Methods of proof

Recall that we considered three methods of proof of a proposition of the form (P $\Rightarrow$ Q):

1. Direct argument: Here we simply assume that P is true and show that Q must be true. Since (P $\Rightarrow$ Q) is only false if P is true and Q is false this will complete the proof.

2. Contrapositive argument: Here we assume Q is false and prove P is also false. This uses the equivalence
(P $\Rightarrow$ Q) $\equiv$ ((**not** Q) $\Rightarrow$ (**not** P)).

3. Proof by contradiction: To show (P $\Rightarrow$ Q) we assume P is true and Q is false and derive a contradiction. That is, we show (P **and** (**not** Q)) is false.

Example: Use a contrapositive argument to show that if the square of a positive integer is an even number then the integer itself must have been even.

Solution: Suppose n is a positive integer and n is not even. We will show that n^2 is also not even.

Recall that an integer which is not even is odd and has the form $2x + 1$ for some integer x.

So $n = 2x + 1$ and therefore

$n^2 = (2x + 1)^2 = 4x^2 + 4x + 1 = 2(2x^2 + x) + 1.$

But $2x^2 + x$ is an integer so that n^2 is an odd integer. Here P was the statement
  n^2 is even
while Q was the statement
  n is even.
Thus **not** Q was the statement
  n is odd
while **not** P was the statement
  n^2 is odd.

Example: Use a proof by contradiction argument to show that there is no $x \in \mathbb{Q}$ (fractions) satisfying $x^2 = 2$.

Note: This fact really puzzled the ancient Greeks. Since fractions can be made arbitrarily small and moved around they expected one of them to be

$\sqrt{2}$. They might proceed as follows: Since $1^2 = 1 < 2$ and $2^2 = 4 > 2$ look for a fraction between 1 and 2. Check that $(3/2)^2 = 9/4 > 2 = 8/4$ so look between 1 and 3/2. Check that $(5/4)^2 = 25/16 < 2 = 32/16$ so look between 5/4 and 3/2. Check that $(11/8)^2 = 121/64 < 2 = 128/64$ so look between 11/8 and 3/2, etc.

Solution: Recall that $\mathbb{Q}$ is the set of rational numbers or fractions, that is, numbers of the form p/q where p and q are integers with $q \neq 0$.

Suppose $x \in \mathbb{Q}$ has form $x = p/q$ where p and q are integers with $q \neq 0$. We can also assume that after cancelling common factors of p and q that p and q are not both even.

Now $(p/q)^2 = 2$ means that $p^2 = 2q^2$. This makes p^2 even. Using the result from the last example this means p is also even. So $p = 2r$ for some integer r. Substituting to get $(2r)^2 = 2q^2$ or $4r^2 = 2q^2$ or $2r^2 = q^2$ allows to deduce that q^2 is even and hence that q is even. This gives the contradiction since we assumed that p and q were not both even.

Here P was the statement

$x^2 = 2$

while Q was the statement

x cannot be expressed as p/q, p and q integers with $q \neq 0$
and p and q are not both even.

Thus **not** Q was the statement

$x = p/q$, p and q integers with $q \neq 0$ and p and q are not both even.

Mathematical Induction

Example: What happens when we sum consecutive odd positive integers? Let's check:

1	1
$1+3$	4
$1+3+5$	9
$1+3+5+7$	16
$\vdots$	$\vdots$

It looks like we get perfect squares. Can we come up with a predicate proposition for this and prove that it is always true? Let's start with the proposition.

A positive odd integer is of the form $2k-1$ for some positive integer k so that the odd positive integers are

$$1 = 2(1) - 1, \quad 3 = 2(2) - 1, \quad 5 = 2(3) - 1, \quad 7 = 2(4) - 1, \ldots$$

Now it looks like our rule should be

$$\mathrm{P}(n) : 1 + 3 + 5 + \ldots + (2n-1) = n^2.$$

We would like to prove that this is always true, that is $\forall n, \mathrm{P}(n)$. How can we prove this for infinitely many values of n in a finite time?

The Principle of Mathematical Induction: Let $\mathrm{P}(n)$ be a predicate that is defined for all integers $n \geq 1$. Suppose that

1. $\mathrm{P}(1)$ is true, and
2. $\forall k \geq 1$, $(\mathrm{P}(k) \Rightarrow \mathrm{P}(k+1))$ is true.

Then $\mathrm{P}(n)$ is true for all $n \geq 1$.

The reasoning is that $\mathrm{P}(1)$ is true by 1 and, by 2 applied repeatedly, $\mathrm{P}(2)$ is true, $\mathrm{P}(3)$ is true, $\mathrm{P}(4)$ is true, etc.