Chapitre 16 : Arithmétique

L'arithmétique, du grec arithmos = nombre, est une branche des mathématiques qui correspond à la science des nombres. Dès l'antiquité (et l'apparition des nombres), on s'intéresse à ceux-ci : pair ou impair (Pythagore), division euclidienne et nombres premiers (Euclide), congruence (Gauss), ...

I) Multiples et diviseurs dans $\mathbb{Z}$

Définition : $\mathbb{N}$: Entiers naturels $\{0; 1; 2; 3; 4; 5; 6; \dots\}$

$\mathbb{Z}$: Entiers relatifs $\{\dots -2; -1; 0; 1; 2; \dots\}$

Division euclidienne :

Soit a et b deux entiers relatifs avec b non nul.

Il existe un unique couple (q, r) tels que $a = b \times q + r$ et $0 \leq r < |b|$

Remarque : La différence avec ce que vous avez déjà vu, c'est que là on peut parler de division euclidienne avec des nombres négatifs. Par exemple : $-27 = -5 \times 5 + 3$

Définition:

Soient des entiers relatifs non nuls n, p tels que le reste de la division euclidienne de n par p soit 0. Il existe donc un entier relatif k tel que : $n = p \times k$

On dit que : n est un **multiple** de p

n est **divisible** par p

p est un **diviseur** de n

Propriété :

Soient trois entiers relatifs m, n et a .

Si m et n sont des multiples de a alors leur somme $(m+n)$, leur différence $(m-n)$ et leur produit sont des multiples de a .

Démonstration de la somme :

Soient m et n deux multiples de a . Il existe donc deux entiers relatifs k_1 et k_2 tels que $m = a \times k_1$ et $n = a \times k_2$.

Nous avons alors $m + n = a k_1 + a k_2 = a(k_1 + k_2)$ et $k_1 + k_2 \in \mathbb{Z}$

Donc $m+n$ est un multiple de a .

Définition: Un **nombre premier** est un nombre qui admet exactement deux diviseurs : 1 et lui-même.

Exemple : 2, 3, 5, 7, 11, 13, 17, 19, 23,

Théorème fondamental de l'arithmétique :

Tout nombre entier, supérieur ou égal à deux, peut se décomposer en produit de facteurs premiers. Cette décomposition est unique.

Démonstration : admise

III) Simplifier une fraction

Méthode 1

Pour simplifier une fraction, il faut diviser en haut et en bas par le même nombre.

$$\frac{35}{140} = \frac{35 \div 7}{140 \div 7} = \frac{5}{20} = \frac{5 \div 5}{20 \div 5} = \frac{1}{4}$$

Définition:

Une fraction est dite irréductible lorsque l'on ne peut plus la simplifier. Elle est irréductible lorsque le numérateur et le dénominateur n'ont pas de diviseurs en commun (à part 1).

Remarque :

Si on vous demande de simplifier une fraction, on veut que vous la simplifier au maximum

Méthode 2

On peut aussi décomposer le numérateur et le dénominateur en produits de facteurs premiers, puis on simplifie en barrant les facteurs commun.

$$\frac{35}{140} = \frac{5 \times 7}{2 \times 2 \times 5 \times 7} = \frac{\cancel{5} \times \cancel{7}}{2 \times 2 \times \cancel{5} \times \cancel{7}} = \frac{1}{4}$$

III) Pairs et impairs

Définition: Soit un nombre entier n . Notons q son quotient et r son reste dans la division euclidienne par 2.

Soit $r = 0$, donc $n = 2q$ et on dit que n est un nombre pair.

Soit $r = 1$, donc $n = 2q + 1$ et on dit que n est un nombre impair.

Parité d'une somme :

La somme de deux nombres pairs est paire.
La somme de deux nombres impairs est paire.
La somme d'un nombre pair et d'un nombre impair est impaire.

Démonstration : vue en cours

Parité d'un carré :

Le carré d'un nombre pair est pair.
Le carré d'un nombre impair est impair.

Démonstration :

Soit n un entier pair. Il existe k tel que $n = 2k$.
 $n^2 = (2k)^2 = 4k^2 = 2 \times (2k^2)$ donc n^2 est pair.

Soit n un entier impair. Il existe k tel que $n = 2k + 1$.
 $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \times (2k^2 + 2k) + 1$ donc n^2 est impair.

A quoi ça sert ?

L'arithmétique trouve des applications dans la cyber-sécurité (mot de passe, code bancaire, ...), les codes (codes barres, code sécu, ...), la cryptographie (messages secrets, ...). Vous pouvez devenir millionnaire en résolvant certains problèmes d'arithmétiques.