4.4 Le ppcm, le plus petit multiple commun

4.4.1 Définition

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$
On appelle plus petit multiple commun à a et à b, un entier $m \in \mathbb{Z}$ tel que la proposition suivante soit vraie :

$$(\forall c \in \mathbb{Z})\,(a \mid c \quad b \mid c) \Longrightarrow (m \mid c)$$

On note $m = \operatorname{ppcm}(a, b)$

4.4.2 Théorème

Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{Z}$, nous avons :

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

Où $m = \operatorname{ppcm}(a, b)$

Démonstration

1. Montrons que $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal
   Cette question est un cas particulier d'un énoncé plus général : voir pour cela l'exercice qui suit.
   — Tout d'abord, l'intersection de 2 sous-groupes est un sous-groupe ; donc $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$
   — Soit $\lambda \in \mathbb{Z}$ et $x \in a\mathbb{Z} \cap b\mathbb{Z}$; il faut montrer que $\lambda x \in a\mathbb{Z} \cap b\mathbb{Z}$
   Tout d'abord, $a\mathbb{Z}$ est un idéal et donc, $\lambda x \in a\mathbb{Z}$; de même, $\lambda x \in b\mathbb{Z}$ donc, $\lambda x \in a\mathbb{Z} \cap b\mathbb{Z}$
   Nous en déduisons que $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$
   Dans la mesure où $\mathbb{Z}$ est un anneau principal, cet idéal est engendré par un seul élément, appelé m ; nous avons donc $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$
2. Il faut maintenant montrer que $m = \operatorname{ppcm}(a, b)$.
   Soit $x \in a\mathbb{Z} \cap b\mathbb{Z}$; alors, x est un multiple de a et un multiple de b ; c'est aussi un multiple de m ; donc $m \mid x$, c'est à dire, en utilisant la définition, que $m = \operatorname{ppcm}(a, b)$

Exercice 30 :

Soit $(R, +, \times)$ un anneau, I et J, deux idéaux de R
Montrer que $I \cap J$ est un idéal de R

Exercice corrigé

Montrez que, pour tout $a \in \mathbb{Z}$, tout $b \in \mathbb{Z}$ et tout $k \in \mathbb{Z}$, $\operatorname{ppcm}(ka, kb) = k\operatorname{ppcm}(a, b)$

On appelle $m' = \operatorname{ppcm}(ka, kb)$ et $m = \operatorname{ppcm}(a, b)$; il faut donc montrer que $m' = km$ ou encore que :

$$(ka)\,\mathbb{Z} \cap (kb)\,\mathbb{Z} = (km)\,\mathbb{Z}$$

1. Montrons que $(ka)\,\mathbb{Z} \cap (kb)\,\mathbb{Z} \subset (km)\,\mathbb{Z}$
   Soit $x \in (ka)\,\mathbb{Z} \cap (kb)\,\mathbb{Z}$. Alors :
   — Il existe $\lambda \in \mathbb{Z}$ tel que $x = \lambda\,(ka)$
   — De même, il existe $\lambda_1 \in \mathbb{Z}$ tel que $x = \lambda_1\,(kb)$
   Or, $x = \lambda\,(ka) = \lambda_1\,(kb) \Longleftrightarrow k\,(\lambda a) = k\,(\lambda_1 b) \Longleftrightarrow \lambda a = \lambda_1 b$
   En posant $\mu = \lambda a = \lambda_1 b$, nous montrons que μ est un multiple de a et de b et donc un multiple de $m = \operatorname{ppcm}(a, b)$. On peut donc écrire $\mu = pm$.
   Donc $x = k\,(pm) = (km)\,p$, c'est à dire que $x \in km\mathbb{Z}$.
   Donc, $(ka)\,\mathbb{Z} \cap (kb)\,\mathbb{Z} \subset (km)\,\mathbb{Z}$

2. <u>Montrons que $(km)\mathbb{Z} \subset (ka)\mathbb{Z} \cap (ka)\mathbb{Z}$</u>
   Soit donc $x \in (km)\mathbb{Z}$. Alors, il existe $\lambda \in \mathbb{Z}$ tel que $x = \lambda(km)$. Or, $m = \operatorname{ppcm}(a,b)$ est donc un multiple commun à a et b et donc, il existe α et β tels que $m = \alpha a = \beta b$. Donc $x = \lambda \times k \times \alpha a = \lambda\alpha \times ka$ ce qui montre que $x \in ka\mathbb{Z}$.
   De même, $x = \lambda \times k \times \beta b = \lambda\beta \times kb$ ce qui montre que $x \in kb\mathbb{Z}$
   Donc, $x \in (ka)\mathbb{Z} \cap (ka)\mathbb{Z}$, et donc $(km)\mathbb{Z} \subset (ka)\mathbb{Z} \cap (ka)\mathbb{Z}$

Ainsi, $(ka)\mathbb{Z} \cap (kb)\mathbb{Z} = (km)\mathbb{Z}$, et nous avons $\operatorname{ppcm}(ka,kb) = k\operatorname{ppcm}(a,b)$

Remarque 13 :

En fait, le schéma suivant montre bien les différentes inclusions *(les flèches représentant les inclusions)* :

$$\begin{tikzcd}
 & a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z} & \\
a\mathbb{Z} \arrow[ur] & & b\mathbb{Z} \arrow[ul] \\
 & a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

4.4.3 Proposition

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$; alors, les 2 propositions suivantes sont équivalentes

1. $m = \operatorname{ppcm}(a,b)$ **et** $m = a'a = b'b$
2. $m = a'a = b'b$ **et** $\operatorname{pgcd}(a',b') = 1$

<u>**Démonstration**</u>

1. <u>On suppose $m = \operatorname{ppcm}(a,b)$ et $m = a'a = b'b$</u>
   Il faut donc montrer que $\operatorname{pgcd}(a',b') = 1$
   Soit δ un diviseur commun à a' et à b'
   Alors, $a' = \alpha\delta$ et $b' = \beta\delta$ et donc $m = a\alpha\delta = b\beta\delta$.
   Si $m' = \dfrac{m}{\delta} \Leftrightarrow m'\delta = m$, nous avons $m' = a\alpha = b\beta$, ce qui montre que m' est un multiple commun à a et à b, ce qui est impossible, sauf si $\delta = 1$
   Donc, $\operatorname{pgcd}(a',b') = 1$
2. <u>Réciproquement, soit $m = a'a = b'b$, avec $\operatorname{pgcd}(a',b') = 1$</u>
   Soit $\mu = \operatorname{ppcm}(a,b)$.
   De $m = a'a = b'b$, nous concluons que m est un multiple de a et b et donc du $\operatorname{ppcm}(a,b)$ qui est μ. Donc, $m = k\mu$
   De cette égalité, on tire que $m = k(ax) = k(by)$, c'est à dire, que $k(ax) = a'a \Longleftrightarrow a' = kx$
   De même, $b' = ky$
   Ainsi, k divise donc a' et b' et donc divise $\operatorname{pgcd}(a',b') = 1$, c'est à dire, $k = 1$, et donc,
   $$m = 1 \times \mu = \operatorname{ppcm}(a,b)$$

4.4.4 Théorème

1. **Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{Z}$** $\operatorname{ppcm}(a,b) \times \operatorname{pgcd}(a,b) = ab$
2. **Et, bien entendu, en corollaire, si a et b sont premiers entre eux,** $\operatorname{ppcm}(a,b) = ab$

Démonstration

Soient $d = \text{pgcd}\,(a,b)$, a' et b' deux nombres tels que $a = a'd$ et $b = b'd$, avec $\text{pgcd}\,(a',b') = 1$
On pose $m = \dfrac{ab}{d}$. Nous aimerions montrer que $m = \text{ppcm}\,(a,b)$
Alors, $m = \dfrac{ab}{d} = \dfrac{(a'd)\,(b'd)}{d} = a'b'd$.
De cette écriture, nous déduisons $m = b'a = a'b$, avec $\text{pgcd}\,(a',b') = 1$
D'après la proposition 4.4.3, nous avons $m = \text{ppcm}\,(a,b)$
On conclue donc bien que $md = ab$, ce qui se traduit aussi par : $\text{ppcm}\,(a,b) \times \text{pgcd}\,(a,b) = ab$

Remarque 14 :

L'utilisation de l'algorithme de recherche du pgcd permet de calculer aussi le ppcm

4.4.5 Lemme chinois

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $a \wedge b = 1$. Alors, l'équation :

$$\begin{cases} x \equiv c & [a] \\ x \equiv d & [b] \end{cases}$$

n'a qu'une seule solution modulo ab

Démonstration

— Comme a et b sont premiers, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + bv = 1$ et nous pouvons donc conclure que :

$$\begin{cases} au \equiv 1 & [b] \\ bv \equiv 1 & [a] \end{cases}$$

— Donc $x_0 = dau + cbv$ est une solution particulière de l'équation.
— Soit x une autre solution de cette équation. Alors :

$$\begin{cases} x - x_0 \equiv 0 & [a] \\ x - x_0 \equiv 0 & [b] \end{cases}$$

Ce qui traduit que $x - x_0$ est à la fois multiple de a et multiple de b, et donc multiple du ppcm de a et b. Comme a et b sont premiers entre eux, $\text{ppcm}\,(a,b) = ab$.
Donc $x - x_0 \equiv 0\,[ab]$, c'est à dire $x \equiv x_0\,[ab]$

4.4.6 Quelques exercices

Exercice 31 :

Résoudre, dans $\mathbb{Z}$ les équations :

$$\begin{cases} x \equiv 3\,[11] \\ x \equiv 7\,[15] \end{cases} \qquad \begin{cases} x \equiv 4\,[10] \\ x \equiv 8\,[14] \end{cases}$$

Exercice 32 :

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Donner $\text{pgcd}\,(a+b, \text{ppcm}\,(a,b))$

Exercice 33 :

Déterminer l'ensemble des couples (x,y) d'entiers naturels tels que :

$$\begin{cases} \delta = 60 \\ \mu = 3600 \end{cases}$$

Où $\delta = \text{pgcd}\,(x,y)$ et $\mu = \text{pppcm}\,(x,y)$