

Divisibilité dans \mathbb{Z}

Divisibilité dans \mathbb{Z} \mathbb{N} désigne l'ensemble des entiers naturels $\{0, 1, 2, \dots\}$

\mathbb{Z} désigne l'ensemble des entiers relatifs $\{\dots, -2, -1, 0, 1, 2, \dots\}$

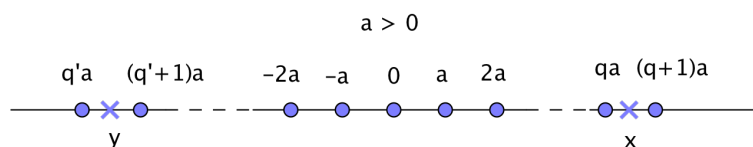
Définition : a et b deux entiers relatifs on dit que b divise a , ou a est un multiple de b (notation $b|a$) lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = bq$

Exemple : $5|10$ car $10 = 5 \times 2$, $-5|10$ car $10 = -5 \times -2$

Exercice 1 Démontrer :

1. $\forall x \in \mathbb{Z}, 1|x$ et $x|0$
2. $0|x \iff x = 0$
3. $a|b \iff -a|b \iff a| -b$
4. $c|a$ et $c|b$ entraîne que $c|(a + b)$ puis $c|(a - b)$ puis plus généralement toute **combinaison linéaire** $au + bv$ où u et v sont des entiers relatifs
5. $\forall x, y, z \in \mathbb{Z}$ si $x|y$ et $y|z$ alors $x|z$ (transitivité de la divisibilité)
6. Si $a|b$ et $b \neq 0$ alors $0 \leq |a| \leq |b|$
7. Si $a|b$ et $b|a$ alors $a = b$ ou $a = -b$

On note $a\mathbb{Z}$ avec $a \in \mathbb{N}$ car $2\mathbb{Z} = -2\mathbb{Z}$ l'ensemble des multiples de a



Intuitivement pour tout $a \in \mathbb{Z}$, l'ensemble $a\mathbb{Z}$ forme un **réseau** de \mathbb{Z} , c'est à dire un sous-ensemble de points de $a\mathbb{Z}$ régulièrement espacés

Il s'agit de démontrer en exercice le théorème suivant

Théorème de la division euclidienne : $\forall a \in \mathbb{Z} \forall b \in \mathbb{N}^* \exists !q \in \mathbb{Z} \exists !r \in \mathbb{N}$ tel que $a = bq + r$ avec $0 \leq r < b$

à partir de la propriété admise suivante

Propriété Toute partie P non vide de \mathbb{N} admet un **unique** plus petit élément notée $\min(P)$

Considérer l'ensemble $E = \{a - kb \geq 0 | k \in \mathbb{Z}\}$. Vérifier que E est non vide (trouver un élément simple de E (pour chaque cas $a > 0$ et $a < 0$ puis utiliser la propriété ci-dessus

Exercice 3 : Pour quelles valeurs de n entier, l'expression $4n + 1$ est un multiple de 3?

Exercice 4 : Montrer que pour tout $n \in \mathbb{N}^*$, $4^n + 1$ n'est pas divisible par 3

(Indication : écrire $4^n + 1 = (3 + 1)^n + 1$ et utiliser la formule de Newton)

Algorithme d'Euclide (voir TP)

Définition $p \in \mathbb{N}$ tel que $p > 2$ est dit premier si les seuls diviseurs de p sont 1 et p

Exemples : 2,3, 5, 7, 11, 13, 17, 19...97

Exercice 5 : Il existe une infinité de nombres premiers (Faire un raisonnement par l'absurde, supposer qu'il existe un nombre fini de nombres premiers p_1, p_2, \dots, p_n et montrer que le nombre $N = p_1 p_2 \dots p_n + 1$ est premier

Théorème 2 : Tout entier relatif se décompose de manière unique en un produit de facteurs premiers

Autrement dit : $\forall a \in \mathbb{Z} \exists p_i$ premiers uniques et α_i entiers naturels uniques tel que $a = \pm \prod_i p_i^{\alpha_i}$

(Pour l'existence faire une démonstration par récurrence sur le nombre de facteurs premiers, pour l'unicité utiliser le théorème de la division euclidienne)

Exercice 6 : Si p premier divise ab mais p ne divise pas a alors p divise b

$0 \times -b$	$\times 1$	$2 \times -b+2$	
$b \bar{0} \times$	$b+1 \bar{1}$	$\bar{2} \times$	$\overline{b-1}$
$\times 2b$	$\times -b+1$	$b+2 \bar{2} \times$	
\times	\times	\times	

Partition de \mathbb{Z} . Congruences dans \mathbb{Z} Avoir le même reste par la division euclidienne par b partitionne \mathbb{Z} , c'est à dire "découpe" \mathbb{Z} en b parties infinies disjointes, autant que les restes possibles par la division par $b : 0, 1, 2, \dots, b-1$

Définition Etant donné n un entier naturel ≥ 2 . On dit que a et b sont congrus modulo n si a et b ont le même reste par la division par n . On note cela $a \equiv b [n]$. Autrement dit a et b différent d'un multiple de n , c'est à dire il existe $q \in \mathbb{Z}$ tel que $a - b = qn$

Exemple : $2017 \equiv 37 [9]$, $-34 \equiv 2 [9]$, $1171291471001 \equiv 1171291471098 [97]$

Exercice 7

Prouver

- $\forall a \in \mathbb{Z} a \equiv a [n]$ (on dit que \equiv est une relation réflexive sur \mathbb{Z}^2)
- $\forall a \in \mathbb{Z}$ si $a \equiv b [n]$ alors $b \equiv a [n]$ (on dit que \equiv est une relation symétrique sur \mathbb{Z}^2)
- $\forall a \in \mathbb{Z}$ si $a \equiv b [n]$ et si $b \equiv c [n]$ alors $a \equiv c [n]$ (on dit que \equiv est une relation transitive sur \mathbb{Z}^2)
- On note $\bar{k} = n\mathbb{Z} + k$ pour k entier tel que $0 \leq k \leq n-1$
 $\forall x \in \bar{k} x \equiv k [n]$
- Les sous ensembles \bar{k} pour $0 \leq k \leq n-1$ forment une partition de \mathbb{Z} , c'est à dire \mathbb{Z} est la réunion disjointe des n sous-ensembles \bar{k}

Exercice 8(compatibilité de \equiv avec $+$ et \times)

Prouver que

- si $a \equiv a' [n]$ et $b \equiv b' [n]$ alors $a + b \equiv a' + b' [n]$
- si $a \equiv a' [n]$ et $b \equiv b' [n]$ alors $a \times b \equiv a' \times b' [n]$
- si $a \equiv b [n]$ alors $a^k \equiv b^k [n]$ pour tout k entier
- si $a \equiv b [n]$ alors $f(a) \equiv f(b) [n]$ où $f(x) = a_n x^n + \dots + a_1 x + a_0$ avec $a_i \in \mathbb{Z}$