# Euclide (vers 300 avant notre ère.)

Mathématicien de la Grèce antique. Son ouvrage le plus célèbre, les Éléments, est un des plus anciens traités connus présentant de manière systématique, à partir d'axiomes et de postulats, un large ensemble de théorèmes accompagnés de leurs démonstrations. Il porte sur la géométrie, tant plane que solide, et l'arithmétique théorique.

# I. Divisibilité dans $\mathbb{Z}$

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

Définition

On dit que $\boldsymbol{b}$ divise $\boldsymbol{a}$ lorsqu'il existe un entier relatif $k$ tel que $a = k \times b$.

On dit alors que $b$ est un diviseur de $a$ ou que $a$ est un multiple de $b$ et on note $b|a$.

Exemples

Quels sont les diviseurs de 30 ? Quels sont les diviseurs de 0 ?
Quels sont les diviseurs de $-60$ ?

Propriété

Soit $n \in \mathbb{N}^*$

Tout diviseur positif de $n$ est compris entre 1 et $n$.

Tout entier naturel non nul possède un nombre fini de diviseurs.

Remarques

- On notera $D(n)$ l'ensemble des diviseurs dans $\mathbb{N}$ de l'entier naturel $n$.
- $\forall n \in \mathbb{N}^*, \; 1 \in D(n)$ et $n \in D(n)$

Propriété

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

Démonstration

Propriété

Si $a$ divise $b$ et $a$ divise $c$ alors $a$ divise $\alpha b + \beta c$ où $\alpha, \beta \in \mathbb{Z}$

Démonstration

Corollaire

Si $a$ divise $b$ et $a$ divise $c$ alors $a$ divise $b + c$ et $a$ divise $b - c$.

Exemple : Quels sont les diviseurs communs à 60 et 63 ?

Théorème : division euclidienne dans $\mathbb{N}$

Si $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ alors il existe un unique couple d'entiers naturels $(q, r)$ tels que $a = bq + r$ où $0 \leq r < b$.

Théorème : division euclidienne dans $\mathbb{Z}$

Si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ alors il existe un unique couple d'entiers $(q, r)$ tels que $a = bq + r$ où $0 \leq r < |b|$ et $q \in \mathbb{Z}$.

Corollaire

$a$ divise $b$ si, et seulement si, le reste de la division euclidienne de $a$ par $b$ est égal à 0.

# II. Congruence

$a$ et $b$ désignent deux entiers relatifs.

Définition

Soit $n \in \mathbb{N}$, on dit que $a$ et $b$ sont congrus modulo $\boldsymbol{n}$ lorsque $\boldsymbol{n}$ divise $\boldsymbol{b-a}$.

On note alors $\boldsymbol{a \equiv b\ [n]}$

Exemples

$29 \equiv 1\ [7]$ $\qquad 29 \equiv 2\ [3]$ $\qquad 29 \equiv 8\ [3]$

$32 \equiv \cdots\ [5]$ $\qquad 44 \equiv \cdots\ [2]$ $\qquad 25 \equiv 1\ [\dots]$

Théorème

Pour tout $n \in \mathbb{N}^*$

$\boldsymbol{a \equiv b\ [n]}$ si, et seulement si, $\boldsymbol{a}$ et $\boldsymbol{b}$ ont le même reste dans la division euclidienne par $\boldsymbol{n}$.

Démonstration :

Corollaire

Soit $n \in \mathbb{N}, n \geq 2$

Il existe un unique entier $\boldsymbol{r}$ tel que $\boldsymbol{0 \leq r <} n$ et $\boldsymbol{a \equiv r\ [n]}$.

Cet entier $r$ est le reste dans la division euclidienne de $\boldsymbol{a}$ par $\boldsymbol{n}$.

Propriétés

Soit $n \in \mathbb{N}, n \geq 2$, $a$, $b$ et $c$ des entiers relatifs,

1) $a \equiv a\ [n]$
2) Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$

Démonstration

Propriétés

Soit $n \in \mathbb{N}, n \geq 2$, $a$, $b$, $c$ et $d$ des entiers relatifs,

1) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$
2) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a \times c \equiv b \times d\ [n]$
3) Si $a \equiv b\ [n]$ alors $a^p \equiv b^p\ [n]$ pour tout $p \in \mathbb{N}^*$

Démonstration

## Propriétés

Soit $n \in \mathbb{N}, n \geq 2$, $a$ un entier relatif,

$$a \equiv 0\ [n] \text{ si, et seulement si, } n \text{ divise } a$$

## Exemple :

Démontrer que, pour tout $n \in \mathbb{N}$, le nombre $9^{2n} - 1$ est divisible par 10.

## Critère de divisibilité :

Soit $d \in \mathbb{N}$, $a_0, a_1, \dots, a_n$ les chiffres de l'écriture décimale de $d$

$$d = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_n \times 10^n = \overline{a_n \dots a_3 a_1 a_0}$$

Retrouver les critères de divisibilités par 2, 5, 3, 9, 4 et 11.