

Arithmétique

Prélude - Historique et contexte

L'arithmétique est la branche des mathématiques qui étudie les nombres entiers. Euclide, vers 300 avant notre ère, démontre déjà qu'il existe une infinité de nombres premiers. Longtemps considérée comme la plus « pure » des mathématiques, sans application pratique, elle est aujourd'hui au cœur de la cryptographie : chaque paiement par carte bancaire ou message chiffré repose sur des propriétés des nombres premiers.

I Entiers naturels et entiers relatifs

Définition

- $\mathbb{N} = \{0 ; 1 ; 2 ; 3 ; \dots\}$ est l'ensemble des **entiers naturels**.
- $\mathbb{Z} = \{\dots ; -2 ; -1 ; 0 ; 1 ; 2 ; \dots\}$ est l'ensemble des **entiers relatifs**. On a $\mathbb{N} \subset \mathbb{Z}$.

II Multiples et diviseurs

Définition

Soient a et b deux entiers relatifs. On dit que a est un **multiple** de b s'il existe un entier relatif k tel que $a = k \times b$.

On dit aussi que b est un **diviseur** de a , ou que b **divise** a .

Exemple

$42 = 6 \times 7$ donc 42 est un multiple de 7 et 7 est un diviseur de 42.

$-15 = (-3) \times 5$ donc -15 est un multiple de 5.

$0 = 0 \times b$: 0 est multiple de tous les entiers.

Propriété (démonstration exigible)

La somme de deux multiples d'un entier a est un multiple de a .

Démonstration : si $m = ka$ et $n = k'a$ avec $k, k' \in \mathbb{Z}$, alors $m + n = ka + k'a = (k + k')a$ et $k + k' \in \mathbb{Z}$.

Rappel - Critères de divisibilité

Un entier est divisible :

- par 2 si son chiffre des unités est 0, 2, 4, 6 ou 8 ;
- par 3 si la somme de ses chiffres est divisible par 3 ;
- par 5 si son chiffre des unités est 0 ou 5 ;
- par 9 si la somme de ses chiffres est divisible par 9 ;
- par 10 si son chiffre des unités est 0.

III Parité

Définition

- Un entier n est **pair** s'il est multiple de 2 : il existe $k \in \mathbb{Z}$ tel que $n = 2k$.
- Un entier n est **impair** s'il n'est pas pair : il existe alors $k \in \mathbb{Z}$ tel que $n = 2k + 1$.

Propriété (démonstration exigible)

Le carré d'un nombre impair est impair.

Démonstration : si $n = 2k + 1$ alors $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ avec $2k^2 + 2k \in \mathbb{Z}$: n^2 est impair.

Exemple

Montrer que la somme de deux entiers consécutifs est toujours impaire.

Deux entiers consécutifs s'écrivent n et $n + 1$. Leur somme vaut $2n + 1$, qui est impair.

IV Nombres premiers

Définition

Un entier naturel est **premier** s'il admet exactement deux diviseurs positifs : 1 et lui-même.

Les premiers nombres premiers sont : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; ... (1 n'est pas premier).

Propriété

Tout entier supérieur ou égal à 2 se décompose en produit de facteurs premiers, de façon unique à l'ordre près.

Exemple : $360 = 2^3 \times 3^2 \times 5$.

Remarque - Python

```
def est_multiple(a, b):  
    return a % b == 0      # % donne le reste de la division  
  
def diviseurs(n):  
    return [d for d in range(1, n + 1) if n % d == 0]
```