Proof Techniques

The majority of UNLV students have never written a proof. We need to change that, at least for this class! I will assume that you understand elementary rules of logic.

Proof by Contradiction

To prove a statement P by contradiction, we first assume P is false, then proceed logically until we reach a conclusion that is false. This will proves that P is true.

The proof, by contradiction, that $\sqrt{2}$ is irrational, is at least 2400 years old. It is said that existence of irrationals caused serious consternation among the Pythagorians, an ancient Philosophical school. One problem is that an important proof in Euclid, out of which I studied geometry, assumes that all numbers are rational. Since our book was printed in modern times, it apologized for this assumption, stating that there is a modern proof that does not use the assumption, but did not give it; it is not likely that many high school students would be able to grasp this modern proof.

Recall that a *rational* number is a number that can be written as a fraction $\frac{p}{q}$ reduced to the lowest terms, that is, p and q are integers whose greatest common divisor is 1.

Theorem 1 *There is no rational number whose square is 2.*

Proof: Assume that there is some fraction $\frac{p}{q}$, reduced to the lowest terms, which is equal to the square root of 2. Then:

$$\begin{aligned}
\sqrt{2} &= \frac{p}{q} \\
2 &= \frac{p^2}{q^2} \\
2q^2 &= p^2 \text{ thus } p^2 \text{ is even} \\
& \text{Thus } p \text{ is even} \\
p &= 2k \text{ for some integer } k \\
p^2 &= 4k^2 \\
2q^2 &= 4k^2 \\
q^2 &= 2p^2 \text{ thus } q^2 \text{ is even} \\
& \text{Thus } q \text{ is even}
\end{aligned}$$

Since p and q are both even, they have a common divisor of 2, which contradicts the fact that their greatest common divisor is 1. We have a contraction, and hence our assumption, that $\sqrt{2}$ is rational, is false. ∎

Proof by Induction

The inductive principle states that if a proposition is true for 1 and, if its true for a positive integer n it is true for $n+1$, then it is true for all positive integers.

Here is an example. Let $F(n) = 1^2 + 2^2 + 3^2 + \cdots + n^2$, the sum of the first n squares. Let $G(n) = \frac{n(n+1)(2n+1)}{6}$ for any n.

Theorem 2 *For any positive integer n, $F(n) = G(n)$.*

Proof: The statement is true for $n = 1$, since $F(1) = 1^2 = 1$ and $G(1) = \frac{1 \cdot (1+1) \cdot (2+1)}{6} = 1$. The *inductive step* is to prove that $F(n) = G(n)$ implies $F(n+1) = G(n+1)$ for any n. By definition, $F(n+1) = F(n) + (n+1)^2$, and

$$\begin{aligned}
G(n+1) &= \frac{(n+1)(n+1+1)(2(n+1)+1)}{6} \\
&= \frac{2n^3 + 9n^2 + 13n + 6}{6} \\
&= \frac{2n^3 + 3n^2 + n}{6} + \frac{6n^2 + 12n + 6}{6} \\
&= G(n) + (n+1)^2 \\
&= F(n) + (n+1)^2 \\
&= F(n+1)
\end{aligned}$$

∎