# Basic Proof Examples

Lisa Oberbroeckling
Loyola University Maryland

Fall 2015

**Note.** In this document, we use the symbol $\neg$ as the negation symbol. Thus $\neg p$ means "not $p$."

There are four basic proof techniques to prove $p \implies q$, where $p$ is the hypothesis (or set of hypotheses) and $q$ is the result.

1. Direct proof
2. Contrapositive
3. Contradiction
4. Mathematical Induction

What follows are some simple examples of proofs. You very likely saw these in MA395: Discrete Methods.

## 1 Direct Proof

Direct proofs use the hypothesis (or hypotheses), definitions, and/or previously proven results (theorems, etc.) to reach the result.

**Theorem 1.1.** If $m \in \mathbb{Z}$ is even, then $m^2$ is even.

*Proof.* Suppose $m \in \mathbb{Z}$ is even. By definition of an even integer, there exists $n \in \mathbb{Z}$ such that

$$m = 2n.$$

Thus we get

$$m^2 = (2n)^2 = 4n^2 = 2(2n^2)$$

and we have $m^2$ is also even. $\square$

The following is an example of a direct proof using cases.

**Theorem 1.2.** If $q$ is not divisible by 3, then $q^2 \equiv 1 \pmod 3$.

*Proof.* If $3 \nmid q$, we know $q \equiv 1 \pmod 3$ or $q \equiv 2 \pmod 3$.

Case 1: $q \equiv 1 \pmod 3$. By definition, $q = 3k + 1$ for some $k \in \mathbb{Z}$. Thus

$$\begin{aligned} q^2 &= (3k+1)^2 = 9k^2 + 6k + 1 \\ &= 3(3k^2 + 2k) + 1 \end{aligned}$$

and we have $q^2 \equiv 1 \pmod 3$.

Case 2: $q \equiv 2 \pmod 3$. By definition, $q = 3k + 2$ for some $k \in Z$. Thus

$$\begin{aligned} q^2 &= (3k+2)^2 = 9k^2 + 12k + 4 \\ &= 9k^2 + 12k + 3 + 1 \\ &= 3(3k^2 + 4k + 1) + 1 \end{aligned}$$

and in this case we again have $q^2 \equiv 1 \pmod 3$.

In either case $q^2 \equiv 1 \pmod 3$ so the result is proven. $\square$

# 2 Contrapositive

Since $p \implies q$ is logically equivavlent to $\neg q \implies \neg p$, we can prove $\neg q \implies \neg p$. It is good form to alert the reader at the beginning that the proof is going to be done by contrapositive.

**Theorem 2.1.** If $q^2$ is divisible by 3, so is $q$.

*Proof.* We will prove the contrapositive; i.e., we will prove if $q$ is not divisible by 3, then $q^2$ is not divisible by 3.

By Theorem 1.2, we know that if $q$ is not divisible by 3, then $q^2 \equiv 1 \pmod 3$. Thus $q^2$ is not divisible by 3. $\square$

# 3 Contradiction

A proof by contradiction is considered an indirect proof. We assume $p \wedge \neg q$ and come to some sort of contradiction.

A proof by contradiction usually has "suppose not" or words in the beginning to alert the reader it is a proof by contradiction.

**Theorem 3.1.** Prove $\sqrt{3}$ is irrational.

*Proof.* Suppose not; i.e., suppose $\sqrt{3} \in \mathbb{Q}$. Then $\exists\ m, n \in \mathbb{Z}$ with $m$ and $n$ relatively prime and $\sqrt{3} = \dfrac{m}{n}$. Then $3 = \dfrac{m^2}{n^2}$, or $3n^2 = m^2$.

Thus $m^2$ is divisible by 3 so by Theorem 2.1, $m$ is also. By definition, $m = 3k$ for some $k \in \mathbb{Z}$. Hence $m^2 = 9k^2 = 3n^2$ and so $3k^2 = n^2$. Thus $n^2$ is divisible by 3 and again by Theorem 2.1, $n$ is also divisible by 3. But $m$, $n$ are relatively prime, a contradiction.

Thus $\sqrt{3} \notin \mathbb{Q}$. $\square$

# 4 Mathematical Induction

Mathematical Induction is a method of proof commonly used for statements involving $\mathbb{N}$, subsets of $\mathbb{N}$ such as odd natural numbers, $\mathbb{Z}$, etc. Below we only state the basic method of induction. It can be modified to prove a statement for any $n \geq N_0$, where $N_0 \in \mathbb{Z}$.

**Theorem 4.1** (Mathematical Induction)**.** Let $P(n)$ be a statement for each $n \in \mathbb{N}$. Suppose

1. $P(1)$ is true
2. If $P(k)$ is true, then $P(k+1)$ is true. The assumption that $P(k)$ true is called the induction hypothesis.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

The theorem uses the **Well-ordering Principle** (or axiom):

Every *non-empty* subset of $\mathbb{N}$ has a smallest element.

What about a largest element? Does $\mathbb{Z}$ follow the well-ordering principle? What about the set $\{\frac{1}{n} : n \in \mathbb{N}\}$?

*Proof of Mathematical Induction.* Proof by contradiction; i.e., suppose $\exists n \in \mathbb{N}$ such that $P(n)$ is false.

Let $A = \{n \in \mathbb{N} \mid P(n) \text{ is false}\}$. By supposition, $A$ is nonempty. By the Well Ordering Principle, $A$ has a smallest element; call it $m$. Since $P(1)$ is true, $1 \notin A$ and so we know $m > 1$. We also know by definition of $A$ that $P(k) = P(m-1)$, with $k = m - 1 \in \mathbb{N}$ is true. But we know if $P(k)$ is true then $P(k+1) = P(m)$ is true, which is a contradiction of $m \in A$.

Thus $P(n)$ is true $\forall n$ $\square$

Mathematical Induction is used to prove many things like the Binomial Theorem and equations such as $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$. As in other proof methods, one should alert the reader at the beginning of the proof that this method is being used.

It is a common mistake to check a few numbers and assume that the pattern holds for all others. But it actually must be proven, and Mathematical Induction is a way to prove things for all natural numbers.

Fermat (1601-1655) conjectured $2^{2^n}+1$ is prime $\forall n$. It was known to be true for $n = 1, 2, 3, 4$.

Many years later, Euler (1707-1783) found the conjecture to be false for $n = 5$: $2^{2^5} + 1 = 641(6{,}700{,}417)$.

**Theorem 4.2.** For any $n \in \mathbb{N}$, 64 is a factor of $3^{2n+2} - 8n - 9$.

*Proof.* Proof by Mathematical Induction.

For the $n = 1$ case, we see that $3^{2n+2} - 8n - 9 = 3^4 - 8 - 9 = 81 - 17 = 64$. Thus $P(1)$ is true.

Now suppose

$$3^{2n+2} - 8n - 9 \equiv 0 \pmod{64}. \tag{1}$$

We need to show that $3^{2(n+1)+2} - 8(n+1) - 9 \equiv 0 \pmod{64}$.

We have

$$\begin{align} 3^{2(n+1)+2} - 8(n+1) - 9 &= 3^{2n+2+2} - 8n - 9 \tag{2} \\ &= (3^{2n+2})3^2 - 8k - 17 \tag{3} \\ &= (3^{2n+2})9 - 8k - 17 \tag{4} \end{align}$$

By the induction hypothesis (1), there exists some $m \in \mathbb{N}$ such that $3^{2n+2} - 8n - 9 = 64m$. Thus $3^{2k+2} = 64m + 8k + 9$ and putting this into (4) we have

$$\begin{aligned} 3^{2(n+1)+2} - 8(n+1) - 9 &= (64m + 8k + 9)9 - 8k - 17 \\ &= 64 \cdot 9m + 72k + 81 - 8k - 17 \\ &= 64 \cdot 9m + 64k + 64 \\ &= 64(9m + k + 1). \end{aligned}$$

Hence $3^{2(n+1)+2} - 8(n+1) - 9$ is divisible by 64. Thus $P(k+1)$ is true, so by Mathematical Induction, $P(n)$ is true $\forall n \in \mathbb{N}$. $\square$