

# Arithmétique

## Table des matières

1	Divisibilité	1
2	Nombres premiers	1
3	Division euclidienne	2
4	Culture	2
5	Liens	2

---

$\mathbb{N}$  désigne l'ensemble des entiers naturels. Les propriétés des opérations usuelles : addition, soustraction, division entière, sont supposées connues.

## 1 Divisibilité

**Définition :** nous dirons que  $b$  *divise*  $a$  s'il existe  $q \in \mathbb{N}^*$  tel que  $a = bq$ .

Il est clair que la relation «divise» est réflexive et transitive ; de plus, si  $a$  divise  $b$  et  $b$  divise  $a$ , alors  $a = b$ . Cette relation est donc un ordre sur  $\mathbb{N}$  ; il n'est que partiel : par exemple, aucun des deux entiers 3 et 5 ne divise l'autre. Toujours pour la relation «divise», le plus petit élément est 1, le plus grand est 0.

## 2 Nombres premiers

**Définition :** un entier  $n$  est *premier* s'il possède exactement deux diviseurs dans  $\mathbb{N}$ , à savoir 1 et  $n$  lui-même.

**Définition :** un entier qui n'est pas premier est dit *composé*. l'ensemble des nombres premiers est infini.

**Remarque :** le plus petit diviseur (autre que 1) d'un entier au moins égal à 2 est un nombre premier.

**Théorème :** l'ensemble des nombres premiers est infini.

**Preuve :** raisonnons par l'absurde, et supposons que l'ensemble des nombres premiers est fini. Notons  $n_1, \dots, n_k$  les nombres premiers. Notons  $N = \prod_{1 \leq j \leq k} n_j$ . De deux choses l'une :

- ou bien  $N + 1$  est premier ; comme il n'est certainement plus grand que tous les  $n_j$ , c'est bien un «nouveau» nombre premier ;
- ou bien  $N + 1$  est composé ; mais alors, avec la remarque faite plus haut,  $d$  est premier ; et il ne peut être diviseur de  $N$  : sinon, il diviserait la différence  $N + 1 - N = 1$ .

Voici une autre preuve : notons  $p$  le plus grand des  $n_j$  et considérons le naturel  $p! + 1$ . Si ce nombre est premier, c'est fini. Sinon, il est composé ; notons  $d$  son plus petit facteur (autre que 1) ; alors  $d$  est premier, et divise  $p! + 1$  ; ce n'est donc pas un diviseur de  $p!$ , ni à plus forte raison de l'un des  $n_j$ . Par suite, c'est un nombre premier autre que ceux de la liste  $(n_j)_{1 \leq j \leq k}$ .

**Théorème :** tout naturel au moins égal à 2 possède une factorisation en produit de nombres premiers ; cette factorisation est unique, à l'ordre d'écriture près.

**Preuve :** soit  $n \geq 2$  ; si  $n$  est premier, c'est fini ; sinon,  $n$  possède au moins deux diviseurs, compris entre 2 et  $n - 1$  inclus. Notons  $d$  le plus petit diviseur : ceci a un sens, car l'ensemble des diviseurs est une partie de l'intervalle discret  $[2, n - 1]$ . Il est clair que  $d$  est premier ; si le quotient  $q = n/d$  est premier, c'est fini ; sinon, on factorise  $q$ , qui est plus petit que  $n$ .

La factorisation de  $n$  peut s'écrire  $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$  où les entiers  $p_1, p_2, \dots, p_k$  sont les facteurs premiers distincts de  $n$  et  $e_1, \dots, e_k$  les exposants de ces facteurs.

**Remarque :** on ne connaît pas actuellement d'algorithme efficace de factorisation d'un entier de grande taille (disons : l'écriture décimale comporte plusieurs centaines de chiffres).

### 3 Division euclidienne

**Théorème :** soient  $a \in \mathbb{N}$  et  $b \in \mathbb{N}^*$ . Il existe un et un seul couple  $(q, r)$  d'entiers vérifiant  $a = bq + r$  et  $0 \leq r < b$ .

Nous dirons que  $q$  est le *quotient* et  $r$  le *reste* dans la division euclidienne de  $a$  par  $b$ . Notez que la définition s'étend aux entiers négatifs. Dans tous les cas, nous aurons  $q = \left\lfloor \frac{a}{b} \right\rfloor$ .

**Preuve :** pour l'unicité, supposons qu'il existe une autre solution  $(q', r')$ . Alors  $bq + r = bq' + r'$ , donc  $b(q - q') = r' - r$ . Mais alors le membre de gauche est multiple de  $b$ , tandis que le membre de droite est dans l'intervalle discret  $\llbracket 1 - b, b - 1 \rrbracket$ . Donc  $r' = r$ , puis  $q' = q$ .

Pour l'existence : c'est l'algorithme de la division, qui, jusqu'à une date récente, était enseigné à l'école élémentaire !

### 4 Culture

Vers 300 avant notre ère, EUCLIDE donne la définition des nombres premiers et la preuve de leur infinité. Il est vraisemblable que ces idées étaient déjà connues.

En 1896, HADAMARD et DE LA VALLÉE POUSSIN en 1896[22] prouvent le *théorème des nombres premiers* : lorsque  $n$  tend vers l'infini, le nombre  $\pi(n)$  de nombre premiers compris entre 1 et  $n$  est équivalent à  $\frac{n}{\ln(n)}$ .

En 1971, MATIJASEVIC montre que l'ensemble des nombres premiers est *diophantien*, c'est-à-dire qu'il existe un polynôme (à plusieurs variables) dont l'ensemble des valeurs positives est l'ensemble des nombres premiers. En 1976, JONES, SATO, WADA et WIENS exhibent un tel polynôme, de degré 25, en 26 variables.

Le premier protocole de cryptographie à clef publique (RSA, de RIVEST, SHAMIR et ADLEMAN) repose sur la difficulté (supposée) de factoriser un «grand» entier (dont l'écriture décimale comptant plusieurs centaines de chiffres).

En 2002, AGRAWAL, SAXENA et KAYAL construisent un test de primalité déterministe, de coût  $\mathcal{O}(|n|^{12})$ , où  $|n|$  est la longueur de l'écriture du naturel  $n$ .

### 5 Liens

Vous trouverez une feuille d'exercices d'arithmétique ici :

<http://bruno.maitresdumonde.com/pcsi2/maths/exos2007/Algebre/Arithmetique.pdf>

FIN