Administrivia

- None.

Proof Techniques — Overview/Rants

- By “proof” we mean informal version, sometimes relying on context, of formal “this follows from that” arguments of chapter 1.
- Goal is to convince human reader. Sometimes a sequence of formulas will do. Other times some prose is needed to explain what they mean. (Ask yourself: Would this make sense to you?)
- If you are asked to show, e.g., that if $x = 5$ then $x^2 = 25$, please do not start by writing $x^2 = 25$! (Don’t write down as “true” things you haven’t shown to be true!)
Exhaustive Proof / Proof By Cases

- Idea here is to prove by considering each “case” separately. Only works if there are finitely many. (Recall result from propositional logic that allows this.)
- Simple example: To show that for all integers \( x \) with \( 0 \leq x \leq 4 \), \( x^2 < 20 \), five cases to consider.
- Slightly more complex example: To show something for all integers, can consider two cases, odd integers and even integers. (Aside: How shall we define “even”? Is zero even?)
- Much more complex example: Computer-assisted proof of 4-color map theorem (1976, used almost 2000 separate cases).

Direct Proof

- Idea here is to show \( P \rightarrow Q \) like we’ve been doing — assume \( P \) and derive \( Q \) — but less formally.
- Example: Show that for integers \( p \) and \( m \), if \( p \) is even and \( m \) is positive, \( p^m \) is even.
Proof by Contraposition

- Idea is based on a derived rule from propositional logic: If $Q' \rightarrow P'$, then $P \rightarrow Q$.
  
  So if proving $P \rightarrow Q$ is difficult, we can try proving $Q' \rightarrow P'$ instead.

- Example: Show that if $m$ and $n$ are integers and $m + n$ is even, either $m$ and $n$ are both even or $m$ and $n$ are both odd.

Proof By Contradiction

- Idea is based on another rule we could prove using propositional logic: If $(P \land Q') \rightarrow \text{false}$, then $P \rightarrow Q$.
  
  So if proving $P \rightarrow Q$ is difficult, we can try assuming $P \land Q'$ and "deriving a contradiction".

  Note that sometimes $P$ is just true.

- Example: Show that $\sqrt{2}$ is irrational.
Minute Essay

- Find a counterexample for the following conjecture: “If \( x \) is an integer, \( \sqrt{x} \) is an integer.”
- To show that there is no largest prime, we could assume \( P \) and derive a contradiction. What is \( P \)? (You don’t have to show there’s no largest prime, just say what \( P \) is.)
- (Reminder: Homework 2 due.)

Minute Essay Answer

- Find a counterexample for the following conjecture: “If \( x \) is an integer, \( \sqrt{x} \) is an integer.”
  \[ x = 2 \]
- To show that there is no largest prime, we could assume \( P \) and derive a contradiction. What is \( P \)? (You don’t have to show there’s no largest prime, just say what \( P \) is.)
  “There is a largest prime.”