

# Arithmétique - PGCD, Théorème de Bézout et Théorème de Gauss

## I nombres premiers

### 1 Nombres premiers



#### Définition

Un entier naturel est premier si il admet deux et seulement deux diviseurs dans  $\mathbb{N}$  qui sont 1 et lui même. L'ensemble des entiers naturel est noté  $\mathbb{P}$ .



#### Exemples

- Les seuls diviseurs positifs de 37 sont 1 et 37, donc 37 est un nombre premier.
- 1 n'a qu'un seul diviseur positif, lui même. Ce n'est donc pas un nombre premier.



#### Propriété

1. Tout entiers naturel distinct de 1 possède au moins un diviseur premier.
2. Soit  $n$  un entier naturel supérieur ou égale à deux.  
Si  $n$  n'est pas un nombre premier, alors il admet un diviseur premier  $p$  tel que  $p \leq \sqrt{n}$ .
3. L'ensemble  $\mathbb{P}$  des nombres premiers est infini.



#### Démonstration

1. Soit  $n \in \mathbb{N}^* \setminus \{1\}$  et  $D$  l'ensemble des diviseurs de  $n$  strictement supérieur à 1.  
 $n$  divise  $n$ , donc  $D$  est une partie non vide de  $\mathbb{N}$ , et par conséquent, possède un plus petit élément  $d_0$ .  
Soit  $d$  un diviseur de  $d_0$  différent de 1, on a alors  $d$  qui divise aussi  $n$  et par conséquent  $d \in D$ , d'où  $d \geq d_0$ .  
or  $d|d_0$  donc  $d \leq d_0$   
d'où  $d = d_0$ .  
 $d_0$  admet donc seulement deux diviseurs distinct, 1 et lui même, c'est donc un nombre premier.  

Donc tout entiers naturel distinct de 1 possède au moins un diviseur premier.
2. On fait une démonstration par l'absurde.  
Soient  $n$  un entier naturel supérieur ou égale à deux qui n'est pas un nombre premier et tel que tous diviseurs premiers de  $p$  vérifient  $p > \sqrt{n}$ .  
Soit  $P_n$  l'ensemble des diviseurs premiers de  $n$ .

D'après la propriété précédente,  $P_n$  est une partie non vide de  $\mathbb{N}$ , elle admet donc un plus petit élément  $p_0$ .

On a donc  $p_0 > \sqrt{n}$  et il existe  $d \in \mathbb{N}^*$  tel que  $p_0 d = n$ .

$n$  n'étant pas premier,  $p_0 \neq n$  donc  $d \neq 1$

$d$  est donc un diviseur de  $n$  différent de 1, donc il admet au moins un diviseur premier  $p_1$  qui sera aussi un diviseur de  $n$ , et par conséquent tel que  $p_1 > \sqrt{n}$ .

$p_0 d \geq p_0 p_1 > \sqrt{n} \times \sqrt{n}$ , et par conséquent  $n > n$ , d'où la contradiction, Donc :

Si  $n$  n'est pas un nombre premier, alors il admet un diviseur premier  $p$  tel que  $p \leq \sqrt{n}$ .

3. Supposons que l'ensemble  $\mathbb{P}$  des nombres premiers est fini. Comme il est non vide et inclus dans  $\mathbb{N}$ , il admet un plus grand élément  $n$ .

Soit  $n_1$  l'entier défini par  $n_1 = n! + 1$ .

D'après la propriété 1,  $n_1$  admet au moins un diviseur premier, donc il existe  $d \in \mathbb{P}$  tel que  $d \leq n$  et  $d|n_1$ .

or  $d|n!$ , donc  $d|n_1 - n!$  et par conséquent  $d|1$ , ce qui est absurde car  $d$  est un nombre premier (donc différent de 1).

Donc  $\mathbb{P}$  est infini.

## 2 Décomposition des nombres en produit de facteurs premiers

### Théorème

Tout entier naturel  $n \geq 2$  peut se décomposer de manière unique sous la forme :

$$n = \prod_{i=1}^m p_i^{\alpha_i}$$

ou

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}$$

où  $p_1, p_2, \dots, p_m$  sont des nombres premiers tels que  $p_1 < p_2 < \dots < p_m$   
et  $\alpha_1, \alpha_2, \dots, \alpha_m$  sont des entiers naturels non nuls.

Cette décomposition est appelée **décomposition de  $n$  en produit de facteurs premiers**

### Démonstration

- Existence.

- \* **Initialisation**

$2 = 2 \times 1$  donc il existe une décomposition de 2 en produit de facteurs premiers.

- \* **Hérédité**

Soit  $n \in \mathbb{N}$  tel que  $n \geq 2$ .

Supposons que pour tout entier  $d \in \llbracket 2; n \rrbracket$  il existe une décomposition en produit de facteurs premiers et démontrons que pour tout entier  $d \in \llbracket 2; n+1 \rrbracket$  il existe une décomposition en produit de facteurs premiers.

— Si  $n+1$  est premier, alors  $(n+1)$  est une décomposition en produit de facteurs premier.

— Si  $n+1$  n'est pas premier, dans ce cas il existe  $(n_0$  et  $n_1)$  appartenant  $p \in \llbracket 2; n \rrbracket$   
et on a  $n+1 = n_0 \times n_1$

Par hypothèse de récurrence, pour  $n_0$  et  $n_1$ , il existe des décompositions en produit

de facteurs premiers, donc, par produit des décompositions,  $n + 1$  admet une décomposition en produit de facteurs premiers.

\* **Conclusion**

Pour tout entier naturel  $n \geq 2$  il existe une décomposition sous la forme :

$$n = \prod_{i=1}^m p_i^{\alpha_i}$$

où  $p_1, p_2, \dots, p_m$  sont des nombres premiers tels que  $p_1 < p_2 < \dots < p_m$

o Unicité


L'unicité sera démontré après avoir vu la section sur le PGCD

 **Exemple**

|  $720 = 2^4 \times 3^2 \times 5$

## II PGCD de deux entiers relatifs

### 1 PGCD

 **Définition**

Soit  $a \in \mathbb{Z}^*$  et  $b \in \mathbb{Z}$ .

L'ensemble des diviseurs communs à  $a$  et  $b$  est une partie non vide de  $\mathbb{Z}$  majorée par  $a$ . Elle possède donc un plus grand élément appelé Plus Grand Diviseur Commun noté  $PGCD(a; b)$ .

Deux entiers relatifs  $a$  et  $b$  sont dit premiers entre eux si  $PGCD(a; b) = 1$ .

 **Exemples**

L'ensemble des diviseurs strictement positifs de 36 est  $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

L'ensemble des diviseurs strictement positifs de 54 est  $D_{54} = \{1, 2, 3, 6, 9, 18, 27, 54\}$

Donc l'ensemble des diviseurs strictement positifs et communs de 36 et 54 est :

$$D_{36} \cap D_{54} = \{1, 2, 3, 6, 9, 18\}$$

Le plus grand élément de  $D_{36} \cap D_{54}$  est 18, donc  $PGCD(36, 54) = 18$

 **Remarque**

Les diviseurs de  $a$  et de  $-a$  étant les mêmes, on a  $PGCD(a; b) = PGCD(|a|; |b|)$ .

### 2 Algorithme d'Euclide

### ♥ Propriété

Soit  $a$  et  $b$  deux entiers relatifs non nuls.

L'ensemble  $D_{ab}$  des diviseurs communs à  $a$  et  $b$  est égale à l'ensemble  $D_{br}$  des diviseurs communs à  $b$  et au reste de la division euclidienne de  $a$  par  $b$ .

### 🔪 Démonstration

Soit  $q$  et  $r$  respectivement le quotient et le reste de la division euclidienne de  $a$  par  $b$ . On a donc :

$$a = bq + r \text{ avec } 0 \leq r < |b|.$$

- Démontrons que l'ensemble  $D_{ab}$  des diviseurs communs à  $a$  et  $b$  est inclus dans l'ensemble  $D_{br}$  des diviseurs communs à  $b$  et à  $r$ .

Soit  $d$  un diviseur commun à  $a$  et  $b$ .

$$\left. \begin{array}{l} d \text{ divise } a \\ d \text{ divise } b \end{array} \right\} \text{ donc } d|a - bq \text{ et par conséquent } d|r$$

Donc  $d$  est un un diviseur commun à  $b$  et  $r$ , et par conséquent  $D_{ab} \subset D_{br}$ .

- Réciproquement démontrons que l'ensemble  $D_{br}$  des diviseurs communs à  $b$  et  $r$  est inclus dans l'ensemble  $D_{ab}$  des diviseurs communs à  $a$  et à  $b$ .

soit  $d$  un diviseur commun à  $b$  et  $r$ .

$$\left. \begin{array}{l} d|b \\ d|r \end{array} \right\} \text{ donc } d|bq + r \text{ d'où } d|a$$

Donc  $d$  est un un diviseur commun à  $a$  et  $b$ , et par conséquent  $D_{br} \subset D_{ab}$ .

- On peut donc conclure que  $D_{ab} = D_{br}$

### 📌 Remarque

Exemple de la nécessité de la double inclusion pour montrer l'égalité.

Si  $d$  est un diviseur de 9, alors  $d$  divise 18. L'ensemble des diviseurs de 9 est par conséquent inclus dans celui des diviseurs de 18. La réciproque et par conséquent l'égalité des deux ensembles n'est cependant pas vraie.

### 📌 Remarque

Soient  $a$  et  $b$  deux entiers naturels non nuls et tel que  $a \geq b$ .

Soient  $q$  et  $r$  le quotient et le reste de la division euclidienne de  $a$  par  $b$  :

Si  $r = 0$ , alors  $PGCD(a; b) = b$ .

Sinon,  $PGCD(a; b) = PGCD(b; r)$

### ♥ Propriété Algorithme d'Euclide

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

- On effectue la division euclidienne de  $a$  par  $b$ . Il existe donc un unique couple  $(q_0, r_0)$  tel que :

$$a = bq_0 + r_0 \text{ et } 0 \leq r_0 < b. \text{ De plus } D_{ab} \subset D_{br_0}.$$

\* si  $r_0 = 0$ , alors  $PGCD(a; b) = b$

\* Sinon,  $PGCD(a; b) = PGCD(b; r_0)$

- On effectue la division euclidienne de  $b$  par  $r_0$ . Il existe donc un unique couple  $(q_1, r_1)$

tel que :

$$b = r_0 q_1 + r_1, 0 \leq r_1 < r_0 \text{ et } D_{br_0} \subset D_{r_0 r_1}.$$

\* si  $r_1 = 0$ , alors  $PGCD(b; r_0) = r_0$

\* Sinon,  $PGCD(b; r_0) = PGCD(r_0; r_1)$

- On effectue la division euclidienne de  $r_0$  par  $r_1$ . Il existe donc un unique couple  $(q_2, r_2)$  tel que :

$$r_0 = r_1 q_2 + r_2, 0 \leq r_2 < r_1 \text{ et } D_{r_0 r_1} \subset D_{r_1 r_2}.$$

\* si  $r_2 = 0$ , alors  $PGCD(r_0; r_1) = r_1$

\* Sinon,  $PGCD(r_0; r_1) = PGCD(r_1; r_2)$

- etc

L'Algorithme d'Euclide nous a permis de construire une suite  $\{b; r_0; r_1; r_2; \dots; r_n\}$  d'entiers naturels non nuls et strictement décroissante. Cette suite finie admet donc un plus petit élément en tant que partie non vide de  $\mathbb{N}$  et par conséquent, il existe un dernier reste non nul  $r_n$ .

On peut donc en déduire :

- $PGCD(a; b)$  est donc le dernier reste non nul obtenu à l'aide de l'algorithme d'euclide.
- $D_{ab} \subset D_{r_n}$ , où  $D_{r_n}$  est l'ensemble des diviseurs de  $r_n$ .

### Exemple

On cherche à déterminer le PGCD de 720 et 508.

En utilisant les divisions euclidiennes de l'algorithme d'Euclide, on obtient :

$$720 = 508 \times 1 + 212$$

$$508 = 212 \times 2 + 84$$

$$212 = 84 \times 2 + 44$$

$$84 = 44 \times 1 + 40$$

$$44 = 40 \times 1 + 4$$

$$40 = 4 \times 10 + 0$$

Le dernier reste **non nul** obtenu avec l'algorithme d'Euclide est 4, donc  $PGCD(720; 508) = 4$ .

### Propriété

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

Si  $d$  est un diviseur commun à  $a$  et  $b$ , alors  $d$  divise  $PGCD(a; b)$

### Démonstration

Cette propriété est déduite de l'algorithme d'Euclide, en effet si  $d$  est un diviseur commun à  $a$  et  $b$ , alors  $d \in D_{ab}$  et par conséquent  $d \in D_{r_n}$ , donc  $d|r_n$ , d'où la propriété.

### Propriété

Si  $a$  et  $b$  deux entiers relatifs non nuls, alors pour tout entier naturel non nul  $k$ , on a :

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

## Démonstration

Soient  $(k, a, n) \in (\mathbb{N}^*)^3$

Soit  $d$  le PGCD de  $a$  et  $b$  et  $d'$  le PGCD de  $ka$  et  $kb$ .

- On a donc  $d|a$  et  $d|b$ , d'où  $kd|ka$  et  $kd|kb$  et par conséquent, d'après la propriété précédente,  $kd|d'$ .
- D'autre part,  $k$  divise  $ka$  et  $kb$ , donc  $k$  divise  $d'$ .

Il existe donc  $p \in \mathbb{N}^*$  tel que  $d' = kp$ .

Or,  $d'$  étant un diviseur commun à  $ka$  et  $kb$ , on a l'existence de  $m \in \mathbb{N}^*$  et  $n \in \mathbb{N}^*$  tels que  $ka = kpn$  et  $kb = kpm$ , d'où  $a = pn$  et  $b = pm$  et par conséquent  $p$  est un diviseur commun à  $a$  et  $b$ , donc  $p|d$  d'après la propriété précédente, d'où  $kp|kd$  et par conséquent  $d'|kd$

- On a donc  $kd|d'$  et  $d'|kd$ ,  $\text{donc } d' = kd$ .

## Propriété

Soit  $a$  et  $b$  deux entiers relatifs non nuls

Si  $d = \text{PGCD}(a; b)$ , alors il existe deux réels  $a'$  et  $b'$  tels que :

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

## Démonstration

Soient  $a$  et  $b$  deux entiers relatifs non nuls et  $d$  le PGCD de  $a$  et  $b$ .

Il existe donc deux entiers naturels non nuls  $a'$  et  $b'$  tels que  $a = da'$  et  $b = db'$  et par conséquent :

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

## III Théorèmes de Bézout et de Gauss

### 1 Théorème de Bézout

#### Théorème de bézout :

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

$\text{PGCD}(a; b) = 1$  si et seulement si ils existent deux entiers relatifs  $u$  et  $v$  tels que  $au + bv = 1$ .

#### Remarque

A l'aide de l'algorithme d'Euclide, on peut montrer que 26 et 527 sont premiers entre eux. Le théorème de Bézout permet donc de justifier l'existence d'un couple d'entiers relatifs  $(u, v)$  tel que  $26u + 527v = 1$ .

Ce théorème ne permet pas de trouver une telle solution.

On verra dans un exemple comment utiliser l'algorithme d'Euclide pour déterminer une solution.

### Démonstration

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

- Supposons qu'il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = 1$ .

Soit  $d$  un diviseur commun à  $a$  et  $b$ .

Dans ce cas, alors  $d$  divise  $au + bv$  donc encore  $d$  divise 1.

Donc  $d = -1$  ou  $d = 1$  et par conséquent  $\text{pgcd}(a, b) = 1$ .

- Réciproquement, supposons que  $\text{pgcd}(a, b) = 1$ .

Soit  $N$  l'ensemble des entiers naturels non nuls  $p$  tel que  $au + bv = p$  où  $u$  et  $v$  sont deux entiers relatifs.  $N$  étant une partie non vide de  $\mathbb{N}$  elle admet un plus petit élément non nul  $p_0$ .

L'objectif est alors de démontrer que  $p_0$  est un diviseur commun à  $a$  et  $b$ .

Soit  $q$  et  $r$  respectivement le reste et le quotient de la division euclidienne de  $a$  par  $p_0$ .

On a donc  $a = qp_0 + r$  où  $0 \leq r < p_0$ .

or  $p_0 \in N$ , donc il existe  $(u_0, v_0) \in \mathbb{Z}^2$  tel que  $au_0 + bv_0 = p_0$ .

On obtient alors que  $a = q(au_0 + bv_0) + r$ , d'où  $a(1 - qu_0) + b(-qv_0) = r$ , avec  $0 \leq r < p_0$ .

$p_0$  étant le plus petit élément (**non nul**) de  $N$ , on a  $r = 0$  et par conséquent  $p_0|a$ .

De même, on montre que  $p_0|b$

On peut alors en déduire que  $p_0$  est un diviseur commun à  $a$  et  $b$  et par conséquent  $p_0|PGCD(a; b)$ , donc  $p_0|1$  d'où  $p_0 = 1$ .


il existe donc deux entiers relatifs  $u$  et  $v$  tels que  $au + bv = 1$ .

## 2 Théorème de Gauss

### Théorème de Gauss

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

Si  $PGCD(a; b) = 1$  et  $a|bc$  alors  $a|c$ .

 Autre formulation : Si  $PGCD(a; b) = 1$  et  $bc \equiv 0[a]$  alors  $c \equiv 0[a]$ .

### Remarque

Le théorème de Gauss est une implication.

La réciproque du théorème de Gauss est fausse comme le montre le contre exemple suivant :

$2|4$  et  $2|4 \times 6$  et pourtant  $\text{pgcd}(2, 6) \neq 1$

### Démonstration

Soient  $a, b$  et  $c$  trois entiers relatifs tels que  $\text{pgcd}(a; b) = 1$  et  $a|bc$ .

$\text{pgcd}(a; b) = 1$ , donc d'après le théorème de Bézout, il existe deux entiers relatifs  $u$  et  $v$  tels que  $au + bv = 1$ .

On a alors  $acu + bcv = c$

De plus  $a$  divise  $bc$ , donc il existe  $k \in \mathbb{Z}^*$  tel que  $bc = ak$ .

On a donc  $acu + akv = c$ , et par conséquent  $a|c$ .

Autre démonstration possible en utilisant le PGCD

## 3 Equation diophantienne



## Définition

On appelle équation diophantienne toute équation du type  $au + bv = c$  ou  $a, b, c, u$  et  $v$  sont des entiers relatifs.



## Exemple

Résoudre dans  $\mathbb{Z}$  l'équation suivante :

$$(E) : 12x + 41y = 1$$

### Solution

Tout d'abord, 2 et 3 étant les seuls diviseurs premiers de 12 et n'étant pas des diviseurs de 41, on a  $\text{pgcd}(12, 41) = 1$ , donc d'après le théorème de Bézout, il existe une solution à l'équation diophantienne  $12x + 41y = 1$ .

- Recherche d'une solution particulière.

On peut parfois rapidement déterminer mentalement une solution particulière de cette équation, néanmoins, si on ne trouve pas de solution particulière évidente, on peut utiliser l'algorithme d'Euclide comme dans l'exemple suivant :

A l'aide de l'algorithme d'Euclide, on obtient :

$$(1) : 41 = 12 \times 3 + 5$$

$$(2) : 12 = 5 \times 2 + 2$$

$$(3) : 5 = 2 \times 2 + 1$$

L'objectif est de "remonter le 1" dans les égalités. C'est à dire :

$$* (3) \text{ donne } 2 \times 2 = 5 - 1$$

En multipliant par 2 l'équation (2), on obtient  $12 \times 2 = 5 \times 4 + 2 \times 2$ .

En substituant  $2 \times 2$  par  $5 - 1$  on obtient  $12 \times 2 = 5 \times 4 + 5 - 1$ , d'où :

$$(2\text{bis}) : 12 \times 2 = 5 \times 5 - 1$$

$$* (2\text{bis}) \text{ donne } 5 \times 5 = 12 \times 2 + 1$$

En multipliant par 5 l'équation (1), on obtient  $41 \times 5 = 12 \times 15 + 5 \times 5$ .

d'où  $41 \times 5 = 12 \times 15 + 12 \times 2 + 1$  et par conséquent :

$$41 \times 5 = 12 \times 17 + 1.$$

$$* \text{ On a donc}$$

$$12 \times (-17) + 41 \times 5 = 1$$

Donc  $(-17, 5)$  est une solution de l'équation  $12x + 41y = 1$

## 4 Petit théorème de Fermat



### Théorème

Pour tout entier naturel  $a$  et tout nombre premier  $p$ , on a :

$$a^p \equiv a \pmod{p}$$

C'est à dire :  $p \mid a^p - a$



 **Démonstration**