

## Some Results on the Greatest Common Divisor of Two Integers

$(bx + cy, b) = (cy, b)$  for all integers  $x$  and  $y$ .

*Proof.*

Since  $(bx + cy, b) \mid (bx + cy)$  and  $(bx + cy, b) \mid bx$ ,  $(bx + cy, b) \mid ((bx + cy) - bx)$ . Thus,  $(bx + cy, b) \mid cy$ . Moreover,  $(bx + cy, b) \mid b$ . Thus,

$$(1) \quad (bx + cy, b) \mid (cy, b).$$

Since  $(cy, b) \mid bx$  and  $(cy, b) \mid cy$ ,  $(cy, b) \mid (bx + cy)$ . Also,  $(cy, b) \mid b$ . Therefore,

$$(2) \quad (cy, b) \mid (bx + cy, b)$$

So

$$(3) \quad (bx + cy, b) = (cy, b)$$

by (1) and (2).

It can be shown by the similar method as above that

$$(4) \quad (bx + cy, c) = (bx, c).$$

If  $(b, c) = 1$  then  $(a, bc) = (a, b)(a, c)$ .

*Proof.*

There exist integers  $m_0$  and  $n_0$  such that  $(a, b) = m_0a + n_0b$ . Similarly,  $(a, c) = ma + nc$  for some integers  $m$  and  $n$ . Since  $(a, bc) \mid a$  and  $a \mid ((m_0a)(ma) + (m_0a)(nc) + (n_0b)(ma))$ ,

$$(5) \quad (a, bc) \mid ((m_0a)(ma) + (m_0a)(nc) + (n_0b)(ma)).$$

Moreover,  $(a, bc) \mid bc$  and  $bc \mid (n_0b)(nc)$ . So

$$(6) \quad (a, bc) \mid (n_0b)(nc).$$

Hence  $(a, bc) \mid ((m_0a)(ma) + (m_0a)(nc) + (n_0b)(ma) + (n_0b)(nc))$  by (5) and (6). In other words,

$$(7) \quad (a, bc) \mid (a, b)(a, c).$$

Since  $(b, c) = 1$ ,  $m'b + n'c = 1$  for some integers  $m'$  and  $n'$ . Since  $(a, b) \mid b$  and  $(a, c) \mid a$ ,  $(a, b)(a, c) \mid ba$ . It follows that

$$(8) \quad (a, b)(a, c) \mid m'ba.$$

Also  $(a, b) \mid a$  and  $(a, c) \mid c$ . Thus  $(a, b)(a, c) \mid ca$ . So

$$(9) \quad (a, b)(a, c) \mid n'ca.$$

From (8) and (9),  $(a, b)(a, c) \mid (m'ba + n'ca)$ . In other words,

$$(10) \quad (a, b)(a, c) \mid a.$$

Since  $(a, b) \mid b$  and  $(a, c) \mid c$ ,

$$(11) \quad (a, b)(a, c) \mid bc.$$

From (10) and (11),

$$(12) \quad (a, b)(a, c) \mid (a, bc).$$

So

$$(13) \quad (a, bc) = (a, b)(a, c).$$

by (7) and (12).

If  $(b, c) = 1$  then  $(cy, b)(bx, c) = (b, y)(c, x)$  for all integers  $x$  and  $y$ .

*Proof.*

Since  $(b, c) = 1$ ,  $mb + nc = 1$  for some integers  $m$  and  $n$ . Since  $(cy, b) \mid mb$  and  $(cy, b) \mid cy$ ,  $(cy, b) \mid (mby + ncy)$ . So  $(cy, b) \mid y$ . Since  $(cy, b) \mid b$  and  $(cy, b) \mid y$ ,

$$(14) \quad (cy, b) \mid (b, y).$$

Since  $(bx, c) \mid bx$  and  $(bx, c) \mid cx$ ,  $(bx, c) \mid (mbx + ncx)$ . So  $(bx, c) \mid x$ . Since  $(bx, c) \mid c$  and  $(bx, c) \mid x$ ,

$$(15) \quad (bx, c) \mid (c, x).$$

Hence

$$(16) \quad (cy, b)(bx, c) \mid (b, y)(c, x)$$

by (14) and (15).

Since  $(b, y) \mid cy$  and  $(b, y) \mid b$ ,

$$(17) \quad (b, y) \mid (cy, b).$$

Since  $(c, x) \mid bx$  and  $(c, x) \mid c$ ,

$$(18) \quad (c, x) \mid (bx, c).$$

Hence

$$(19) \quad (b, y)(c, x) \mid (cy, b)(bx, c)$$

by (17) and (18).

Therefore

$$(20) \quad (cy, b)(bx, c) = (b, y)(c, x)$$

by (16) and (19).

If  $(b, c) = 1$  then  $(bx + cy, bc) = (b, y)(c, x)$  for all integers  $x$  and  $y$ .

*Proof.*

$$\begin{aligned} (bx + cy, bc) &= (bx + cy, b)(bx + cy, c) && \text{by (13)} \\ &= (cy, b)(bx, c) && \text{by (3) and (4)} \\ &= (b, y)(c, x) && \text{by (20)} \end{aligned}$$