Mathématiques expertes
Arithmétique 1

Serge Bays

Lycée les Eucalyptus

31 août 2021

L'objectif de ce chapitre est d'étudier quelques propriétés des ensembles $\mathbb{N}$ et $\mathbb{Z}$ ainsi que certaines relations des nombres entre eux et avec des opérations (l'addition et la multiplication sont les opérations de base).
La division euclidienne et les nombres premiers sont des outils privilégiés.

Quelques mathématiciens

1. Pythagore (grec 580 av JC-495 av JC)
2. Euclide (grec 300 av JC)
3. Eratosthène (grec 3e siècle av JC)
4. Bachet de Méziriac (français 1581-1638)
5. Pierre de Fermat (français 1607-1665)
6. Bézout (français 1730-1783)
7. Gauss (allemand 1777-1855)
8. Euler (suisse 1707-1783)
9. Péano (italien 1858-1932)

Théorème
Soit A une partie de $\mathbb{N}$;
si $0 \in A$ et si pour tout n appartenant à $\mathbb{N}$, $n \in A \Rightarrow (n+1) \in A$
alors $A = \mathbb{N}$

Remarque : $(n+1)$ est appelé le successeur de n.

Ce théorème dit que :
si [A est une partie de $\mathbb{N}$ contenant 0 et si A contient un entier alors il contient aussi son successeur],
alors $A = \mathbb{N}$.

Théorème

Soit $P(n)$ une propriété dépendant de n. Si $P(n)$ vérifie les deux conditions suivantes :

- $P(0)$ est vraie
- pour tout $n \in \mathbb{N}$, si $P(n)$ est vraie alors $P(n+1)$ est vraie (on dit que $P(n)$ est héréditaire)

Alors $P(n)$ est vraie pour tout n.

Remarques

Ce théorème constitue le principe du raisonnement par récurrence.

Si on remplace dans le théorème « $P(0)$ est vraie » par « $P(a)$ est vraie » où a est un entier naturel déterminé alors la conclusion est que $P(n)$ est vraie pour tout n tel que $a \leq n$.

Propriété 1
Si a et b sont deux entiers naturels avec b non nul alors il existe un entier n tel que $a \leq nb$.

Démonstration
Si $a = 0$ nous pouvons prendre $n = 1$
Si a est non nul nous pouvons prendre $n = a$ puisque $1 \leq b \Rightarrow a \leq ab$.

Propriété 2
Si A est une partie de $\mathbb{N}$ non vide alors elle admet un plus petit élément.
C'est-à-dire qu'il existe un entier a de A tel que pour tout n appartenant à A, $a \leq n$.

Cette propriété est admise.

Théorème et définition

Soient a et b deux entiers naturels quelconques avec b non nul. Il existe un couple unique d'entiers naturels (q, r) tel que $a = bq + r$ et $r < b$.

Les nombres q et r s'appellent respectivement le *quotient* et le *reste* de la division euclidienne de a, nommé le *dividende*, par b, nommé le *diviseur*.

Démonstration

- Existence de q et de r

D'après la propriété (1), l'ensemble A de tous les entiers n tel que $a < nb$ est non vide.
D'après la propriété (2), A possède un plus petit élément m.
Puisque $a < mb$, on a $1 \leq m$.
Posons $q = m - 1$. Alors $qb \leq a < b(q+1)$.
C'est-à-dire $a < bq + b$; donc en posant $r = a - bq$, l'entier r vérifie $r < b$ et $a = bq + r$.

- Unicité de q et r
Supposons qu'il existe deux couples (q_1, r_1) et (q_2, r_2) vérifiant $a = bq_1 + r_1 = bq_2 + r_2$, $r_1 < b$ et $r_2 < b$.
Alors $r_2 - r_1 = b(q_1 - q_2)$.
Si $r_1 \neq r_2$, par exemple $r_1 < r_2$, on $q_2 < q_1$. On en déduit que $1 \leq q_1 - q_2$, d'où $b \leq b(q_1 - q_2)$, c'est-à-dire $b \leq r_2 - r_1$.
Alors $b \leq r_2$ ce qui est en contradiction avec l'hypothèse $r_2 < b$.
Donc $r_1 = r_2$ ce qui entraîne $q_1 = q_2$.

L'opération soustraction n'est pas toujours possible dans $\mathbb{N}$.
A partir de l'ensemble $\mathbb{N}$, on construit un ensemble plus vaste $\mathbb{Z}$, ensemble des entiers relatifs, sur lequel on étend les propriétés des opérations de $\mathbb{N}$. Sur ce nouvel ensemble l'opération soustraction est toujours possible.

Théorème

Soit a appartenant à $\mathbb{Z}$ et b appartenant à $\mathbb{N}$ avec b non nul ; alors il existe au moins un couple (q, r) d'éléments de $\mathbb{Z}$ tel que $a = bq + r$ et $-b < r < b$.

Démonstration

A partir de la division euclidienne de a par b, où a et b sont des entiers naturels avec b non nul, soit $a = bq + r$ et $0 \leq r < b$, on obtient l'égalité : $(-a) = b(-q) + (-r)$.
Si $0 \leq r < b$ alors $-b < -r \leq 0$.

Division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{N}^*$

Si $a \in \mathbb{Z}$, si b est un entier naturel non nul alors il existe un couple (q, r) unique tel que $a = bq + r$ et $0 \leq r < b$.

Démonstration

Si $a \geq 0$, c'est la division euclidienne dans $\mathbb{N}$.
Si $a < 0$, alors d'après le théorème précédent, il existe deux entiers relatifs négatifs q' et r' tels que $a = bq' + r'$ avec $-b < r' \leq 0$.
On pose $q = q' - 1$ et $r = r' + b$.
Alors $a = bq + r$ avec $0 \leq r < b$.

Définition

Soient a et b deux entiers relatifs.
S'il existe un entier relatif k tel que $b = ka$, on dit que b est un *multiple* de a.

Propriétés et définition

Pour tout entier relatif n,

- 0 est un multiple de n ;
- Si $n \neq 0$, l'ensemble des multiples de n est infini ;
- L'ensemble des multiples de n est l'ensemble des nombres kn où k appartient à $\mathbb{Z}$.

Exemples :

ensemble des multiples de 3 : $\{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

ensemble des multiples de 0 : $\{ 0 \}$

Propriétés

- Pour tout entier relatif n, les multiples de n sont les multiples de $(-n)$
- Si a est un entier relatif multiple de n, alors $(-a)$ est un multiple de n.
- Si a et b sont deux entiers relatifs multiples de n, alors $(a+b)$ est un multiple de n.

Définition

Soit a et b deux entiers relatifs. On dit que a divise b, ou que a est un diviseur de b, ou que b est divisible par a si et seulement si b est un multiple de a, c'est-à-dire :
il existe un entier relatif k tel que $b = ka$.

On note $a \mid b$.

Propriétés

- 0 a une infinité de diviseurs.
- Tout entier relatif n a au moins quatre diviseurs : $1, -1, n, -n$.
- Tout entier relatif n non nul a un nombre fini de diviseurs. On note cet ensemble D_n.
  Exemple : L'ensemble des diviseurs de 6 est $D_6 = \{-6, -3, -2, -1, 1, 2, 3, 6\}$.

Propriété

Etant donnés a, b et c entiers relatifs quelconques
Si a divise b et si b divise c alors a divise c.

Démonstration

S'il existe k et k' entiers relatifs tels que $b = ka$ et $c = k'b$ alors $c = k'ka$.

Propriété

Etant donnés a, b et c entiers relatifs quelconques.
Si a divise b et c alors a divise $(b+c)$ et $(b-c)$.

Démonstration

Si $b = k_1 a$ et $c = k_2 a$, alors $(b+c) = (k_1 + k_2)a$ et $(b-c) = (k_1 - k_2)a$.

Définition

Soit n un entier naturel non nul.
Deux entiers relatifs a et b sont dits congrus modulo n si et seulement si $a - b$ est un multiple de n.

Autrement dit, il existe un entier relatif k tel que $a = b + kn$
On dit que a est congru à b modulo n et on écrit $a \equiv b \ [n]$.

(On écrit aussi : $a \equiv b \mod n$).

Remarque

Un entier relatif a est divisible par n si et seulement si $a \equiv 0 \ [n]$.

Exemples : $185 = 37 \times 5$ donc $185 \equiv 0 \ [5]$.
$187 - 2 = 37 \times 5$ donc $187 \equiv 2 \ [5]$.

Propriété

Soit n un entier naturel non nul.
Deux entiers relatifs a et b sont congrus modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration

Effectuons la division euclidienne de a par n : $a = nq + r$, avec $0 \leq r < n$.
D'où $a - r = nq$, c'est-à-dire $a - r$ est un multiple de n.
a et b sont congrus modulo n si et seulement si $a - b = kn$ avec $k \in \mathbb{Z}$.
Ceci est équivalent à : $a - r = nq$ et $(a - r) - (a - b) = n(q - k)$, soit à : $a - r = nq$ et $b - r = nq'$.
Puisque $0 \leq r < n$, ceci signifie que a et b ont le même reste r dans la division euclidienne par n.

Théorème

Soient a, b, r, s quatre entiers relatifs tels que $a \equiv r \ [n]$ et $b \equiv s \ [n]$. Alors

$a + b \equiv r + s \ [n]$

$a - b \equiv r - s \ [n]$

$a \times b \equiv r \times s \ [n]$

$a^k \equiv r^k \ [n]$ (pour tout k appartenant à $\mathbb{N}$)

Démonstrations en exercice.

Remarque

On peut traduire le théorème précédent en terme de reste.
Si r et s sont les restes respectifs des divisions euclidiennes de a et b par n alors dans la division euclidienne par n :
$a + b$ a le même reste que $r + s$
$a - b$ a le même reste que $r - s$
$a \times b$ a le même reste que $r \times s$
a^k le même reste que r^k