

Theorem 1 If $x, y, m \in \mathbb{Z}$ then $\gcd(x, y) = \gcd(x, y - mx)$

PROOF Given $m \in \mathbb{Z}$

It must be true that

$$(y - mx) = (y \bmod x)$$

Thus we are really trying to prove..

$$\begin{aligned}\gcd(x, y) &= \gcd(x, y - mx) \\ &= \gcd(x, y \bmod x)\end{aligned}$$

That being true, there are two cases that must be considered for this proof.

Case 1 where $x = y = 0$

$$\begin{aligned}\gcd(0, 0) &= \gcd(0, 0 - 0) \\ &= \gcd(0, 0)\end{aligned}$$

Case 2 Assume at least one of x, y is non zero

Suppose $d|x$ and $d|y$

We now must prove that $d|y - mx$

Since $(d|x \wedge y)(\exists k_0, k_1)$ such that $(x = d * k_0)(y = d * k_1)$ given $(k_0, k_1 \in \mathbb{Z})$

$$\begin{aligned}\gcd(x, y) &= \gcd(x, y - mx) \\ &= \gcd(x, y \bmod x) \\ &= d \\ &= ax + by \\ &= ax + y(\end{aligned}$$