Mathématiques expertes
Arithmétique 2

Serge Bays

Lycée les Eucalyptus

21 novembre 2021

Définition

Soient a et b deux entiers relatifs tels que $(a, b) \neq (0, 0)$. L'ensemble des diviseurs communs de a et b admet un plus grand élément d qu'on appelle le *plus grand commun diviseur* de a et b.

On note $d = PGCD(a, b)$.

Remarque

L'ensemble des diviseurs communs de a et b est un ensemble fini car si x divise a, alors $-|a| \leq x \leq |a|$. Cet ensemble est non vide puisqu'il contient 1. Donc cet ensemble admet un plus grand élément qui est non nul.

Propriétés

Soient a et b deux entiers relatifs :
$PGCD(a, b) = PGCD(|a|, |b|)$

Soient a, b et k trois entiers relatifs non nuls :
$PGCD(ka, kb) = |k|\ PGCD(a, b)$

Si d est un diviseur commun à a et b alors

$$PGCD\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{|d|} PGCD(a, b)$$

Propriété
Soient a et b deux entiers relatifs non nuls.
Alors : $PGCD(a,b) = d \Leftrightarrow D_a \cap D_b = D_d$

Le nombre d est donc le seul entier naturel possédant les deux propriétés :
- d divise a et b ;
- tout diviseur de a et b divise d (si d' divise a et b alors d' divise tous les multiples de d, en particulier d' divise d).

Lemme d'Euclide

Soient a et b deux entiers relatifs non nuls et r le reste de la division euclidienne de a par b :

si $r = 0$ alors $PGCD(a, b) = b$
si $r \neq 0$ alors $PGCD(a, b) = PGCD(b, r)$

Algorithme d'Euclide

Cet algorithme utilise la division euclidienne.

Si a et b sont deux entiers relatifs non nuls alors :
$PGCD(a, b) = PGCD(|a|, |b|)$
On peut donc limiter la recherche du PGCD à a et b entiers naturels non nuls.

Soient a et b deux entiers naturels non nuls. On pose $b = r_0$ et on effectue les divisions euclidiennes successives :

de a par b (si $b \neq 0$) : $a = bq_1 + r_1$
de b par r_1 (si $r_1 \neq 0$) : $b = r_1 q_2 + r_2$
de r_1 par r_2 (si $r_2 \neq 0$) : $r_1 = r_2 q_3 + r_3$
etc ... On arrête si on trouve un reste nul.

La suite (r_i) ainsi définie est strictement décroissante et elle est finie.

Si $r_1 \neq 0$ alors $PGCD(a, b) = PGCD(b, r_1)$, puis
$PGCD(a, b) = PGCD(r_{k-2}, r_{k-1})$ où r_k est le premier reste nul.
On déduit que le PGCD de a et b est le dernier reste non nul.

Définition

Soient a et b deux entiers relatifs non nuls. On dit que a et b sont *premiers entre eux* si et seulement si $PGCD(a,b) = 1$.

Les seuls diviseurs communs de a et b sont 1 et -1.

Identité de Bézout

Soient a et b deux entiers relatifs non nuls : alors il existe un couple (u, v) d'entiers relatifs tel que $au + bv = PGCD(a, b)$.

Théorème de Bézout

Soient a et b deux entiers relatifs non nuls : a et b sont premiers entre eux si et seulement si il existe un couple (u, v) d'entiers relatifs tel que $au + bv = 1$.

Démonstration

Soit d le pgcd de (a, b).

Si a et b sont premiers entre eux, alors $d = 1$ et l'identité de Bézout permet d'affirmer qu'il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = 1$.

Réciproquement, s'il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = 1$, tout diviseur commun à a et b divise $au + bv$ donc divise 1. D'où $d = 1$, donc a et b sont premiers entre eux.

Théorème de Gauss

Soient a, b, c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux
alors a divise c.

Démonstration

Il existe k, u, v entiers relatifs tels que $bc = ka$ et $au + bv = 1$.
D'où $auc + bvc = c$, soit $auc + vka = c$, c'est-à-dire
$a(uc + vk) = c$. Donc a divise c.

Conséquences

Si a est premier avec b et c, alors a est premier avec bc

Démonstration

Il existe u, v, u', v' tels que $au + bv = 1$ et $au' + cv' = 1$
En multipliant membre à membre ces deux égalités, on obtient
$a(uu'a + ucv' + bvu') + bcvv' = 1$

Propriété

Si a et b sont premiers entre eux, si a divise c et si b divise c, alors ab divise c.

Si d est un diviseur de a et b,

$d = \text{pgcd}\,(a, b) \Leftrightarrow \dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.