Problem 1. Let a and b be natural numbers that are not both zero and let d be their greatest common divisor. Prove that it is possible to find integers x and y such that $ax + by = d$. You may use without proof that the greatest common divisor of a and b exists.

Suggestion: Structure your proof as an induction on a whose induction step contains an induction on b.

Hint: You may want to make use of the facts that $\gcd(a, b) = \gcd(b, a)$ and $\gcd(a, b) = \gcd(a, b - a)$.

Solution. For each $a \in \mathbb{N}$, let

$$S_a = \{b \in \mathbb{N} : ax + by = \gcd(a, b) \text{ has a solution}\}.$$

We want to show that $S_a = \mathbb{N}$ for all $\mathbb{N}$.[1]

The proof is by induction on a. Base case: If $a = 0$ then $b \neq 0$ and $\gcd(a, b) = b$ so the equation $ax + by = d$ is solved by $x = 0$ and $y = 1$.

Induction step: Assume that $S_0 = S_1 = \cdots = S_{a-1} = \mathbb{N}$. We wish to deduce that $S_a = \mathbb{N}$. We prove this by induction on b.

The base case of the inner induction is $b = 0$. In this case, $a \neq 0$ and $\gcd(a, b) = a$ so the equation $ax + by = d$ is soved by $x = 1$ and $y = 0$.

Inner induction step: We assume that $a'x + b'y = \gcd(a', b')$ has a solution if $a' < a$ or if $a' = a$ and $b' < b$ and we wish to deduce that $ax + by = \gcd(a, b)$ has a solution.

We consider three possibilities based on $b < a$ or $b \geq a$. If $b < a$ then $bx + ay = \gcd(b, a)$ has a solution by the induction hypothesis. Switching x and y gives a solution to $ax + by = \gcd(a, b)$ since $\gcd(a, b) = \gcd(b, a)$.

If $a \leq b$ then $b - a \geq 0$. Therefore $ax + (b - a)y = \gcd(a, b - a)$ has a solution in integers x and y. But $\gcd(a, b - a) = \gcd(a, b)$: If e divides a and b then it divides a and $b - a$ by exercise 5.11; similarly, if e divides a and $b - a$ then it divides a and $(b - a) + a = b$, also by exercise 5.11. Thus $ax + (b - a)y = \gcd(a, b)$ has a solution.

But rearranging this we get $a(x + y) + by = \gcd(a, b)$. Since $x + y$ and y are both integers, this completes the proof of inner inductive step. By induction, this completes the outer inductive step as well. Then by the outer induction, we deduce that $S_a = \mathbb{N}$ for all $a \in \mathbb{N}$. $\square$

Solution. Let S be the set of all numbers in $\mathbb{N}$ that can be written as $ax + by$ where a and b are integers. We would like to show that S contains d. It certainly has a least element, say e.

Certainly $e \leq a$ and $e \leq b$ since both a and b are in S. I claim that this e must divide both a and b. Suppose that e did not divide a. Then by the division algorithm, there would be an integer q and an integer r with $0 < r < e$ such that $a = qe + r$. (Note that $r \neq 0$ because e does not divide a.) Written another way,

$$r = a - qd = a - q(ax + by) = (1 - qx)a + yb.$$

[1] If $\gcd(a, b)$ does not exist, we declare that $ax + by = \gcd(a, b)$ has a solution. This only applies when $a = b = 0$.

This means that $r \in S$. But $r < e$, contradicting the minimality of e. This shows that the assumption that e did not divide a was false. A similar argument with the roles of a and b exchanged shows that e also divides b. Therefore $e \leq d$ since d is the greatest common divisor of a and b.

On the other hand, any number of the form $ax + by$ must be divisible by d since $d|a|ax$ and $d|b|by$. Therefore $d \leq e$. Put together, we have $d \leq e \leq d$ so $d = e$. $\square$