Arithmétique – Partie 1 : pgcd

Savoir.

- ☐ Connaître les conditions qui définissent la division euclidienne.
- ☐ Connaître le lien entre pgcd et ppcm.

Savoir-faire.

- ☐ Savoir poser une division d'entiers afin de calculer le quotient et le reste.
- ☐ Savoir calculer un pgcd à l'aide de l'algorithme d'Euclide.

Division euclidienne

Dans tout ce chapitre, les lettres utilisées désigneront par défaut des nombres entiers. Des spécifications seront apportées dans les énoncés si besoin.

— **Définition de la division euclidienne.** Soit a un entier positif et b un entier strictement positif. Alors il existe des entiers q et r uniques tels que :

$$\boxed{a = bq + r \qquad \text{avec } 0 \leqslant r \leqslant b - 1.}$$

— *Exemple.* $45 = 7 \times 6 + 3$ ou encore $117 = 13 \times 9 + 0$.

— On dit que b **divise** a s'il existe un entier k tel que $a = kb$. On note alors $b|a$. Cela revient à dire que le reste dans la division euclidienne de a par b est nul.

Il revient au même de dire que b *divise* a et que a *est un multiple de* b.

— Sur les exemples précédents $13 \mid 117$, mais 7 ne divise pas 45.

— **Proposition.** Si $a|b$ et $a|c$, alors pour tous les entiers m et n, $a|mb + nc$. En particulier a divise $b + c$ et $b - c$.

Preuve. Il s'agit d'une simple factorisation. On écrit $b = ka$ et $c = la$. Alors $mb + nc = mka + nla = (mk + nl)a$ qui est bien un multiple de a.

Critères de divisibilité

— Un entier est divisible par 2 (autrement dit c'est un entier pair) si et seulement si son chiffre des unités est 0, 2, 4, 6 ou 8.

— Un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

— Un entier est divisible par 5 si et seulement si son chiffre des unités est 0 ou 5.

— Un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Exemple. $n = 35\,418$. Le chiffre des unités est 8 donc n est divisible par 2 mais pas par 5. La somme des chiffres est $3 + 5 + 4 + 1 + 8 = 21$. Comme 21 est divisible par 3 alors n est divisible par 3. En plus, comme 21 n'est divisible par 9 alors n n'est pas divisible par 9.

pgcd

- **Définition du pgcd.** Soient a et b deux entiers positifs. Le plus grand nombre entier qui divise à la fois a et b est appelé le **plus grand diviseur commun** de a et b. On le note $\mathrm{pgcd}(a,b)$.
- *Exemple.* Les diviseurs communs de 24 et 36 sont les entiers : $1,2,3,4,6,8,12$. Ainsi le pgcd de 24 et 36 est 12.
- Le pgcd possède les propriétés suivantes :

$$\mathrm{pgcd}(na,nb) = n\,\mathrm{pgcd}(a,b) \qquad \mathrm{pgcd}(a,0) = a \qquad \mathrm{pgcd}(a,1) = 1$$

Algorithme d'Euclide

Une méthode pour calculer un pgcd est l'algorithme d'Euclide. Cette méthode est basée sur le résultat suivant :
Proposition. Soient deux entiers $a \geqslant 0$ et $b > 0$, et $a = bq + r$ le résultat de la division euclidienne de a par b. Alors $\boxed{\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)}$.
Preuve. Soit d un diviseur de a et de b. Alors d divise $a - bq$ donc d divise r. Réciproquement, si d divise b et r, il divise $bq + r$ donc il divise a. Ainsi les diviseurs communs de a et de b sont les mêmes que ceux de b et de r, donc en particulier le plus grand (le pgcd) est identique.

L'algorithme d'Euclide repose sur la proposition précédente : pour trouver le pgcd de deux entiers positifs a et b, on effectue la division euclidienne de a par b (ou le contraire si $b > a$) : $a = bq_0 + r_0$. Si le reste r_0 est nul, b est un diviseur de a, et par conséquent $\mathrm{pgcd}(a,b) = b$. Sinon, on recommence en effectuant la division euclidienne de b par r_0 : $b = q_1 r_0 + r_1$. Si r_1 est nul, $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r_0) = r_0$. Sinon, on poursuit avec la division euclidienne de r_0 par r_1, et ainsi de suite.
Le processus se termine, car les restes forme une suite d'entiers positifs strictement décroissants. Enfin :

$$\boxed{\text{Le pgcd de } a \text{ et } b \text{ sera le dernier reste non nul.}}$$

Exemple. Recherchons $\mathrm{pgcd}(1\,188, 120)$:

$$\begin{aligned} 1\,188 &= 120 \times 9 + 108 && \rightarrow && \mathrm{pgcd}(1\,188,120) = \mathrm{pgcd}(120,108) \\ 120 &= 108 \times 1 + \boxed{12} && \rightarrow && \mathrm{pgcd}(120,108) = \mathrm{pgcd}(108,12) \\ 108 &= 12 \times 9 + 0 && \rightarrow && \mathrm{pgcd}(108,12) = \mathrm{pgcd}(12,0) = 12 \end{aligned}$$

Ainsi on a $\mathrm{pgcd}(1\,188,120) = 12$.

Exemple. Cherchons maintenant à déterminer $\mathrm{pgcd}(144,48)$:

$$144 = 48 \times 3 + 0 \quad \rightarrow \quad \mathrm{pgcd}(144,48) = 48$$

48 est un diviseur de 144, donc $\mathrm{pgcd}(144,48) = 48$.

Exercice. Déterminer $\mathrm{pgcd}(585,247)$ et $\mathrm{pgcd}(121,73)$.

ppcm

- **Définition du ppcm.** Soient deux entiers positifs a et b, le **plus petit multiple commun** de a et b, noté $\mathrm{ppcm}(a,b)$, est le plus petit entier positif qui est à la fois un multiple de a et un multiple de b.
- *Exemple.* Les multiples (positifs) commun à 9 et 12 sont 36, 72, 108,... Le ppcm de 9 et 12 est donc 36.
- *Lien entre le pgcd et le ppcm.* Le pgcd et le ppcm sont liés par la formule

$$\boxed{ab = \mathrm{pgcd}(a,b) \times \mathrm{ppcm}(a,b)}$$

Ceci permet d'obtenir le ppcm une fois qu'on a calculé le pgcd : $\text{ppcm}(a, b) = \frac{ab}{\text{pgcd}(a,b)}$

— *Exemple.* Puisque $\text{pgcd}(1\,188, 120) = 12$, on a : $\text{ppcm}(1\,188, 120) = \frac{1\,188\times120}{12} = 11\,880$.

— *Autre exemple.* $\text{pgcd}(144, 48) = 48 \implies \text{ppcm}(144, 48) = \frac{144\times48}{48} = 144$, ce qui est normal puisque 144 est lui-même un multiple de 48.

— *Facultatif.* Voici des explications concernant la relation pgcd/ppcm : $d|a$ donc $a = kd$, et $d|b$ donc $b = ld$. Ainsi $\frac{ab}{d} = kb = la$ est bien un multiple de a et de b. Pour montrer que $\frac{ab}{\text{pgcd}(a,b)}$ est bien le plus petit des multiples communs à a et b, nous aurons besoin soit du *lemme de Gauss*, soit de la *décomposition en facteurs premiers*, ce que nous verrons dans la suite.