6

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 $n, k \in \mathbf{Z}$ tel qu'il existe $k' \in \mathbf{Z}$ 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.

Exercice

1. Déterminer tous les multiples positifs de 7 strictement inférieurs à 60.
2. Déterminer les diviseurs de 100 supérieurs ou égaux à 12.

Propriété | Somme, différence et produit

Soient $a, n, m \in \mathbf{Z}$. 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.

Démonstration. Il suffit de décomposer n et m en $n = ka$ et $m = k'a$ puis de considérer $n+m$, $n-m$ et nm. □

Définition | Nombre premier

Un **nombre premier** est un nombre entier naturel différent de 1 dont les seuls diviseurs positifs 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 $15 = 3 \times 5$.

Exercice

Soient a et b deux entiers naturels tel que $a^2 - b^2$ est premier.
Montrer que a et b sont consécutifs.

Théorème | Décomposition en produit de facteurs premiers

Soit $n \in \mathbf{N}^*$ différent de 1.
Il existe une unique décomposition :

$$n = p_1^{i_1} \times p_2^{i_2} \times \cdots \times p_l^{i_l}$$

où $l \in \mathbf{N}^*$, $i_1, i_2, \ldots, i_l \in \mathbf{N}^*$ et $p_1, p_2, \ldots, p_l$ sont des nombres premiers distincts.

Démonstration. Admise. □

Exemples Donnons quelques "décompositions en nombres premiers".

- $12 = 2^2 \times 3^1$
- $17 = 17^1$
- $528 = 2^4 \times 3^1 \times 11^1$
- $1\,070 = 2^1 \times 3^2 \times 5^1 \times 13^1$

Propriétés

Soient n et m deux entiers naturels décomposés en nombres premiers :

$$n = p_1^{i_1} \times p_2^{i_2} \times \cdots \times p_l^{i_l} \qquad \text{et} \qquad m = p_1^{j_1} \times p_2^{j_2} \times \cdots \times p_l^{j_l}$$

où les exposants sont potentiellement nuls.

- $\text{pgcd}(n,m) = p_1^{\min(i_1,j_1)} \times p_2^{\min(i_2,j_2)} \times \cdots \times p_l^{\min(i_l,j_l)}$
- $\text{ppcm}(n,m) = p_1^{\max(i_1,j_1)} \times p_2^{\max(i_2,j_2)} \times \cdots \times p_l^{\max(i_l,j_l)}$

Exemple On a $528 = 2^4 \times 3^1 \times 5^0 \times 11^1 \times 13^0$ et $1\,070 = 2^1 \times 3^2 \times 5^1 \times 11^0 \times 13^1$. Ainsi :

- $\text{pgcd}(528, 1\,070) = 2^1 \times 3^1 \times 5^0 \times 11^0 \times 13^0 = 6$;
- $\text{ppcm}(528, 1\,070) = 2^4 \times 3^2 \times 5^1 \times 11^1 \times 13^1 = 102\,960$.

2 Parité

Définitions

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

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

Démonstration. Immédiat en revenant aux définitions. □

Propriété | Parité d'un carré

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

- 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 $k \in \mathbf{Z}$ 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 $k \in \mathbf{Z}$ tel que $n = 2k+1$.
  Dans cas, $n^2 = (2k+1)^2 = (2k)^2 + 2 \times (2k) \times 1 + 1^2 = 2 \times 2k^2 + 2 \times 2k + 1 = 2 \times (2k^2 + 2k) + 1$. □

Exercice

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

1. On suppose que n^2 est un entier pair.
   a) n peut-il être impair ?
   b) En déduire la parité de n.
2. On suppose que n^2 est impair.
   Déterminer la parité de n.

Exercice

Soit p premier différent de 2.

1. Quelle est la parité de p ?
2. Quelle est la parité de $p+1$? De $p-1$?
3. Démontrer que $p^2 - 1$ est divisible par 4.

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

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

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 $\sqrt{2} \in \mathbf{Q}$, alors il existe $p, q \in \mathbf{Z}^*$ 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 $p' \in \mathbf{Z}$ 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 $\sqrt{2} \notin \mathbf{Q}$.

□