PGCD – NOMBRES PREMIERS ENTRE EUX

1) PLUS GRAND COMMUN DIVISEUR : PGCD

A) DEFINITION - PROPRIETES

Exemple :

Pour simplifier la fraction $\frac{159390}{49005}$ on peut diviser successivement le numérateur et le dénominateur par 5, puis par 9 puis par 11 .

$$\frac{159390}{49005} = \frac{31878}{9801} = \frac{3542}{1089} = \frac{322}{99}$$

La fraction $\frac{322}{99}$ alors obtenue ne peut plus être simplifiée . Pour passer de $\frac{159390}{49005}$ à $\frac{322}{99}$ on a simplifié par $5 \times 9 \times 11 = 495$

495 correspond au plus grand diviseur qui soit commun aux deux nombres 159390 et 49005

Propriété - Définition

Soit 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).

Preuve :

Soit 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)

Exemples :

- Dans $\mathbb{N}$ l'ensemble des diviseurs de 15 est {1 ; 3 ; 5 ; 15} et l'ensemble des diviseurs de 12 est {1 ; 2 ; 3 ; 4 ; 6 ; 12}

L'ensemble des diviseurs communs à 12 et à 15 est donc D(12 ; 15) = {1 ; 3} . On a alors PGCD(15 ; 12) = 3

- En écrivant l'ensemble des diviseurs de 159390 et l'ensemble des diviseurs de 49005, on peut obtenir PGCD(159390 ; 49005) = 495 ... mais c'est laborieux !

Remarque :

a étant un entier naturel, l'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$.
On pourra étendre, si besoin est, la notion de PGCD à des nombres entiers relatifs.
On dira par exemple que PGCD(-15 ; 12) = PGCD(15 ; 12) = 3

Propriétés

Soit a et b deux entiers naturels non nuls.

- PGCD(a ; b) ≤ a
- PGCD(a ; b) ≤ b
- PGCD(a ; b) = PGCD(b ; a)
- Si b divise a, on a PGCD(a ; b) = b
- PGCD (a ; 1) = 1
- PGCD (a ; a) = a

Preuve :

- 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) ≤ a
- On montre de même que PGCD(a ; b) ≤ 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 ; i)
- 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) ≥ b .
  Or on a vu précédemment que PGCD(a ; b) ≤ 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)

Exemple :

6 est un diviseur de 18 donc PGCD(6 ; 18) = 6

B) ALGORITHME D'EUCLIDE

Propriété – Lemme d'Euclide

Soit a et b deux entiers naturels non nuls.
Soit q et r le quotient et le reste de la division euclidienne de a par b.

- Si $r = 0$, PGCD(a ; b) = b
- Si $r \neq 0$, PGCD(a ; b) = PGCD(b ; r)

Preuve :

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 alors $a = b \times q + r$ 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 $PGCD(a ; b) = PGCD(b ; r)$

Exemple :

Pour trouver le PGCD de 2414 et 804, on peut écrire la division euclidienne de 2414 par 804 : $2414 = 804 \times 3 + 2$
On en déduit alors $PGCD(2414 ; 804) = PGCD(804 ; 2)$
Il est immédiat que $PGCD(804 ; 2) = 2$ (car 2 divise 804) . On en déduit donc $PGCD(2414 ; 804) = 2$

Propriété – algorithme d'Euclide

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

Preuve :

Soit a et b deux entiers naturels non nuls.
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 : $r_1 < r_0 \Rightarrow r_1 < b \Rightarrow r_1 \leq b - 1$
$r_2 < r_1 \Rightarrow r_2 \leq r_1 - 1 \Rightarrow r_2 \leq b - 2$
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 $r_{b+1} \in \mathbb{N}$

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 $r_n = 0$. On en déduit que $r_n = 0$ 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 $PGCD(a ; b) = r_{n_0}$

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 $b \leq a$

Exemples :

Pour déterminer le PGCD de 410258 et de 126 écrivons les divisions euclidiennes successives :
$410258 = 126 \times 3256 + 2$
$126 = 2 \times 63 + 0$

Donc $PGCD(410258 ; 126) = 2$

Pour déterminer le PGCD de 15648 et de 657 écrivons les divisions euclidiennes successives :
$15648 = 657 \times 23 + 537$
$657 = 537 \times 1 + 120$
$537 = 120 \times 4 + 57$
$120 = 57 \times 2 + 6$
$57 = 6 \times 9 + 3$
$6 = 3 \times 2 + 0$

Donc $PGCD(15648 ; 657) = 3$

C) CONSEQUENCES DE L'ALGORITHME D'EUCLIDE

Propriété

Soit 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.

Preuve :

a et b sont deux entiers naturels non nuls . On note 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.
  On en déduit que 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.

  On en déduit que tout diviseur commun à a et b est un diviseur de leur PGCD.

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

Propriété - homogénéité

Soit a , b et k trois entiers naturels non nuls.

$$PGCD(ka ; kb) = k\, PGCD(a ; b)$$

Preuve :

Si $a = b\,q + r$ avec $0 \leq r < b$, alors $ka = k\,b\,q + kr$ avec $0 \leq kr < kb$ (car $k \in \mathbb{N}$)
Donc kr est le reste de la division de ka par kb d'après l'unicité de l'écriture.
En utilisant les notations de l'algorithme d'Euclide et multipliant chaque membres des égalités par k, on obtient :

$$PGCD(ka ; kb) = PGCD(kb ; kr_0) = \ldots = k\, r_n = k\, PGCD(a ; b)$$

2) NOMBRES PREMIERS ENTRE EUX

Exemple :

On voudrait savoir s'il est possible de simplifier la fraction $\frac{1223}{717}$.

Pour cela on peut déterminer le PGCD de 1223 et 717. On trouve PGCD(1223 ; 717) = 1.
Par conséquent les nombres 1223 et 717 n'ont pas de diviseur commun autre que 1 (et -1).
On dit que ces deux nombres sont **premiers entre eux**.
La fraction $\frac{1223}{717}$ ne peut pas être simplifiée. On dit que c'est une fraction **irréductible**.

Définition :

Soit a et b deux entiers relatifs non nuls.
On dit que a et b sont **premiers entre eux** si leur PGCD est égal à 1.

Remarques :

- Deux nombres sont donc premiers entre eux s'ils n'ont d'autres diviseurs communs que 1 et -1.
- On dit aussi que a est premier avec b, ou que b est premier avec a.
- On dit aussi parfois que a et b sont **étrangers**.

Rappel :

On dit qu'un entier naturel non nul p est premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

Propriété :

Soit a un entier relatif non nul.
Si p est un nombre premier qui ne divise pas a, alors PGCD(a ; p) = 1, c'est-à-dire que a et p sont premiers entre eux.
(Si p est un nombre premier, p est premier avec tout entier qui n'est pas un de ses multiples)

Preuve :

p est un nombre premier, donc dans $\mathbb{N}$ l'ensemble des diviseurs de p est $\{1 ; p\}$.
Puisque p ne divise pas a, p n'appartient pas à l'ensemble des diviseurs de a.
Donc dans $\mathbb{N}$, le seul diviseur commun à p et a est 1 et PGCD(a ; p) = 1 .

Exemple :

Démontrons que la fraction $\frac{12866}{13}$ est irréductible.

La division euclidienne de 12866 par 13 peut s'écrire $12866 = 989 \times 13 + 9$. Donc 12866 n'est pas divisible par 13.

Comme 13 est un nombre premier, on en déduit que 12866 et 13 sont premiers entre eux, c'est-à-dire que la fraction $\frac{12866}{13}$ est irréductible.

Propriété :

Soit a et b des entiers relatifs non nuls.
Si D = PGCD(a ; b), alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
(il existe a' et b' deux entiers relatifs non nuls premiers entre eux tels que $a = Da'$ et $b = Db'$)

Preuve :

D = PGCD(a ; b) alors D divise a et D divise b.
On en déduit qu' il existe a' et b' deux entiers relatifs non nuls tels que $a = Da'$ et $b = Db'$.
Donc $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls.

Soit $d \in \mathbb{N}$ un diviseur commun à $\frac{a}{D}$ et $\frac{b}{D}$, alors $\frac{a}{D} = da''$ et $\frac{b}{D} = db''$ avec $a'' \in \mathbb{Z}^*$ et $b'' \in \mathbb{Z}^*$.

Ainsi $a = dDa''$ et $b = dDb''$,
Donc dD est un diviseur commun à a et b.
Comme D est le PGCD de a et b, on en déduit que $d = 1$ et que $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux.