I - Divisibilité dans $\mathbb{Z}$

Définition 1 : Diviseur d'un enter relatif

Soient a et b deux entiers relatifs.

Dire que a divise b signifie qu'il existe un entier relatif k tel que $b = ka$. On note généralement $a \mid b$.

Exemples

1. 70 divise 210 car $210 = 3 \times 70$
2. -12 divise 24 car $24 = -2 \times (-12)$

Remarques

1. Tout entier relatif divise 0
2. Tout entier relatif a admet pour diviseurs -1, 1, $-a$ et a

Propriété 1 : Transitivité de la divisibilité

Soient a, b et c trois entiers relatifs tels que a et b sont non nuls.

$$\text{Si } a \mid b \text{ et } b \mid c \text{ alors } a \mid c$$

Propriété 2

Soient a, b deux entiers relatifs non nuls.

$$\text{Si } a \mid b \text{ et } b \mid a \text{ alors } a = b \text{ ou } a = -b.$$

Propriété 3 : Divisibilité et combinaisons linéaires

Soient a, b et c trois entiers relatifs tels que $a \neq 0$.

$$\text{Si } a \mid b \text{ et } a \mid c \text{ alors } a \mid b + c \text{ et } a \mid b - c.$$

Plus généralement,

$$a \mid ub + vc \text{ où } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z}$$

Exercices

1. Soit un entier $n \geq 2$. Montrer que $n - 1 \mid n^2 - 1$.
2. Soient $n \in \mathbb{Z}$ et $a \in \mathbb{Z}$ tels que $a \mid n + 4$ et $a \mid 2n - 3$. Montrer que $a \mid 11$.
3. Déterminer les entiers relatifs tels que $2n - 5 \mid n + 3$.

II - Division euclidienne

Propriété 4 : Existence et unicité de la division euclidienne dans $\mathbb{N}$

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

Exemples

1. $57 = 8 \times 7 + 1$ est la division euclidienne de 57 par 7
2. $211 = 13 \times 16 + 3$ est la division euclidienne de 211 par 16
3. $48 = 6 \times 8 + 0$ est la division euclidienne de 48 par 6

Remarque

Dire que $a \mid b$ équivaut à dire que le reste de la division euclidienne de a par b est nul. Voir le dernier exemple précédent.

Définition 2 : Division euclidienne

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.
Effectuer la division euclidienne dans $\mathbb{N}$ de a par b, c'est déterminer le couple (q, r) d'entiers naturels, tel que

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

q est le **quotient** et r est le **reste** de la division euclidienne.

Propriété 5 : Division euclidienne dans $\mathbb{Z}$

La division euclidienne se généralise dans $\mathbb{Z}$. Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.
Il **existe** un **unique** couple d'entiers relatifs (q, r) tels que $a = bq + r$ et $0 \leq r < |b|$.

Exercice

Effectuer la division euclidienne de -1159 par 24.

Conséquence très importante

Soit $b \in \mathbb{N}^*$ et $n \in \mathbb{Z}$.
En effectuant la division euclidienne de n par b, tout entier relatif n s'écrit $n = bq + r$ où $q \in \mathbb{Z}$ et $0 \leq r \leq b - 1$

Exemple

Avec $b = 2$. Tout nombre entier n s'écrit sous la forme $n = 2k$ ou $n = 2k + 1$ où $k \in \mathbb{Z}$. Autrement dit, tout nombre entier est soit **pair**, soit **impair**.

III - Congruences dans $\mathbb{Z}$

Définition 3 : Congruence de deux entiers

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Dire que a et b sont **congrus modulo** n signifie que a et b ont le même reste dans la division euclidienne par n. On écrit $a \equiv b\,[n]$ (ou $a \equiv b\,(n)$ ou $a \equiv b\,(\text{mod } n)$).

Propriété 6 : Définition équivalente

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. $a \equiv b\,[n]$ si et seulement si $n \mid a - b$.

Exemple

1. $21 = 4 \times 5 + 1$ et $25 = 4 \times 6 + 1$ donc $21 \equiv 25\,[4]$
2. $-19 - (-5) = -14 = -2 \times 7$ donc $-19 \equiv -5\,[7]$

Propriété 7 : Divisibilité et congruences

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. $n \mid a$ si et seulement si $a \equiv 0\,[n]$.

Propriété 8 : Division euclidienne et congruences

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. r est le reste de la division euclidienne de a par n si et seulement si $a \equiv r\,[n]$ et $0 \leq r < n$.

Propriété 9 : Propriétés de la relation de congruence

Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

1. $a \equiv a\,[n]$
2. Si $a \equiv b\,[n]$ alors $b \equiv a\,[n]$
3. Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$

Propriété 10 : Opérations sur les congruences

Soient $a, b, c, d \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Alors

1. **Somme de congruences**
   Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$ alors $a + c \equiv b + d\,[n]$ et $a - c \equiv b - d\,[n]$.
2. **Produit de congruences**
   Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$ alors $ac \equiv bd\,[n]$.
3. **Puissances d'une congruence**
   Si $a \equiv b\,[n]$, alors $\forall p \in \mathbb{N}^*$, $a^p \equiv b^p\,[n]$.
4. **Produit et somme par un entier**
   Si $a \equiv b\,[n]$, alors $\forall c \in \mathbb{Z}$, $a + c \equiv b + c\,[n]$ et $ac \equiv bc\,[n]$.