

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

Lemma A. $p|q \wedge p|r \implies p|q+r$

Assume p, q, r are all integers such that $p, q, r \neq 0$

Let $p|q$ and $p|r$ evenly

Since $p|q \implies (\exists k_1)(q = pk_1)$

$p|r \implies (\exists k_2)(r = pk_2)$

$q + r = p(k_1 + k_2)$

$q + r = p(k_3)$ for some integer $k_3 = k_1 + k_2$

By definition of divisibility $p|q+r$

Lemma B. Let a, b, c be integers such that $a, b, c \neq 0$

$a|b \implies a|bc$

$b = ar$ where $r \in \mathbb{Z}$

$bc = arc = (ar)c$

Since rc is an integer $a|bc$

PROOF There are two cases that must be considered for this proof.

Case 1 where $x = y = 0$

Let $d_0|x \wedge y$

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

Hence, it must be true for this case.

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

Suppose $d_1|x$ and $d_1|y$

Let $n = -mx$

By Lemma B it is true that $d_1|n$

Since $d_1|x \wedge d_1|n$ by Lemma A it must be true that $d_1|y+n$

Hence $d_1|y+n$

$d_1|y - mx$