

4.1 Divisibilité dans \mathbb{Z}

4.1.1 Quelques notations

- * \mathbb{N} est l'ensemble des entiers naturels : $\mathbb{N} = \{0; 1; 2; 3 \dots\}$.
- * \mathbb{Z} est l'ensemble des entiers relatifs : $\mathbb{Z} = \{\dots; -3; -2; -1; 0; 1; \dots\}$.
- * \implies est la notation mathématique de l'implication.
- * \iff est la notation mathématique de l'équivalence.
- * \forall est le symbole mathématique de « pour tout ».
- * $\llbracket 1; n \rrbracket = \{1; 2; 3; 4 \dots; n\}$.

4.1.2 Diviseurs, multiples

Définition 1.4.

Soient a et b deux entiers relatifs avec $b \neq 0$.

Dire que b *divise* a (ou que a est un *multiple* de b) signifie qu'il existe un entier relatif k tel que :

$$a =$$

Remarque.

0 est un multiple de **tout** entier car $0 = n \times 0$ pour tout entier n . En revanche, 0 n'est un diviseur d'aucun nombre !

Exemple 1.4.

21 est un multiple de -7 : en effet, $21 = -7 \times (-3)$.

Application 2.4.

1. Soit p et q deux entiers relatifs. Montrer que $18p^2 - 9q$ est divisible par 9.
2. Déterminer les entiers naturels n tels que 5 divise $n + 11$.
3. Montrer que, quelque soit l'entier relatif n , $6n + 7$ n'est jamais divisible par 3.

Propriété 1.4.

Soient a et b deux entiers relatifs avec $b \neq 0$. On a les implications suivantes :

- Si b divise a alors les *multiples* de a sont des *multiples* de b .
- Si b divise a alors les *diviseurs* de b sont des *diviseurs* de a .

► Note 1.4.

L'ensemble des multiples d'un entier relatif b dans \mathbb{Z} est noté $b\mathbb{Z}$ et l'ensemble des diviseurs de b est noté $\mathcal{D}(b)$

Exemple 2.4.

Les multiples de 6 sont aussi des multiples de 3 donc $6\mathbb{Z} \subset 3\mathbb{Z}$.

🔖 Application 3.4. Déterminer, dans \mathbb{Z} , la liste des diviseurs de 7 et en déduire les entiers relatifs n tels que $4n + 1$ divise 7.

Propriété 2.4.

Soient a et b deux entiers relatifs avec $b \neq 0$.

$$b|a \iff -b|a \iff b|-a \iff -b|-a.$$

Conséquence : a et $-a$ ont les mêmes diviseurs dans \mathbb{Z} . Les diviseurs de $-a$ étant les opposés des diviseurs positifs de a , on restreindra souvent l'étude à la divisibilité dans \mathbb{N} .

Démonstration.

□

Propriété 3.4.

Tout entier n non nul a pour **diviseurs** 1, -1 , n et $-n$ et a un nombre fini de diviseurs tous compris entre n et $-n$.

Remarque.

Un entier *non nul* a une infinité de multiples.

4.1.3 Divisibilité et transitivité**Propriété 4.4.**

Soient a , b et c des entiers relatifs tels que $b \neq 0$ et $c \neq 0$.

Si c divise b et b divise a , alors c divise a .

Démonstration. Par hypothèse, c divise b donc il existe un entier relatif k tel que $b = kc$.
 De même, b divise a , il existe donc un entier relatif k' tel que $a = k'b$.
 Ainsi $a = k'kc$ où kk' est un entier relatif.
 Donc a est un multiple de c , avec c non nul, autrement dit c divise a . \square

4.1.4 Divisibilité et combinaison linéaire

Propriété 5.4.

Soient a , b et c des entiers relatifs tels que $c \neq 0$.

Si c est un diviseur commun à a et b , alors c divise $ua + vb$ pour tous entiers relatifs u et v .

Démonstration. Si c est un diviseur commun de a et b alors il existe deux entiers relatifs a' et b' tels que $a = a'c$ et $b = b'c$.

Par conséquent, pour u et v entiers relatifs quelconques,

$$\begin{aligned} ua + vb &= u(a'c) + v(b'c) \\ &= (ua' + vb')c \\ &= kc \end{aligned}$$

où k est un entier.

Donc $ua + vb$ est multiple de c avec c non nul, par conséquent c divise $ua + vb$. \square

 **Application 5.4.** Déterminer les entiers relatifs n tels que $n + 3$ divise $2n + 8$.

4.2 Division euclidienne

Théorème.


Soient a et b deux entiers naturels avec $b \neq 0$.

Il existe un unique couple (q, r) d'entiers naturels tels que :

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

On dit que a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste** de la division euclidienne de a par b .

dividende	diviseur
	quotient
reste	

 Il y a de multiples écritures de a sous la forme $bq + r$. Prenons par exemple $a = 103$ et $b = 13$.
 On a $103 = 13 \times 7 + 12$ ou $103 = 13 \times 6 + 25$ ou encore $103 = 13 \times 5 + 38$, etc.
 Mais seule la 1^{re} égalité, où $0 \leq r < b$, est la **relation de la division euclidienne** de a par b .

Propriété 6.4.

Dans la division euclidienne de a par b , il y a b restes possibles :

$$0, 1, 2, \dots, b-1.$$

Propriété 7.4.

Soient a un entier naturel et b un entier naturel non nul.

b divise a **si et seulement si** le reste dans la division euclidienne de a par b est nul.


Propriété 8.4.

Soit b un entier naturel supérieur ou égal à 2.

Tout *entier relatif* s'écrit sous l'une des formes suivantes : $bq, bq+1, bq+2, \dots, bq+(b-1)$ où q est un entier relatif.

Exemple 3.4.

Tout entier a pour reste 0, 1, 2 ou 3 dans la division euclidienne par 4, donc s'écrit sous la forme $4k, 4k+1, 4k+2$ ou $4k+3$ avec k entier.

 **Application 6.4.** En utilisant la méthode de disjonction des cas, démontrer que $n^2 + 1, n \in \mathbb{Z}$, n'est jamais divisible par 3.

4.3 Congruences dans \mathbb{Z}

4.3.1 Propriété et définition

Propriété 9.4.

Soit n un entier naturel non nul.

Deux entiers relatifs a et b ont même reste dans la division euclidienne par n **si et seulement si** $a-b$ est multiple de n .

Démonstration. On écrit les relations de division euclidienne par n :

$$a = nq + r, 0 \leq r < n \text{ et } b = nq' + r', 0 \leq r' < n.$$

On en déduit que $a-b = n(q-q') + r-r'$ et que $-n < r-r' < n$.

- Supposons que $r = r'$ alors $a-b = n(q-q')$ avec $q-q'$ entier, donc $a-b$ multiple de n .
- Réciproquement, si $a-b$ multiple de n , alors $n|a-b$ et comme $n|n(q-q')$ alors $n|a-b-n(q-q')$ c'est-à-dire $n|r-r'$. Or $-n < r-r' < n$, il faut avoir $r-r' = 0$ c'est-à-dire $r = r'$.

□

Définition 2.4.

Soit n un entier naturel non nul.

Si a et b ont même reste dans la division euclidienne par n , on dit que a et b sont *congrus modulo* n et on écrit : $a \equiv b \pmod{n}$ ou $a \equiv b \pmod{n}$ ou encore $a \equiv b \pmod{n}$, notation qu'on privilégiera.

Exemple 4.4.

Sur la droite numérique, on a repéré en bleu des multiples de 4 et en rouge des nombres ayant tous pour reste 1 dans la division par 4 ; ils sont tous congrus entre eux.

$$5 \equiv 1 \pmod{4}, -7 \equiv 1 \pmod{4}, -3 \equiv 5 \pmod{4}.$$

Illustration :**► Note 2.4.**

$$a \equiv b [n] \iff b \equiv a [n].$$

On dit aussi que a et b sont *congrus modulo n* .

Propriété 10.4.

Soient a et b deux entiers relatifs et n un entier naturel non nul.

- $a \equiv 0 [n]$ si et seulement si a est *divisible* par n .
- $a \equiv a [n]$.
- r est le reste de la division euclidienne de a par n **si et seulement si** $a \equiv r [n]$ et $0 \leq r < n$.

4.3.2 Congruence et transitivité**Propriété 11.4.**

Soient a, b, c des entiers relatifs et n un entier naturel non nul.

Si $a \equiv b [n]$ et $b \equiv c [n]$ alors $a \equiv c [n]$.

Démonstration. Par hypothèse, il existe k et k' entiers relatifs tels que $a = b + kn$ et $b = c + k'n$... \square

4.3.3 Compatibilité avec les opérations algébriques**Propriété 12.4.**

Soient a, b, c et d quatre entiers relatifs et n un entier naturel non nul.

Si $a \equiv b [n]$ et $c \equiv d [n]$ alors :

- $a + c \equiv b + d [n]$
- $a - c \equiv b - d [n]$
- $ac \equiv bd [n]$
- $a^p \equiv b^p [n]$ pour tout entier naturel p .

En particulier, si $a \equiv b [n]$, pour tout entier relatif m , on a : $ma \equiv mb [n]$.



La réciproque est fautive ! On ne peut pas simplifier une congruence comme une égalité. Par exemple, on a $22 \equiv 18 (4)$ mais 11 et 9 ne sont pas congrus modulo 4.

📄 Application 7.4.

1. Résoudre dans \mathbb{Z} l'équation $3x \equiv 2 [5]$.
2. Montrer que pour tout entier naturel n non nul, $2^{6n} - 1$ est multiple de 7.
3. Déterminer le reste dans la division euclidienne de 11^{2023} par 3.