Corollaire : *(du théorème de Gauss)*

Soient a et b deux entiers relatifs non nuls et p un nombre premier, si p divise le produit $a{\cdot}b$ alors p divise a ou p divise b.

Preuve :

Pour prouver ce corollaire, effectuons la disjonction de cas sur la divisibilité de a :

Soit p un nombre premier divisant le produit $a{\cdot}b$:

- Si a est divisible par p :
  le corollaire est alors vérifié : p divise a.
- Si a n'est pas divisible par p.
  p étant un nombre premier et n'admettant que 1 et p comme diviseur, on en déduit que :
  $\text{pgcd}\,(a\,;p) = p$ ou $\text{pgcd}\,(a\,;p) = 1$
  Le premier cas étant impossible puisqu'on a supposé que p ne divise par a, on en déduit que :
  $\text{pgcd}\,(a\,;p) = 1$.
  Ainsi, les nombres a et p sont premiers entre eux. De plus, p divise le produit $a{\cdot}b$.
  D'après le théorème de Gauss, l'entier p divise b.
  Ce qui vérifie le corollaire.

Dans les deux cas, le corollaire est vérifié.

Définition :

- Soit a un entier non-nul, on note $\mathcal{D}(a)$ l'ensemble des diviseurs de positifs de a.
- Soit a et b deux entiers non-nul, on note $\mathcal{D}(a\,;\,b)$ l'ensemble des diviseurs positifs de a et de b.

Remarque :

- On a la relation : $\mathcal{D}(a\,;\,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.
- L'ensemble $\mathcal{D}(a\,;\,b)$ est non-vide car le nombre 1 est un diviseur commun à a et b : $1 \in \mathcal{D}(a,b)$.
- L'ensemble $\mathcal{D}(a\,;\,b)$ est majoré par a et majoré par b. On en déduit que l'ensemble $\mathcal{D}(a\,;\,b)$ possède un plus grand élément.

Définition : *(et proposition)*

Le plus grand élément de l'ensemble $\mathcal{D}(a\,;\,b)$ est le plus grand diviseur de a et de b. On le note $\text{pgcd}\,(a\,;b)$.

Remarque :

Soit a et b deux entiers non-nuls, on a :
$\text{pgcd}\,\big(|a|\,;|b|\big) = \text{pgcd}\,(a\,;b)$

Proposition :

Soit a et b deux entiers non-nuls. On a l'équivalence suivante :
$\text{pgcd}\,(a\,;b) = a \iff a$ divise b

Preuve :

- Montrons que a divise $b \Longrightarrow \text{pgcd}\,(a\,;b) = a$
  Supposons que a divise b, alors $a \in \mathcal{D}(b)$.
  De plus :
  - On sait que a divise a : a appartient à $\mathcal{D}(a)$.
    $a \in \mathcal{D}(a)$
  - a est le plus grand élément de $\mathcal{D}(a)$:
    a est un majorant de $\mathcal{D}(a\,;\,b)$.

  a est donc le plus grand élément de $\mathcal{D}(a\,;\,b)$:
  $a = \text{pgcd}\,(a\,;b)$
- Montrons que $\text{pgcd}\,(a\,;b) = a \Longrightarrow a$ divise b
  Supposons que $\text{pgcd}\,(a\,;b) = a$.
  Des deux propriétés ensemblistes :
  $\text{pgcd}\,(a\,;b) \in \mathcal{D}(a\,;\,b)$; $\mathcal{D}(a\,;\,b) \subset \mathcal{D}(b)$
  On en déduit que $a \in \mathcal{D}(b)$: a est un diviseur du nombre b.

Voici un exemple d'utilisation de l'algorithme d'Euclide qui a été vu en classe de troisième :

Dividende	Diviseur	Reste	
288	108	72	$288 = 2\times 108 + 72$
108	72	36	$108 = 1\times 72 + 36$
72	36	0	$72 = 2\times 36 + 0$

Cette algorithme donne : $\text{pgcd}\,(288\,;108) = 36$

Si on applique l'algorithme d'Euclide au couple $(108\,;72)$, on obtiendra :
$\text{pgcd}\,(108\,;72) = 36$

On en déduit l'égalité :
$\text{pgcd}\,(288\,;108) = \text{pgcd}\,(108\,;72)$
Or, en considérant la division euclidienne de 288 par 108, on peut écrire la relation :
$\text{pgcd}\,(a\,;b) = \text{pgcd}\,(b\,;r)$

On généralise cette propriété qui est la "*clé*" de construction de l'algorithme d'Euclide.

Lemme : *(d'Euclide)*

Soit a, b, q, r quatre entiers relatifs non-nuls tels que :
$a = q{\cdot}b + r$
Alors on a : $\text{pgcd}\,(a\,;b) = \text{pgcd}\,(b\,;r)$

Remarque :

Le couple $(q\,;r)$ n'est pas nécessairement le couple obtenu par la division euclidienne de a par b puisque la condition $0 \leqslant r < b$ n'est pas imposée.
Mais le couple $(q\,;r)$ vérifie la relation arithmétique :
$a = q{\cdot}b + r$

Preuve :

Pour montrer l'égalté $\text{pgcd}\left(a\,;b\right) = \text{pgcd}\left(b\,;r\right)$, nous allons montrer l'égalité des deux ensembles :
$\mathcal{D}(a\,;\,b) = \mathcal{D}(q\,;\,r)$
Pour cela, établissons les deux inclusions suivantes :

- $\mathcal{D}(a\,;\,b) \subset \mathcal{D}(b\,;\,r)$:
  C'est à dire qu'on doit établir la relation :
  $k{\in}\mathcal{D}(a\,;\,b) \Longrightarrow k{\in}\mathcal{D}(b\,;\,r)$

  Soit $k{\in}\mathcal{D}(a\,;\,b)$
  $\Longrightarrow k$ divise a et k divise $q{\cdot}b$
  $\Longrightarrow k$ divise $a - q{\cdot}$
  $\Longrightarrow k$ divise r
  $\Longrightarrow k$ appartient à $\mathcal{D}$.

  On en déduit que $k{\in}\mathcal{D}(r)$. Or :
  $k{\in}\mathcal{D}(a\,;\,b) \Longrightarrow k{\in}\mathcal{D}(b)$
  On en déduit $k{\in}\mathcal{D}(b){\cap}\mathcal{D}(r) = \mathcal{D}(b\,;\,r)$

- $\mathcal{D}(b\,;\,r) \subset \mathcal{D}(a\,;\,b)$:
  C'est à dire qu'on doit établir la relation :
  $k\mathcal{D}(b\,;\,r) \Longrightarrow k{\in}\mathcal{D}(a\,;\,b)$

  Soit $k\mathcal{D}(b\,;\,r)$:
  $\Longrightarrow k$ divise b et k divise r
  $\Longrightarrow k$ divise $q{\cdot}b$ et k divise r
  $\Longrightarrow k$ divise $q{\cdot}b + r$

  On en déduit que $k{\in}\mathcal{D}(a,b)$.

Le point central de la démonstration de ces deux implications est :
Si k divise u et v deux entiers non-nuls, alors pour tout α et β entiers relatifs :
k divise $\alpha{\cdot}u + \beta{\cdot}v$

On dit que $\alpha{\cdot}u + \beta{\cdot}v$ est une combinaison linéarire de u et de v.

Proposition :

Soit a et b deux entiers relatifs non-nul et $k{\in}\mathbb{N}^*$. On a l'égalité suivante :
$\text{pgcd}\left(k{\cdot}a\,;k{\cdot}b\right) = k{\cdot}\text{pgcd}\left(a\,;b\right)$

Preuve :

La division euclidienne de a par b donne l'existence du couple $(q\,;r)$ vérifiant la relation :
$a = q{\cdot}b + r \quad \text{où } 0 \leqslant r < b$

Soit k un entier naturel non-nul. On a la relation :
$k{\cdot}a = k{\cdot}q{\cdot}b + k{\cdot}r \quad \text{où } 0 \leqslant k{\cdot}r < k{\cdot}b$
On en déduit que le couple $\left(k{\cdot}q\,;k{\cdot}r\right)$ est obtenu par la division euclidienne de $k{\cdot}a$ par $k{\cdot}b$.

Ainsi, les divisions euclidiennes obtenues par l'algorithme d'Euclide pour obtenir le $PGCD$ de a et de b sont les même, mais multipliés par k que les divisions euclidiennes obtenues par l'algorithme d'Euclide pour obtenir le $PGCD$ de $k{\cdot}a$ et de $k{\cdot}b$.
Ainsi, les deux dernières lignes obtenues dans les deux algorithmes d'Euclide sont équivalentes au facteur k près :
$\text{pgcd}\left(a\,;b\right) = \text{pgcd}\left(k{\cdot}a\,;k{\cdot}b\right)$

Définition :

On dit que les entiers a et b sont premiers entre eux si :
$\text{pgcd}\left(a\,;b\right) = 1$

Propriété :

Soit a et b deux entiers relatifs non-nuls.
On a l'équivalence suivante :
$\text{pgcd}\left(a\,;b\right) = d$
si, et seulement si,
il existe deux entiers relatifs non nuls a' et b' tels que :
$\begin{cases} a = d{\cdot}a' \\ b = d{\cdot}b' \end{cases}$ où a' et b' sont premiers entre eux.

Preuve :

Démontrons les deux implications présentes dans cette équivalence :

- Supposons que $\text{pgcd}\left(a\,;b\right) = d$
  d est un diviseur de a et de b. On a l'existence de deux entiers relatifs a et a' vérifiant :
  $a = a'{\cdot}d \quad ; \quad b = b'{\cdot}d$

  On a les égalités suivantes :
  $$\text{pgcd}\left(a\,;b\right) = d$$
  $$\text{pgcd}\left(a'{\cdot}d\,;b'{\cdot}d\right) = d$$

  D'après la propriété précédente :
  $$d{\cdot}\text{pgcd}\left(a'\,;b'\right) = d$$
  $$\text{pgcd}\left(a'\,;b'\right) = 1$$

  On en déduit que les nombres a' et b' sont premiers entre eux.

- Supposons qu'il existe a' et b' premiers entre eux tels :
  $a = a'{\cdot}d \quad ; \quad b = b'{\cdot}d$

  On a les égalités suivantes :
  $$\text{pgcd}\left(a'\,;b'\right) = 1$$
  $$d{\cdot}\text{pgcd}\left(a'\,;b'\right) = d$$

  D'après la propriété précédente :
  $$\text{pgcd}\left(d{\cdot}a'\,;d{\cdot}b'\right) = d$$
  $$\text{pgcd}\left(a\,;b\right) = d$$