

Preuve du théorème fondamental de l'arithmétique

Théorème fondamental de l'arithmétique
(unicité de la décomposition en facteurs premiers dans \mathbb{Z})

Récurrence

Lemme de Gauss :
 $a \mid bc, a \wedge c = 1 \implies a \mid b$
ou Lemme d'Euclide
 p premier, $p \mid ab \implies p \mid a$
ou $p \mid b$

$$ua + vc = 1 \implies uab + vbc = b \implies a \mid b$$

Identité de Bezout

$$(a, b) := \{ua + vb, u, v \in \mathbb{Z}\} = (a) + (b) = (a \wedge b)$$

\mathbb{Z} est principal

Division euclidienne par $d > 0$ minimal de l'idéal

Division euclidienne dans \mathbb{Z}