PGCD de deux entiers relatifs

1 Plus grand commun diviseur de deux entiers relatifs

Définition 1 *Etant donné deux entiers relatifs a et b il existe un unique entier* ***naturel*** *d tel que d est un diviseur commun à a et à b et c'est le plus grand des diviseurs communs à a et à b*

On dit que d est le plus grand commun diviseur à a et à b et on note $d = \text{pgcd}(a, b)$

Cette définition a un **sens** car :

1. L'ensemble des diviseurs communs à a et b est une partie **finie** et **non vide** de $\mathbb{Z}$ car 1 est un diviseur commun à a et b
2. Toute partie **finie** et **non vide** de $\mathbb{Z}$ a un plus **grand** élément

Exemple : $\text{pgcd}(42, 70) = 14$

Théorème 1 *1. Pour tout $a \in \mathbb{Z}$ on a $\text{pgcd}(a, 0) = |a|$*

2. Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ on a $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$

3. Si d est une combinaison linéaire de a et b alors $\text{pgcd}(a, b)|d$

4. Pour tout $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ puisqu'il existe q et r entiers naturels uniques tel que $0 \leqslant r < b$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$

Preuve

1. Tout nombre divise 0 donc les diviseurs communs à a et à 0 sont les diviseurs de a. Par conséquent le plus grand des diviseurs communs est a si $a > 0$ ou $-a$ si $a < 0$ donc c'est $|a|$
2. Les diviseurs communs à $|a|$ et à $|b|$ sont l'intersection de $\mathbb{N}$ avec les diviseurs communs de a et b par conséquent on obtient le même plus grand élément
3. pgcd(70,42) = 14 et 70 - 42 = 28. En effet si $d = aw + bt$ est une combinaison linéaire de a et b alors $\text{pgcd}(a, b)$ étant un diviseur commun à a et à b divise toute combinaison linéaire de a et b donc d
4. Notons $\mathcal{D}(a) \cap \mathcal{D}(b)$ l'ensemble des diviseurs communs à a et b

   Montrons que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$ en utilisant la **méthode de la double inclusion** (il s'ensuivra que $\text{pgcd}(a, b) = \text{pgcd}(b, r)$) $E = F \iff E \subset F$ et $F \subset E \iff \forall x \in E\ x \in F$ et $\forall x \in F\ x \in E$

   (a) $\forall x \in \mathcal{D}(a) \cap \mathcal{D}(b)$, x divise toute **combinaison linéaire** de a et b or $r = a - bq$ est une combinaison linéaire de a et b donc x divise r or x divise b par hypothèse donc $x \in \mathcal{D}(b) \cap \mathcal{D}(r)$

   (b) $\forall x \in \mathcal{D}(b) \cap \mathcal{D}(r)$, x divise toute **combinaison linéaire** de b et r or $a = bq + r$ est une combinaison linéaire de b et r donc x divise a or x divise b par hypothèse donc $x \in \mathcal{D}(a) \cap \mathcal{D}(b)$

2 Algorithme d'Euclide

Utilisons plusieurs fois la propriété 3 du théorème 1 sur un exemple
$70 = 42 \times 1 + 28$ donc $\text{pgcd}(70, 42) = \text{pgcd}(42, 28)$
$42 = 28 \times 1 + 14$ donc $\text{pgcd}(42, 28) = \text{pgcd}(28, 14)$
$28 = 14 \times 2 + 0$ donc $\text{pgcd}(28, 14) = \text{pgcd}(14, 0) = 14$
On finit par obtenir $\text{pgcd}(70, 42)$
Pourquoi ?
Ecrivons le processus dans le cas général : ($a > 0$ et $b > 0$)

$a = bq + r_1$ avec $0 \leqslant r_1 < b$
$b = r_1q_1 + r_2$ avec $0 \leqslant r_2 < r_1 < b$
$r_1 = r_2q_2 + r_3$ avec $0 \leqslant r_3 < r_2 < r_1 < b$
.....
$r_{n-1} = r_nq_n + r_{n+1}$ avec $0 \leqslant r_{n+1} < r_n < r_{n-1} < ... < r_2 < r_1 < b$
On a donc une suite d'entiers naturels **strictement décroissante**, or

Lemme 1 *Toute suite strictement décroissante d'entiers naturels s'annule à partir d'un certain rang*

Donc il existe un rang N tel que :
$r_{N-1} = r_Nq_N$ avec $0 \leqslant r_N < r_{N-1} < ... < r_2 < r_1 < b$ et $\text{pgcd}(a, b) = r_N$
On retiendra que le plus grand commun diviseur de a et b est le dernier reste non nul de l'algorithme d'Euclide d'où la fonction Python permettant de calculer le $\text{pgcd}(a, b)$ avec $a > 0$ et $b > 0$

```
def pgcd(a,b):
    dividende = a
    diviseur = b
    reste = dividende \% diviseur
    while reste != 0:
        dividende = diviseur
        diviseur = reste
        reste = dividende \% diviseur
    return diviseur
```

Comment être sûr que cet algorithme "est efficace", qu'il donne toujours le $\text{pgcd}(a, b)$?
Faut-il le tester sur de nombreux cas particuliers ? Et même s'il donne les "bons pgcd" sur un grand nombre de cas particuliers, est ce suffisant pour dire qu'il "fonctionnera" toujours.
Nous allons parler de **"preuve de programme"** et **d'"invariant de boucle"**
Un invariant de boucle est une relation entre les variables du programme est, qui comme son nom l'indique, reste invariante à chaque tour de boucle
Ici la relation est **reste = dividende % diviseur** . Ici il y a un abus de langage, `reste` n'est pas la variable mais la valeur associée à cette variable.
Démontrons par récurrence que **reste = dividende % diviseur** reste vraie à chaque tour de boucle.

1. **Vrai** avant le premier tour de boucle car la valeur de `dividende` est a celle de `diviseur` est b et celle de `reste` est $r = a - bq$ donc c'est vrai

2. S'il y a eu k tours de boucle donc à la fin de la boucle
   reste = dividende % diviseur ensuite au $k+1$ ième tour de boucle `dividende` et `diviseur` changent de valeur mais à la fin de la boucle on a encore
   reste = dividende % diviseur
3. L'initialisation et l'hérédité font qu'à la fin de la boucle la relation reste invariante. Or à la fin de la boucle la valeur de `reste` est 0 donc le pgcd est la valeur de `diviseur`, donc la fonction retourne bien le pgcd de a et b

3 Théorème de Bezout

Etienne Bezout est un mathématicien français du XVIII ième siècle.

De l'algorithme d'Euclide on peut en plus du pgcd de a et b, exprimer le pgcd comme une combinaison linéaire de a et b. Regardons cela sur une exemple avant de généraliser

On dit que l'on "remonte" l'algorithme d'Euclide de la fin vers le début.

On part de l'avant dernière ligne :

$42 = 28 \times 1 + 14$ donc $\underline{14} = \underline{42} - 28 \times 1$

Je ne touche aux termes devant apparaître dans la combinaison linéaire (termes soulignés)

Or dans la première ligne $28 = 70 - 42 \times 1$

Donc $14 = 42 - (70 - 42) = -1 \times 70 + 2 \times 42$

Théorème 2 ***(Bezout)*** *Etant donné deux entiers naturels a et b , il existe deux entiers relatifs u et v tel que $au + bv = d$ où $d = \text{pgcd}(a, b)$*

Preuve

Ecrivons les N lignes vues précédemment : (on n'utilise pas la dernière ligne de l'algorithme d'Euclide)

$a = bq + r_1$ avec $k = N$ (k désigne le numéro de ligne mais on part de l'avant dernière ligne)

$b = r_1 q_1 + r_2$ avec $k = N - 1$

$r_1 = r_2 q_2 + r_3$ avec $k = N - 2$

.....

$r_{N-3} = r_{N-2} q_{N-2} + r_{N-1}$ avec $k = 2$

$r_{N-2} = r_{N-1} q_{N-1} + r_N$ avec $k = 1$

$r_{N-1} = r_N q_N$ avec $r_N = \text{pgcd}(a, b)$

(On remarque que le numéro de ligne plus l'indice du reste de la division euclidienne est toujours égal à $N + 1$) (*)

Démontrons par récurrence sur k que :

Pour tout k avec $1 \leqslant k \leqslant N$ on a $r_N = CL(r_{N-k}, r_{N-k-1})$ où CL signifie combinaison linéaire

(Pour que la notation soit cohérente on notera a par r_{-1} et b par r_0)

1. **Vrai pour $k = 1$**
   $r_N = r_{N-2} - r_{N-1} q_{N-1}$ que l'on écrit $r_N = CL(r_{N-1}, r_{N-2})$

2. Supposons que la propriété est vraie pour $k \geqslant 1$ et montrons qu'elle est vraie pour $k+1$
   Si $r_N = CL(r_{N-k}, r_{N-k-1})$ or à la ligne $k+1$ (voir remarque (*)) on peut écrire $r_{N-k} = CL(r_{N-k-1}, r_{N-k-2}$
   donc $r_N = CL(r_{N-k-1}, r_{N-k-2})$
3. L'initialisation et l'hérédité font que la propriété reste vraie jusqu'au bout de la "remontée" donc elle vraie pour $k = N$
   Donc $r_N = CL(r_0, r_{-1}) = CL(b, a)$

Attention ! cette combinaison linéaire n'est pas unique
par exemple $14 = -1 \times 70 + 2 \times 42 = 2 \times 70 - 3 \times 42$
(Voir prochain chapitre : équations diophantiennes)

Définition 2 *Deux entiers relatifs sont dits premiers entre eux lorsque leur pgcd est égal à 1*

Exemple : 12 et 7 sont premiers entre eux
Propriété *Deux entiers consécutifs sont premiers entre eux*
Preuve
Soit deux entiers consécutifs n et $n+1$ alors tout diviseur d commun à n et $n+1$ divise la combinaison linéaire particulière $n+1-n=1$ donc d vaut 1 ou -1 donc le pgcd vaut 1
Corollaires du Théorème de Bezout :

1. *Si d est un diviseur commun à a et à b alors d divise* $\text{pgcd}(a, b)$
2. *a et b premiers entre eux $\iff$ il existe u et v entiers relatifs tel que $au+bv=1$*
3. (**Lemme de Gauss**) *si a divise bc et a et b premiers entre eux alors a divise c*
4. Si d = $\text{pgcd}(a, b)$ alors $a' = \dfrac{a}{d}$ et $b' = \dfrac{b}{d}$ sont premiers entre eux

Preuve

1. Si d est un diviseur commun à a et à b alors il divise toute combinaison linéaire de a et b or le pgcd de a et b est une combinaison particulière donc $d|$ $\text{pgcd}(a, b)$
2. Démontrons le sens $\Leftarrow$ Si $au+bv=1$ alors $\text{pgcd}(a, b)|1$ donc $\text{pgcd}(a, b) = 1$
3. Si a divise bc il existe k entier relatif tel que $bc = ka$ or a et b sont premiers entre eux donc il existe u et v entiers relatifs tel que $au+bv=1$ si on multiplie de part et d'autre par c on a $acu+bcv=c$ donc $acu+kav=c$ donc $a(cu+kv)=c$ ce qui signifie que $a|c$
4. $d = au+bv$ donc $\dfrac{d}{d} = \dfrac{a}{d}u + \dfrac{b}{d}v$ donc $1 = a'u+b'v$

4 Equation (E) : $ax + by = c$ avec a,b, c des entiers relatifs donnés

Méthode :

1. On calcule d le pgcd de a et b
2. Si d ne divise pas c il n'y a pas de solution car le pgcd divise toute combinaison linéaire de a et b
3. Sinon on pose $a' = \dfrac{a}{d}$, $b' = \dfrac{b}{d}$ et $c' = \dfrac{c}{d}$
   et on résout $a'X + b'Y = 1$ car on sait que a' et b' sont premiers entre eux
   Avec l'algorithme d'Euclide on a une solution particulière (X_0, Y_0) toute autre solution (X, Y) vérifie $a'X + b'Y = a'X_0 + b'Y_0$
   $\iff$ $a'(X - X_0) = b'(Y_0 - Y)$ donc a' divise $b'(Y_0 - Y)$ et puisque a' et b' sont premiers entre eux on a a' divise $Y_0 - Y$ donc il existe k relatif tel que $Y_0 - Y = ka'$
   De même il existe l relatif tel que $X - X_0 = lb'$ et par conséquent $a'lb' = b'ka'$ donc $l = k$
   On a montré que si (X, Y) est une solution de $a'X + b'Y = 1$ alors $X = X_0 + kb'$ et $Y = Y_0 - ka'$ pour une certain k entier relatif
   Considérons maintenant tous les nombres $X = X_0 + kb'$ et $Y = Y_0 - ka'$ avec $k \in \mathbb{Z}$, ils sont tous solutions de $a'X + b'Y = 1$
   Donc les solutions de $a'X + b'Y = 1$ sont les nombres $X = X_0 + kb'$ et $Y = Y_0 - ka'$ avec $k \in \mathbb{Z}$
4. Les solutions de $a'x + b'y = c'$ sont les nombres $c'X = c'X_0 + kc'b'$ et $c'Y = c'Y_0 - kc'a'$ avec $k \in \mathbb{Z}$

Exemples

1. Résoudre $70x + 42y = 5$
   Pas de solution car $\text{pgcd}(70, 42) = 14$ ne divise pas 5
2. Résoudre $70x + 42y = 28$
   On cherche à résoudre $5x + 3y = 1$, en appliquant la méthode on trouve que toutes les solutions sont les couples $(-1 + 3k, 2 - 5k)$ avec $k \in \mathbb{Z}$
   Donc les solutions de l'équation sont $(-2 + 6k, 4 - 10k)$ avec $k \in \mathbb{Z}$