# PGCD
# Théorème de Bézout
# Théorème de Gauss

Christophe ROSSIGNOL*

Année scolaire 2018/2019

---

## Table des matières



## Liste des algorithmes



## Table des figures

---

**Activité :** Problème 1 page 40 [1] et problème 2 page 41 [2] [TransMath]

Dans tout ce chapitre, on n'utilisera que des nombres entiers naturels. Lorsque l'on parlera de diviseurs d'un entier naturel, il s'agira de ses diviseurs positifs.

# 1 PGCD, Nombres premiers entre eux

## 1.1 PGCD de deux nombres entiers naturels

**Définitions :** Soient $a$ et $b$ deux entiers naturels non nuls.

1. L'ensemble des diviseurs de $a$ est noté $\mathcal{D}(a)$.
2. L'ensemble des diviseurs communs à $a$ et $b$ est noté $\mathcal{D}(a\,;\,b)$.

**Exemple :** $\mathcal{D}(12) = \{1\,;\,2\,;\,3\,;\,4\,;\,6\,;\,12\}$ et $\mathcal{D}(63) = \{1\,;\,3\,;7\,;\,9\,;\,21\,;\,63\}$.
On a donc $\mathcal{D}(12\,;\,63) = \{1\,;\,3\}$.

**Remarques :**

1. De la définition découle directement que $\mathcal{D}(a\,;\,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.
2. L'ensemble $\mathcal{D}(a\,;\,b)$ est non vide (il contient toujours 1) et tous ces éléments sont plus petits que $a$ et $b$. Si l'on admet que toute partie de $\mathbb{N}$ non vide et majorée admet un plus grand élément, on peut en déduire la définition suivante :

**Définition :** Soient $a$ et $b$ deux entiers naturels non nuls.
Le plus grand diviseur commun de $a$ et $b$ est noté $\text{PGCD}(a\,;\,b)$. Il s'agit du plus grand élément de $\mathcal{D}(a\,;\,b)$.

**Exemple :** On a donc $\text{PGCD}(12\,;\,63) = 3$.

**Propriété 1 :** Soient $a$ et $b$ deux entiers naturels non nuls.
Si $b$ divise $a$ alors $\mathcal{D}(a\,;\,b) = \mathcal{D}(b)$.
On a donc $\text{PGCD}(a\,;\,b) = b$.

**Démonstration :**
Si $b$ est un diviseur de $a$, tout diviseur de $b$ est un diviseur de $a$. On a donc $\mathcal{D}(b) \subset \mathcal{D}(a)$.
Par suite $\mathcal{D}(a\,;\,b) = \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b)$.
Le PGCD de $a$ et de $b$ est donc le plus grand élément de $\mathcal{D}(b)$, c'est-à-dire le plus grand diviseur de $b$. C'est donc bien $b$.

**Propriété 2 :** Soient $a$ et $b$ deux entiers naturels non nuls.
Si la division euclidienne de $a$ par $b$ s'écrit $a = bq + r$ avec $0 < r < b$ alors $\mathcal{D}(a\,;\,b) = \mathcal{D}(b\,;\,r)$.
On a donc $\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r)$.

**Démonstration :**
Si $d$ divise $a$ et $b$ alors $d$ divise toute combinaison linéaire de $a$ et $b$. Donc $d$ divise $a - bq$, c'est-à-dire $d$ divise $r$.
$d$ est donc un diviseur commun de $b$ et $r$. On a donc $\mathcal{D}(a\,;\,b) \subset \mathcal{D}(b\,;\,r)$.
Si $d$ divise $b$ et $r$ alors $d$ divise toute combinaison linéaire de $b$ et $r$. Donc $d$ divise $bq + r$, c'est-à-dire $d$ divise $a$.
$d$ est donc un diviseur commun de $a$ et $b$. On a donc $\mathcal{D}(b\,;\,r) \subset \mathcal{D}(a\,;\,b)$.

1. Un rangement optimal.
2. Dimensions mystères.

## 1.2 Algorithme d'Euclide

L'algorithme d'Euclide consiste à effectuer les divisions euclidiennes successives des diviseurs et des restes en en suivant ces étapes :

$$\begin{array}{lll} (1) & a = bq_1 + r_1 & \text{avec } 0 \leq r_1 < b \\ (2) & b = r_1 q_2 + r_2 & \text{avec } 0 \leq r_2 < r_1 \\ (3) & r_1 = r_2 q_3 + r_3 & \text{avec } 0 \leq r_3 < r_2 \\ & \dots & \end{array}$$

La suite $(r_n)$ obtenu est une suite strictement décroissante d'entiers naturels. Il existe donc une étape $n$ où $r_n = 0$.
Or, d'après la propriété 2, on a :

$$\mathcal{D}(a\,;b) = \mathcal{D}(b\,;r_1) = \mathcal{D}(r_1\,;r_2) = \cdots = \mathcal{D}(r_{n-2}\,;r_{n-1})$$

De plus, comme $r_n = 0$, on a $r_{n-2} = r_{n-1}q_n + 0$ donc $r_{n-1}$ divise $r_{n-2}$. D'après la propriété 1, on alors $\mathcal{D}(r_{n-2}\,;r_{n-1}) = \mathcal{D}(r_{n-1})$.
On a donc $\mathcal{D}(a\,;b) = \mathcal{D}(r_{n-1})$. Le PGCD de $a$ et $b$ est donc $r_{n-1}$, c'est-à-dire le dernier reste non nul.
On trouvera dans l'algorithme 1 une écriture de l'algorithme d'EUCLIDE.

**Algorithme 1** Algorithme d'EUCLIDE

```
Variables
    a, b, r : nombres entiers naturels
Algorithme
    Saisir a, b
    r prend la valeur 1
    Tant que r≠0 faire :
        r prend la valeur du reste de la division euclidienne de a par b
        a prend la valeur b
        b prend la valeur r
    Fin Tantque
    Afficher a
```

**Exemple :** On veut déterminer le PGCD de 168 et 204.

$$\begin{array}{ll} (1) & 204 = 168 \times 1 + 36 \\ (2) & 168 = 36 \times 4 + 24 \\ (3) & 36 = 24 \times 1 + 12 \\ (4) & 24 = 2 \times 12 + 0 \end{array}$$

Donc PGCD $(168\,;204) = 12$.

**Conséquences :**

1. On déduit de l'algorithme d'EUCLIDE que $\mathcal{D}(a\,;b) = \mathcal{D}(\text{PGCD}(a\,;b))$.
   C'est-à-dire que l'ensemble des diviseurs communs de $a$ et $b$ est exactement l'ensemble des diviseurs de leur PGCD.
2. Autrement dit : tout diviseur de $a$ et de $b$ est un diviseur de PGCD $(a\,;b)$.
3. On peut remarquer qu'en multipliant toutes les lignes de l'algorithme d'EUCLIDE par un entier $k$, cela reste un algorithme d'EUCLIDE pour les nombres $ka$ et $kb$, dont le résultat sera $kr_{n-1}$. On peut donc en déduire que, si $k$ entier naturel non nul, PGCD $(ka\,;kb) = k \times$ PGCD $(a\,;b)$ .

**Exercices :** 4, 5 page 45 et 53, 56, 58 page 65 [3] – 3 page 45 et 57 page 65 [4] –1, 2 page 44 et 61, 63 page 65 [5] – 67 page 65 [6] – 59 page 65 [7] [TransMath]

### 1.3 Nombres premiers entre eux

**Définition :** Soient $a$ et $b$ deux entiers naturels non nuls.
On dit que $a$ et $b$ sont premiers entre eux si et seulement si leur PGCD est égal à 1.

**Remarque :** cela signifie qu'ils n'ont aucun diviseur commun différent de 1.

**Propriété :** Soient $a$ et $b$ deux entiers naturels non nuls.
$d$ est le PGCD de $a$ et $b$ si et seulement si il existe deux entiers naturels $a'$ et $b'$ premiers entre eux tels que $a = da'$ et $b = db'$.

**Démonstration :**
Si $d$ est le PGCD de $a$ et $b$ alors $d$ est un diviseur commun de $a$ et $b$. Donc on a $a = da'$ et $b = db'$.
Montrons que $a'$ et $b'$ sont premiers entre eux.
Soit $d'$ un diviseur de $a'$ et $b'$. On a donc $a' = d'a_1$ et $b' = d'b_1$. Par suite $a = dd'a_1$ et $b = dd'b_1$.
Donc $dd'$ est un diviseur commun de de $a$ et $b$.
Comme $d$ est le PGCD de $a$ et $b$, on a $d' = 1$. Donc $a'$ et $b'$ sont premiers entre eux.
Si $a = da'$ et $b = db'$ avec $a'$ et $b'$ premiers entre eux, alors

$$\text{PGCD}\,(a\,;\,b) = \text{PGCD}\,(da'\,;\,db') = d\text{PGCD}\,(a'\,;\,b') = d \times 1 = d$$

.

**Exercices :** 7, 9, 10 page 46 [8] – 12, 13, 14, 15 page 47 [9] [TransMath]

## 2 Théorème de Bézout - Applications

### 2.1 Le théorème de Bézout

**Théorème de Bézout :** Soient $a$ et $b$ deux entiers naturels non nuls.
$a$ et $b$ sont premiers entre eux si et seulement si il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = 1$.

**Remarque :** on admettra pour cette démonstration que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

**Démonstration :**
Si $au + bv = 1$ : si $d$ est un diviseur commun de $a$ et $b$, alors $d$ divise $au + bv = 1$.
donc $d = 1$ et $a$ et $b$ sont premiers entre eux.
Si $a$ et $b$ sont premiers entre eux : On note $\mathcal{E}$ l'ensemble des nombres entiers naturels non nuls pouvant s'écrire sous la forme $au + bv$, avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.
Comme $a \in \mathcal{E}$ (en prenant $u = 1$ et $v = 0$), $\mathcal{E}$ est une partie non vide de $\mathbb{N}$. Notons $m = au_1 + bv_1$ son plus petit élément.
La division euclidienne de $a$ par $m$ s'écrit $a = mq + r$ avec $0 \leq r < m$. On a donc :

$$\begin{aligned} r &= a - mq \\ &= a - q\,(au_1 + bv_1) \\ &= a - aqu_1 + bv_1 \\ &= a\,(1 - qu_1) + bv_1 \end{aligned}$$

3. Détermination du PGCD par l'algorithme d'Euclide
4. Restes connus.
5. Avec des congruences.
6. Disjonction des cas.
7. Un autre algorithme d'Euclide.
8. Caractérisation du PGCD.
9. Détermination de PGCD.

Donc, si $r \neq 0$, $r \in \mathcal{E}$. Ce qui est impossible car $m$ est le plus petit élément de $\mathcal{E}$ et $r < m$.
Par suite, $r = 0$ et donc $m$ divise $a$.
Par un raisonnement analogue, on obtient que $m$ divise $b$.
Comme on a supposé que $a$ et $b$ sont premiers entre eux, on a donc $m = 1$, c'est-à-dire $au_1 + bv_1 = 1$.

**Exercices :** 16, 18, 19, 20, 21 page 52 et 75 page 66 [10] [TransMath]

**Module :** Problème 3 page 48 [11] [TransMath]

## 2.2 Détermination pratique des coefficients de l'identité de Bézout

Il suffit d'utiliser l'algorithme d'Euclide pour déterminer les coefficients de Bézout.
Les nombres $a = 89$ et $b = 41$ sont premiers entre eux. En utilisant l'algorithme d'Euclide, on obtient :

(1) $89 = 41 \times 2 + 7$ donc $7 = 89 - 41 \times 2 = a - 2b$
(2) $41 = 7 \times 5 + 6$ donc $6 = 41 - 7 \times 5 = b - 5(a - 2b) = b - 5a + 10b = -5a + 11b$
(3) $7 = 6 \times 1 + 1$ donc $1 = 7 - 6 = a - 2b - (-5a + 11b) = a - 2b + 5a - 11b = 6a - 13b$

On a donc montré que $6a + (-3)b = 1$. Donc les coefficients $u = 6$ et $b = -3$ sont des coefficients de l'identité de Bézout.

**Exercices :** 71, 74 page 66 [12] [TransMath]

**Module :** Problème 4 page 49 [13] [TransMath]

## 2.3 Une nouvelle caractérisation du PGCD

**Propriété (admise) :** Soient $a$ et $b$ deux entiers naturels non nuls.
$d$ est le PGCD de $a$ et $b$ si et seulement si $d$ est un diviseur commun $a$ et $b$ et il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = d$.

**Exercices :** 22, 23 page 53 [14] [TransMath]

# 3 Théorème de Gauss – Applications

## 3.1 Le théorème de Gauss

**Théorème de Gauss :** Soient $a$, $b$ et $c$ trois entiers naturels non nuls.
Si $a$ divise le produit $bc$ et si $a$ est premier avec $b$ alors $a$ divise $c$.

**Démonstration :**
comme $a$ et $b$ sont premiers entre eux, il existe $u$, $v \in \mathbb{Z}$ tels que $au + bv = 1$.
On a donc $(ac)u + (bc)v = c$.
Or $a$ divise $ac$ et $bc$ donc $a$ divise $c$.

**Remarque :** Cela revient à dire que si un entier divise un produit de deux facteurs et est premier avec l'un des deux facteurs, alors il divise l'autre.

**Exercices :** 26, 27, 28, 29 page 57 [15] [TransMath]

10. Utilisation du théorème de Bézout.
11. Arithmétique et cryptographie.
12. Détermination des coefficients de Bézout.
13. Déterminer les coefficients de l'identité de Bézout.
14. Nouvelle caractérisation du PGCD.
15. Utilisation du théorème de Gauss.

## 3.2 Un corollaire important

**Théorème :** Soient $a$, $b$ et $n$ trois entiers naturels non nuls, avec $a$ et $b$ premiers entre eux.
Si $n$ est divisible par $a$ et $b$ alors $n$ est divisible par le produit $ab$.

**Démonstration :**
On a $n = aq$ et $n = bq'$ donc $aq = bq'$.
$b$ divise le produit $aq$ et $a$ et $b$ premiers entre eux, donc, d'après le théorème de GAUSS, $b$ divise $q$.
On a donc $q = bq''$ et $n = aq = abq''$ donc $ab$ divise $n$.

**Remarques :**

1. Ainsi, par exemple, pour montrer qu'un nombre et divisible par 6, il suffit de montrer qu'il est divisible par 2 et par 3.
2. Attention ! L'hypothèse « $a$ et $b$ premiers entre eux » est essentielle : 12 est divisible par 4 et par 6, mais n'est pas divisible par 24.

**Exercices :** 30, 31, 32, 34, 35 page 58 [16] et 83, 86 page 66[TransMath]

## 3.3 Résolution d'équations diophantiennes

Une équation diophantienne est une équation de la forme :

$$ax + by = c$$

où $a$, $b$ et $c$ sont des entiers relatifs et où les inconnues $x$ et $y$ sont aussi des entiers relatifs.

**Exemple :** On veut résoudre l'équation dans $\mathbb{Z}$ l'équation $5x - 3y = 7$

1. *On cherche une solution particulière de l'équation.*
   Ici, il y a une solution évidente, le couple $(2\,;\,1)$ car $5 \times 2 - 3 \times 1 = 7$.
2. *On cherche la solution générale de l'équation* en soustrayant termes à termes l'équation et l'égalité de la solution particulière.
   On a $\begin{cases} 5x - 3y = 7 \\ 5 \times 2 - 3 \times 1 = 7 \end{cases}$.
   En soustrayant les deux égalités, on obtient : $5(x-2) - 3(y-1) = 0$, c'est-à-dire $5(x-2) = 3(y-1)$.
3. *On trouve le forme des solution en utilisant le théorème de* GAUSS.
   3 divise $5(x-2)$, et comme 3 et 5 sont premiers entres eux, d'après le théorème de GAUSS, 3 divise $x-2$.
   On a donc $x - 2 = 3k$, avec $k \in \mathbb{Z}$, c'est-à-dire $x = 2 + 3k$, avec $k \in \mathbb{Z}$.
   En remplaçant dans l'égalité précédente, on obtient :

$$\begin{aligned} 3(y-1) &= 5(x-2) \\ 3(y-1) &= 5(2+5k-2) \\ 3(y-1) &= 15k \\ y-1 &= 5k \\ y &= 1+5k \end{aligned}$$

   Les solutions sont donc de la forme $\begin{cases} x = 2+3k \\ y = 1+5k \end{cases}$, avec $k \in \mathbb{Z}$.
4. *Réciproquement, on vérifie que ces solutions vérifient toujours l'équation.*
   Si $\begin{cases} x = 2+3k \\ y = 1+5k \end{cases}$, avec $k \in \mathbb{Z}$ alors :

$$\begin{aligned} 5x - 3y &= 5(2+3k) - 3(1+5k) \\ &= 10 + 15k - 3 - 15k = 7 \end{aligned}$$

16. Utilisation du corollaire du théorème de GAUSS.

**Remarque :** Dans certains cas, pour trouver une solution particulière, on peut être amené à déterminer des coefficients de BÉZOUT.

**Exercices :** 8 page 66 ; 96 page 67 ; 97, 98, 100 page 68 [17] –41 page 60 [18] [TransMath]

**Exercices de synthèse :** 110, 111, 112 page 71 ; 119, 120 page 72 et 121, 124 page 73 [19] [TransMath]

# Références

[TransMath] TransMATH Term S Spécialité, programme 2012 (NATHAN)

2, 4, 5, 6, 7

17. Équations diophantiennes.
18. Thèoréme des restes chinois.
19. Type BAC.