

TEOREMA DI BEZOUT

SIANO $a, b \in \mathbb{Z}$ CON $(a, b) = m$ M.C.D.

$\Rightarrow \exists x, y \in \mathbb{Z}$ s.c. $ax + by = m$

DIM CON DIVISIONE EUCLIDEA \square

TEOREMA

Il più grande comun divisore tra due numeri interi è sempre divisibile per ogni altro comun divisore.

SIA m M.C.D. DI a E b

SIA $n < m$ UN DIVISORE DI a E b

$\leadsto a = \alpha n, b = \beta n$

PER IL TEOREMA DI BEZOUT

$\leadsto m = ax + by = \alpha n x + \beta n y = n(\alpha x + \beta y)$

$\Rightarrow n$ DIVIDE m \square