MATH 2001
Proof by Contradiction

Our next style of proof is proof by contradiction.

The main idea: To prove a statement P, we start by assuming $\sim P$. Using logical reasoning, we search for, and find, two statements that stand in contradiction to each other. In other words, we show $C \wedge \sim C$.

The principle on which proof by contradiction is based:

$\sim P \Rightarrow (C \wedge \sim C)$ IS LOGICALLY EQUIVALENT TO P

Proof of this principle:

P	C	$\sim P$	$C \wedge \sim C$	$\sim P \Rightarrow (C \wedge \sim C)$
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

The truth values of $\sim P \Rightarrow (C \wedge \sim C)$ are the same as those of P for all possible input values of P and C. So $\sim P \Rightarrow (C \wedge \sim C)$ is logically equivalent to P.

Template for proof by contradiction:

STATEMENT TO PROVE: P
PROOF: By way of contradiction, assume $\sim P$.
⋮
therefore $C \wedge \sim C$, a contradiction
Therefore P.

Example 1: Prove that for all integers a and b, $a^2 - 4b \neq 2$.

Proof: For the sake of contradiction, suppose there are integers a, b such that $a^2 - 4b = 2$.

Then $a^2 = 2 + 4b = 2(1+2b)$, so a^2 is even.

Thus a is even. Choose $c \in \mathbb{Z}$ such that $a = 2c$.

Substituting gives

$$(2c)^2 = 2(1+2b),$$

so $$4c^2 = 2(1+2b),$$

thus $$2c^2 = 1 + 2b,$$

and $$1 = 2b - 2c^2 = 2(b - c^2)$$

So 1 is even. This is a contradiction.

So $\forall a, b \in \mathbb{Z}$ $a^2 - 4b \neq 2$. ∎

Example 2: Prove that there are no integers a, b for which $18a + 6b = 1$.

Proof: By way of contradiction, suppose there are integers a, b for which $18a+6b=1$. Then $1 = 2(9a+3b)$, so 1 is even. This is a contradiction. Thus there are no integers a, b for which $18a+6b=1$. ▨

Using contradiction to prove conditional statements:
If we want to prove $P \implies Q$ using proof by contradiction, we should assume $\underline{\sim(P \Rightarrow Q)}$.
This can be rewritten as:

$\underline{\sim(\sim P \vee Q) = P \wedge \sim Q}$.

Template for proof by contradiction for a conditional statement:

STATEMENT TO PROVE: $P \Rightarrow Q$.
PROOF. For the sake of contradiction, suppose P and $\sim Q$.
⋮
Therefore $C \wedge \sim C$, a contradiction
Therefore $P \Rightarrow Q$.

Example 3: Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

Proof: Suppose a is rational and ab is irrational and b is rational.
Choose $p \in \mathbb{Z}$ and $q \in \mathbb{Z}$ so that $a = \frac{p}{q}$ and choose $r, s \in \mathbb{Z}$ such that $b = \frac{r}{s}$. (def. of rational)
Then $ab = \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$. We know $pr \in \mathbb{Z}$ and $qs \in \mathbb{Z}$ ($\mathbb{Z}$ is closed under multiplication), so ab is rational (def. of rational). This is a contradiction.
Thus if a is rational and ab is irrational, then b is irrational. ▨