Ch. 1 - Arithmétique entière
PGCD - PPCM

R. Absil (abs)

3 octobre 2017

Les fonctions de PGCM et de PPCM sont très utilisées pour le calcul de multiples et de diviseurs communs en informatique, notamment en cryptographie. Elles ont par ailleurs de nombreuses applications en logistique, dans la composition de configurations d'objets de taille uniforme, etc.

Plus formellement, on définit le PGCD et le PPCM de la manière suivante.

Définition 1

Soient a et b deux naturels, on définit

- *le* plus grand commun diviseur *de a et de b, noté $PGCD\,(a,b)$, comme le plus grand naturel qui divise à la fois a et b ;*
- *le* plus petit commun multiple *de a et de b, noté $PPCM\,(()\,a,b)$, comme le plus petit naturel qui est multiple à la fois de a et de b.*

Exemple 1. Soient $a = 48$ et $b = 42$, on peut calculer $PGCD\,(48,42)$ de la façon suivante, par énumération des diviseurs de 48 et de 42.

- Diviseurs de 48 : $1, 2, 3, 4, \boxed{6}, 8, 12, 16, 24, 48$.
- Diviseurs de 42 : $1, 2, 3, \boxed{6}, 7, 14, 21, 42$.

On remarque le plus grand nombre qui divise à la fois 48 et 42 est 6. On a donc $PGCD\,(48,42) \;=\; 6$.

Exemple 2. Soient $a = 6$ et $b = 8$, on peut calculer $PPCM(6,8)$ de la façon suivante, par énumération des premiers multiples de 6 et 8.

- Multiples de 6 : $6, 12, 18, \boxed{24}, 30, 36, 42, 48, \ldots$
- Multiples de 8 : $8, 16, \boxed{24}, 32, 40, 48, \ldots$

On remarque que le plus petit nombre qui est multiple à la fois de 6 et de 8 est 24. On a donc $PPCM(6,8) \;=\; 24$.

Notons que cette manière de calculer le PGCD et le PPCM est assez fastidieuse, et rébarbative, surtout si les nombres sur lesquels ont calcule le PGCD et le PPCM sont « grands ». Néanmoins, en dépit des applications modernes de ces fonctions, des techniques efficaces de leur calcul sont connues depuis l'antiquité grecque.

À ce titre, on présente ici *l'algorithme d'Euclide*, permettant de très rapidement de calculer le PGCD de deux naturels.

Algorithme 1 Algorithme du P.G.C.D. d'Euclide

Entrée(s) : Deux naturels a et b.
Sortie(s) : Le P.G.C.D. de a et b.

```
1: Si b = 0 alors
2:     retourner a
3: Sinon
4:     retourner PGCD(b, a mod b)
```

Exemple 3. Soient $a = 48$ et $b = 68$, avec l'algorithme d'Euclide, on a

$$\begin{aligned} PGCD\,(48, 68) &= PGCD\,(68, 48) && \text{car } 48 \bmod 68 = 48 \\ &= PGCD\,(48, 20) && \text{car } 68 \bmod 48 = 20 \\ &= PGCD\,(20, 8) && \text{car } 48 \bmod 20 = 8 \\ &= PGCD\,(8, 4) && \text{car } 20 \bmod 8 = 4 \\ &= PGCD\,(4, 0) && \text{car } 8 \bmod 4 = 0 \\ &= 4 && \text{car } b = 0 \end{aligned}$$

Exemple 4. Soient $a = 56$ et $b = 72$, on a

$$\begin{aligned} PGCD\,(56, 72) &= PGCD\,(72, 56) && \text{car } 56 \bmod 72 = 56 \\ &= PGCD\,(56, 16) && \text{car } 72 \bmod 56 = 16 \\ &= PGCD\,(16, 8) && \text{car } 56 \bmod 16 = 8 \\ &= PGCD\,(8, 0) && \text{car } 16 \bmod 8 = 0 \\ &= 8 && \text{car } b = 0 \end{aligned}$$

Pour calculer le PPCM de deux naturels a et b, on remarque que ab est un multiple à la fois de a et b. Ce n'est néanmoins pas le plus petit. On peut en effet diviser ab par les diviseurs en commun de a et b. Si l'on divise par le plus grand de ces diviseurs (le P.G.C.D.), on obtient donc le plus petit des multiples communs à a et b.

On a donc la propriété suivante de calcul du PPCM.

Propriété 2

Soient a et b deux naturels, avec $b \neq 0$, on a

$$PPCM(a, b) = \frac{ab}{PGCD(a, b)}.$$

Notons que comme on possède un algorithme rapide pour calculer la PGCD, à l'aide de cette propriété, on possède également un algorithme rapide pour calculer le PPCM.

Exemple 5. Soient $a = 6$ et $b = 8$, on peut calculer $PPCM(6, 8)$ de la façon suivante, à l'aide de la propriété ci-dessus.

$$\begin{aligned} PPCM(6,8) &= \frac{6 \cdot 8}{PGCD(6,8)} \\ &= \frac{48}{2} \\ &= 24 \end{aligned}$$