1. Proofs

Def: A proof is

Good:

Bad:

How do you confirm your beliefs are correct?

Math

Science
A proof is a finite list of statements, each of which is logically implied by the previous statement, which is used to establish the truth of some proposition.

For now:

Theorem: \( \text{nat_abs_add_le} : (a + b) \leq a + \text{nat_abs} b \)

```ocaml
begin
  have : \( a, b : \mathbb{N} \), \( \text{nat_abs} (\text{sub_nat_nat} a (\text{nat.succ} b)) \leq \text{nat.succ} (a + b) \),
  { refine (\( \lambda a, b : \mathbb{N} \), \( \text{sub_nat_nat} \text{elim} a \text{.succ} \)),
    (\( \lambda m, n : \mathbb{N} \), n = b.\text{succ} \Rightarrow \text{nat_abs} i \leq (m + b).\text{succ} \) _ rfl);,
  intros i n e,
  { subst e, rw [\text{add_comm} _ i, \text{add_assoc}]},
  exact \( \text{nat.le_add_right} i (b.\text{succ} + b).\text{succ} \) },
  { apply \text{succ_le_succ},
    rw [+ succ.inj e, + add_assoc, \text{add_comm},
    apply \text{nat.le_add_right} },
  cases a; cases b with b b; simp [\text{nat_abs}, \text{nat.succ_add}];
  try (rfl); [skip, rw \text{add_comm} a b]; apply this
end
```
② How to prove things

How you should prove a proposition depends on the logical structure of the proposition

<table>
<thead>
<tr>
<th>Structure</th>
<th>How to prove it</th>
</tr>
</thead>
<tbody>
<tr>
<td>P \land Q</td>
<td></td>
</tr>
<tr>
<td>P \Rightarrow Q</td>
<td></td>
</tr>
<tr>
<td>P \Leftrightarrow Q</td>
<td></td>
</tr>
<tr>
<td>\exists x \in S, P(x)</td>
<td></td>
</tr>
<tr>
<td>\forall x \in S, P(x)</td>
<td></td>
</tr>
</tbody>
</table>

Can also replace the proposition to be proved with a logically equivalent proposition that has a different structure.

Example
3 Direct proof

A direct proof

Theorem: For every natural number, there is a natural number greater than it.

Example

proof

Remainder

∀x ∈ S, P(x)  Let a be an arbitrary element of S and prove P(a)
∃x ∈ S, P(x)  Provide some a ∈ S and prove P(a)
Def: Given $n, m \in \mathbb{Z}$, we say $n$ divides $m$, written $n \mid m$, if $m = nk$ for some $k \in \mathbb{Z}$.

Example

Then For all $a, b, n \in \mathbb{Z}$, if $n \mid a$ and $n \mid b$ then $n \mid (a - b)$

proof

Reminder: $P \Rightarrow Q$ Assume $P$ is true and prove $Q$

One lesson:
4. Proof by contraposition

A proof by contraposition

Fact: \( n \in \mathbb{Z} \) is even if and only if odd.

Theorem: For every \( n \in \mathbb{Z} \), if \( n^2 \) is even then so is \( n \).

Example

Direct proof?

Proof: Let \( n \) be an integer.
Proof by contraposition is especially useful if you are trying to prove something of the form

**Def** A real number $r$ is **rational** if  
Otherwise, $r$ is **irrational**.

Thus for every real number $a$, if $a$ is irrational 
then so is $3a$.

**Proof** Let $a$ be a real number.
5. Proof by contradiction

A proof by contradiction

Comment: Why does this work?

Useful for proving non-existence statements

= statements of the form
Def: A natural number is prime if

Example

Fact: Every natural number greater than 1

Thus (Euclid?) There are infinitely many prime numbers

proof: Suppose for contradiction that there are only finitely many primes, \( p_1, p_2, \ldots, p_n \).
Fact If $a \in \mathbb{Q}$ then there are $p, q \in \mathbb{Z}$ such that $q \neq 0$, $a = \frac{p}{q}$ and

Then $\sqrt{2}$ is irrational.

Example

Proof Suppose for contradiction $\sqrt{2}$ is rational.
Proof by Cases

A proof by cases proves a proposition $P$

i.e.

There are irrational numbers $a$ and $b$ such that $a^b$ is rational.

Example

proof

Case 1:

Case 2:
Sometimes proof by cases is really cool, other times...

Fact For every natural number $n$, there is a natural number $k$ such that one of the following holds:

\[ \text{Thm} \quad \text{For all } n \in \mathbb{N}, \quad 3 \mid (n^3 - n) \]

**proof** Let $n$ be a natural number and

Case 1:

Case 2:

Case 3:
<table>
<thead>
<tr>
<th>Method</th>
<th>Goal</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct proof</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof by contraposition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof by contradiction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof by cases</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
⑧ Other comments

Today I wrote full proofs

Usually:

Problem solving:

Proof writing:

A common pattern

①
②
③
④
⑨ Some tips

When you are trying to prove something, ask yourself:

What do I have/know?

What am I trying to build/prove/etc?

What proofs have I seen before which do something similar to what I am trying to do here?
Challenge question

Can you find a propositional formula using only $P$, $Q$, and $\wedge$ which is logically equivalent to $P \implies Q$? If not, can you prove it?

What about logically equivalent to $P \wedge Q$ using only $P$, $Q$, and $\implies$?