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

Soit a, b, c trois entiers relatifs non nuls.

1. Supposons que a divise b et b divise c.
   Dans ce cas il existe deux entiers relatifs k et k' tel que $b = ka$ et $c = k'b$.
   D'où $c = k'ka$ et par conséquent $\boxed{a \text{ divise } c}$.
2. - Supposons que a divise b et b divise a.
     Dans ce cas il existe deux entiers relatifs k et k' tel que $b = ka$ et $a = k'b$.
     Dons on a $a = k'ka$.
     or $a \neq 0$, donc $k'k = 1$, ce qui signifie que k est un diviseur de 1 et par conséquent $k = 1$ ou $k = -1$. donc $a = b$ ou $a = -b$
   - **réciproquement**
     Si $a = b$ ou $a = -b$, alors a divise b et b divise a.
   - Donc $\boxed{a \text{ divise } b \text{ et } b \text{ divise } a \text{ si et seulement si } a = b \text{ ou } a = -b}$
3. Supposons que a divise b et a divise c, donc il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = kb$.

Soient α et β deux entiers relatifs
. On a alors $\alpha b + \beta c = \alpha \times ka + \beta \times k'a = a \times (\alpha k + \beta k')$, $\boxed{\text{donc } a \text{ divise } \alpha b + \beta c}$

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 :
Soient $n \in \mathbb{N}$ et d un diviseur commun à $2n+3$ et $6n+8$.
Donc d divise $3 \times (2n+3) - (6n+8)$, et par conséquent d divise 1, donc $d \in \{-1; 1\}$.
D'autre part 1 et -1 sont deux diviseurs communs de $2n+3$ et $6n+8$. Donc $2n+3$ et $6n+8$ sont premier entre eux.

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

1. Existence
   $\mathbb{N}$ étant archimédien, l'ensemble des entiers naturels n tels que $a < nb$ est non vide. Il admet donc un plus petit élément que l'on note q_0.
   On a donc $(q_0 - 1)b \leq a < q_0 b$
   On pose $q = q_0 - 1$, d'où :

$$\begin{array}{rcccl} qb & \leq & a & < & (q+1)b \\ qb-qb & \leq & a-qb & < & (q+1)b-qb \\ 0 & \leq & a-qb & < & b \end{array}$$

On pose $r = a - qb$ et on a :

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

D'ou l'existence de deux entiers naturels tels que :

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

2. 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 $\begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases}$.
Alors $bq + r = bq' + r'$, ce qui donne $b(q - q') = r - r'$.
$r - r'$ est donc un multiple de b
De plus $\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases}$ d'où $\begin{cases} 0 \leq r < b \\ -b < -r' \leq 0 \end{cases}$ donc $-b < r - r' < b$.
Or le seul multiple de b strictement compris entre $-b$ et b est 0, donc $r - r' = 0$.
On alors $r = r'$.
D'où $b(q - q') = r - r' = 0$, or $b \neq 0$ et par conséquent on a $q - q' = 0$, donc $q = q'$.
Le couple (q, r) est donc unique.

Exemples

- $46 = 3 \times 12 + 10$ et $0 \leqslant 10 < 12$, donc 3 et 10 sont respectivement le quotient et le reste dans la division euclidienne de 46 par 12.
- $46 = 15 \times 3 + 1$ et $0 \leqslant 1 < 3$, donc 15 et 1 sont respectivement le quotient et le reste dans la division euclidienne de 46 par 3.

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

Si $a \in \mathbb{N}$, la division euclidienne dans N assure l'existence et l'unicité du quotient et du reste dans la division euclidienne de a par $b \in \mathbb{N}^*$.

Supposons alors $a < 0$.

1. Existence :
   Dans ce cas, $-a \in \mathbb{N}$, donc in existe un unique couple d'entiers naturel (q', r') tels que :
   $$\begin{cases} -a = bq' + r' \\ 0 \leqslant r' < b \end{cases}$$
   On a deux cas :
   - Si $r' = 0$, alors $a = b \times (-q')$, d'où l'existence et l'unicité du couple d'entier relatifs $(q, 0)$ définissant le quotient et le reste de la division euclidienne de a par b.
   - Supposons $r \neq 0$.
     On a alors :
     $a = -bq - r = -bq' - b + b - r' = b(-q' - 1) + b - r'$
     or $0 < r' < b$ donc $0 > -r' > -b$ et par conséquent $b > b - r' > 0$.
     On pose $q = -q' - 1$ et $r = b - r'$, d'où l'existence du couple d'entier relatifs $(q, 0)$ définissant le quotient et le reste de la division euclidienne de a par b.
2. Unicité
   Le même raisonnement que celui fait dans la démonstration de l'unicité du quotient et du reste dans la division euclidienne dans $\mathbb{N}$ permettra de conclure à l'unicité du couple (q, r).

Exemples

- $-46 = -4 \times 12 + 2$ et $0 \leqslant 2 < 12$, donc -4 et 2 sont respectivement le quotient et le reste dans la division euclidienne de -46 par 12.
- $-46 = -16 \times 3 + 2$ et $0 \leqslant 2 < 3$, donc -15 et 2 sont respectivement le quotient et le reste dans la division euclidienne de -46 par 3.

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 $aa' \equiv bb' \ \ [n]$

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 $a^p \equiv b^p \ \ [n]$.