Direct Proofs

These are usually the simplest kinds of proofs; we want to show that one statement implies another (i.e. $p \to q$).

1. Show that any positive integer divisible by 4 can be written as a difference of two squares. (e.g. $20 = 5 * 4 = 6^2 - 4^2$) Write the above problem in the form of $p \to q$, then prove it.

2. A rational number (an element of $\mathbb{Q}$), is a number of the form $\frac{a}{b}$ where a and b are integers and $b \neq 0$. Prove that the sum of two rational numbers is another rational number. (State the problem in the form $p \to q$.)

Proof by Contraposition

Often times, in order to show $p \to q$, it will be easier to prove $\neg q \to \neg p$, the contrapositive. This works because $p \to q \equiv \neg q \to \neg p$. The purpose of this technique is often to get a starting situation to work with.

1. Let x, y be two integers. Suppose $x^2(y^2 - 2y)$ is odd. Prove that x and y are odd. State the contrapositive, and then prove it.

2. Let x and y be integers. Suppose xy is not divisible by 5. Then show that x and y are not divisible by 5. As before, state the contrapositive and prove it.

Proof by Contradiction

Sometimes, when the above techniques fail, it can be useful to assume that q is false. Then derive a contradictionusing the starting information (p) and the assumption ($\neg q$). This means that your assumption could not have been true.

1. Show that $\sqrt[3]{2}$ is irrational.

2. Let x, y be positive integers. Show that $x^2 - y^2 \neq 1$.

Proofs of Equivalence

To prove statements of the form $p \leftrightarrow q$, you must show both $p \rightarrow q$ (the statement) and $q \rightarrow p$ (the converse).

State the converses of the statements on the previous side. Are any of them true?

Proof by cases

It is often useful to break up a problem into cases to give yourself more structure.

1. Let n be a positive integer. Prove that if the remainder when dividing n by 3 is 2, that n is not a square.

   Proof: Work with the contrapositive: If n is a square, then the remainder when dividing n by 3 is not 2. First, since n is a square, write $n = k^2$. Consider the following:

   $k = 3l$: $n = k^2 = (3l)^2 = 9l^2$ is divisible by 3.

   $k = 3l + 1$: $n = k^2 = (3l + 1)^2 = 9l^2 + 6l + 1$ has remainder 1 when divided by 3

   $k = 3l + 2$: $n = k^2 = (3l + 2)^2 = 9l^2 + 12l + 4$ has remainder 1 when divided by 3.

   (Why are these three cases enough?)