Chapitre 13 : Arithmétique

Table des matières

Contenu

- Notations $\mathbb{N}$ et $\mathbb{Z}$.
- Définition des notions de multiple, de diviseur, de nombre pair, de nombre impair.

1 Divisibilité dans $\mathbb{Z}$

Définition:
Soit $a, b \in \mathbb{Z}$, on dit que a divise b, noté $a|b$, s'il existe $k \in \mathbb{Z}^*$ tel que $b = ak$

Exemple:

- 4 divise 12 car $12 = 4 \times 3$.
- 15 divise 75 car $75 = 15 \times 5$

Remarque

La formulation "a divise b" est la même que :

- "a est un diviseur de b".
- "b est divisible par a".
- "b est un multiple de a".

Exemple:
-7 est un diviseur de 63 car $63 = (-7) \times (-9)$
L'ensemble des diviseurs de 63 est $\{-63, -21, -9, -7, -3, -1, 1, 3, 7, 9, 21, 63\}$

Remarque

- 0 est multiple de tout entier relatif n car $n \times 0 = 0$.
- Tout entier n a au moins $1, -1, n$ et $-n$ comme diviseurs.

Exercice:

1. Déterminer les entiers naturels n tels que 9 divise $n + 4$.
2. Déterminer les entiers naturels n tels que $2n + 7$ divise 10.

Propriété:
Soit $a, b, c \in \mathbb{Z}$ tels que $a|b$ et $b|c$, alors $a|c$

Démonstration: *(Hors programme)*
Supposons que $a|b$ et $b|c$, il existe alors $k, k' \in \mathbb{Z}$ tels que :

$$b = ka \quad \text{et} \quad c = k'b$$

On a alors :

$$c = k'b = kk'a \implies a|c$$

Définition:
Un entier est pair s'il est multiple de 2. Sinon, il est impair.
Un entier pair est de la forme $2k$ où $k \in \mathbb{Z}$ et un entier impair $2k+1$.

Propriété:

- Si un entier n est pair, alors n^2 est pair.
- Si un entier n est impair, alors n^2 est impair.

Les contraposées sont donc vraies.

Démonstration:
Démontrons le premier point, le deuxième reposant sur le même principe.
Soit n un entier pair, il existe alors $k \in \mathbb{Z}$ tel que $n = 2k$.
On a alors $n^2 = 4k^2 = 2k' \in 2\mathbb{Z}$ avec $k' = 2k^2$. D'où le résultat.

Exercice:
Déterminer tous les entiers n tels que $n^2 - 1$ soit multiple de 4.

2 Nombres premiers

Définition:
Un nombre est dit premier s'il n'admet que deux diviseurs positifs : 1 et lui même.

Exemple:
$2, 3, 5, 7, 11, 13, 17...$

Propriété:
Il existe une infinité de nombres premiers.

Démonstration: *(Hors programme)*
Supposons par l'absurde qu'il n'en existe qu'un nombre fini n ordonné tels que p_1 soit le plus petit et p_n le plus grand.
Posons $N = p_1...p_n + 1$.
On a

$$\begin{aligned} N &\equiv 1 \pmod{p_1} \\ N &\equiv 1 \pmod{p_2} \\ &.... \\ N &\equiv 1 \pmod{p_n} \end{aligned} \tag{1}$$

C'est-à-dire que N n'est divisible par aucun autre nombre premier que 1 et lui même d'après le théorème fondamental de l'arithmétique. N est par ailleurs évidemment supérieur strictement à p_n. D'où l'absurdité. D'où le résultat.

Propriété: *Crible d'Eratosthène*
Soit n un nombre entier supérieur ou égal à 2. Alors, il admet un diviseur premier.
Si de plus n n'est pas premier, alors il admet un diviseur premier inférieur ou égal à $\sqrt{n}$

Theorème: *Fondamental de l'arithmétique*
Tout entier naturel, supérieur ou égal à 2, est soit un nombre premier, soit décomposable de manière unique en un produit de nombres premiers.

Démonstration: *(Hors programme)*
Il y a deux choses à montrer ici, l'existence et l'unicité.

- **Existence:** Raisonnons par récurrence:
  - Initialisation :
    Nous avons que $2 = 1 \times 2$ d'où l'écriture en produit de facteurs premiers.
  - Hérédité: Soit $n \geq 2$, supposons que tout entier strictement inférieur à n s'écrit comme produit de facteurs premiers.
    Soit $p > 1$ le plus petit entier divisant n (celui-ci existe bien car l'ensemble des diviseurs de n est une partie finie de $\mathbb{N}$).
    On a alors que p est premier, en effet tout diviseur de p est diviseur de n et donc vaut p ou 1 par minimalité de p.
    On peut alors écrire $n = p \times \frac{n}{p}$.
    $\frac{n}{p}$ est un entier qui peut s'écrire comme produit de facteurs premiers par hyptohèse de récurrence et p est premier.
    D'où l'hérédité.
  - Conclusion: La propriété est initialisée et est héréditaire, elle est donc vraie sur $\mathbb{N}$.
- **Unicité:**
  Supposons par l'absurde qu'un entier n possède deux décompositions en facteurs premiers distinctes :

$$n = p_1 \ldots p_r \quad \text{et} \quad n = q_1 \ldots q_s \implies p_1 \ldots p_r = q_1 \ldots q_s$$

  On a alors par exemple que $p_1 | q_1$ ou $p_1 | q_2$ ou ... ou $p_1 | q_s$.
  Or les q_i sont des nombres premiers, on a donc par exemple (à renommage près) que $p_1 = q_1 \neq 0$. On a alors :

$$p_2 \ldots p_r = q_2 \ldots q_s$$

  On réitère ce processus et on obtient donc l'unicité.

Exemple:
On a $250 = 2 \cdot 5^3$

3 Exercice bilan

- Décomposer en produit de facteurs premiers les nombres suivants :
  486 ; 42 ; 36 ; 27 ; 1848 ; 105 ; 126.
- Simplifier les fractions suivantes en utilisant la décomposition en facteurs premiers :
  $\frac{36}{42}$; $\frac{486}{1848}$; $\frac{126}{105}$