PGCD de deux entiers naturels

I. Le plus grand commun diviseur (PGCD)

1.Le PGCD de deux entiers naturels

Par convention, lorsqu'on parlera de diviseurs d'un entier naturel, il s'agira toujours de diviseurs positifs.

Diviseurs communs à deux nombres :

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

$D(a)$ contient toujours 1 et a.

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

$\star$ Pour tous entiers naturels a et b non nuls, on note $D(a,b)$ l'ensemble des diviseurs communs à a et b.

L'ensemble $D(a,b)$ est non vide : il contient toujours 1.

De plus, tous les nombres qu'il contient sont inférieurs ou égaux à a et b.

Donc $D(a,b)$ a un plus grand élément appelé le *plus grand commun diviseur* et noté le PGCD de a et b.

EXEMPLE :

$D(6) = \{\ 1, 2, 3, 6\ \}$

Définition 1 :

a et b sont deux entiers naturels.Le Plus Grand Commun Diviseur à a et b est noté $PGCD(a,b)$.

Conséquences :

Si b divise a alors pgcd(a,b)=b.En effet, tout diviseur de b est un diviseur de a donc $D(b) c D(a)$.

Comme b est le plus grand élément de $D(b)$, alors b est le $PGCD(a,b)$.

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 $PGCD(a,b)$, on utilise l'algorithme d'Euclide.

Base de l'algorithme d'Euclide :

Théorème 1 :

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

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 (r_n) telle que $0 \leq \; ... < r_{k+1} < r_k < ... r_2 < r_1 < r_0 < b$.

Cette suite est une suite décroissante et strictement positive 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 :

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

Théorème 2 :

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

Théorème 3 :

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, $PGCD(ac,bc)=c\times\ PGCD(a,b)$.

3.Nombres premiers entre eux.

Définition 2 :

Dire que deux entiers naturels 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 $PGCD(a,b)$ équivaut à il existe deux entiers naturels a' et b' tels que :$a=\Delta\,a'$, $b=\Delta\,b'$ et $PGCD(a',b')=1$.