Démonstration du Théorème de Bézout

Enoncé du théorème

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

$$au + bv = 1$$

Si et seulement si => Implication dans les deux sens

Sens direct :

Immédiat grâce à l'identité de Bézout

$$\text{Soit } a \text{ et } b \in Z, \exists (u, v) \in \mathbb{Z}^2 : au + bv = PGCD(a, b)$$

Ici, vu que PGCD (a,b) = 1, le théorème est validé dans ce sens.

Réciproque:

On suppose qu'il existe deux entiers u et v tels que

$$au + bv = 1$$
$$\text{Si } \ D = PGCD(a, b), \text{alors } \ D \mid a \text{ et } D \mid b \text{ donc } D \mid au + bv$$

Donc D divise 1. On a alors bien D = 1 car 1 est son seul diviseur et deux nombres tels que PGCD(a,b) = 1 sont forcément premiers entre eux.