BURHAN

# Arithmétique dans $\mathbb{Z}$

1ère Année Baccalauréat · Sciences Mathématiques · Mathématiques

Version en ligne : burhan.ma/1bac/sciences-mathematiques/mathematiques/arithmetique-dans-z/cours

| Chapitre | Semestre |
| --- | --- |
| Arithmétique dans $\mathbb{Z}$ | Semestre 2 |

## Pourquoi l'arithmétique

Aujourd'hui, nous sommes lundi. Quel jour de la semaine serons-nous dans $2^{50}$ jours ?

Ce nombre a seize chiffres : $2^{50} = 1125899906842624$. Compter les jours un par un est hors de question.

Pourtant, la réponse tient en quelques lignes de calcul. Tu la trouveras toi-même avant la fin du chapitre.

**Devine : Une prédiction**

Les jours de la semaine reviennent tous les $7$ jours. Pour trouver le jour cherché, de quoi a-t-on besoin ?

**A.** De l'écriture complète de $2^{50}$, chiffre par chiffre.

**Faux.**

Elle ne suffit pas : il faudrait encore la diviser par $7$. Et on peut s'en passer.

**B.** Du reste de la division de $2^{50}$ par $7$.

**Juste.**

Juste : sept jours plus tard, on retombe sur le même jour. Seul ce reste compte.

**C.** De la parité de $2^{50}$, qui est pair.

**Faux.**

La parité ne dit rien des semaines : dans $14$ jours et dans $16$ jours, on ne sera pas le même jour.

**D.** Du dernier chiffre de $2^{50}$, qui est $4$.

**Faux.**

Le dernier chiffre renseigne sur la division par $10$. Or $4$ et $14$ finissent par $4$, et ne tombent pas le même jour.

**Correction**

Tous les $7$ jours, on retombe sur le même jour de la semaine.

Si $2^{50} = 7q + r$ avec $0 \leq r < 7$, le jour cherché est lundi plus $r$ jours. Il suffit donc de connaître le reste $r$.

Les congruences le donneront sans jamais écrire $2^{50}$.

Dans ce chapitre, tu prolonges aux entiers relatifs l'arithmétique vue au tronc commun.

Tu sauras écrire une division euclidienne et raisonner selon les restes. Tu sauras reconnaître un nombre premier, décomposer un entier, calculer un PGCD et un PPCM.

Tu calculeras avec les congruences, puis dans $\mathbb{Z}/n\mathbb{Z}$. Et surtout, tu sauras **démontrer** ces résultats.

## Divisibilité dans $\mathbb{Z}$

### Multiples et diviseurs dans $\mathbb{Z}$

**Devine : Compter des diviseurs**

Dans $\mathbb{N}$, $3$ divise $12$ car $12 = 3 \times 4$. Dans $\mathbb{Z}$, on garde la même idée avec des entiers relatifs : $-12 = 3 \times (-4)$, donc $3$ divise aussi $-12$.

Combien l'entier $-6$ a-t-il de diviseurs dans $\mathbb{Z}$ ?

**A.** $4$ : $1$, $2$, $3$ et $6$.

**Faux.**

Ce sont ses diviseurs positifs. Dans $\mathbb{Z}$, leurs opposés le divisent aussi : $-6 = (-1) \times 6$.

**B.** Aucun, car $-6$ est négatif.

**Faux.**

Un entier négatif a des diviseurs : $-6 = 2 \times (-3)$, donc $2$ divise $-6$.

**C.** $8$ : $\pm 1$, $\pm 2$, $\pm 3$ et $\pm 6$.

**Juste.**

Juste : chaque diviseur positif vient avec son opposé.

**D.** Une infinité, comme $0$.

**Faux.**

Seul $0$ a une infinité de diviseurs. Tu le montreras bientôt : un diviseur de $-6$ est compris entre $-6$ et $6$.

**Correction**

Les diviseurs positifs de $6$ sont $1$, $2$, $3$ et $6$.

Si $-6 = ka$, alors aussi $-6 = (-k)(-a)$ : l'opposé d'un diviseur est un diviseur.

Les diviseurs de $-6$ dans $\mathbb{Z}$ sont donc $-6$, $-3$, $-2$, $-1$, $1$, $2$, $3$ et $6$ : il y en a $8$.

**Définition : Divisibilité dans $\mathbb{Z}$**

Soient $a$ et $b$ deux entiers relatifs. On dit que $a$ **divise** $b$, et on note $a \mid b$, s'il existe un entier relatif $k$ tel que $b = ka$.

On dit aussi que $a$ est un **diviseur** de $b$, et que $b$ est un **multiple** de $a$. Lorsque $a$ ne divise pas $b$, on note $a \nmid b$.

**Exemple : lire la définition**

- $-5 \mid 35$, car $35 = (-7) \times (-5)$.
- $4 \nmid 18$ : $4 \times 4 = 16$ et $4 \times 5 = 20$, donc aucun entier $k$ ne vérifie $18 = 4k$.
- $7 \mid 0$, car $0 = 0 \times 7$ : tout entier divise $0$.
- $0 \nmid 5$, car $k \times 0 = 0 \neq 5$ pour tout entier $k$ : $0$ ne divise que $0$.

## Transitivité et combinaisons

Prends $7$, qui divise $21$ et $35$. Il divise aussi leur somme, et une combinaison des deux :

$$21 + 35 = 56 = 7 \times 8,$$
$$3 \times 21 - 2 \times 35 = -7 = 7 \times (-1).$$

**Pourquoi est-ce vrai ?** On met $7$ en facteur :

$$3 \times 21 - 2 \times 35$$
$$= 7 \times (3 \times 3 - 2 \times 5).$$

Ce calcul marche pour toute combinaison.

**Propriété : Transitivité et combinaisons linéaires**

Soient $a$, $b$ et $c$ des entiers relatifs.

1. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
2. Si $a \mid b$ et $a \mid c$, alors pour tous entiers relatifs $u$ et $v$, on a $a \mid bu + cv$.

---

**Démonstration**

**Étape 1 (transitivité).** Par hypothèse, il existe des entiers relatifs $k$ et $k'$ tels que $b = ka$ et $c = k'b$. Donc $c = k'(ka) = (k'k)a$, et $k'k$ est un entier relatif : ainsi $a \mid c$ (définition de la divisibilité).

**Étape 2 (combinaisons).** Par hypothèse, il existe des entiers relatifs $k$ et $k'$ tels que $b = ka$ et $c = k'a$. Soient $u$ et $v$ deux entiers relatifs. Alors $bu + cv = (ku + k'v)a$, et $ku + k'v$ est un entier relatif. Donc $a \mid bu + cv$ (définition de la divisibilité).

**À retenir : Retenir de la preuve : mettre en facteur**

Pour prouver que $a$ divise un nombre, on écrit ce nombre sous la forme $a \times k$, avec $k$ entier : on **met $a$ en facteur**.

Dans une combinaison $bu + cv$, les entiers $u$ et $v$ sont libres. On les choisit pour faire disparaître ce qui gêne.

**Vérifie : Le pas clé**

Dans l'étape 2 de la preuve, $b = ka$ et $c = k'a$. Qu'est-ce qui permet de conclure que $a \mid bu + cv$ ?

**A.** L'égalité $bu + cv = (ku + k'v)a$, avec $ku + k'v$ entier.

**Juste.**

Juste : c'est exactement la définition de la divisibilité.

**B.** Le calcul de $\dfrac{bu + cv}{a}$, qui est un nombre.

**Faux.**

Ce quotient n'existe que si $a \neq 0$, et il faudrait encore montrer qu'il est entier.

**C.** La transitivité, avec $a \mid b$ et $b \mid bu + cv$.

**Faux.**

« $b \mid bu + cv$ » est faux en général : avec $b = 2$, $c = 3$, $u = 0$ et $v = 1$, on a $2 \nmid 3$.

**D.** Le fait que $a$ divise les entiers $u$ et $v$.

**Faux.**

Rien n'est supposé sur $u$ et $v$ : ce sont des entiers quelconques.

**Correction**

Par hypothèse, $b = ka$ et $c = k'a$. Donc

$$\begin{aligned} bu + cv &= kau + k'av \\ &= (ku + k'v)a. \end{aligned}$$

Le nombre $ku + k'v$ est un entier relatif, car $k$, $k'$, $u$ et $v$ en sont.

**Conclusion.** Par définition de la divisibilité, $a \mid bu + cv$.

## Éliminer une inconnue

**Exemple : faire disparaître n**

Soient $n$ un entier relatif et $d$ un diviseur commun de $n + 2$ et de $3n + 1$. On choisit $u = 3$ et $v = -1$ :

$$3(n + 2) - (3n + 1) = 5.$$

D'après les propriétés de la divisibilité, $d$ divise $5$. Ainsi $d$ vaut $-5$, $-1$, $1$ ou $5$.

Pour $n = 3$, on obtient $5$ et $10$ : le diviseur commun $5$ est atteint.

**Méthode : montrer qu'un entier en divise un autre**

1. **Par la définition** : écris $b = ka$, en donnant l'entier $k$ explicitement.

2. **Par une combinaison** : si $a$ divise deux nombres, il divise $bu + cv$ ; choisis $u$ et $v$ pour éliminer l'inconnue.
3. **Pour une expression en** $n$ : factorise, ou raisonne par récurrence.
4. **Conclus** en nommant la propriété employée.

Exemple **: Exemple guidé : une divisibilité par récurrence**

**Petit rappel.** Une récurrence prouve $P(0)$, puis « $P(n)$ vraie entraîne $P(n+1)$ vraie » : alors $P(n)$ est vraie pour tout $n$.

**Énoncé.** Pour tout entier $n \geq 0$, $P(n)$ : « $7 \mid 8^n - 1$ ».

**Initialisation.** $8^0 - 1 = 0 = 7 \times 0$ : $P(0)$ est vraie.

**Hérédité.** Soit $n \geq 0$ un entier tel que $P(n)$ soit vraie. On écrit

$$\begin{aligned} 8^{n+1} - 1 &= 8 \times 8^n - 8 + 7 \\ &= 8(8^n - 1) + 7. \end{aligned}$$

D'après l'hypothèse de récurrence, 7 divise $8^n - 1$ ; il divise aussi 7. Par combinaison, $7 \mid 8^{n+1} - 1$ : c'est $P(n+1)$.

**Conclusion.** D'après le principe de récurrence, $P(n)$ est vraie pour tout entier $n \geq 0$.

## Piège et entraînement

Attention **: « divise » n'est pas une division**

✗ « $3 \mid 12 = 4$ ».

✓ $3 \mid 12$ est une **proposition** : elle est vraie ou fausse. Le nombre $4$ est le quotient $\frac{12}{3}$. On écrit : « $3 \mid 12$, car $12 = 4 \times 3$ ».

De même, $12 \mid 3$ est une proposition fausse, et non le nombre $\frac{3}{12}$.

**À toi : Un diviseur commun**

Soit $n$ un entier relatif. Montre que tout diviseur commun de $n+4$ et de $2n+5$ divise 3. Pour $n = 5$, donne les diviseurs communs positifs de ces deux nombres. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Cherche des entiers $u$ et $v$ qui font disparaître $n$ dans $u(n+4) + v(2n+5)$.
**Indice 2**
Le coefficient de $n$ est le même dans $2(n+4)$ et dans $2n+5$.

**Indice 3**

Point délicat : pour $n = 5$, liste les diviseurs positifs de chacun des deux nombres avant de les comparer.

**Réponse**

**Combinaison.** Soit $d$ un diviseur commun de $n + 4$ et de $2n + 5$. On élimine $n$ :

$$2(n + 4) - (2n + 5) = 3.$$

D'après les propriétés de la divisibilité, $d$ divise $3$.

**Cas $n = 5$.** On a $n + 4 = 9$ et $2n + 5 = 15$. Les diviseurs positifs de $9$ sont $1$, $3$ et $9$ ; ceux de $15$ sont $1$, $3$, $5$ et $15$.

**Conclusion.** Tout diviseur commun de $n + 4$ et de $2n + 5$ divise $3$. Pour $n = 5$, les diviseurs communs positifs sont $1$ et $3$ : ils divisent bien $3$.

## Valeur absolue et division euclidienne

## Comparer les valeurs absolues

**Devine : Diviseur et multiple**

Les diviseurs positifs de $15$ sont $1$, $3$, $5$ et $15$ : aucun ne dépasse $15$. Soit $a$ un entier relatif tel que $a \mid 15$ et $15 \mid a$. Que peut valoir $a$ ?

**A.** Seulement $15$.

**Faux.**

Pense aux négatifs : $15 = (-1) \times (-15)$ et $-15 = (-1) \times 15$, donc $-15$ convient aussi.

**B.** N'importe quel diviseur de $15$.

**Faux.**

Pour $a = 3$, $15$ ne divise pas $3$ : la seconde condition échoue.

**C.** $1$ ou $15$.

**Faux.**

Pour $a = 1$, « $15 \mid 1$ » est fausse : aucun entier $k$ ne vérifie $1 = 15k$.

**D.** $15$ ou $-15$.

**Juste.**

Juste : ces deux valeurs conviennent, et ce sont les seules.

**Correction**

Les valeurs $15$ et $-15$ conviennent, et ce sont les seules.

Comme $a \mid 15$, la valeur absolue de $a$ est au plus $15$ ; comme $15 \mid a$, elle est au moins $15$. Donc $|a| = 15$.

**Pourquoi est-ce vrai ?** Si $b = ka$ avec $b \neq 0$, l'entier $k$ n'est pas nul, donc $|k| \geq 1$. Multiplier par $k$ ne fait pas diminuer la valeur absolue.

**Propriété : Divisibilité et valeur absolue**

Soient $a$ et $b$ deux entiers relatifs.

1. Si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$.
2. Si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$.

**Démonstration**

**Étape 1.** Supposons $a \mid b$ et $b \neq 0$. Il existe un entier relatif $k$ tel que $b = ka$. Comme $b \neq 0$, on a $k \neq 0$, donc $|k| \geq 1$ car $k$ est un entier. Ainsi $|b| = |k|\,|a| \geq |a|$.

**Étape 2.** Supposons $a \mid b$ et $b \mid a$. Si $b = 0$, alors $a$, multiple de $b$, est nul : $a = b$. Si $b \neq 0$, alors $a \neq 0$, car $b$ est un multiple de $a$. L'étape 1 donne $|a| \leq |b|$ et, en échangeant les rôles de $a$ et $b$, $|b| \leq |a|$. Donc $|a| = |b|$, c'est-à-dire $a = b$ ou $a = -b$.

**À retenir : Retenir de la preuve : comparer les valeurs absolues**

Un entier non nul $k$ vérifie $|k| \geq 1$ : c'est tout le ressort de la preuve.

Retiens le réflexe : pour **borner** un diviseur, compare les valeurs absolues. Et deux entiers qui se divisent l'un l'autre sont égaux ou opposés.

**Vérifie : Une hypothèse utile**

Dans l'étape 1 de la preuve, à quoi sert l'hypothèse $b \neq 0$ ?

**A.** À garantir que $b$ est positif.
**Faux.**
Rien n'impose le signe de $b$ : la preuve travaille avec $|b|$.

**B.** À garantir $k \neq 0$, donc $|k| \geq 1$.
**Juste.**
Juste : $b = ka$ avec $b \neq 0$ interdit $k = 0$.

**C.** À pouvoir diviser $b$ par $a$.
**Faux.**
La preuve ne divise jamais : elle écrit $b = ka$ et compare des valeurs absolues.

**D.** À rien : l'inégalité reste vraie si $b = 0$.
**Faux.**
Pour $b = 0$ et $a = 7$, on a $7 \mid 0$, mais $|7| > |0|$.

**Correction**

Si $b \neq 0$, l'égalité $b = ka$ interdit $k = 0$. Un entier non nul vérifie $|k| \geq 1$, d'où

$$|b| = |k|\,|a| \geq |a|.$$

Sans cette hypothèse, $k$ pourrait être nul.

**Exemple : Contre-exemple : l'hypothèse b non nul est nécessaire**

Avec $b = 0$, la comparaison échoue. Par exemple, $100 \mid 0$, car $0 = 0 \times 100$, et pourtant $|100| > |0|$.

L'entier $0$ a des diviseurs aussi grands qu'on veut : c'est le seul entier dans ce cas.

## La division euclidienne

On range $47$ œufs dans des boîtes de $6$. On remplit $7$ boîtes, et il reste $5$ œufs :

$$47 = 6 \times 7 + 5,$$

avec $0 \leq 5 < 6$. Pour un dividende négatif, on garde un reste positif :

$$-47 = 6 \times (-8) + 1,$$

avec $0 \leq 1 < 6$.

**Pourquoi est-ce vrai ?** Pour $47$ et $6$, retire $6$ autant de fois que possible : $47, 41, 35, \ldots, 11, 5$. On s'arrête à $5$, car un pas de plus donnerait un nombre négatif. Ce plus petit nombre positif ou nul est le reste.

**Théorème : Division euclidienne dans $\mathbb{Z}$**

Soient $a$ un entier relatif et $b$ un entier naturel non nul. Il existe un unique couple $(q, r)$ d'entiers relatifs tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

L'entier $q$ est le **quotient** et $r$ le **reste** de la division euclidienne de $a$ par $b$. De plus, $b \mid a$ si et seulement si $r = 0$.

---

**Démonstration**

**Étape 1 (existence).** Les entiers $a - bk$, pour $k \in \mathbb{Z}$, qui sont positifs ou nuls forment une partie non vide de $\mathbb{N}$ : pour $k = -|a|$, $a - bk = a + b|a| \geq a + |a| \geq 0$. Elle admet un plus petit élément $r = a - bq$ (propriété de $\mathbb{N}$, admise). Si l'on avait $r \geq b$, l'entier $r - b = a - b(q + 1)$ serait un élément plus petit : contradiction. Donc $0 \leq r < b$.

**Étape 2 (unicité).** Si $bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$, alors $b \mid r' - r$ et $|r' - r| < b$. Si l'on avait $r' \neq r$, la comparaison des valeurs absolues donnerait $b \leq |r' - r|$ : contradiction. Donc $r = r'$ ; puis $bq = bq'$, donc $q = q'$.

**Étape 3.** Si $r = 0$, alors $a = bq$ et $b \mid a$. Si $a = bk$, le couple $(k, 0)$ convient ; par unicité, $r = 0$.

**Remarque : Une propriété admise**

La preuve de l'existence choisit le plus petit élément d'une partie de $\mathbb{N}$.

Elle s'appuie sur la propriété : toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Cette propriété de $\mathbb{N}$ est admise.

Elle resservira pour le plus petit diviseur d'un entier, pour la décomposition en facteurs premiers et pour la définition du PPCM.

**Vérifie : Pourquoi le reste est plus petit**

Dans l'étape 1, $r = a - bq$ est le plus petit entier positif ou nul de la forme $a - bk$. Si l'on avait $r \geq b$, quel entier contredirait ce choix ?

**A.** L'entier $r + b = a - b(q - 1)$.

**Faux.**
Il est de la bonne forme, mais plus grand que $r$ : aucune contradiction.

**B.** Le quotient $q$ lui-même.

**Faux.**
$q$ n'est pas de la forme $a - bk$ en général.

**C.** L'entier $r - b = a - b(q + 1)$.

**Juste.**
Juste : il est positif ou nul, de la bonne forme, et plus petit que $r$.

**D.** L'entier $0$, plus petit que $r$.

**Faux.**
$0$ n'est de la forme $a - bk$ que si $b \mid a$ : ce n'est pas le cas en général.

**Correction**
Si $r \geq b$, alors $r - b \geq 0$. Or

$$\begin{aligned} r - b &= a - bq - b \\ &= a - b(q + 1). \end{aligned}$$

C'est un entier de la forme $a - bk$, positif ou nul. Il est strictement plus petit que $r$, car $b > 0$.

**Conclusion.** Cela contredit le choix de $r$ ; donc $r < b$.

**À retenir : Retenir de la preuve : le plus petit reste**

> Le reste est le plus petit des nombres $a - bk$ positifs ou nuls : on retire $b$ autant de fois que possible.
>
> L'unicité vient de la comparaison des valeurs absolues. Deux restes possibles diffèrent de moins de $b$, et leur différence est un multiple de $b$ : elle est nulle.

## Raisonner selon les restes

**Exemple : un dividende négatif**

Divisons $-38$ par $7$. On divise d'abord $38$ :

$$38 = 7 \times 5 + 3.$$

Donc $-38 = 7 \times (-5) - 3$, mais $-3$ est négatif : ce n'est pas un reste. On retire un $7$ de plus :

$$-38 = 7 \times (-6) + 4,$$

avec $0 \leq 4 < 7$. Le quotient est $-6$ et le reste est $4$.

**Attention : le reste est positif et plus petit que le diviseur**

✗ « $29 = 4 \times 5 + 9$, donc le reste de $29$ par $4$ est $9$. »

✓ L'égalité est juste, mais $9 \geq 4$ : ce n'est pas la division euclidienne. On a $29 = 4 \times 7 + 1$, et le reste est $1$.

De même, $-29 = 4 \times (-8) + 3$ : le reste est $3$, et non $-1$.

**Méthode : raisonner selon les restes**

1. **Choisis** le diviseur $b$ adapté à la question, par exemple $2$, $3$ ou $4$.
2. **Annonce** les cas : d'après la division euclidienne, tout entier $n$ s'écrit $n = bq + r$, avec $q \in \mathbb{Z}$ et $r \in \{0, 1, \ldots, b-1\}$.
3. **Traite** chaque cas en remplaçant $n$ par $bq + r$.
4. **Conclus** : les $b$ cas couvrent tous les entiers.

**Exemple : Exemple guidé : trois cas selon le reste par 3**

**Énoncé.** Pour tout entier relatif $n$, $3 \mid n(n^2 + 2)$.

Soit $n \in \mathbb{Z}$. D'après la division euclidienne par $3$, il existe $q \in \mathbb{Z}$ tel que $n = 3q$, $n = 3q + 1$ ou $n = 3q + 2$.

**Cas 1 :** $n = 3q$**.** Alors $n(n^2+2) = 3 \times q(n^2+2)$ : c'est un multiple de $3$.

**Cas 2 :** $n = 3q+1$**.** Alors

$$\begin{aligned} n^2+2 &= 9q^2+6q+3 \\ &= 3(3q^2+2q+1). \end{aligned}$$

**Cas 3 :** $n = 3q+2$**.** Alors

$$\begin{aligned} n^2+2 &= 9q^2+12q+6 \\ &= 3(3q^2+4q+2). \end{aligned}$$

Dans les trois cas, $3$ divise $n$ ou $n^2+2$, donc leur produit.

**Conclusion.** Pour tout entier relatif $n$, $3 \mid n(n^2+2)$.

**À toi : Le carré d'un entier**

Soit $n$ un entier relatif. Montre que le reste de $n^2$ dans la division euclidienne par $4$ est $0$ ou $1$. Déduis-en que $1003$ n'est le carré d'aucun entier. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Raisonne selon le reste de $n$ dans la division par $2$ : deux cas.
**Indice 2**
Pour $n = 2q+1$, développe : $n^2 = 4q^2+4q+1$.
**Indice 3**
Point délicat : écris la division euclidienne de $1003$ par $4$, avec un reste entre $0$ et $3$.

**Réponse**
Soit $n \in \mathbb{Z}$. D'après la division euclidienne par $2$, il existe $q \in \mathbb{Z}$ tel que $n = 2q$ ou $n = 2q+1$.

**Cas 1 :** $n = 2q$**.** Alors $n^2 = 4 \times q^2 + 0$ : le reste est $0$.

**Cas 2 :** $n = 2q+1$**.** Alors

$$\begin{aligned} n^2 &= 4q^2+4q+1 \\ &= 4(q^2+q)+1, \end{aligned}$$

avec $0 \leq 1 < 4$ : le reste est $1$.

Dans les deux cas, le reste de $n^2$ dans la division par $4$ est $0$ ou $1$.

**Conséquence.** Or $1003 = 4 \times 250 + 3$ : son reste est $3$.

**Conclusion.** L'entier $1003$ n'est le carré d'aucun entier.

## Nombres premiers et test de primalité

## Les nombres premiers

**Devine : Un nombre premier ?**

Les nombres premiers sont les briques des entiers : on les reconnaît, puis on casse chaque entier en briques. Commençons par les reconnaître.

**Petit rappel.** Au tronc commun, un nombre premier est un entier naturel qui a exactement deux diviseurs positifs. Lequel de ces nombres est premier ?

**A.** $53$

**Juste.**
Juste : $53$ n'a que deux diviseurs positifs, $1$ et $53$.

**B.** $1$

**Faux.**
$1$ n'a qu'un seul diviseur positif : il n'est pas premier.

**C.** $51$

**Faux.**
$51 = 3 \times 17$ : il est impair, mais composé.

**D.** $57$

**Faux.**
$57 = 3 \times 19$ : il est impair, mais composé.

**Correction**
$1$ n'a qu'un diviseur positif. $51 = 3 \times 17$ et $57 = 3 \times 19$ ont d'autres diviseurs que $1$ et eux-mêmes.

Quant à $53$, il n'est divisible ni par $2$, ni par $3$, ni par $5$, ni par $7$, et $8 \times 8 = 64 > 53$.

Tu verras plus loin pourquoi ces essais suffisent : $53$ est premier.

**Définition : Nombre premier**

Un entier naturel $p$ est **premier** si $p \geq 2$ et si ses seuls diviseurs positifs sont $1$ et $p$. On note $\mathbb{P}$ l'ensemble des nombres premiers.

Un entier naturel $n \geq 2$ qui n'est pas premier est dit **composé** : il admet un diviseur positif $d$ autre que $1$ et $n$, et alors $1 < d < n$.

**Exemple : premiers et plus petit diviseur**

Les nombres premiers inférieurs à $30$ sont $2$, $3$, $5$, $7$, $11$, $13$, $17$, $19$, $23$ et $29$. Seul $2$ est pair.

Les diviseurs de $91$ supérieurs ou égaux à $2$ sont $7$, $13$ et $91$ ; le plus petit, $7$, est premier.

**Pourquoi est-ce vrai ?** Si ce plus petit diviseur $d$ avait un diviseur $e$ tel que $1 < e < d$, alors $e$ diviserait aussi $91$. Ce serait un diviseur plus petit que $d$.

## Le plus petit diviseur

**Propriété : Plus petit diviseur d'un entier**

Soit $n$ un entier naturel tel que $n \geq 2$. Le plus petit diviseur $d$ de $n$ tel que $d \geq 2$ est un nombre premier. En particulier, tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

**Démonstration**

**Étape 1.** Les diviseurs de $n$ supérieurs ou égaux à $2$ forment une partie non vide de $\mathbb{N}$, car elle contient $n$. Elle admet un plus petit élément $d$ (propriété de $\mathbb{N}$, admise).

**Étape 2.** Supposons par l'absurde que $d$ n'est pas premier. Comme $d \geq 2$, il admet un diviseur $e$ tel que $1 < e < d$ (définition d'un nombre premier). Or $e \mid d$ et $d \mid n$, donc $e \mid n$ (propriétés de la divisibilité). Ainsi $e$ est un diviseur de $n$, avec $e \geq 2$ et $e < d$ : cela contredit le choix de $d$.

**Étape 3.** Donc $d$ est premier, et c'est un diviseur premier de $n$.

**À retenir : Retenir de la preuve : le plus petit diviseur**

On choisit le **plus petit** diviseur supérieur ou égal à $2$, puis on raisonne par l'absurde : s'il n'était pas premier, il en existerait un plus petit.

Ce schéma, « un plus petit élément, puis une contradiction », reviendra pour la décomposition.

**Vérifie : Le plus petit diviseur**

Quel est le plus petit diviseur de $143$ supérieur ou égal à $2$ ?

**A.** $7$

**Faux.**
$143 = 7 \times 20 + 3$ : $7$ ne divise pas $143$.

**B.** $11$

**Juste.**
Juste : $143 = 11 \times 13$, et aucun entier de $2$ à $10$ ne divise $143$.

**C.** $13$

**Faux.**
$13$ divise $143$, mais il existe un diviseur plus petit.

**D.** $143$, car il est premier.

**Faux.**
$143 = 11 \times 13$ : il n'est pas premier.

**Correction**

On essaie les nombres premiers dans l'ordre :

$$143 = 2 \times 71 + 1,$$
$$143 = 3 \times 47 + 2,$$
$$143 = 5 \times 28 + 3,$$
$$143 = 7 \times 20 + 3.$$

Enfin, $143 = 11 \times 13$.

**Conclusion.** Le plus petit diviseur cherché est $11$, et il est bien premier.

**Exemple : chercher un diviseur premier**

Prenons $n = 221$. Aucun des nombres $2$, $3$, $5$, $7$, $11$ ne divise $221$. Puis $221 = 13 \times 17$.

Le plus petit diviseur supérieur ou égal à $2$ est donc $13$, premier, et $13^2 = 169 \leq 221$.

Pour $n = 1$, il n'y a aucun diviseur supérieur ou égal à $2$ : l'hypothèse $n \geq 2$ est nécessaire.

**Pourquoi est-ce vrai ?** Si $n$ est composé, écrivons $n = pm$, avec $p$ son plus petit diviseur supérieur ou égal à $2$. Le cofacteur $m$ divise aussi $n$, et $m \geq 2$ car $p \neq n$ ; donc $m \geq p$, d'où $p^2 \leq pm = n$.

## Le test de primalité

**Propriété : Test de primalité**

Soit $n$ un entier naturel tel que $n \geq 2$. Si $n$ n'est pas premier, alors $n$ admet un diviseur premier $p$ tel que $p^2 \leq n$.

Par contraposée : si aucun nombre premier $p$ tel que $p^2 \leq n$ ne divise $n$, alors $n$ est premier.

---

**Démonstration**

**Étape 1.** Supposons $n$ composé. Notons $p$ le plus petit diviseur de $n$ supérieur ou égal à $2$ : $p$ est premier (plus petit diviseur). Il existe un entier naturel $m$ tel que $n = pm$.

**Étape 2.** Comme $n$ n'est pas premier, $p \neq n$, donc $m \neq 1$ ; et $m \neq 0$ car $n \neq 0$. Ainsi $m \geq 2$. Or $m$ divise $n$ ; par le choix de $p$, on a $p \leq m$.

**Étape 3.** Donc $p^2 \leq pm = n$. La seconde phrase de l'énoncé est la contraposée de la première.

**À retenir : Retenir de la preuve : le cofacteur**

Dans $n = pm$, avec $p$ le plus petit diviseur, on a $p \leq m$, donc $p^2 \leq n$.

Conséquence pratique : pour prouver que $n$ est premier, il suffit de tester les nombres premiers $p$ tels que $p^2 \leq n$.

**Vérifie : Le cofacteur**

Dans l'étape 2 de la preuve, pourquoi a-t-on $p \leq m$ ?

**A.** Car $p$ est premier, alors que $m$ ne l'est pas forcément.

**Faux.**

Être premier ne compare pas $p$ à $m$.

**B.** Car $m$ est lui aussi premier, et plus grand que $p$.

**Faux.**

Rien ne le dit : pour $n = 12$, $p = 2$ et $m = 6$.

**C.** Car $m \geq 2$ divise $n$, et $p$ est le plus petit tel diviseur.

**Juste.**

Juste : c'est le choix de $p$ qui fait tout.

**D.** Car on sait déjà que $p^2 \leq n$.

**Faux.**

C'est la conclusion, pas l'argument.

**Correction**

Le cofacteur $m$ divise $n$ et vérifie $m \geq 2$. Par le choix de $p$, plus petit diviseur de $n$ supérieur ou égal à $2$, on a $p \leq m$.

En multipliant par $p > 0$ :

$$p^2 \leq pm = n.$$

## Tester un entier

**Méthode : reconnaître un nombre premier**

1. **Liste**, pour un entier $n \geq 2$, les nombres premiers $p$ tels que $p^2 \leq n$ : $2, 3, 5, 7, \ldots$
2. **Teste** la divisibilité de $n$ par chacun, dans l'ordre.
3. **Si l'un d'eux divise** $n$, alors $n$ est composé : comme $p^2 \leq n$, le diviseur $p$ vérifie $1 < p < n$.
4. **Si aucun ne divise** $n$, alors $n$ est premier, d'après le test de primalité.

**Exemple : Exemple guidé : 323 et 331**

**Pour $323$.** On a

$$17^2 = 289 \leq 323 < 324 = 18^2.$$

Aucun des nombres $2, 3, 5, 7, 11, 13$ ne divise $323$. Puis $323 = 17 \times 19$ : $323$ est composé.

**Pour $331$.** On a

$$18^2 = 324 \leq 331 < 361 = 19^2.$$

On teste $2$, $3$, $5$, $7$, $11$, $13$ et $17$ : les restes sont $1$, $1$, $1$, $2$, $1$, $6$ et $8$. Aucun n'est nul : $331$ est premier.

**À toi : Premier ou composé ?**

Décide si $247$ et $251$ sont premiers, en justifiant chaque essai. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Pour chaque nombre, cherche le plus grand entier dont le carré ne le dépasse pas.
**Indice 2**
$15^2 = 225$ et $16^2 = 256$ : les nombres premiers à tester sont au plus égaux à $13$.
**Indice 3**
Point délicat : un seul diviseur trouvé suffit pour conclure « composé » ; pour « premier », il faut tous les essais.

**Réponse**
**Bornes.** On a

$$15^2 = 225 \leq 247 < 251 < 256 = 16^2.$$

On teste donc $2$, $3$, $5$, $7$, $11$ et $13$.

**Pour $247$.** Ni $2$, ni $3$, ni $5$, ni $7$, ni $11$ ne divise $247$, mais $247 = 13 \times 19$. Donc $247$ est composé.

**Pour $251$.** Les restes par $2$, $3$, $5$, $7$, $11$ et $13$ sont $1$, $2$, $1$, $6$, $9$ et $4$. Aucun n'est nul : $251$ est premier.

**Attention : 1 n'est pas premier, et impair ne veut pas dire premier**

✗ « $39$ est impair et ne finit pas par $5$, donc il est premier. »

✓ $39 = 3 \times 13$ est composé. Être impair élimine seulement le diviseur $2$. Seul le test des nombres premiers $p$ tels que $p^2 \leq n$ permet de conclure.

Et $1$ n'est pas premier : il n'a qu'un diviseur positif.

## Une infinité de nombres premiers

## La liste s'arrête-t-elle ?

**Devine : Une liste qui s'arrête ?**

Entre $1$ et $100$, il y a $25$ nombres premiers. Entre $901$ et $1000$, il n'y en a plus que $14$. D'après toi, la liste des nombres premiers s'arrête-t-elle ?

**A.** Oui : au-delà d'un certain entier, il n'y en a plus.

**Faux.**

Leur raréfaction ne prouve pas leur disparition : tu vas voir qu'il en reste toujours.

**B.** Oui, avant $10000$, car ils deviennent rares.

**Faux.**

Par exemple, $10007$ est premier.

**C.** Personne ne le sait encore aujourd'hui.

**Faux.**

La question est tranchée depuis l'Antiquité, par une preuve courte.

**D.** Non : il y en a une infinité.

**Juste.**

Juste : c'est le théorème qui suit.

**Correction**

La liste ne s'arrête pas.

**Pourquoi est-ce vrai ?** Donne-toi une liste finie de nombres premiers. Multiplie-les et ajoute $1$ : le nombre obtenu n'est divisible par aucun d'eux. Un de ses diviseurs premiers manque donc à la liste.

**Théorème : Infinité des nombres premiers**

L'ensemble $\mathbb{P}$ des nombres premiers est infini.

**Démonstration**

**Étape 1.** Supposons par l'absurde que $\mathbb{P}$ est fini, formé des nombres premiers $p_1, p_2, \dots, p_k$. Posons $N = p_1 p_2 \cdots p_k + 1$.

**Étape 2.** Comme $p_1 p_2 \cdots p_k \geq 1$, on a $N \geq 2$ : $N$ admet un diviseur premier $p$ (plus petit diviseur). Ce nombre $p$ est l'un des $p_i$, et le produit $p_1 p_2 \cdots p_k$ est $p_i$ multiplié par un entier : $p \mid p_1 p_2 \cdots p_k$ (définition de la divisibilité).

**Étape 3.** Comme $p \mid N$ et $p \mid p_1 p_2 \cdots p_k$, $p$ divise leur différence, $N - p_1 p_2 \cdots p_k = 1$ (propriétés de la divisibilité). Par comparaison des valeurs absolues, $p \leq 1$, ce qui contredit $p \geq 2$.

**Étape 4.** Donc $\mathbb{P}$ est infini.

**À retenir : Retenir de la preuve : l'argument d'Euclide**

Pour montrer qu'un ensemble est infini, on le suppose fini, puis on fabrique un objet qui échappe à la liste.

Ici, $N = p_1 p_2 \cdots p_k + 1$ laisse le reste $1$ dans la division par chaque $p_i$. Aucun $p_i$ ne le divise.

**Vérifie : La contradiction**

Dans l'étape 3, le nombre premier $p$ divise $N$ et $p_1 p_2 \cdots p_k$. Quel nombre divise-t-il alors, ce qui donne la contradiction ?

**A.** Le nombre $1$, leur différence.

**Juste.**

Juste : un diviseur positif de $1$ vérifie $p \leq 1$, impossible pour un nombre premier.

**B.** Le nombre $N$, qui est donc premier.

**Faux.**

$p$ divise $N$ par construction ; cela ne dit pas que $N$ est premier.

**C.** Leur somme $N + p_1 p_2 \cdots p_k$.

**Faux.**

Il la divise bien, mais elle vaut $2p_1 p_2 \cdots p_k + 1$ : aucune contradiction.

**D.** Le produit $p_1 p_2 \cdots p_k$ seulement.

**Faux.**

C'est ce que dit l'étape 2, pas ce qui contredit l'hypothèse.

**Correction**

Comme $p \mid N$ et $p \mid p_1 p_2 \cdots p_k$, l'entier $p$ divise leur différence, d'après les propriétés de la divisibilité :

$$N - p_1 p_2 \cdots p_k = 1.$$

La comparaison des valeurs absolues donne $p \leq 1$. Or un nombre premier vérifie $p \geq 2$ : contradiction.

## Le nombre construit

**Exemple : Contre-exemple : le nombre construit n'est pas toujours premier**

Avec les six plus petits nombres premiers :

$$\begin{aligned} & 2 \times 3 \times 5 \times 7 \times 11 \times 13 \\ & \quad + 1 \\ & = 30031 = 59 \times 509. \end{aligned}$$

Ce nombre est composé. La preuve n'affirme donc pas que $N$ est premier.

Elle affirme seulement que ses diviseurs premiers, ici $59$ et $509$, sont absents de la liste.

**À toi : Hors de la liste**

Soit

$$\begin{aligned} N &= 2 \times 3 \times 5 \times 7 \times 11 + 1 \\ &= 2311. \end{aligned}$$

Donne le reste de $N$ dans la division par $2$, $3$, $5$, $7$ et $11$. Explique pourquoi tout diviseur premier de $N$ est au moins égal à $13$. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Pour la division par $3$, écris $N = 3 \times (2 \times 5 \times 7 \times 11) + 1$.
**Indice 2**
Vérifie que l'écriture obtenue est une division euclidienne : $0 \leq 1 < 3$.
**Indice 3**
Point délicat : un nombre premier plus petit que $13$ est l'un des cinq nombres de la liste.

**Réponse**
**Restes.** Pour chaque $p$ de la liste, $N = p \times m + 1$, où $m$ est le produit des quatre autres nombres. Comme $0 \leq 1 < p$, c'est la division euclidienne : le reste est $1$, pour $p = 2$, $3$, $5$, $7$ et $11$.

**Diviseurs premiers.** Aucun de ces nombres ne divise donc $N$. Or les nombres premiers plus petits que $13$ sont exactement $2$, $3$, $5$, $7$ et $11$.

**Conclusion.** Tout diviseur premier de $N$ est au moins égal à $13$.

## Décomposition en produit de facteurs premiers

## Casser un entier en facteurs premiers

**Devine : Deux chemins**

On décompose $360$ de deux façons : en partant de $360 = 8 \times 45$, ou de $360 = 12 \times 30$. On casse chaque facteur jusqu'à n'avoir que des nombres premiers. Que trouve-t-on ?

**A.** Deux produits différents, selon le départ.
**Faux.**
Fais les deux calculs : ils donnent les mêmes facteurs, dans un autre ordre.

**B.** On reste bloqué sur un facteur comme $45$.
**Faux.**
$45 = 3 \times 3 \times 5$ : on peut toujours continuer jusqu'à des nombres premiers.

**C.** Le même produit, à l'ordre des facteurs près.
**Juste.**
Juste : $2^3 \times 3^2 \times 5$ dans les deux cas.

**D.** Un produit qui contient le facteur $4$.

**Faux.**
$4 = 2 \times 2$ n'est pas premier : on le casse encore.

**Correction**
**Premier chemin.** $8 = 2 \times 2 \times 2$ et $45 = 3 \times 3 \times 5$.

**Second chemin.** $12 = 2 \times 2 \times 3$ et $30 = 2 \times 3 \times 5$.

Dans les deux cas, on obtient trois facteurs $2$, deux facteurs $3$ et un facteur $5$ :

$$360 = 2^3 \times 3^2 \times 5.$$

Tant qu'un facteur est composé, on peut le casser en deux facteurs plus petits. Et le procédé s'arrête, car les facteurs diminuent.

**Pourquoi est-ce vrai ?** S'il existait des entiers $n \geq 2$ qui ne sont pas des produits de nombres premiers, on regarderait le plus petit. Il serait composé, produit de deux entiers plus petits, eux-mêmes décomposables.

## L'existence

**Théorème : Existence de la décomposition en facteurs premiers**

Tout entier naturel $n \geq 2$ est un produit de nombres premiers : il existe un entier $k \geq 1$ et des nombres premiers $p_1 \leq p_2 \leq \cdots \leq p_k$ tels que $n = p_1 p_2 \cdots p_k$.

**Démonstration**
**Étape 1.** Supposons par l'absurde que certains entiers $n \geq 2$ ne soient pas des produits de nombres premiers. Ils forment une partie non vide de $\mathbb{N}$, qui admet un plus petit élément $m$ (propriété de $\mathbb{N}$, admise).

**Étape 2.** L'entier $m$ n'est pas premier, sinon il serait le produit d'un seul nombre premier. Il admet donc un diviseur $a$ tel que $1 < a < m$ (définition d'un nombre premier) ; on écrit $m = ab$ ; comme $1 < a < m$, on a $1 < b < m$.

**Étape 3.** Par le choix de $m$, $a$ et $b$, compris entre $2$ et $m - 1$, sont des produits de nombres premiers. En réunissant ces deux produits, facteurs rangés, $m = ab$ en est un aussi : contradiction.

**Étape 4.** Donc tout entier $n \geq 2$ est un produit de nombres premiers.

**À retenir : Retenir de la preuve : le plus petit contre-exemple**

C'est la méthode du **plus petit contre-exemple** : on suppose qu'il existe des contre-exemples, on prend le plus petit, et on le contredit.

La propriété admise du plus petit élément d'une partie de $\mathbb{N}$ rend ce raisonnement possible.

**Vérifie : Le choix du plus petit**

Dans l'étape 3 de la preuve, pourquoi $a$ et $b$ sont-ils des produits de nombres premiers ?

**A.** Parce que $a$ et $b$ sont des diviseurs premiers de $m$.

**Faux.**

Rien ne le garantit : $a$ est seulement un diviseur de $m$ tel que $1 < a < m$.

**B.** Parce que $a, b < m$ et $m$ est le plus petit contre-exemple.

**Juste.**

Juste : sous $m$, tout entier supérieur ou égal à $2$ est un produit de nombres premiers.

**C.** Parce que l'un des deux facteurs est forcément pair.

**Faux.**

La parité ne joue aucun rôle dans la preuve.

**D.** Parce que $m$ est premier, donc ses diviseurs aussi.

**Faux.**

L'étape 2 montre au contraire que $m$ n'est pas premier.

**Correction**

Les entiers $a$ et $b$ sont compris entre $2$ et $m-1$. Or $m$ est le plus petit entier supérieur ou égal à $2$ qui n'est pas un produit de nombres premiers. Donc $a$ et $b$ en sont.

En réunissant leurs facteurs, $m = ab$ en est un aussi : contradiction.

## Décomposer en pratique

**Méthode : décomposer un entier**

1. **Divise** $n$ par le plus petit nombre premier qui le divise, autant de fois que possible.
2. **Recommence** avec le quotient et les nombres premiers suivants : $3, 5, 7, 11\ldots$
3. **Arrête-toi** quand le quotient vaut $1$, ou quand le quotient $m$ n'a aucun diviseur premier $p$ avec $p^2 \leq m$ : il est alors premier.
4. **Écris** $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, avec $p_1 < \cdots < p_r$.

**Exemple : Exemple guidé : décomposer 1386**

**Divisions.**

$$\begin{aligned} 1386 &= 2 \times 693, \\ 693 &= 3 \times 231, \\ 231 &= 3 \times 77. \end{aligned}$$

Le quotient $77$ n'est divisible ni par $3$ ni par $5$ ; $77 = 7 \times 11$, et $11$ est premier.

**Décomposition.**

$$1386 = 2 \times 3^2 \times 7 \times 11.$$

**Contrôle.** $2 \times 9 \times 7 \times 11 = 18 \times 77 = 1386$.

**Attention : chaque facteur doit être premier**

✗ « $360 = 4 \times 9 \times 10$ : voici la décomposition de $360$. »

✓ Ni $4$, ni $9$, ni $10$ n'est premier. On continue : $4 = 2^2$, $9 = 3^2$ et $10 = 2 \times 5$.

La décomposition est $360 = 2^3 \times 3^2 \times 5$.

## L'unicité

**Théorème : Unicité de la décomposition en facteurs premiers**

Cette décomposition est unique : si $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, avec des nombres premiers $p_1 \leq \cdots \leq p_k$ et $q_1 \leq \cdots \leq q_l$, alors $k = l$ et $p_i = q_i$ pour tout $i$.

En regroupant les facteurs égaux, tout entier $n \geq 2$ s'écrit donc de façon unique

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

avec des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des entiers $\alpha_i \geq 1$ : c'est la **décomposition en produit de facteurs premiers** de $n$.

**Remarque : Un résultat admis**

Ce résultat est admis. Sa preuve demande un outil que tu rencontreras en 2BAC SM.

Il garantit que les deux chemins de l'activité d'ouverture devaient aboutir au même produit.

**À toi : Deux décompositions**

Décompose $1584$ et $4199$ en produits de facteurs premiers. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Commence par diviser $1584$ par $2$ autant de fois que possible.
**Indice 2**
Pour $4199$ : ni $2$, ni $3$, ni $5$, ni $7$, ni $11$ ne le divise ; essaie $13$.
**Indice 3**
Point délicat : vérifie que chaque facteur final est premier, puis contrôle en refaisant le produit.

**Réponse**

**Pour $1584$.** On divise par $2$ autant de fois que possible :

$$\begin{aligned} 1584 &= 2 \times 792 \\ &= 2^2 \times 396 \\ &= 2^3 \times 198 \\ &= 2^4 \times 99. \end{aligned}$$

Puis $99 = 3^2 \times 11$. Donc

$$1584 = 2^4 \times 3^2 \times 11.$$

**Pour $4199$.** On a $4199 = 13 \times 323$, et $323 = 17 \times 19$. Donc

$$4199 = 13 \times 17 \times 19.$$

## Diviseurs d'un entier

## Compter les diviseurs

**Devine : Combien de diviseurs ?**

On a $12 = 2^2 \times 3$. Combien $12$ a-t-il de diviseurs positifs ?

**A.** $3$

**Faux.**

Tu comptes peut-être les facteurs $2$, $2$ et $3$ ; mais $1$, $4$, $6$ et $12$ divisent aussi $12$.

**B.** $4$

**Faux.**

Il en manque : liste-les tous, de $1$ à $12$.

**C.** $5$

**Faux.**

Il en manque un : as-tu pensé à $1$ et à $12$ ?

**D.** $6$

**Juste.**

Juste : $1$, $2$, $3$, $4$, $6$ et $12$.

**Correction**

Les diviseurs positifs de $12$ sont $1, 2, 3, 4, 6$ et $12$. Chacun s'écrit $2^\beta \times 3^\gamma$, avec $\beta \in \{0, 1, 2\}$ et $\gamma \in \{0, 1\}$.

Range-les dans un tableau : une ligne par valeur de $\beta$ ($3$ lignes), une colonne par valeur de $\gamma$ ($2$ colonnes). Il y a $3 \times 2 = 6$ cases, donc $6$ diviseurs.

**Propriété : Diviseurs d'un entier**

Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ la décomposition en produit de facteurs premiers d'un entier $n \geq 2$. Les diviseurs positifs de $n$ sont exactement les entiers

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \quad \text{avec } 0 \leq \beta_i \leq \alpha_i \text{ pour tout } i.$$

Le nombre de diviseurs positifs de $n$ est $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$.

---

**Démonstration**

Idée de la preuve. Un tel produit divise $n$ : on complète avec les facteurs $p_i^{\alpha_i - \beta_i}$. Réciproquement, si $n = dd'$, on écrit côte à côte des décompositions de $d$ et de $d'$ ; par unicité de la décomposition, les facteurs premiers de $d$ sont parmi $p_1, \ldots, p_r$, avec des exposants au plus égaux aux $\alpha_i$. Chaque $\beta_i$ prend $\alpha_i + 1$ valeurs, et deux choix différents donnent deux entiers différents, encore par unicité. Étapes omises : les cas $d = 1$ et $d = n$, et la rédaction du décompte des choix.

**Remarque : Une preuve esquissée**

La preuve est seulement esquissée. Elle repose sur l'unicité de la décomposition, admise.

Elle omet les cas $d = 1$ et $d = n$, ainsi que la rédaction du décompte des choix d'exposants.

**Exemple : les diviseurs de 180**

On a $180 = 2^2 \times 3^2 \times 5$. Un diviseur positif s'écrit

$$2^{\beta} \times 3^{\gamma} \times 5^{\delta},$$

avec $0 \leq \beta \leq 2$, $0 \leq \gamma \leq 2$ et $0 \leq \delta \leq 1$.

Un tableau pour $2$ et $3$ a $3 \times 3 = 9$ cases ; l'exposant de $5$ les double : $9 \times 2 = 18$ diviseurs.

Par exemple, $2 \times 3^2 = 18$ divise $180$. Mais $2^3 = 8$ ne le divise pas : l'exposant $3$ dépasse $2$.

## En devoir

**Remarque : Coin devoir : déterminer les diviseurs d'un entier**

En devoir, « détermine les diviseurs positifs de $n$ » se traite en trois temps :

1. la décomposition, avec ses divisions ;
2. la forme des diviseurs et leur nombre, d'après la propriété des diviseurs d'un entier ;
3. la liste, rangée dans un tableau : une ligne par puissance d'un nombre premier, une colonne par puissance de l'autre.

Le nombre de cases contrôle la liste.

**À toi : Les diviseurs de 200**

Détermine le nombre de diviseurs positifs de $200$, puis leur liste. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Décompose d'abord $200$ en produit de facteurs premiers.
**Indice 2**
Un diviseur s'écrit $2^\beta \times 5^\gamma$ : donne les valeurs possibles de $\beta$ et de $\gamma$.
**Indice 3**
Point délicat : n'oublie ni $1$, où tous les exposants sont nuls, ni $200$ lui-même.

**Réponse**
$200 = 2^3 \times 5^2$. Un diviseur positif s'écrit $2^\beta \times 5^\gamma$, avec $0 \leq \beta \leq 3$ et $0 \leq \gamma \leq 2$. Il y en a $(3+1)(2+1) = 12$.

| $\times$ | $5^0$ | $5^1$ | $5^2$ |
|---|---|---|---|
| $2^0$ | $1$ | $5$ | $25$ |
| $2^1$ | $2$ | $10$ | $50$ |
| $2^2$ | $4$ | $20$ | $100$ |
| $2^3$ | $8$ | $40$ | $200$ |

## PGCD et division euclidienne

### Le plus grand diviseur commun

Les diviseurs positifs de $24$ sont $1, 2, 3, 4, 6, 8, 12$ et $24$. Ceux de $36$ sont $1, 2, 3, 4, 6, 9, 12, 18$ et $36$.

Les diviseurs communs positifs sont $1, 2, 3, 4, 6$ et $12$. Le plus grand est $12$ : c'est le plus grand diviseur commun de $24$ et $36$.

**Devine : Avec un nombre négatif**

Quel est le plus grand diviseur commun à $-18$ et $30$ ?

**A.** $6$
**Juste.**
Juste : les diviseurs de $-18$ sont ceux de $18$.

**B.** $-6$
**Faux.**
$-6$ est un diviseur commun, mais $6$ est plus grand.

**C.** $18$
**Faux.**

$18$ ne divise pas $30$.

**D.** $2$

**Faux.**

$2$ est un diviseur commun, mais pas le plus grand.

**Correction**

Les diviseurs de $-18$ sont ceux de $18$. Les diviseurs communs positifs de $18$ et $30$ sont $1$, $2$, $3$ et $6$.

Le plus grand diviseur commun à $-18$ et $30$ est donc $6$.

**Définition : PGCD de deux entiers**

Soient $a$ et $b$ deux entiers relatifs non tous les deux nuls. Les diviseurs communs à $a$ et à $b$ sont en nombre fini (comparaison des valeurs absolues) et $1$ en fait partie. Le plus grand d'entre eux est le **plus grand commun diviseur** de $a$ et $b$, noté $a \wedge b$ ou $\mathrm{pgcd}(a, b)$. C'est un entier naturel non nul.

**Exemple : quelques PGCD**

- $(-20) \wedge (-30) = 10$ et $13 \wedge 26 = 13$.
- $45 \wedge 0 = 45$ : tout entier divise $0$, donc les diviseurs communs sont ceux de $45$.
- $0 \wedge 0$ n'est pas défini : tout entier divise $0$, il n'y a pas de plus grand diviseur commun.

Un raccourci : $84 = 60 \times 1 + 24$, et

$$84 \wedge 60 = 60 \wedge 24 = 12.$$

**Pourquoi est-ce vrai ?** Un diviseur commun de $84$ et $60$ divise $84 - 60 = 24$. Un diviseur commun de $60$ et $24$ divise $60 + 24 = 84$.

## PGCD et division euclidienne

**Propriété : PGCD et division euclidienne**

Soient $a$ un entier relatif, $b$ un entier naturel non nul, et $r$ le reste de la division euclidienne de $a$ par $b$. Les diviseurs communs à $a$ et à $b$ sont exactement les diviseurs communs à $b$ et à $r$. En particulier,

$$a \wedge b = b \wedge r,$$

et $b \wedge 0 = b$.

---

**Démonstration**

**Étape 1.** Écrivons $a = bq + r$ (division euclidienne). Soit $d$ un diviseur commun à $a$ et $b$. Alors $d$ divise $a \times 1 + b \times (-q)$, c'est-à-dire $r$ (propriétés de la divisibilité).

**Étape 2.** Soit $d$ un diviseur commun à $b$ et $r$. Alors $d$ divise $b \times q + r \times 1$, c'est-à-dire $a$ (propriétés de la divisibilité).

**Étape 3.** Les deux ensembles de diviseurs communs sont donc égaux : ils ont le même plus grand élément, d'où $a \wedge b = b \wedge r$ (définition du PGCD).

**Étape 4.** Tout entier divise $0$. Les diviseurs communs à $b$ et $0$ sont donc les diviseurs de $b$, dont le plus grand est $b$ (comparaison des valeurs absolues) : $b \wedge 0 = b$.

**À retenir : Retenir de la preuve : les deux inclusions**

Pour montrer que deux ensembles de diviseurs communs sont égaux, on prouve les deux inclusions.

Chacune s'obtient par une combinaison : $r = a - bq$ dans un sens, $a = bq + r$ dans l'autre. Le PGCD ne change donc pas quand on remplace $(a, b)$ par $(b, r)$.

**Vérifie : Une combinaison**

Dans l'étape 1 de la preuve, $a = bq + r$. Quelle combinaison de $a$ et $b$ donne $r$ ?

**A.** $a + bq$

**Faux.**

$a + bq = 2bq + r$ : ce n'est pas $r$.

**B.** $a \times b - q$

**Faux.**

Pour $a = 7, b = 3$ et $q = 2$, ce nombre vaut $19$, alors que $r = 1$.

**C.** $a \times 1 + b \times (-q)$

**Juste.**

Juste : $a - bq = r$.

**D.** $\dfrac{a}{b}$

**Faux.**

Ce quotient n'est pas entier en général : ce n'est pas une combinaison à coefficients entiers.

**Correction**

De $a = bq + r$, on tire

$$r = a \times 1 + b \times (-q).$$

Les coefficients $1$ et $-q$ sont des entiers. Un diviseur commun de $a$ et $b$ divise donc $r$, d'après les propriétés de la divisibilité.

**Exemple : un PGCD qui dépend de n**

Soit $n$ un entier tel que $n > 5$. La division euclidienne de $n+5$ par $n$ s'écrit

$$n + 5 = n \times 1 + 5,$$

avec $0 \leq 5 < n$. Donc $(n+5) \wedge n = n \wedge 5$.

Ce PGCD divise $5$ : il vaut $5$ si $5 \mid n$, et $1$ sinon. Pour $n = 15$, on trouve $20 \wedge 15 = 5$.

**À toi : Par la division**

Soit $n$ un entier tel que $n \geq 3$. Calcule $(3n+2) \wedge n$ selon les valeurs de $n$, à l'aide d'une division euclidienne. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Écris la division euclidienne de $3n+2$ par $n$.
**Indice 2**
Vérifie la condition sur le reste : $0 \leq 2 < n$.
**Indice 3**
Point délicat : $n \wedge 2$ dépend de la parité de $n$.

**Réponse**
**Division euclidienne.** Soit $n$ un entier tel que $n \geq 3$. On a

$$3n + 2 = n \times 3 + 2,$$

avec $0 \leq 2 < n$ : c'est la division euclidienne de $3n+2$ par $n$.

**Réduction.** D'après la propriété du PGCD et de la division euclidienne, $(3n+2) \wedge n = n \wedge 2$.

**Conclusion.** Les diviseurs positifs de $2$ sont $1$ et $2$. Donc $(3n+2) \wedge n$ vaut $2$ si $n$ est pair, et $1$ si $n$ est impair.

## L'algorithme d'Euclide

## Répéter la division

**Devine : Des divisions en cascade**

On écrit les divisions successives :

$$\begin{aligned} 252 &= 198 \times 1 + 54 \\ 198 &= 54 \times 3 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 + 0 \end{aligned}$$

D'après la propriété précédente, que vaut $252 \wedge 198$ ?

**A.** $54$

**Faux.**

$54$ est le premier reste ; or $54$ ne divise pas $198$.

**B.** $36$

**Faux.**

$36$ ne divise pas $54$ : ce n'est pas un diviseur commun.

**C.** $18$

**Juste.**

Juste : c'est le dernier reste non nul.

**D.** $0$

**Faux.**

$0$ est le dernier reste, et un PGCD n'est jamais nul.

**Correction**

La propriété « PGCD et division euclidienne » s'applique à chaque ligne :

$$\begin{aligned} 252 \wedge 198 &= 198 \wedge 54 \\ &= 54 \wedge 36 \\ &= 36 \wedge 18 \\ &= 18 \wedge 0 = 18. \end{aligned}$$

**Pourquoi est-ce vrai ?** Chaque division conserve le PGCD. Et les restes sont des entiers naturels qui décroissent strictement : un reste nul finit par apparaître.

**Théorème : Algorithme d'Euclide**

Soient $a$ un entier relatif et $b$ un entier naturel non nul. On pose $r_0 = b$ et on note $r_1$ le reste de la division euclidienne de $a$ par $b$. Pour $k \geq 1$, tant que $r_k \neq 0$, on note $r_{k+1}$ le reste de la division euclidienne de $r_{k-1}$ par $r_k$.

Il existe un rang $m \geq 1$ tel que $r_m = 0$, et $a \wedge b$ est le **dernier reste non nul** : $a \wedge b = r_{m-1}$.

**Démonstration**

**Étape 1 (arrêt).** Chaque reste est positif ou nul et strictement inférieur au diviseur de sa division (division euclidienne) : tant que les restes sont non nuls, $b = r_0 > r_1 > r_2 > \cdots \geq 0$. Des entiers naturels strictement décroissants à partir de $b$ sont au plus $b + 1$. Un reste nul $r_m$ apparaît donc, avec $1 \leq m \leq b$.

**Étape 2 (PGCD).** D'après la propriété « PGCD et division euclidienne » appliquée à la première division, $a \wedge b = r_0 \wedge r_1$. Appliquée à chaque division suivante, elle donne $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$. De proche en proche, $a \wedge b = r_{m-1} \wedge r_m = r_{m-1} \wedge 0 = r_{m-1}$ (PGCD et division euclidienne).

**À retenir : Retenir de la preuve : l'algorithme d'Euclide**

Deux idées portent la preuve. Le PGCD se **conserve** d'une division à la suivante. Et une suite d'entiers naturels strictement décroissante est finie : l'algorithme **s'arrête**.

On lit alors le PGCD dans la dernière division : $r_{m-1} \wedge 0 = r_{m-1}$.

**Vérifie : L'arrêt**

Pourquoi l'algorithme d'Euclide s'arrête-t-il toujours ?

**A.** Parce que les quotients finissent par devenir nuls.

**Faux.**
À partir de la deuxième division, $r_{k-1} > r_k$ : chaque quotient est au moins égal à $1$.

**B.** Parce que les restes sont des entiers naturels strictement décroissants.

**Juste.**
Juste : une telle suite ne peut pas continuer indéfiniment.

**C.** Parce que chaque reste est au plus la moitié du précédent.

**Faux.**
C'est faux en général : $198 = 54 \times 3 + 36$ donne le reste $36$, plus grand que la moitié de $54$.

**D.** Parce que le premier reste divise toujours $b$.

**Faux.**
Pour $252$ et $198$, le premier reste $54$ ne divise pas $198$.

**Correction**
Chaque reste est positif ou nul et strictement inférieur au diviseur de sa division. Tant que les restes sont non nuls,

$$b = r_0 > r_1 > r_2 > \cdots \geq 0.$$

Une telle suite d'entiers naturels ne peut pas continuer indéfiniment : un reste nul apparaît, au plus tard après $b$ divisions.

## Calculer un PGCD

**Méthode : l'algorithme d'Euclide**

1. **Divise** $a$ par $b$ : $a = bq_1 + r_1$, avec $0 \leq r_1 < b$.

2. **Recommence** avec $b$ et $r_1$, puis avec les deux derniers restes, tant que le reste n'est pas nul.
3. **Lis** le PGCD : c'est le dernier reste non nul. Si le premier reste est déjà nul, c'est-à-dire si $b \mid a$, alors $a \wedge b = b$.
4. **Présente** une division par ligne, en colonne, pour pouvoir te relire.

**Exemple : Exemple guidé : le PGCD de 1078 et 322**

$$1078 = 322 \times 3 + 112$$
$$322 = 112 \times 2 + 98$$
$$112 = 98 \times 1 + 14$$
$$98 = 14 \times 7 + 0$$

Chaque reste est positif ou nul et plus petit que le diviseur de sa ligne.

**Conclusion.** Le dernier reste non nul est $14$ : $1078 \wedge 322 = 14$.

Le PGCD résume tous les diviseurs communs. Et il passe à travers un facteur commun. Voyons ces deux faits.

## Deux conséquences

**Propriété : Diviseurs communs et PGCD**

Soient $a$ et $b$ deux entiers relatifs non tous les deux nuls, et $d$ un entier relatif. Alors

$$\big(d \mid a \text{ et } d \mid b\big) \Leftrightarrow d \mid a \wedge b.$$

Les diviseurs communs à $a$ et à $b$ sont exactement les diviseurs de $a \wedge b$.

**Démonstration**

Idée de la preuve. Un diviseur de $a \wedge b$ divise $a$ et $b$, par transitivité. Réciproquement, on suit les divisions de l'algorithme d'Euclide : d'après la propriété « PGCD et division euclidienne », un diviseur commun à $a$ et $b$ est un diviseur commun à deux restes consécutifs, donc divise le dernier reste non nul, qui est $a \wedge b$. Étapes omises : la réduction au cas $b \geq 1$ et le passage d'une division à la suivante, rédigé de proche en proche.

**Exemple : tous les diviseurs communs**

**Une preuve esquissée.** La preuve est seulement esquissée. Elle omet la réduction au cas $b \geq 1$ et la rédaction, division par division, du passage d'un reste au suivant.

Les diviseurs communs à $1078$ et $322$ sont exactement les diviseurs de $14$ : $-14$, $-7$, $-2$, $-1$, $1$, $2$, $7$ et $14$.

Inutile de lister les diviseurs de $1078$ : le PGCD suffit.

**Propriété : PGCD et multiplication par un entier**

Soient $a$ et $b$ deux entiers relatifs non tous les deux nuls, et $k$ un entier naturel non nul. Alors

$$(ka) \wedge (kb) = k(a \wedge b).$$

**Démonstration**

Idée de la preuve. On multiplie par $k$ chaque division de l'algorithme d'Euclide appliqué à $a$ et $b$ : on obtient exactement les divisions de l'algorithme appliqué à $ka$ et $kb$, car $0 \leq kr < kb$ lorsque $0 \leq r < b$. Les restes sont multipliés par $k$, donc le dernier reste non nul aussi. Étapes omises : le cas où $a$ ou $b$ est négatif ou nul, et la vérification division par division.

**Exemple : mettre un facteur en commun**

**Une preuve esquissée.** La preuve est seulement esquissée. Elle omet le cas où $a$ ou $b$ est négatif ou nul, et la vérification division par division.

On a $600 = 120 \times 5$ et $840 = 120 \times 7$. Donc

$$\begin{aligned} 600 \wedge 840 &= 120 \times (5 \wedge 7) \\ &= 120 \times 1 = 120. \end{aligned}$$

Contrôle par l'algorithme :

$$\begin{aligned} 840 &= 600 \times 1 + 240 \\ 600 &= 240 \times 2 + 120 \\ 240 &= 120 \times 2 + 0 \end{aligned}$$

## À toi

**À toi : Un PGCD et ses diviseurs**

Calcule $2093 \wedge 1547$ par l'algorithme d'Euclide. Déduis-en les diviseurs communs positifs de $2093$ et $1547$. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Commence par la division de $2093$ par $1547$.
**Indice 2**
Le deuxième reste est $455$ ; continue jusqu'à un reste nul.
**Indice 3**
Point délicat : les diviseurs communs sont les diviseurs du PGCD ; décompose-le.

**Réponse**

**Divisions.**

$$\begin{aligned} 2093 &= 1547 \times 1 + 546 \\ 1547 &= 546 \times 2 + 455 \\ 546 &= 455 \times 1 + 91 \\ 455 &= 91 \times 5 + 0 \end{aligned}$$

**PGCD.** Le dernier reste non nul est $91$ : $2093 \wedge 1547 = 91$.

**Diviseurs communs.** D'après la propriété des diviseurs communs et du PGCD, ce sont les diviseurs de $91 = 7 \times 13$.

**Conclusion.** $2093 \wedge 1547 = 91$, et les diviseurs communs positifs de $2093$ et $1547$ sont $1$, $7$, $13$ et $91$.

Remarque **: Coin devoir : un PGCD d'expressions en n**

En devoir, chaque ligne de l'algorithme doit être une vraie division euclidienne. Exemple : soit $n$ un entier tel que $n \geq 2$.

$$\begin{aligned} 2n + 1 &= (n + 1) \times 1 + n, \\ n + 1 &= n \times 1 + 1, \\ n &= 1 \times n + 0. \end{aligned}$$

Vérifie chaque reste : $0 \leq n < n + 1$, puis $0 \leq 1 < n$.

Conclus : « le dernier reste non nul est $1$, donc $(2n + 1) \wedge (n + 1) = 1$ ».

## PPCM ; PGCD et PPCM par les décompositions

### Multiples communs

Deux phares s'allument ensemble à minuit. Le premier clignote toutes les $6$ secondes, le second toutes les $8$ secondes.

Ils s'allument de nouveau ensemble après $24$, $48$, $72$ secondes, et ainsi de suite : aux multiples communs de $6$ et $8$. Le plus petit multiple commun strictement positif est $24$.

**Devine : Un multiple commun**

Lequel de ces entiers est un multiple commun de $6$ et de $8$ ?

**A.** $96$

**Juste.**
Juste : $96 = 16 \times 6 = 12 \times 8$.

**B.** $100$

**Faux.**
$6 \nmid 100$ et $8 \nmid 100$.

**C.** $36$

**Faux.**

$36 = 6 \times 6$, mais $8 \nmid 36$.

**D.** $56$

**Faux.**

$56 = 7 \times 8$, mais $6 \nmid 56$.

**Correction**

$96 = 16 \times 6$ et $96 = 12 \times 8$ : c'est un multiple commun. C'est aussi un multiple de $24$, car $96 = 4 \times 24$.

Les multiples communs de $6$ et $8$ semblent être exactement les multiples de $24$.

**Pourquoi est-ce vrai ?** Divise un multiple commun par $24$ : le reste est encore un multiple commun, positif ou nul et plus petit que $24$. Il est donc nul.

**Définition : PPCM de deux entiers**

Soient $a$ et $b$ deux entiers relatifs non nuls. Les multiples communs à $a$ et à $b$ strictement positifs existent, par exemple $|ab|$. Le plus petit d'entre eux est le **plus petit commun multiple** de $a$ et $b$, noté $a \vee b$ ou $\mathrm{ppcm}(a, b)$.

## Les multiples communs

**Propriété : Multiples communs et PPCM**

Soient $a$ et $b$ deux entiers relatifs non nuls, et $m$ un entier relatif. Alors

$$\big(a \mid m \text{ et } b \mid m\big) \Leftrightarrow a \vee b \mid m.$$

Les multiples communs à $a$ et à $b$ sont exactement les multiples de $a \vee b$.

---

**Démonstration**

**Étape 1.** Supposons $a \vee b \mid m$. Comme $a \mid a \vee b$, on obtient $a \mid m$ (propriétés de la divisibilité) ; de même, $b \mid m$.

**Étape 2.** Réciproquement, supposons $a \mid m$ et $b \mid m$. Notons $\mu = a \vee b$ et écrivons $m = \mu q + r$, avec $0 \leq r < \mu$ (division euclidienne). Comme $a$ divise $m$ et $\mu$, il divise $m - \mu q = r$ (propriétés de la divisibilité) ; de même, $b \mid r$.

**Étape 3.** Si l'on avait $r \neq 0$, $r$ serait un multiple commun à $a$ et $b$, strictement positif et strictement inférieur à $\mu$ : cela contredit la définition du PPCM. Donc $r = 0$ et $\mu \mid m$ (division euclidienne).

**À retenir : Retenir de la preuve : diviser par le PPCM**

On divise le multiple commun $m$ par le PPCM $\mu$. Le reste $r = m - \mu q$ est un multiple commun, et $0 \leq r < \mu$. Le choix de $\mu$, le plus petit, oblige $r = 0$.

C'est le même geste que pour le plus petit diviseur : le plus petit interdit un plus petit encore.

**Vérifie : Le reste**

Dans l'étape 2 de la preuve, pourquoi le reste $r$ est-il un multiple de $a$ ?

**A.** Parce que $r < \mu$.

**Faux.**
L'inégalité dit que $r$ est petit, pas qu'il est multiple de $a$.

**B.** Parce que $r$ est positif ou nul.

**Faux.**
Être positif ne rend pas multiple de $a$.

**C.** Parce que $a$ divise $\mu$ et $r$ divise $m$.

**Faux.**
Rien ne dit que $r$ divise $m$ ; c'est $a$ qui divise $m$.

**D.** Parce que $r = m - \mu q$, et $a$ divise $m$ et $\mu$.

**Juste.**
Juste : c'est une combinaison de deux multiples de $a$.

**Correction**
On a

$$\begin{aligned} r &= m - \mu q \\ &= m \times 1 + \mu \times (-q). \end{aligned}$$

Par hypothèse, $a \mid m$ ; et $a \mid \mu$, car $\mu$ est un multiple de $a$. D'après les propriétés de la divisibilité, $a$ divise cette combinaison : $a \mid r$. De même, $b \mid r$.

**Contre-exemple : l'hypothèse $a$ et $b$ non nuls est nécessaire.** Si $a = 0$, le seul multiple de $a$ est $0$ : il n'existe aucun multiple commun strictement positif, et $a \vee b$ n'est pas défini.

## Par les décompositions

**Propriété : PGCD, PPCM et décompositions**

Soient $a$ et $b$ deux entiers naturels supérieurs ou égaux à $2$, écrits avec les mêmes nombres premiers $p_1 < p_2 < \cdots < p_r$ et des exposants entiers naturels, éventuellement nuls :

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

Alors $a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \cdots p_r^{\min(\alpha_r,\beta_r)}$, $a \vee b = p_1^{\max(\alpha_1,\beta_1)} \cdots p_r^{\max(\alpha_r,\beta_r)}$, et

$$(a \wedge b)(a \vee b) = ab.$$

**Démonstration**

Idée de la preuve. D'après la propriété des diviseurs d'un entier, les diviseurs communs positifs de $a$ et $b$ sont les $p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ avec $\gamma_i \leq \alpha_i$ et $\gamma_i \leq \beta_i$ : le plus grand s'obtient pour $\gamma_i = \min(\alpha_i, \beta_i)$. De même, la même propriété appliquée à un multiple commun $m$ montre que l'exposant de $p_i$ dans $m$ est au moins $\max(\alpha_i, \beta_i)$ : le plus petit multiple commun positif s'obtient en prenant ces exposants. Enfin, $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$ donne le produit. Étapes omises : la rédaction détaillée de ces comparaisons d'exposants.

**Remarque : Une preuve esquissée**

La preuve est esquissée : elle compare les exposants, grâce à la description des diviseurs d'un entier. Celle-ci repose sur l'unicité de la décomposition, admise.

Ce qui compte ici, c'est l'usage : petits exposants pour le PGCD, grands exposants pour le PPCM.

## Calculer par les décompositions

**Méthode : PGCD et PPCM par les décompositions**

1. **Décompose** $a$ et $b$ en produits de facteurs premiers.
2. **PGCD** : pour chaque nombre premier commun, garde le **plus petit** exposant.
3. **PPCM** : pour chaque nombre premier présent dans $a$ ou dans $b$, garde le **plus grand** exposant.
4. **Contrôle** avec l'égalité $(a \wedge b)(a \vee b) = ab$.

**Exemple : Exemple guidé : 1350 et 1260**

**Décompositions.** $1350 = 2 \times 3^3 \times 5^2$ et $1260 = 2^2 \times 3^2 \times 5 \times 7$. Avec les mêmes nombres premiers :

$$1350 = 2^1 \times 3^3 \times 5^2 \times 7^0.$$

**PGCD.** On garde les plus petits exposants :

$$\begin{aligned} &1350 \wedge 1260 \\ &= 2^1 \times 3^2 \times 5^1 \times 7^0 \\ &= 90. \end{aligned}$$

**PPCM.** On garde les plus grands exposants :

$$\begin{aligned} &1350 \vee 1260 \\ &= 2^2 \times 3^3 \times 5^2 \times 7^1 \\ &= 18900. \end{aligned}$$

**Contrôle.**

$$\begin{aligned} 90 \times 18900 &= 1701000 \\ &= 1350 \times 1260. \end{aligned}$$

**Attention : ne pas échanger les exposants**

✗ « $12 = 2^2 \times 3$ et $18 = 2 \times 3^2$, donc $12 \wedge 18 = 2^2 \times 3^2 = 36$. »

✓ $36$ est un multiple de $12$, pas un diviseur : c'est le PPCM. Le PGCD garde les plus petits exposants : $12 \wedge 18 = 2 \times 3 = 6$.

Contrôle : $6 \times 36 = 216 = 12 \times 18$.

**À toi : PGCD et PPCM**

Décompose $756$ et $1176$. Déduis-en $756 \wedge 1176$ et $756 \vee 1176$, puis contrôle ton résultat. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
$756 = 4 \times 189$ et $1176 = 8 \times 147$ : continue avec $189$ et $147$.
**Indice 2**
Écris les deux nombres avec les mêmes nombres premiers $2$, $3$ et $7$.
**Indice 3**
Point délicat : pour le PPCM, prends le plus grand exposant de chaque nombre premier, même s'il vient de l'autre nombre.

**Réponse**
**Décompositions.** $756 = 2^2 \times 3^3 \times 7$ et $1176 = 2^3 \times 3 \times 7^2$.

**PGCD.** On garde les plus petits exposants :

$$\begin{aligned} 756 \wedge 1176 &= 2^2 \times 3 \times 7 \\ &= 84. \end{aligned}$$

**PPCM.** On garde les plus grands exposants :

$$\begin{aligned} &756 \vee 1176 \\ &= 2^3 \times 3^3 \times 7^2 \\ &= 10584. \end{aligned}$$

**Contrôle.**

$$\begin{aligned} & 84 \times 10584 \\ & = 889056 \\ & = 756 \times 1176. \end{aligned}$$

## Congruence modulo n

## Même reste

**Devine : Même reste**

Sur une horloge, $9$ h plus $30$ heures donne $3$ h, car $39 = 12 \times 3 + 3$. Les entiers $39$ et $3$ ont le même reste dans la division par $12$, et $39 - 3 = 36$ est un multiple de $12$.

Lequel de ces entiers a le même reste que $20$ dans la division par $6$ ?

**A.** $4$

**Faux.**
Le reste de $4$ par $6$ est $4$ ; celui de $20$ est $2$.

**B.** $-4$

**Juste.**
Juste : $-4 = 6 \times (-1) + 2$, et $20 - (-4) = 24 = 6 \times 4$.

**C.** $-2$

**Faux.**
$-2 = 6 \times (-1) + 4$ : le reste est $4$, pas $2$.

**D.** $33$

**Faux.**
$33 = 6 \times 5 + 3$ : le reste est $3$.

**Correction**
$20 = 6 \times 3 + 2$ : le reste est $2$. Et $-4 = 6 \times (-1) + 2$, avec $0 \leq 2 < 6$ : même reste.

On remarque que $20 - (-4) = 24$ est un multiple de $6$.

Pour $4$, $-2$ et $33$, les restes sont $4$, $4$ et $3$.

**Définition : Congruence modulo n**

Soit $n$ un entier naturel non nul. Deux entiers relatifs $a$ et $b$ sont **congrus modulo** $n$ si $n \mid a - b$. On note

$$a \equiv b \ [n],$$

et on lit « $a$ est congru à $b$ modulo $n$ ».

**Exemple : lire une congruence**

- $38 \equiv 3\ [7]$, car $38 - 3 = 35 = 7 \times 5$.
- $-10 \equiv 4\ [7]$, car $-10 - 4 = -14 = 7 \times (-2)$.
- $23 \not\equiv 5\ [7]$, car $23 - 5 = 18$ et $7 \nmid 18$.

Note que $38$ et $3$ ont le même reste, $3$, dans la division par $7$.

**Pourquoi est-ce vrai ?** Si $a = nq + r$ et $b = nq' + r$, alors $a - b = n(q - q')$ : le reste disparaît dans la différence.

## Congruence et reste

**Propriété : Congruence et reste**

Soient $n$ un entier naturel non nul, et $a$ et $b$ deux entiers relatifs. Alors $a \equiv b\ [n]$ si et seulement si $a$ et $b$ ont le même reste dans la division euclidienne par $n$.

En particulier, si $r$ est le reste de la division euclidienne de $a$ par $n$, alors $a \equiv r\ [n]$ ; et $a \equiv 0\ [n]$ si et seulement si $n \mid a$.

---

**Démonstration**

**Étape 1.** Écrivons $a = nq + r$ et $b = nq' + r'$, avec $0 \leq r < n$ et $0 \leq r' < n$ (division euclidienne). Alors $a - b = n(q - q') + (r - r')$.

**Étape 2.** Si $r = r'$, alors $a - b = n(q - q')$, donc $n \mid a - b$.

**Étape 3.** Réciproquement, si $n \mid a - b$, alors $n$ divise $(a - b) - n(q - q') = r - r'$ (propriétés de la divisibilité). Or $|r - r'| < n$. Si l'on avait $r \neq r'$, la comparaison des valeurs absolues donnerait $n \leq |r - r'|$ : contradiction. Donc $r = r'$.

**Étape 4.** Comme $a - r = nq$, on a $a \equiv r\ [n]$. Enfin, $a \equiv 0\ [n]$ signifie $n \mid a - 0$ (définition de la congruence).

**À retenir : Retenir de la preuve : le même reste**

On écrit les deux divisions euclidiennes et on soustrait :

$$a - b = n(q - q') + (r - r').$$

Les restes vérifient $|r - r'| < n$, et un multiple de $n$ aussi petit est nul.

Retiens : « congrus modulo $n$ » et « même reste par $n$ » disent la même chose.

**Vérifie : L'étape clé**

Dans l'étape 3 de la preuve, $n$ divise $r - r'$. Pourquoi en déduit-on $r = r'$ ?

**A.** Parce que deux restes sont toujours égaux.

**Faux.**

Les restes de $5$ et de $6$ dans la division par $7$ sont $5$ et $6$ : ils diffèrent.

**B.** Parce que $r$ et $r'$ sont positifs.

**Faux.**

La positivité seule ne suffit pas : $1$ et $8$ sont positifs, et $7 \mid 8 - 1$.

**C.** Parce que $n$ divise $r$ et $r'$.

**Faux.**

Rien ne le dit : $n$ divise seulement leur différence.

**D.** Parce que $|r - r'| < n$, et un multiple de $n$ aussi petit est nul.

**Juste.**

Juste : c'est la comparaison des valeurs absolues.

**Correction**

Les restes vérifient $0 \leq r < n$ et $0 \leq r' < n$, donc $|r - r'| < n$.

Si l'on avait $r \neq r'$, la comparaison des valeurs absolues donnerait $n \leq |r - r'|$ : contradiction. Donc $r = r'$.

**Exemple : remplacer un entier par son reste**

$100 = 7 \times 14 + 2$, donc $100 \equiv 2\ [7]$. De même, $-15 = 4 \times (-4) + 1$, donc $-15 \equiv 1\ [4]$. Et $91 \equiv 0\ [13]$, car $91 = 13 \times 7$.

Une congruence se manie presque comme une égalité.

**Pourquoi est-ce vrai ?** Le nombre $0$, l'opposé d'un multiple de $n$ et la somme de deux multiples de $n$ sont des multiples de $n$.

## Comme une égalité

**Propriété : Réflexivité, symétrie, transitivité**

Soit $n$ un entier naturel non nul. Pour tous entiers relatifs $a$, $b$ et $c$ :

1. $a \equiv a\ [n]$ ;
2. si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$ ;
3. si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.

**Démonstration**

**Étape 1.** $a - a = 0 = 0 \times n$, donc $n \mid a - a$ (définition de la divisibilité).

**Étape 2.** Si $n \mid a - b$, alors $n$ divise $(a - b) \times (-1) = b - a$ (propriétés de la divisibilité).

**Étape 3.** Si $n \mid a - b$ et $n \mid b - c$, alors $n$ divise leur somme $(a - b) + (b - c) = a - c$ (propriétés de la divisibilité).

**À retenir : Retenir de la preuve : se ramener à un multiple**

Chaque règle se ramène à un multiple de $n$ : $a - a = 0$, puis $b - a = -(a - b)$, puis $a - c = (a - b) + (b - c)$.

Conséquence pratique : dans une chaîne de congruences de même module, on enchaîne comme avec des égalités.

**Vérifie : La transitivité**

Dans l'étape 3, quelle égalité montre que $n \mid a - c$ ?

**A.** $(a - b) - (b - c) = a - c$

**Faux.**

Faux : on obtient $a - 2b + c$.

**B.** $(a - b)(b - c) = a - c$

**Faux.**

Faux : pour $a = 2, b = 1, c = 0$, le produit vaut $1$ et $a - c = 2$.

**C.** $a - c = a - b$

**Faux.**

Faux dès que $b \neq c$.

**D.** $(a - b) + (b - c) = a - c$

**Juste.**

Juste : une somme de deux multiples de $n$.

**Correction**

Par hypothèse, $n$ divise $a - b$ et $b - c$. D'après les propriétés de la divisibilité, il divise leur somme :

$$(a - b) + (b - c) = a - c.$$

Donc $a \equiv c \ [n]$.

**Exemple : une chaîne de congruences**

On a $47 \equiv 12 \ [5]$, car $47 - 12 = 35 = 5 \times 7$ ; et $12 \equiv 2 \ [5]$, car $12 - 2 = 10 = 5 \times 2$.

Par transitivité, $47 \equiv 2\ [5]$. Contrôle : $47 = 5 \times 9 + 2$.

## Piège et entraînement

**Attention : une congruence sans module ne veut rien dire**

✗ « $22 \equiv 7$ ».

✓ Il faut écrire le module : $22 \equiv 7\ [5]$ est vraie, mais $22 \equiv 7\ [4]$ est fausse.

Et une congruence n'est pas une égalité : $22 \equiv 7\ [5]$, alors que $22 \neq 7$.

**À toi : Vraie ou fausse ?**

Pour chaque proposition, dis si elle est vraie, en justifiant : (a) $53 \equiv -3\ [8]$ ; (b) $-21 \equiv 5\ [9]$ ; (c) $144 \equiv 0\ [12]$. Donne ensuite le reste de $-21$ dans la division par $9$. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Reviens à la définition : calcule chaque différence $a - b$.
**Indice 2**
Cherche si cette différence est un multiple du module.
**Indice 3**
Point délicat : pour le reste de $-21$, le quotient est négatif et le reste doit vérifier $0 \leq r < 9$.

**Réponse**
(a) $53 - (-3) = 56 = 8 \times 7$ : la proposition est vraie.

(b) $-21 - 5 = -26$, et $9 \nmid 26$ : la proposition est fausse.

(c) $144 - 0 = 144 = 12 \times 12$ : la proposition est vraie.

**Reste.** Enfin, $-21 = 9 \times (-3) + 6$, avec $0 \leq 6 < 9$ : le reste de $-21$ dans la division par $9$ est $6$, et $-21 \equiv 6\ [9]$.

## Calculer avec les congruences

### Additionner et multiplier

**Devine : Un reste sans tout calculer**

On a $38 \equiv 3\ [7]$ et $50 \equiv 1\ [7]$. Quel est le reste de $38 \times 50$ dans la division par $7$ ?

**A.** $4$

**Faux.**
$4 = 3 + 1$ : c'est le reste de la somme $38 + 50 = 88$, pas celui du produit.

**B.** $1$

**Faux.**

Tu as gardé le reste de $50$ seulement.

**C.** $3$

**Juste.**

Juste : $3 \times 1 = 3$, et $1900 = 7 \times 271 + 3$.

**D.** $0$

**Faux.**

$7$ ne divise ni $38$ ni $50$, et le reste du produit est celui de $3 \times 1$.

**Correction**

On remplace chaque facteur par son reste :

$$38 \times 50 \equiv 3 \times 1 \ [7],$$

c'est-à-dire $38 \times 50 \equiv 3 \ [7]$. Contrôle : $38 \times 50 = 1900 = 7 \times 271 + 3$.

**Pourquoi est-ce vrai ?** On a $ac - bd = a(c-d) + d(a-b)$ : si $n$ divise $a-b$ et $c-d$, il divise $ac - bd$.

Propriété **: Congruences, addition et multiplication**

Soient $n$ un entier naturel non nul et $a, b, c, d$ des entiers relatifs tels que $a \equiv b \ [n]$ et $c \equiv d \ [n]$. Alors

$$a + c \equiv b + d \ [n], \quad a - c \equiv b - d \ [n] \quad \text{et} \quad ac \equiv bd \ [n].$$

En particulier, $ka \equiv kb \ [n]$ pour tout entier relatif $k$.

---

**Démonstration**

**Étape 1.** On a $(a+c) - (b+d) = (a-b) + (c-d)$ et $(a-c) - (b-d) = (a-b) - (c-d)$. Comme $n$ divise $a-b$ et $c-d$, il divise ces deux nombres (propriétés de la divisibilité).

**Étape 2.** On a $ac - bd = a(c-d) + d(a-b)$. Comme $n$ divise $c-d$ et $a-b$, il divise $ac-bd$ (propriétés de la divisibilité).

**Étape 3.** En prenant $c = d = k$, qui vérifie $k \equiv k \ [n]$ (réflexivité, symétrie, transitivité), l'étape 2 donne $ka \equiv kb \ [n]$.

À retenir **: Retenir de la preuve : ajouter et retrancher**

Tout repose sur deux écritures :

$$\begin{aligned}(a+c) - (b+d) \\ = (a-b) + (c-d), \\ ac - bd \\ = a(c-d) + d(a-b).\end{aligned}$$

Retiens l'usage : dans une somme ou un produit, on peut remplacer chaque nombre par un nombre congru, avec le **même module**.

**Vérifie : Le produit**

Dans l'étape 2 de la preuve, quelle égalité montre que $n$ divise $ac - bd$ ?

**A.** $ac - bd = a(c - d) + d(a - b)$

**Juste.**

Juste : les deux termes sont des multiples de $n$.

**B.** $ac - bd = (a - b)(c - d)$

**Faux.**

Faux : pour $a = 2$ et $b = c = d = 1$, on a $ac - bd = 1$, et $(a - b)(c - d) = 0$.

**C.** $ac - bd = (a - c) + (b - d)$

**Faux.**

Faux : pour $a = c = 2$ et $b = d = 1$, on a $ac - bd = 3$, et $(a - c) + (b - d) = 0$.

**D.** $ac - bd = (a + b)(c - d)$

**Faux.**

Faux : pour $a = b = c = 1$ et $d = 0$, on a $ac - bd = 1$, et $(a + b)(c - d) = 2$.

**Correction**

On ajoute et on retranche $ad$ :

$$\begin{aligned} ac - bd &= ac - ad + ad - bd \\ &= a(c - d) + d(a - b). \end{aligned}$$

Comme $n$ divise $c - d$ et $a - b$, il divise cette combinaison, d'après les propriétés de la divisibilité. Donc $ac \equiv bd \ [n]$.

**Exemple : calculer modulo 7**

On a $38 \equiv 3 \ [7]$. Par compatibilité avec la multiplication :

$$38^2 = 38 \times 38 \equiv 3 \times 3 \ [7],$$

soit $38^2 \equiv 9 \ [7]$, puis $38^2 \equiv 2 \ [7]$, car $9 \equiv 2 \ [7]$. Contrôle : $38^2 = 1444 = 7 \times 206 + 2$.

Pour une puissance quelconque, on répète la multiplication.

**Pourquoi est-ce vrai ?** Une récurrence rend rigoureux ce « on répète $k$ fois ».

## Les puissances

**Propriété : Congruences et puissances**

Soient $n$ un entier naturel non nul, et $a$ et $b$ deux entiers relatifs tels que $a \equiv b\ [n]$. Pour tout entier naturel non nul $k$,

$$a^k \equiv b^k\ [n].$$

**Démonstration**

Raisonnons par récurrence sur l'entier $k \geq 1$.

**Étape 1 (initialisation).** Pour $k = 1$ : $a^1 = a$, $b^1 = b$ et $a \equiv b\ [n]$ par hypothèse.

**Étape 2 (hérédité).** Soit $k \geq 1$ un entier tel que $a^k \equiv b^k\ [n]$. Avec $a \equiv b\ [n]$, la compatibilité avec la multiplication donne $a^k \times a \equiv b^k \times b\ [n]$, c'est-à-dire $a^{k+1} \equiv b^{k+1}\ [n]$.

**Étape 3 (conclusion).** D'après le principe de récurrence, $a^k \equiv b^k\ [n]$ pour tout entier naturel $k \geq 1$.

**À retenir : Retenir de la preuve : la récurrence**

La récurrence transforme « multiplier $k$ fois » en une preuve : l'hérédité multiplie $a^k \equiv b^k\ [n]$ par $a \equiv b\ [n]$.

Retiens l'usage : pour une puissance, on remplace d'abord la base par un nombre congru plus simple, par exemple $1$ ou $-1$.

**Vérifie : L'hérédité**

Dans l'hérédité, quelle propriété permet de passer de $a^k \equiv b^k\ [n]$ à $a^{k+1} \equiv b^{k+1}\ [n]$ ?

**A.** La compatibilité avec l'addition.

**Faux.**

On ne fait aucune somme : $a^{k+1} = a^k \times a$.

**B.** La compatibilité avec la multiplication.

**Juste.**

Juste : on multiplie $a^k \equiv b^k\ [n]$ par $a \equiv b\ [n]$.

**C.** La transitivité, et elle seule.

**Faux.**

La transitivité enchaîne deux congruences ; elle ne fabrique pas un produit.

**D.** La simplification par $a$.

**Faux.**

On ne simplifie pas une congruence en général ; ici, on multiplie.

**Correction**

On multiplie membre à membre $a^k \equiv b^k\ [n]$ et $a \equiv b\ [n]$. La compatibilité avec la multiplication donne

$$a^k \times a \equiv b^k \times b \ [n],$$

c'est-à-dire $a^{k+1} \equiv b^{k+1} \ [n]$.

## Le reste d'une grande puissance

**Méthode : trouver le reste d'une grande puissance**

1. **Calcule** $a$, $a^2$, $a^3$… modulo $n$, en remplaçant chaque résultat par son reste.
2. **Repère** un exposant $k \geq 1$ tel que $a^k \equiv 1 \ [n]$. Un tel exposant n'existe pas toujours : par exemple, $2^k \equiv 0 \ [4]$ pour tout $k \geq 2$. Si aucune puissance ne donne le reste $1$, les étapes suivantes ne s'appliquent pas ; conclus directement, comme ici $2^N \equiv 0 \ [4]$ pour tout $N \geq 2$.
3. **Divise** l'exposant $N$ par $k$ : $N = kq + s$, avec $0 \leq s < k$.
4. **Conclus** : $a^N = (a^k)^q \times a^s$, donc $a^N \equiv a^s \ [n]$ ; puis lis le reste.

**Exemple : Exemple guidé : le jour dans $2^{50}$ jours**

On cherche le reste de $2^{50}$ dans la division par $7$.

**Premières puissances.** $2^1 = 2$, $2^2 = 4$ et $2^3 = 8$, avec $8 \equiv 1 \ [7]$ : on prend $k = 3$.

**Exposant.** $50 = 3 \times 16 + 2$, avec $0 \leq 2 < 3$.

**Calcul.** D'après la propriété des puissances et la compatibilité avec la multiplication :

$$\begin{aligned} 2^{50} &= (2^3)^{16} \times 2^2 \\ &\equiv 1^{16} \times 4 \ [7], \end{aligned}$$

soit $2^{50} \equiv 4 \ [7]$.

**Conclusion.** Le reste est $4$. Lundi plus $4$ jours : dans $2^{50}$ jours, on sera **vendredi**. C'est la réponse à la question d'ouverture du chapitre.

## Un critère de divisibilité

**Méthode : établir un critère de divisibilité**

1. **Écris** l'entier avec ses chiffres : $A = a_k 10^k + \cdots + a_1 \times 10 + a_0$.
2. **Réduis** $10$ modulo $n$, par exemple $10 \equiv 1 \ [9]$ ou $10 \equiv -1 \ [11]$, puis ses puissances.
3. **Remplace** dans l'écriture de $A$ pour obtenir une congruence simple.
4. **Conclus** : $A \equiv 0 \ [n]$ si et seulement si $n \mid A$.

**Exemple : Exemple guidé : la divisibilité par 11**

Comme $10 \equiv -1\ [11]$, on a $10^i \equiv (-1)^i\ [11]$ pour tout entier $i \geq 1$, d'après la propriété des puissances. C'est vrai aussi pour $i = 0$, car $10^0 = 1 = (-1)^0$.

Pour $A = 918082$, on remplace chaque puissance de $10$ :

$$A \equiv 2 - 8 + 0 - 8 + 1 - 9\ [11],$$

soit $A \equiv -22\ [11]$. Or $-22 = 11 \times (-2)$, donc $A \equiv 0\ [11]$ : $11 \mid 918082$.

Contrôle : $918082 = 11 \times 83462$.

**Attention : on ne simplifie pas une congruence**

✗ « $4 \times 5 \equiv 4 \times 2\ [12]$, donc $5 \equiv 2\ [12]$. »

✓ La première congruence est vraie : $20 - 8 = 12$. La seconde est fausse : $5 - 2 = 3$, et $12 \nmid 3$.

Avec les congruences, on additionne, on soustrait, on multiplie, on élève à une puissance ; on ne divise pas.

## À toi

**À toi : Une divisibilité pour tout n**

Montre que, pour tout entier naturel $n$, $7$ divise $3^{2n+1} + 2^{n+2}$. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Écris $3^{2n+1} = 3 \times 9^n$ et $2^{n+2} = 4 \times 2^n$.
**Indice 2**
Réduis $9$ modulo $7$, puis utilise les puissances.
**Indice 3**
Point délicat : écris le module à chaque congruence, jusqu'à la conclusion.

**Réponse**
Soit $n$ un entier naturel.

**Puissances.** On a $9 \equiv 2\ [7]$, donc $9^n \equiv 2^n\ [7]$, d'après la propriété des puissances ; pour $n = 0$, les deux membres valent $1$.

**Réduction.** Par compatibilité avec la multiplication et l'addition :

$$\begin{aligned} &3^{2n+1} + 2^{n+2} \\ &= 3 \times 9^n + 4 \times 2^n \\ &\equiv 3 \times 2^n + 4 \times 2^n\ [7] \\ &\equiv 7 \times 2^n\ [7]. \end{aligned}$$

Or $7 \times 2^n \equiv 0\ [7]$.

**Conclusion.** Pour tout entier naturel $n$, $7$ divise $3^{2n+1} + 2^{n+2}$.

**Remarque : Coin devoir : rédiger un calcul de reste**

En devoir, chaque ligne d'un calcul de reste porte son module et sa justification. Par exemple : « $2^3 \equiv 1\ [7]$, donc $(2^3)^{16} \equiv 1\ [7]$, d'après la propriété des puissances ».

Écris la division de l'exposant, avec son reste.

Termine par une phrase : « le reste de la division de … par … est … », avec un reste compris entre $0$ et $n-1$.

## Classes modulo n et $\mathbb{Z}/n\mathbb{Z}$

### Ranger les entiers

**Devine : Dans quel tiroir ?**

On range tous les entiers relatifs dans quatre tiroirs, selon leur reste dans la division par $4$ : $0$, $1$, $2$ ou $3$. Dans quel tiroir range-t-on $-7$ ?

**A.** Le tiroir $3$.
**Faux.**
On a bien $7 = 4 \times 1 + 3$, mais c'est le reste de $7$. Pour $-7$, le quotient est négatif.

**B.** Aucun : un nombre négatif n'a pas de reste.
**Faux.**
Tout entier relatif a un reste, d'après la division euclidienne.

**C.** Le tiroir $1$.
**Juste.**
Juste : $-7 = 4 \times (-2) + 1$.

**D.** Le tiroir $2$.
**Faux.**
Le reste de $-7$ par $4$ n'est pas $2$ : $-7 - 2 = -9$ n'est pas un multiple de $4$.

**Correction**
$-7 = 4 \times (-2) + 1$, avec $0 \leq 1 < 4$ : le reste est $1$.

Le tiroir $1$ contient $\ldots, -7, -3, 1, 5, 9, \ldots$ : deux voisins diffèrent de $4$. Ces tiroirs sont les **classes** modulo $4$.

**Définition : Classe modulo n ; ensemble $\mathbb{Z}/n\mathbb{Z}$**

Soient $n$ un entier naturel non nul et $a$ un entier relatif. La **classe** de $a$ modulo $n$ est l'ensemble des entiers relatifs congrus à $a$ modulo $n$ :

$$\overline{a} = \{b \in \mathbb{Z} \,/\, b \equiv a\ [n]\} = \{a + kn \,/\, k \in \mathbb{Z}\},$$

car $b \equiv a\ [n]$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $b - a = kn$. L'ensemble des classes modulo $n$ est noté $\mathbb{Z}/n\mathbb{Z}$.

**Exemple : les classes modulo 4**

Modulo $4$ :

$$\overline{1} = \{\dots, -7, -3, 1, 5, 9, \dots\},$$
$$\overline{5} = \{\dots, -3, 1, 5, 9, 13, \dots\}.$$

Ce sont les mêmes ensembles : $\overline{5} = \overline{1}$, et $5 \equiv 1\ [4]$.

**Pourquoi est-ce vrai ?** Si $a \equiv b\ [n]$, tout entier congru à $a$ est congru à $b$, par transitivité. Et tout entier est congru à son reste.

## Décrire Z/nZ

**Propriété : Description de $\mathbb{Z}$/n$\mathbb{Z}$**

Soit $n$ un entier naturel non nul. Pour tous entiers relatifs $a$ et $b$,

$$\overline{a} = \overline{b} \Leftrightarrow a \equiv b\ [n].$$

De plus, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, et ces $n$ classes sont deux à deux distinctes.

---

**Démonstration**

**Étape 1.** Supposons $\overline{a} = \overline{b}$. Comme $a \equiv a\ [n]$ (réflexivité, symétrie, transitivité), $a \in \overline{a} = \overline{b}$, donc $a \equiv b\ [n]$ (définition des classes).

**Étape 2.** Réciproquement, supposons $a \equiv b\ [n]$. Si $c \in \overline{a}$, alors $c \equiv a$ et $a \equiv b\ [n]$, donc $c \equiv b\ [n]$ (réflexivité, symétrie, transitivité) : $c \in \overline{b}$. Ainsi $\overline{a} \subset \overline{b}$ ; comme $b \equiv a\ [n]$ (réflexivité, symétrie, transitivité), de même $\overline{b} \subset \overline{a}$.

**Étape 3.** Soit $a$ un entier relatif, de reste $r$ dans la division par $n$. Alors $a \equiv r\ [n]$ (congruence et reste), donc $\overline{a} = \overline{r}$ (étape 2), avec $0 \leq r \leq n-1$.

**Étape 4.** Si $0 \leq r < r' \leq n-1$, les restes de $r$ et $r'$ par $n$ sont $r$ et $r'$, différents : $r \not\equiv r'\ [n]$ (congruence et reste), donc, par contraposée de l'étape 1, $\overline{r} \neq \overline{r'}$.

**À retenir : Retenir de la preuve : la classe du reste**

Deux classes sont égales dès que leurs représentants sont congrus : on prouve deux inclusions, avec la transitivité.

Chaque entier est dans la classe de son reste. Il y a donc exactement $n$ classes, celles de $0, 1, \dots, n-1$.

**Vérifie : Combien de classes ?**

Combien l'ensemble $\mathbb{Z}/6\mathbb{Z}$ a-t-il d'éléments ?

**A.** Une infinité, car $\mathbb{Z}$ est infini.

**Faux.**

Chaque classe contient une infinité d'entiers, mais il n'y a que $6$ classes.

**B.** $5$ : $\overline{1}, \dots, \overline{5}$.

**Faux.**

Tu as oublié $\overline{0}$, la classe des multiples de $6$.

**C.** $7$ : $\overline{0}, \dots, \overline{6}$.

**Faux.**

$\overline{6} = \overline{0}$, car $6 \equiv 0\ [6]$ : ces deux classes n'en font qu'une.

**D.** $6$ : $\overline{0}, \dots, \overline{5}$.

**Juste.**

Juste : les restes possibles sont $0, 1, \dots, 5$.

**Correction**

D'après la description de $\mathbb{Z}/n\mathbb{Z}$,

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\},$$

et ces classes sont deux à deux distinctes. Il y a $6$ éléments.

**Exemple : l'ensemble Z/3Z**

$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. Modulo $3$ : $\overline{10} = \overline{1}$, $\overline{-1} = \overline{2}$ et $\overline{3} = \overline{0}$.

En revanche, $\overline{1} \neq \overline{2}$, car $3 \nmid 2 - 1$.

**À toi : Un représentant entre 0 et 5**

Dans $\mathbb{Z}/6\mathbb{Z}$, écris $\overline{27}$, $\overline{-15}$ et $\overline{100}$ sous la forme $\overline{r}$, avec $0 \leq r \leq 5$. Deux de ces classes sont-elles égales ? Écris ta réponse avant de dévoiler la correction.

**Indice 1**

Pour chaque entier, écris sa division euclidienne par $6$.

**Indice 2**
Pour $-15$, le quotient est $-3$.
**Indice 3**
Point délicat : deux classes sont égales si et seulement si leurs représentants sont congrus modulo $6$.

**Réponse**
**Restes.**

- $27 = 6 \times 4 + 3$, donc $\overline{27} = \overline{3}$ ;
- $-15 = 6 \times (-3) + 3$, donc $\overline{-15} = \overline{3}$ ;
- $100 = 6 \times 16 + 4$, donc $\overline{100} = \overline{4}$.

**Conclusion.** $\overline{27} = \overline{-15}$, car $27 - (-15) = 42 = 6 \times 7$. La troisième classe, $\overline{100} = \overline{4}$, est différente des deux autres.

## Calculer dans $\mathbb{Z}/n\mathbb{Z}$

## Additionner des classes

**Devine : Le choix du représentant**

Dans $\mathbb{Z}/5\mathbb{Z}$, on veut définir $\overline{3} + \overline{4}$. Avec les représentants $3$ et $4$, on obtient $\overline{7}$. Avec les représentants $8$ et $9$ des mêmes classes, que trouve-t-on ?

**A.** $\overline{17}$, une classe différente de $\overline{7}$.
**Faux.**
$17 - 7 = 10$ est un multiple de $5$ : $\overline{17} = \overline{7}$.

**B.** $\overline{17}$, la même classe que $\overline{7}$.
**Juste.**
Juste : $17 \equiv 7\ [5]$, et ces deux classes valent $\overline{2}$.

**C.** $\overline{12}$, car on ajoute $8$ et $4$.
**Faux.**
On ajoute les représentants choisis, $8$ et $9$ : $8 + 9 = 17$.

**D.** Un résultat qui dépend des représentants choisis.
**Faux.**
C'est la crainte légitime ; la propriété qui suit montre que le résultat n'en dépend pas.

**Correction**
On a $8 \equiv 3\ [5]$ et $9 \equiv 4\ [5]$. On trouve $8 + 9 = 17$, et $17 \equiv 7\ [5]$ :

$$\overline{17} = \overline{7} = \overline{2}.$$

Le résultat ne dépend pas des représentants choisis.

**Pourquoi est-ce vrai ?** Les congruences sont compatibles avec l'addition et la multiplication : changer de représentants ne change pas la classe du résultat.

**Propriété : Addition et multiplication dans $\mathbb{Z}$/n$\mathbb{Z}$**

Soit $n$ un entier naturel non nul. Si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

On définit donc, dans $\mathbb{Z}/n\mathbb{Z}$,

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a} \times \overline{b} = \overline{ab},$$

et le résultat ne dépend pas des entiers $a$ et $b$ choisis pour représenter les classes.

**Démonstration**

**Étape 1.** D'après la description de $\mathbb{Z}$/n$\mathbb{Z}$, les hypothèses s'écrivent $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$.

**Étape 2.** Par compatibilité des congruences avec l'addition et la multiplication, $a + b \equiv a' + b' \ [n]$ et $ab \equiv a'b' \ [n]$.

**Étape 3.** Par la description de $\mathbb{Z}$/n$\mathbb{Z}$, $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

**À retenir : Retenir de la preuve : le choix des représentants**

Une opération sur des classes se définit à l'aide de représentants. Avant de l'utiliser, on vérifie que le résultat **ne dépend pas** des représentants choisis.

Ici, la compatibilité des congruences fait tout le travail.

**Vérifie : Le premier pas**

Dans l'étape 1 de la preuve, quelle propriété traduit $\overline{a} = \overline{a'}$ en $a \equiv a' \ [n]$ ?

**A.** La description de $\mathbb{Z}/n\mathbb{Z}$.
**Juste.**
Juste : $\overline{a} = \overline{b}$ si et seulement si $a \equiv b \ [n]$.

**B.** La compatibilité avec l'addition.
**Faux.**
Elle sert à l'étape 2, pour $a + b$.

**C.** La définition de la divisibilité.
**Faux.**
Elle se cache dans la définition de la congruence ; ici, on passe d'une égalité de classes à une congruence.

**D.** La division euclidienne de $a$ par $n$.

**Faux.**
Aucune division n'est écrite dans cette preuve.

**Correction**
La description de $\mathbb{Z}/n\mathbb{Z}$ dit : $\overline{a} = \overline{b}$ si et seulement si $a \equiv b\ [n]$.

L'étape 1 l'emploie dans le sens « égalité de classes, donc congruence ». L'étape 3 l'emploie dans l'autre sens.

## Règles et tables

**Propriété : Règles de calcul dans $\mathbb{Z}$/n$\mathbb{Z}$**

Soit $n$ un entier naturel non nul. Pour toutes classes $x$, $y$ et $z$ de $\mathbb{Z}/n\mathbb{Z}$ :

1. $x + y = y + x$ et $x \times y = y \times x$ ;
2. $(x + y) + z = x + (y + z)$ et $(x \times y) \times z = x \times (y \times z)$ ;
3. $x \times (y + z) = x \times y + x \times z$ ;
4. $x + \overline{0} = x$, $x \times \overline{1} = x$, et $\overline{a} + \overline{-a} = \overline{0}$ pour tout entier relatif $a$.

**Démonstration**
Idée de la preuve. On écrit $x = \overline{a}$, $y = \overline{b}$ et $z = \overline{c}$ (description de $\mathbb{Z}$/n$\mathbb{Z}$), puis on calcule avec la définition des opérations (opérations dans $\mathbb{Z}$/n$\mathbb{Z}$) : par exemple, $x \times (y + z) = \overline{a(b + c)} = \overline{ab + ac} = x \times y + x \times z$, car la règle correspondante est vraie dans $\mathbb{Z}$. Étapes omises : les calculs, identiques, des autres règles.

**Exemple : les tables de $\mathbb{Z}/4\mathbb{Z}$**

**Une preuve esquissée.** La preuve est seulement esquissée : une seule règle est calculée ; les autres se vérifient de la même façon.

Addition et multiplication dans $\mathbb{Z}/4\mathbb{Z}$ :

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |

| $\times$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |

| $\times$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{0}$ | $\overline{2}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Par exemple, $\overline{3} \times \overline{3} = \overline{9} = \overline{1}$, et $\overline{2} \times \overline{2} = \overline{0}$.

## Résoudre une équation

**Méthode : résoudre une équation dans Z/nZ**

1. **Liste** les $n$ classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.
2. **Calcule** le membre de gauche pour chaque classe, en réduisant chaque résultat modulo $n$, ou lis une table.
3. **Garde** les classes qui conviennent : il peut n'y en avoir aucune, une ou plusieurs.
4. **Traduis** au besoin dans $\mathbb{Z}$ : la solution $\overline{r}$ correspond aux entiers $x$ tels que $x \equiv r\ [n]$.

**Exemple : Exemple guidé : une équation dans Z/8Z**

On résout $x^2 = \overline{1}$ dans $\mathbb{Z}/8\mathbb{Z}$ en essayant les huit classes :

| $x$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{7}$ |
|---|---|---|---|---|---|---|---|---|
| $x^2$ | $\overline{0}$ | $\overline{1}$ | $\overline{4}$ | $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{4}$ | $\overline{1}$ |

Par exemple, $\overline{5}^2 = \overline{25} = \overline{1}$, car $25 = 8 \times 3 + 1$.

**Conclusion.** Les solutions sont $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$ : quatre solutions, et non deux comme dans $\mathbb{R}$.

**Attention : un produit nul sans facteur nul**

✗ « Dans $\mathbb{Z}/10\mathbb{Z}$, $x \times \overline{5} = \overline{0}$, donc $x = \overline{0}$. »

✓ $\overline{2} \times \overline{5} = \overline{10} = \overline{0}$, alors que $\overline{2} \neq \overline{0}$. Dans $\mathbb{Z}/n\mathbb{Z}$, un produit peut être nul sans qu'aucun facteur ne le soit.

Ici, les solutions sont $\overline{0}$, $\overline{2}$, $\overline{4}$, $\overline{6}$ et $\overline{8}$.

## À toi

> **À toi : Une équation dans Z/6Z**

Résous dans $\mathbb{Z}/6\mathbb{Z}$ l'équation $x^2 + \overline{2}x = \overline{3}$. Traduis ensuite le résultat par une condition sur un entier $n$. Écris ta réponse avant de dévoiler la correction.

**Indice 1**
Essaie les six classes, de $\overline{0}$ à $\overline{5}$.
**Indice 2**
Pour $x = \overline{3}$ : $\overline{9} + \overline{6} = \overline{15}$ ; réduis modulo $6$.
**Indice 3**
Point délicat : une solution $\overline{r}$ correspond à tous les entiers $n$ tels que $n \equiv r\ [6]$.

**Réponse**
**Essais.**

| $x$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|---|
| $x^2 + \overline{2}x$ | $\overline{0}$ | $\overline{3}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ | $\overline{5}$ |

**Solutions.** Les solutions dans $\mathbb{Z}/6\mathbb{Z}$ sont $\overline{1}$ et $\overline{3}$.

**Conclusion.** Pour tout entier $n$, $n^2 + 2n \equiv 3\ [6]$ si et seulement si $n \equiv 1\ [6]$ ou $n \equiv 3\ [6]$.

**Remarque : Coin devoir : rédiger une résolution dans Z/nZ**

En devoir, une résolution dans $\mathbb{Z}/n\mathbb{Z}$ se présente en trois temps :

1. un tableau des $n$ classes, avec chaque calcul réduit modulo $n$ ;
2. la conclusion : « l'ensemble des solutions est … » ;
3. si l'énoncé porte sur des entiers, la traduction par des congruences, module écrit.

## Synthèse

**À retenir : quel outil pour quelle question**

- « Montrer que $a$ divise $b$ » : écrire $b = ka$, ou combiner deux divisibilités.
- Une propriété de tout entier $n$ : raisonner selon les restes, ou par récurrence.
- « $n$ est-il premier ? » : tester les nombres premiers $p$ tels que $p^2 \leq n$.
- Diviseurs, PGCD et PPCM d'entiers donnés : les décompositions.
- PGCD de grands nombres ou d'expressions en $n$ : l'algorithme d'Euclide.
- Un reste, une divisibilité par $n$ : les congruences modulo $n$.
- Une équation dans $\mathbb{Z}/n\mathbb{Z}$ : essayer les $n$ classes.

**Le mot du prof.** Tu sais maintenant démontrer qu'un entier en divise un autre, et calculer un reste sans écrire de nombres gigantesques.

Ces outils reviendront à l'examen de 2BAC SM, enrichis de nouveaux théorèmes. Garde l'habitude prise ici : chaque congruence avec son module, chaque cas annoncé.

SOURCES

Référentiel BURHAN du chapitre « Arithmétique dans $\mathbb{Z}$ » (1bac · sciences-mathematiques · mathematiques)