1.1 Le PGCD de deux entiers naturels

Par convention dans ce paragraphe, comme dans le reste du chapitre, lorsqu'on parlera de diviseurs d'un entier naturel, il s'agira toujours de **diviseurs positifs**.

Diviseurs communs à deux nombres

- Pour tout entier naturel a, on note $\mathcal{D}(a)$ l'ensemble de ses diviseurs. $\mathcal{D}(1) = \{1\}$; $\mathcal{D}(0) = \mathbb{N}$.

$\mathcal{D}(a)$ contient toujours 1 et a.

Lorsque $a \neq 0$, le plus grand élément de $\mathcal{D}(a)$ est a.

- Pour tous entiers naturels a et b non nuls, on note $\mathcal{D}(a\,;b)$ l'**ensemble des diviseurs communs** à a et b.

L'ensemble $\mathcal{D}(a\,;b)$ est non vide : il contient toujours 1. De plus, tous les nombres qu'il contient sont inférieurs ou égaux à a et b. Donc $\mathcal{D}(a\,;b)$ a un plus grand élément appelé le **PGCD de a et b**.

Toute partie non vide et majorée de $\mathbb{N}$ a un plus grand élément.

Exemple. $\mathcal{D}(6) = \{1\,;2\,;3\,;6\}$; $\mathcal{D}(15) = \{1\,;3\,;5\,;15\}$. Donc $\mathcal{D}(6\,;15) = \{1\,;3\}$ et PGCD$(6\,;15) = 3$.

Définition 1

a et b sont deux entiers naturels non nuls.
Le plus grand commun diviseur de a et b est noté

PGCD $(a\,;b)$.

On définit de la même manière le PGCD de deux entiers relatifs non nuls. $\Delta =$ PGCD $(|a|\,;|b|)$.

Conséquence. Si b divise a, alors PGCD $(a\,;b) = b$.

En effet tout diviseur de b est un diviseur de a donc $\mathcal{D}(b) \subset \mathcal{D}(a)$.

Comme b est le plus grand élément de $\mathcal{D}(b)$, alors b est le PGCD de a et b.

1.2 Recherche du PGCD : l'algorithme d'Euclide

a et b sont deux entiers naturels non nuls, $a > b$. Lorsque b ne divise pas a, pour déterminer le PGCD de a et b, on utilise l'algorithme d'Euclide.

Base de l'algorithme d'Euclide

Théorème 1

a et b sont deux entiers naturels non nuls tels que la division euclidienne de a par b se traduit par $a = bq + r$ avec $0 < r < b$.
Alors $\mathcal{D}(a\,;b) = \mathcal{D}(b\,;r)$ ce qui entraîne que PGCD$(a\,;b) =$ PGCD$(b\,;r)$.

Comme b ne divise pas a, $0 < r$.

Démonstration. • Démontrons que si d divise a et b, alors d divise b et r.

Si d divise a et b, d divise toute combinaison linéaire de a et b, donc en particulier $a - bq$, soit r.

Il en résulte que $\mathcal{D}(a\,;b) \subset \mathcal{D}(b\,;r)$.

• Démontrons que si δ divise b et r, alors δ divise a et b.

Si δ divise b et r, δ divise toute combinaison linéaire de b et r, donc en particulier $bq + r$, soit a.
Il en résulte que $\mathcal{D}(b\,;r) \subset$ D$(a\,;b)$.

La double inclusion équivaut donc à $\mathcal{D}(a\,;b) = \mathcal{D}(b\,;r)$.

• Ces deux ensembles étant identiques, ils ont le même plus grand élément donc :

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

Algorithme d'Euclide

Action	Division	Reste	Commentaire
On divise a par b.	$a = bq_0 + r_0$	$0 \leqslant r_0 < b$	$\mathcal{D}(a\,;b) = \mathcal{D}(b\,;r_0)$ d'où PGCD$(a\,;b)$ = PGCD$(b\,;r_0)$
Si $r_0 \neq 0$, on divise b par r_0.	$b = r_0q_1 + r_1$	$0 \leqslant r_1 < r_0$	$\mathcal{D}(b\,;r_0) = \mathcal{D}(r_0\,;r_1)$ d'où PGCD$(b\,;r_0)$ = PGCD$(r_0\,;r_1)$
Si $r_1 \neq 0$, on divise r_0 par r_1.	$r_0 = r_1q_2 + r_2$	$0 \leqslant r_2 < r_1$	$\mathcal{D}(r_0\,;r_1) = \mathcal{D}(r_1\,;r_2)$ d'où PGCD$(r_0\,;r_1)$ = PGCD$(r_1\,;r_2)$
Si $r_k \neq 0$, on divise r_{k-1} par r_k.	$r_{k-1} = r_kq_{k+1} + r_{k+1}$	$0 \leqslant r_{k+1} < r_k$	$\mathcal{D}(r_{k-1}\,;r_k) = \mathcal{D}(r_k\,;r_{k+1})$ d'où PGCD$(r_{k-1}\,;r_k)$ = PGCD$(r_k\,;r_{k+1})$

On définit ainsi une suite d'entiers r_n tels que $0 \leqslant \ldots < r_{k+1} < r_k < \ldots < r_2 < r_1 < r_0 < b$.

Cette suite est une suite strictement décroissante d'entiers naturels. Donc c'est une suite finie et il existe un entier n tel que $r_n \neq 0$ et $r_{n+1} = 0$. Or, $r_{n+1} = 0$ signifie que r_n divise r_{n-1}, d'où :

$$\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r_0) = \text{PGCD}(r_0\,;r_1) = \ldots = \text{PGCD}(r_{n-1}\,;r_n) = r_n.$$

Théorème 2

Lorsque b ne divise pas a, le PGCD de a et b est le dernier reste non nul dans l'algorithme d'Euclide.

Théorème 3

Conséquences de l'algorithme d'Euclide

a et b sont deux entiers naturels non nuls.

① L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de PGCD$(a\,;b)$.

② Quel que soit l'entier $c > 0$: **PGCD$(ac\,;bc) = c \times$ PGCD$(a\,;b)$.**

Démonstration

1. D'après l'algorithme d'Euclide : $\mathcal{D}(a\,;b) = \mathcal{D}(r_{n-1}\,;r_n) = \mathcal{D}(r_n)$ car r_n divise r_{n-1}. Et r_n = PGCD$(a\,;b)$.

2. Dans l'algorithme d'Euclide, il suffit de multiplier par c chaque membre des égalités (colonne 2) et des inégalités (colonne 3).

1.3 Nombres premiers entre eux

Définition 2

Dire que deux entiers naturels non nuls a et b sont premiers entre eux signifie que leur PGCD est égal à 1.

Théorème 4

Caractérisation du PGCD. a et b sont deux entiers naturels non nuls.

« Δ est le PGCD de a et b » équivaut à « Il existe deux entiers naturels a' et b' tels que $a = \Delta a'$, $b = \Delta b'$ et PGCD$(a'\,;b') = 1$ ».

RAISONNER
Démonstration par double implication.

Démonstration

- Supposons que Δ = PGCD$(a\,;b)$. Alors il existe deux entiers a' et b' tels que $a = \Delta a'$ et $b = \Delta b'$. Démontrons que PGCD$(a'\,;b') = 1$. Si d est un diviseur commun à a' et b', alors $a' = da_1$ et $b' = db_1$. Donc $a = \Delta da_1$ et $b = \Delta db_1$. Il en résulte que Δd divise a et b. Or, Δ est le plus grand des diviseurs communs, donc $d = 1$ soit PGCD$(a'\,;b') = 1$.
- Supposons qu'il existe deux entiers a' et b' tels que $a = \Delta a'$, $b = \Delta b'$ et PGCD$(a'\,;b') = 1$.

Démontrons que Δ est le PGCD de a et b.

D'après le théorème 3, PGCD$(\Delta a'\,;\Delta b') = \Delta \times$ PGCD$(a'\,;b') = \Delta$.

2.1 Le théorème de Bézout

Théorème 5

a et b sont deux entiers naturels non nuls. Dire « a et b sont premiers entre eux » équivaut à dire « Il existe deux entiers relatifs u et v tels que $\boldsymbol{au + bv = 1}$ ».

Démonstration

1. Supposons qu'il existe deux entiers u et v tels que $au + bv = 1$ et prouvons que a et b sont premiers entre eux. On note $\Delta = \text{PGCD}(a\,;b)$. Δ divise a et b donc Δ divise $au + bv$.
Comme $au + bv = 1$, $\Delta = 1$ et a et b sont premiers entre eux.

2. Supposons a et b premiers entre eux et démontrons que 1 « s'écrit » sous la forme $au + bv$.

Soit $\mathscr{E}$ l'ensemble des nombres de la forme $au + bv$, avec $u \in \mathbb{N}$ et $v \in \mathbb{N}$.

L'ensemble $\mathscr{E}$ n'est pas vide car pour $u = 1$ et $v = 0$, $a \in \mathscr{E}$. (Il en est de même pour b.)

Une partie non vide de $\mathbb{N}$ contient un plus petit élément.

Ainsi $\mathscr{E}$ contient des entiers strictement positifs et, parmi eux, un plus petit que tous les autres. Notons $m = au_1 + bv_1$ ce plus petit élément. La division euclidienne de a par m s'écrit $a = mq + r$ avec $0 \leqslant r < m$ soit $r = a - mq = a - (au_1 + bv_1)q = a(1 - u_1q) + b(-v_1q)$.

Ainsi $r \in \mathscr{E}$. Or m est le plus petit entier strictement positif de $\mathscr{E}$ donc $r = 0$. Ainsi m divise a.

On montre de même que m divise b.

Comme a et b sont premiers entre eux, $m = 1$ et $au_1 + bv_1 = 1$.

En pratique, comment trouver u et v ?

Pour déterminer les coefficients, on utilise l'algorithme d'Euclide. Donnons un exemple.

On cherche un couple $(x\,;y)$ d'entiers relatifs tels que $89x + 41y = 1$ (1).

89 et 41 sont premiers entre eux donc il existe deux entiers relatifs x et y vérifiant **(1)**.

On pose $a = 89$ et $b = 41$.

$89 = 41 \times 2 + 7$ donc $7 = 89 - 2 \times 41 = a - 2b$.

$41 = 7 \times 5 + 6$ donc $6 = 41 - 7 \times 5 = b - 5(a - 2b) = 11b - 5a$.

$7 = 6 \times 1 + 1$ donc $1 = 7 - 6 = a - 2b - 11b + 5a = 6a - 13b$.

On effectue les divisions euclidiennes et on exprime les restes au fur et à mesure.

Soit $89 \times 6 + 41 \times (-13) = 1$. Ainsi $(x_0\,;y_0) = (6\,;-13)$ est solution de **(1)**.

2.2 Une nouvelle caractérisation du PGCD

Théorème 6

a et b sont deux entiers naturels non nuls.

Dire que « Δ est le PGCD de a et b » équivaut à dire que « Δ est un diviseur de a et b et il existe deux entiers relatifs u et v tels que $\boldsymbol{\Delta = au + bv}$ ».

RAISONNER

Démonstration par double implication.

Démonstration. • Supposons que Δ est le PGCD de a et b. Alors, par définition, Δ est un diviseur de a et b. De plus, d'après le théorème 4, il existe deux entiers naturels a' et b' tels que $a = \Delta a'$ et $b = \Delta b'$ et $\text{PGCD}(a'\,;b') = 1$.

Donc, d'après le théorème 5, il existe deux entiers relatifs u et v tels que $a'u + b'v = 1$.

On en déduit que $\Delta a'u + \Delta b'v = \Delta$ soit $au + bv = \Delta$.

• Supposons que Δ divise a et b et qu'il existe des entiers relatifs u et v tels que $au + bv = \Delta$. Notons δ le PGCD de a et b. Δ divise a et b donc $\Delta \leqslant \delta$. Et, puisque δ divise a et b, δ divise $au + bv = \Delta$ d'où $\delta \leqslant \Delta$. Donc $\delta = \Delta$; Δ est le PGCD de a et b.

3.1 Énoncé du théorème de Gauss

Théorème 7 a, b, c sont des entiers strictement positifs tels que a divise le produit bc et a est **premier avec** b.
Alors a divise c.

Autrement dit Si un entier naturel divise un produit de deux facteurs et s'il est premier avec l'un d'eux, il divise l'autre.

Démonstration

Puisque a et b sont premiers entre eux, d'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $au + bv = 1$. Donc $(ac)u + (bc)v = c$. Or a divise ac et bc donc a divise $acu + bcv$. Il en résulte que a divise c.

3.2 Corollaire du théorème de Gauss

Si un entier naturel n est divisible par deux entiers naturels a et b **premiers entre eux**, il est divisible par leur produit.

Démonstration

Par hypothèse, $n = aq$ et $n = bq'$ avec q et q' deux entiers naturels. Donc $aq = bq'$.

Puisque b divise aq et que b est premier avec a, il divise q (théorème 7). Donc $q = bp$ et $n = abp$.

On conclut que le produit ab divise n.

Généralisation

Si n est divisible par plusieurs entiers **premiers entre eux deux à deux**, n est divisible par leur produit.

Exemple

Si un nombre est divisible par 3, 7 et 11, alors il est divisible par 231 car 3, 7 et 11 sont des entiers premiers entre eux deux à deux.

Application

Pour prouver, par exemple, qu'un nombre est divisible par 6, il **suffit** de prouver qu'il est divisible par 2 et 3 car 2 et 3 sont premiers entre eux.

Ainsi, pour tout entier naturel $n > 1$, $(n - 1)\,n(n + 1)$ est divisible par 6.

En effet, $n(n + 1)$ est le produit de deux entiers consécutifs : il est donc divisible par 2.

Et $(n - 1)\,n(n + 1)$ est le produit de trois entiers consécutifs : il est donc divisible par 3.

Il en résulte que $(n - 1)\,n(n + 1)$ est divisible par 6.

Attention

L'hypothèse « a et b premiers entre eux » est une **hypothèse essentielle**.

Si on démontre qu'un nombre est divisible par 4 et 6, on peut seulement conclure qu'il est divisible par 12, et non pas par 24. Ainsi 36 est divisible par 4 et 6, mais n'est pas divisible par 24.

Source : Transmath Term S spécialité, éd. Nathan (programme 2012)