DIVISIBILITÉ ET CONGRUENCES (SPÉCIALITÉ)

1. DIVISION EUCLIDIENNE

DÉFINITION

Soient a et b deux entiers relatifs tels qu'il existe un entier relatif k tel que $a = bk$.

On dit alors que :

- b **divise** a ;
- b est un **diviseur** de a ;
- a est un **multiple** de b.

Ceci se note $b|a$

EXEMPLE

$15 = 3 \times 5$ donc :

- 3 divise 15.
- 3 est un diviseur de 15.
- 15 est un multiple de 3.

REMARQUES

- 0 est un multiple de tout entier relatif.
- 1 et -1 sont des diviseurs de tout entier relatif.
- a et $-a$ ont les mêmes diviseurs.

PROPRIÉTÉS

- Si a divise b et b divise a, alors a et b sont égaux ou opposés.
- Si a divise b et b divise c, alors a divise c.
- Si c divise a et c divise b, alors c divise toute combinaison linéaire de a et b (c'est-à-dire tout nombre de la forme $au + bv$; $u \in \mathbb{Z}$, $v \in \mathbb{Z}$).

THÉORÈME ET DÉFINITIONS

Division euclidienne dans $\mathbb{Z}$

Soient a et b deux entiers relatifs avec $b \neq 0$.

Il existe un et un seul couple d'entiers relatifs (q, r) tels que :

$$a = bq + r \text{ et } 0 \leqslant r < |b|.$$

q et r s'appelle respectivement le **quotient** et le **reste** de la **division euclidienne** de a par b.

EXEMPLE

-14=3×(-5)+1 et 0⩽1<3

La division euclidienne de -14 par 3 donne un quotient de -5 est un reste de 1.

REMARQUES

- **Attention!** Ne pas oublier la condition $0 \leqslant r < |b|$. La seule égalité $a = bq+r$ ne suffit pas à prouver que q et r sont les quotient et reste dans la division euclidienne de a par b.
- a est divisible par b si et seulement si le reste de la division de a par b est égal à zéro.

2. CONGRUENCES

DÉFINITION

On dit que deux entiers relatifs a et b son congrus modulo n ($n \in \mathbb{N}^*$) et l'on écrit $a \equiv b\,[n]$ si et seulement si a et b ont le même reste dans la division par n.

EXEMPLE

$18 \equiv 23\,[5]$ car 18 et 23 ont tous les deux 3 comme reste dans la division par 5.

PROPRIÉTÉS

- $a \equiv b\,[n]$ si et seulement si n divise $a - b$ en particulier $a \equiv 0\,[n]$ si et seulement si n divise a.
- Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$.

PROPRIÉTÉS (CONGRUENCES ET OPÉRATIONS)

Soient quatre entiers relatifs a, b, c, d tels que $a \equiv b\,[n]$ et $c \equiv d\,[n]$. Alors :

- $a + c \equiv b + d\,[n]$ et $a - c \equiv b - d\,[n]$.
- $ac \equiv bd\,[n]$.
- $ka \equiv kb\,[n]$ pour tout entier relatif k.
- $a^m \equiv b^m\,[n]$ pour tout entier naturel m.

PROPRIÉTÉ

r est le reste de la division euclidienne de a par b si et seulement si :

$$\begin{cases} r \equiv a\,[b] \\ r < |b| \end{cases}$$

EXEMPLE

On cherche à déterminer le reste de la division euclidienne de 2009^{2009} par 5.

$2009 \equiv -1\,[5]$ car 2009-(-1)=2010 est divisible par 5.

Donc :

$2009^{2009} \equiv (-1)^{2009}\,[5]$ c'est-à-dire $2009^{2009} \equiv -1\,[5]$

Or $-1 \equiv 4\,[5]$ donc $2009^{2009} \equiv 4\,[5]$

Comme $0 \leqslant 4 < 5$, le reste de la division euclidienne de 2009^{2009} par 5 est 4.