Décomposition en base b

Théorème

Soit $b \geq 2$ un entier. Tout entier $a \geq 0$ s'écrit de façon unique sous la forme

$$a = a_0 + a_1 b + a_2 b^2 + \cdots + a_k b^k$$

où k est un entier, les a_i sont des entiers compris entre 0 et $b-1$ où $a_k \neq 0$. On note parfois :

$$a = (a_k a_{k-1} \cdots a_1 a_0)_b$$

Remarque : Dans le cas où $b = 10$, les a_i correspondent exactement aux chiffres usuels de a.

Preuve : La méthode consiste à effectuer des divisions euclidiennes par b successives.

On commence par écrire $a = bq_0 + a_0$ avec $0 \leq a_0 \leq b-1$

Si $q_0 = 0$ on a fini, sinon on continue en écrivant

$q_0 = bq_1 + a_1$ avec $0 \leq a_1 \leq b-1$. On a alors

$$a = a_0 + a_1 b + q_1 b^2$$

De même, si $q_1 = 0$ on a fini. Sinon on continue, construisant ainsi a_3, q_3 et ainsi de suite. On obtient successivement des égalités du type $a = a_0 + a_1 b + \cdots + a_i b^i + q_i b^{i+1}$

La suite des q_i est une suite d'entiers positifs strictement décroissante. Elle doit donc s'arrêter, ce qui n'est donc réalisé que si $q_i = 0$. À ce moment, on a bien la décomposition souhaitée.

Reste à prouver l'unicité. Supposons que l'on puisse écrire :

$$a_0 + a_1 b + \cdots + a_\ell b^\ell = a'_0 + a'_1 b + \cdots + a'_\ell b^\ell$$

pour des entiers $0 \leq a_i \leq b-1$. Alors $a_0 - a'_0$ est un multiple de b et $|a_0 - a'_0| < b$. D'où $a_0 = a'_0$. On simplifie alors par a_0, puis on divise par b. En appliquant le même argument que précédemment, on obtient $a = a'_1$ et ainsi de suite ∎

PGCD et PPCM

Proposition / Définition :
Soit $a \geq 1$ et $b \geq 1$ deux entiers. Alors il existe un unique entier $m \geq 1$ tel que pour tout entier $c \geq 1$

c est un multiple de a et $b \iff c$ est un multiple de m

m est appelé le plus petit commun multiple de a et de b et est noté $\mathrm{ppcm}(a,b)$ (ou parfois $a \vee b$)

De plus il existe un unique entier $d \geq 1$ tel que pour

tout entier $c \geq 1$,

c divise a et b $\Leftrightarrow$ c divise d

d est appelé le plus grand commun diviseur et est noté $pgcd(a,b)$ (ou parfois $a \wedge b$).

Preuve :

Montrons l'existence de m.

Soit $A \subseteq \mathbb{N}$ l'ensemble des entiers strictement positifs simultanément multiples de a et de b. L'ensemble A n'est pas vide puisqu'il contient l'entier ab. Il admet donc un plus petit élément m.

On vérifie que cet entier m convient :

- Si c est un multiple commun de a et b, montrons que c est un multiple de m. Pour ce faire, effectuons la division euclidienne de c par m, soit $n = mq + r$ avec $0 \leq r < m$.

Comme c et m sont des multiples de a, $r = c - mq$ aussi ; de même avec b. Ainsi r est un multiple commun de a et b. Si r était un entier strictement positif, vu l'inégalité $r < m$, il contredirait la minimalité de m. C'est donc que c est un multiple de m.

- Réciproquement si c est un multiple de m, il est multiple de a et b vu que m est multiple de a et b.

Montrons maintenant l'unicité de m :

Soit m et m' vérifiant les hypothèses du théorème. Comme m est un multiple lui-même, il est multiple de a et b donc un multiple de m'. De même, m' est un multiple de m.

Cela implique que m et m' sont forcément égaux à signe près. Comme ils sont tous les deux strictement positifs, ils sont égaux.

Montrons maintenant l'existence de d :

On pose $d = \frac{ab}{ppcm(a,b)}$. Remarquons que d est bien un entier : en effet, ab étant un multiple commun de a et b c'est un multiple de leur ppcm. Montrons que d vérifie les propriétés demandées :

- Si c est un diviseur commun de a et b alors $a = kc$ et $b = lc$ avec $k, l \in \mathbb{N}$. Alors le nombre klc est un multiple de a et de b donc multiple de $ppcm(a,b)$. donc

$$\frac{ab}{c} = klc = n \cdot ppcm(a,b)$$

soit $d = \frac{ab}{ppcm(a,b)} = c \cdot n$. donc c divise d.

- Réciproquement, puisque $a = d \cdot \frac{ppcm(a,b)}{b}$, où $\frac{ppcm(a,b)}{b}$ est un entier, d divise a, et de même d divise b. Donc si c divise d, alors c divise a et b.

La preuve de l'unicité de d est la même que celle du ppcm.

Notons qu'on peut aussi démontrer la proposition suivante :

Proposition : Soient $a \geq 1$ et $b \geq 1$ deux entiers. Alors :

$$\text{ppcm}(a,b)\,\text{pgcd}(a,b) = ab.$$

Remarque : Si $a = 0$, alors on a

$$\text{ppcm}(a,b) = 0 \quad \text{et} \quad \text{pgcd}(a,b) = b$$

Proposition : On a $\forall\, a, b, k \in \mathbb{N}$,

1) $\text{pgcd}(a,b) = \text{pgcd}(a - kb, b)$

2) $\text{pgcd}(ka, kb) = k\,\text{pgcd}(a,b)$

Définition : Si $\text{pgcd}(a,b) = 1$, on dit que a et b sont premiers entre eux.

L'Algorithme d'Euclide

On suppose $a, b \geq 1$. Nous effectuons des divisions euclidiennes successives :

de a par b : $a = bq_1 + r_1$ $\quad 0 \leq r_1 < b$

de b par r_1 : $b = r_1 q_2 + r_2$ $\quad 0 \leq r_2 < r_1$

de r_1 par r_2 : $r_1 = r_2 q_3 + r_3$ $\quad 0 \leq r_3 < r_2$

$\vdots$

de r_{n-2} par r_{n-1} : $r_{n-2} = r_{n-1} q_n + \boxed{r_n}$ $\quad 0 \leq r_n < r_{n-1}$

de r_{n-1} par r_n : $r_{n-1} = r_n q_{n+1} + 0$ $\quad$ avec $r_{n+1} = 0$

$\boxed{r_n}$: le dernier reste non nul.

Proposition : $\mathrm{pgcd}(a, b)$ est le dernier reste non nul ($= r_n$) dans cette série de divisions euclidiennes.

Preuve : Montrons d'abord qu'il existe un rang n tel que $r_{n+1} = 0$.

Par construction, $\forall\, p \geq 1$, $\quad 0 \leq r_{p+1} < r_p$.

La suite $(r_p)_{p \geq 1}$ est donc positive, et strictement décroissante tant qu'elle n'est pas égale à 0. Il existe donc bien un rang n à partir duquel $\forall\, p > n+1$, $r_p = 0$.

Maintenant, on a que

$$r_{i-2} = r_{i-1} q_i + r_i$$

implique que

$$\begin{aligned} pgcd(r_{i-2}, r_{i-1}) &= pgcd(r_{i-2} - q_i r_{i-1}, r_{i-1}) \\ &= pgcd(r_i, r_{i-1}) \\ &= pgcd(r_{i-1}, r_i) \end{aligned}$$

Donc le pgcd des deux facteurs dans la division euclidienne reste le même à chaque étape, i.e :

$$pgcd(a,b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \cdots = pgcd(r_n, 0) = r_n$$

■

L'algorithme d'Euclide fournit une méthode pour calculer le pgcd de deux entiers naturels.

Exemple : prenons $a = 125$ et $b = 35$. Alors :

$$125 = 35 \cdot 3 + 20$$
$$35 = 20 \cdot 1 + 15$$
$$20 = 15 \cdot 1 + 5$$
$$15 = 5 \cdot 3 + 0$$

donc $pgcd(125, 35) = 0$.

A chaque étape de l'algorithme d'Euclide, on a une égalité de la forme : $r_{i-2} = r_{i-1} q_i + r_i$

où par convention $r_{-2} = a$ et $r_{-1} = b$. A l'avant dernière étape, on a $r_n = \text{pgcd}(a,b)$ et donc une égalité de la forme :

$$r_{n-2} = r_{n-1} q_n + \text{pgcd}(a,b)$$

soit encore :

$$\text{pgcd}(a,b) = r_{n-2} - r_{n-1} q_n$$

A l'étape précédente, on a de même

$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$$

donc en réinjectant, on obtient une expression de d comme une combinaison linéaire de r_{n-3} et r_{n-2}. En continuant à remonter, on trouve finalement une égalité de la forme :

$$d = u r_{-2} + v r_{-1} = au + bv$$

pour des entiers u et v. On en déduit le théorème suivant :

Théorème (identité de Bézout)

Soient $(a,b) \in \mathbb{N}^2 \setminus \{(0,0)\}$ (non simultanément nuls). Alors il existe des entiers $(u,v) \in \mathbb{Z}^2$ tels que

$$\text{pgcd}(a,b) = ua + bv$$

En particulier, a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.