

PGCD et Applications

Table des matières

1	Divisibilité	1
1.1	Une propriété fondamentale de $\mathbb{N}$	1
1.2	Divisibilité dans $\mathbb{Z}$	2
2	Division euclidienne	3
2.1	Division euclidienne dans $\mathbb{N}$	3
2.2	Division euclidienne dans $\mathbb{Z}$	4
3	Définition du PGCD	4
3.1	Définition	4
3.2	Algorithmes de détermination	5
3.3	Propriétés	6
4	Applications	7
4.1	Théorème de Bezout	7
4.2	Détermination des coefficients de Bezout	8
4.3	Théorème de Gauss et son corollaire.	8

1 Divisibilité

On rappelle que $\mathbb{N}$ est l'ensemble des entiers naturels : $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ et que $\mathbb{Z}$ est l'ensemble des entiers relatifs : $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$. Lorsqu'on ne précisera pas, « nombre entier » sous-entendra « Nombre entier relatif ».

1.1 Une propriété fondamentale de $\mathbb{N}$

Nous admettrons le théorème suivant, qui est équivalent au principe de récurrence :

Théorème 1 (Axiomes de $\mathbb{N}$).

- Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.
- Toute suite de $\mathbb{N}$ strictement décroissante est finie
- Si on range $n + 1$ objets dans n tiroirs, alors l'un des tiroirs au moins 2 objets.

Ce théorème, donné en tout début d'année, sera utilisé dans de nombreuses occasions en arithmétique.

1.2 Divisibilité dans $\mathbb{Z}$ **Définition 1.**

Soient a et b deux nombres entiers relatifs et $b \neq 0$.

a est un multiple de b (b est un diviseur de a) s'il existe un entier relatif k tel que $a = kb$

■ Exemple 1:

-6 est un diviseur de 18 car $\underbrace{18}_a = \underbrace{-6}_b \times \underbrace{(-3)}_k$

L'ensemble des diviseurs de 18 est : $\{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}$ et se note $\mathcal{D}_{18}$.

L'ensemble des multiples de 3 est infini et se note $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$.

Remarque 1.

- 0 est multiple de tout nombre entier n car $0 = n \times 0$
- Tout nombre entier n possède **au moins** quatre diviseurs : $-n$, n , -1 et 1 .
- Si n est un nombre entier. Les multiples de n sont les multiples de $-n$, donc en terme d'ensembles : $n\mathbb{Z} = -n\mathbb{Z}$.
On peut donc dire que l'ensemble des multiples de -3 se note $3\mathbb{Z}$.

► Exercice 1 Diviseurs d'un entier

1. Déterminer les couples $(x; y)$ d'entiers naturels tels que $x^2 = y^2 + 21$
2. Déterminer les entiers relatifs n tels que : $n^2 + n = 20$

Propriété 1 (Transitivité).

Soient a , b et c trois entiers relatifs.

Si a est un multiple de b et b est un multiple de c , alors a est un multiple de c .

Les multiples de 6 sont aussi des multiples de 2 et de 3 .

Propriété 2 (Combinaison linéaire).

Soient a , b , c trois entiers. Si c divise a et c divise b , alors c divise toute combinaison linéaire de a et b , autrement dit
quels que soient les entiers u et v , c divise $ua + bv$.

► Exercice 2 Utiliser la définition de la divisibilité

1. Démontrer que $(n-4)$ divise $n+17$ équivaut à $n-4$ divise 21 .

2. Déterminer alors toutes les valeurs de $n > 4$ telles que $\frac{n+17}{n-4}$ soit un entier.

► Exercice 3

Déterminer les entiers relatifs n tels que $n-4$ divise $3n-17$.

2 Division euclidienne

2.1 Division euclidienne dans $\mathbb{N}$

Théorème 2 (et définition).

Étant donnés deux nombres entiers naturels a et b ($b \neq 0$), il existe un couple unique $(q; r)$ tel que

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

Le nombre a est alors appelé *dividende*, b *diviseur*, q et r respectivement *quotient* et *reste* dans la *division euclidienne* de a par b .

Démonstration

Soient a et b deux entiers naturels. On note q la partie entière du quotient de a par b : $q = \left\lfloor \frac{a}{b} \right\rfloor$.

On a alors $q \leq \frac{a}{b} < q+1$ donc $qb \leq a < qb+b$. On a alors $0 \leq a - qb < b$.

On pose $r = a - qb$ donc on peut écrire

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

q et r sont définis de façon unique.

□

Remarque 2.

Attention : b est le *diviseur* de a dans la division euclidienne n'a pas le même sens que « b est un *diviseur* de a » ! En effet, b est un diviseur de a si et seulement si le reste est nul.

Remarque 3 (Obtention du reste par les logiciels).

- En Python, la fonction `%` renvoie le reste de la division euclidienne :

```
>>> 47%10
7
>>> 47%4
3
```

- Sur la calculatrice, il faut taper $a - \text{ent}(a/b) \times b$ pour obtenir le reste
- Sur le tableur, c'est la commande `MOD(a,b)` qu'il faut taper.

Propriété 3 (Nombre de restes possibles).

Dans la division euclidienne de a par b , il y a b restes possibles : $\{0, 1, 2, \dots, b-1\}$

2.2 Division euclidienne dans $\mathbb{Z}$ **Théorème 3** (Division euclidienne dans $\mathbb{Z}$ (admis)).

Étant donnés deux nombres entiers relatifs a et b , avec $b \neq 0$. Il existe un unique couple (q, r) avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

■ Exemple 2:

Déterminer le quotient et le reste de -23 divisé par -7 , de 23 divisé par -7 et de -23 divisé par 7 .

3 Définition du PGCD**3.1 Définition****Théorème 4** (Rappel - admis).

1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
2. Toute partie finie et non vide de $\mathbb{Z}$ admet un plus grand élément.

Propriété 4 (Et définition du PGCD).

Si a et b sont deux nombres entiers relatifs non tous les deux nuls. L'ensemble des diviseurs communs de a et de b , noté $\mathcal{D}(a; b) = \mathcal{D}(a) \cap \mathcal{D}(b)$ admet un plus grand élément d appelé *Plus Grand Commun Diviseur*. On notera $d = \text{pgcd}(a; b)$. On notera plus tard $d = a \wedge b$.

Démonstration

L'existence de ce plus grand élément est assuré par l'inclusion :

$$\mathcal{D}(a; b) \subset \llbracket \min(-|a|; -|b|); \max(|a|; |b|) \rrbracket$$

donc $\mathcal{D}(a; b)$ est finie et contient 1.

Ainsi, $\mathcal{D}(a; b)$ admet un plus grand élément $d(> 0)$.

□

Remarque 4 (Restriction à l'étude sur $\mathbb{N}$).

Comme $\text{pgcd}(|a|; |b|) = \text{pgcd}(a; b) > 0$, on traite en général le cas où a et b sont des entiers naturels.

■ Exemple 3:

$\text{pgcd}(54; 720) = 18$:

$\mathcal{D}(54)$ $\begin{matrix} \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{6} \\ 54 & 27 & 18 & 9 \end{matrix}$

On a aussi tous les opposés !

$\mathcal{D}(720)$ $\begin{matrix} \textcircled{1} & \textcircled{2} & \textcircled{3} & 4 & 5 & \textcircled{6} & 8 & \textcircled{9} & 10 & 12 & 15 & 16 & \textcircled{18} & 20 & 24 \\ 720 & 360 & 240 & 180 & 144 & 120 & 90 & 80 & 72 & 60 & 48 & 45 & 40 & 36 & 30 \end{matrix}$

Définition 2 (Entiers premiers entre eux).

Soient a et b deux entiers relatifs. a et b sont premiers entre eux si et seulement si $\text{pgcd}(a; b) = 1$.

Conséquence 1 (Caractérisations d'entiers premiers entre eux).

Soient $a, b \in \mathbb{N}$

$a \wedge b = 1 \iff a$ et b sont premiers entre eux $\iff \mathcal{D}(a; b) = \{-1; 1\} \iff \frac{a}{b}$ est irréductible.

► Exercice 4

Démontrer que pour tous $a, b \in \mathbb{N}$, $\text{pgcd}(a; b) = \text{pgcd}(4a + 3b; 5a + 4b)$.

Déterminer un pgcd par recherche des diviseurs peut s'avérer assez compliqué dès qu'on a affaire à de grands nombres. On a donc recours à des méthodes algorithmiques.

3.2 Algorithmes de détermination

Les algorithmes de détermination du PGCD sont basés sur les propriétés suivantes :

Propriété 5 (Conservation des ensembles des diviseurs).

1. $\mathcal{D}(a; b) = \mathcal{D}(a - b; b)$
2. Si r est le reste dans la division euclidienne de a par b , $\mathcal{D}(a; b) = \mathcal{D}(r; b)$.

Démonstration

1. *Démonstration par double-inclusion :*

- $\boxed{\subset}$: Supposons que d divise a et b , alors d divise toute combinaison linéaire entière donc $a - b$.

Ainsi, $\mathcal{D}(a; b) \subset \mathcal{D}(a - b; b)$

- $\boxed{\supset}$: Si e divise $a - b$ et b , alors e divise $a - b + b$ et b .

Ainsi, $\mathcal{D}(a - b; b) \subset \mathcal{D}(a; b)$

Ainsi, $\mathcal{D}(a; b) = \mathcal{D}(a - b; b)$.

2. En répétant l'opération, on a $\mathcal{D}(a; b) = \mathcal{D}(a - kb; b)$ pour tout $k \in \mathbb{Z}$.

On a $a = bq + r$ donc $r = a - bq$.

Ainsi, $\mathcal{D}(a; b) = \mathcal{D}(r; b)$, où $r = a - qb$.

□

L'algorithme dit "d'Euclide" applique la deuxième propriété pour déterminer le PGCD de deux entiers naturels.

Propriété 6 (Algorithme d'Euclide).

Tant que $r \neq 0$
 Calculer le reste r de la division euclidienne de a par b .
 remplacer a par b puis b par r .
 Le PGCD est a (le dernier reste non nul).

Démonstration

Algorithme d'Euclide et descente infinie

Lemme équivalent au th 1 : Une suite d'entiers naturels strictement décroissante est nécessairement finie.

Posons $a = r_0$ et $b = r_1$ les deux entiers. On pose maintenant la division euclidienne $r_0 = r_1 q_1 + r_2$ avec $0 \leq r_2 < r_1$. On a clairement $\text{pgcd}(r_0; r_1) = \text{pgcd}(r_1; r_2)$. On a alors deux possibilités :

- $r_2 = 0$ cela signifie que $\text{pgcd}(r_0; r_1) = r_1$ et c'est terminé.
- Sinon on pose $r_1 = r_2 q_2 + r_3$ avec $0 \leq r_3 < r_2$ la nouvelle div eucl.

Et on recommence (on continue par récurrence). (blague sur les polytechniciens)

On engendre ainsi une suite d'éléments $r_0, r_1, r_2, r_3, \dots$ d'entiers strictement décroissante.

Il existe donc un plus petit élément non nul r_n (tel que $r_{n+1} = 0$). On a donc $r_{n-1} = q_n r_n + 0$ et donc $\text{pgcd}(r_0; r_1) = \text{pgcd}(r_n; 0) = r_n$.

□

Écrire un programme sur la calculatrice permettant d'obtenir le pgcd de deux nombres.

► **Exercice 5** Applications de l'algorithme d'Euclide

Déterminer les PGCD des nombres suivants : (144; 840), (202; 138), (441; 777), (2004; 9185) et (4847; 5633)

3.3 Propriétés

Propriété 7 (Homogénéité).

Si $\lambda \neq 0$, alors $\text{pgcd}(\lambda a; \lambda b) = \lambda \text{pgcd}(a; b)$

■ **Exemple 4:**

$$\text{pgcd}(540; 360) = 10 \times \text{pgcd}(54; 36) = 90 \times \text{pgcd}(6; 4) = 180 \times \text{pgcd}(3; 2) = 180$$

On a par conséquent la propriété suivante dont nous nous servirons plus tard lorsque nous résoudrons des équations Diophantiennes.

Conséquence 2.

$$\text{pgcd}(a; b) = d \iff \text{pgcd}\left(\frac{a}{d}; \frac{b}{d}\right) = 1$$

4 Applications**4.1 Théorème de Bezout****Propriété 8 (Identité de Bezout).**

Si a et b sont deux entiers relatifs non tous les deux nuls et d leur PGCD, alors il existe un couple $(u; v)$ d'entiers relatifs tels que $d = au + bv$.

Démonstration

Soit $d = \text{pgcd}(a; b)$.

On considère $E = \{am + bn \cap \mathbb{N}^* \text{ avec } (m; n) \in \mathbb{Z} \times \mathbb{Z}\}$ l'ensemble des combinaisons linéaires strictement positives de a et b .

$E \subset \mathbb{N}$ et E n'est pas vide car il contient $|a|$ par exemple. D'après la propriété de $\mathbb{N}$ citée dans les prérequis, E admet un plus petit élément k (il existe donc deux entiers u et v tels que $k = au + bv$). Nous allons démontrer que $k = \text{pgcd}(a; b)$.

k est une combinaison linéaire de a et de b . Or, d est un diviseur commun de a et de b donc d divise k (donc $d \leq k$).

(Montrons que $k \in \mathcal{D}(a; b)$) Effectuons la division euclidienne de a par k : $a = kq + r$ avec $0 \leq r < k$.

On a alors $r = a - kq = a - (au + bv)q = (1 - qu)a + (-qv)b$ est donc une combinaison linéaire (positive ou nulle par hypothèse) de a et b . Si $r \neq 0$, alors cela contredit l'hypothèse de minimalité de k dans E . On en déduit donc que $r = 0$ et donc k divise a . On montrerait de même que k divise b . Donc k est un diviseur commun de a et de b . Donc k divise leur pgcd ($k \leq d$).

On a donc $k = d = \text{pgcd}(a; b)$.

□

Théorème 5 (Théorème de Bachet-Bezout).

a et b sont premiers entre eux si et seulement s'il existe un couple d'entiers $(u; v)$ appelés coefficients de Bezout tels que $au + bv = 1$

Démonstration



L'identité de Bezout assure que si $\text{pgcd}(a; b) = 1$ alors il existe u et v entiers tels que $1 = au + bv$.



Soient u et v deux entiers tels que $au + bv = 1$. Posons $d = \text{pgcd}(a; b)$ alors d divise toute combinaison linéaire de a et b . En particulier, d divise 1. Donc $d = 1$.

□

Remarque 5.

$\text{pgcd}(a; b) = 1 \iff a$ et b sont premiers entre eux $\iff \mathcal{D}(a; b) = \{-1; 1\} \iff \frac{a}{b}$ est irréductible $\iff \exists (u; v) \in \mathbb{Z}^2 \mid au + bv = 1$.

Propriété 9 (Structure de $\mathcal{D}(a, b)$).

Les diviseurs communs de a et b sont les diviseurs du PGCD.

Démonstration

Soit $d = \text{pgcd}(a; b)$, soit n un diviseur de a et b . D'après le théorème de Bezout, il existe deux entiers relatifs u et v tels que $d = au + bv$. Si n divise a et b , alors par combinaison linéaire, n divise d .

□

4.2 Détermination des coefficients de Bezout

■ Exemple 5:

On sait que $\text{pgcd}(75; 54) = 3$, on cherche u et v tels que $75u + 54v = 3$.

On va « remonter » l'algorithme d'Euclide :

$$\begin{array}{l|l}
 75 = 54 \times 1 + 21 & 3 = 54 \times 2 - 5 \times (75 - 54 \times 1) = 7 \times 54 - 5 \times 75 \\
 54 = 21 \times 2 + 12 & 3 = (54 - 21 \times 2) \times 2 - 21 \times 1 = -5 \times 21 + 54 \times 2 \\
 21 = 12 \times 1 + 9 & 3 = 12 - (21 - 12 \times 1) = 12 \times 2 - 21 \times 1 \\
 12 = 9 \times 1 + 3 & 3 = 12 - 9 \times 1 \\
 9 = 3 \times 3 + 0 &
 \end{array}$$

4.3 Théorème de Gauss et son corollaire.

Théorème 6 (Théorème de Gauss).

Si $\text{pgcd}(a; b) = 1$ et $a \mid bc$ alors $a \mid c$

Démonstration

Utilisons les hypothèses :

- $\text{pgcd}(a; b) = 1 \iff \exists(u; v) / au + bv = 1$
- $a \mid bc \iff \exists k / bc = ak$

Multiplions la première égalité par c :

$$auc + bcv = 1 \iff auv + akv = c \iff a \underbrace{(uv + kv)}_{\in \mathbb{Z}} = c$$

prouve que $a \mid c$.

□

Propriété 10 (Corollaire du théorème de Gauss).

$a, b, c \in \mathbb{N}$. Si $\text{pgcd}(a; b) = 1$ et a et b divisent c , alors ab divise c .

Démonstration

a divise c donc il existe k tel que $c = ka$;
 b divise c donc il existe k' tel que $c = k'b$. Donc a divise $k'b$.
 $\text{pgcd}(a; b) = 1$ donc a divise k' d'après Gauss. Donc il existe k'' tel que $k' = k''a$. Ainsi $c = k''ab$ ce qui signifie que ab divise c .

□

► Exercice 6 Équations Diophantiennes

Résoudre l'équation (E) à valeurs dans $\mathbb{Z}$: $17x - 33y = 1$ (méthode)

Application : Équation $15x + 8y = 5$ puis $29x - 13y = 6$