I had a request to do a couple homework problems before we move on, so here are they are:

**Problem.** (1. iii.) If \( x^2 = y^2 \) then \( x = y \) or \( x = -y \).

*Proof.* Rewrite \( x^2 = y^2 \) as \( x^2 - y^2 = 0 \) and use the previous part of the problem to obtain \( (x - y)(x + y) = 0 \). The book proves that if \( ab = 0 \) then \( a = 0 \) or \( b = 0 \), but the proof is easy: suppose \( b \neq 0 \). Then \( (ab) \cdot b^{-1} = 0 \cdot b^{-1} = 0 \) so \( a = 0 \). □

**Problem.** (3. i.) If \( b, c \neq 0 \) then \( \frac{a}{b} = \frac{ac}{bc} \).

*Proof.* Write \( \frac{a}{b} = ab^{-1} = a \cdot 1 \cdot b^{-1} = a \cdot c \cdot c^{-1} \cdot b^{-1} = (a \cdot c)(bc)^{-1} = \frac{ac}{bc} \). □

**Order in \( \mathbb{R} \)**

The two fields we encounter the most in applications are the real and complex numbers. The biggest difference (in my opinion anyway) between these two is that although the complex numbers are closed under roots (for example, for every complex \( x \) there is a number \( y \) so that \( y^2 = x \)) the reals are ordered. That is for any real numbers we have \( a < b \) \( a = b \) or \( a > b \). The remaining axioms describe the property of the reals as an ordered field: there is a set \( P \) with the following properties.

- (P10) Trichotomy: Exactly one of the following holds: i.) \( a = 0 \), ii.) \( a \in P \) or iii.) \( -a \in P \).
- (P11) If \( a, b \in P \) then \( a + b \in P \)
- (P12) If \( a, b \in P \) then \( a \cdot b \in P \)

These properties distinguish the reals from the complex numbers. There is another property that distinguishes the real numbers from the rationals, which we will discuss later. For now, we can use this definition of positive numbers to define the order on \( \mathbb{R} \). We say that \( a > b \) if \( a - b \in P \), \( a = b \) if \( a - b = 0 \) and \( a < b \) if \( -(a - b) \in P \).

**Claim.** If \( a > b \) and \( b > c \) then \( a > c \).

*Proof.* \( a - b \in P \) and \( b - c \in P \) so \( (a - b) + (b - c) \in P \) by (P11). But then \( a + ((-b + b) - c) = a - c \in P \) and so \( a > c \). □
Induction

Mathematical induction is basically a formal version of arguments that read “and keep doing the same thing until you get to this case”. We can think of it as providing someone else with an algorithm for solving a recursive problem. You provide them with a first step, then tell them how to proceed from one step to the next. There are two parts to a proof by induction: the base case and the induction step. The base case is where you show that your 'algorithm' actually runs when you start it. The induction step then tells the other person how to proceed from one case to the next. We will begin with a very simple example of a proof by induction:

Example. $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof. Base case ($n = 1$) then $1 + 2 = 3 - 1 = 2^{1+1} - 1$. So the base case is true.

Induction step: Suppose we know that the result holds for $n$ (That is, suppose we know that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$). We want to show that $\sum_{i=0}^{n+1} 2^i = 2^{(n+1)+1} - 1$.

Then

$$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1}$$

Now we use the 'induction hypothesis' that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ to write this as

$$2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{(n+1)+1} - 1$$

which is what we wanted to show. □

Remark. If you want to, you can think of the induction step as a machine that lets us pass from the case of $n = 1$ (which we proved) to $n = 2$ and then from $n = 2$ to $n = 3$ and so on. The only thing that matters here is that we do it abstractly (never writing out $n = 2$) so that we don’t have to do a bunch of extra work. Remember though: when we say “assume the induction hypothesis” we are not actually assuming anything. It just means that you plug one of the cases you have already proven into the machine, let it run, then plug the result back in.

Remark. It is very important to prove the base case. Notice that if we forget to do this, we could 'prove' that

$$\sum_{i=10}^{n} 2^i = 2^{n+1} - 1$$

since the induction hypothesis ($\sum_{i=10}^{n} 2^i = 2^{n+1} - 1$) would give

$$\sum_{i=10}^{n+1} 2^i = \sum_{i=10}^{n} 2^i + 2^{n+1} = 2(2^{n+1}) - 1 = 2^{(n+1)+1} - 1$$

The reason that this 'proof by induction' fails is that we only gave the step that lets us pass from one case to the next: we never proved that it works for even one case. If you think of this like an algorithm, that says that it never initializes.
Sums like the one above are particularly well suited to induction, because the definition of the sum is recursive (recursion and induction are really two sides of the same idea):

\[ \sum_{i=1}^{n+1} a_i = a_{n+1} + \sum_{i=1}^{n} a_i \]

Another class of examples particularly well suited to induction proofs are inequalities involving natural numbers:

**Example.** \( n < 2^n \)

**Proof.** Base Case: \( n = 1 \): Since \( 1 < 2^1 \), the result holds for \( n = 1 \).

Induction Step: Suppose the result holds for \( n \) (that is, suppose we know that \( n < 2^n \)). We want to show that \( n+1 < 2^{n+1} \). By the induction step \( n+1 < 2^n + 1 \) and since \( 1 < 2^n \) for \( n \geq 1 \) we have that \( 2^n + 1 < 2 \cdot 2^n = 2^{n+1} \) and therefore \( n + 1 < 2^{n+1} \). □

**Example.** Suppose that coins come in denominations of 4 cents and 5 cents. Show that you can make change for any amount of money greater than 11 cents.

(Formally, show that every integer \( n \geq 12 \) can be written as \( n = 4m + 5k \) for \( m, k \in \mathbb{N} \))

**Proof.** The idea behind this proof is to write \( n = (n - 4) + 4 \) and then use the induction hypothesis on \( n - 4 \). Because we are going to need to go back 4 numbers, we need to use the strong version of induction we talked about in class. For strong induction, you sometimes need more than one base case (in our case, we will need 4 so that our algorithm can start with 16 and then move on).

Base Cases: \( 12 = 3 \cdot 4, 13 = 2 \cdot 4 + 5, 14 = 2 \cdot 5 + 4, 15 = 3 \cdot 5 \)

Induction step: Suppose that for \( 12 \leq p \leq n \) we can write \( p = 4m + 5k \) for \( m, k \in \mathbb{N} \). Then \( n + 1 = (n - 3) + 4 \). Since \( n - 3 \) satisfies the induction hypothesis or is one of 12, 13, or 14 we can write \( n - 3 = 4m + 5k \) and therefore \( p = 4(m + 1) + 5k \). □

**Example.** \( a^{n+m} = a^n a^m \) for all \( n, m \in \mathbb{N} \)

**Proof.** This is a little trickier because we have two variables. What we want to do is simultaneously induct on both variables and there are a couple ways to do this. Before actually doing the induction though, think about it intuitively. We need to show that \( a^2 = a \cdot a \) and that we can increase the powers one at a time while keeping equality. Pictorially we want to show that we can go

\[ a^2 = a \cdot a \mapsto a^{n+1} = a^n \cdot a \mapsto a^{n+m} = a^n \cdot a^m \]

These correspond to the three parts of this induction: we first show the base case, then show the induction step for \( n \) with \( m = 1 \), then show the induction step for \( m \) with \( n \) fixed, but arbitrary.

Base Case: \( a^2 = a \cdot a \) is a definition, so that holds.
Induction Step 1: Suppose that $a^n \cdot a = a^{n+1}$. We want to show that $a^{n+2} = a^{n+1} \cdot a$, which is actually the definition.

Induction Step 2: Suppose that $a^n \cdot a^m = a^{n+m}$. We want to show that $a^n a^{m+1} = a^{n+m+1}$. We know that $a^{n+1} = a^m \cdot a$ and that $a^n \cdot a^m = a^{n+m}$ so we have

$$a^n a^{m+1} = a^n \cdot a^m \cdot a = a^{n+m} \cdot a = a^{n+m+1}$$

which completes the induction. □

**Problem.** Show that

$$\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$$

**Proof.** The base case $n = 1$ is that $1 \cdot 2 = \frac{1(2)(3)}{3}$. Now we assume the induction step $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

$$\sum_{i=1}^{n+1} i(i+1) = \sum_{i=1}^{n} i(i+1) + (n+1)(n+2)$$

$$= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2)$$

$$= \frac{(n+1)(n+2)(n+3)}{3}$$ □

**Problem.** Show that for $n \geq 4$ (pay attention to the base case here!)

$$2^n \geq n^2$$

**Proof.** As someone noticed in the first class, this is substantially easier to do by strong induction. We observe that if

$$2^n \geq n^2$$

then multiplication by 4 gives that

$$2^{n+2} \geq (2n)^2$$

since for $n \geq 4$ we have $2n \geq n + 2$ this implies

$$2^{n+2} \geq (n + 2)^2$$ □

To make this formal, we now proceed by strong induction. Because we go back two steps, we need two base cases.

Base Cases: If $n = 4$ or 5 then $16 = 16$ and $32 > 25$ so the base cases hold.

Inductive Step: Assume the result for $4 \leq p \leq n$ and consider that by the same computation as above

$$2^{n+1} = 2^{(n-1)+2} = 4 \cdot 2^{n-1} \geq 4(n - 1)^2$$
\[(2n - 2)^2 \geq (n + 1)^2\]

**Problem.** Show that if \(a_i \leq b_i \) for \(i = 1, \ldots, n\) then \(\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i\).

**Proof.** The base case \(a_1 \leq b_1\) is given, so assume the induction hypothesis \(\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i\).

\[
\sum_{i=1}^{n+1} a_i = \sum_{i=1}^{n} a_i + a_{n+1} \leq \sum_{i=1}^{n} b_i + a_{n+1}
\]

\[
\leq \sum_{i=1}^{n} b_i + b_{n+1} = \sum_{i=1}^{n+1} b_i
\]

\(\square\)