You will prove on HW10:

Lemma: For any $a, b \in \mathbb{Z}$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Let's use this to prove:

Thm: For any $a, b, c \in \mathbb{Z}$ with $a \neq 0$, if $a \cdot b = a \cdot c$, then $b = c$.
[Multiplicative Cancellation]

Proof: Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Suppose $a \cdot b = a \cdot c$. Then

$$a \cdot b - a \cdot c = 0$$
$$a \cdot (b - c) = 0.$$

By the Lemma, $a = 0$ or $b - c = 0$. But $a \neq 0$, so $b - c = 0$.

That is, $b = c$. ∎

Note: No division required!
(And no division **defined** in $\mathbb{Z}$.)

Order Properties of $\mathbb{Z}$

Def: For $a, b \in \mathbb{Z}$, $a < b$ means $b - a \in \mathbb{N}$.

- $a \leq b$ means $a < b$ or $a = b$.
- $a > b$ means $b < a$.

Ex: $0 < a \iff a - 0 \in \mathbb{N} \iff a \in \mathbb{N}$.

Lemma: For any $a, b \in \mathbb{Z}$, exactly one of the following is true:

(i) $a < b$
(ii) $a = b$
(iii) $a > b$

Proof: Exercise.

[In other words, $\mathbb{Z}$ is <u>linearly ordered</u> by $<$.]

<u>Lemma</u>: Let $a, b, c \in \mathbb{Z}$.

1. If $a < b$, then $a + c < b + c$
2. If $a < b$ and $c > 0$, then $a \cdot c < b \cdot c$.

<u>Proof</u>: 1. Suppose $a < b$. Then $b - a \in \mathbb{N}$.
Since

$$(b+c) - (a+c) = b - a,$$

we have $(b+c) - (a+c) \in \mathbb{N}$.
That is,

$$a + c < b + c.$$

2. Suppose $a < b$ and $c > 0$. Then
$b - a \in \mathbb{N}$ and $c \in \mathbb{N}$.
By Positive Closure, $(b-a) \cdot c \in \mathbb{N}$.
By the Distributive Law,

$$b \cdot c - a \cdot c \in \mathbb{N},$$

i.e. $a \cdot c < b \cdot c$.

$\blacksquare$

The Well-Ordering axiom (#10) is the only one we haven't used yet. It says that any non-empty subset of $\mathbb{N}$ has a <u>smallest element</u>.

An element $a \in S$ is the <u>smallest element</u> of S if for all $x \in S$, $a \leq x$.

In symbols: $(\forall x \in S)(a \leq x)$

Observe that a smallest element in S, if it exists, is unique.

$$(\forall x \in S)(a \leq x) \text{ and } (\forall x \in S)(b \leq x)$$

implies $a \leq b$ and $b \leq a$, so $a = b$.

<u>Lemma</u>: The integer 1 is the smallest element of $\mathbb{N}$.

<u>Proof</u>: First, we know $\mathbb{N}$ has a smallest element by the Well-Ordering axiom. Call it a.

Since $a \leq n$ for every $n \in \mathbb{N}$, we have $a \leq 1$. Therefore $a = 1$ or $a < 1$. If $a = 1$, we are done.

To show $a < 1$ is false, we will assume it's true and derive a contradiction.

Formally, if $P \Rightarrow$ (a false statement) is true, then it must be that P is false.

So assume $a < 1$. Because $a \in \mathbb{N}$, $0 < a$.

Multiply the inequality $a < 1$ by $a > 0$ to get

$$a \cdot a < 1 \cdot a = a.$$

Now, $a \cdot a \in \mathbb{N}$ by Positive Closure, which contradicts a being the smallest element of $\mathbb{N}$.

Thus, our assumption that $a < 1$ is false, so $a = 1$. $\blacksquare$

This actually shows that the integers are what you think they are:

- We know $0, 1 \in \mathbb{Z}$ by the Identity axiom.

- We also know
$$\begin{aligned} 1+1 &= 2 \\ 2+1 &= 3 \\ 3+1 &= 4 \\ &\vdots \end{aligned}$$

  are positive integers.

  If there was another positive number x not on this list, then it would satisfy $n < x < n+1$ for some $n \in \mathbb{N}$. But then $0 < x - n < 1$, which violates the theorem.

- The only other integers, by Trichotomy, satisfy $-a \in \mathbb{N}$. That is, they are the additive inverses of elements in $\mathbb{N}$.

Together, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Note: The handout shows this slightly more rigorously, by proving the Principle of Mathematical Induction.