CS 173 Lecture 26b: Counterpoints to Contradiction

- When do we use proof technique X?

  something along the lines of

  - direct proof
  - contrapositive (if applicable)
  - cases (can be hard if cases are not obvious)
  - induction (for proving states quantified over $n \geq a$, $n \in \mathbb{Z}$)
  - contradiction (when all else fails)

- can be difficult b/c goal of "False" is quite nebulous

- people who dislike proof by contradiction
  - it gives them uncomfortable feelings: assume fictional world where $\neg p$, then discover that the fictional world was a lie.
  - e.g. direct proofs give useful intermediaries.

    $p \to r_1 \to r_2 \to r_3 \to q$

    gives $p \to r_1$, $p \to r_2$, $p \to r_3$

    $\neg q \to \neg r_3$, $\neg q \to \neg r_2$, $\neg q \to \neg r_1$

    r_1, r_2, r_3 might be interesting or useful outside of proving q.

    in contradiction, intermediaries come from assuming a falsehood

    $\to$ kind of untrustworthy.

- pedagogically:
  - students have habit after learning contradiction of trying proof by contradiction

- Students have habit after learning contradiction of trying proof by contradiction when they don't know where to start
- this is bad because you don't know what the concrete goal is
- don't know where to start, don't know where to end

- taste:
  some people think that often people write proof by contradiction instead of a more straightforward proof

Claim: $\forall a, b \in \mathbb{Z}$, $a^2 - 4b \neq 2$

Pf. Case a is even, $a = 2k$, $k \in \mathbb{Z}$.

$$a^2 - 4b = 4k^2 - 4b = 4(k^2 - b)$$

By division alg, $4(k^2-b)$ has remainder 0 when dividing by 4, 2 has remainder 2.

So $4(k^2-b) \neq 2$.

Case a is odd, $a = 2k+1$, $k \in \mathbb{Z}$

$$a^2 - 4b = 4k^2 + 4k + 1 - 4b$$
$$= 4(k^2 + k - b) + 1$$

which has remainder 1 when dividing by 4 but 2 has remainder 2.

So $4(k^2+k-b)+1 \neq 2$. $\square$