Théorème de Bézout

Propriété

Soit a et b deux entiers naturels non nuls tels que $d = PGCD(a;b)$.
Il **existe toujours** deux entiers relatifs u et v tels que $a \times u + b \times v = d$.

Les deux nombres u et v sont appelés les **coefficients de Bézout**. C'est en réécrivant les différentes étapes de l'algorithme d'Euclide que l'on peut déterminer ce couple de nombres.

Théorème

Soit a et b deux entiers naturels non nuls. Les nombres a et b sont **premiers entre eux** si et seulement si il existe **deux entiers relatifs** u et v tels que $\boxed{a \times u + b \times v = 1}$.

Théorème de Gauss

Théorème

Soit a, b et c trois entiers naturels non nuls.
Si a divise le produit $b \times c$ et si a est premier avec b alors a divise c.

La démonstration de ce théorème se base sur l'utilisation du théorème de Bézout.

Equation diophantienne

Une équation diophantienne est une équation dont tous les **coefficients** sont **entiers** et dont les **solutions** recherchées sont **entières** elles aussi.

Les équations du type $ax + by = c$ avec a, b, c, x et y entiers sont dites diophantiennes.

Les deux théorèmes de Bézout et de Gauss sont **à la base** du procédé de résolution des équations diophantiennes.

Petit théorème de Fermat

Théorème

Si p est un **nombre premier** et si a est un entier naturel supérieur ou égal à deux **non divisible** par p,
Alors $a^{p-1} - 1$ est **divisible** par p, c'est-à-dire $\boxed{a^{p-1} \equiv 1[p]}$.

Conséquence

Si p est un **nombre premier** et si a est un entier naturel supérieur ou égal à deux,
Alors $a^p - a$ est **divisible** par p, c'est-à-dire $\boxed{a^p \equiv a[p]}$.