1 Lema de Euclides

1.1 enunciado

Sejam a, b, q e $r \in \mathbb{Z}$, se $a = bq + r$, então $mdc(a, b) = mdc(b, r)$.

Demonstração: Sejam D_a, D_b, D_r os conjuntos de divisores de a, b e r respectivamente. Para provarmos que $mdc(a, b) = mdc(b, r)$ basta mostrar que $D_a \cap D_b = D_b \cap D_r$, pois, se esses conjuntos forem iguais, então os seus máximos também são iguais.

Suponha que $d \in D_a \cap D_b$, então $d|a - qb = r \Rightarrow d \in D_b \cap D_r$.

Se $d \in D_b \cap D_r$, então $d|bq + r = a \Rightarrow d \in D_a \cap D_b$.

Logo $D_a \cap D_b = D_b \cap D_r$

$\square$