

Théorème : Deux entiers a et b sont premiers entre eux si, et seulement si, il existe des entiers u et v tels que $au + bv = 1$.

Démonstration :

• On suppose a et b premiers entre eux ; leur PGCD est 1. Ainsi, l'un des deux au moins est non nul, par exemple a .

Soit l'ensemble E des entiers de la forme $au + bv$, avec u et v entiers. Cet ensemble n'est pas vide, car il contient a (avec $u = 1$ et $v = 0$) et $-a$ (avec $u = -1$ et $v = 0$). E contient a et $-a$, et l'un de ces deux entiers est strictement positif, donc E contient au moins un entier strictement positif.

Soit δ le plus petit d'entre eux ; il existe ainsi u_0 et v_0 entiers tels que : $\delta = au_0 + bv_0$.

La division euclidienne de a par δ s'écrit : $a = \delta q + r$, avec $0 \leq r < \delta$.

D'où : $r = a - \delta q = a - (au_0 + bv_0)q = a(1 - qu_0) + b(-v_0q)$.

Ainsi, r appartient à E car il est de la forme $au + bv$ avec u et v entiers ($u = 1 - qu_0$ et $v = -qv_0$). Comme δ est le plus petit élément strictement positif de E , l'inégalité

$0 \leq r < \delta$ montre que r est nul, d'où $a = \delta q$ et δ divise a .

On montre de même que δ divise b , d'où $\delta = 1$ car a et b sont premiers entre eux : il existe bien des entiers u_0 et v_0 tels que $au_0 + bv_0 = 1$.

• S'il existe des entiers u et v tels que $au + bv = 1$, alors, si d est le PGCD de a et b , il divise a et b , donc $au + bv$, c'est-à-dire 1 : ainsi, d vaut 1, et a et b sont premiers entre eux.

La relation $au + bv = 1$ est parfois appelée relation de Bézout relative aux entiers a et b .