ARITHMÉTIQUE ÉLÉMENTAIRE

Plan

Cadre

- On se place sur l'ensemble $\mathbb{N}$ des entiers naturels, muni de ses lois internes $+$ et $\times$
- $\mathbb{N}$ est aussi naturellement muni d'une relation d'ordre (total), qui en fait un ensemble bien ordonné (*toute partie non vide admet un plus petit élément*)
- Il est vite nécessaire (coefficients de Bézout) de se placer sur l'ensemble $\mathbb{Z}$ des entiers relatifs qui, muni des lois $+$ et $\times$, forme un anneau commutatif
  (lois associatives et commutatives, admettant un élément neutre, existence d'un opposé, distributivité)

Dans la suite, le terme « entier » signifie « élément de $\mathbb{Z}$ ».

Définition

Soit a et b deux entiers. On dit que a divise b, ou que a est un diviseur de b, ou encore que b est un multiple de a, et on écrit $a \mid b$, s'il existe un entier k tel que $b = ka$.

Remarques.

- Zéro n'est diviseur d'aucun entier, et multiple de tous.
- Un entier a est toujours divisible par 1 et par a (ainsi que par -1 et par $-a$).

Plus Grand Commun Diviseur

Soit a et b deux entiers. L'ensemble des diviseurs positifs communs à a et à b n'est pas vide (il contient au moins 1), et fini (tout diviseur de a est inférieur à $|a|$).
Il admet donc un plus grand élément :
le plus grand diviseur commun à a et b, noté $\text{pgcd}(a, b)$.

Plan

Division euclidienne (rappel)

Soit a et b deux entiers **positifs**, avec $b > 0$. Il existe un unique couple d'entiers positifs (q, r) tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Les entier q et r sont appelés respectivement quotient et reste de la division euclidienne de a par b.

Démonstration.

Il suffit de remarquer que $\{a - bx \mid x \in \mathbb{N},\ a - bx \geq 0\}$ est un ensemble non vide (il y a au moins a) qui admet donc un plus petit élément, d'où r, puis q … $\square$

Le calcul de pgcd(a, b) peut-être obtenu par une suite de divisions euclidiennes : c'est l'algorithme d'Euclide.
Comme il est évident que pgcd$(a, 0) = a$, on peut supposer $0 < b \leq a$:

$$\begin{array}{rcl} a & = & bq_1 + r_1 \\ b & = & r_1 q_2 + r_2 \\ r_1 & = & r_2 q_3 + r_3 \\ \dots & \dots & \dots \\ r_{n-2} & = & r_{n-1} q_n + r_n \\ r_{n-1} & = & r_n q_{n+1} + 0 \end{array}$$

1. La suite des restes est strictement décroissante à valeur positive donc finit par prendre la valeur 0 : arrêt de l'algorithme
2. En parcourant les lignes de calcul de haut en bas, on voit que tout diviseur de a et b est diviseur de la suite des restes
3. En les parcourant de bas en haut, on voit que r_n est diviseur commun de a et de b ; on en déduit $r_n = \text{pgcd}(a, b)$

On peut aussi utiliser chacune des divisions euclidiennes de l'algorithme d'Euclide, de haut en bas, pour exprimer le reste r_k comme combinaison linéaire de a et de b, ce qui donne, pour $k = n$:

Identité de Bézout

Pour tous entiers positifs a, b, il existe des entiers (relatifs) u et v (parfois appelés « coefficients de Bézout ») tels que :

$$au + bv = \mathrm{pgcd}(a, b)$$

Deux conséquences de l'identité de Bézout :

Corollaire

1. a et b sont premiers entre eux (i. e. $\mathrm{pgcd}(a, b) = 1$) si et seulement s'il existe des entiers u et v tels que $au + bv = 1$
2. Lemme de Gauß :
   si $a \mid bc$ et $\mathrm{pgcd}(a, b) = 1$, alors $a \mid c$

Plan

1. Divisibilité

2. Algorithme d'Euclide

3. Théorème fondamental de l'arithmétique

Définition

Un entier positif est dit premier s'il possède exactement deux diviseurs positifs.

Les résultats suivants son démontrés dans les *Éléments* d'Euclide, IV^{e} s. AEC :

Proposition

1. Soit a un entier positif :
   - ou bien a est premier,
   - ou bien a admet un diviseur premier inférieur ou égal à $\sqrt{a}$.
2. Il existe une infinité de nombres premiers.

Démonstration.

- En effet, si a n'est pas premier, il admet des diviseurs, et le plus petit d'entre eux sera premier ...
- Par l'absurde, en considérant le produit de tous les premiers augmenté de 1 ... □

Soit $\mathcal{P}$ l'ensemble (infini) des nombres premiers.

Théorème (Th. Fondamental de l'arithmétique)

Tout entier positif admet une décomposition unique, à l'ordre près des facteurs, comme produit de nombres premiers :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)},$$

où les entiers $v_p(n)$ sont nuls sauf pour un nombre fini de premiers p.

Démonstration.
L'existence est une récurrence facile sur les entiers, l'unicité est la partie la plus « forte » de l'énoncé : c'est aussi une récurrence sur les entiers, où le cas de « base » est celui des nombres premiers, et où l'étape de récurrence s'appuie sur le lemme de Gauß. □

Remarque. Il n'y a pas d'algorithme **efficace** connu permettant de générer les nombres premiers, ou de factoriser un entier.