Answer on Question #52569 – Math, Combinatorics – Number Theory

Question. If $(a, b) = 1$, then prove that $(a - b, a + b, ab) = 1$.

Solution. Notice that the statement $(a, b) = 1$ is equivalent to the assumption that there exist integer numbers p, q such that

$$ap + bq = 1.$$

We should prove that $(a - b, a + b, ab) = 1$, i.e. that the greatest common divisor of all three numbers $a + b$ $a - b$ and ab is 1. However, it may happens that some of them are not relatively prime.

For instance $(5, 3) = 1$, but $(5 + 3, 5 - 3) = 2$. Nevertheless in this case we have that $(5 + 3, 5 - 3, 5 \cdot 3) = 1$.

It suffices to show that

$$(a + b, ab) = 1,$$

that is $a + b$ and ab has no nontrivial common divisors. This will imply that all three numbers $a - b$, $a + b$ and ab has no nontrivial common divisors, i.e. $(a - b, a + b, ab) = 1$. For the proof we need two lemmas.

Lemma 1. If $(a, b) = 1$, then $(a, a + b) = (b, a + b) = 1$ as well.
Proof. It suffices only to prove that $(a, a + b) = 1$. From $ap + bq = 1$, we geet

$$1 = (a, b) = ap + bq = ap - aq + aq + bq = a(p - q) + (a + b)q = (a, a + b)$$

Lemma 1 is proved. □

Lemma 2. *If* $(x, a) = (x, b) = 1$ *and* $(a, b) = 1$*, then* $(x, ab) = 1$ *as well.*
Proof. By assumption there are integer numbers $\alpha, \beta, \gamma, \delta$ such that

$$(x, a) = \alpha x + \beta a = 1,$$
$$(x, b) = \gamma x + \delta b = 1.$$

Multiplying the first equation by bq and the second by ap and adding them we get

$$(\alpha x + \beta a)bq + (\gamma x + \delta b)ap = bq + ap.$$

Taking to account that $(a, b) = ap + bq = 1$, we see that the right hand side is 1, whence

$$(\alpha x + \beta a)bq + (\gamma x + \delta b)ap = 1,$$
$$x(\alpha bq + \gamma qp) + ab(\beta q + \delta p) = 1.$$

thus $(x, ab) = 1$ as well. Lemma 2 is proved. □

Corollary 3. $(a + b, ab) = 1$.
Proof. By Lemma 1 we have that $(a+b, a) = (a+b, b) = 1$. Then from Lemma 2 applied to $x = a + b$ it follows that $(a + b, ab) = 1$. Corollary 3 is proved. □

Now we can complete the proof. Notice that by definition $(a-b, a+b, ab)$ divides $a+b$ and ab, whence it must divide $(a+b, ab) = 1$. Therefore $(a-b, a+b, ab) = (a+b, ab) = 1$.