Propriété - Définition (voir démonstration 01)

Soient a et b deux entiers naturels non nuls.
Un entier naturel qui divise a et qui divise b est appelé diviseur commun à a et b.
L'ensemble des diviseurs communs à a et à b possède un plus grand élément que l'on appelle le plus grand commun diviseur de a et b, on le note PGCD(a ; b).

Démonstration 01 (retour au cours)

a et b sont deux entiers naturels non nuls.
Considérons l'ensemble D(a ; b), ensemble des diviseurs communs à a et b.
Le nombre 1 est un diviseur commun à a et b.
D(a ; b) est donc une partie non vide de $\mathbb{N}$.
De plus on sait que tout diviseur commun à a et b sera inférieur ou égal à a et à b.
Donc D(a ; b) est une partie finie de $\mathbb{N}$.
D(a ; b) a donc un plus grand élément que l'on peut obtenir en rangeant dans l'ordre croissant (ou décroissant) les éléments de D(a ; b).
C'est ce plus grand élément de D(a ; b) qui est noté PGCD(a ; b)

Propriétés (voir démonstration 02)

Soient a et b deux entiers naturels non nuls.
On a PGCD(a ; b) $\leq$ a ; PGCD(a ; b) $\leq$ b ; PGCD(a ; b) = PGCD(b ; a)
Si b divise a, on a PGCD(a ; b) = b , en particulier PGCD(a ; 1) = 1 et PGCD(a ; a) = a

Démonstration 02 (retour au cours)

a étant un entier naturel, on sait que tous les diviseurs de a sont inférieurs ou égaux à a.
PGCD(a ; b) est un diviseur de a, donc PGCD(a ; b) $\leq$ a

b étant un entier naturel, on sait que tous les diviseurs de b sont inférieurs ou égaux à b.
PGCD(a ; b) est un diviseur de b, donc PGCD(a ; b) $\leq$ b

Il est immédiat que les diviseurs communs à a et b, sont aussi les diviseurs communs à b et a.
Donc PGCD(a ; b) = PGCD(b ; a)

Si b divise a, alors b est un diviseur de a
Mais b est aussi un diviseur de b
Donc b est un diviseur commun à a et b ,
PGCD(a ; b) étant le plus grand des diviseurs communs à a et b, on a donc PGCD(a ; b) $\geq$ b
Or on a vu précédemment que PGCD(a ; b) $\leq$ b
On en déduit : PGCD(a ; b) = b
En prenant b = 1, et comme 1 divise a, on a PGCD(a ; 1) = 1 (résultat qui est par ailleurs évident)
En prenant b = a, et comme a divise a, on a PGCD(a ; a) = a (résultat qui est par ailleurs évident)

Propriété (voir démonstration 03)

Soient a et b deux entiers naturels non nuls.
Soient q et r le quotient et le reste de la division euclidienne de a par b. (On a a = b x q + r)
Alors Si r = 0, PGCD(a ; b) = b
Si r $\neq$ 0, PGCD(a ; b) = PGCD(b ; r)

Démonstration 03 (retour au cours)

a et b sont deux entiers naturels non nuls.
q et r sont le quotient et le reste de la division euclidienne de a par b.
On a $a = b \times q + r$ avec $q \in \mathbb{N}$, $r \in \mathbb{N}$ et $0 \leq r < b$

- Si $r = 0$, alors $a = b \times q$ avec $q \in \mathbb{N}$, donc b divise a et par conséquent $PGCD(a ; b) = b$
- Si $r \neq 0$,

Considérons d un diviseur commun à a et b.
On peut écrire $r = a - b \times q$
Comme d divise a et b, on en déduit que d divise r
Donc d est un diviseur commun à b et r. On a donc $D(a ; b) \subset D(b ; r)$

Considérons d un diviseur commun à b et r.
On sait que $a = b \times q + r$
Comme d divise b et r, on en déduit que d divise a
Donc d est un diviseur commun à a et b. On a donc $D(b ; r) \subset D(a ; b)$

On a donc démontré que $D(a ; b) = D(b ; r)$
Le plus grand élément de D(a ; b) est donc aussi le plus grand élément de D(b ; r)
c'est-à-dire $PGCD(a ; b) = PGCD(b ; r)$

Propriété - Algorithme d'Euclide (voir démonstration 04)

Soient a et b deux entiers naturels non nuls.
On définit la suite r_n d'entiers naturels de la façon suivante :

$r_0 = b$; r_1 est le reste de la division euclidienne de a par b

Pour $n \geq 1$: si $r_n = 0$ alors $r_{n+1} = 0$

si $r_n \neq 0$ alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n

Alors il existe un entier n_0 tel que $r_{n_0} \neq 0$ et pour tout $n > n_0$, $r_n = 0$

On a $PGCD(a ; b) = r_{n_0}$

Remarque

En effectuant ainsi des divisions euclidiennes successives: de a par b, puis du diviseur par le reste, ... le premier reste non nul est le PGCD de a et de b. C'est l'algorithme d'Euclide
Suivant les nombres a et b, le nombre d'itérations à effectuer peut être plus ou moins grand.
Sachant que PGCD(a ; b) = PGCD(b ; a) on aura toujours intérêt à prendre $b \leq a$

Démonstration 04 (retour au cours)

a et b sont deux entiers naturels non nuls.

La suite r_n d'entiers naturels est définie par :

$r_0 = b$; r_1 est le reste de la division euclidienne de a par b

Pour $n \geq 1$: si $r_n = 0$ alors $r_{n+1} = 0$

si $r_n \neq 0$ alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n

Supposons que pour tout entier n, on a $r_n \neq 0$
Alors pour tout entier n, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n
D'après l'encadrement du reste dans une division euclidienne on a $r_{n+1} < r_n$
On a alors $r_1 < r_0$ donc $r_1 < b$ donc $r_1 \leq b - 1$
$r_2 < r_1$ donc $r_2 \leq r_1 - 1$ donc $r_2 \leq b - 2$
On pourrait alors démontrer par récurrence que pour tout n $r_n \leq b - n$
On aurait alors $r_{b+1} \leq b - (b + 1)$ c'est-à-dire $r_{b+1} \leq -1$ ce qui est absurde puisque $r_{b+1} \in \mathbb{N}$
En supposant que $r_n \neq 0$ pour tout entier n, on aboutit à une contradiction.

Il existe donc un entier n tel que $r_n = 0$
Considérons l'ensemble E des entiers n tels que $r_n = 0$
Cet ensemble est une partie non vide de $\mathbb{N}$. Elle a donc un plus petit élément n_1 .
On a donc $r_{n_1} = 0$ et d'après la définition de la suite (r_n) il est immédiat que $r_n = 0$ pour tout $n \geq n_1$

Posons $n_0 = n_1 - 1$

Puisque n_1 est le plus petit élément de E, $n_0 \notin E$ donc $r_{n_0} \neq 0$
De plus si $n > n_0$ on a $n \geq n_1$ et par conséquent $r_n = 0$ donc $r_n = 0$ pour tout n tel que $n > n_0$

On a vu que lorsque r est le reste non nul de la division euclidienne de a par b, on a
PGCD(a ; b) = PGCD(b ; r)

En utilisant cette propriété avec les éléments de la suite (r_n) pour $n \leq n_0$ on peut écrire :

$PGCD(a ; b) = PGCD(a ; r_0) = PGCD(r_0 ; r_1) = PGCD(r_1 ; r_2) = ... = PGCD(r_{n_0-1} ; r_{n_0})$

Comme de plus $r_{n_0+1} = r_{n_1} = 0$, cela signifie que r_{n_0-1} est divisible par r_{n_0} et donc $PGCD(r_{n_0-1} ; r_{n_0}) = r_{n_0}$

On a alors obtenu $PGCD(a ; b) = r_{n_0}$

Propriété (voir démonstration 05)

Soient a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

Démonstration 05 (retour au cours)

a et b sont deux entiers naturels non nuls.

Notons D = PGCD(a ; b)

Soit d un diviseur de D. d divise D et D divise a, donc d divise a
d divise D et D divise b, donc d divise b.
Donc d est un diviseur commun à a et b.
Tout diviseur du PGCD est un diviseur commun à a et b.

Soit d un diviseur commun à a et b. (on peut supposer que $b \leq a$)

- Si b divise a, alors PGCD(a ; b) = b, donc D = b, donc d divise D
- Si b ne divise pas a.
  Écrivons la division euclidienne de a par b, $a = b \times q + r$ avec $0 < r < b$
  On a D = PGCD(a ; b) = PGCD(b ; r)
  Si r divise b, alors D = PGCD(b ; r) = r,
  D'autre part puisque d divise a et b, alors d divise $r = a - b \times q$, donc d divise D
  Si r ne divise pas b, on peut alors recommencer l'opération.
  Or, d'après l'algorithme d'Euclide, on obtiendra $D = PGCD(r_{n-1} ; r_n)$
  avec r_n le dernier reste non nul, c'est-à-dire avec r_n diviseur de r_{n-1} . Donc $D = r_n$
  A chaque étape on pourra écrire que d divise r_i et par conséquent d divise r_n =

On aura donc démontré que d divise D.
Tout diviseur commun à a et b est donc un diviseur de leur PGCD.

L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur PGCD.