Three Sample Proofs

1 An Induction Proof

Recall that induction is a method to prove statements that apply to all integers n starting at some initial value n_0, i.e. to all integers $n \geq n_0$. Every induction proof requires proof of two statements:

1. *Base case*: prove the statement for the starting value, i.e. the smallest value n_0 for which the statement is asserted to be true. This can generally be done with simple arithmetic.
2. Assuming the *induction hypothesis* which is the claimed statement for some integer $k \geq n_0$, prove it for $k + 1$. (For so-called "strong" induction, the induction hypothesis is not only assumed for k, but for all the integers between n_0 and k.) This is the *induction step* and is the part of the induction proof that requires thought and work.

Problem. Prove that $n! > 3^n$ for all integers $n \geq 7$.

Answer. First, a side note on the initial value $n_0 = 7$. A quick bit of arithmetic reveals that $n! \leq 3^n$ for $0 \leq n \leq 6$, so the statement $n! > 3^n$ is false for $0 \leq n \leq 6$.

The base case asserts that $n! > 3^n$ for $n = 7$, which is easily seem to hold by substituting $n = 7$: $7! = 5040$ and $3^7 = 2187$, so $7! > 3^7$.

Our induction hypothesis asserts that $k! > 3^k$ for some $k \geq 7$. Assuming that this holds, we wish to prove that $(k + 1)! > 3^{k+1}$. When we prove this, our first (informal!) attempt should be to "work backwards" from our assertion $(k+1)! > 3^{k+1}$ and manipulate this inequality in a way that we can somehow "recognize" the assumed induction hypothesis in the modified expression and then use it to prove or claim.

In our case, we note that $(k + 1)! = (k + 1)k!$ and $k!$ is a quantity that appears in the induction hypothesis. Similarly, $3^{k+1} = 3 \cdot 3^k$ and 3^k appears in the induction hypothesis. So let's try this, starting with what we want:

$$(k + 1)! > 3^{k+1}$$
$$(k + 1)k! > 3 \cdot 3^k$$

By the induction hypothesis. $k! > 3^k$. Happily, $k + 1$ is also bigger than 3 for our range of k values, namely $k \geq 7$. So this will work, and we are now ready to write our proof formally. We have already proved the base case, so we only need to perform the induction step.

Induction hypothesis: Assume that $k! > 3^k$ for some $k \geq 7$.

Induction Claim: Prove that $(k + 1)! > 3^{k+1}$.

Proof. We have $(k+1)! = (k+1)k!$. By induction hypothesis, $k! > 3^k$. It is also clear that $k+1 > 3$ when $k \geq 7$ because $k + 1 \geq 7 + 1 = 8 > 3$. Hence

$$(k + 1)! = (k + 1)k! > (k + 1)3^k > 3 \cdot 3^k = 3^{k+1} ,$$

where the first inequality follows from the induction hypothesis and the second inequality follows because $k + 1 > 3$ when $k \geq 7$.

By induction, we conclude that $n! > 3^n$ for all $n \geq 7$. □

2 A Proof By Contradiction

A proof by contradiction is set up as follows. Suppose you wish to prove some statement P. Then you assume the opposite, i.e. the negation $\neg P$. If P is true (which you wish to prove), then $\neg P$ is false. Starting at $\neg P$, you apply deductive reasoning to obtain a sequence of statements until one of them is evidently false. *A priori*, you don't know what this false statement will be and how it comes about. But it represents a contradiction to your original assumption that $\neg P$ holds. You conclude that $\neg P$ is false, and hence P is true.

Problem. For all positive real numbers x, y with $x \neq y$, prove that $\dfrac{x}{y} + \dfrac{y}{x} > 2$.

To prove this statement by contradiction, we need to assume its negation. The statement has the form "for all ...", followed by an inequality using ">". For the negation, the "for all" becomes "there exist" and the ">" changes to "≤". So we assume that

> There exist real numbers x, y with $x \neq y$ such that $\dfrac{x}{y} + \dfrac{y}{x} \leq 2$

and derive a contradiction. We manipulate the inequality above via a sequence of mathematically equivalent inequalities until one of them is false and hence generates a contradiction. This contradiction is to our assumption that there exist distinct positive real numbers x, y such that $x/y + y/x \leq 2$. So then that assumption must be false; hence its negation is true. This then proves the original problem statement, namely that for all distinct positive real numbers x, y, the inequality $x/y + y/x > 2$ holds.

Note that when assuming the negation of our problem statement, we are not allowed to make any assumptions about x and y (other than that they are distinct positive real numbers as assumed). We just know that they exist, but nothing more.

Proof. Assume there exist real numbers x, y with $x \neq y$ such that $\dfrac{x}{y} + \dfrac{y}{x} \leq 2$. Then we have the following sequence of logical equivalences:

$$\begin{aligned} & \frac{x}{y} + \frac{y}{x} \leq 2 & \\ \iff \quad & x^2 + y^2 \leq 2xy & \text{(multiply the inequality by } xy\text{)} \\ \iff \quad & x^2 - 2xy + y^2 \leq 0 & \text{(subtract } 2xy \text{ on both sides)} \\ \iff \quad & (x-y)^2 \leq 0 & \text{(binomial theorem)} \end{aligned}$$

Now the left hand side of the last inequality is a square of a real number and hence non-negative, i.e. $(x-y)^2 \geq 0$. The inequality asserts that $(x-y)^2 \leq 0$. These two conditions are simultaneously satisfied if and only if $x - y = 0$, or equivalently, if and only if $x = y$. But be assumed that $x \neq y$. So this is a contradiction. So our initial assumption (in the first sentence of the proof) is false. Hence its negation is true, so our original problem statement is true. □

One final subtle point. In moving from the first inequality above to the second, we multiply both sides by xy. Recall that inequalities are preserved when multiplying by positive numbers, "flip" (i.e. ">" changes to "<" and vice versa) when multiplied by negative numbers, and become the useless identity $0 = 0$ when multiplied by 0. In this case, we multiply by xy which is a positive real number because both x and y are positive real numbers. So the first and second inequalities above are indeed equivalent.

3 A Proof Via Contrapositive

Recall for an implication $A \Rightarrow B$, where A and B are statemens, the *contrapostive* is the implication $\neg B \Rightarrow \neg A$ where $\neg P$ is the negation of a statement P. The contrapositive is logically equivalent to the original implication; that is, the implication $A \Rightarrow B$ is true if and only if its contrapostive $\neg B \Rightarrow \neg A$ is true. Sometimes it is easier to prove the contrapositive rather than the original implication.

Recall that for two integers a, n with n non-zero, n is said to *divide* a if there exits $r \in \mathbb{Z}$ such that $a = rn$. (Intuitively, this is saying that the quotient a/n is an integer, denoted r here.) We use the notation $n \mid a$ to mean that n divides a and $n \nmid a$ to mean that n does not divide a.

Problem. Let a, b, n be integers with $n \neq 0$. Prove that $n \nmid ab$ implies $n \nmid a$ and $n \nmid b$.

Answer. In general, it is easier to prove a statement that is true (such as one integer dividing another) than one that is not true (e.g. some integer does not divide another). So let's try proving the contrapositive instead. Our implication has the form $A \Rightarrow B \wedge C$, where $\wedge$ denotes logical "and". So the contrapositive is $\neg(B \wedge C) \Rightarrow \neg A$. Recall that negation changes "and" to "or", so the contrapositive implication becomes $\neg B \vee \neg C \Rightarrow \neg A$, where $\vee$ denotes logical "or". So instead of proving our original implication, let's prove its contrapositive:

> Let a, b, n be integers with $n \neq 0$. Prove that $n \mid a$ or $n \mid b$ implies $n \mid ab$.

Let's write down what our assumption and our assertion mean. We are assuming $n \mid a$ or $n \mid b$. $n \mid a$ means that there exists $r \in \mathbb{Z}$ with $a = rn$, $n \mid b$ means that there exists $s \in \mathbb{Z}$ with $b = sn$, and $n \mid ab$ means that there exists $t \in \mathbb{Z}$ with $ab = tn$. At least one of $n \mid a$ or $n \mid b$ is assumed, so at least one of r or s exists. We need to infer the existence of t from this.

So how to you get from a statement about a to a statement about ab? You multiply the statement about a by b. So if $a = rn$, then $ab = (rn)b = (rb)n$. Hence, we can chose t to be $t = bn$ and thus guarantee the existence of t, given that r exists. Analogous reasoning gets us from $n \mid b$ to $n \mid ab$. Now we are ready for our formal proof.

Proof. Suppose first that $n \mid a$. Then there exists $r \in \mathbb{Z}$ such that $a = rn$. Multiplying this equality by b yields $ab = (rn)b = (rb)n$. Since rn is an integer, it follows that $n \mid ab$.

An analogous argument holds under the assumption that $n \mid b$. In this case, there exists $s \in \mathbb{Z}$ such that $b = sn$. Then $ab = a(sn) = (as)n$. Since as is an integer, $n \mid ab$. □