Proof by Contradiction

Suppose you want to show

$$A \Rightarrow B.$$

Direct method: Assume A; conclude B.
Contrapositive: We saw this is equivalent to the contrapositive,

$$\neg B \Rightarrow \neg A.$$

Prove the contrapositive directly: Assume $\neg B$; conclude $\neg A$.
Today: Recall that

$$A \Rightarrow B \quad \text{is equivalent to} \quad B \vee \neg A.$$

So showing $A \Rightarrow B$ is true is the same as showing $\neg(A \Rightarrow B)$ is false, is the same as showing

showing $\quad \neg(B \vee \neg A) \equiv (A \wedge \neg B) \quad$ is **false**.

Method of Proof by Contradiction.
Assume $A \wedge \neg B$; conclude something known to be false.
In other words, show

$$(A \wedge \neg B) \Rightarrow \text{False statement.}$$

Conclude $A \wedge \neg B$ must be false, and hence $A \Rightarrow B$ is true.

Method of Proof by Contradiction.
Assume $A \wedge \neg B$; conclude something known to be false.
In other words, show

$$(A \wedge \neg B) \Rightarrow \text{False statement.}$$

Conclude $A \wedge \neg B$ must be false, and hence $A \Rightarrow B$ is true.

Reasoning:
The only way for

$$(\text{Statement } X) \Rightarrow (\text{False Statement } Y)$$

to be true is if X is false to begin with.

X	Y	$X \Rightarrow Y$
T	T	T
T	F	F
F	T	T
F	F	T

Claim: Suppose that n is an odd integer. Then n^2 is odd as well.

Proof 1. (Direct method) If n is odd, then $n = 2k + 1$ for some $k \in \mathbb{Z}$. So

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

So since $2k^2 + 2$ is an integer, n^2 must be odd as well. □

Proof 2. (By contradiction)

> **Outline:**
> *Let A be the statement "n is an odd integer"*
> *and B be the statement "n^2 is an odd integer".*
> *Goal: Assume $(A \wedge \neg B)$; conclude something statement.*

Suppose $n \in \mathbb{Z}$ is odd and n^2 is even. Then $n = 2k + 1$ and $n^2 = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Consider $n^2 + n$. On the one hand,

$$n^2 + n = 2\ell + 2k + 1 = 2(\ell + k) + 1$$

is odd. But also,

$$n^2 + n = n(n+1) = (2k+1)(2k+1+1) = 2(2k+1)(k+1)$$

is even. Since it's not possible for $n^2 + n$ to be even and odd, this is a contradiction. Therefore, if n is odd, then n^2 is odd as well. □

Claim.

There are no positive integers x and y such that $x^2 - y^2 = 1$.

Rewriting the statement:

$$\begin{aligned} \neg\left(\exists x, y \in \mathbb{Z}_{>0}(x^2 - y^2 = 1)\right) \\ &\equiv \forall x, y \in \mathbb{Z}_{>0}(x^2 - y^2 \neq 1) \\ &\equiv (x, y \in \mathbb{Z}_{>0}) \Rightarrow (x^2 - y^2 \neq 1). \end{aligned}$$

Proof. (By contradiction)

> **Outline:**
> *Let A be the statement "x and y are positive integers"*
> *and B be the statement "$x^2 - y^2 \neq 1$".*
> *Goal: Assume $(A \wedge \neg B)$; conclude something statement.*

Let $x, y \in \mathbb{Z}_{>0}$ with $x^2 - y^2 = 1$. Thus

$$1 = x^2 - y^2 = (x+y)(x-y).$$

But since $x, y \in \mathbb{Z}_{>0}$, we have $x + y \in \mathbb{Z}_{>0}$ as well. The only positive divisor of 1 is 1, so that $x + y = 1$. But $x, y \geqslant 1$ implies

$$1 = x + y \geqslant 1 + 1 = 2.$$

This is a contradiction. So $x^2 - y^2 \neq 1$ for all $x, y \in \mathbb{Z}_{>0}$. □

Theorem.

If $p > 0$ is prime, then $\sqrt{p}$ is irrational.

Rewriting the statement:

$$\sqrt{p} \notin \mathbb{Q} \equiv \neg\left(\sqrt{p} \in \mathbb{Q}\right).$$

Proof. (By contradiction)

> **Outline:**
> *Let A be the statement "$p > 0$ is prime"*
> *and B be the statement "$\sqrt{p}$ is irrational".*
> *Goal: Assume $(A \wedge \neg B)$; conclude something statement.*

Theorem.

If $p > 0$ is prime, then $\sqrt{p}$ is irrational.

Rewriting the statement:

$$\sqrt{p} \notin \mathbb{Q} \equiv \neg\left(\sqrt{p} \in \mathbb{Q}\right).$$

Proof. (By contradiction)

Let $p > 0$ be prime, and suppose that $\sqrt{p}$ is rational. Namely, that there are $a, b \in \mathbb{Z}$ with $b \neq 0$ and so that $\sqrt{p} = a/b$, in lowest terms ($\gcd(a,b) = 1$). Thus since $p > 0$,

$$p = (\sqrt{p})^2 = (a/b)^2 = a^2/b^2.$$

Thus $a^2 = pb^2$, so that $p|a^2$. By Euclid's lemma, this implies $p|a$. But then $a = pk$ for some $k \in \mathbb{Z}$, so that

$$pb^2 = (pk)^2 = p(pk^2). \qquad \text{So } b^2 = pk^2$$

(since $p \neq 0$), so that $p|b^2$. Therefore, by Euclid's lemma again, $p|b$. But that means that $p|a$ and $p|b$, which contradicts a/b being in lowest terms. Thus no such a and b exist, so that $\sqrt{p} \notin \mathbb{Q}$. $\square$

You try: (1) Retrace this proof for $p = 2$. (2) Retrace this proof for $p = 4$ and identify where the "contradiction" fails if p is not prime.

Theorem.
If $p > 0$ is prime, then $\sqrt{p}$ is irrational.

Recall: We proved the following in Lecture 9:

Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors). Thus

$$a^2 = (m/n)^2 = m^2/n^2.$$

But since any prime factor of m^2 would also be a prime factor of m (and similarly for n^2 and n), we have m^2/n^2 is in lowest terms. *

So since $m^2/n^2 \in \mathbb{Z}$, we have $n^2 = 1$. So $n = \pm 1$. And thus $a = m/n \in \mathbb{Z}$, as desired. □

*This was a subtle little proof by contradiction, nested in a direct proof.

Theorem. There are an infinite number of prime numbers.
Proof (by contradiction).
Suppose there are a finite number of prime numbers. Let $p_1, p_2, \ldots, p_\ell$ be a complete list of the positive primes, and consider $n = 1 + p_1 p_2 \cdots p_\ell$. Since $p_i > 1$ for all i, we have

$$p_i < 1 + p_1 p_2 \cdots p_\ell = n \quad \text{for all } i.$$

In particular, $n \neq p_i$ for all i; so n is not prime. Thus n has a prime factorization; fix j such that p_j is one of the prime factors of n. Then there is some $k \in \mathbb{Z}$ such that

$$p_j k = n = 1 + p_j \cdot \prod_{i \neq j} p_i.$$

Thus

$$1 = p_j \underbrace{\left(k - \prod_{i \neq j} p_i\right)}_{\in \mathbb{Z}},$$

so that $p_j | 1$, which is a contradiction. Thus, there are an infinite number of primes. □

When to consider proof by contradiction

Good indicator: "There does not exist..."

For example:

There are no integers such that...;
Blah is not rational...;
Blah is unbounded....

Why:

It's hard to do operations with something that does not exist; so assuming something exists gives us something to work with.

Direct proofs are better than proof by contradiction!

Direct proofs explain why something if true.
Proofs by contradiction explain why something isn't false.

Example: The book presented the following proof by contradiction.

> **Example 23.1**
>
> Suppose that n is an odd integer. Then n^2 is an odd integer.
>
> **Proof.** Assume the contrary. That is, we suppose that n is an odd integer but that the conclusion is false, i.e. n^2 is an even integer.
>
> =2(2k^2+2k) + 1
>
> As n is odd, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Thus $n^2 = (2k+1)^2 = 4k + 2k + 1$ which contradicts that n^2 is even. Thus our assumption that n^2 is even must be wrong, i.e. n^2 must be odd. □

We can edit this down easily to turn this proof by contradiction into a direct proof:

> **Proof.** ~~Assume the contrary. That is, we~~ S suppose that n is an odd integer. ~~but that the conclusion is false, i.e. n^2 is an even integer.~~
>
> =2(2k^2+2k) + 1
>
> As n is odd, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Thus $n^2 = (2k+1)^2 = 4k + 2k + 1$. ~~which contradicts that n^2 is even. Thus our assumption that n^2 is even must be wrong, i.e.~~ Thus n^2 must be odd. □

Moral: After writing a PbC, always check to see if you can turn it around!

Warning: When setting up the contradiction, make sure you've correctly negated the statement.

Example: For any natural number n, the sum of all natural numbers less than n is not equal to n.

An incorrect proof by contradiction: Assume that for any natural number n, the sum of all smaller natural numbers is equal to n. But this is clearly false, because, for example,

$$5 \neq 1 + 2 + 3 + 4.$$

We have reached a contradiction, so our assumption was false and the theorem must be true. □

The error: The statement is

$$\forall n \in \mathbb{Z}_{>0} \left(\sum_{i=1}^{n-1} i \neq n \right).$$

The negation of this statement is

$$\neg \left(\forall n \in \mathbb{Z}_{>0} \left(\sum_{i=1}^{n-1} i \neq n \right) \right) \equiv \exists n \in \mathbb{Z}_{>0} \left(\sum_{i=1}^{n-1} i = n \right).$$

Warning: When setting up the contradiction, make sure you've correctly negated the statement.

Example: For any natural number n, the sum of all natural numbers less than n is not equal to n.

The error: The statement is

$$\forall n \in \mathbb{Z}_{>0} \left(\sum_{i=1}^{n-1} i \neq n \right).$$

The negation of this statement is

$$\neg \left(\forall n \in \mathbb{Z}_{>0} \left(\sum_{i=1}^{n-1} i \neq n \right) \right) \equiv \exists n \in \mathbb{Z}_{>0} \left(\sum_{i=1}^{n-1} i = n \right).$$

Correct proof by contradiction: Suppose that, for some $n \in \mathbb{Z}_{>0}$ we have

$$n = \sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}.$$

So

$$2n = (n-1)n = n^2 - n. \quad \text{Thus } 0 = n^2 + n = n(n+1).$$

Therefore either $n = 0$ or $n + 1 = 0$. This contradicts $n > 0$, so no such n exists. □