Divisibilité dans l'ensemble des entiers naturels et relatifs

Notation : $\mathbb{Z}$ l'ensemble des entiers relatifs ; $|a|$ est la valeur absolue de a (c.à.d. a, si ce nombre est positif ou nul, et $-a$ autrement) ; $\Leftrightarrow$ est 'si et seulement si'.

1 Division euclidienne pour les entiers

Le dividende peut être un entier relatif, le diviseur est un entier relatif non nul (on ne divise jamais par zéro !). Le reste sera toujours positif ou nul.

Théorème de la division euclidienne
Soient $a, b \in \mathbb{Z}$, avec $b \neq 0$. Il existe un unique quotient q et un unique reste r vérifiant les propriétés suivantes :
• $q, r \in \mathbb{Z}$
• $a = bq + r$
• $0 \leqslant r < |b|$.

Les quotient et reste vérifient ces propriétés ; de plus deux nombres q, r avec ces propriétés sont forcément le quotient et le reste. On peut donc deviner quotient et reste, mais ils faut vérifier les propriétés.

En pratique : On peux faire la division entre les valeurs absolues comme à l'école, et adapter ensuites le résultat (en manipulant l'équation de la division).

Exemples : Quelques exemples de division euclidienne.

$13 : 5$	$q = 2, r = 3$	$3 : 5$	$q = 0, r = 3$
$13 : (-5)$	$q = -2, r = 3$	$3 : (-5)$	$q = 0, r = 3$
$(-13) : 5$	$q = -3, r = 2$	$(-3) : 5$	$q = -1, r = 2$
$(-13) : (-5)$	$q = 3, r = 2$	$(-3) : (-5)$	$q = 1, r = 2$
$5 : 3$	$q = 1, r = 2$	$8 : 4$	$q = 2, r = 0$
$5 : (-3)$	$q = -1, r = 2$	$8 : (-4)$	$q = -2, r = 0$
$(-5) : 3$	$q = -2, r = 1$	$(-8) : 4$	$q = -2, r = 0$
$(-5) : (-3)$	$q = 2, r = 1$	$(-8) : (-4)$	$q = 2, r = 0$

Remarque : Pour les nombres naturels, mais pas en général, le quotient est la partie entière du nombre rationnel dividende/diviseur (c.à.d. le plus grand entier inférieur ou égal à ce nombre). Ce qui est vrai en général : diviseur$\times$quotient est le plus grand multiple du diviseur inférieur ou égal au dividende.

2 Divisibilité

Définition (divisibilité) Soient $a, b \in \mathbb{Z}$. On dit que a est divisible par b (ou que b est un diviseur de a, ou que a est un multiple de b), s'il existe $z \in \mathbb{Z}$ tel que $a = zb$.
On écrit alors $b \mid a$.

Examples : Les entiers pairs sont les multiples du nombre 2. Les multiples de 3 sont $0, \pm 3, \pm 6, \pm 9, \ldots$. Cas special : le seul multiple de 0 est 0 ; chaque nombre est un diviseur de 0.

Diviseurs triviaux : On a $\pm a \mid a$ et $\pm 1 \mid a$ pour tout $a \in \mathbb{Z}$.

Signes : Un signe ne change pas la divisibilité (moins un diviseur est encore un diviseur, et moins un multiple est encore un multiple).

Remarque : Soients $a, b \in \mathbb{Z}$. Si $b \neq 0$, on peut faire la division $a : b$. Les propriétés suivantes sont équivalentes (et on peut utiliser à chaque fois la plus pratique) :
• il existe $z \in \mathbb{Z}$ avec $a = zb$;
• le reste de la division $a : b$ est zéro ;
• le nombre rationnel $\frac{a}{b}$ est un entier.

Propriété "Transitivité" : Si $a \mid b$ et $b \mid c$, on en déduit que $a \mid c$. [Preuve : Si $b = ta$ et $c = sb$ avec $t, s \in \mathbb{Z}$, on a aussi $c = sta$ avec $st \in \mathbb{Z}$.]

Théorème ("Double divisibilité") : Soient $a, b \in \mathbb{Z}$. Si $a \mid b$ et $b \mid a$, on a forcément $|a| = |b|$ (c.à.d. $a = b$ ou $a = -b$). [Si les nombres sont des entiers naturels, ou ont le même signe, on en déduit que $a = b$. Par contre, on a $2 \mid -2$ et $-2 \mid 2$.]

Propriété "Produit/Simplification" : Soient $a, b, c \in \mathbb{Z} \setminus \{0\}$. On a

$$a \mid b \qquad \Leftrightarrow \qquad ac \mid bc\,.$$

Propriété "Combinaisons" : Soient $a, b, c \in \mathbb{Z} \setminus \{0\}$. On a

$$a \mid b \quad \text{et} \quad a \mid c \quad \Rightarrow \qquad a \mid (bz + cz') \quad \text{pour tout } z, z' \in \mathbb{Z}.$$

En particulier on a une règle pour la somme ($a \mid (b+c)$) et pour la différence ($a \mid (b-c)$).

Propriété "Les diviseurs sont petits" : Soient $a, b \in \mathbb{Z} \setminus \{0\}$. Si a divise b, on a $|a| \leqslant |b|$. [Preuve : Si $b = qa$ avec $q \in \mathbb{Z}$, il faut que $|q| \geqslant 1$ (car $b \neq 0$), et on a donc $|b| = |qa| = |q| \cdot |a| \geqslant |a|$.]