Pour tout $x \in \mathbb{R}$ on pose : $|x| \overset{\text{def}}{=} \sqrt{x^2}$.

$P$ Soient $x$ et $y$ deux réels, on a :

- $|x| \geqslant 0$
- $|0| = 0$ et $|1| = 1$
- si $x \geqslant 0$ alors $|x| = x$ , et si $x < 0$ alors $|x| = -x$
- $|x \times y| = |x| \times |y|$
- $|x| = 0 \Leftrightarrow x = 0$

**A05 Démontrer chacun des points de la propriété précédente.**

- **montrons que $|x| \geqslant 0$**

Soit $x \in \mathbb{R}$. Le résultat d'une racine carré est un réel positif ou nul donc : $\sqrt{x^2} \geqslant 0$ autrement dit $|x| \geqslant 0$.

- **montrons que : si $x \geqslant 0$ alors $|x| = x$, et si $x < 0$ alors $|x| = -x$**

Soit $x \geqslant 0$, $|x| = \sqrt{x^2} = x$ (par définition de $\sqrt{\ }$).

Si $x < 0$ donc $-x > 0$, on a : $|x| = \sqrt{x^2} = \sqrt{(-x)^2} = -x$ d'après le cas précédent.

- **déterminons $|1|$ et $|0|$**

$|1| = \sqrt{1^2} = \sqrt{1} = 1$ et $|0| = \sqrt{0^2} = \sqrt{0} = 0$

- **montrons que : $|x \times y| = |x| \times |y|$**

$|x \times y| = \sqrt{(x \times y)^2} = \sqrt{x^2 \times y^2} = \sqrt{x^2} \times \sqrt{y^2} = |x| \times |y|$

- **montrons que $|x| = 0 \Leftrightarrow x = 0$**

– montrons que $x = 0 \Rightarrow |x| = 0$

si $x = 0$, alors $|x| = |0| = 0$.

On a donc bien : $x = 0 \Rightarrow |x| = 0$

– montrons que $|x| = 0 \Rightarrow x = 0$

méthode 1

On procède par disjonction de cas :

si $x \geqslant 0$

supposons $|x| = 0$

$x$ est positif ou nul donc $|x| = x$ par conséquent

l'égalité $|x| = 0$ s'écrit aussi $x = 0$ ✔

si $x < 0$

supposons $|x| = 0$

$x$ est strictement négatif donc $|x| = -x$

par conséquent l'égalité $|x| = 0$ s'écrit aussi $-x = 0$

ou encore $(-x) \times (-1) = 0 \times (-1)$ i.e. $x = 0$ ✔

Pour tout $x \in \mathbb{R}$, on a l'implication : $|x| = 0 \Rightarrow x = 0$

deuxième méthode

$|x| = 0 \Leftrightarrow \sqrt{x^2} = 0 \Rightarrow \left(\sqrt{x^2}\right)^2 = 0^2 \Leftrightarrow x^2 = 0 \Leftrightarrow x = 0$

Pour tout $x \in \mathbb{R}$, on a l'implication : $|x| = 0 \Rightarrow x = 0$

Résumons : $|x| = 0 \Rightarrow x = 0$ et $x = 0 \Rightarrow |x| = 0$ donc on a démontré l'équivalence : $|x| = 0 \Leftrightarrow x = 0$

$P$ Soit $a$ un entier relatif non nul et $d$ un diviseur positif de $a$, alors $d$ est compris au sens large entre 1 et $|a|$ : $1 \leqslant d \leqslant |a|$,

autrement dit on a l'implication : $\begin{cases} \boldsymbol{a \in \mathbb{Z} \setminus \{0\}} \\ \boldsymbol{d \in \mathbb{N}} \textbf{ et } \boldsymbol{d|a} \end{cases} \Rightarrow \boldsymbol{1 \leqslant d \leqslant |a|}$.

**A06 Démontrer la propriété précédente.**

Soit $a \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{N}$ et $d|a$.

Démontrons que : $1 \underset{①}{\leqslant} d \underset{②}{\leqslant} |a|$.

$d|a$ donc il existe $k \in \mathbb{Z}$ tel que $a = k \times d$, d'où :

$$|a| = |k \times d| = |k| \times |d| = |k| \times d$$

Résumons : $|a| = |k| \times d \quad (*)$

- **Montrons que $\boldsymbol{1 \underset{①}{\leqslant} d}$**

$a \neq 0$ donc $|a| \neq 0$

$d$ est diviseurs de $|a| \neq 0$ donc $d \neq 0$ et comme $d$ est un entier naturel on en déduit que : $1 \leqslant d$ ✔

- **Montrons que $\boldsymbol{d \underset{②}{\leqslant} |a|}$**

$(*)$ montre que $|k|$ divise $|a|$ et comme $|a| \neq 0$ on en déduit $|k| \neq 0$

$|k| \in \mathbb{N}$ et $|k| \neq 0$ donc $1 \leqslant |k|$ puis en multipliant par $d > 0$ on obtient : $1 \times d \leqslant |k| \times d$, c'est-à-dire $d \leqslant |a|$ ✔

Conclusion : $1 \leqslant d \leqslant |a|$.

**A07** **Un élève affirme « si $a \in \mathbb{Z}$, $d \in \mathbb{N}$ et $d|a$, alors $1 \leqslant d \leqslant |a|$ ». Montrer que cet élève se trompe.**

On a : $0 = 6 \times 0$ donc $6|0$, mais « $1 \leqslant 6 \leqslant |0|$ » est faux. On a trouvé un contre-exemple donc l'affirmation de l'élève est fausse.

**A08** **Donner sans justification les diviseurs positifs de $(-15)$ puis donner sans justification tous les diviseurs de $(-15)$.**

On recherche les diviseurs positifs de $(-15)$ dans $[\![1; |-15|]\!]$, c'est-à-dire dans $[\![1; 15]\!]$.

Les diviseurs positif de $(-15)$ : $1, 3, 5, 15$.

Tous les diviseurs de $(-15)$ : $-15, -5, -3, -1, 1, 3, 5$ et $15$.

**A09** **Démontrer que pour tout $(a, b) \in \mathbb{Z}^2$ : $4|(a+b)^2 - (a-b)^2$.**

Soient $a$ et $b$ deux entiers relatifs, on a :

$$(a+b)^2 - (a-b)^2 = a^2 + 2ab + b^2 - (a^2 - 2ab + b^2)$$
$$= a^2 + 2a + b^2 - a^2 + 2ab - b^2 = 4ab$$

Résumons : $(a+b)^2 - (a-b)^2 = 4ab$.

Il existe $k \in \mathbb{Z}$ tel que $(a+b)^2 - (a-b)^2 = 4k$, à savoir $k = ab$, donc : $4|(a+b)^2 - (a-b)^2$.

**A10** Pour bien comprendre la question, on peut commencer au brouillon par tester quelques valeurs de n mais cela n'est pas obligatoire :

• $n = 0$

$2^0 + 2^{0+1} = 2^0 + 2^1 = 1 + 2 = 3 = 1 \times 3$

$2^0 + 2^{0+1} = 1 \times 3$ donc $3|(2^0 + 2^{0+1})$

• $n = 1$

$2^1 + 2^{1+1} = 2^1 + 2^2 = 2 + 4 = 6 = 2 \times 3$

$2^1 + 2^{1+1} = 2 \times 3$ donc $3|(2^1 + 2^{1+1})$

Soit $n \in \mathbb{N}$, montrons que : $3|(2^n + 2^{n+1})$.

On a : $2^n + 2^{n+1} = 2^n \times 1 + 2^n \times 2^1 = 2^n(1 + 2^1) = 2^n \times 3$.

On a : $2^n + 2^{n+1} = 2^n \times 3$, il existe $k \in \mathbb{Z}$ tel que $2^n + 2^{n+1} = k \times 3$,

à savoir $k = 2^n$ donc : $3|2^n + 2^{n+1}$.

Conclusion : $\forall n \in \mathbb{N}$, $3|2^n + 2^{n+1}$.

$D$ Des **entiers consécutifs** sont des entiers dont la différence est 1.

**A11** **Que penser de l'affirmation d'un élève « la somme de trois entiers relatifs consécutifs est divisible par 3 » ?**

On se donne trois entiers relatifs consécutifs, en notant $n$ le plus petit d'entre eux, les deux autres sont égaux à $n+1$ et $n+2$.

On a :

$n + (n+1) + (n+2) = n + n + 1 + n + 2 = 3n + 3 = 3(n+1)$

Résumons : $n + (n+1) + (n+2) = 3(n+1)$.

Il existe $k \in \mathbb{Z}$ tel que $n + (n+1) + (n+2) = 3k$, à savoir $k = (n+1)$, donc $3|n + (n+1) + (n+2)$.

L'affirmation de cet élève est donc exacte.

$P$ ▶ **transitivité de la divisibilité**

Pour tout $(a, b, c) \in \mathbb{Z}^3$ on a l'implication : $a|b$ **et** $b|c \Rightarrow a|c$

**A12** **Démontrer la propriété « transitivité de la divisibilité ».**

Soient $a$, $b$ et $c$ trois entier relatifs tels que $a|b$ et $b|c$.

On a : $a|b$, donc il existe $k \in \mathbb{Z}$ tel que : $b = k \times a$

et on a : $b|c$, donc il existe $k' \in \mathbb{Z}$ tel que : $c = k' \times b$.

D'où : $c = k' \times b = k' \times (k \times a) = k' \times (k \times a) = (k' \times k) \times a$.

Il existe $k'' \in \mathbb{Z}$ tel que $c = k'' \times a$, à savoir $k'' = k' \times k$ donc $a|c$.

Pour tout $(a, b, c) \in \mathbb{Z}^3$ , on a l'implication : $a|b$ et $b|c \Rightarrow a|c$.

$P$ ▶ **divisibilité et combinaison linéaire**

Pour tout $(a,b,c) \in \mathbb{Z}^3$, on a l'implication :

$$\boldsymbol{a|b \text{ et } a|c \Rightarrow \forall (m,n) \in \mathbb{Z}^2, a|(mb+nc)}$$

Un entier qui divise deux nombres divise toute combinaison linéaire de ces deux nombres.

**A13 Démontrer la propriété « divisibilité et combinaison linéaire ».**

Soient $a$, $b$, $c$ trois entiers relatifs tels que $a|b$ et $a|c$, $m$ et $n$ deux entiers relatifs.

On a : $a|b$, donc il existe $k \in \mathbb{Z}$ tel que : $b = ka$,

et on a : $a|c$, donc il existe $k' \in \mathbb{Z}$ tel que : $c = k'a$.

D'où : $mb + nc = mka + nk'a = (mk + nk')a$.

Il existe $k'' \in \mathbb{Z}$ tel que $mb + nc = k''a$, à savoir $k'' = mk + nk'$,

donc : $a|(mb + nc)$.

$P$ Pour tout $(a,b,c) \in \mathbb{Z}^3$, on a les implications :

$$\boldsymbol{a|b \text{ et } a|c \Rightarrow a|b+c}$$
$$\boldsymbol{a|b \text{ et } a|c \Rightarrow a|b-c}$$

Si un entier divise deux nombres, alors il divise leur somme et leur différence.

**A14 Justifier la propriété précédente.**

méthode 1

Soient $a$, $b$ et $c$ trois entiers relatifs tels que $a|b$ et $a|c$.

$a|b$ donc il existe $k \in \mathbb{Z}$ tel que $b = k \times a$

$a|c$ donc il existe $k' \in \mathbb{Z}$ tel que $c = k' \times a$

D'où : $b + c = k \times a + k' \times a = (k + k') \times a$.

Il existe $k'' \in \mathbb{Z}$ tel que $b + c = k'' \times a$ donc $a|b + c$.

D'autre part : $b - c = k \times a - k' \times a = (k - k') \times a$.

Il existe $k''' \in \mathbb{Z}$ tel que $b - c = k''' \times a$ donc $a|b - c$.

méthode 2

On a : $a|b$ et $a|c$ donc $a$ divise toute combinaison linéaire de $b$ et $c$, en particulier : $a|1 \times b + 1 \times c$, c'est-à-dire : $a|b + c$.

On a : $a|b$ et $a|c$ donc $a$ divise toute combinaison linéaire de $b$ et $c$, en particulier : $a|1 \times b + (-1) \times c$, c'est-à-dire : $a|b - c$.

**A15 Un élève : « pour tous entiers relatifs $a$, $b$, $c$, $d$ on a l'implication : $a|b$ et $c|d \Rightarrow a + c|b + d$ et $a - c|b - d$ ».**

**Montrer qu'il se trompe.**

On a : $6|18$ et $2|4$, $6 + 2 = 8$ et $18 + 4 = 22$ et pourtant $non(8|22)$

de même $6 - 2 = 4$ et $18 - 4 = 14$ et pourtant $non(4|14)$.

Les deux contre-exemples précédents montrent que l'affirmation de l'élève est fausse.

On **ne peut pas** ajouter ou soustraire « membre à membre » des relations de divisibilité.

**A16 Un programme Python**

**Rappel Pour $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, dire que $b$ est un diviseur de $a$ revient à dire que le reste de la division euclidienne de $a$ par $b$ est nul.**

**Écrire un programme Python qui demande d'entrer un entier naturel non nul puis affiche la liste des diviseurs positifs.**

```
1 a=int(input("a="))
2 L=[]
3 for k in range(1,a+1):
4     if a%k==0:
5         L.append(k)
6 print("liste des diviseurs positifs de",a,":",L)
```

**A17 Déterminer tous les entiers naturels $n$ tels que : $n - 3|7$.**

Dire que $n - 3|7$ revient à dire que $n - 3$ est un diviseur de 7.

Or, les diviseurs de 7 sont : $-7$, $-1$, 1 et 7 donc quatre cas seulement peuvent se présenter :

- $n - 3 = -7 \Leftrightarrow n = -4$
- $n - 3 = -1 \Leftrightarrow n = 2$
- $n - 3 = 1 \Leftrightarrow n = 4$
- $n - 3 = 7 \Leftrightarrow n = 10$

Les entiers naturels $n$ cherchés sont donc : 2, 4 et 10.

**A18** Déterminer tous les entiers relatifs $n$ vérifiant le système :

$$(S)\begin{cases} n+1 | 2n+3 \\ n+1 | 3n+2 \end{cases}$$

Ecrire un programme python qui recherche les entiers $n$ vérifiant $(S)$ dans l'intervalle $[\![-100\,;100]\!]$.

$P$ Pour tout $a \in \mathbb{Z}-\{0\}$, si $d|a$, alors : $-|a| \leqslant d \leqslant |a|$ et $d \neq 0$.
Autrement dit tout diviseurs (dans $\mathbb{Z}$) de $a \in \mathbb{Z} \setminus \{0\}$ est compris entre : $-|a|$ et $|a|$.

**A19** Déterminer les entiers relatifs $n$ tels que : $n+3 | 2n+1$.
Vérifier en écrivant un programme Python qui recherche $n$ dans $[\![-100; 100]\!]$.

$P$ ▶Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, on a l'implication : $a|b \Rightarrow \forall c \in \mathbb{Z}, a|b \times c$.

**A20** Démontrer la propriété précédente.

$P$ Pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ on a l'implication :

$$a|b \Rightarrow a \times c | b \times c$$

Autrement dit : on peut multiplier les deux membres d'une relation de divisibilité par un même entier relatif et c'est une implication.

**A21** Démontrer la propriété précédente.

**A22** Un élève dit « pour tout $(a,b,c) \in \mathbb{Z}^3$ on a l'implication : $a \times c | b \times c \Rightarrow a|b$ ». Que faut-il penser de cette affirmation ?
Et si on ajoute la condition $c \neq 0$ ?

**A23** Un élève dit « soient $a$, $b$ deux entiers relatifs tels que $a|b$, alors pour tout entier relatif $c$ on a : $a+c|b+c$ ».
Trouver un contre-exemple.

$i$ Dans une relation de divisibilité on ne peut pas ajouter/retrancher le même entier relatif à chaque membre.

$D$ La **partie entière** d'un réel $x$ est l'unique **entier relatif** note $E(x)$ vérifiant : $\boldsymbol{E(x) \leqslant x < E(x)+1}$.

$i$ En Python la partie entière est `floor(...)` accessible après chargement de la bibliothèque math par : `from math import *`
💣 Il ne faut pas utiliser int(...).

$P$ Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, alors il existe un unique couple $(q,r)$ d'entiers naturels vérifiant : $a = q \times b + r$ avec $0 \leqslant r < b$.

$D$ **Division euclidienne dans $\mathbb{N}$**
Pour $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, **effectuer la division euclidienne** de $a$ par $b$ c'est déterminer les deux entiers naturels $q$ et $r$ tels que :

$$\boldsymbol{a = q \times b + r} \text{ avec } \boldsymbol{0 \leqslant r < b}$$

$i$ on a $b$ valeurs possibles pour le reste $r$ : $0, 1, \ldots, b-1$.

**A24** On souhaite démontrer la propriété précédente.
Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, on travaille dans $\mathbb{R}$, on pose $q = E\left(\frac{a}{b}\right)$.

1. **Existence**
   - **a.** Justifier que $q \geqslant 0$ puis montrer que : $0 \leqslant a - qb < b$.
   - **b.** On pose $r = a - qb$, justifier que : $a = qb + r$ et $0 \leqslant r < b$.
2. **Unicité**
   Soient $q$, $r$, $q'$ et $r'$ des entiers naturels vérifiant :
   $a = qb + r$, $a = q'b + r'$, $0 \leqslant r < b$ et $0 \leqslant r' < b$ avec $r \geqslant r'$
   - **a.** Démontrer que : $b | r - r'$.
   - **b.** Démontrer que : $-b < r - r' < b$.
   - **c.** Montrer que $r = r'$, en déduire que $q = q'$.

**A25** Le produit de trois entiers relatifs consécutifs est-il toujours divisible par 3 ?

**A18 Déterminer tous les entiers relatifs $n$ vérifiant le système :**

$$(S)\begin{cases} n+1 | 2n+3 \\ n+1 | 3n+2 \end{cases}$$

**Ecrire un programme python qui recherche les entiers $n$ vérifiant $(S)$ l'intervalle $[\![-100\,;100]\!]$.**

Analyse

On a : $n+1|2n+3$ et $n+1|3n+2$ donc $n+1$ divise toute combinaison linéaire de $2n+3$ et $3n+2$ et en particulier :

$n+1|3(2n+3)-2(3n+2)$ c'est-à-dire

$n+1|6n+9-6n-4$, soit finalement : $n+1|5$.

Or, les diviseurs de 5 dans $\mathbb{Z}$ sont $-5$, $-1$, 1 et 5 donc quatre cas seulement peuvent se présenter :

- $n+1=-5$ qui donne $n=-6$
- $n+1=-1$ qui donne $n=-2$
- $n+1=1$ qui donne $n=0$
- $n+1=5$ qui donne $n=4$

Synthèse

- si $n=-6$

alors $n+1=-6+1=-5$

$2n+3=2(-6)+3=-9$

$non((-5)|(-9))$ donc $n=-6$ est refusé

- si $n=-2$

$n+1=-2+1=-1$

$2n+3=2(-2)+3=-1$

$3n+2=3(-2)+2=-6+2=-4$

On a $(-1)|(-1)$ et $(-1)|(-4)$ donc $n=-2$ est accepté.

- si $n=0$

$n+1=0+1=1$

$2n+3=2(0)+3=3$

$3n+2=3(0)+2=2$

On a : $1|3$ et $1|2$ donc $n=0$ est accepté.

- si $n=4$

$n+1=4+1=5$

$2n+3=2(4)+3=8+3=11$

$non\ (5|11)$ donc $n=4$ est refusé.

Conclusion

Les entiers relatifs $n$ vérifiant $\begin{cases} n+1|2n+3 \\ n+1|3n+2 \end{cases}$ sont : $-2$ **et** $0$.

```
1  for n in range(-100,101):
2      if (n+1)!=0:
3          if ((2*n+3)%(n+1)==0 and (3*n+2)%(n+1)==0):
4              print(n,end=" ")
```

```
Shell
>>> %Run 'Maths XP A18 2024-25.py'
-2 0
```

$P$ Pour tout $a \in \mathbb{Z}-\{0\}$, si $d|a$, alors : $-|a| \leqslant d \leqslant |a|$ et $d \neq 0$.
Autrement dit : tout diviseurs (dans $\mathbb{Z}$) de $a \in \mathbb{Z} \setminus \{0\}$ est compris entre $-|a|$ et $|a|$.

**A19 Déterminer les entiers relatifs $n$ tels que : $n+3|2n+1$.**
**Vérifier en écrivant un programme Python qui recherche $n$ dans $[\![-100;100]\!]$.**

Analyse

Soit $n \in \mathbb{Z}$ tel que : $n+3|2n+1$.On a : $n+3|n+3$ et $n+3|2n+1$ donc $n+3$ divise toute combinaison linéaire de $n+3$ et $2n+1$, en particulier :

$n+3|2(n+3)+(-1)(2n+1) \Leftrightarrow n+3|2n+6-2n- \Leftrightarrow n+3|5$

Or, les diviseurs de 5 dans $\mathbb{Z}$ sont : $-5$, $-1$, 1 et 5 donc quatre cas seulement peuvent se présenter :

- $n+3=-5 \Leftrightarrow n=-8$
- $n+3=-1 \Leftrightarrow n=-4$
- $n+3=1 \Leftrightarrow n=-2$
- $n+3=5 \Leftrightarrow n=2$

Synthèse

• si $n = -8$

$n + 3 = -8 + 3 = -5$

$2n + 1 = 2(-8) + 1 = -15$

On a : $-5|-15$ donc $n = -8$ est accepté

• si $n = -4$

$n + 3 = -4 + 3 = -1$

$2n + 1 = 2(-4) + 1 = -7$

$-1|-7$ donc $n = -4$ est accepté

• si $n = -2$

$n + 3 = -2 + 3 = 1$

$2n + 1 = 2(-2) + 1 = -3$

$1|-3$ donc $n = -2$ est accepté

• si $n = 2$

$n + 3 = 2 + 3 = 5$

$2n + 1 = 2(2) + 1 = 5$

$5|5$ donc $n = 2$ est accepté

Conclusion

Les entiers relatifs $n$ tels que $(n + 3)|(2n + 1)$ sont : $\mathbf{-8, -4, -2, 2}$.

```
1 for n in range(-100,101):
2     if (not((n+3)==0) and ((2*n+1)%(n+3)==0)):
3             print(n,end=" ")
```

Shell

```
>>> %Run 'ARITH ARITH A19 2022-23.py'
-8 -4 -2 2
```

$P$ Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $a|b$, alors $\forall c \in \mathbb{Z}$ on a : $a|b \times c$.

**A20 Démontrer la propriété précédente.**

Soient $a$, $b$ deux entiers relatifs tels que $a|b$ et $c \in \mathbb{Z}$.
On a : $a|b$ donc il existe $k \in \mathbb{Z}$ tel que $b = ka$.
Alors : $bc = ka \times c = kc \times a$. Il existe $k' \in \mathbb{Z}$ tel que $b \times c = k' \times a$, à savoir $k' = k \times c$, donc $a|bc$.

$P$ Pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ on a l'implication :

$$a|b \Rightarrow a \times c|b \times c$$

Autrement dit : on peut multiplier les deux membres d'une relation de divisibilité par un même entier relatif et c'est une implication.

**A21 Démontrer la propriété précédente.**

Soient $a$,$b$ deux entiers relatifs tels que $a|b$ et $c \in \mathbb{Z}$.
On a : $a|b$ donc il existe $k \in \mathbb{Z}$ tel que $b = ka$.
Alors : $b \times c = ka \times c = k \times (a \times c)$.
Il existe $k \in \mathbb{Z}$ tel que $b \times c = k \times (a \times c)$ donc $a \times c|b \times c$.

**A22 Un élève dit « pour tout $(a, b, c) \in \mathbb{Z}^3$ on a l'implication : $a \times c|b \times c \Rightarrow a|b$ ». Que faut-il penser de cette affirmation ? Et si on ajoute la condition $c \neq 0$ ?**

On a : $3 \times 0|4 \times 0$ mais $non(3|4)$, on a trouvé un contre-exemple donc l'affirmation est fausse. On peut cependant montrer que :
**si $c \neq 0$, alors on a l'implication : $a \times c|b \times c \Rightarrow a|b$.**
Supposons : $a \times c|b \times c$, il existe $k \in \mathbb{Z}$ tel que $b \times c = k \times a \times c$, ce qui s'écrit aussi : $bc - kac = 0$, ou encore $c(b - ka) = 0$, or $c \neq 0$ donc $b - ka = 0$ autrement dit $b = ka$ donc : $a|b$.

**A23 Un élève : « soient $a$, $b$ deux entiers relatifs tels que $a|b$, alors pour tout entier relatif $c$ on a : $a + c|b + c$ ».**
**Trouver un contre-exemple.**
Contre-exemple : on a $4|8$ mais $non(4 + 1|8 + 1)$.

$i$ Dans une relation de divisibilité on ne peut pas ajouter/retrancher un même entier à chaque membre.

$D$ La **partie entière** d'un réel $x$ est l'unique (admis) entier relatif $n$ tel que : $n \leqslant x < n+1$. En notant $E(x)$ la partie entière de $x$ on a donc : $\boldsymbol{E(x) \in \mathbb{Z}}$ et $\boldsymbol{E(x) \leqslant x < E(x)+1}$.

$i$ En Python la partie entière est `floor(…)` accessible après chargement de la bibliothèque `math` : il ne faut pas utiliser int(…).

$P$ Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, alors il existe un et un seul couple $(q,r)$ d'entiers naturels vérifiant : $a = q \times b + r$ avec $0 \leqslant r < b$.

$D$ **Division euclidienne dans $\mathbb{N}$**

Pour $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, **effectuer la division euclidienne** de $a$ par $b$ c'est déterminer les deux entiers naturels $q$ et $r$ tels que :

$$a = q \times b + r \ \ et \ \ 0 \leqslant r < b$$

**A24 On souhaite démontrer la propriété précédente.**

**Soit $\boldsymbol{a \in \mathbb{N}}$ et $\boldsymbol{b \in \mathbb{N} \setminus \{0\}}$, on travaille dans $\mathbb{R}$ et on pose $\boldsymbol{q = E\left(\frac{a}{b}\right)}$.**

1. **Existence**

   a. **Justifier que $\boldsymbol{q \geqslant 0}$ puis que : $\boldsymbol{0 \leqslant a - qb < b}$.**

   $a \geqslant 0$ et $b > 0$ donc $\frac{a}{b} \geqslant 0$, donc $E\left(\frac{a}{b}\right) \geqslant 0$ i.e. $\boldsymbol{q \geqslant 0}$.

   Par définition de la partie entière, on a :

   $$E\left(\frac{a}{b}\right) \leqslant \frac{a}{b} < E\left(\frac{a}{b}\right) + 1$$

   autrement dit : $q \leqslant \frac{a}{b} < q+1$, puis en multipliant par $q > 0$ on obtient :

   $$q \times b \leqslant \frac{a}{b} \times b < (q+1) \times b \Leftrightarrow qb \leqslant a < qb + b$$
   $$\Leftrightarrow qb - qb \leqslant a - qb < qb + b - qb \Leftrightarrow \boldsymbol{0 \leqslant a - qb < b} \ (*)$$

   b. **On pose $\boldsymbol{r = a - qb}$, justifier que : $\boldsymbol{a = qb + r}$ et $\boldsymbol{0 \leqslant r < b}$.**

   $r = a - qb \Leftrightarrow r + qb = a - qb + qb \Leftrightarrow qb + r = a$
   $\Leftrightarrow a = qb + r$. En posant $r = a - qb$, l'inégalité $(*)$ devient : $0 \leqslant r < b$. Résumons : $\boldsymbol{a = qb + r}$ **et** $\boldsymbol{0 \leqslant r < b}$.

2. **Unicité**

   **Soient $\boldsymbol{q, r, q'}$ et $\boldsymbol{r'}$ des entiers naturels vérifiant :**
   **$\boldsymbol{a = qb + r, a = q'b + r', 0 \leqslant r < b}$ et $\boldsymbol{0 \leqslant r' < b}$ avec $\boldsymbol{r \geqslant r'}$**

   a. **Démontrer que : $\boldsymbol{b | r - r'}$**

   $a = qb + r$ s'écrit aussi : $r = a - qb$
   $a = q'b + r'$ s'écrit aussi : $r' = a - q'b$.
   On a donc :
   $r - r' = a - qb - (a - q'b) = -qb + q'b = (-q + q')b$
   Il existe $k \in \mathbb{Z}$ tel que $r - r' = kb$, à savoir $k = -q + q'$, donc : $\boldsymbol{b | r - r'}$.

   b. **Démontrer que : $\boldsymbol{-b < r - r' < b}$**

   On a d'une part : $0 \leqslant r < b \ (*)$
   d'autre part on a : $0 \leqslant r' < b$ donc $0 \geqslant -r' > -b$
   autrement dit : $-b < -r' \leqslant 0 \ (**)$.
   En ajoutant membre à membre $(*)$ et $(**)$ on obtient :
   $0 + (-b) < r + (-r') < b + 0$, i.e. : $\boldsymbol{-b < r - r' < b}$.

   c. **Montrer que $\boldsymbol{r = r'}$, en déduire que $\boldsymbol{q = q'}$**

   Effectuons un raisonnement par l'absurde.
   Faisons l'hypothèse que $r \neq r'$ alors $r - r' \neq 0$ ; d'après **a.** on a : $b | r - r'$. On a : $r - r' \neq 0$, $b \in \mathbb{N}$, $b | r - r'$ donc $1 \leqslant b \leqslant r - r'$ d'où en particulier $b \leqslant r - r'$ ce qui est contradiction avec la conséquence $r - r' < b$ de l'inégalité $-b < r - r' < b$ démontrée en **b.** donc il faut rejeter l'hypothèse $r \neq r'$ autrement dit on peut à présent affirmer que $r = r'$. On a ensuite les équivalences :
   $r = r' \Leftrightarrow a - qb = a - q'b \Leftrightarrow q'b - qb = 0$
   $\Leftrightarrow (q' - q)b = 0 \Leftrightarrow q' - q = 0 \ ou \ b = 0$, or $b \neq 0$ donc $q' - q = 0$ autrement dit $q' = q$. L'unicité est démontrée.

**A25 Le produit de trois entiers relatifs consécutifs est-il toujours divisible par 3 ?**

On se donne trois entiers relatifs consécutifs : $n$, $n+1$ et $n+2$.
Leur produit est $n(n+1)(n+2)$.

Nous allons procéder par disjonction de cas suivant le reste de la division euclidienne de $n$ par $3$.

• **1er cas : le reste est $0$**

Il existe $k \in \mathbb{Z}$ tel que $n = 3k$, alors :

$$n(n+1)(n+2) = 3k(3k+1)(3k+2)$$

Il existe $k' \in \mathbb{Z}$ tel que $n(n+1)(n+2 = 3k'$,

à savoir $k' = k(3k+1)(3k+2)$, donc $3|n(n+1)(n+2)$

• **2e cas : le reste est $1$**

Il existe $k \in \mathbb{Z}$ tel que $n = 3k+1$, alors :

$$n(n+1)(n+2) = (3k+1)(3k+2)(3k+3)$$
$$= 3(3k+1)(3k+2)(k+1)$$

Il existe $k' \in \mathbb{Z}$ tel que $n(n+1)(n+2 = 3k'$,

à savoir $k' = (3k+1)(3k+2)(k+1)$, donc $3|n(n+1)(n+2)$

• **3e cas : le reste est $2$**

Il existe $k \in \mathbb{Z}$ tel que $n = 3k+2$, alors :

$$n(n+1)(n+2) = (3k+2)(3k+3)(3k+4)$$
$$= 3(3k+2)(k+1)(3k+4)$$

Il existe $k' \in \mathbb{Z}$ tel que $n(n+1)(n+2 = 3k'$,

à savoir $k' = (3k+2)(k+1)(3k+4)$, donc $3|n(n+1)(n+2)$

<u>Conclusion</u>

$\forall n \in \mathbb{Z}, 3|n(n+1)(n+2)$ donc **le produit de trois entiers relatifs consécutifs est toujours divisible par $3$**.

**A26** On vérifie facilement que : $1\,336 = 57 \times 23 + 25$.
Quel est le reste et le quotient de la division euclidienne de $1\,336$ par $23$ ? Vérifier à l'aide de la calculatrice.

**A27** Sachant que le reste de la division euclidienne d'un entier naturel $a$ par $5$ est $4$, déterminer le reste de la division euclidienne de $2a$ par $5$ et celui de la division euclidienne de $3a$ par $5$.

**A28** Déterminer le quotient et le reste de la division euclidienne de $16\,881$ par $12$.

**A29** Poser la division euclidienne de $2024$ par $3$ puis écrire l'égalité qui en résulte, en déduire le quotient et le reste de la division euclidienne de $2024$ par $6$.

**A30** Pour tout $n \in \mathbb{N}$, on pose $a_n = 10n^2 + 22n + 14$, $b_n = 2n + 3$ et on note $r_n$ le reste de la division euclidienne de $a_n$ par $b_n$.

• vérifier que, pour tout $n \in \mathbb{N}$, on a :
$$10n^2 + 22n + 14 = (5n + 3)(2n + 3) + n + 5$$

• un élève affirme que, pour tout $n \in \mathbb{N}$, $r_n = n + 5$ : donner un contre-exemple

• déterminer $r_n$ en fonction de $n$ en distinguant plusieurs cas

**A31** Pour tout $n \in \mathbb{N}$, on pose $a_n = 7n + 17$, $b_n = 2n + 5$
et on note $r_n$ le reste de la division euclidienne de $a_n$ par $b_n$.

1. Déterminer $a_0$ et $b_0$ puis poser la division euclidienne de $a_0$ par $b_0$, en déduire $c_0$.
   Procéder de même pour $a_1$ et $b_1$, déterminer $r_1$.
2. À l'aide de la calculatrice, énoncer une conjecture sur $r_n$ en fonction de $n$ puis la démontrer.
3. On se propose de retrouver $r_n$ en fonction de $n$ : poser la division euclidienne de $a_n$ par $b_n$, en déduire une égalité puis vérifier que celle-ci décrit bien la division euclidienne de $a_n$ par $b_n$.

**D** Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$ il existe un unique couple $(q\,;r)$ tel que $q \in \mathbb{Z}$, $r \in \mathbb{N}$ et $\boldsymbol{a = qb + r}$ avec $\boldsymbol{0 \leqslant r < |b|}$.
On dit que pour la division euclidienne de $a$ par $b \neq 0$ : $a$ est le **dividende**, $q$ est le **quotient**, $b$ est le **diviseur** et $r$ est le **reste**.
le **reste $r$** est **toujours positif ou nul**

**i** Si $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$ la division euclidienne dans $\mathbb{N}$ et celle dans $\mathbb{Z}$ donnent le même couple d'entiers $(q, r)$ : il est donc alors inutile de préciser dans lequel de ces deux ensembles on raisonne.

**A32** Poser la division euclidienne de $125$ par $10$ et écrire l'égalité qui en résulte puis déterminer le quotient et le reste de la division euclidienne de $125$ par $(-10)$.

**i** Pour une division euclidienne dans $\mathbb{N}$ : la commande partEnt(…) et la commande reste(…) de la calculatrice sont utilisables, les commandes // et % de Python sont utilisable.
Elles ne doivent pas être utilisées lorsque le dividende ou diviseur de la division euclidienne est négatif.

**A33** Déterminer le quotient et le reste de la division euclidienne de $132$ par $(-5)$.

**A34** Déterminer le quotient et le reste de la division euclidienne de $(-1245)$ par $(-12)$.

**A35** Déterminer le quotient et le reste de la division euclidienne de $(-75)$ par $80$.

**D** On dit que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont **congrus modulo $m \in \mathbb{N} \setminus \{0\}$** lorsque $a$ et $b$ ont le **même reste** pour la division euclidienne par $m$, et on écrit lors : $\boldsymbol{a \equiv b\ [m]}$, $\boldsymbol{a \equiv b\ (m)}$ ou encore $\boldsymbol{a \equiv b\ \mod m}$.
i Le nombre $m$ du modulo est nécessairement strictement positif.

**A36** Justifier que $176 \equiv 41\ [5]$.

**A26** **On vérifie facilement que : $1\,336 = 57 \times 23 + 25$.**
**Quel est le reste et le quotient de la division euclidienne de $1\,336$ par $23$ ? Vérifier à l'aide de la calculatrice.**

• en posant la multiplication $57 \times 23$ on obtient $1\,311$, on en déduit que : $57 \times 23 + 25 = 1\,311 + 25 = 1\,336$

dans l'égalité $1\,336 = 57 \times 23 + 25$, $non(0 \leqslant 25 < 23)$

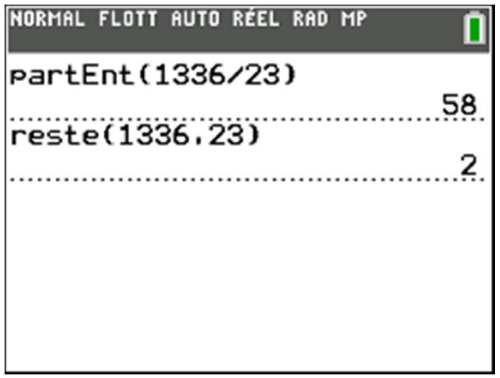
donc $25$ n'est pas le reste de la division euclidienne de $1\,336$ par $23$.

On a :

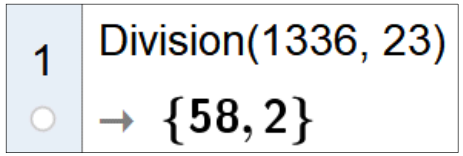
$$1\,336 = 57 \times 23 + 25$$
$$1\,336 = 57 \times 23 + 1 \times 23 + 2$$
$$1\,336 = (57 + 1) \times 23 + 2$$
$$1\,336 = 58 \times 23 + 2$$

On a : $1\,336 = 58 \times 23 + 2$ avec $0 \leqslant 2 < 23$ donc pour la division euclidienne de $1\,336$ par $23$ le reste est $2$ et le quotient $58$.

Vérification avec la calculatrice :




Avec GeoGebra :




**A27** **Sachant que le reste de la division euclidienne d'un entier naturel $a$ par $5$ est $4$, déterminer le reste de la division euclidienne de $2a$ par $5$ et celui de la division euclidienne de $3a$ par $5$.**

Recherche

On peut d'abord se donner un exemple : $a = 4$ convient.
Le reste de la division euclidienne de $2a = 8$ par $5$ est $3$,
le reste de la division euclidienne de $3a = 12$ par $5$ est $2$.

Pour la division euclidienne de $a$ par $5$, le reste est $4$ donc il existe $q \in \mathbb{N}$ tel que $a = q \times 5 + 4 = 5q + 4$. On a d'une part :
$2a = 2(5q + 4) = 10q + 8 = 10q + 5 \times 1 + 3 = 5(2q + 1) + 3$
Résumons : $2a = (2q + 1) \times 5 + 3$ avec $0 \leqslant 3 < 5$ donc **pour la division euclidienne de $2a$ par $5$ le reste est $3$**. D'autre part, on a :
$3a = 3(5q + 4) = 15q + 12 = 15q + 10 + 2 = 5(3q + 2) + 2$
Résumons : $3a = (3q + 2) \times 5 + 2$ avec $0 \leqslant 2 < 5$ donc **pour la division euclidienne de $3a$ par $5$ le reste est $2$**.

**A28** **… quotient et reste de la division euclidienne $16\,881$ par $12$**

Posons la division euclidienne de $16\,881$ par $12$ :

| | | | | | |
|---|---|---|---|---|---|
| 1 | 6 | 8 | 8 | 1 | 12 |
| −1 | 2 | ↓ | | | 1406 |
| | 4 | 8 | | | |
| | −4 | 8 | ↓ | | |
| | | 0 | 8 | | |
| | | − | 0 | ↓ | |
| | | | 8 | 1 | |
| | | | −7 | 2 | |
| | | | | 9 | |

Pour la division euclidienne de $16\,881$ par $12$ le quotient est $1\,406$ et le reste $9$, on a : $16\,881 = 1\,406 \times 12 + 9$, $0 \leqslant 9 < 12$.

**A29** **Poser la division euclidienne de $2024$ par $3$ puis écrire l'égalité qui en résulte, en déduire le quotient et le reste de la division euclidienne de $2024$ par $6$.**

En posant la division euclidienne (N.R.) de $2\,024$ par $3$ on obtient :
$2\,024 = 674 \times 3 + 2$ avec $0 \leqslant 2 < 3$.
On en déduit : $2\,024 = 2 \times 337 \times 3 + 2 = 337 \times 6 + 2$.
On a : $2\,024 = 337 \times 6 + 2$ avec $0 \leqslant 2 < 6$ donc pour la division euclidienne de $2\,024$ par $6$ **le quotient est $337$ et le reste $2$**.

**A30** $\forall n \in \mathbb{N}$, **on pose $a_n = 10n^2 + 22n + 14$, $b_n = 2n + 3$**
**on note $r_n$ le reste de la division euclidienne dans $\mathbb{N}$ de $a_n$ par $b_n$.**
**• vérifier que, pour tout $n \in \mathbb{N}$, on a :**

$$10n^2 + 22n + 14 = (5n + 3)(2n + 3) + n + 5$$

**• un élève affirme que, pour tout $n \in \mathbb{N}$, $r_n = n + 5$ : trouver un contre-exemple**
**• déterminer $r_n$ en fonction de $n$ en distinguant plusieurs cas**

• soit $n \in \mathbb{N}$, on a :

$$(5n + 3)(2n + 3) + n + 5 = 10n^2 + 15n + 6n + 9 + n + 5$$
$$= 10n^2 + 22n + 5$$

On a donc bien :

$$\forall n \in \mathbb{N}, 10n^2 + 22n + 14 = (5n + 3)(2n + 3) + n + 5$$

• l'égalité suivante, valable pour tout $n \in \mathbb{N}$, s'écrit aussi :

$$a_n = (5n + 3)b_n + n + 5$$

Elle traduit la division euclidienne de $a_n$ par $b_n$ si et seulement si $0 \leqslant n + 5 < b_n$ ce qui est équivalent à : $0 \leqslant n + 5 < 2n + 3$
Pour tout $n \in \mathbb{N}$, on a : $0 \leqslant n + 5$, donc elle est équivalente à

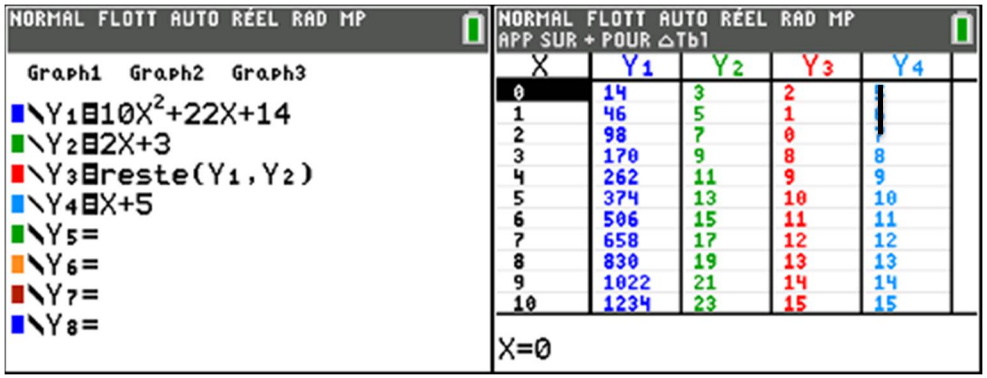
$$n + 5 < 2n + 3 \Leftrightarrow n + 5 - n < 2n + 3 - n \Leftrightarrow 5 < n + 3$$
$$\Leftrightarrow 5 - 3 < n + 3 - 3 \Leftrightarrow 2 < n$$

On doit donc étudier séparément les cas $n = 0$, $n = 1$ et $n = 2$.
• pour $n = 0$
$a_0 = 14$, $b_0 = 3$, on a : $14 = 4 \times 3 + 2$ avec $0 \leqslant 2 < 3$
donc : $r_0 = 2$

• pour $n = 1$
$a_1 = 10 + 22 + 14 = 46$, $b_1 = 5$, on a : $46 = 9 \times 5 + 1$ avec $0 \leqslant 1 < 5$ donc $r_1 = 1$
• pour $n = 2$
$a_2 = 10 \times 4 + 22 \times 2 + 14 = 98$, $b_2 = 2(2) + 3 = 7$,
on a : $98 = 14 \times 7 + 0$ avec $0 \leqslant 0 < 7$ donc $r_2 = 0$

Conclusion
$\boldsymbol{r_0 = 2, r_1 = 1, r_2 = 0}$ et pour $\boldsymbol{n \geqslant 3, r_n = n + 5}$.

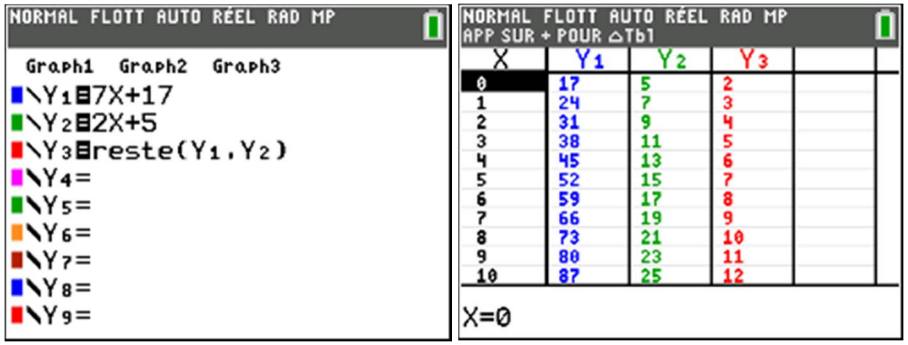
Vérifions avec la calculatrice :



**A31** **Pour tout $n \in \mathbb{N}$, on pose $a_n = 7n + 17$, $b_n = 2n + 5$ et on note $r_n$ le reste de la division euclidienne de $a_n$ par $b_n$.**

1. **Déterminer $a_0$, $b_0$, poser la division euclidienne de $a_0$ par $b_0$, en déduire $c_0$. Procéder de même pour $a_1$et $b_1$, déterminer $r_1$.**
   $a_0 = 7(0) + 17 = 17$, $b_0 = 2(0) + 5 = 5$
   $17 = 3 \times 5 + 2$ avec $0 \leqslant 2 < 5$ donc $r_0 = 2$
   $a_1 = 7(1) + 17 = 24$, $b_1 = 2(1) + 5 = 7$
   $24 = 3 \times 7 + 3$ avec $0 \leqslant 3 < 7$ donc $r_1 = 3$

2. **À l'aide de la calculatrice, énoncer une conjecture sur $r_n$ en fonction de $n$ puis la démontrer.**




On peut conjecturer que : « $\forall n \in \mathbb{N}, r_n = n + 2$ ».
Soit $n \in \mathbb{N}$, on a :
$7n + 17 = 7n + 17 - (n + 2) + n + 2 = 6n + 15 + n + 2$
$= 3(2n + 5) + n + 2$
Résumons :
On a : $2n + 5 - (n + 2) = n + 3 > 0$ donc : $2n + 5 > n + 2$.
Résumons :
$7n + 17 = 3 \times (2n + 5) + n + 2$ avec $0 \leqslant n + 2 < 2n + 5$
Or, $a_n = 7n + 17$, $b_n = 2n + 5$ donc :
$a_n = 3b_n + n + 2$ avec $0 \leqslant n + 2 < b_n$
ce qui montre que $r_n = n + 2$.
Conclusion : $\forall \boldsymbol{n \in \mathbb{N}, r_n = n + 2}$.

$\boxed{D}$ Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$ il existe un unique couple $(q\,; r)$ tel que $q \in \mathbb{Z}$, $r \in \mathbb{N}$ et $\boldsymbol{a = qb + r}$ avec $\boldsymbol{0 \leqslant r < |b|}$.
On dit que pour la division euclidienne de $a$ par $b \neq 0$ : $a$ est le **dividende**, $q$ est le **quotient**, $b$ est le **diviseur** et $r$ est le **reste**.
on retiendra que le reste $r$ est toujours positif ou nul

$\boxed{i}$ Si $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, alors la division euclidienne dans $\mathbb{N}$ et celle dans $\mathbb{Z}$ donnent le même couple $(q, r)$ : il est donc alors inutile de préciser dans lequel de ces deux ensembles on travaille.

**A32** **Poser la division euclidienne de $125$ par $10$ et écrire l'égalité qui en résulte puis déterminer le quotient et le reste de la division euclidienne de $125$ par $(-10)$.**

$125 = 12 \times 10 + 5$ avec $0 \leqslant 5 < 10$.
On en déduit que : $125 = (-12) \times (-10) + 5$ avec $0 \leqslant 5 < |-10|$
donc pour la division euclidienne de $125$ par $(-10)$ le quotient est $(-12)$ et le reste $5$.

**A33** **Déterminer le quotient et le reste de la division euclidienne de $132$ par $(-5)$.**
On commence par poser la division euclidienne avec les entiers naturels correspondants, puis on modifie l'égalité qui en résulte.
On a : $132 = 130 + 2 = 26 \times 5 + 2$ donc :
$132 = (-26) \times (-5) + 2$ avec $0 \leqslant 2 < |-5|$ .
Pour la division euclidienne de $132$ par $(-5)$, le quotient est $(-26)$ et le reste $2$.

**A34** **Déterminer le quotient et le reste de la division euclidienne de $(-1\,245)$ par $(-12)$.**
On commence par poser la division euclidienne par les deux naturels correspondants, puis on modifie l'égalité qui en résulte.
La division euclidienne de $1\,245$ par $12$ donne $1245 = 103 \times 12 + 9$
Donc : $-1\,245 = -103 \times 12 - 9$

On en déduit :
$-1\,245 = 103 \times (-12) - 12 + 12 - 9$
$-1\,245 = 103 \times (-12) + 1 \times (-12) + 3$
$-1\,245 = 104 \times (-12) + 3$ avec $0 \leqslant 3 < |-12|$.
Conclusion
Pour la division euclidienne de $(-1\,245)$ par $(-12)$ **le quotient est $\mathbf{104}$ et le reste $\mathbf{3}$**.

**A35 Déterminer le quotient et le reste de la division euclidienne de $(-75)$ par $80$.**

On a : $-75 = (-1) \times 80 + 5$ avec $0 \leqslant 5 < 80$ donc pour la division euclidienne de $(-75)$ par $80$ **le quotient est $(-1)$ et le reste $5$**.

$\boxed{D}$ On dit que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont **congrus modulo $m \in \mathbb{N} \setminus \{0\}$** lorsque $a$ et $b$ ont le même reste pour la division euclidienne par $m$, on écrit : $a \equiv b\ [m]$, $a \equiv b\ (m)$ ou encore $a \equiv b \mod m$.
$\boxed{i}$ le « nombre modulo » est un entier strictement positif.

**A36 Justifier que $176 \equiv 41\ [5]$.**
En posant la division euclidienne de $176$ par $5$ on obtient :
$176 = 35 \times 5 + \boxed{1}$ avec $0 \leqslant 1 < 5$ donc le reste de cette division est $1$.
En posant la division euclidienne de $41$ par $5$ on obtient :
$41 = 8 \times 5 + \boxed{1}$ avec $0 \leqslant 1 < 5$ donc le reste de cette division est encore $1$.
$176$ et $41$ ont même reste pour la division euclidienne par $5$ donc $\mathbf{176 \equiv 41\ [5]}$.

**A37** Justifier que $32 \equiv 20\ [6]$.

$P$ ▶ Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$, on a l'équivalence :

$$\boldsymbol{a \equiv b\ [m] \Leftrightarrow m|a-b}$$

Autrement dit deux entiers relatifs sont congrus modulo $m$ si et seulement le **nombre $m$ divise leur différence**.

**A38** On souhaite démontrer la propriété précédente.

Lemme : Pour tout réel $x$ et tout réel strictement positif $\varepsilon$, on a l'équivalence : $-\varepsilon < x < \varepsilon \Leftrightarrow |x| < \varepsilon$.

La divisions euclidiennes de $a$ et $b$ par $m$ s'écrivent respectivement $a = qm + r$ et $b = q'm + r'$ avec $0 \leqslant r < m$ et $0 \leqslant r' < m$.

1. Montrer que : $|r - r'| < m$.
2. On suppose $a \equiv b\ [m]$, montrer que : $m|a-b$.
3. On suppose $m|a-b$.
   a. Montrer que : $m|r-r'$.
   b. On suppose que $r \neq r'$, déduire de **a.** que $m \leqslant |r-r'|$. Mettre en évidence une contradiction, en déduire $a \equiv b\ [m]$.
4. Démontrer le Lemme.

**A39** Justifier que : $567 \equiv 17\ [50]$.

$P$ Pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ :

▶ $\boldsymbol{a \equiv a\ [m]}$

▶ on a l'équivalence : $\boldsymbol{a \equiv b\ [m] \Leftrightarrow b \equiv a\ [m]}$

▶ on a l'implication : $\boldsymbol{a \equiv b\ [m]}$ **et** $\boldsymbol{b \equiv c\ [m] \Rightarrow a \equiv c\ [m]}$

$i$ Ces trois points sont la **réflexivité**, la **symétrie** et la **transitivité**.

▶ on a l'équivalence : $\boldsymbol{m|a \Leftrightarrow a \equiv 0\ [m]}$

Une relation de **divisibilité** avec diviseur positif **se traduit par une congruence à zéro**.

**A40** Démontrer les quatre points précédents.

**A41** Déterminer les entiers relatifs $x$ tels que : $x \equiv 3\ [7]$.

$P$ Pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$ on a les équivalences :

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a + c \equiv b + c\ [m]}$

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a - c \equiv b - c\ [m]}$

et on a l'**implication** :

▶ $\boldsymbol{a \equiv b\ [m] \Rightarrow a \times c \equiv b \times c\ [m]}$ c'est une **implication** !

**A42** Démontrer les trois points précédents.

**A43** Justifier que : $5 \times 6 \equiv 1 \times 6\ [3]$ ; a-t-on « $5 \equiv 1\ [3]$ » ?

$i$ Dans une congruence il est **interdit de simplifier «en divisant»** par un même nombre, même non nul.

$P$ Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$, on a les équivalences :

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow \exists k \in \mathbb{Z}, a = b + km}$

**A44** Démontrer la propriété précédente puis l'utiliser pour traduire :

• $x \equiv 4\ [9]$ • $\exists k \in \mathbb{Z}, y = 3 + 5k$

**A45** Déterminer les entiers relatifs $x$ tels que : $x - 1 \equiv 2\ [8]$.

$i$ On dit aussi « Résoudre dans $\mathbb{Z}$ : $x - 1 \equiv 2\ [8]$ ».

**A46** Déterminer les entiers relatifs $x$ compris entre 10 et 20 tels que : $x + 3 \equiv 5\ [6]$.

$i$ On dit aussi « Résoudre dans $[\![10\,;20]\!]$ : $x + 3 \equiv 5\ [6]$ ».

$P$ Pour tout $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$ on a les équivalences :

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a \equiv b + km\ [m]}$

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a \equiv b - km\ [m]}$

📖 On peut ajouter/soustraire des multiples du modulo dans l'un ou l'autre des membres d'une congruence.

**A47** Démontrer le premier « ▶ » .

**A48** Vérifier que : $5^2 \equiv 3^2\ [8]$ ; a-t-on $5 \equiv 3\ [8]$ ?

**A37** **Justifier que $32 \equiv 20\ [6]$.**

$32 = 5 \times 6 + 2$ avec $0 \leqslant 2 < 6$ donc pour la division euclidienne de 32 par 6 le reste est 2

$20 = 3 \times 6 + 2$ avec $0 \leqslant 2 < 6$ donc pour la division euclidienne de 20 par 6 le reste est 2

Les deux division euclidienne ont même reste donc : $32 \equiv 20\ [6]$

$P$ ▶ Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$, on a les équivalences :

$$\boldsymbol{a \equiv b\ [m] \Leftrightarrow m|a-b}$$

Autrement dit deux entiers relatifs sont congrus si et seulement le nombre du modulo divise leur différence.

Remarquons que l'on a aussi : $a \equiv b\ [m] \Leftrightarrow m|b-a$

**A38** **Démontrer la propriété précédente.**

**Lemme** **Pour tout réel $x$ et tout réel strictement positif $\varepsilon$, on a l'équivalence : $-\varepsilon < x < \varepsilon \Leftrightarrow |x| < \varepsilon$.**

**$a = qm + r$ et $b = q'm + r'$ avec $0 \leqslant r < m$ et $0 \leqslant r' < m$**

1. **Montrer que : $|r - r'| < m$.**

   On a d'une part : $0 \leqslant r < m$ et d'autre part :

   $0 \leqslant r' < m$ donc $0 \geqslant -r' > -m \Leftrightarrow -m < -r' \leqslant 0$

   d'où par somme : $0 + (-m) < r + (-r') < m + 0$

   c'est-à-dire : $-m < r - r' < m$, ce qui revient à dire que :

   $|r - r'| < m$.

   rappel : on peut ajouter membre à membre des inégalités mais il est interdit de les soustraire.

2. **On suppose $a \equiv b\ [m]$. Montrer que : $m|a-b$.**

   On a : $a \equiv b\ [m]$ donc $r = r'$ et il vient :

   $$a - b = qm + r - (q'm + r) = qm - q'm = (q - q')m$$

   Résumons : $a - b = (q - q')m$.

   Il existe $k \in \mathbb{Z}$ tel que $a - b = km$, à avoir $k = q - q'$,

   autrement dit $m|a-b$,

3. **On suppose $m|a-b$.**

   a. **Montrer que : $m|r-r'$.**

   On suppose : $m|a-b$

   $r - r' = (a - qm) - (b - q'm) = (a-b) + (q' - q)m$

   Ona : $m|a-b$ et $m|m$ donc $m$ divise toute combinaison linéaire de $a-b$ et $m$, en particulier $m|(a-b) + (q'-q)m$

   c'est-à-dire : $\boldsymbol{m|r-r'}$

   b. **On suppose que $r \neq r'$, déduire de a. que $m \leqslant |r-r'|$.**

   On a montré que $m|r-r'$ donc si $r \neq r'$ alors $m$ est un diviseur positif de $r - r' \neq 0$ donc $1 \leqslant m \leqslant |r-r'|$

   en particulier $m \leqslant |r-r'|$.

   ce qui est en contradiction avec $|r-r'| < m$ obtenu à la question 1. donc il faut rejeter l'hypothèse $r \neq r'$ par conséquent $r = r'$, donc $a \equiv b\ [m]$ .

   On vient de démontrer que $m|a-b \Rightarrow a \equiv b\ [m]$.

4. **Démontrons le Lemme.**

   Soit $\varepsilon \in \mathbb{R}^{+*}$, alors pour tout $x \in \mathbb{R}$ on a l'équivalence :

   $$-\varepsilon < x < \varepsilon \Leftrightarrow |x| < \varepsilon$$

   Procédons par disjonction de cas suivante le signe de $x$ :

   • **1er cas : $x \geqslant 0$**

   rappel

   Pour tout $a \in \mathbb{R}$, si $a \geqslant 0$ alors $|a| = a$.

   ☐ supposons $-\varepsilon < x < \varepsilon$ et montrons que $|x| < \varepsilon$

   $-\varepsilon < x < \varepsilon \Rightarrow x < \varepsilon$, or $|x| = x$, donc : $|x| < \varepsilon$

   on a donc : $-\varepsilon < x < \varepsilon \Rightarrow |x| < \varepsilon$ ☐☐

   ☐ supposons que $|x| < \varepsilon$ et et montrons que $-\varepsilon < x < \varepsilon$

   $|x| < \varepsilon$ s'écrit, puisque $|x| = x$, $x < \varepsilon$

   or $\varepsilon > 0$ et $-\varepsilon < 0$ donc : $-\varepsilon < 0 \leqslant x < \varepsilon$

   d'où : $-\varepsilon < x < \varepsilon$

   On a donc : $|x| < \varepsilon \Rightarrow -\varepsilon < x < \varepsilon$ ☐☐

• 2e cas : $x < 0$

rappels
– pour tout $a \in \mathbb{R}$, si $a < 0$ alors $|a| = -a$
– pour tout $a \in \mathbb{R}, |-a| = |a|$

$x < 0$ donc $-x > 0$ et en utilisant le premier cas sur $(-x)$ :

$$-\varepsilon < -x < \varepsilon \Leftrightarrow |-x| < \varepsilon \ (*)$$

Or,
d'une part on a l'équivalence :

$$-\varepsilon < -x < \varepsilon \Leftrightarrow (-1) \times (-\varepsilon) > (-1) \times (-x) > (-1) \times \varepsilon$$
$$\Leftrightarrow \varepsilon > x > -\varepsilon \Leftrightarrow -\varepsilon < x < \varepsilon$$

d'autre part : $|-x| = |x|$
donc $(*)$ s'écrit : $-\varepsilon < x < \varepsilon \Leftrightarrow |x| < \varepsilon$

Conclusion
$\forall x \in \mathbb{R}$ on a l'équivalence : $-\varepsilon < x < \varepsilon \Leftrightarrow |x| < \varepsilon$
par conséquent le Lemme est démontré.

**A39 Justifier que : $567 \equiv 17\ [50]$.**

**Méthode 1**
En posant la division euclidienne de 567 par 50 on obtient :
$567 = 112 \times 50 + 7$ avec $0 \leqslant 7 < 50$
et en posant la division euclidienne de 17 par 50 on obtient :
$17 = 0 \times 50 + 17$ avec $0 \leqslant 17 < 50$
Les nombres 567 et 17 ont même reste pour la diviison euclidienne par 50 donc $\mathbf{567 \equiv 17\ [50]}$.

**Méthode 2**
Question : $50|567 - 17$ ?
On a : $567 - 17 = 550 = 11 \times 50$ donc $50|567 - 17$,
par conséquent : $\mathbf{567 \equiv 17\ [50]}$.

$P$ Pour $a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ :
▶ $\boldsymbol{a \equiv a\ [m]}$
▶ on a l'équivalence : $\boldsymbol{a \equiv b\ [m] \Leftrightarrow b \equiv a\ [m]}$
▶ on a l'implication : $\boldsymbol{a \equiv b\ [m]}$ **et** $\boldsymbol{b \equiv c\ [m] \Rightarrow a \equiv c\ [m]}$

$i$ Ces trois points sont la **réflexivité**, la **symétrie** et la **transitivité**.

▶ on a l'équivalence : $\boldsymbol{m|a \Leftrightarrow a \equiv 0\ [m]}$

Une relation de divisibilité avec diviseur positif se traduit par une congruence à zéro.

**A40 Démontrer les quatre points précédents.**
• $a - a = 0 = 0 \times m$ donc $m|a - a \Leftrightarrow a \equiv a\ [m]$
• $a \equiv b\ [m] \Leftrightarrow m|a - b \Leftrightarrow m|-(a - b) \Leftrightarrow m|b - a$
$\Leftrightarrow b \equiv a\ [m]$
• supposons $a \equiv b\ [m]$ et $b \equiv c\ [m]$
On a les équivalences :
$a \equiv b\ [m] \Leftrightarrow m|a - b$ et $b \equiv c\ [m] \Leftrightarrow m|b - c$
On a : $m|a - b$ et $m|b - c$ donc $m$ divise toute combinaison linéaire de $a - b$ et $b - c$, en particulier : $m|(a - b) + (b - c)$ c'est-à-dire $m|a - c$, autrement dit $a \equiv c\ [m]$
• on a les équivalences : $m|a \Leftrightarrow m|a - 0 \Leftrightarrow a \equiv 0\ [m]$

**A41 Déterminer les entiers relatifs $x$ tels que : $x \equiv 3\ [7]$.**

$x \equiv 3\ [7] \Leftrightarrow 7|x - 3 \Leftrightarrow \exists k \in \mathbb{Z}, x - 3 = 7k$
Or $x - 3 = 7k \Leftrightarrow x = 3 + 7k$,
donc : $x \equiv 3\ [7] \Leftrightarrow \exists k \in \mathbb{Z}, x = 3 + 7k$

$P$ Pour tous $a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}, m \in \mathbb{N} \setminus \{0\}$ on a les équivalences :
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a + c \equiv b + c\ [m]}$
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a - c \equiv b - c\ [m]}$
et on a l'**implication** :
▶ $\boldsymbol{a \equiv b\ [m] \Rightarrow a \times c \equiv b \times c\ [m]}$ c'est une **implication** !

**A42 Démontrer les trois points précédents.**

• $a \equiv b\ [m] \Leftrightarrow m|a-b \Leftrightarrow m|a+c-(b+c) \Leftrightarrow a+c \equiv b+c\ [m]$
• $a \equiv b\ [m] \Leftrightarrow m|a-b \Leftrightarrow m|a-c-(b-c) \Leftrightarrow a-c \equiv b-c\ [m]$
• Rappel $\forall (a,b) \in \mathbb{Z}^2$ on a l'implication : $a|b \Rightarrow \forall c \in \mathbb{Z}, a|bc$
$a \equiv b\ [m] \Leftrightarrow m|a-b \Rightarrow m|(a-b)\times c \Leftrightarrow m|ac-bc$
$\Leftrightarrow ac \equiv bc\ [m]$
on a donc bien l'implication : $a \equiv b\ [m] \Rightarrow ac \equiv bc\ [m]$

**A43 Justifier que : $5\times 6 \equiv 1\times 6\ [3]$ ; a-t-on « $5 \equiv 1\ [3]$ » ?**
Question : $3|5\times 6-1\times 6$ ?
On a : $5\times 6-1\times 6 = 30-6 = 24 = 3\times 8$ donc $3|5\times 6-1\times 6$,
autrement dit : $5\times 6 \equiv 1\times 6\ [3]$, mais $non(5 \equiv 1\ [3])$.
$i$ Dans une congruence il est **interdit de simplifier «en divisant»** par un même nombre, même non nul.

$P$ Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N}\setminus\{0\}$, on a les équivalences :
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow \exists k \in \mathbb{Z}, a = b+km}$

**A44 Démontrer la propriété précédente puis traduire :**
• $\boldsymbol{x \equiv 4\ [9]}$ • $\boldsymbol{\exists k \in \mathbb{Z}, y = 3+5k}$

$a \equiv b\ [m] \Leftrightarrow m|a-b \Leftrightarrow \exists k \in \mathbb{Z}, a-b = km$,
or $a-b = km \Leftrightarrow a = b+km$
donc : $a \equiv b\ [m] \Leftrightarrow \exists k \in \mathbb{Z}, a = b+km$
• $x \equiv 4\ [9] \Leftrightarrow \exists k \in \mathbb{Z}, x = 4+9k$
• $\exists k \in \mathbb{Z}, y = 3+5k \Leftrightarrow y \equiv 3\ [5]$

**A45 Déterminer les entiers relatifs $x$ tels que : $x-1 \equiv 2\ [8]$.**
**$i$ On dit aussi « Résoudre dans $\mathbb{Z}$ : $x-1 \equiv 2\ [8]$ ».**
On a les équivalences :
$x-1 \equiv 2\ [8] \Leftrightarrow x-1+1 \equiv 2+1\ [8] \Leftrightarrow x \equiv 3\ [8]$
$\Leftrightarrow \exists k \in \mathbb{Z}, x = 3+8k$
Autre solution
$x-1 \equiv 2\ [8] \Leftrightarrow 8|(x-1)-2 \Leftrightarrow 8|x-3 \Leftrightarrow x \equiv 3\ [8]$
$\Leftrightarrow \exists k \in \mathbb{Z}, x = 3+8k$

**A46 Déterminer les entiers relatifs $x$ compris entre 10 et 20 tels que : $x+3 \equiv 5\ [6]$.**
$x+3 \equiv 5\ [6] \Leftrightarrow 6|(x+3)-5 \Leftrightarrow 6|x-2 \Leftrightarrow x \equiv 2\ [6]$
$\Leftrightarrow \exists k \in \mathbb{Z}, x = 2+6k$
variante
$x+3 \equiv 5\ [6] \Leftrightarrow x+3-3 \equiv 5-3\ [6] \Leftrightarrow x \equiv 2\ [6]$
$\Leftrightarrow \exists k \in \mathbb{Z}, x = 2+6k$
Or, $x$ est compris entre 10 et 20 :
$10 \leqslant 2+6k \leqslant 20 \Leftrightarrow 10-2 \leqslant 2+6k-2 \leqslant 20-2$
$\Leftrightarrow 8 \leqslant 6k \leqslant 18 \Leftrightarrow 4 \leqslant 3k \leqslant 9$
On travaille dans $\mathbb{R}$ :
$$4 \leqslant 3k \leqslant 9 \Leftrightarrow \frac{4}{3} \leqslant \frac{3k}{3} \leqslant \frac{9}{3} \Leftrightarrow \frac{4}{3} \leqslant k \leqslant 3\ (*)$$
or $\frac{4}{3} \approx 1{,}3$ donc les seuls entiers $k$ vérifiant $(*)$ sont $k = 2$ et $k = 3$ :
• pour $k = 2$, on obtient : $x = 2+6(2) = 2+12 = 14$.
• pour $k = 3$, on obtient : $x = 2+6(3) = 2+18 = 20$.
Il y a deux nombres qui répondent à la question : **14** et **20**.

$P$ Pour tout $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $m \in \mathbb{N}\setminus\{0\}$ on a les équivalences :
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a \equiv b+km\ [m]}$
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a \equiv b-km\ [m]}$
📖 On peut ajouter/soustraire des multiples du modulo $m$ dans l'un ou l'autre des membres d'une congruence.

**A47 Démontrer le premier « ▶ »**
• **montrons que l'on a : $a \equiv b\ [m] \Rightarrow \forall k \in \mathbb{Z}, a \equiv b+km\ [m]$**
$a \equiv b\ [m]$ revient à dire $m|a-b$
On a : $m|a-b$ et $m|m$ donc $m$ divise toute combinaison linéaire de $a-b$ et $m$, en particulier : $m|1(a-b)+(-k)m$
autrement dit : $m|a-(b+km)$, c'est-à-dire : $a \equiv b+km\ [m]$
• **montrons que l'on a : $a \equiv b+km\ [m] \Rightarrow a \equiv b\ [m]$**
$a \equiv b+km\ [m] \Rightarrow a \equiv b+km+(-k)m\ [m]$ (d'après le point précédent) $\Leftrightarrow a \equiv b+km-km\ [m] \Leftrightarrow a \equiv b\ [m]$

Résumons

Pour tout $a \in \mathbb{Z}, b \in \mathbb{Z}, k \in \mathbb{Z}$, on a :

$a \equiv b\ [m] \Rightarrow a \equiv b + km\ [m]$ et $a \equiv b + km\ [m] \Rightarrow a \equiv b\ [m]$

ce qui démontre l'équivalence : $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a \equiv b + km\ [m].}$

**A48 Vérifier que : $5^2 \equiv 3^2\ [8]$; a-t-on $5 \equiv 3\ [8]$ ?**

$5^2 - 3^2 = 25 - 9 = 16 = 2 \times 8$ donc $8|5^2 - 3^2 \Leftrightarrow 5^2 \equiv 3^2\ [8]$

On a donc bien : $5^2 \equiv 3^2\ [8]$.

Mais $non(8|5-3)$ donc $non\big(5 \equiv 3\ [8]\ \big)$.

$P$ Pour tous $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ on a l'implication :
▶ $a \equiv b\ [m] \Rightarrow \forall n \in \mathbb{N}, a^n \equiv b^n\ [m]$.
Autrement dit la congruence est compatible avec l'élévation à un même exposant naturel et c'est une implication.
$i$ On convient dans le cours d'arithmétique de poser : $0^0 = 1$.

**A49** [Démonstration de la propriété précédente]
Soient $m \in \mathbb{N} \setminus \{0\}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, tels que $a \equiv b\ [m]$.
Démontrer par récurrence que : pour tout $n \in \mathbb{N}$, $a^n \equiv b^n\ [m]$.

**A50** Démontrer que : $21^{135} \equiv 1\ [4]$.

**A51** Un élève affirme « pour tout entier naturel $n$ : $7|8^n - 1$».
Sui cette affirmation est fausse en trouver un contre-exemple, sinon la démontrer.

**A52** Un élève affirme « pour tout entier naturel $n$ : $5|2^{5n} - 12^n$ ».
Si cette affirmation est fausse en trouver un contre-exemple, sinon la démontrer.

$P$ Pour $a$, $b$, $c$, $d$ entiers relatifs et $m \in \mathbb{N} \setminus \{0\}$, on a les implications :
• $a \equiv b\ [m]$ et $c \equiv d\ [m] \Rightarrow a + c \equiv b + d\ [m]$
• $a \equiv b\ [m]$ et $c \equiv d\ [m] \Rightarrow a - c \equiv b - d\ [m]$
Autrement dit on peut ajouter/soustraire membre à membre des relations de congruence de même modulo et c'est une implication.

**A53** Démontrer le premier point de la propriété précédente.

**A54** Démontrer que : $\forall n \in \mathbb{N}$, on a : $7|22^n + 15^n - 2$.

**A55** Démontrer que : $\forall n \in \mathbb{N}$, on a : $5|2^{4n} + 6^n - 2$.

$D$ Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $m \in \mathbb{N} \setminus \{0\}$ : $b$ est le **reste modulo $m$** de $a$
$\underset{déf}{\Leftrightarrow}$ le reste de la division euclidienne de $a$ par $m$ est $b$.

$P$ Pour tous $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ on a l'implication :
▶ $a \equiv b\ [m] \Rightarrow \forall n \in \mathbb{N}, a^n \equiv b^n\ [m]$.
Autrement dit la congruence est compatible avec l'élévation à un même exposant naturel et c'est une implication.
$i$ On convient dans le cours d'arithmétique de poser : $0^0 = 1$.

**A49 [Démonstration de la propriété précédente]**
**Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$.**
**Démontrer par récurrence que : pour tout $n \in \mathbb{N}$, $a^n \equiv b^n\ [m]$.**
Pour tout $n \in \mathbb{N}$ on considère la proposition $P_n$ : « $a^n \equiv b^n\ [m]$ ».
• initialisation
$a^0 - b^0 = 1 - 1 = 0$ et $m|0$ donc $m|a^0 - b^0 \Leftrightarrow a^0 \equiv b^0\ [m]$
par conséquent $P_0$ est vraie.

• hérédité
Soit $k \in \mathbb{N}$ tel que $P_k$ : « $a^k \equiv b^k\ [m]$ » est vraie (H.R.) et montrons que $P_{k+1}$ : « $a^{k+1} \equiv b^{k+1}\ [m]$ » est vraie.
L'hypothèse de récurrence s'écrit aussi : $m|a^k - b^k\ (*)$
Question : $m|a^{k+1} - b^{k+1}$ ?
On a :
$a^{k+1} - b^{k+1} = a \times a^k - a \times b^k + a \times b^k - b \times b^k$
$= a(a^k - b^k) + (a - b) \times b^k = a(a^k - b^k) + b^k(a - b)$
Or, $m|a^k - b^k\ (*)$ et $m|a - b$ donc $m$ divise toute combinaison linéaire de $a^k - b^k$ et $a - b$, en particulier :
$m|a(a^k - b^k) + b^k(a - b)$ autrement dit : $m|a^{k+1} - b^{k+1}$
ce qui s'écrit aussi : $a^{k+1} \equiv b^{k+1}\ [m]$ donc $P_{k+1}$ est vraie.

Conclusion
Il résulte des deux points précédents et du principe de récurrence que : $\forall n \in \mathbb{N}$, $P_n$ est vraie, autrement dit : $\forall n \in \mathbb{N}, a^n \equiv b^n\ [m]$.

**A50 Démontrer que : $21^{135} \equiv 1\ [4]$.**
$21 \equiv 1\ [4]$ donc $21^{135} \equiv 1^{135}\ [4]$, or $1^{135} = 1\ [4]$
donc : $\mathbf{21^{135} \equiv 1\ [4]}$.

**A51 Un élève affirme « pour tout entier naturel $n$ : $7|8^n-1$». Si cette affirmation est fausse en trouver un contre-exemple, sinon la démontrer.**

Soit $n \in \mathbb{N}$.

On a : $8 \equiv 1\ [7]$ donc $8^n \equiv 1^n\ [7]$, or $1^n = 1$

donc $8^n \equiv 1\ [7]$ autrement dit : $7|8^n-1$.

Conclusion : **pour tout $n \in \mathbb{N}$, $7|8^n-1$.**

**A52 Un élève affirme « pour tout entier naturel $n$ : $5|2^{5n}-12^n$ ». Si cette affirmation est fausse en trouver un contre-exemple, sinon la démontrer.**

Soit $n \in \mathbb{N}$.

Remarquons d'abord que : $32-12=20=4\times 5$ donc $5|32-12$ autrement dit : $32 \equiv 12\ [5]$.

On a : $32 \equiv 12\ [5]$ donc $32^n \equiv 12^n\ [5] \Leftrightarrow (2^5)^n \equiv 12^n\ [5]$

$\Leftrightarrow 2^{5n} \equiv 12^n\ [5] \Leftrightarrow 5|2^{5n}-12^n$

Conclusion : $\forall n \in \mathbb{N}$, $5|2^{5n}-12^n$.

$P$ Pour $a, b, c, d$ entiers relatifs et $m \in \mathbb{N}\setminus\{0\}$, on a les implications :

- $a \equiv b\ [m]$ et $c \equiv d\ [m] \Rightarrow a+c \equiv b+d\ [m]$
- $a \equiv b\ [m]$ et $c \equiv d\ [m] \Rightarrow a-c \equiv b-d\ [m]$

Autrement dit on peut ajouter/soustraire membre à membre des relations de congruence de même modulo et c'est une implication.

**A53 Démontrer le premier point de la propriété précédente.**

Soient $a, b, c, d$ des entiers relatifs et $m \in \mathbb{N}\setminus\{0\}$ tels que $a \equiv b\ [m]$ et $c \equiv d\ [m]$.

On a d'une part : $a \equiv b\ [m]$, autrement dit : $m|a-b$

et d'autre part on a : $c \equiv d\ [m]$, autrement dit : $m|c-d$

On a : $m|a-b$ et $m|c-d$ donc $m$ divise toute combinaison linéaire de $a-b$ et $c-d$, en particulier $m|(a-b)+(c-d)$

$\Leftrightarrow m|a-b+c-d \Leftrightarrow m|a+c-(b+d) \Leftrightarrow a+c \equiv b+d\ [m]$

On montrerait de même que $a-c \equiv b-d\ [m]$.

**A54 Démontrer que : $\forall n \in \mathbb{N}$, on a : $7|22^n+15^n-2$.**

Soit $n \in \mathbb{N}$.

On a : $22 \equiv 1\ [7]$ donc $22^n \equiv 1^n\ [7]$, or $1^n = 1$,

donc : $22^n \equiv 1\ [7]$.

De même : $15 \equiv 1\ [7]$ donc $15^n \equiv 1^n\ [7]$ autrement dit : $15^n \equiv 1\ [7]$

On a : $22^n \equiv 1\ [7]$ et $15^n \equiv 1\ [7]$ donc par somme membre à membre : $22^n+15^n \equiv 1+1\ [7] \Leftrightarrow 22^n+15^n \equiv 2\ [7]$

$\Leftrightarrow 7|22^n+15^n-2$.

Conclusion : $\forall n \in \mathbb{N}$, $7|22^n+15^n-2$.

**A55 Démontrer que : $\forall n \in \mathbb{N}$ : $5|2^{4n}+6^n-2$.**

Soit $n \in \mathbb{N}$.

On a : $16 \equiv 1\ [5]$ donc $16^n \equiv 1^n\ [5]$ autrement dit : $16^n \equiv 1\ [5]$.

De même : $6 \equiv 1\ [5]$ donc $6^n \equiv 1^n\ [5] \Leftrightarrow 6^n \equiv 1\ [5]$.

On a $16^n \equiv 1\ [5]$ et $6^n \equiv 1\ [5]$ donc par somme membre à membre :

$16^n+6^n \equiv 1+1\ [5] \Leftrightarrow 16^n+6^n \equiv 2\ [5] \Leftrightarrow 5|16^n+6^n-2$

Or $16^n=(2^4)^n=2^{4\times n}=2^{4n}$ donc $5|2^{4n}+6^n-2$.

Conclusion : $\forall n \in \mathbb{N}$, $5|2^{4n}+6^n-2$.

$D$ Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $m \in \mathbb{N}\setminus\{0\}$, alors :

$b$ est le reste modulo $m$ de $a \overset{déf}{\Leftrightarrow}$ le reste de la division euclidienne de $a$ par $m$ est $b$.

$P$ Pour tous $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ on a l'équivalence :
$b$ est le reste modulo $m$ de $a \Leftrightarrow a \equiv b\ [m]$ et $0 \leqslant b < m$

**A56** Déterminer le reste modulo 6 de $17^{213}$.

**A57** Vérifier que $4 \equiv 1\ [3]$ ; a-t-on : $2^4 \equiv 2^1\ [3]$ ?

$i$ Rappel si $a \equiv b\ [m]$ alors pour tout $n \in \mathbb{N}$, $a^n \equiv b^n\ [m]$
si $p \equiv q\ [m]$ très souvent : $a^p \not\equiv a^q\ [m]$.

**A58** Déterminer le reste modulo 5 de $7^{143}$.

**A59** Déterminer le reste modulo 6 de $19^{123}$.

**A60** Déterminer le reste modulo 9 de $13^{208}$.

**A61** Déterminer le reste modulo 3 de $11^{157}$.

**A62** Déterminer le reste modulo 11 de $7^{152}$.

**A63** Démontrer que : $\forall n \in \mathbb{N}$, on a : $7|8^n + 15^n - 2$.

**A64** Démontrer que : $\forall n \in \mathbb{N}$ : $5|2^{4n} + 6^n - 2$.

D Soit $m \in \mathbb{N} \setminus \{0\}$, $a \in \mathbb{Z}$ est **inversible modulo $m$** $\overset{déf}{\Leftrightarrow}$ il existe $b \in \mathbb{Z}$ tel que : $a \times b \equiv 1\ [m]$ ou encore : $b \times a \equiv 1\ [m]$.

**A65** Donner un inverse de 7 modulo 5, en trouver un deuxième.

**A66** Soit $b$ un inverse de $a$ modulo $m$ : montrer que pour tout entier relatif $k$ : $b + km$ est un inverse de $a$ modulo $m$.

**A67** Montrer que 4 n'admet pas d'inverse modulo 6.

Un entier relatif $a$ n'admet pas toujours d'inverse modulo $m$, et lorsqu'il en admet il n'est pas unique.

**A68** Résoudre dans $\mathbb{Z}$ l'équation $(E) : 5x \equiv 2\ [3]$.

$P$ Pour tous $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ on a l'équivalence :
$b$ est le reste modulo $m$ de $a \Leftrightarrow a \equiv b\ [m]$ et $0 \leqslant b < m$

**A56 Déterminer le reste modulo 6 de $17^{213}$.**
On a : $17 \equiv 17 - 3 \times 6 \equiv -1\ [6]$ donc $17^{213} \equiv (-1)^{213}\ [6]$
Or $(-1)^{213} = -1$ donc $17^{213} \equiv -1 \equiv -1 + 6 \equiv 5\ [6]$
$5^{213} \equiv 5\ [6]$ et $0 \leqslant 5 < 6$ donc **le reste modulo 6 de $5^{213}$ est 5**.

**A57 Vérifier que $4 \equiv 1\ [3]$ ; a-t-on : $2^4 \equiv 2^1\ [3]$.**
$3|4 - 1$ autrement dit : $4 \equiv 1\ [3]$
$2^4 - 2^1 = 16 - 2 = 14$ et $non(3|14)$ donc $2^4 \not\equiv 2^1\ [3]$.

$i$ Rappel si $a \equiv b\ [m]$ alors pour tout $n \in \mathbb{N}$, $a^n \equiv b^n\ [m]$
si $p \equiv q\ [m]$ très souvent : $a^p \not\equiv a^q\ [m]$.

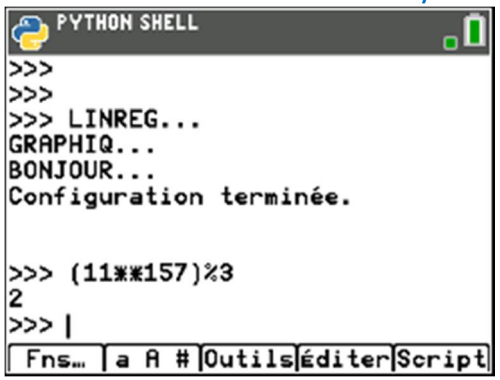
**A58 Déterminer le reste modulo 5 de $7^{143}$.**
$7 \equiv 2\ [5]$
$7^2 \equiv 49 \equiv 49 - 10 \times 5 \equiv -1\ [5]$
En posant la division euclidienne de 143 par 2 : $143 = 71 \times 2 + 1$.
$7^{143} = 7^{71 \times 2 + 1} = 7^{71 \times 2} \times 7^1 = (7^2)^{71} \times 7 \equiv (-1)^{71} \times 2 \equiv -2$
$\equiv -2 + 5 \equiv 3\ [5]$
$7^{143} \equiv 3\ [5]$ et $0 \leqslant 3 < 5$ donc le reste modulo 5 de $7^{143}$ est **3**.

**A59 Déterminer le reste modulo 6 de $19^{123}$.**
On a : $19 \equiv 19 - 3 \times 6 \equiv 1\ [6]$ donc $19^{123} \equiv 1^{123} \equiv 1\ [6]$
$19^{123} \equiv 1\ [6]$ et $0 \leqslant 1 < 6$ donc le reste modulo 6 de $19^{123}$ est **1**.

**A60 Déterminer le reste modulo 9 de $13^{208}$.**
$13 \equiv 4\ [9]$
$13^2 \equiv 4^2 \equiv 16 \equiv 16 - 9 \equiv 7\ [9]$
$13^3 \equiv 13^2 \times 13 \equiv 7 \times 4 \equiv (-2) \times 4 \equiv -8 \equiv 1\ [9]$
La division euclidienne de 208 par 3 donne : $208 = 69 \times 3 + 1$
$13^{208} = 13^{69 \times 3 + 1} = (13^3)^{69} \times 13^1 \equiv 1^{69} \times 4 \equiv 4\ [9]$
On a : $13^{208} \equiv 4\ [9]$ et $0 \leqslant 4 < 9$ donc le reste modulo 9 de $13^{208}$ est 4.

**A61 Déterminer le reste modulo 3 de $11^{157}$.**

On a : $11 \equiv 11 - 4 \times 3 \equiv 11 - 12 \equiv -1\ [3]$
Donc : $11^{157} \equiv (-1)^{157} \equiv -1 \equiv -1 + 3 \equiv 2\ [3]$
On a : $11^{157} \equiv 2\ [3]$ avec $0 \leqslant 2 < 3$ donc le reste modulo 3 de $11^{157}$ est $\mathbf{2}$.
Vérification à la calculatrice Python :




**A62 Déterminer le reste modulo 11 de $7^{152}$.**

On a :
$7 \equiv 7\ [11]$
$7^2 = 49 \equiv 49 - 4 \times 11 \equiv 5\ [11]$
$7^3 = 7^2 \times 7 \equiv 5 \times 7 \equiv 35 \equiv 35 - 3 \times 11 \equiv 2\ [11]$
$7^4 = (7^2)^2 \equiv 5^2 \equiv 25 \equiv 25 - 2 \times 11 \equiv 3\ [11]$
$7^5 = 7^2 \times 7^3 \equiv 5 \times 2 \equiv 10 \equiv 10 - 11 \equiv -1\ [11]$
La division euclidienne de 152 par 5 donne : $152 = 30 \times 5 + 2$.
$7^{152} = 7^{30\times5+2} = (7^5)^{30} \times 7^2 \equiv (-1)^{30} \times 5 \equiv 1 \times 5 \equiv 5\ [11]$
$7^{152} \equiv 5\ [11]$ et $0 \leqslant 5 < 11$ donc le reste modulo 11 de $7^{152}$ est $\mathbf{5}$.

**A63 Démontrer que : $\forall n \in \mathbb{N}$, on a : $7|8^n + 15^n - 2$**

Soit $n \in \mathbb{N}$.
On a : $8 \equiv 1\ [7]$ et $15 \equiv 1\ [7]$, donc :
$$8^n + 15^n - 2 \equiv 1^n + 1^n - 2 \equiv 1 + 1 - 2 \equiv 0\ [7]$$
On a : $8^n + 15^n - 2 \equiv 0\ [7]$, autrement dit : $7|8^n + 15^n - 2$.

Conclusion : $\forall n \in \mathbb{N}, 7|8^n + 15^n - 2$.

**A64 Démontrer que : $\forall n \in \mathbb{N} : 5|2^{4n} + 6^n - 2$.**

Soit $n \in \mathbb{N}$.
Remarquons que : $16 \equiv 1\ [5]$ et $6 \equiv 1\ [5]$
On a :
$2^{4n} + 6^n = (2^4)^n + 6^n = 16^n + 6^n \equiv 1^n + 1^n \equiv 1 + 1 \equiv 2\ [5]$
On a : $2^{4n} + 6^n \equiv 2\ [5]$, autrement dit : $5|2^{4n} + 6^n - 2$.
Conclusion : $\forall n \in \mathbb{N}, 5|2^{4n} + 6^n - 2$.

**A65 Donner un inverse de 7 modulo 5, en trouver un deuxième.**

On a :
$7 \times 1 = 7 \equiv 2\ [5]$
$7 \times 2 = 14 \equiv 4\ [5]$
$7 \times 3 = 21 \equiv 1\ [5]$
On a : $7 \times 3 \equiv 1\ [5]$ donc 3 est un inverse de 7 modulo 5.
… et 7 est un inverse de 3 modulo 5 mais ce n'est ici la question !
D'autre part : $8 \times 7 \equiv 3 \times 2 \equiv 6 \equiv 1\ [5]$
On a : $11 \times 7 \equiv 1\ [5]$ donc 11 est aussi un inverse de 7 modulo 5.

**A66 Soit $b$ un inverse de $a$ modulo $m$ : montrer que pour tout entier relatif $k$, $b + km$ est un inverse de $a$ modulo $m$.**

Soit $b$ un inverse de $a$ modulo $m$ : $b \times a \equiv 1\ [m]$.
Soit $k \in \mathbb{Z}$, on a :
$(b + km)a = ba + kma \equiv ba + kma - ka \times m \equiv b \times a \equiv 1\ [m]$
Résumons : $(b + km) \times a \equiv 1\ [m]$ donc $b + km$ est un inverse de $a$ modulo $m$.

Un entier relatif a n'admet pas toujours d'inverse modulo $m$, et lorsqu'il en admet un il n'est pas unique.

**A67 Montrer que 4 n'admet pas d'inverse modulo 6.**

On va montrer par disjonction de cas suivant le reste modulo 3 de $n$ que $n \times 4 \not\equiv 1\ [6]$.
- $n \equiv 0\ [6] : n \times 4 \equiv 0 \times 4 \equiv 0 \not\equiv 1\ [6]$
- $n \equiv 1\ [6] : n \times 4 \equiv 1 \times 4 \equiv 4 \not\equiv 1\ [6]$
- $n \equiv 2\ [6] : n \times 4 \equiv 2 \times 4 \equiv 8 \equiv 2 \not\equiv 1\ [6]$

• $n \equiv 3\ [6] : n \times 4 \equiv 3 \times 4 \equiv 12 \equiv 12 - 2 \times 6 \equiv 0 \not\equiv 1\ [6]$
• $n \equiv 4\ [6] : n \times 4 \equiv 4 \times 4 \equiv 16 \equiv 16 - 2 \times 6 \equiv 4 \not\equiv 1\ [6]$
• $n \equiv 5\ [6] : n \times 4 \equiv 5 \times 4 \equiv 20 \equiv 20 - 3 \times 6 \equiv 2 \not\equiv 1\ [6]$

Conclusion

Pour tout $n \in \mathbb{Z}$, $n \times 4 \not\equiv 1\ [6]$ donc il n'existe pas $n \in \mathbb{Z}$ tel que $n \times 4 \equiv 1\ [6]$ autrement dit $4$ n'a pas d'inverse modulo $6$.

Autre présentation

Tableau de congruence **modulo 6**

| $n \equiv$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ |
|---|---|---|---|---|---|---|
| $n \times 4 \equiv$ | $0 \times 4$ $\equiv \mathbf{0}$ | $1 \times 4$ $\equiv \mathbf{4}$ | $2 \times 4$ $\equiv 8$ $\equiv \mathbf{2}$ | $3 \times 4$ $\equiv 12$ $\equiv \mathbf{0}$ | $4 \times 4$ $\equiv (-2) \times (-2)$ $\equiv \mathbf{4}$ | $5 \times 4$ $\equiv (-1) \times 4$ $\equiv -4$ $\equiv \mathbf{2}$ |

Par disjonction de cas on déduit de la dernière ligne de ce tableau que, pour tout $n \in \mathbb{Z}$, $n \times 4 \not\equiv 1\ [6]$ donc il n'existe pas $n \in \mathbb{Z}$ tel que $n \times 4 \equiv 1\ [6]$ autrement dit **$4$ n'a pas d'inverse modulo $6$**.

**A68 Résoudre dans $\mathbb{Z}$ l'équation $(E)$ : $5x \equiv 2\ [3]$.**

Méthode 1 (déconseillée)

On souhaite faire disparaître $5$ pour se ramener à une équation de la forme $x \equiv \cdots\ [3]$, on va multiplier chaque membre par un inverse de $5$ modulo $3$.

Analyse

$1 \times 5 = 5 \equiv 2\ [3]$
$2 \times 5 = 10 \equiv 10 - 3 \times 3 \equiv 1\ [3]$
On a : $2 \times 5 \equiv 1\ [3]$ donc $2$ est un inverse de $5$ modulo $3$.
On a :
$5x \equiv 11\ [3] \Rightarrow 2 \times 5x \equiv 2 \times 11\ [3] \Leftrightarrow 2 \times 5 \times x \equiv 22\ [3]$
$\Leftrightarrow 1x \equiv 22 - 7 \times 3\ [3] \Leftrightarrow x \equiv 1\ [3]$
Les candidats sont les nombres $x \in \mathbb{Z}$ tels que : $x \equiv 1\ [3]$.

Synthèse

Soit $x$ tel que : $x \equiv 1\ [3]$, alors $5 \times x \equiv 5 \times 1\ [3]$
$\Leftrightarrow 5x \equiv 5 - 3\ [3] \Leftrightarrow 5x \equiv 2\ [3]$ donc $x$ est accepté

Conclusion

Les solutions de $(E)$ sont les nombres $x \in \mathbb{Z}$ tel que $x \equiv 1\ [3]$.
Remarque : ce sont les entiers relatifs de la forme $1 + 3k$, $k \in \mathbb{Z}$.

Méthode 2 (très fortement conseillée)

Tableau de congruence **modulo 3**

| $x \equiv \cdots$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $5x \equiv \cdots$ | $5 \times 0$ $\equiv 0$ | $5(1)$ $\equiv 5$ $\equiv 5 - 3$ $\equiv 2$ | $5(2)$ $\equiv 10$ $\equiv 10 - 3(3)$ $\equiv 1$ |

Par disjonctions de cas la dernière ligne de ce tableau montre l'équivalence : $5x \equiv 2\ [3] \Leftrightarrow \boldsymbol{x \equiv 2\ [3]}$.