Compléments de CM9

Division euclidienne

Nous avons vu le théorème suivant:

Théorème (Division euclidienne). Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* := \mathbb{Z}\backslash\{0\}$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ vérifiant

$$a = qb + r, \qquad 0 \leqslant r < |b|.$$

□

Cette propriété de $\mathbb{Z}$ est très importante et elle nous permet de montrer pas mal de théorèmes significatifs. Par exemple, les deux théorèmes suivants sont des corollaires du théorème:

Théorème (PPCM) Soient a et b deux entiers non nuls. Alors, un entier m qui est un multiple commun de a et de b et un multiple de $\mathrm{ppcm}(a, b)$. □

Théorème (PGCD) Soient a et b deux entiers non nuls. Alors, un entier d qui est un diviseur commun de a et de b et un diviseur de $\mathrm{pgcd}(a, b)$. □

Ici, montrons le théorème suivant:

Théorème Soient $a, b \in \mathbb{N}^*$. Alors, $a \cdot b = \mathrm{ppcm}(a, b) \cdot \mathrm{pgcd}(a, b)$. □

Preuve Posons $l = \mathrm{ppcm}(a, b)$. Comme l est un multiple de a et de b, il existent $a', b' \in \mathbb{N}^*$ tels que

$$l = ab' = a'b. \tag{1}$$

Comme ab est un multiple commun de a et b, c'est un multiple de l, i.e., il existe $d \in \mathbb{N}^*$ tel que

$$ab = dl. \tag{2}$$

D'après (1), on a $ab = da'b = dab'$, d'où

$$a = da', \qquad b = db'. \tag{3}$$

Posons $m = \mathrm{pgcd}(a, b)$. Comme (3) implique que d est un diviseur commun de a et b, il existe $e \in \mathbb{N}^*$ tel que $m = de$. Comme m est un diviseur de a et b, (3) implique que a', b' sont divisible par e, i.e., il existe $a'', b'' \in \mathbb{N}^*$ tels que $a' = ea'', b' = eb''$. Donc, (1) implique que

$$l = ab''e = ba''e.$$

Si $e > 1$, alors, l/e devient un multiple commun qui est plus petit que l, ce qui est absurde. Donc, on a $e = 1$, i.e., $m = d$, ceci implique (2). □

Étant donné deux entiers $a, b \in \mathbb{N}^*$, le PGCD de a et b est calculable avec l'aide de ce que l'on appelle l'**algorithme d'Euclide**, d'où ce théorème nous permet de calculer le PPCM de a et b.