PGCD de deux entiers – Algorithme d'Euclide

Terminale – Option Mathématiques expertes

1 Diviseurs d'un entier

Rappelons qu'un entier d *divise* un entier a s'il existe un entier k tel que $a = dk$. On note $d \mid a$.

Diviseurs d'un entier

Soit a un entier non nul.

- L'ensemble des diviseurs de a est fini : tout diviseur d de a vérifie $|d| \leq |a|$.
- Les diviseurs de a et de $-a$ sont les mêmes ; les diviseurs de a vont par paires $\{d, -d\}$.
- Si $a \in \mathbb{N}^*$ et si d est un diviseur de a, alors $\dfrac{a}{d}$ est aussi un diviseur de a ; les diviseurs positifs vont donc par paires $\left\{d, \dfrac{a}{d}\right\}$ avec $d \leq \sqrt{a}$ ou $\dfrac{a}{d} \leq \sqrt{a}$.

Méthode : déterminer les diviseurs positifs d'un entier a

On teste la divisibilité de a par tous les entiers d tels que $1 \leq d \leq \sqrt{a}$. Chaque diviseur d trouvé fournit un second diviseur $\dfrac{a}{d}$.

Exemple

Diviseurs positifs de 84 : on a $\sqrt{84} \approx 9{,}2$, on teste donc $d = 1, \ldots, 9$.

d	1	2	3	4	5	6	7	8	9
$d \mid 84$?	oui	oui	oui	oui	non	oui	oui	non	non
$84/d$	84	42	28	21	–	14	12	–	–

L'ensemble des diviseurs positifs de 84 est $\{1; 2; 3; 4; 6; 7; 12; 14; 21; 28; 42; 84\}$.

Diviseurs communs

Soient a et b deux entiers. Un entier d est un **diviseur commun** à a et b s'il divise à la fois a et b.

2 PGCD de deux entiers

PGCD

Soient a et b deux entiers **non tous deux nuls**. L'ensemble des diviseurs communs à a et b est non vide (il contient 1) et fini. Son plus grand élément est appelé le **plus grand commun diviseur** de a et b, noté $\mathrm{PGCD}(a, b)$.

Exemple

Diviseurs positifs de 84 : $\{1; 2; 3; 4; 6; 7; 12; 14; 21; 28; 42; 84\}$.
Diviseurs positifs de 36 : $\{1; 2; 3; 4; 6; 9; 12; 18; 36\}$.
Diviseurs positifs communs : $\{1; 2; 3; 4; 6; 12\}$. Donc $\mathrm{PGCD}(84, 36) = 12$.

Premières propriétés

Soient a et b deux entiers non tous deux nuls.

1. $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,a)$ et $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(|a|,|b|)$;
2. $\mathrm{PGCD}(a,0) = |a|$ pour $a \neq 0$; $\mathrm{PGCD}(a,1) = 1$;
3. si b divise a (avec $b \neq 0$), alors $\mathrm{PGCD}(a,b) = |b|$;
4. $\mathrm{PGCD}(a,b) \geq 1$.

Démonstration. Les diviseurs de a et de $-a$ sont les mêmes, d'où la propriété 1. Pour 2 : tout entier divise 0, donc les diviseurs communs à a et 0 sont les diviseurs de a, dont le plus grand est $|a|$. Pour 3 : si $b \mid a$, tout diviseur de b divise a, donc les diviseurs communs à a et b sont exactement les diviseurs de b, dont le plus grand est $|b|$. La propriété 4 vient de ce que 1 est un diviseur commun. □

Entiers premiers entre eux

Deux entiers a et b sont dits **premiers entre eux** si $\mathrm{PGCD}(a,b) = 1$, c'est-à-dire si leurs seuls diviseurs communs sont 1 et -1.

Exemple

$\mathrm{PGCD}(15,28) = 1$: les diviseurs positifs de 15 sont $1;3;5;15$, ceux de 28 sont $1;2;4;7;14;28$, et le seul diviseur commun est 1. Ainsi 15 et 28 sont premiers entre eux, bien qu'aucun des deux ne soit premier.

Remarque : par la décomposition en facteurs premiers

Si l'on connaît les décompositions de a et b en produit de facteurs premiers, $\mathrm{PGCD}(a,b)$ est le produit des facteurs premiers communs, chacun affecté du plus petit des deux exposants. Par exemple, $84 = 2^2 \times 3 \times 7$ et $36 = 2^2 \times 3^2$ donnent $\mathrm{PGCD}(84,36) = 2^2 \times 3 = 12$. Cette méthode devient toutefois très coûteuse pour de grands nombres, d'où l'intérêt de l'algorithme d'Euclide.

3 Un lemme fondamental

Lemme d'Euclide

Soient a et b deux entiers, avec $b \neq 0$, et soit $a = bq + r$ une égalité avec q et r entiers (en particulier, la division euclidienne de a par b si $b > 0$ et $0 \leq r < b$). Alors

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r).$$

Démonstration. Montrons que les couples (a,b) et (b,r) ont les mêmes diviseurs communs.

— Si d divise a et b, alors d divise $r = a - bq$. Donc d est un diviseur commun de b et r.
— Réciproquement, si d divise b et r, alors d divise $a = bq + r$. Donc d est un diviseur commun de a et b.

Les deux ensembles de diviseurs communs sont égaux, ils ont donc le même plus grand élément. □

Exemple

$84 = 36\times2+12$, donc $\mathrm{PGCD}(84,36) = \mathrm{PGCD}(36,12)$. Or 12 divise 36, donc $\mathrm{PGCD}(36,12) = 12$.

4 Algorithme d'Euclide

Soient a et b deux entiers naturels avec $a \geq b > 0$. On effectue des divisions euclidiennes successives :

$$\begin{aligned} a &= b\,q_1 + r_1 & 0 \leq r_1 < b \\ b &= r_1\,q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= r_2\,q_3 + r_3 & 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

tant que le reste obtenu est non nul : on divise à chaque étape le diviseur précédent par le reste précédent.

Algorithme d'Euclide

La suite des restes $b > r_1 > r_2 > \cdots \geq 0$ est une suite strictement décroissante d'entiers naturels : elle atteint donc 0 au bout d'un nombre fini d'étapes. De plus,

$$\boxed{\text{PGCD}(a,b) = \text{le dernier reste non nul.}}$$

Démonstration. Une suite strictement décroissante d'entiers naturels est nécessairement finie ; il existe donc un entier n tel que $r_n \neq 0$ et $r_{n+1} = 0$. D'après le lemme d'Euclide appliqué à chaque étape,

$$\text{PGCD}(a,b) = \text{PGCD}(b,r_1) = \text{PGCD}(r_1,r_2) = \cdots = \text{PGCD}(r_{n-1},r_n).$$

Or $r_{n+1} = 0$ signifie que r_n divise r_{n-1}, donc $\text{PGCD}(r_{n-1},r_n) = r_n$. □

Méthode : calculer un PGCD avec l'algorithme d'Euclide

On pose les divisions euclidiennes successives en remplaçant à chaque étape le couple (dividende, diviseur) par (diviseur, reste), jusqu'à obtenir un reste nul. Le PGCD est le dernier reste non nul.

Exemple 1

Calculons $\text{PGCD}(1071, 462)$.

$$\begin{aligned} 1071 &= 462 \times 2 + 147 \\ 462 &= 147 \times 3 + 21 \\ 147 &= 21 \times 7 + 0 \end{aligned}$$

Le dernier reste non nul est 21, donc $\text{PGCD}(1071, 462) = 21$.

Exemple 2

Calculons $\text{PGCD}(252, 198)$.

$$\begin{aligned} 252 &= 198 \times 1 + 54 \\ 198 &= 54 \times 3 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 + 0 \end{aligned}$$

Donc $\text{PGCD}(252, 198) = 18$.

Algorithme en Python

```
def pgcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

Ici `a % b` désigne le reste de la division euclidienne de `a` par `b`. À chaque passage dans la boucle, le couple (a, b) est remplacé par (b, r) où r est le reste de la division de a par b : d'après le lemme d'Euclide, le PGCD ne change pas. La boucle s'arrête quand $b = 0$, et le PGCD vaut alors a.

5 Une propriété du PGCD

PGCD et multiplication

Soient a et b deux entiers naturels non tous deux nuls et k un entier naturel non nul. Alors

$$\text{PGCD}(ka, kb) = k \text{ PGCD}(a, b).$$

Démonstration. Supposons $a \geq b > 0$ (les autres cas sont immédiats). Si $a = bq + r$ avec $0 \leq r < b$, alors $ka = kbq + kr$ avec $0 \leq kr < kb$: c'est la division euclidienne de ka par kb. Ainsi, dans l'algorithme d'Euclide appliqué à (ka, kb), tous les restes sont ceux obtenus pour (a, b) multipliés par k. Le dernier reste non nul est donc k fois celui obtenu pour (a, b), d'où l'égalité. □

Corollaire : simplifier par le PGCD

Soient a et b deux entiers naturels non nuls et $d = \text{PGCD}(a, b)$. Il existe deux entiers a' et b' **premiers entre eux** tels que $a = da'$ et $b = db'$.

Démonstration. Comme d divise a et b, on peut écrire $a = da'$ et $b = db'$. D'après la propriété précédente, $d = \text{PGCD}(da', db') = d \text{ PGCD}(a', b')$, donc $\text{PGCD}(a', b') = 1$. □

Exemple

$\text{PGCD}(84, 36) = 12$ et $84 = 12 \times 7$, $36 = 12 \times 3$ avec $\text{PGCD}(7, 3) = 1$. On retrouve ainsi que la fraction $\dfrac{84}{36}$ se simplifie en la fraction irréductible $\dfrac{7}{3}$.

À retenir

- $\text{PGCD}(a, b)$ est le plus grand des diviseurs communs de a et b ; a et b sont premiers entre eux lorsque $\text{PGCD}(a, b) = 1$.
- Si $a = bq + r$, alors $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.
- Algorithme d'Euclide : divisions euclidiennes successives ; le PGCD est le dernier reste non nul.
- $\text{PGCD}(ka, kb) = k \text{ PGCD}(a, b)$; en divisant a et b par leur PGCD, on obtient deux entiers premiers entre eux.