Sets and Logic, Dr. Block, Lecture Notes, 3-13-2020

First, we look at Proposition 69 in my course notes:

Proposition 69. Suppose that a and b are positive integers. Then there exist integers k and ℓ such that

$$gcd(a, b) = ak + b\ell.$$

This appears in the text as Proposition 7.1 on page 152. You should study the details of this proof in the text. Here is an outline of the steps in the proof.

Step 1. Consider the set $A = \{ax + by : x, y \in \mathbb{Z}\}$, and $B = \{w \in A : w \geq 1\}$. The set B is not given a name in the proof in the text, but is still involved in the proof. Verify that B is not empty. So B has a smallest element which we call d.

Step 2. Note that since $d \in B$ we have $d \geq 1$ and for some integers k and ℓ we have

$$d = ak + b\ell.$$

Note that the integers k and ℓ are now fixed for the rest of the proof.

Step 3. Prove that d is a common divsor of a and b.

Step 4. Prove that d is a multiple of $gcd(a, b)$.

Conclusion. It follows from Step 4 that $d \geq gcd(a, b)$. Then from Step 3, $d = gcd(a, b)$. Therefore, by Step 2,

$$gcd(a, b) = ak + b\ell.$$

□

Next, we use Proposition 69 in one of the exercises in the text.

Exercise 30. Suppose $a, b, p \in \mathbb{Z}$ and p is prime. Prove that if $p|ab$ then $p|a$ or $p|b$.

Before giving the proof, consider the form of the statement we are asked to prove. The form is $P \Rightarrow (Q \vee R)$. So we will begin the proof with the statement "Suppose P." Then we have to prove $(Q \vee R)$. Recall the ways of proving a statement of this form:

* Suppose $\sim Q$ and prove R.
* Suppose $\sim R$ and prove Q.
* Proceed by contradiction.
* Make cases and deal with each case separately. When you do this the cases must cover every possibility. Here is one example: Suppose that x is an integer.

Case 1. x is even.
Case 2. x is odd.
In the following proof that follows we will use the first way listed above:

* Suppose $\sim Q$ and prove R. Here is the proof.

Proof of Exercise 30. Suppose that $a, b, p \in \mathbb{Z}$ and p is prime. Suppose that $p|ab$. Suppose also that p does not divide a. Then, since p is prime, we must have $gcd(a, p) = 1$. It follows from Proposition 69 that for some integers k and ℓ we have

$$ak + p\ell = 1.$$

Multiplying both sides by b we obtain

$$abk + pb\ell = b.$$

Now, since $p|ab$, there is some integer x satisfying $ab = px$. Substituting this in the last displayed equality, we obtain

$$pxk + pb\ell = b.$$

Therefore, $p(xk + b\ell) = b$, and thus, $p|b$.
□

Next, we look at Exercise 32.

Exercise 32. If $n \in \mathbb{Z}$, then $gcd(n, n + 2) \in \{1, 2\}$.

The stategy here is to give a name to the greatest common divisor, and the use the fact that it divides both n and $n+2$. We also use the fact that a positive integer j can not divide a positive integer smaller that j. See Propostion 42, in the course notes.

Proof of Exercise 32.

Suppose that $n \in \mathbb{Z}$. Let $d = gcd(n, n+2)$. Then for some integers x and y we have $n = dx$ and $n + 2 = dy$. It follows that

$$2 = n + 2 - n = dy - dx = d(y - x).$$

So, $d|2$. Since $d \geq 1$, it follows that $d \in \{1, 2\}$. Therefore,

$$gcd(n, n+2) \in \{1, 2\}.$$

□

Finally, we look at Exercise 18.

Exercise 18. There is a set X for which $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$.

To prove this we must exhibit a set X that satisfies the desired properties. Here is a proof.

Proof of Exercise 18. Consider the set

$$X = \{\mathbb{N}\} \cup \mathbb{N} = \{\mathbb{N}, 1, 2, 3, \ldots\}.$$

We see that $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$.

□