5

Arithmétique

Résumé

D'abord d'intérêt ludique pour les mathématiciens, l'arithmétique a su prendre une importance cruciale dans nos vies avec l'arrivée des ordinateurs et de la cryptologie où l'arithmétique y est centrale. Tour d'horizon de choses connues et de quelques propriétés plus avancées.

1 Multiples et diviseurs

Définitions

Soient $n, k \in \mathbb{Z}$ tel qu'il existe $k' \in \mathbb{Z}$ tel que $n = kk'$. On dit que :

- k est un **diviseur** de n.
- n est un **multiple** de k.

Exemple On a $42 = 6 \times 7$ donc 42 est un multiple de 6 et 6 est un diviseur de 42. On dit aussi que 42 est **divisible** par 6 ou que 6 **divise** 42.
L'ensemble des diviseurs de 42 est $\{42, 21, 7, 6, 3, 2, 1, -1, -2, -3, -6, -7, -21, -42\}$.

Remarque Tout nombre entier relatif non nul n est toujours divisible, au moins, par 1 et lui-même et admet une infinité de multiples : n, $2n$, $3n$, $-n$, $-2n$, etc.

Propriété | Somme, différence et produit

Soient $a, n, m \in \mathbb{Z}$. Si les entiers n et m sont deux multiples de a, alors la somme $m + n$, la différence $n - m$ et le produit nm sont aussi des multiples de a.

Définition | Nombre premier

Un **nombre premier** est un nombre entier naturel différent de 1 dont les seuls diviseurs sont 1 et lui-même.

Exemples

- Donnons quelques nombres premiers :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

- 15 n'est pas premier car $15 = 3 \times 5$.

2 Parité

Définitions

Soit $n \in \mathbb{Z}$.

- Si n est divisible par 2, on dit que n est **pair**. Il existe $k \in \mathbb{Z}$ tel que $n = 2k$.
- Sinon, n est dit **impair**. Il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$.

Propriétés | Somme d'entiers

- La somme de deux entiers **pairs** est un nombre **pair**.
- La somme de deux entiers **impairs** est un nombre **pair**.
- La somme d'un entier **pair** et d'un entier **impair** est un nombre **impair**.

Propriété | Parité d'un carré

Soit $n \in \mathbb{Z}$.

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

Démonstration. Soit n un entier relatif.

- Si n est pair, il existe $k \in \mathbb{Z}$ tel que $n = 2k$.
  Dans cas, $n^2 = (2k)^2 = (2k) \times (2k) = 2 \times (2k^2)$ et 2 divise n^2.
- Si n est impair, il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$.
  Dans cas, $n^2 = (2k+1)^2 = (2k)^2 + 2 \times (2k) \times 1 + 1^2 = 2 \times 2k^2 + 2 \times 2k + 1 = 2 \times (2k^2 + 2k) + 1$.

$\square$

Remarque Notons que nous avons les réciproques de ces deux propositions.
Pour la première, n est pair si, et seulement si, n^2 est pair. En effet, si n^2 est pair alors n ne peut pas être impair sinon p^2 est aussi impair (au lieu d'être pair).

Théorème | $\mathbb{R} \neq \mathbb{Q}$

$\sqrt{2}$ est irrationnel. C'est-à-dire, $\sqrt{2} \notin \mathbb{Q}$.

Démonstration. Supposons, **par l'absurde**, que $\sqrt{2}$ est rationnel. Montrons qu'on arrive à quelque chose d'impossible : une **absurdité**. Ainsi, notre hypothèse sera fausse et on aura montré que $\sqrt{2}$ est irrationnel.
Si $\sqrt{2} \in \mathbb{Q}$, alors il existe $p, q \in \mathbb{Z}^*$ tels que $\sqrt{2} = \dfrac{p}{q}$ et la fraction est irréductible. On peut ainsi calculer le carré de cette quantité, à savoir $(\sqrt{2})^2 = \left(\dfrac{p}{q}\right)^2$ et donc $p^2 = 2q^2$ est pair.
Par la propriété de parité d'un carré, p^2 est pair donc p **est pair**.
On peut écrire $p = 2p'$ où $p' \in \mathbb{Z}$ et donc $2 = \dfrac{4p'^2}{q^2}$, ce qui implique que $q^2 = 2p'^2$. q^2 est pair donc q **est aussi pair**.
Nous venons de montrer que 2 divise p et q donc la fraction $\dfrac{p}{q}$ n'est pas irréductible. C'est impossible puisque nous avons supposé le contraire.
Nous obtenons une **absurdité** et donc l'hypothèse sur $\sqrt{2}$ est fausse. Nous avons démontré **par l'absurde** que $\sqrt{2} \notin \mathbb{Q}$.

$\square$