MATH 321: 9-17 AND 9-22 GROUPWORK

Having finished the section on logic, our next topic is about strategies for coming up with mathematical proofs. Before you write your own, however, I want you to look at an example of how to do it. We will look at a theorem from number theory, and analyze a proof of it. First we need to discuss some definitions. I have interspaced exercises for you to work out throughout the following, and your homework for this week will be to submit these exercises. In usual mathematical writing, you won't see exercises like this mixed in, as it breaks the flow of the writing. But you should ask yourself these kinds of questions when reading, constantly checking that you understand what's going on.

Before we start, one thing I want to emphasize is that when writing mathematical proofs, you never start from nothing. There are always known mathematical facts you use. For example, below we freely use some facts about arithmetic and natural numbers without actually proving them. Of course, if you desire you could prove those facts from even more basic principles, and you could try to reduce those to yet more basic principles. But you will always have to start with some given statements you didn't prove—call them axioms, if you like.

Definition. Let a and b be integers. Say that a *divides* b, written $a \mid b$, if there is an integer n so that $an = b$.

Exercise 1. *Write a logical formula with the free variables a and b which expresses $a \mid b$.*

Exercise 2. *Check that $a \mid 0$ and $a \mid a$ for any integer a. What are the witnessing integers n?*

Exercise 3. *Check that $a \mid b$ does not imply $b \mid a$ by coming up with a counterexample.*

Definition. Let a and b be integers. The *greatest common divisor* of a and b, written $\gcd(a, b)$ is the largest integer c so that $c \mid a$ and $c \mid b$.

Exercise 4. *Write a logical formula with free variables a, b, and c which expresses $c = \gcd(a, b)$. [Hint: you need to say more than $c \mid a$ and $c \mid b$.]*

Exercise 5. *Check that $\gcd(a, a) = |a|$. Check that if $a = 0$ and $b \neq 0$ then $\gcd(a, b) = |b|$. Explain why $\gcd(0, 0)$ is undefined.*

Theorem (Bézout's identity)**.** *For all integers a and b, with at least one of them nonzero, there are integers x and y so that $ax + by = \gcd(a, b)$.*

Exercise 6. *Write this theorem as a logical formula with no free variables.*

Exercise 7. *Find integers x and y which satisfy Bézout's identity for the following values for a and b:*

- $a = 3$, $b = 0$.
- $a = 6$, $b = 4$.
- $a = 6$, $b = 14$.

Proof. Fix arbitrary integers a and b with at least one of them nonzero. Without loss of generality, say that $a \neq 0$. Consider the set $X = \{n \in \mathbb{N} : n = ax + by \text{ for some integers } x, y\}$. This set is nonempty, because either a or $|a|$ is in it.

Exercise 8. *Write a logical formula which expresses $n \in X$.*

Exercise 9. *When is $a \in X$, versus when is $|a| \in X$? For both cases, determine the values of x and y which witness this.*

Because X is a nonempty subset of $\mathbb{N}$, it has a smallest element, call it $c_0 = ax_0 + by_0$. We will now check that $c_0 = \gcd(a, b)$. There are two things to check. First, we must check that $c_0 \mid a$ and $c_0 \mid b$. Second, we must check that c_0 is the largest number with this property.

We will only check that $a \mid c_0$. The argument that $b \mid c_0$ is similar. Let q and r be the unique integers with $0 \leq r < c_0$ so that $a = qc_0 + r$.

Exercise 10. *Why are there unique such q and r? [Hint: q stands for "quotient" and r stands for remainder.]*

Now do some algebra to get $r = a - qc_0$. By substitution we then get $r = a - q(ax_0 + by_0) = a(1 - qx_0) + by_0$. That is, we have seen that $r \in X \cup \{0\}$. But $r < c_0$ and c_0 is the smallest element of X, so $r \neq 0$. Thus $r = 0$. Substituting this back in we get $a = qc_0$. That is, $c_0 \mid a$, as desired.

Exercise 11. *Explain how to modify this argument to show $c_0 \mid b$.*

Now consider any integer c so that $c \mid a$ and $c \mid b$. We want to see that $c \leq c_0$. Fix the integers n and m so that $cn = a$ and $cm = b$. By substitution we then get $cnx_0 + cmy_0 = c_0$. A bit of algebra then gives $c(nx_0 + my_0) = c_0$. So $c \mid c_0$, whence we conclude $c \leq c_0$.

Exercise 12. *Come up with two integers k, ℓ so that $k \mid \ell$ but $k > \ell$.*

Exercise 13. *Fill in the missing detail for this last step. Why can we conclude $c \leq c_0$ from $c \mid c_0$ in this case?*

To summarize: we have seen that $\gcd(a, b) = c_0 = ax_0 + by_0$. That is, we have seen that there are integers x and y so that $ax + by = \gcd(a, b)$, completing the proof. □

Here is the same material, but without the exercises mixed in.

Definition. Let a and b be integers. Say that a *divides* b, written $a \mid b$, if there is an integer n so that $an = b$.

Definition. Let a and b be integers. The *greatest common divisor* of a and b, written $\gcd(a, b)$ is the largest integer c so that $c \mid a$ and $c \mid b$.

Theorem (Bézout's identity)**.** *For all integers a and b, with at least one of them nonzero, there are integers x and y so that $ax + by = \gcd(a, b)$.*

Proof. Fix arbitrary integers a and b with at least one of them nonzero. Without loss of generality, say that $a \neq 0$. Consider the set $X = \{n \in \mathbb{N} : n = ax + by \text{ for some integers } x, y\}$. This set is nonempty, because either a or $|a|$ is in it. Because X is a nonempty subset of $\mathbb{N}$, it has a smallest element, call it $c_0 = ax_0 + by_0$. We will now check that $c_0 = \gcd(a, b)$. There are two things to check. First, we must check that $c_0 \mid a$ and $c_0 \mid b$. Second, we must check that c_0 is the largest number with this property.

We will only check that $a \mid c_0$. The argument that $b \mid c_0$ is similar. Let q and r be the unique integers with $0 \leq r < c_0$ so that $a = qc_0 + r$. Now do some algebra to get $r = a - qc_0$. By substitution we then get $r = a - q(ax_0 + by_0) = a(1 - qx_0) + by_0$. That is, we have seen that $r \in X \cup \{0\}$. But $r < c_0$ and c_0 is the smallest element of X, so $r \neq 0$. Thus $r = 0$. Substituting this back in we get $a = qc_0$. That is, $c_0 \mid a$, as desired.

Now consider any integer c so that $c \mid a$ and $c \mid b$. We want to see that $c \leq c_0$. Fix the integers n and m so that $cn = a$ and $cm = b$. By substitution we then get $cnx_0 + cmy_0 = c_0$. A bit of algebra then gives $c(nx_0 + my_0) = c_0$. So $c \mid c_0$, whence we conclude $c \leq c_0$.

To summarize: we have seen that $\gcd(a, b) = c_0 = ax_0 + by_0$. That is, we have seen that there are integers x and y so that $ax + by = \gcd(a, b)$, completing the proof. □