PGCD et PPCM

Notation : $Div(a)$ est l'ensemble des diviseurs du nombre a ; $a\mathbb{Z}$ est l'ensemble des multiples du nombre a ; $a\mathbb{Z} + b\mathbb{Z}$ est l'ensemble des nombres de la forme $az + bz'$ avec $z, z' \in \mathbb{Z}$ (ici on appele ces nombres 'combinaisons').

1 Le plus grand commun diviseur

Le PGCD de deux entiers relatifs est le plus grand entier qui les divise simultanément (si les deux nombres sont zéro, on définit le PGCD comme zéro).

Soient $a, b \in \mathbb{Z}$ tels que a ou b soit non-nul. Plusieurs définitions pour le $\mathrm{PGCD}(a, b)$ sont possibles (le PGCD satisfait toutes les propriétés de ces définitions et si un nombre satisfait l'une de ces définitions, il est forcément le PGCD) :

• Le plus grand élément de l'ensemble des diviseurs communs à a et b, c.à.d.

$$\max\Big(Div(a) \cap Div(b)\Big)\,.$$

• Le diviseur commun à a et b qui est multiple de chaque diviseur commun à a et b et qui est positif.
• La plus petite combinaison des nombres a et b qui est strictement positive, c.à.d.

$$\min\Big((a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{Z}_{>0}\Big)\,.$$

Algorithme d'Euclide pour le PGCD : Pour calculer le PGCD on peut utiliser la division euclidienne et remarquer que

$$\mathrm{PGCD}(Dividende, Diviseur) = \mathrm{PGCD}(Diviseur, Reste)\,.$$

[Preuve : On peut montrer facilement que les deux couples de nombres ont les mêmes diviseurs communs.] L'avantage est que les deux nombres deviennent de plus en plus petit : à la fin on va forcément trouver quelque chose de la forme $\mathrm{PGCD}(n, 0)$ pour un entier naturel n, et le PGCD cherché sera donc n.

Propriétés du PGCD de deux nombres : Soient $a, b \in \mathbb{Z}$ tels que a ou b soit non-nul.
• L'ordre des deux nombres, ou leur signe, n'a aucun effet sur le PGCD.
• Les diviseurs du PGCD sont les diviseurs communs aux deux nombres.
• La valeur $\mathrm{PGCD}(a, b)$ peut aller de 1 au $\min\{|a|, |b|\}$ (on est dans le dernier cas si et seulement si on a une divisibilité entre les nombres).
• Si $c \in \mathbb{Z} \setminus \{0\}$ on a

$$\mathrm{PGCD}(ac, bc) = |c| \cdot \mathrm{PGCD}(a, b)$$

• **Combinaisons :** Les combinaisons $a\mathbb{Z} + b\mathbb{Z}$ sont exactement les multiples du PGCD.

2 Nombres premiers entre eux

Deux nombres sont **premiers entre eux** si leur PGCD est 1. De manière équivalente, 1 est une combinaison de ces deux nombres, et donc que chaque entier est une combinaison de ces deux nombres.
Plusieurs nombres sont **premiers entre eux deux à deux** si le PGCD de chaque paire de nombres est 1 (en particulier, ces nombres n'ont pas de facteurs communs). Attention : $6, 10, 15$ n'ont pas de facteurs communs, mais ils ne sont pas premiers entre eux deux à deux.

Si on divise deux nombres par leur PGCD, les quotients obtenus sont premiers entre eux (car on a enlevé tous les facteurs communs).

• Pour tout $a, b, c \in \mathbb{Z}$ on a : "si un nombre divise un produit de deux facteurs, et est premier avec l'un des facteurs, alors il divise le deuxième facteur"

$$a \mid bc \text{ et } \mathrm{PGCD}(a, b) = 1 \Longrightarrow a|c\,.$$

• Pour tout $a, b, c \in \mathbb{Z}$ on a : "si deux diviseurs d'un nombre sont premiers entre eux, leur produit est encore un diviseur de ce nombre"

$$a \mid c \text{ et } b \mid c \text{ et } \mathrm{PGCD}(a, b) = 1 \implies ab \mid c.$$

[Ces propriétés sont fausses sans l'hypothèse des nombres premiers entre eux.]

Remarque générale : Une propriété arithmétique pour deux nombres premiers entre eux se généralise souvent à plusieurs nombres qui sont premiers entre eux deux à deux (par contre, la condition de ne pas avoir de facteur commun est trop faible).

3 PGCD de plusieurs nombres

Définir le $\mathrm{PGCD}(a_1, \ldots, a_n)$ de plusieurs nombres entiers et en écrire les propriétés est un exercice utile de généralisation.

Une nouvelle propriété : Si $N \geq n \geq 2$, et $a_1, \ldots, a_N \in \mathbb{Z}$, on a

$$\mathrm{PGCD}(a_1, \ldots, a_N) \mid \mathrm{PGCD}(a_1, \ldots, a_n)\,.$$

Un point de vue utile : on peut considérer le PGCD de deux nombres comme une opération. On peux vérifier facilement que cette opération est commutative et associative. Le PGCD de plusieurs nombres s'obtient en faisant plusieurs PGCD de deux nombres (dans la même façon qu'une somme de plusieurs nombres). En utilisant l'associativité on peut montrer par exemple :

$$\mathrm{PGCD}(a, b, c, d, e) = \mathrm{PGCD}(\mathrm{PGCD}(a, b), \mathrm{PGCD}(c, d), e)\,.$$

4 Le plus petit commun multiple

Le PPCM de deux entiers relatifs est le plus petit entier qui est strictement positif et est un multiple de deux nombres (si au moins un des deux nombres est zéro, on définit le PPCM comme zéro).

Soient $a, b \in \mathbb{Z}$, tels que a ou b soient non-nuls. Plusieurs définitions pour le $\mathrm{PPCM}(a, b)$ sont possibles, par exemple :
• Le plus petit élément strictement positif des ensemble des multiples communs à a et b, c.à.d.

$$\min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{Z}_{>0}\right).$$

• Le multiple commun à a et b que divise chaque multiple commun à a et b et qui est strictement positif.

Propriétés du PPCM de deux nombres : Soient $a, b \in \mathbb{Z}$, tels que a ou b soit non-nul.
• L'ordre des deux nombres, ou leur signe, n'as aucun effet sur le PPCM.
• Les multiples du PPCM sont les multiples communs des deux nombres.
• La valeur $\mathrm{PPCM}(a, b)$ peut aller de $\max\{|a|, |b|\}$ à $|ab|$ (on est dans le premier cas si et seulement si l'on a une divisibilité entre les nombres). Puisque ab est un multiple commun à a et b, le PPCM le divise.
• Si $c \in \mathbb{Z} \setminus \{0\}$, on a

$$\mathrm{PPCM}(ac, bc) = |c| \cdot \mathrm{PPCM}(a, b).$$

Attention ! Contrairement au PGCD, il n'ya pas un lien direct entre le PPCM et les combinaisons des nombres. Bien que $\mathrm{PGCD}(a + bz, b) = \mathrm{PGCD}(a, b)$ pour tout $z \in \mathbb{Z}$, on a $\mathrm{PPCM}(a + bz, b) \neq \mathrm{PPCM}(a, b)$ en général (les deux couples ont les mêmes diviseurs communs, mais pas les même multiples : comparer par exemple $(2, 3)$ avec $(2 + 3, 3)$).

On calcule le PPCM avec le PGCD, grâce à la formule suivante :

$$\mathrm{PGCD}(a, b) \cdot \mathrm{PPCM}(a, b) = |a \cdot b|.$$

Attention ! Cette formule est fausse pour plusieurs nombres (essayer des exemples).

Définir le $\mathrm{PPCM}(a_1, \ldots, a_n)$ de plusieurs nombres entiers et en écrire les propriétés est un exercice utile de généralisation. Comme le PGCD, le PPCM est aussi une opération associative et commutative, et on peut calculer le PPCM de plusieurs nombres en faisant plusieurs PPCM de deux nombres. De façon analogue, si $N \geq n \geq 2$, et $a_1, \ldots, a_N \in \mathbb{Z}$, on a

$$\mathrm{PPCM}(a_1, \ldots, a_n) \mid \mathrm{PPCM}(a_1, \ldots, a_N).$$