Arithmétique. Cours

Théorème de Bezout

Propriété

Cette propriété se nomme l'identité de $Bezout$
Soient a et b deux entiers relatifs non nuls tels que $PGCD(a,b) = d$
Alors il existe u et v entiers relatifs tels que $au + bv = d$

Preuve

Soit $A = \{au + bv\}$ l'ensemble des combinaisons linéaires strictement positives de a et b
A est non vide. (il contient $|a|$)
Toute partie non vide de $\mathbb{N}$ admet un plus petit élément, Appelons le m
Nous allons montrer que $d = m$
$d \mid a$ et $d \mid b$ donc d divise toute combinaison linéaire de a et b. **d divise donc m.**

Réalisons la division euclidienne de d par m
$d = gm + h$ avec $0 \leq h < m$

Il vient $au + bv = gm + h$. Or m est par définition combinaison linéaire de u et v.
Il existe (k,l) dans $\mathbb{Z}^2$ tels que $m = ak + bl$
Nous avons donc $au + bv = g(ak + bl) + h \Rightarrow h = a(u - gk) + b(v - gl)$
Donc h est aussi combinaison linéaire positive de a et de b. Or $h < m$, m étant le plus petit élément de A
Cela n'est possible que si $h = 0$

On a donc $d = gm \Rightarrow$ **m divise d**

$d|m$ et $m|d \Rightarrow m = d$. d est donc bien combinaison linéaire de a et de b

Méthode

Une question émerge : comment trouver ces u et v ? Avec l'algorithme d'Euclide.
Reprenons un exemple précédent où nous avons démontré que le $PGCD$ de 1958 et 4539 est 89
L'algorithme d'Euclide appliqué à 1958 et 4539 nous donne :

$$4539 = 1958 * 2 + 623$$
$$1958 = 623 * 3 + 89$$
$$623 = 89 * 7 + 0$$

Donc $89 = 1958 - 623 * 3$. Or $623 = 4539 - 1958 * 2$
Donc $89 = 1958 - (4539 - 1958 * 2) * 3 = 1958 - 4539 * 3 + 2 * 3 * 1958 = 1958 * 7 - 4539 * 3$

Nous avons bien trouvé u et v

Propriété

Soient a et b deux entiers relatifs non nuls tels que $PGCD(a,b) = d$
Tout diviseur commun à a et b divise d

Preuve

Soit D un diviseur commun à a et b. Alors il divise toute combinaison linéaire de a et b.
d est une combinaison linéaire de a et b. Donc $D \mid d$

Théorème

Cette identité nous donne une implication :
$PGCD(a,b) = d \Rightarrow$ il existe u et v entiers relatifs tels que $au + bv = d$
Dans le cas où a et b sont premiers entre eux alors nous avons la réciproque. C'est le :

Théorème de Bezout :
Soient a et b deux entiers relatifs non nuls
$PGCD(a,b) = 1 \Leftrightarrow$ il existe u et v entiers relatifs tels que $au + bv = 1$

Preuve

Le sens $PGCD(a,b) = 1 \Rightarrow$ il existe u et v entiers relatifs tels que $au + bv = 1$ est donné par l'identité de Bezout.
Réciproquement : Supposons qu'il existe u et v entiers relatifs tels que $au + bv = 1$
Soit d un diviseur de a et de b. d divise donc toute combinaison linéaire de a et de b. Donc d divise 1. Donc $PGCD(a,b) = 1$.

Exemple	71 et 60 sont premiers entre eux. Utilisons l'algorithme d'Euclide pour le montrer. $$71 = 60 * 1 + 11$$ $$60 = 11 * 5 + 5$$ $$11 = 2 * 5 + 1$$ $$5 = 1 * 5 + 0$$ Le $PGCD$ de 71 et 60 est donc le dernier reste non nul : 1. Le théorème de Bezout nous renseigne sur le fait qu'il existe u et v entiers relatifs tels que $71u + 60v = 1$ Nous allons trouver u et v en remontrant l'algorithme d'Euclide. $$1 = 11 - 2 * 5 = (71 - 60) - 2 * (60 - 11 * 5) = 71 - 3 * 60 + 10 * 11 = 71 - 3 * 60 + 10(71 - 60)$$ $$= 11 * 71 - 13 * 60$$