DIVISIBILITÉ

Jean Chanzy

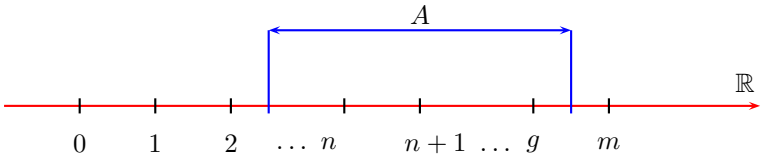
Université de Paris-Sud *

L'Arithmétique est l'étude des nombres entiers. Le domaine privilégié d'application est l'informatique, où l'on code l'information en utilisant des suites de 0 et de 1 (représentation binaire). L'Arithmétique étudie l'ensemble $\mathbb{N}$ des entiers naturels ($\mathbb{N} = \{0; 1; 2; \ldots; n; \ldots\}$), et l'ensemble $\mathbb{Z}$ des entiers relatifs ($\mathbb{Z} = \{\ldots; -m; \ldots; -2; -1; 0; 1; 2; \ldots; m; \ldots\}$). $\mathbb{N} \subset \mathbb{Z}$.

1 Propriétés de $\mathbb{N}$:

On utilisera dans $\mathbb{N}$ les trois axiomes suivants, dits de Péano :

1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
2. Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
   Soit A; $A \neq \emptyset$; $A \subset \mathbb{N}$, ce qui revient à dire que A est une partie ou un sous-ensemble non vide de $\mathbb{N}$. Écrire :
   $$\forall x \in A,\ \exists m \in \mathbb{N};\ x \leq m,$$
   c'est écrire que la partie A de $\mathbb{N}$ est majorée par m. Le plus petit de tous les entiers naturels m vérifiant cette propriété est le plus grand élément g de A. On dit alors que g est le plus petit majorant de A.



3. Toute suite d'entiers naturels strictement décroissante est finie.

Propriété fondamentale de $\mathbb{N}$; raisonnement par récurrence : *Le raisonnement par récurrence est utilisé pour démontrer qu'une propriété $\mathcal{P}(n)$, dépendant d'un paramètre $n \in \mathbb{N}$ est vraie $\forall n$. Il y a deux étapes dans une démonstration par récurrence :*

1. *Initialisation : On démontre que la propriété $\mathcal{P}(0)$ est vraie, en prenant pour n la plus petite valeur possible de n, ici $n = 0$.*
2. *Propriété héréditaire : On démontre que $\forall n \in \mathbb{N}$, $\mathcal{P}(n)$ vraie $\Rightarrow \mathcal{P}(n+1)$ vraie.*

Remarque : Il y a deux variantes possibles dans la démonstration par récurrence :

1. La propriété peut n'être vraie qu'à partir du rang n_0, et donc l'initialisation se fait à partir de $n = n_0$.
2. L'hypothèse de récurrence peut être $\forall k \in \mathbb{N}$ tel que $0 \leq k \leq n$, $\mathcal{P}(k)$ est vraie, et ainsi la propriété héréditaire se démontre de la manière suivante :
   $$(\forall k \in \mathbb{N};\ 0 \leq k \leq n;\ \mathcal{P}(k)\ vraie) \Rightarrow \mathcal{P}(n+1)\ vraie$$

♣

*Université de Paris-Sud,Bâtiment 425;F-91405 Orsay Cedex

2 Divisibilité dans $\mathbb{Z}$:

Définition 2.1. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On dit que a divise b s'il existe un entier q, appelé « quotient de b par a », tel que $b = aq$. Si a divise b, on note $a|b$.*

Remarque : Si a divise b, on dit aussi « b est divisible par a », ou « a est un diviseur de b », ou « b est un multiple de a ». ♣

Propriétés

1. *Tout entier naturel non nul a un nombre fini de diviseurs.*
2. *Tout diviseur positif d d'un entier naturel n vérifie $1 \leq d \leq n$, et tout diviseur d d'un entier relatif m vérifie $-m \leq d \leq m$.*
   Démonstration des deux propriétés précédentes : Soit n un entier naturel non nul. L'entier d divise n s'il existe un entier q tel que $n = qd$. Si $d > 0$, $q > 0$ et $q \geq 1$. D'où $n \geq d$. Alors n a au plus n diviseurs dans $\mathbb{N}$, et $1 \leq d \leq n$ si $d \in \mathbb{N}$. Si $d \in \mathbb{Z}$, n a au plus $2n$ diviseurs dans $\mathbb{Z}$. □

   Exemple : $n = 10$. L'ensemble des diviseurs de 10 est $\mathcal{D}(10) = \{1; 2; 5; 10\}$ dans $\mathbb{N}$, et $\mathcal{D}(10) = \{-10; -5; -2; -1; 1; 2; 5; 10\}$ dans $\mathbb{Z}$. ♣
3. $1|a$, $\forall a \in \mathbb{Z}$.
4. $a|a$, $\forall a \in \mathbb{Z}^*$.
   Démonstration des deux propriétés précédentes : $a = a \times 1$ et $a = 1 \times a$. □

Théorème *Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$.*

1. *Si $a|b$, alors $a|bc$, $\forall c \in \mathbb{Z}$.*
2. *Si $a|b$ et $b|c$, alors $a|c$, $\forall c \in \mathbb{Z}$.*
3. *Si $a|b$ et $a|c$, alors $a|mb + nc$, $\forall m \in \mathbb{Z}$, $\forall n \in \mathbb{Z}$.*
4. *Si $a|b$ et $b \neq 0$, alors $|a| \leq |b|$.*
5. *Si $a|b$ et $b|a$, alors $b = a$ ou $b = -a$.*

Démonstration :

1. Si $a|b$, alors $\exists q \in \mathbb{Z}$ tel que $b = qa$, et $bc = qac = (qc)a$, donc $a|bc$.
2. Si $a|b$ et $b|c$, alors $\exists q \in \mathbb{Z}$, $\exists k \in \mathbb{Z}$ tels que $b = qa$ et $c = kb$. Dans ces conditions, $c = (kq)a$, et $a|c$.
3. Si $a|b$ et $a|c$, alors $\exists q \in \mathbb{Z}$, $\exists k \in \mathbb{Z}$ tels que $b = qa$ et $c = ka$. Dans ces conditions, $\forall m \in \mathbb{Z}$, $\forall n \in \mathbb{Z}$, $mb + nc = m(qa) + n(ka) = (mq + nk)a$ et $a|mb + nc$.
4. Si $a|b$ et $b \neq 0$, alors $\exists q \in \mathbb{Z}^*$ tel que $b = qa$. Dans ces conditions, $|b| = |q||a|$. Comme $|q| \geq 1$, $|b| \geq |a|$.
5. Si $a|b$ et $b|a$, alors $\exists q \in \mathbb{Z}$, $\exists k \in \mathbb{Z}$ tel que $b = qa$ et $a = kb$. Dans ces conditions, $b = (qk)b$, et $qk = 1$, donc $q = k = 1$ ou $q = k = -1$.

□