Announcements:
- Posted notes from last three classes.
- Midterms available in MLC.
  - Will also have grades on Canvas.
- Final Exam is April 13.

Proof by Contradiction:

Suppose I want to prove a statement P

Pf: 1) Assume P is false

This is where the work is

2) Use this assumption to get a contradiction.
That is, produce another statement S
and prove

$$\sim P \Rightarrow \underbrace{(S \wedge \sim S)}_{\text{contradiction}}$$

3) Conclude that $\sim P$ is false. So P is true.

Prop: There is no smallest positive real number.

Pf: Suppose there is a [smallest positive real number. Call it x.]

Consider the number $\frac{x}{2}$.

- It's positive.
- It's less than x, because $\frac{x}{2} < \frac{x}{2} + \frac{x}{2} = x$.

So, [$\frac{x}{2}$ is a positive real number smaller than x.]

This contradicts the assumption that x is the smallest positive real number! $\rightarrow\leftarrow$ indicates contradiction.

Therefore, our initial assumption was false.

Therefore, there is no smallest positive real number. ∎

More generally, if I wanted to prove

Prop: There's no smallest blah.

Pf:
- Assume there is. Call it $blah_1$
- Somehow construct a smaller $blah_2$
- Obtain a contradiction.

Ex: Division Algorithm.

Recall: The rational numbers are the set

$$\mathbb{Q} := \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}.$$

Def: A real number $x \in \mathbb{R}$ is called irrational if $x \notin \mathbb{Q}$.

Prop: The sum of an irrational number with a rational number, is irrational.

$\forall x$ irrational $\forall y$ rational, ($x+y$ is irrational.)

Pf: Suppose $\exists x$ irrational $\exists y$ rational, such that $x+y$ is rational.

Write $y = \frac{a}{b}$. and $x+y = \frac{c}{d}$ $(a,b,c,d \in \mathbb{Z})$

Then $x = (x+y) - y = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$

So x is rational. This contradicts our assumption that x was irrational! $\rightarrow\leftarrow$

So our initial assumption was false. ■

(You can also do a direct proof. $\forall x,y.$ (y is rational $\wedge$ $x+y$ is rational)

$\Downarrow$

x is rational.)

P

Exercise: If $a, b \in \mathbb{Z}$ and $(a \geq 2)$, then $(a \nmid b$ or $a \nmid b+1)$

$P \Rightarrow Q$ ... Q

("$a \nmid b$ means "a doesn't divide b"")

Proof: Assume $P \wedge \sim Q$. I.e.

$$a \geq 2 \text{ and } a \mid b \text{ and } a \mid b+1.$$

Write $b = ax$ for some $x \in \mathbb{Z}$

$b+1 = ay$ —— $y \in \mathbb{Z}$

So then $1 = (b+1) - b = ay - ax$
$= a(y-x)$.

Therefore, $a \mid 1$. So $a = 1$ or $a = -1$

We have a contradiction! $\rightarrow\leftarrow$

Therefore, the proof is complete. ∎

Note: You can also do proof by contrapositive.

Thm (Euclid, ~300 BCE): There are infinitely many prime numbers.

Pf: We first prove a Lemma.

Lemma: Let $n \geq 2$ be an integer. Then n has a prime factor.

Proof: Proved in Class 14 (Feb 7). (Used contradiction + WOP).

Suppose there are only finitely many primes.
2 is prime, so the set of primes is nonempty.

Set of all primes $= \{p_1, p_2, \ldots, p_n\}$. for some $n \in \mathbb{N}$.

Consider the number $N = p_1 p_2 \cdots p_n + 1$.

- By the Lemma, N has a prime factor, p
- By the Exercise, $p_1 \nmid N$, $p_2 \nmid N$, ..., $p_n \nmid N$.

So p is a prime and $p \notin \{p_1, p_2, \ldots, p_n\}$.

Contradiction! $\rightarrow\leftarrow$ ∎