



### I. PGCD de deux nombres entiers (*gcd in english*)

#### Définition 1

Soient  $a$  et  $b$  deux entiers relatifs non simultanément nuls. L'ensemble des diviseurs communs à  $a$  et  $b$  est une partie non vide de  $\mathbb{Z}$  (elle contient 1) et majorée (par le maximum entre  $|a|$  et  $|b|$ ).  
 Cet ensemble admet un plus grand élément appelé Plus Grand Diviseur Commun de  $a$  et  $b$ .  
 On le note  $PGCD(a, b)$  ou parfois  $a \wedge b$ .



#### Remarque

- on a :  $PGCD(a, b) = PGCD(b, a)$ .
- On utilise le lemme suivant : « Toute partie non vide et majorée de  $\mathbb{Z}$  admet un unique plus grand élément. »



#### Exemple

Déterminer le  $PGCD$  de 30 et de  $-12$ .  
 .....  
 .....  
 .....  
 .....

#### Propriété 1

Soient  $a$  et  $b$  deux entiers relatifs non simultanément nuls.  
 On a  $PGCD(a; b) = PGCD(|a|; |b|)$  et pour tout couple  $(a; b) \in \mathbb{N}^2$  avec  $a \neq 0$  :

1.  $PGCD(a; b) \geq 1$ ,  $PGCD(a; 0) = a$  et  $PGCD(a; 1) = 1$ .

2.  $a$  divise  $b$  si et seulement si  $PGCD(a; b) = a$ .

$$PGCD(a; b) = a \iff a|b$$

3. Méthode de soustraction (avec  $a \geq b$ ) :

$$PGCD(a; b) = PGCD(a - b; b)$$



#### Preuve

On note  $P$  le  $PGCD$  de  $a$  et  $b$ .

1.  $PGCD(a; b) \geq 1$ ,  $PGCD(a; 0) = a$  et  $PGCD(a; 1) = 1$ .

- 1 est un diviseur commun à tous les entiers, donc le plus grand commun diviseur de deux entiers est au moins égal à 1 (donc positif).
- Si  $b = 0$ , alors  $P$  est un diviseur commun à  $a$  et 0. Or  $a$  est un diviseur commun à lui-même et 0. Comme  $a$  est le plus grand diviseur de  $a$ ,  $P = a$ .
- Si  $b = 1$ , alors le plus grand diviseur de  $b$  est 1. De plus 1 divise aussi  $a$ . Donc  $P = 1$ .

2.  $a$  divise  $b$  si et seulement si  $\text{PGCD}(a; b) = a$ .

- Si  $a|b$ , alors  $a$  est un diviseur commun à  $a$  et  $b$ . Et comme  $a$  est son plus grand diviseur, on a  $P = a$ .
- réciproquement si  $P = a$ , alors  $a$  est un diviseur commun à  $a$  et  $b$ . En particulier,  $a|b$ .
- On a donc, au final, démontré l'équivalence :

$$P = a \iff a|b$$

3. Méthode de soustraction :

$$\text{PGCD}(a; b) = \text{PGCD}(a - b; b)$$

- Supposons que  $a \geq b$ . Puisque  $P$  divise  $a$  et  $b$ , alors  $P$  divise  $a - b$ . Ainsi,  $P$  est un diviseur commun à  $a - b$  et  $b$ , et donc  $P \leq \text{PGCD}(a - b; b)$ .
- Réciproquement, si  $d$  est un diviseur commun à  $a - b$  et  $b$ , alors  $d$  divise  $(a - b) + b = a$ , donc  $d$  est un diviseur commun à  $a$  et  $b$ .  
En particulier,  $\text{PGCD}(a - b; b)$  est un diviseur commun à  $a$  et  $b$ , donc  $\text{PGCD}(a - b; b) \leq P$ .
- On vient de montrer qu'on a à la fois  $P \leq \text{PGCD}(a - b; b)$  et  $\text{PGCD}(a - b; b) \leq P$  donc, en conclusion,  $P = \text{PGCD}(a - b; b)$ .

## II. Détermination rapide du PGCD

Dans cette partie,  $a$  et  $b$  sont deux entiers naturels non nuls avec  $a > b$ .

### II.1 Lemme d'Euclide

#### Propriété 2

$a, b, q$  et  $r$  sont des entiers relatifs non nuls.

On note  $q$  et  $r$  le quotient et le reste de la division euclidienne de  $a$  par  $b$ .

$$a = bq + r \quad ; \quad 0 \leq r < b$$

Avec ces notations,

$$\boxed{\text{PGCD}(a; b) = \text{PGCD}(b; r)}$$

On a aussi : l'ensemble des diviseurs de  $a$  et de  $b$  est égal à l'ensemble des diviseurs de  $b$  et de  $r$ .



#### Preuve

- Soit  $d$  un diviseur commun à  $a$  et  $b$ . Par définition,  $a = bq + r$  donc  $r = a - bq$ .  
 $r$  s'écrit donc comme une combinaison linéaire de  $a$  et de  $b$  et  $d$  divise à la fois  $a$  et  $b$ .  
Donc  $d$  divise  $r$ .  
En particulier,  $d$  est un diviseur commun à  $b$  et  $r$ .
- De même,  $a$  est une combinaison linéaire de  $b$  et  $r$ , donc tout diviseur commun à  $b$  et  $r$  divise  $a$ .
- Ainsi, l'ensemble des diviseurs communs à  $a$  et  $b$  est confondu avec l'ensemble des diviseurs communs à  $b$  et  $r$ . Ils ont donc le même plus grand élément d'où

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

## II.2 Algorithme d'Euclide

$a$  et  $b$  sont deux entiers naturels non nuls avec  $a > b$ .

### Propriété 3

$a$  et  $b$  sont deux entiers naturels non nuls avec  $a > b$ .

- Si  $b$  divise  $a$ , le *PGCD* de  $a$  et de  $b$  est égal à  $b$ .
- Si  $b$  ne divise pas  $a$ , le *PGCD* de  $a$  et de  $b$  est le dernier reste non nul dans l'exécution de l'algorithme d'Euclide.



### Exercice 1

| Déterminer, avec l'algorithme d'Euclide, le *PGCD* de 6 825 et 15 675.



### Correction



### Exercice 2

| Compléter cette fonction Python qui traduit l'algorithme d'Euclide :

```
1 def pgcd(a,b) :  
2     if b > a : # on échange a et b si b > a  
3         a,b = b,a  
4     while .....:  
5         reste = ....  
6         a = b  
7         b = reste  
8     return .....
```

### III. Des propriétés utiles

**Propriété 4**

$a, b$  et  $\lambda a + b$  sont des entiers naturels non nuls. Alors

$$PGCD(a, b) = PGCD(a, \lambda a + b)$$



**Exercice 3**

$n$  est un entier naturel non nul. Quel est le  $PGCD$  de  $n$  et  $n + 2$ ?



**Correction**

**Propriété 5**

$a, b$  et  $k$  sont des entiers naturels non nuls. Alors

$$PGCD(ka, kb) = k \times PGCD(a, b)$$



**Preuve**

- Étape 1 :

La division euclidienne de  $a$  par  $b$  s'écrit

$$a = qb + r \quad \text{avec } 0 \leq r < b.$$

En multipliant cette égalité par  $k \in \mathbb{N}^*$ , on obtient

$$ka = q(kb) + kr.$$

Puisque  $r < b$ , il suit que  $kr < kb$ , ce qui montre que l'égalité précédente est la division euclidienne de  $ka$  par  $kb$ .

- Étape 2 : On sait que  $\text{PGCD}(a, b)$  est le dernier reste non nul dans la suite des restes obtenus par l'algorithme d'Euclide. Soit  $(r_n)_{n \geq 0}$  la suite des restes construite par cet algorithme appliqué aux entiers  $a$  et  $b$ , et soit  $m \geq 0$  l'entier tel que

$$r_m \neq 0 \quad \text{et} \quad r_{m+1} = 0.$$

Alors,

$$\text{PGCD}(a, b) = r_m.$$

D'après ce qui précède, on a

$$\text{PGCD}(ka, kb) = \text{PGCD}(kb, kr_0) = \dots = \text{PGCD}(kr_m, kr_{m+1}) = kr_m,$$

puisque  $r_{m+1} = 0$ . On en déduit que

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

□

### Propriété 6

Soient  $a$  et  $b$  deux entiers non simultanément nuls.

$d$  est un diviseur commun à  $a$  et  $b$  si, et seulement si,  $d$  divise  $\text{PGCD}(a; b)$ .



### Preuve

- Soit  $d \in \mathbb{Z}$  est un diviseur commun de  $a$  et  $b$ .

Soit  $(a, b) \in \mathbb{Z}^2$ .

On suppose que  $a$  et  $b$  ne sont pas simultanément nuls et que  $d \in \mathbb{Z}$  est un diviseur commun de  $a$  et  $b$ . On sait qu'il en existe au moins un, 1 (même si ils sont premiers entre eux).

Nous allons montrer que  $d$  divise  $\text{PGCD}(a, b)$  en prouvant par récurrence que  $d$  divise tous les restes obtenus par l'algorithme d'Euclide.

- **Initialisation.** Soient  $q$  et  $r_0$  respectivement le quotient et le reste de la division euclidienne de  $a$  par  $b$ . On a alors

$$r_0 = a - bq.$$

Puisque  $r_0$  est une combinaison linéaire de  $a$  et  $b$ , il en découle que  $d$  divise  $r_0$ .

- **Hérédité.** Supposons que nous avons construit la suite des restes  $r_0, r_1, \dots, r_m$  de sorte que, pour tout  $k \in \{1, \dots, m-1\}$ , le terme  $r_{k+1}$  est le reste de la division euclidienne de  $r_{k-1}$  par  $r_k$ , et que  $d$  divise à la fois  $r_{m-1}$  et  $r_m$ . D'après la division euclidienne, on a

$$r_{m-1} = q_m r_m + r_{m+1},$$

ce qui s'écrit

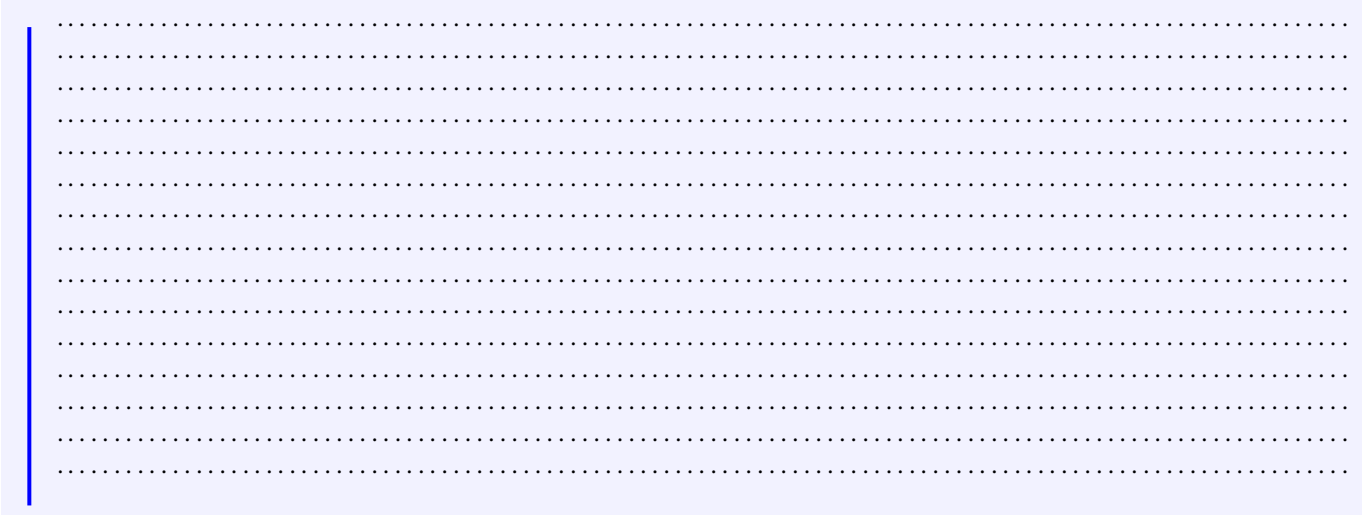
$$r_{m+1} = r_{m-1} - q_m r_m.$$

Comme  $d$  divise  $r_{m-1}$  et  $r_m$ , il divise aussi  $r_{m+1}$  par linéarité.

- **Conclusion.** Par récurrence, pour tout  $k \in \{1, \dots, m\}$ , le reste  $r_k$  est divisible par  $d$ . Comme  $\text{PGCD}(a, b)$  est le dernier terme non nul de cette suite, il en résulte que  $d$  divise  $\text{PGCD}(a, b)$ .
- Réciproquement :  
si  $d$  divise  $\text{PGCD}(a, b)$ , alors, puisque  $\text{PGCD}(a, b)$  divise  $a$  et  $b$ , par transitivité  $d$  divise aussi  $a$  et  $b$ .
- En conclusion, les diviseurs de  $\text{PGCD}(a, b)$  sont exactement les diviseurs communs à  $a$  et  $b$ .





A large rectangular area with a light blue background and a grid of small dots, intended for writing answers. The grid consists of approximately 20 rows and 90 columns of dots. A solid blue vertical line is positioned on the left side of the grid, about 5% of the way across.



**Exercice 7**

$n$  est un entier naturel. On pose :  $a = 3n + 4$  et  $b = 2n + 3$ .

Montrer que  $a$  et  $b$  sont premiers entre eux.

**Correction**



.....  
 .....



**Remarque**

| **Attention!** Le couple  $(u; v)$  n'est pas unique. Trouver deux couples  $(u; v)$  pour  $a = 3$  et  $b = 2$ .



**Correction**

.....  
 .....



**Remarque**

| **Attention encore!** La réciproque de l'identité de Bézout est fausse.  
 Utiliser l'égalité  $3 \times 2 + 2 \times (-2) = 2$  pour vous en convaincre.

**Exercice 8**

| Déterminer le PGCD  $d$  de 235 et 45 puis des coefficients de Bézout associés.

**Correction**

A large area of dotted lines for writing the solution.

**Propriété 9**

Soient  $a$ ,  $b$  et  $c$  trois entiers tels que  $a$  et  $b$  ne soient pas simultanément nuls.  
L'équation

$$ax + by = c$$

admet des couples d'entiers  $(x, y)$  solutions si, et seulement si, le nombre  $c$  est un multiple de  $\text{PGCD}(a, b)$ .

**Preuve****1. Montrer que si l'équation  $ax + by = c$  admet des solutions, alors  $\text{PGCD}(a, b) \mid c$ .**

On pose  $d = \text{PGCD}(a, b)$ . Il existe deux entiers  $a'$  et  $b'$  tels que  $a = da'$  et  $b = db'$ . Soit maintenant  $(x, y)$  un couple d'entiers solution de l'équation  $ax + by = c$ . Alors on peut réécrire cette égalité comme suit :

$$da'x + db'y = c,$$

autrement dit,

$$d(a'x + b'y) = c.$$

Ainsi,  $d \mid c$ .

**2. Réciproquement, supposons que  $c$  est un multiple de  $\text{PGCD}(a, b)$ .**

Soit  $c'$  l'entier tel que  $c = c' \cdot \text{PGCD}(a, b)$ . Déduisons de l'identité de Bézout qu'il existe un couple solution de l'équation  $ax + by = c$ .

D'après l'identité de Bézout, il existe deux entiers  $x$  et  $y$  tels que :

$$ax + by = \text{PGCD}(a, b).$$

En multipliant les deux membres de l'égalité par  $c'$ , on obtient alors :

$$a(c'x) + b(c'y) = c.$$

Le couple d'entiers  $(c'x, c'y)$  est donc solution de l'équation  $ax + by = c$ .

**Exemple**

1. L'équation  $12x + 4y = 32$  admet des couples d'entiers  $(x, y)$  parmi ses solutions car  $\text{PGCD}(12, 4) = 4$  et  $4 \mid 32$ .
2. L'équation  $2x + 6y = 3$  n'admet pas de couples de solutions entières car  $\text{PGCD}(2, 6) = 2$  et  $2 \nmid 3$ .

## VI. Théorème de Gauss

### VI.1 Le théorème du Gauss

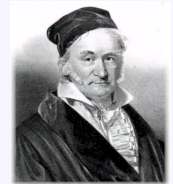
**Théorème 2** (Carl Friedrich Gauss, 1777-1855)

Soit  $a, b, c$  des entiers.

Si  $\begin{cases} a \text{ divise le produit } bc \\ a \text{ et } b \text{ sont premiers entre eux} \end{cases}$ , alors  $a$  divise  $c$ .

Ce que l'on peut écrire :

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$



**Remarque** : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorème (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».



#### Preuve

## VI.2 Une conséquence du théorème

## Propriété 10

$a$ ,  $b$  et  $c$  sont trois entiers relatifs non nuls.

**Si**  $b$  et  $c$  sont premiers entre eux **et si**  $b$  et  $c$  divisent  $a$ , **alors**  $bc$  divise  $a$ .

Ce que l'on peut écrire :

$$\begin{cases} b \mid a \text{ et } c \mid a \\ b \wedge c = 1 \end{cases} \implies bc \mid a$$



## Preuve

### VI.3 Application : Équation Diophantienne

#### Exercice 9

Déterminer TOUS les entiers  $u$  et  $v$  tels que  $6u + 11v = 1$



#### Correction

- Une solution particulière.

Par divisions euclidiennes successives on obtient avec  $a = 11$  et  $b = 6$  :

Division euclidienne	Reste	Egalité avec $a$ et $b$
$11 = 6 \times 1 + 5$	$5 = 11 - 1 \times 6$	$5 = a - 1 b$
$6 = 5 \times 1 + 1$	$1 = 6 - 1 \times 5$	$1 = b - 1 \times (a - 1 b)$ $1 = -1 a + 2 b$

Le PGCD des nombres 11 et 6 est le dernier reste non nul du procédé, c'est-à-dire 1.

Les nombres 11 et 6 sont donc premiers entre eux et le théorème 1 dit de Bézout-Bachet assure donc l'existence de couples  $(u ; v)$  d'entiers relatifs solutions de l'équation :

$$6 u + 11 v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de  $a$  et  $b$  pour chaque ligne du procédé. Un couple solution de l'équation  $6 u + 11 v = 1$  est donc :

$$(u = 2 ; v = -1)$$

- Solutions générales.

- Transformation de l'équation

Puisque le couple  $(2 ; -1)$  est une solution particulière de l'équation  $(E)$  on a :  $6 \times 2 + 11 \times (-1) = 1$ .  
Donc

$$\begin{cases} 6 \times u + 11 \times v = 1 \\ 6 \times 2 + 11 \times (-1) = 1 \end{cases} \xrightarrow{\text{par soustraction}} 6(u - 2) + 11(v + 1) = 0$$

Donc l'équation  $(E)$  devient :

$$(E) : 6(u - 2) = 11(-v - 1)$$

- Application du théorème de Gauss

#### Théorème 3 (Carl Friedrich Gauss, 1777-1855)

Soit  $a, b, c$  des entiers.

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$

**Remarque** : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorème (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».



$$(E) : 6(u - 2) = 11(-v - 1)$$

Puisque 6 et 11 sont premiers entre eux, alors en appliquant le théorème de Gauss, l'entier 6 divise  $(-v - 1)$  et 11 divise  $(u - 2)$ .

Il existe donc des entiers  $k$  et  $k'$  tels que :

$$\begin{cases} -v - 1 = 6k \\ u - 2 = 11k' \end{cases}$$

En reportant dans l'équation  $(E)$  on obtient

$$6 \times 11k' = 11 \times 6k \iff k = k'$$

Ainsi, les solutions de l'équation  $(E)$  sont les couples de la forme

$$\boxed{(2 + 11k ; -1 - 6k) ; k \in \mathbb{Z}}$$

↩ **Fin du cours** ↪