Arithmétiques - Divisibilité et congruences

I Divisibilité dans $\mathbb{Z}$

Définition

Soit a et b deux entiers. On dit que a divise b (noté $a|b$) si il existe $k \in \mathbb{Z}$ tel que $b = ka$. On dit aussi dans ce cas que b est un multiple de a.

Remarques

- Les seuls diviseurs de 1 et de -1 dans $\mathbb{Z}$ sont 1 et -1.
- Tout éléments de $\mathbb{Z}$ est un diviseur de 0
- 0 ne divise qu'un seul nombre, lui même

Propriétés

Soit a, b, c trois entiers relatifs non nuls

1. si a divise b et b divise c, alors a divise c.
2. a divise b et b divise a si et seulement si $a = b$ ou $a = -b$
3. si a divise b et a divise c, alors pour tout $\alpha \in \mathbb{Z}$ et $\beta \in \mathbb{Z}$, a divise $\alpha b + \beta c$

Démonstration

Danger

La réciproque de la propriété 3 est fausse, en effet 5 divise 5 et $5 = 2 + 3$ et pourtant 5 ne divise ni 2 ni 3 ;

Exemples

On peut, en utilisant la propriété 3, démontrer que pour tout entiers naturel n, $2n + 3$ et $6n + 8$ sont premiers entre eux, c'est à dire que leur seuls diviseurs communs sont 1 et -1.
En effet :

II Division euclidienne dans $\mathbb{N}$

Propriété admise

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

Propriété $\mathbb{N}$ est Archimédien - Admis

Si b est un entier naturel non nul, alors pour tout entiers naturels a, Il existe $n \in \mathbb{N}$ tel que $a < nb$.

Théorème

Si a et b sont deux entiers naturels avec $b \neq 0$, alors il existe un unique couple (q, r) d'entiers naturels tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

q et r sont appelés respectivement le quotient et le reste de la division euclidienne de a par b.

Démonstration

- **Existence**

- **Unicité**
  Supposons qu'il existe deux couples (q, r) et (q', r') tels que :
  $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$ et $\begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases}$.

Exemples

III Division euclidienne dans $\mathbb{Z}$

Théorème

Si $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, alors il existe un unique couple (q, r) d'entiers relatifs tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

q et r sont appelés respectivement le quotient et le reste de la division euclidienne de a par b.

Démonstration

Exemples

IV Congruence

1 Définition et propriétés

Définition

Soit n un entier naturel non nul. Soit a et b deux entiers relatifs.
On dit que a est congru à b modulo n si a et b on le même reste dans la division euclidienne par n.
On écrit $a \equiv b \ \ [n]$.

Remarque

Soit n un entier naturel non nul et a et b deux entiers relatifs.

1. $a \equiv 0 \ \ [n]$ si et seulement si n divise a
2. $a \equiv b \ \ [n]$ si et seulement si $a - b \equiv 0 \ \ [n]$, c'est à dire n divise $a - b$.

Propriété

Soit n et n' deux entiers naturels non nuls et a et b deux entiers relatifs.
si n' divise n et $a \equiv b \ \ [n]$, alors $a \equiv b \ \ [n']$

Démonstration

Remarque

La réciproque de cette propriété est fausse.

2 Compatibilité avec les opérations

Propriétés

Soit a, b, a' et b' quatre entiers relatifs et n un entiers naturel non nul.

1. Compatibilité avec l'addition
   Si $a \equiv b \ \ [n]$ et $a' \equiv b' \ \ [n]$, alors $a + a' \equiv b + b' \ \ [n]$
2. Compatibilité avec la multiplication
   Si $a \equiv b \ \ [n]$ et $a' \equiv b' \ \ [n]$, alors $aa' \equiv bb' \ \ [n]$

Démonstration

Propriétés Conséquence

Soit a et b deux entiers relatifs et n un entier supérieur ou égal à 2

1. Si $a \equiv b \ \ [n]$, alors pour tout entier relatif k, on a $ka \equiv kb \ \ [n]$.
2. Si $a \equiv b \ \ [n]$, alors pour tout entier naturel p, on a $a^p \equiv b^p \ \ [n]$.

Exemples