PGCD de deux entiers naturels

Terminale S spécialité - Lycée Saint-Charles

Patrice Jacquet - www.mathxy.fr - 2015-2016

1 Diviseurs communs à deux entiers naturels

Propriété 1

Soit a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs à a et à b admet un plus grand élément.

Preuve. L'ensemble des diviseurs commun à a et à b est non vide (il contient au moins 1) et fini (c'est l'intersection de deux ensembles finis) : il admet donc un plus grand élément.

Définition 1 – PGCD

Soit a et b deux entiers naturels non nuls.
Le plus grand diviseur commun à a et à b est noté $\text{PGCD}(a;b)$.

Exemple. Détermination de $\text{PGCD}(6;15)$
L'ensemble des diviseurs de 6 est : $\{1;2;3;6\}$
L'ensemble des diviseurs de 15 est : $\{1;3;5;15\}$
donc $\text{PGCD}(6;15) = 3$

Remarque. Si b divise a alors $\text{PGCD}(a;b) = b$.
exemple : $\text{PGCD}(10;5) = 5$.

2 Recherche du PGCD : l'algorithme d'Euclide

Propriété 2

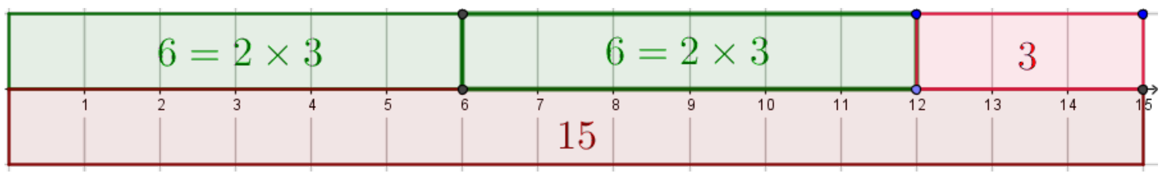
Soit a et b deux entiers naturels non nuls tels que la division euclidienne de a par b donne :
$a = bq + r$ avec $0 < r < b$.
Alors l'ensemble des diviseurs commun à a et à b est égal à l'ensemble des diviseurs communs à b et à r.

Preuve. Si d divise a et b alors d divise $a - bq$, soit r. Donc d divise r.
Si d divise b et r alors d divise $bq + r$, soit a. Donc d divise a.

Propriété 3 – (*se déduit immédiatement de la propriété précédente*)

Soit a et b deux entiers naturels non nuls tels que la division euclidienne de a par b donne :
$a = bq + r$ avec $0 < r < b$.
Alors PGCD$(a; b)$ =PGCD$(b; r)$.

Exemple. PGCD$(15; 6)$
$15 = 6 \times 2 + 3$
PGCD$(15; 6)$ =PGCD$(6; 3) = 3$



Propriété 4 – Recherche du PGCD par l'algorithme d'Euclide

Soit a et b deux entiers naturels non nuls tels que b ne divise pas a.

On fait la suite des divisions euclidiennes :

a par b	$a = bq_0 + r_0$	$0 \leqslant r_0 < b$	PGCD$(a; b)$ =PGCD$(b; r_0)$
b par r_0 (si $r_0 \neq 0$)	$b = r_0 q_1 + r_1$	$0 \leqslant r_1 < r_0$	PGCD$(b; r_0)$ =PGCD$(r_0; r_1)$
r_0 par r_1 (si $r_1 \neq 0$)	$r_0 = r_1 q_2 + r_2$	$0 \leqslant r_2 < r_1$	PGCD$(r_0; r_1)$ =PGCD$(r_1; r_2)$
...	...	...	...
r_{i-1} par r_i ($r_i \neq 0$)	$r_i = r_{i-1} q_{i+1} + r_{i+1}$	$0 \leqslant r_{i+1} < r_i$	PGCD$(r_{i-1}; r_i)$ =PGCD$(r_i; r_{i+1})$
...	...	...	...

On s'arrête quand le reste r_i est nul.

Le **dernier reste non nul** dans l'algorithme d'Euclide est le PGCD de a et b.

Exemple. PGCD$(450; 147)$
$450 = 147 \times 3 + 9$
$147 = 9 \times 16 + \mathbf{3}$
$9 = 3 \times 3 + 0$
3 est le dernier reste non nul dans l'algorithme d'Euclide donc PGCD$(450; 147) = 3$.

Propriété 5

Soit a, b et c trois entiers naturels non nuls. PGCD$(ac; bc) = c\times$PGCD$(a; b)$.

Preuve. Dans l'algorithme d'Euclide on multiplie par c chaque membre des égalités (division) et des inégalités (reste).

2.1 Nombres premiers entre eux

Définition 2

On dit que deux entiers naturels a et b sont premiers entre eux lorsque leur PGCD est égal à 1.

Propriété 6 – caractérisation du PGCD

Soit a et b deux entiers naturels non nuls. Dire que d est le PGCD de a et de b *équivaut à dire* que $a = da'$ et $b = db'$ avec $\text{PGCD}(a';b') = 1$.

Preuve. *Sens direct* :
Supposons que $\text{PGCD}(a;b) = d$, on peut donc écrire $a = da'$ et $b = db'$.
Or, d'après la propriété 5, $\text{PGCD}(da';db') = d\times\text{PGCD}(a';b')$.
On a donc $d = d\times\text{PGCD}(a';b')$, ce qui prouve que $\text{PGCD}(a';b') = 1$.

Réciproquement :
si $a = da'$ et $b = db'$ et si $\text{PGCD}(a';b') = 1$, alors :
$\text{PGCD}(a;b) = \text{PGCD}(da';db') = d\times\text{PGCD}(a';b') = d$.