① Proofs

Def A proof is

Good:

Bad:

How do you confirm your beliefs are correct?

Math

Science

Def 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.

```
theorem nat_abs_add_le (a b : ℤ) : nat_abs (a + b) ≤ nat_abs a + nat_abs b :=
begin
  have : ∀ (a b : ℕ), nat_abs (sub_nat_nat a (nat.succ b)) ≤ nat.succ (a + b),
  { refine (λ a b : ℕ, sub_nat_nat_elim a b.succ
      (λ m n i, n = b.succ → nat_abs i ≤ (m + b).succ) _ _ rfl);
    intros i n e,
    { subst e, rw [add_comm _ i, add_assoc],
      exact nat.le_add_right i (b.succ + b).succ },
    { apply succ_le_succ,
      rw [← succ.inj e, ← add_assoc, add_comm],
      apply nat.le_add_right } },
  cases a; cases b with b b; simp [nat_abs, nat.succ_add];
  try {refl}; [skip, rw add_comm a b]; apply this
end
```

My advice: Imagine your proof is being read by

For now:

② How to prove things

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

Structure	How to prove it
$P \wedge Q$	
$P \Rightarrow Q$	
$P \Leftrightarrow Q$	
$\exists x \in S, P(x)$	
$\forall x \in S, P(x)$	

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

Example

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

proof

Reminder

$\forall x \in S, P(x)$ Let a be an arbitrary element of S and prove $P(a)$

$\exists x \in S, P(x)$ Provide some $a \in S$ and prove $P(a)$

Def Given $n, m \in \mathbb{Z}$, we say n divides m, written $n \mid m$, if

Example

Example **Thm** 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

Example

Fact $n \in \mathbb{Z}$ is even iff and odd iff

Thm For every $n \in \mathbb{Z}$, if n^2 is even then so is n.

Direct proof?

proof Let n be an integer.

Proof by contraposition is especially useful if you are trying to prove something of the form

Example

<u>Def</u> A real number r is rational if

Otherwise, r is irrational.

<u>Thm</u> For every real number a, if a is irrational then so is $3a$.

<u>proof</u> Let a be a real number.

⑤ Proof by contradiction

A proof by contradiction

<u>Comment</u> Why does this work?

P			
T			
F			

Useful for proving nonexistence statements

= statements of the form

Example

Def A natural number is prime if

Example

Fact Every natural number greater than 1

Thm (Euclid?) There are infinitely many prime numbers

proof Suppose for contradiction that there are only finitely many primes, $p_1, p_2, \ldots, p_n$.

Example

Fact If $a \in \mathbb{Q}$ then there are $p, q \in \mathbb{Z}$ such that $q \neq 0$, $a = \frac{p}{q}$ and

Thm $\sqrt{2}$ is irrational.

proof Suppose for contradiction $\sqrt{2}$ is rational.

⑥ Proof by Cases

A proof by cases proves a proposition P

i.e.

Example

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

proof

Case 1:

Case 2:

Sometimes proof by cases is really cool, other times...

<u>Fact</u> For every natural number n, there is a natural number k such that one of the following holds:

<u>Thm</u> For all $n \in \mathbb{N}$, $3 \mid (n^3 - n)$

<u>proof</u> Let n be a natural number and

<u>Case 1:</u>

<u>Case 2:</u>

<u>Case 3:</u>

⑦ Summary

Direct proof

Goal:
Method:

Proof by contraposition

Goal:
Method:

Proof by contradiction

Goal:
Method:

Proof by cases

Goal:
Method:

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 $P \Rightarrow Q$? If not, can you prove it?

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