

PGCD

Remarque : lorsqu'on parlera de *diviseurs*, il sera sous-entendu qu'il s'agit de diviseurs *positifs*

I Définition et propriétés

Soient a et b deux entiers naturels non nuls.

Le plus grand diviseurs commun à a et b est noté $\text{PGCD}(a ; b)$

Remarque : si l'on note $\mathcal{D}(a ; b)$ l'ensemble des diviseurs communs à a et b (non nuls) alors :

- $\mathcal{D}(a ; b) \neq \emptyset$ car $1 \in \mathcal{D}(a ; b)$
- $\mathcal{D}(a ; b)$ contient un nombre fini d'éléments car si $k \in \mathcal{D}(a ; b)$ alors $k \leq a$ par exemple

$\Rightarrow$ Ces deux constats permettent de justifier que le PGCD existe bien.

Ex : Déterminer le PGCD de 30 et 42.

Les diviseurs de 30 sont 1, 30, 2, 15, 3, 10, 5 et 6.

Les diviseurs de 42 sont 1, 42, 2, 21, 3, 14, 6 et 7.

Les diviseurs communs de 30 et 42 sont donc 1, 2, 3 et 6 et donc $\text{PGCD}(30 ; 42) = 6$

Propriétés : 1. $\text{PGCD}(a ; 0) = a$

2. $\text{PGCD}(a ; 1) = 1$

3. Si b divise a alors $\text{PGCD}(a ; b) = b$

Preuves : 1. $a|a$ et $a|0$ donc a est un diviseur commun de a et 0.

Par ailleurs, si d est un diviseur commun de a et 0 alors $d|a$ et donc $d \leq a$.

Donc a est bien le PGCD de a et 0.

2. Le seul diviseur de 1 est 1 ; et 1 divise a donc c'est le PGCD de a et 1.

3. $b|b$ et $b|a$ donc b est un diviseur commun de a et b .

Par ailleurs, si d est un diviseur commun de a et b alors $d|b$ et donc $d \leq b$.

Donc b est bien le PGCD de a et b .

II Algorithme d'Euclide

Propriété : Soient a et b deux entiers naturels non nuls, avec $a > b$ et tels que b ne divise pas a .

On peut écrire $a = bq + r$ avec $0 < r < b$ (b ne divise pas a donc $r \neq 0$)

Et on a alors $\text{PGCD}(a ; b) = \text{PGCD}(b ; r)$

Preuve : si $d|a$ et $d|b$ alors $d|(a - bq)$ c'est-à-dire $d|r$

Ainsi, tout diviseur commun de a et b est aussi un diviseur commun de b et r .

Et réciproquement, si $d|b$ et $d|r$ alors $d|(bq + r)$ c'est-à-dire $d|a$.

Ainsi, tout diviseur commun de b et r est aussi un diviseur commun de a et b .

Donc $(a ; b)$ et $(b ; r)$ ont exactement les mêmes diviseurs, et donc le même PGCD.

Remarque : plus généralement, si $a = bq + r$ sans que r soit nécessairement le reste de la division euclidienne de a par b , alors $\text{PGCD}(a ; b) = \text{PGCD}(b ; r)$. (algorithme de la différence)



L'algorithme d'Euclide permet de déterminer le PGCD de deux nombres en utilisant plusieurs fois à la suite la propriété précédente.

Propriété : le PGCD de a et b est le dernier reste non nul dans l'algorithme d'Euclide.

Preuve : Effectuons la division euclidienne de a par b : $a = bq_0 + r_0$ avec $0 \leq r_0 < b$

↪ Si $r_0 = 0$ alors $b|a$ et donc $\text{PGCD}(a ; b) = b$.

↪ Si $r_0 \neq 0$, alors $\text{PGCD}(a ; b) = \text{PGCD}(b ; r_0)$

On effectue alors la division euclidienne de b par r_0 : $b = r_0q_1 + r_1$ avec $0 \leq r_1 < r_0$

↪ Si $r_1 = 0$ alors $r_0|b$.

Donc $\text{PGCD}(b ; r_0) = r_0$ c'est-à-dire $\text{PGCD}(a ; b) = r_0$ (dernier reste non nul)

↪ Si $r_1 \neq 0$, alors $\text{PGCD}(b ; r_0) = \text{PGCD}(r_0 ; r_1) = \text{PGCD}(a ; b)$

On effectue alors la division euclidienne de r_0 par r_1 : $r_0 = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$

↪ Si $r_2 = 0$ alors $r_1|r_0$

Donc $\text{PGCD}(r_0 ; r_1) = r_1$ c'est-à-dire $\text{PGCD}(a ; b) = r_1$ (dernier reste non nul)

↪ Si $r_2 \neq 0$, alors $\text{PGCD}(r_0 ; r_1) = \text{PGCD}(r_1 ; r_2) = \text{PGCD}(a ; b)$

Et ainsi de suite : $r_1 = r_2q_3 + r_3$ avec $0 \leq r_3 < r_2$

$$r_2 = r_3q_4 + r_4 \text{ avec } 0 \leq r_4 < r_3$$

La suite d'entiers naturels (r_n) ainsi définie est donc strictement décroissante.

Il existe alors nécessairement un entier n_0 tel que $r_{n_0} \neq 0$ et $r_{n_0+1} = 0$.

Or, $r_{n_0-1} = r_{n_0}q_{n_0+1} + r_{n_0+1} = r_{n_0}q_{n_0+1}$ donc $r_{n_0}|r_{n_0-1}$.

Donc $\text{PGCD}(r_{n_0-1} ; r_{n_0}) = r_{n_0}$ c'est-à-dire $\text{PGCD}(a ; b) = r_{n_0}$ (dernier reste non nul)

Remarques : 1. L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur PGCD.

2. Quel que soit l'entier $c > 0$, $\text{PGCD}(ac ; bc) = c \times \text{PGCD}(a ; b)$

Ex : Déterminer $\text{PGCD}(1\,820 ; 5\,733)$

$$5\,733 = 1\,820 \times 3 + 273$$

$$1\,820 = 273 \times 6 + 182$$

$$273 = 182 \times 1 + 91$$

$$182 = 91 \times 2 + 0$$

Donc $\text{PGCD}(1\,820 ; 5\,733) = 91$

Remarque : les diviseurs communs de 1 820 et 5 733 sont donc les diviseurs de 91, c'est-à-dire 1, 7, 13 et 91

Propriété : Soient a et b deux entiers naturels non nuls.

$\Delta = \text{PGCD}(a ; b) \Leftrightarrow$ Il existe deux entiers naturels a' et b' tels que
$$\begin{cases} a = \Delta a' \\ b = \Delta b' \\ \text{PGCD}(a' ; b') = 1 \end{cases}$$

Preuve : On procède par double implication.

($\Rightarrow$) Notons Δ le PGCD de a et b .

Δ est un diviseur commun à a et b donc il existe deux entiers naturels a' et b' tels que $a = \Delta a'$ et $b = \Delta b'$.

Soit d un diviseur commun à a' et b' . On a donc $a' = da_1$ et $b' = db_1$.

D'où $a = \Delta da_1$ et $b = \Delta db_1$.

Ainsi, Δd est un diviseur commun à a et b .

Par conséquent, $\Delta d \leq \Delta$ car Δ est le *plus grand* diviseur commun à a et b .

Donc $d \leq 1$ ce qui fait que $d = 1$.

Ainsi, le seul diviseur commun à a' et b' est 1, donc $\text{PGCD}(a' ; b') = 1$

($\Leftarrow$) Réciproquement, supposons que $a = \Delta a'$, $b = \Delta b'$ et $\text{PGCD}(a' ; b') = 1$.

$$\begin{aligned} \text{PGCD}(a ; b) &= \text{PGCD}(\Delta a' ; \Delta b') \\ &= \Delta \times \text{PGCD}(a' ; b') \\ &= \Delta \times 1 = \Delta \end{aligned}$$

Ex 1 : Déterminer les couples d'entiers naturels a et b vérifiant $a + b = 112$ et $\text{PGCD}(a ; b) = 14$.

$\text{PGCD}(a ; b) = 14$ donc $a = 14x$ et $b = 14y$ avec $\text{PGCD}(x ; y) = 1$

Or, $a + b = 112$ donc $14x + 14y = 112$

$$14(x + y) = 112$$

$$x + y = 112 : 14 = 8$$

$$x + y = 8$$

Les couples possibles pour x et y sont $(1 ; 7)$, $(2 ; 6)$, $(3 ; 5)$ et $(4 ; 4)$

Or, $\text{PGCD}(x ; y) = 1$ donc les seuls couples acceptables sont $(1 ; 7)$ et $(3 ; 5)$.

D'où $a = 14$ et $b = 108$ ou $a = 42$ et $b = 70$.

Ex 2 : Soit n un entier naturel. On pose $a = n + 3$ et $b = 2n + 1$.

Quelles sont les valeurs possibles du PGCD de a et b ?

Discuter selon les valeurs de n .

Soit d un diviseur commun de a et b .

$d|a$ et $d|b$ donc $d|2a - b$

Autrement dit, $d|2(n + 3) - (2n + 1)$

$$d|2n + 6 - 2n - 1$$

$$d|5$$

Donc $d = 1$ ou $d = 5$.

Les seules valeurs possibles pour le PGCD de a et b sont donc 1 et 5.

On observe alors les congruences modulo 5 :

n	0	1	2	3	4
$a = n + 3$	3	4	0	1	2
$b = 2n + 1$	1	3	0	2	4

Le seul cas où a et b sont congrus à 0 modulo 5 est $n \equiv 2 \pmod{5}$.

Autrement dit, $\text{PGCD}(a ; b) = 5$ si et seulement si $n \equiv 2 \pmod{5}$

Donc si $n = 5k + 2$ avec $k \in \mathbb{N}$ alors $\text{PGCD}(a ; b) = 5$.

Et sinon, $\text{PGCD}(a ; b) = 1$.

III Applications concrètes

⇒ Composition de groupes

Ex : Un chef d'orchestre doit faire répéter 1 058 choristes : 322 hommes et 736 femmes. Il veut faire des groupes de répétitions de sorte que tous les choristes soient dans un groupe et que tous les groupes aient la même composition homme/femme.

Quel est le nombre maximal de groupes qu'il pourra faire ?

Et quelle sera alors la composition de chacun de ces groupes ?

⇒ *Il pourrait faire un groupe avec tout le monde, ou deux groupes avec 115 hommes et 253 femmes, etc...*

Le nombre de groupes est nécessairement un **diviseur commun** à 322 et 736 pour que tous les choristes soient dans un groupe, et **c'est le PGCD** puisqu'on veut le **plus grand nombre de groupes**.

$$736 = 322 \times 2 + 92$$

$$322 = 92 \times 3 + 46$$

$$92 = 46 \times 2 + 0$$

$$\text{PGCD}(322 ; 736) = 46$$

On pourra donc faire 46 groupes.

$$322 : 46 = 7 \text{ et } 736 : 46 = 16$$

Chaque groupe comprendra 16 femmes et 7 hommes.

⇒ Fractions irréductibles

Une fraction simplifiée par le PGCD de son numérateur et de son dénominateur devient irréductible.

Ex : Rendre la fraction $\frac{60\,775}{114\,400}$ irréductible.

$$114\,400 = 60\,775 \times 1 + 53\,625$$

$$60\,775 = 53\,625 \times 1 + 7\,150$$

$$53\,625 = 7\,150 \times 7 + 3\,575$$

$$7\,150 = 3\,575 \times 2 + 0$$

$$\text{PGCD}(60\,775 ; 114\,400) = 3\,575$$

$$\text{Donc } \frac{60\,775}{114\,400} = \frac{3\,575 \times 17}{3\,575 \times 32} = \frac{17}{32}$$