Frozen Fish - Solution

Recall Bézout's Lemma from the course Group Theory, which is a useful partial result that tells us whether it is even possible to find a solution (x, y) without the restriction that $x, y \geq 0$.

Lemma 1 (Bézout)**.** *Given two positive integers a, b and an integer c, there exist integers x, y (not necessarily positive) such that*

$$a \cdot x + b \cdot y = c$$

if and only if $\gcd(a, b) \mid c$.

The $\Rightarrow$ implication of Bézout's lemma should be obvious. This should be a big hint, indicating that we want to look for the greatest common divisor $\gcd(a, b)$. This can be done using the Euclidean algorithm. In fact, a solution (x, y) from Bézout's algorithm is found using the so-called extended Euclidean algorithm. The proof of this algorithm (which also proves the $\Leftarrow$ implication of Bézout) takes too far but we can show how the algorithm works with a small example.

1 Step 1

First, we execute the Euclidean algorithm, as shown in table 1

a	b	k	l
189	87		
15	87	2	
15	12		5
3	12	1	
3	0		4

Table 1: The Euclidean algorithm finding the gcd of 189 and 87. In each step, we substract the smallest integer from the largest. *k.l* denote how many substractions we do in each step.

In the 'extended' step of the extended Euclidean algorithm, we will write the greatest common divisor as a difference of a, b. In this case we start at the bottom with $3 = 15 - 12$, as we have found in the second to last step. Then in

each step, we will write the smallest number as a difference of the two a, b in the step above using k, l, as shown below:

$$\begin{aligned}
3 &= 15 - 12 \\
3 &= 15 - (87 - 5 \cdot 15) \\
3 &= 6 \cdot 15 - 87 \\
3 &= 6 \cdot (189 - 2 \cdot 87) - 87 \\
3 &= 6 \cdot 189 - 13 \cdot 87.
\end{aligned}$$

We have now executed the extended Euclidean algorithm to find (x, y) such that $\gcd(a, b) = a \cdot x + b \cdot y$.

2 Step 2

Now, if $\gcd(a, b) \mid c$ of course, we multiply the above equation by $\frac{c}{\gcd(a,b)}$ to find x', y' such that

$$c = a \cdot x' + b \cdot y'.$$

3 Step 3

The last step uses lemma 2 shown below.

Lemma 2. *If we have two solutions (x, y) and (x', y') for the equation*

$$a \cdot x + b \cdot y = c,$$

then there exists some integer n such that $x' = x + \frac{b}{\gcd(a,b)} n$ and $y' = x - \frac{a}{\gcd(a,b)} n$.

This lemma looks difficult, but it says nothing more than that if we start with a solution (x, y), then by changing the solution to

$$(x', y') = \left(x + \frac{b}{\gcd(a, b)}, y - \frac{a}{\gcd(a, b)} \right)$$

a number of times, we can find all other solutions. Indeed, this is exactly what we should do in this step. In step 2, one of (x, y) is negative. Without loss of generality, assume $x < 0$ for now. Then we increase x by an increment of $\frac{b}{\gcd(a,b)}$ until x is positive. Now, if y has now flipped signs, then a solution (x, y) does not exist. If it didn't, then we have found a non-negative solution (x, y), as wanted.

□