More Examples on Proof Writing

Here are two more examples of simple proof–writing exercises. We will approach them in the manner of the "Tips on Proof Writing" handout.

Example 1. Prove: Let $a, b \in \mathbb{Z}$, and let $m > 0$ be an integer. Then

$$\gcd(ma, mb) = m \cdot \gcd(a, b).$$

Let's outline our plan of attack.

- What are we trying to prove? We need to show that $\gcd(ma, mb) = m \cdot \gcd(a, b)$. Our plan will be to show that $\gcd(ma, mb) \le m \cdot \gcd(a, b)$, and that $m \cdot \gcd(ma, mb) \le \gcd(ma, mb)$.
- What are the hypotheses? We are simply given that $a, b, m \in \mathbb{Z}$, and that $m > 0$.
- What theorems or definitions might be useful? We know that $d = \gcd(a, b)$ divides a and b, so md divides both ma and mb. Also, Bézout's lemma says that there are integers x and y satisfying
$$ax + by = d,$$
so
$$max + mby = md.$$
- Put it all together: $md \mid ma$ and $md \mid mb \implies md$ is a (positive) common divisor of $ma, mb \implies md \le \gcd(ma, mb)$. Also,
$$max + mby = md \implies \gcd(ma, mb) \mid md,$$
so $\gcd(ma, mb) \le md$. Thus $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Now we'll write it up.

Proof. Let $d = \gcd(a, b)$. Since d divides both a and b, md divides both ma and mb. Since $m > 0$, md is a positive common divisor of ma and mb, so it must be smaller than the greatest common divisor. That is, $md \le \gcd(ma, mb)$. Also, Bézout's lemma implies that there are integers x and y satisfying

$$ax + by = d.$$

Multiplying both sides by m, we get

$$max + mby = md.$$

Since $\gcd(ma, mb)$ divides both ma and mb, it divides the left side of this equation. Thus $\gcd(ma, mb)$ divides md, so we must have

$$\gcd(ma, mb) \le md.$$

Therefore, $md = \gcd(ma, mb)$, or $m \cdot \gcd(a, b) = \gcd(ma, mb)$. □

Example 2. Prove: The equation

$$ax + by = c$$

has integer solutions x and y if and only if $\gcd(a, b)$ divides c.
There are two directions here, so we need to handle them one at a time.

- For the first direction, what are we being asked to prove? We need to show that $\gcd(a, b)$ divides c.
- What are the hypotheses? We are given that there are integers x and y such that $ax + by = c$.
- What theorems or definitions might be useful? We'll use the definition of the greatest common divisor, namely that it dives a and b. If we let $d = \gcd(a, b)$, we can write

  $$a = ed \quad \text{and} \quad b = fd$$

  for some integers e and f.
- Now let's put it together.

  $$\begin{aligned} a = ed \quad \text{and} \quad b = fd &\implies c = ax + by = edx + fdy \\ &\implies c = d(ex + fy) \\ &\implies d \text{ divides } c \end{aligned}$$

- What do we need to do for the other direction? We assume that $\gcd(a, b)$ divides c, and we show that $ax + by = c$ has integer solutions.
- What can we use? First, if $d = \gcd(a, b)$ divides c, we can write $c = kd$ for some $k \in \mathbb{Z}$. Second, we have Bézout's lemma: there exist $x_0, y_0 \in \mathbb{Z}$ such that

  $$ax_0 + by_0 = d.$$

- Now put it together:

  $$\begin{aligned} ax_0 + by_0 = d &\implies kax_0 + kby_0 = kd = c \\ &\implies a(kx_0) + b(ky_0) = c \end{aligned}$$

  so we can take $x = kx_0$ and $y = ky_0$.

Now we'll try to write it up nicely.

Proof. Suppose first that there are integers $x, y \in \mathbb{Z}$ such that $ax + by = c$. Let $d = \gcd(a, b)$. Since d divides both a and b, there are integers $e, f \in \mathbb{Z}$ such that $a = ed$ and $b = fd$. Then

$$ax + by = edx + fdy = d(ex + fy).$$

But $ax + by = c$, so

$$c = d(ex + fy),$$

and d divides c.

Conversely, suppose that d divides c. Then there is an integer k satisfying $c = kd$. By Bézout's lemma, there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + by_0 = d.$$

Thus

$$k(ax_0 + by_0) = kd,$$

or

$$a(kx_0) + b(ky_0) = c.$$

If we set $x = kx_0$ and $y = ky_0$, then $ax + by = c$, so we are done. $\square$