

Why the Euclidean Algorithm Works

Definition: A linear combination of two integers a and b is any integer of the form $ax + by$, where $x, y \in \mathbb{Z}$.

Lemma: Let $a, b \in \mathbb{Z}$ and suppose r is a linear combination of a and b . Then any common divisor of b and a is a common divisor of b and r .

Lemma: Let a and b be non-zero integers and suppose $a = qb + r$. Then the gcd of a and b is equal to the gcd of b and r .