
Problem. Prove the following:

$$\forall a, b \in \mathbb{Z}^+ \left(\exists s, t \in \mathbb{Z} \left(as + bt = GCD(a, b)\right)\right).$$

Solution. This statement leads to a beautiful area of math called number theory. It boils down to the Euclidean Algorithm. The process is easiest seen by example before writing it out in a general form, which tends to look a little clunky.

So let's start with $a = 164$ and $b = 24$, for example. Then we want to find c_1, d_1 so that

$$164 = 24c_1 + d_1$$

and $0 \le d_1 < 24$. We get $c_1 = 6$, which makes $d_1 = 20$. So our equation is

$$164 = 24(6) + (20)$$

Then we swap out our a with 24 and b with 20 and try to find c_2, d_2 so that

$$24 = 20c_2 + d_2$$

and $0 \le d_2 < 20$. Clearly $c_2 = 1$ and $d_2 = 4$, so our equation is

$$24 = 20(1) + (4).$$

Swapping out a for 20 and b for 4, we again want to find c_3, d_3 so that

$$20 = 4c_3 + d_3$$

and $0 \le d_3 < 4$. We see that $c_3 = 5$ works and in fact leaves $d_3 = 0$. THIS TELLS US THIS IS WHERE WE STOP! Let's list each equation we got along the way:

$$164 = 24(6) + (20)$$

$$24 = 20(1) + (4)$$

Notice the LAST non-zero d_i that we got was $d_2 = 4$ and that $GCD(164, 24) = 4$. This is always the case. Now we can use the last equation to write

$$4 = 24 - 20(1)$$

The first equation tells us that

$$20 = 164 - 24(6).$$

Plugging this into the equation we just got gives us a way to write 4, the GCD, as a linear combination of 164 and 24:

$$4 = 24 - (164 - 24(6))(1) = (-1)164 + (7)24 = GCD(164, 24).$$

Now we want to translate that into a proof for the general case with a, b. Assuming that $a > b$, we want to find c_1, d_1 so that $a = c_1 b + d_1$ with $0 \le d_1 < c_1$. Then we swap a with b

and b with d_1 and try to find c_2, d_2 so that $b = c_2 d_1 + d_2$. Then we swap out a with d_1 and b with d_2, and so on. We continue to do this until we reach the first $d_k = 0$. Then we have a bunch of equations:

$$a = c_1 b + d_1$$

$$b = c_2 d_1 + d_2$$

$$d_1 = c_3 d_2 + d_3$$

$$\vdots$$

$$d_{k-3} = c_{k-1} d_{k-2} + d_{k-1}.$$

The important thing to remember is that since $d_k = 0$, we know that $d_{k-1} = GCD(a, b)$. So then we use each of these equations to continue substituting values until we find s, t so that $as + bt = d_{k-1} = GCD(a, b)$. For example, if we get $d_3 = 0$, the equations we get are

$$a = c_1 b + d_1$$

$$b = c_2 d_1 + d_2$$

which tells us $d_2 = b - c_2 d_1$ and $d_1 = a - c_1 b$, meaning

$$d_2 = GCD(a, b) = b - c_2(a - c_1 b) = (-c_2)a + (1 + c_1 c_2)b.$$

So in this case, $s = -c_2$ and $t = 1 + c_1 c_2$.

Although it would be tough to write this out for a big value of k for which $d_k = 0$, the important thing is that we CAN do this algorithm, rather than actually doing it. The fact that we're able to always find such an s, t is exactly what we wanted to prove, so we're done!