# Synthèse de cours PanaMaths
# → Divisibilité et congruences

Rappelons que, sans plus de précision, « nombre entier » désigne un élément de $\mathbb{Z}$.

## Division euclidienne

### *Diviseurs*

Soit $a$ et $b$ deux nombres entiers.
On dit que « $b$ est un diviseur de $a$ » ou que « $b$ divise $a$ » s'il existe un nombre entier $k$ tel que :

$$a = bk$$

On peut écrire : $b \mid a$.
On dit que également que « $a$ est un multiple de $b$ ».

Remarques :

- Tout entier non nul divise 0.
- Tout entier non nul admet un nombre fini de diviseurs.
- L'ensemble des multiples de l'entier $b$ est noté « $b\mathbb{Z}$ » (si $b = 0$ cet ensemble est réduit à $\{0\}$).

### *Division euclidienne*

Soit $a$ un nombre entier et $b$ un nombre entier naturel non nul.
Il existe un unique couple de nombres entiers $(q, r)$ tel que :

$$a = bq + r \text{ et } 0 \leq r < b$$

L'égalité « $a = bq + r$ » est appelée « division euclidienne de l'entier $a$ par l'entier naturel $b$ ».
Les entiers $a$, $b$, $q$ et $r$ sont respectivement appelés « dividende », « diviseur », « quotient » et « reste » de la division.

Remarques :

- si $b = 1$, on a $q = a$ et $r = 0$. Cette situation est peu intéressante …
- si $a = b$, on a : $q = 1$ et $r = 0$.

# PGCD et PPCM de deux entiers

## *Théorème définition*

Soit $a$ et $b$ deux nombres entiers non nuls.

L'ensemble des diviseurs communs à $a$ et à $b$ admet un plus grand élément appelé « plus grand diviseur commun de $a$ et $b$ » et noté : $\text{PGCD}(a,b)$ ou $a \wedge b$.
Il est souvent désigné par la lettre $d$.

L'ensemble des multiples strictement positifs communs à $a$ et à $b$ admet un plus petit élément appelé « plus petit commun multiple de $a$ et $b$ » et noté : $\text{PPCM}(a,b)$ ou $a \vee b$.
Il est souvent désigné par la lettre $m$.

Remarques :

- les deux entiers $\text{PGCD}(a,b)$ et $\text{PPCM}(a,b)$ sont strictement positifs.
- $\text{PGCD}(a,b) = \text{PGCD}(-a,b) = \text{PGCD}(a,-b) = \text{PGCD}(-a,-b) = \text{PGCD}(|a|,|b|)$.
  On se ramènera ainsi souvent au calcul du PGCD de deux entiers naturels non nuls.
- $\text{PPCM}(a,b) = \text{PPCM}(-a,b) = \text{PPCM}(a,-b) = \text{PPCM}(-a,-b) = \text{PPCM}(|a|,|b|)$.

## *Entiers premiers entre eux*

Deux nombres entiers sont dits « premiers entre eux » ou « étrangers » si leur PGCD est égal à 1.

## *Propriétés*

Soit $a$ et $b$ deux nombres entiers non nuls.
Soit $d$ et $m$ leur PGCD et PPCM respectivement.

- Il existe deux nombres entiers $a'$ et $b'$ premiers entre eux tels que :

$$a = a'd \text{ et } b = b'd$$

$$m = a'b'd = ab' = a'b \text{ et } md = ab$$

- Les diviseurs communs à $a$ et à $b$ sont les diviseurs de $d$.
- Les multiples communs à $a$ et à $b$ sont les multiples de $m$.

*L'algorithme d'Euclide*

## Propriété fondamentale

Soit $a$ et $b$ deux nombres entiers naturels non nuls.

Soit $q$ et $r$, respectivement le quotient et le diviseur dans la division euclidienne de $a$ par $b$ :

$$a = bq + r \text{ et } 0 \leq r < b$$

On a alors :

$$\text{PGCD}(a, b) = \text{PGCD}(b, r)$$

La propriété fondamentale précédente conduit à un procédé itératif (algorithme) permettant de calculer le PGCD de deux entiers naturels non nuls.

## L'algorithme d'Euclide

Soit $a$ et $b$ deux nombres entiers naturels non nuls.

On note : $a = bq_0 + r_0$ la division euclidienne de $a$ par $b$. On a : $0 \leq r_0 < b$.
D'après la propriété fondamentale : $\text{PGCD}(a, b) = \text{PGCD}(b, r_0)$.

On note ensuite : $b = r_0 q_1 + r_1$ la division euclidienne de $b$ par $r_0$. On a : $0 \leq r_1 < r_0$.
D'après la propriété fondamentale : $\text{PGCD}(b, r_0) = \text{PGCD}(r_0, r_1)$.

En itérant le procédé, on construit une suite $(r_n)$ de restes. Cette suite est strictement décroissante minorée par 0. Or, tant que le reste courant $r_i$ est non nul, on peut diviser $r_{i-1}$ par $r_i$ pour obtenir un nouveau reste $r_{i+1}$ tel que :

$$\text{PGCD}(r_{i-1}, r_i) = \text{PGCD}(r_i, r_{i+1}) \text{ et } 0 \leq r_{i+1} < r_i$$

On va ainsi finir par obtenir un premier reste $r_{n+1}$ nul. Le PGCD de $a$ et $b$ sera alors simplement égal au dernier reste non nul : $r_n$.

*Le théorème de Bezout*

## Le théorème

Soit $a$ et $b$ deux nombres entiers non nuls.
Soit $d$ leur PGCD.

Alors il existe deux nombres entiers $u$ et $v$ tels que :

$$au+bv=d$$

Cette égalité est appelée « égalité de Bezout ».

## Corollaires

Soit $a$ et $b$ deux nombres entiers non nuls.

S'il existe trois entiers $u$, $v$ et $c$ ($c$ non nul) tels que :

$$au+bv=c$$

alors le PGCD de $a$ et $b$ divise $c$.

Soit $a$ et $b$ deux nombres entiers non nuls.

On a l'équivalence :

$a$ et $b$ sont premiers entre eux

$\Leftrightarrow$

il existe deux entiers $u$ et $v$ tels que : $au+bv=1$

Soit $a$, $b$ et $c$ trois nombres entiers non nuls.

L'équation :

$$ax+by=c$$

admet des solutions entières si, et seulement si, $c$ est un multiple de $\text{PGCD}(a,b)$.

*Le théorème de Gauss*

## Le théorème

Soit *a*, *b* et *c* trois nombres entiers non nuls.

Si *a* divise le produit *bc* et si *a* et *b* sont premiers entre eux alors *a* divise *c*.

Remarque : on peut énoncer ce théorème sous une forme plus mathématique :

$$\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*, \forall c \in \mathbb{Z}^*, a \mid bc \text{ et } a \wedge b = 1 \Rightarrow a \mid c$$

## Corollaires

Soit *a*, *b* et *c* trois nombres entiers non nuls.

Si *a* divise *c* et *b* divise *c* et si *a* et *b* sont premiers entre eux alors *ab* divise *c*.

Remarque : on peut énoncer ce corollaire sous une forme plus mathématique :

$$\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*, \forall c \in \mathbb{Z}^*, a \mid c \text{ et } b \mid c \text{ et } a \wedge b = 1 \Rightarrow ab \mid c$$

Soit *a*, *b* et *c* trois nombres entiers non nuls.

Si *a* et *b* sont premiers entre eux et si *a* et *c* sont premiers entre eux alors *a* et *bc* sont premiers entre eux.

Remarque :

- on peut énoncer ce corollaire sous une forme plus mathématique :

$$\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*, \forall c \in \mathbb{Z}^*, a \wedge b = 1 \text{ et } a \wedge c = 1 \Rightarrow a \wedge bc = 1$$

- on peut généraliser ce corollaire :

Si $a$, $b_1, b_2, ..., b_n$ sont $n+1$ nombres entiers non nuls et si, pour tout *i* dans $\{1 ; 2 ; 3 ; ... ; n\}$, *a* est premier avec $b_i$ alors *a* est premier avec le produit $b_1 b_2 ... b_n$.

# Congruences

## *Entiers congrus*

Soit $a$ et $b$ deux nombres entiers et $n$ un entier naturel différent de 0 et 1.

On dit que « $a$ et $b$ sont congrus modulo $n$ » s'ils admettent le même reste dans la division euclidienne par $n$.

On écrit alors :

$$a \equiv b \ \left(\text{modulo } n\right) \text{ ou } a \equiv b \ \left(n\right)$$

Remarque : on peut également parler de « la relation de congruence ».

## *Caractérisation*

Soit $a$ et $b$ deux nombres entiers et $n$ un entier naturel différent de 0 et 1.

On a l'équivalence :

$$a \equiv b \ \left(n\right) \Leftrightarrow a - b \text{ est un multiple de } n$$

## *Propriétés*

Soit $n$ un entier naturel différent de 0 et 1.
Soit $a$, $b$, $a'$ et $b'$ quatre nombres entiers tels que : $a \equiv b \ \left(n\right)$ et $a' \equiv b' \ \left(n\right)$.

On a alors :

$$a + a' \equiv b + b' \ \left(n\right)$$

$$aa' \equiv bb' \ \left(n\right)$$

$$\forall p \in \mathbb{N}, a^p \equiv b^p \ \left(n\right)$$

On dit que « la relation de congruence est compatible avec l'addition et la multiplication dans l'ensemble $\mathbb{Z}$ ».