Divisibilité

1 Divisibilité dans $\mathbb{Z}$ & congruences

Définition 1

a et $b \neq 0$ sont deux entiers relatifs.
b **divise** a s'il existe un entier relatif k tel que $bk = a$. On note alors $b|a$.
Si c'est le cas, on dit b est un **diviseur** de a et que a est un **multiple** de b.

Exemple 1

Comme $274 = 137 \times 2$, on peut dire que $2|274$.

Remarque : 1 et -1 divisent tout entier.

Propriété 1 : Critères de divisibilité

- Un entier est divisible par 2 si et seulement si son chiffre des unités est un entier pair.
- Un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.
- Un entier est divisible par 4 si et seulement si son chiffre des dizaines et des unités forment un multiple de 4.
- Un entier est divisible par 5 si et seulement si son chiffre des unités vaut 0 ou 5.
- Un entier est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.
- Un entier est divisible par 10 si et seulement si son chiffre des unités vaut 0.

Propriété 2

Pour deux entiers a et $b \neq 0$, $b|a$ si et seulement si $\dfrac{a}{b} = a \div b$ est un entier.

Propriété 3 : Anti-symétrie de la divisibilité

Pour deux entiers relatifs a et b non nuls, si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$.

Propriété 4 : Transitivité de la divisibilité

a ; b et c sont trois entiers relatifs non nuls. On suppose que $a|b$ et que $b|c$.
Alors, $a|c$.

Exemple 2

Comme $3|6$ et que $6|36$, on en déduit que $3|36$.

Propriété 5 : Divisibilité et combinaison linéaire

a ; b et $d \neq 0$ sont trois entiers relatifs. On suppose que $d|a$ et $d|b$.
Alors pour tous entiers relatifs u et v,
d divise $au + bv$ (qui est une **combinaison linéaire** de a et b).
En particulier d divise $a + b$ et $a - b$.

2 Division euclidienne dans $\mathbb{N}$

Théorème 1 : Division euclidienne dans $\mathbb{N}$

a et $b \neq 0$ sont deux entier naturels.
Alors il existe un unique entier naturel q et un unique $0 \leqslant r < b$ entier naturel tel que $a = bq + r$.
On dit alors que l'on a effectué la **division euclidienne de a par b**.
a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

Exemple 3

En effectuant la division euclidienne de 229 par 5, on trouve $229 = 5 \times 45 + 4$.

Propriété 6

Pour une division euclidienne présentée sous la forme $a = bq + r$, q est la partie entière de $\frac{a}{b}$ (*i.e.* l'arrondi à l'entier près par défaut).

Propriété 7

Pour deux entiers naturels a et $b \neq 0$, $b|a$ si et seulement si le reste de la division euclidienne de a par b vaut 0.

Exemple 4

Pour effectuer la division euclidienne de $a = 1\ 301$ par $b = 114$, on cherche
$\frac{a}{b} = \frac{1\ 301}{114} \approx 11,4$.
Le quotient est donc $q = 11$. On trouve le reste en faisant
$r = a - bq = 1\ 301 - 114 \times 11 = 47$, et on a bien $0 \leqslant 47 < 114$.

3 Division euclidienne dans $\mathbb{Z}$

Propriété 8

Pour tout nombre réel x, on note $|x| = \begin{cases} -x \text{ si } x \leqslant 0 \\ x \text{ si } x \geqslant 0 \end{cases}$: c'est la **valeur absolue de x**.
Ainsi, pour tout nombre réel x, $|x| \geqslant 0$.

Théorème 2 : Division euclidienne dans $\mathbb{Z}$

a et $b \neq 0$ sont deux entier relatifs.
Alors il existe un unique entier relatif q et un unique $0 \leqslant r < |b|$ entier naturel tel que $a = bq + r$.

Exemple 5

Pour effectuer la division euclidienne de -998 par 13, on cherche $\frac{-988}{13} \approx -76,8$.
Le quotient est donc -77. On trouve le reste en faisant
$-998 + 13 \times |-77| = 3$, et on a bien $0 \leqslant 3 < |-77|$.

4 Congruences

Définition 2

Pour un entier naturel $m \neq 0$, deux entiers relatifs a et b sont **congrus modulo** m si m divise $b-a$. On note alors $a \equiv b \pmod{m}$.

Exemple 6

- $1 \equiv 5 \pmod{4}$.
- $-7 \equiv 1 \pmod{8}$.
- $10 \equiv 0 \pmod{10}$.

Propriété 9

Pour un entier naturel $m \neq 0$ et deux entiers relatifs a et b, on a
$a \equiv b \pmod{m}$
si et seulement si a et b ont le même reste dans la division euclidienne par m
si et seulement si $\dfrac{a}{m}$ et $\dfrac{b}{m}$ ont la même partie décimale
si et seulement si $\dfrac{b-a}{m}$ et est un entier.

Propriété 10

Pour un entier naturel $m \neq 0$ et entier relatif a, on a

- $0 \equiv m \pmod{m}$;
- $a \equiv a+m \pmod{m}$.

Exemple 7

- $1 \equiv 8 \pmod{7}$.
- $19 \equiv 1 \pmod{3}$.

Propriété 11 : Transitivité de la congruence

Pour un entier naturel $m \neq 0$ et trois entiers relatifs a ; b et c, on suppose que $a \equiv b \pmod{m}$ et $b \equiv c \pmod{m}$.
Alors $a \equiv c \pmod{m}$.

Propriété 12 : Congruence & somme

Pour un entier naturel $m \neq 0$ et quatre entiers relatifs a ; b ; a' et b', on suppose que $a \equiv b \pmod{m}$ et $a' \equiv b' \pmod{m}$. Alors

- $a + a' \equiv b + b' \pmod{m}$;
- $a - a' \equiv b - b' \pmod{m}$.

Propriété 13 : Congruence & produit

Pour un entier naturel $m \neq 0$, quatre entiers relatifs a ; b ; a' et b' et p un entier naturel, on suppose que $a \equiv b \pmod{m}$ et $a' \equiv b' \pmod{m}$. Alors

- $a \times a' \equiv b \times b' \pmod{m}$;
- $a^p \equiv b^p \pmod{m}$.

Exemple 8

$5 \equiv 1 \pmod{4}$, donc pour tout entier naturel p, $5^p \equiv 1^p \pmod{4}$ et donc $5^p \equiv 1 \pmod{4}$.
Ainsi, le reste de la division euclidienne de 5 ; 25 ; 125 ; 625 ; 3 125 ; *etc.* par 4 vaut 1.