BURHAN

Résumé : Arithmétique dans $\mathbb{Z}$

1ère Année Baccalauréat · Sciences Mathématiques · Mathématiques

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

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

Divisibilité dans $\mathbb{Z}$

> **À retenir : Le réflexe : un facteur entier exact**
>
> $a \mid b$ se lit « a divise b » : on obtient b en multipliant a par un entier. Ainsi $-6 \mid 42$, car $42 = (-7) \times (-6)$.
>
> Tout entier divise 0, car $0 = 0 \times a$; en revanche, 0 ne divise que 0. Un entier et son opposé ont les mêmes diviseurs.

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 $a \nmid b$.

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 $a \mid bu + cv$.

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 $a = -b$.

Méthode : montrer une divisibilité

1. **Exhibe** l'entier k : écris $b = ka$, avec k entier et explicite.

2. **Combine** deux divisibilités connues : si $a \mid b$ et $a \mid c$, alors a divise $bu + cv$. Choisis u et v pour faire apparaître l'expression voulue.
3. **Pour une expression en** n : factorise, raisonne selon les restes, par récurrence ou par congruences.
4. **Conclus** en nommant la propriété utilisée.

Exemple

Énoncé. Soient a et b deux entiers tels que $7 \mid a + 2b$. Montre que $7 \mid 3a - b$.

Combinaison. On écrit $3a - b = 3(a + 2b) - 7b$. En effet :

$$\begin{aligned} 3(a+2b) - 7b &= 3a + 6b - 7b \\ &= 3a - b. \end{aligned}$$

Conclusion. 7 divise $a + 2b$, et 7 divise $7b$. Par combinaison linéaire, 7 divise $3(a + 2b) - 7b$, donc $7 \mid 3a - b$.

Attention : La divisibilité n'est pas un quotient

$a \mid b$ est une affirmation, vraie ou fausse ; ce n'est pas un nombre. N'écris pas $4 \mid 28 = 7$: écris $28 = 7 \times 4$, donc $4 \mid 28$.

Ne confonds pas non plus $a \mid b$ et $b \mid a$: $4 \mid 28$, mais $28 \nmid 4$.

Division euclidienne et raisonnement selon les restes

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 $r = 0$.

À retenir : Diviser un entier négatif

Pour un dividende négatif, le quotient est négatif, et le reste, lui, est positif ou nul.

Encadre d'abord a entre deux multiples consécutifs de b :

$$bq \leq a < b(q + 1).$$

Le reste vaut alors $r = a - bq$, et il vérifie $0 \leq r < b$.

Exemple

Énoncé. Effectue la division euclidienne de -47 par 6.

Encadrement. $6 \times (-8) = -48$ et $6 \times (-7) = -42$, donc $-48 \leq -47 < -42$.

Résultat. $-47 = 6 \times (-8) + 1$, avec $0 \leq 1 < 6$: le quotient est -8 et le reste est 1.

Attention : Un reste n'est jamais négatif

L'égalité $-47 = 6 \times (-7) - 5$ est juste, mais ce n'est pas la division euclidienne : le reste doit vérifier $0 \leq r < 6$.

De même, $50 = 6 \times 7 + 8$ ne convient pas, car $8 \geq 6$.

Méthode : raisonner selon les restes

1. **Choisis** le diviseur b qui convient : 2 pour la parité, 3, 4 ou un autre selon la question.
2. **Annonce** les b cas : d'après la division euclidienne, $n = bq + r$ avec $r \in \{0, 1, \ldots, b-1\}$.
3. **Remplace** n par $bq + r$ dans chaque cas, puis calcule.
4. **Conclus** : les cas couvrent tous les entiers, donc la propriété vaut pour tout n.

Exemple

Énoncé. Montre que, pour tout $n \in \mathbb{Z}$, $3 \nmid n^2 + 1$.

Cas. Soit $n \in \mathbb{Z}$, et $n = 3q + r$ sa division euclidienne par 3, avec $r \in \{0, 1, 2\}$.

- Si $r = 0$: $n^2 + 1 = 3(3q^2) + 1$.
- Si $r = 1$: $n^2 + 1 = 3(3q^2 + 2q) + 2$.
- Si $r = 2$: $n^2 + 1 = 3(3q^2 + 4q + 1) + 2$.

Conclusion. Le reste de $n^2 + 1$ par 3 vaut 1 ou 2, jamais 0. Donc $3 \nmid n^2 + 1$.

Nombres premiers

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 $1 < d < n$.

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.

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.

Théorème : Infinité des nombres premiers

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

Méthode : tester la primalité d'un entier

1. **Liste**, pour un entier $n \geq 2$, les nombres premiers p tels que $p^2 \leq n$; arrête-toi dès qu'un carré dépasse n.
2. **Teste** si chacun d'eux divise n, par une division euclidienne.
3. **Conclus** : si l'un d'eux divise n, alors n est composé, car $1 < p < n$; si aucun ne le divise, n est premier, d'après le test de primalité.

Exemple

Énoncé. L'entier 251 est-il premier ?

Bornes. $13^2 = 169 \leq 251$ et $17^2 = 289 > 251$. On teste donc 2, 3, 5, 7, 11 et 13.

Tests.

$$\begin{aligned} 251 &= 2 \times 125 + 1 \\ &= 3 \times 83 + 2 \\ &= 5 \times 50 + 1 \\ &= 7 \times 35 + 6 \\ &= 11 \times 22 + 9 \\ &= 13 \times 19 + 4. \end{aligned}$$

Conclusion. Aucun de ces nombres premiers ne divise 251 : il est premier.

Attention : Ni 1, ni tout nombre impair

1 n'est pas premier : il n'a qu'un seul diviseur positif. Un nombre impair n'est pas forcément premier : $91 = 7 \times 13$.

Enfin, le test s'arrête dès que $p^2 > n$; tester au-delà ne sert à rien.

Décomposition en facteurs premiers et diviseurs

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 $n = p_1 p_2 \cdots p_k$.

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

Ce résultat est admis. Tu l'utilises librement pour comparer deux décompositions ou pour lister les diviseurs d'un entier.

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

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$

avec $0 \leq \beta_i \leq \alpha_i$ pour tout i. Le nombre de diviseurs positifs de n est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Méthode : décomposer, puis compter les diviseurs

1. **Divise** n par 2 autant de fois que possible, puis par 3, par 5, par 7, et ainsi de suite.
2. **Recommence** avec chaque quotient, jusqu'au quotient 1.
3. **Contrôle** que chaque facteur est premier, puis regroupe : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

4. **Compte** les diviseurs positifs : il y en a $(\alpha_1+1)\cdots(\alpha_r+1)$.

Exemple

Énoncé. Décompose $1\,400$ et donne son nombre de diviseurs positifs.

Divisions.

$$\begin{aligned} 1\,400 &= 2 \times 700 \\ &= 2^2 \times 350 \\ &= 2^3 \times 175, \end{aligned}$$

puis

$$\begin{aligned} 175 &= 5 \times 35 \\ &= 5^2 \times 7. \end{aligned}$$

Décomposition. $1\,400 = 2^3 \times 5^2 \times 7$.

Diviseurs. Le nombre de diviseurs positifs de $1\,400$ est

$$(3+1)(2+1)(1+1) = 24.$$

Attention : Des facteurs premiers, et seulement eux

$1\,400 = 8 \times 175$ n'est pas une décomposition : ni 8 ni 175 ne sont premiers. Continue tant qu'un facteur se décompose encore.

Dans le décompte des diviseurs, n'oublie pas l'exposant 1 : le facteur $7 = 7^1$ apporte $1+1=2$.

PGCD et algorithme d'Euclide

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 $\operatorname{pgcd}(a,b)$. C'est un entier naturel non nul.

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 $b \wedge 0 = b$.

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** : $a \wedge b = r_{m-1}$.

Méthode : l'algorithme d'Euclide

1. **Écris** la division de a par b : $a = bq_1 + r_1$, avec $0 \leq r_1 < b$.
2. **Décale** : divise b par r_1, puis r_1 par le nouveau reste, et continue ainsi.
3. **Arrête-toi** au premier reste égal à 0 : le reste précédent, non nul, est $a \wedge b$. Cas particulier : quand b divise a, la toute première division a un reste nul, et $a \wedge b = b$.
4. **Aligne** les égalités en colonne : chaque ligne se vérifie d'un coup d'œil.

Exemple

Énoncé. Calcule $1\,078 \wedge 322$.

Divisions successives.

$$\begin{aligned} 1\,078 &= 322 \times 3 + 112 \\ 322 &= 112 \times 2 + 98 \\ 112 &= 98 \times 1 + 14 \\ 98 &= 14 \times 7 + 0 \end{aligned}$$

Conclusion. Le dernier reste non nul est 14 : $1\,078 \wedge 322 = 14$.

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 $a \wedge b$.

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

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

À retenir : Ce que donne le PGCD

Les diviseurs communs à $1\,078$ et à 322 sont donc les diviseurs de 14 : ± 1, ± 2, ± 7 et ± 14.

En multipliant par 5, on obtient sans calcul $5\,390 \wedge 1\,610 = 5 \times 14 = 70$.

PPCM ; calculs par les décompositions

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 $\operatorname{ppcm}(a, b)$.

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 $a \vee b$.

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 :

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

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

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

Méthode : PGCD et PPCM par les décompositions

1. **Décompose** a et b, puis écris-les avec les mêmes nombres premiers, quitte à mettre un exposant nul.
2. **PGCD** : pour chaque nombre premier, garde le plus petit des deux exposants.
3. **PPCM** : garde le plus grand des deux exposants.
4. **Contrôle** le résultat avec $(a \wedge b)(a \vee b) = ab$.

Exemple

Énoncé. Calcule $360 \wedge 756$ et $360 \vee 756$.

Décompositions. Avec les mêmes nombres premiers :

$$360 = 2^3 \times 3^2 \times 5 \times 7^0,$$
$$756 = 2^2 \times 3^3 \times 5^0 \times 7.$$

PGCD. On garde les plus petits exposants : $360 \wedge 756 = 2^2 \times 3^2 = 36$.

PPCM. On garde les plus grands exposants :

$$\begin{aligned} 360 \vee 756 &= 2^3 \times 3^3 \times 5 \times 7 \\ &= 7\,560. \end{aligned}$$

Contrôle.

$$\begin{aligned} 36 \times 7\,560 &= 272\,160 \\ &= 360 \times 756. \end{aligned}$$

Attention : Ne pas échanger les exposants

Le PGCD prend le **plus petit** exposant, le PPCM le **plus grand**.

Un nombre premier absent de l'un des deux entiers y a l'exposant 0 : il disparaît du PGCD. Ici, 5 et 7 ne divisent pas $360 \wedge 756$.

Congruences modulo n

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 ».

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 $n \mid a$.

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 $a \equiv c\ [n]$.

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

$$\begin{aligned} a + c &\equiv b + d\ [n], \\ a - c &\equiv b - d\ [n], \\ ac &\equiv bd\ [n]. \end{aligned}$$

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

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,

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

Définition

$$a \equiv b\ [n] \Leftrightarrow n \mid a - b$$

Reste

$$a = nq + r \text{ et } 0 \leq r < n \Rightarrow a \equiv r\ [n]$$

Divisibilité

$$a \equiv 0\ [n] \Leftrightarrow n \mid a$$

Somme

$$a \equiv b\ [n] \text{ et } c \equiv d\ [n] \Rightarrow a + c \equiv b + d\ [n]$$

Produit

$$a \equiv b\ [n] \text{ et } c \equiv d\ [n] \Rightarrow ac \equiv bd\ [n]$$

Puissance

$$a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n] \quad (k \in \mathbb{N}^*)$$

Attention : Toujours écrire le module

Une congruence sans module n'a pas de sens : écris toujours $[n]$. Une congruence n'est pas une égalité : $23 \equiv 2\ [7]$, alors que $23 \neq 2$.

Un entier est même congru à une infinité d'autres : 2, 9, 16, 23, et ainsi de suite, modulo 7.

Attention : On ne divise pas une congruence

De $ka \equiv kb\ [n]$, tu ne peux pas déduire $a \equiv b\ [n]$ en général.

Par exemple, $4 \times 5 \equiv 4 \times 2\ [12]$, car $20 - 8 = 12$. Pourtant $5 \not\equiv 2\ [12]$.

Les opérations permises sont l'addition, la soustraction, la multiplication et la puissance.

Restes de puissances et critères de divisibilité

Méthode : le reste d'une grande puissance

1. **Calcule** $a, a^2, a^3, \ldots$ modulo n, en réduisant chaque résultat.
2. **Repère** un exposant $k \geq 1$ tel que $a^k \equiv 1\ [n]$. Il peut manquer : modulo 4, on a $2^k \equiv 0\ [4]$ dès que $k \geq 2$. Les étapes suivantes ne s'appliquent alors pas ; conclus directement, 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** : $a^N = (a^k)^q \times a^s \equiv a^s\ [n]$, puis lis le reste.

Exemple

Énoncé. Trouve le reste de la division euclidienne de 7^{1001} par 9.

Premières puissances. $7^2 = 49 \equiv 4\ [9]$, puis

$$\begin{aligned} 7^3 = 7^2 \times 7 &\equiv 4 \times 7\ [9] \\ &\equiv 28\ [9] \\ &\equiv 1\ [9]. \end{aligned}$$

Exposant. $1\,001 = 3 \times 333 + 2$, avec $0 \leq 2 < 3$.

Conclusion. D'après la propriété des puissances :

$$\begin{aligned} 7^{1001} &= (7^3)^{333} \times 7^2 \\ &\equiv 1 \times 4\ [9]. \end{aligned}$$

Le reste cherché est 4.

Méthode : établir un critère de divisibilité

1. **Écris** N avec ses chiffres : $N = a_k 10^k + \cdots + a_1 \times 10 + a_0$.
2. **Réduis** 10 modulo n, puis ses puissances : par exemple $10 \equiv 1\ [9]$ et $10 \equiv -1\ [11]$.
3. **Remplace** dans l'écriture de N, grâce à la compatibilité avec la somme et le produit.
4. **Conclus** : $n \mid N$ si et seulement si $N \equiv 0\ [n]$.

Exemple

Énoncé. Montre que 11 divise $82\,918$.

Réduction. $10 \equiv -1\ [11]$, donc $10^k \equiv (-1)^k\ [11]$ pour tout $k \in \mathbb{N}^*$, et $10^0 = 1 = (-1)^0$.

Calcul. On écrit l'entier avec ses chiffres :

$$\begin{aligned} 82\,918 &= 8 \times 10^4 + 2 \times 10^3 \\ &\quad + 9 \times 10^2 + 1 \times 10 + 8. \end{aligned}$$

Donc

$$82\,918 \equiv 8 - 2 + 9 - 1 + 8\ [11],$$

soit $82\,918 \equiv 22\ [11]$.

Conclusion. $22 = 11 \times 2$, donc $82\,918 \equiv 0\ [11]$ et $11 \mid 82\,918$.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$

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 :

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

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 $\mathbb{Z}/n\mathbb{Z}$.

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.

Exemple

Classes modulo 4. On a

$$\overline{3} = \{\dots, -5, -1, 3, 7, 11, \dots\},$$

et $\overline{-1} = \overline{3}$, car $3 - (-1) = 4$. Ainsi $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Par exemple, $\overline{14} = \overline{2}$, car $14 = 4 \times 3 + 2$.

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 $\mathbb{Z}/n\mathbb{Z}$,

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

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

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.

Exemple

Table de multiplication de $\mathbb{Z}/5\mathbb{Z}$. Chaque case contient la classe du produit, réduite modulo 5.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Hors de la ligne et de la colonne de $\overline{0}$, aucune case ne contient $\overline{0}$.

Méthode : résoudre une équation dans $\mathbb{Z}/n\mathbb{Z}$

1. **Liste** les représentants $0, 1, \ldots, n-1$: chaque classe de $\mathbb{Z}/n\mathbb{Z}$ en a un.
2. **Évalue** l'expression en chacun d'eux, avec un résultat réduit modulo n ; une table déjà dressée fait gagner du temps.
3. **Retiens** toutes les classes qui vérifient l'équation : zéro, une ou plusieurs sont possibles.

4. **Reviens** dans $\mathbb{Z}$ si l'énoncé le demande : $\overline{x} = \overline{r}$ équivaut à $x \equiv r\ [n]$.

Exemple

Énoncé. Résous l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/8\mathbb{Z}$.

Essais.

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

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

Attention : Un produit nul sans facteur nul

Dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{2} \times \overline{2} = \overline{4} = \overline{0}$, alors que $\overline{2} \neq \overline{0}$.

La règle « un produit est nul si et seulement si un facteur est nul » ne vaut donc pas dans tout $\mathbb{Z}/n\mathbb{Z}$. Essaie chaque classe au lieu de factoriser.

Quel outil pour quelle question ?

Méthode : Quel outil pour quelle question ?

Repère la forme de la question, puis choisis l'outil.

On te demande	Outil à essayer
$a \mid b$, avec a et b donnés	écrire $b = ka$, ou effectuer la division euclidienne
un multiple de d qui dépend de n	factorisation, combinaison linéaire, cas selon les restes, récurrence, congruences
les diviseurs communs à deux expressions en n	combinaison qui élimine n, puis diviseurs du nombre obtenu
si n est premier	test des nombres premiers p tels que $p^2 \leq n$
les diviseurs de n, ou leur nombre	décomposition en facteurs premiers
un PGCD	algorithme d'Euclide, ou décompositions et plus petits exposants
un PPCM	décompositions et plus grands exposants, ou $(a \wedge b)(a \vee b) = ab$
le reste d'une grande puissance	congruences, avec un exposant k tel que $a^k \equiv 1\ [n]$
un critère de divisibilité	réduire 10 modulo n
une équation dans $\mathbb{Z}/n\mathbb{Z}$	essayer les n classes, ou lire une table
une propriété pour tout $n \geq n_0$	récurrence, si l'on relie le rang $n+1$ au rang n

À retenir : Rédiger en devoir

Introduis chaque entier avant de t'en servir : « Soit $n \in \mathbb{Z}$ ». Écris toujours le module d'une congruence, et la condition $0 \leq r < b$ d'un reste.

Annonce les cas et vérifie qu'ils couvrent tous les entiers. Nomme le résultat utilisé : « par l'algorithme d'Euclide », « d'après le test de primalité ».