Answer on Question #52570 – Math, Combinatorics – Number Theory

Question. If $a = bq + r$ then show that $(a, b) = (b, r)$.

Solution. First recall that the relation $(a, b) = 1$ is equivalent to the assumption that there exist integer numbers x, y such that

$$ax + by = 1.$$

Using this we can prove the required statement. The proof uses the following lemma.

Lemma. *If $(a, b) = 1$, then $(ad, bd) = d$ for each $d \geq 1$.*
Proof. Indeed, by definition d divides ad and bd. Conversely, suppose e divides ad and bd, so $ad = \bar{a}e$ and $bd = \bar{b}e$ for some integers $\bar{a}$ and $\bar{b}$. Since $(a, b) = 1$, i.e. $ax + by = 1$ for some x, y, we have that

$$d = adx + bdy = \bar{a}ex + \bar{b}ey = (\bar{a}x + \bar{b}y)e,$$

and so e divides d. Thus d is the greatest common divisor of ad and bd, i.e. $(ad, bd) = d$. Lemma is proved. □

Consider now two cases.

Case 1. First suppose that $(a, b) = 1$, so $ax + by = 1$ for some integer x, y. We should show that $(b, r) = 1$ as well, that is $bt + rs = 1$ for some integer r, s. We have that

$$1 = ax + by = (bq + r)x + by = b(q + y) + rx,$$

and so $(b, r) = 1$.

Case 2. Now suppose $(a, b) = d$ for some $d > 1$. This means that $a = \bar{a}d$ and $b = \bar{b}d$, where $(\bar{a}, \bar{b}) = 1$.

Then from $a = bq + r$ we get that

$$\bar{a}d = \bar{b}dq + r,$$
$$r = (\underbrace{\bar{a} - \bar{b}q}_{\bar{r}})d.$$

Denote the expression in the brackets by $\bar{r}$:

$$\bar{r} = \bar{a} - \bar{b}q,$$

then

$$r = \bar{r}d, \qquad \bar{a} = \bar{b}q + \bar{r}.$$

Since $(\bar{a}, \bar{b}) = 1$, it follows from Case 1 that $(\bar{a}, \bar{b}) = (\bar{b}, \bar{r}) = 1$. Hence by Lemma

$$(b, r) = (\bar{b}d, \bar{r}d) = (b, r)d = d.$$

In both cases we showed that (a,b)=(b,r).