This week we will be continuing with the topic from last week so that the class can get a little ahead of discussion. Typically, I will try to keep discussion running one week behind. The professor asked me to cover one topic from the third week, so I will present that first, then we will go back to induction and well-ordering.

Just to make sure that everyone remembers, \( \mathbb{R}^+ = \{ x \in \mathbb{R} : x \geq 0 \} \).

**Problem.** (25.) We would like to find a function \( f \) so that there exists \( g \) with \( g \circ f = I \) but so that there is no function \( h \) with \( f \circ h = I \).

The basic idea behind this is that there are two properties required for a function to have an inverse. If \( f : A \to B \) then for \( f \) to have a left inverse, we require that \( f \) be injective. Injectivity means that \( f \) maps distinct values to distinct values. For example, \( f(x) = x^2 \) is not injective from \( \mathbb{R} \to \mathbb{R} \): \( 1^2 = (-1)^2 = 1 \). Notice, however, that if we only consider positive values (that is, we think of \( f \) as a function from \( \mathbb{R}^+ \) to \( \mathbb{R} \), then \( f \) is injective: we can identify \( x \) if we know \( x^2 \).

Surjectivity means that \( f \) actually achieves every value in \( B \). The big issue here is that when we try to define \( f^{-1} : B \to A \) we need \( f^{-1} \) to be a function—it won’t be if \( f^{-1} \) is not defined on all of \( B \). We can see that \( f(x) = x^2 \) is also not surjective from \( \mathbb{R} \to \mathbb{R} \), since \( f(x) = x^2 \geq 0 \). We can always fix this problem by changing our domain or range. In this case, if we think of \( f(x) = x^2 \) as a function from \( \mathbb{R} \) to \( \mathbb{R}^+ \) then it is surjective, but not injective. If we think of it as a function from \( \mathbb{R}^+ \) to \( \mathbb{R} \) then it is injective but not surjective. Finally, if we think of \( f(x) = x^2 \) as a function from \( \mathbb{R}^+ \) to \( \mathbb{R}^+ \) then it is both injective and surjective and its inverse function is \( f^{-1}(x) = \sqrt{x} \) since \( \sqrt{x^2} = x = \sqrt{x^2} \) for \( x \geq 0 \).

Let’s turn this into an example for this problem. We can see that if \( f(x) = x^2 \) where we think of \( f \) as a function from \( \mathbb{R}^+ \) to \( \mathbb{R} \) then for \( g(x) = \sqrt{x} \) we have \( f \circ g(x) = (\sqrt{x})^2 = x \) for every \( x \in \mathbb{R}^+ \). Notice, however, that for any function \( h \) since \( f(h(x)) \geq 0 \) for any \( x \), we have \( f(h(x)) \neq -1 \) for all \( x \in \mathbb{R}^+ \). Therefore there is no function \( h \) with \( f(h(-1)) = -1 \).

**Well-Ordering and Induction.** Last week we talked about the two equivalent ideas of induction and well-ordering. This week, we will do a few examples of converting between those ideas as well as becoming more acquainted with how to use the well-ordering principle. We begin with a statement of well ordering in the context that we will use it:
**Definition.** (Well Ordering) The natural numbers are well-ordered. That is, every subset $S \subseteq \mathbb{N}$ has the property that there exists $x \in S$ so that $x \leq y$ for all $y \in S$.

The professor showed in class how to prove that this principle is equivalent to the principle of weak induction. One of the homework problems for last week was to show that well-ordering implies strong induction as well, so we will start with that as an example:

**Definition.** A set $S \subseteq \mathbb{N}$ is said to be strongly inductive if the following two properties hold:

- $1 \in S$
- $1, \ldots, n \in S \implies n + 1 \in S$

The principle of strong induction is that if $S$ is strongly inductive then $S = \mathbb{N}$

**Example.** Well ordering implies the principle of strong induction.

**Proof.** Suppose that $S$ is a strongly inductive set and $S \neq \mathbb{N}$. Then since $S \subseteq \mathbb{N}$ and $S^c \subseteq \mathbb{N}$ (which is notation for the set of all things in $\mathbb{N}$ that are not in $S$) is not empty there is a minimal $k \in S^c$. Notice that $k \neq 1$ (since we know that $1 \in S$) and so $\{1, \ldots, k - 1\}$ is not empty. But $k$ is minimal and therefore $\{1, \ldots, k - 1\} \subseteq S$. The second hypothesis of $S$ being strongly inductive implies that $k \in S$, which is a contradiction since we know that $k \in S^c$ (which is the same as saying $k \in \mathbb{N}$ and $k \notin S$).

Typically, this is how you should try to use well ordering. To prove a proposition $P$, consider the set of numbers for which the proposition fails, select a minimal element of that set, and get a contradiction. Very often, the contradiction will be showing that you could construct a smaller counterexample, as is the case here:

**Example.** Show that any fraction $\frac{n}{m}$ with $n, m \in \mathbb{N}$ can be written in reduced form (i.e. so that $n$ and $m$ are coprime).

**Proof.** Suppose that there exists a number $k \in \mathbb{Q}$ so that $k$ cannot be written in reduced form and let $S = \{n : \exists m \in \mathbb{N} \text{ so that } \frac{m}{n} \text{ cannot be written in reduced form}\}$. Since $S$ is nonempty, $S$ has a smallest element, call it $n_0$. By definition of $S$ there is $m_0$ so that $\frac{m_0}{n_0}$ cannot be written in reduced form, i.e. $n_0$ and $m_0$ are not coprime. Call their common factor $p > 1$ (the fact that $p$ is greater than one is part of the definition of coprime). Then

$$\frac{m_0}{n_0} = \frac{m_0}{m_0} \cdot \frac{\frac{m_0}{n_0}}{\frac{m_0}{n_0}}.$$

But observe that by hypothesis we have $\frac{m_0}{p} \in \mathbb{N}$ and $\frac{m_0}{p} \in \mathbb{N}$ and $\frac{m_0}{p} < n_0$. These two fractions are equal and therefore neither can be written in reduced form (because of how we chose $n_0$ and $m_0$). Therefore $\frac{m_0}{p} \in S$, which is a contradiction.
since we chose $n_0$ to be minimal in $S$ (the contradiction here is that $\frac{n_0}{p} < n_0$ when we know that $n_0$ satisfies $n_0 \leq k \forall k \in S$).

Before moving on to some problems, I just want to do one more classical example of how to use the well-ordering principle to do a proof.

**Example.** Show that every $k \in \mathbb{N}$ can be written as a product of primes $k = \prod_{i=1}^{n} p_i$.

*Proof.*** Suppose that there exists a number that cannot be written as a product of primes and define the set $C = \{ k \in \mathbb{N} : \text{k cannot be written as a product of primes} \}$. By hypothesis, $C \neq \emptyset$ so we may take $k_0$ minimal in $C$. Notice that $k_0$ cannot be prime, since if it were it would be a product of primes. Therefore there exist $l, m$ with $1 < l, m < k_0$ so that $k_0 = l \cdot m$. But by minimality of $k_0$ it must be the case that $l = \prod_{i=1}^{n_l} p_{i,l}$ and $m = \prod_{i=1}^{n_m} p_{i,m}$ and therefore $k = \prod_{i=1}^{n_l} p_{i,l} \prod_{i=1}^{n_m} p_{i,m}$ (the extra subscripts here are just to keep track of the fact that the primes we use to write out $l$ depend on $l$ and the primes we use to write out $m$ depend on $m$), which contradicts our assumption that $k$ cannot be written in this form.

**Problem.** Prove that $\forall n \in \mathbb{N}$ with $n \geq 12, \exists k, m \in \mathbb{N}$ so that $n = 4m + 5k$ using the well-ordering principle.

*Proof.*** Suppose that there exists $k \geq 12$ that cannot be written as $4m + 5k$ for natural numbers $m, k$. We can compute that $12 = 4 \cdot 3, 13 = 4 \cdot 2 + 5 \cdot 1, 14 = 4 \cdot 1 + 5 \cdot 2$ and $15 = 5 \cdot 3$. Define $C = \{ k : \text{k cannot be written as $4m + 5k$ for natural numbers $m, k$} \}$. Our hypothesis gives that $C \neq \emptyset$ so we may take $k_0$ minimal in $C$. $k_0 \geq 16$ so $k_0 - 4$ must satisfy $k_0 - 4 = 4m + 5k$ for some $m, k$ and therefore $k_0 = 4(m + 1) + 5k$, a contradiction.

**Problem.** Show that $3|2^{2n} - 1$ for $n \geq 1$ (using whatever you want)

*Proof.*** I am doing all of these with well-ordering just to give more examples of proofs in this style. This problem looks nicer with induction.

Since $3|3$ we know the result holds for $n = 1$. Let $C = \{ n : 2^{2n} - 1 \text{ is not divisible by } n \}$ and suppose that $C$ is nonempty. Then $C$ has a smallest element, call it $n_0$ and notice that $n_0 > 1$. In particular then $2^{2(n_0-1)} - 1 = 3k$ for some $k \in \mathbb{N}$ so $2^{2^{n_0}} = 4(3k + 1) = 3 \cdot (4k + 1) + 1$ and therefore $2^{2^{n_0}} - 1 = 3 \cdot (4k + 1)$, a contradiction.

**Problem.** Show that every $n \in \mathbb{N}$ is either even or odd.

*Proof.*** Notice that 1 is odd and suppose that the set $C = \{ n \in \mathbb{N} : n \text{ is neither even nor odd} \}$ is nonempty. Then it has a least element $n_0 > 1$. Then $n_0 - 1 \in \mathbb{N}$ is either even or odd. If it is even, $n_0 - 1 = 2m$ for some integer $m$ and therefore $n_0 = 2m + 1$ is odd, a contradiction. But if $n_0 - 1 = 2m + 1$ for some integer $m$ then $n_0 = 2(m + 1)$ is even, a contradiction. Since we reach a contradiction in either case, we conclude that $C$ is empty.
**Problem.** Show that $\sqrt{20}$ is irrational.

**Proof.** Suppose that $\frac{a}{b} = \sqrt{20}$ where $\frac{a}{b}$ is in reduced form. Then $\frac{a^2}{b^2} = 20$ and $a^2 = 20b^2$. Then $2|a$ and $5|a$, so we can write $a = 2n$ where $a \in \mathbb{N}$. This now reads $(2n)^2 = 20b^2$ so $n^2 = 5b^2$ and $n$ and $b$ are still coprime. Notice that $5|n$ so we can write $n = 5k$ and this becomes $(5k)^2 = 5b^2$ or, after dividing by 5, $5k^2 = b^2$. Therefore $5|b$, a contradiction since this implies $a$ and $b$ are not coprime. $\square$