

Fiche A1.1 : Divisibilité dans $\mathbb{Z}$

1 - Diviseurs et multiples

- L'arithmétique étudie les nombres entiers. On travaille dans $\mathbb{Z} = \{\dots; -2; -1; 0; 1; 2; \dots\}$, l'ensemble des **entiers relatifs**. Elle remonte aux *Éléments* d'Euclide (III^e siècle av. J.-C.) et sert aujourd'hui en cryptographie et dans les codes de contrôle.

Définition 1 : Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b s'il existe un entier relatif k tel que $b = ka$. On note $a|b$.

On dit aussi que a est un **diviseur** de b , que b est un **multiple** de a , ou que b est **divisible** par a .

Remarques :

- $a|b$ est une **affirmation** (vraie ou fausse), et non un nombre : ne pas confondre $a|b$ avec la fraction $\frac{b}{a}$.

Pour $a \neq 0$: $a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z}$.

- 0 est multiple de tout entier ($0 = 0 \times a$), mais 0 ne divise que 0.
- 1 et -1 divisent tout entier ; tout entier a divise a et $-a$.
- $a|b \Leftrightarrow (-a)|b \Leftrightarrow a|(-b)$: les diviseurs d'un entier vont par **paires opposées**. On cherche donc les diviseurs positifs, puis on ajoute leurs opposés.

Exemple 1 : a) -6 divise-t-il 42 ? 4 divise-t-il 30 ? b) Montrer que pour tout $n \in \mathbb{Z}$, 3 divise $6n + 9$.

a)

b)

Propriété 1 : Soient a et b deux entiers avec $b \neq 0$. Si $a|b$, alors $|a| \leq |b|$. En particulier, un entier non nul n'a qu'un **nombre fini** de diviseurs.

Démonstration : Si $a|b$, on a $b = ka$ avec $k \in \mathbb{Z}$. Comme $b \neq 0$, on a $k \neq 0$, donc $|k| \geq 1$ et $|b| = |k| \times |a| \geq |a|$. $\square$

Méthode (lister les diviseurs d'un entier $n \geq 1$) : on teste les entiers d de 1 à $\sqrt{n}$; chaque diviseur d trouvé fournit le couple $\left(d; \frac{n}{d}\right)$ car $n = d \times \frac{n}{d}$. On ajoute ensuite les opposés.

Exemple 2 : Déterminer l'ensemble des diviseurs de 60 dans $\mathbb{Z}$.

-
-
-

Exemple 3 : Déterminer les couples $(x; y)$ d'entiers naturels tels que $x^2 - y^2 = 15$.

Remarque : Ce type d'équation dont on cherche les solutions entières est appelé **équation diophantienne**.

2 - Propriétés de la divisibilité

Propriété 2 : Soient a, b, c trois entiers relatifs.

- **Transitivité** : si $a|b$ et $b|c$, alors $a|c$.
- Si $a|b$, alors $a|bc$.
- Si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$.

Démonstration :

- Si $b = ka$ et $c = k'a$ avec $k, k' \in \mathbb{Z}$, alors $c = (k'k)a$ avec $k, k' \in \mathbb{Z}$, donc $a|c$.
- De même $bc = (kc)a$.
- Si $b = ka$ et $a = k'b$, alors $a = k'ka$. Si $a = 0$, alors $b = 0 = a$.
Sinon ; $k'k = 1$ avec k, k' entiers, donc $k = k' = 1$ ou $k = k' = -1$: $b = a$ ou $b = -a$. $\square$

Propriété 3 (combinaisons linéaires) : Soient a, b, c trois entiers relatifs. Si $a|b$ et $a|c$, alors

- $a|b + c$ et $a|b - c$.
- Plus généralement, pour tous entiers relatifs u et v : $a|bu + cv$.

Remarque : $bu + cv$ est appelée une **combinaison linéaire** de b et c .

Démonstration : Il existe $k, k' \in \mathbb{Z}$ tels que $b = ka$ et $c = k'a$.

Alors $bu + cv = kau + k'av = (ku + k'v)a$ avec $ku + k'v \in \mathbb{Z}$, donc $a|bu + cv$. $\square$

Point de vigilance : les réciproques de ces deux propriétés sont fausses :

Contre-exemples : $3|4 + 5$, mais $3 \nmid 4$ et $3 \nmid 5$. De même, $6|3 \times 4$, mais $6 \nmid 3$ et $6 \nmid 4$.

Méthode (trouver les entiers n tels que $n + a$ divise une expression) : on fait apparaître une **combinaison** des deux expressions qui ne dépend plus de n . On obtient une **condition nécessaire** ; on vérifie ensuite chaque valeur trouvée.

Exemple 4 : Déterminer les entiers naturels n tels que $n + 1$ divise $n + 5$.

-
-
-

Exemple 5 : Déterminer les entiers relatifs n tels que $n - 2$ divise $3n + 1$.

-
-
-