Théorème de Bézout

Théorème

Deux entiers *a* et *b* sont premiers entre eux si et seulement si il existe deux entiers *u* et *v* tels que :

$$au+bv=1$$

Démonstration.

Condition suffisante.

$au+bv=1$

Soit d un diviseur commun à *a* et *b* alors *d* divise $ax+by$ pour tout couple d'entiers $(x\,;y)$ donc *d* divise $au+bv=1$ donc *d* = 1. Le seul diviseur commun est 1, *a* et *b* sont premiers entre eux.

Condition nécessaire.

Soit *a* et *b* premiers entre eux. Soit *E* l'ensemble des nombres $ax+by$, $(x\,,y)\in\mathbb{Z}^2$, strictement positif. Cet ensemble contient $a=1\times a+0\times b$, si *a* est positif, ou $-a=-1\times a+0\times b$, si *a* est négatif, donc il n'est pas vide. Cet ensemble ne contient que des entiers strictement positifs donc il a un plus petit élément égal à $m=au+bv$.

Montrons que *m* divise *a* et *b*. Effectuons la division euclidienne de *a* par *m*.

$a=mq+r\,,\ 0\leqslant r<m\ \Rightarrow\ a=(au+bv)q+r\ \Rightarrow\ a(1-u)+b(-vq)=r\,,\ 0\leqslant r$

Si $r>0$ alors $0<r<m$ et $r\in E$. *m* est le plus petit élément donc c'est impossible et $r=0$, *m* divise *a*.

On démontre de même que *m* divise *b*.

m divise *a* et *b* premiers entre eux donc *m* = 1 et $au+bv=1$.

Remarques.

On emploie une méthode classique pour démontrer que *m* divise *a*. On effectue la division euclidienne de *a* par *m* et on montre que le reste est nul.

Le couple $(u\,,v)$ n'est pas unique. $au+bv=1\ \Rightarrow\ a(u+kb)+b(v-ka)=1$