<u>Goal</u>: Check that the axioms for $\mathbb{Z}$ define the integers we think we know, i.e.,

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

The key is Axiom 10, the only one we haven't used yet. It is

<u>The Well-Ordering Principle</u>

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 $a \leq x$ for all $x \in S$.

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

<u>Observation</u>: A smallest element in S, if it exists, must be unique:

$(\forall x \in S)(a \le x)$ and $(\forall x \in S)(b \le x)$

imply $a \le b$ and $b \le a$, so $a = b$.

<u>Thm 11</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 Principle (Axiom 10).

Call it $a \in \mathbb{N}$.

We also know $1 \in \mathbb{N}$ (Lemma 6). So $a \le 1$, because a is the smallest element in $\mathbb{N}$.

To get a contradiction, assume that $a \neq 1$. Then $a < 1$.

Because $a \in \mathbb{N}$ (i.e. $a > 0$), we can multiply both sides of $a < 1$ by a to get

$$a \cdot a < 1 \cdot a \qquad \text{(Lemma 10)}$$

or

$$a^2 < a.$$

But $a^2 = a \cdot a \in \mathbb{N}$ by Positive Closure (Axiom 8), so this contradicts a being the smallest element in $\mathbb{N}$.

Thus, $a = 1$, as desired. $\blacksquare$

This actually completes our goal!
Why?

- $0, 1 \in \mathbb{Z}$ by Axiom 5
- $1 \in \mathbb{N}$ by Lemma 6
- Thus,
$$\begin{aligned} 1+1 &= 2 \\ 2+1 &= 3 \\ 3+1 &= 4 \\ &\text{etc.} \end{aligned}$$
are in $\mathbb{N}$ by Axiom 8.

So $\mathbb{N}$ contains $\{1, 2, 3, 4, \ldots\}$.

If there were another $x \in \mathbb{N}$ not on this list, then we would have

$$n < x < n+1$$

for some $n \in \mathbb{N}$. But then $0 < \underbrace{x-n}_{\in \mathbb{Z} \text{ (Axiom 1)}} < 1$, contradicting Thm 11. ✓

So $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.

Now, by Trichotomy (Axiom 9), the only other integers are the additive inverses of elements of $\mathbb{N}$.

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

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

Divisibility

Def: Let d and n be integers. We say <u>d divides n</u> if there exists an integer k such that $n = dk$.

Note on definitions: A definition is a $\Leftrightarrow$ statement, but it is often written as a $\Rightarrow$ statement.

So

$$d \text{ divides } n \Leftrightarrow (\exists k \in \mathbb{Z})(n = dk)$$

Notation: $d \mid n$ means "d divides n"

Ex: $2 \mid n \Leftrightarrow n = 2k$ for some $k \in \mathbb{Z}$

$\Leftrightarrow n$ is even.

Ex: $3 \mid n \Leftrightarrow n = 3k$ for some $k \in \mathbb{Z}$

So 3 divides 3 $(3 = 3 \cdot 1)$

" " 9 $(9 = 3 \cdot 3)$

" " -6 $(-6 = 3 \cdot (-2))$

" " 0 $(0 = 3 \cdot 0)$

Def: When $d \mid n$, we say d is a <u>divisor</u> of n and n is a <u>multiple</u> of d.