Answer on Question #52639 – Math, Combinatorics – Number Theory

Question. Show that if $(b, c) = 1$ then $(a, bc) = (a, b)(a, c)$.

Proof. Denote $d_b = (a, b)$, $d_c = (a, c)$, and $d = (a, bc)$. We have to prove that $d = d_b d_c$.

First we show that

$$(d_b, d_c) = 1.$$

Indeed, denote $k = (d_b, d_c)$. Then k divides d_b which in turn divides b, and k also divides d_c which in turn divides c. Therefore k divides both b and c, whence it divides their greatest common divisor $(b, c) = 1$. Hence $k = (d_b, d_c) = 1$.

Further notice that both d_b and d_c divide a and bc, whence

$$d_b \textit{ and } d_c \textit{ divide } d = (a, bc).$$

We will now show that

$$\textit{the product } d_b d_c \textit{ divides } d.$$

Indeed, we have that $d = pd_b = qd_c$ for some integers p, q. Moreover, the relation $(d_b, d_c) = 1$ means that there exist integers x, y such that

$$xd_b + yd_c = 1.$$

Multiplying both sides of this identity by d we get

$$xd_b d + yd_c d = d,$$

$$xd_b d_c q + yd_c d_b p = d,$$

so

$$d = d_b d_c (xq + yp).$$

Thus $d_b d_c$ divides d.

It remains to prove the inverse statement that

$$d \textit{ divides the product } d_b d_c.$$

We have proved that $d = d_b d_c u$ for some integer u. If $u = 1$, then $d = d_b d_c$ and our statement is proved.

Suppose $u > 1$. Then u has some prime divisor $p > 1$, so $u = pv$ for some integer v, and thus

$$d = d_b d_c pv.$$

In particular, both pd_b and pd_c divide a, as d does so.

Write $b = \bar{b} d_b$, $c = \bar{c} d_c$ and $bc = wd$ for some integers $\bar{b}$, $\bar{c}$, w. Then

$$bc = \bar{b} d_b \bar{c} d_c = wd = wd_b d_c pv,$$

whence

$$\bar{b}\bar{c} = wpv.$$

Thus p divides $\bar{b}\bar{c}$. But since p is prime it must divide either $\bar{b}$ or $\bar{c}$.

If p divides $\bar{b}$, then pd_b divides $\bar{b} d_b = b$. However, as noted above, pd_b also divides a, whence pd_b divides the greatest common divisor $d_b = (a, b)$. Therefore $pd_b \leq d_b$, which is possible only when $p = 1$. The latter contradicts to the assumption that $p > 1$. Therefore p can not divide b.

By similar arguments p can not divide c.

Thus we get a contradiction with the assumption $u > 1$. Therefore $u = 1$, whence $d = d_b d_c$.