S. KIMMEL

Goals

- Describe & write proof by contradiction
- Describe & write proof by strong induction

Proof by Contradiction

Proof needs to do two things

① (Direct) $\lceil P \rightarrow Q$

② (Direct) $\lceil P \rightarrow \lceil Q$

$\therefore P$

} Most common

S. KIMMEL

Q: Prove $\sqrt{2}$ is irrational

* Not of form $P \to Q$

A: For contradiction, suppose $\sqrt{2}$ is rational. Then $\exists\, a, b \in \mathbb{Z} : \frac{a}{b} = \sqrt{2}$ where the fraction is fully simplified, so $\neg \exists\, c \in \mathbb{Z} : c|a \wedge c|b$. Squaring both sides, we have

$$a^2 = 2b^2.$$

Thus $2|a^2$. But we've previous proved this implies $2|a$. This means $\exists\, m \in \mathbb{Z} : 2m = a$. Plugging in, we have

$$4a^2 = 2b^2.$$

Dividing by 2, we get

$$2a^2 = b^2.$$

But this means $2|b^2$, and so $2|b$. But this means $2|a$ and $2|b$, which contradicts the fact that $\frac{a}{b}$ is fully simplified. $\square$

S. KIMMEL

Try: $\neg \exists x, y \in \mathbb{Z}: x^2 = 4y + 2$ (1st step: is x^2 even or odd)

for contradiction, there

Suppose $\wedge$ exist $x, y \in \mathbb{Z}: x^2 = 4y + 2$. Then x^2 is even, so x is even. Thus $\exists m \in \mathbb{Z}: x = 2m$. Plugging in,

$$4m^2 = 4y + 2,$$

$$y = \frac{4m^2 - 2}{4} = m^2 - \frac{1}{2}$$

Since m is an integer, $m^2 - \frac{1}{2}$ is <u>not</u> an integer, a contradiction.

Approaches:

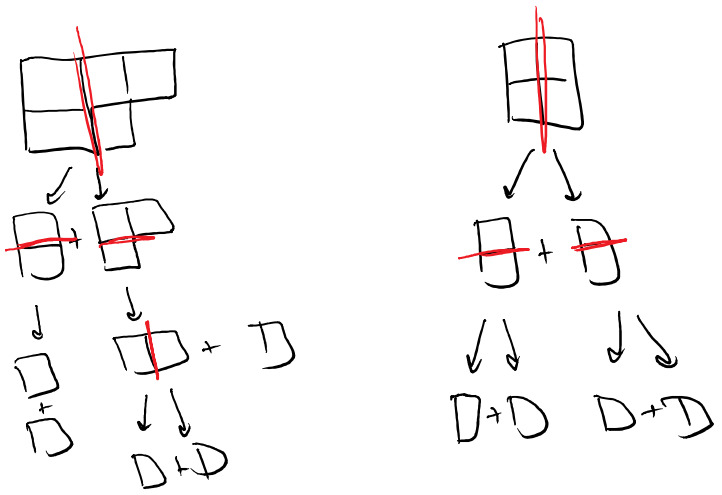
Prove P $\Longrightarrow$ Prove $\neg P \to P$

Prove $P \to Q$ $\Longrightarrow$ Prove $\underbrace{(P \wedge \neg Q)}_{= \neg(P \to Q)} \to \neg P$ or Q or $C \wedge \neg C$

S. KIMMEL

Strong Induction

Q: Suppose you have a bar of chocolate containing n small joined squares. How many times do you have to break the chocolate along a row or column before you have n separate squares?



always seems to be $n-1$!

Proof?

Induction seems good, because after breaking, end up with smaller chocolate bars (smaller problems!)

BUT

smaller bar might not have $n-1$ pieces

S. KIMMEL

Strong Induction Proof Structure

Set-up

Let $P(n)$ be the predicate _____ We will prove $P(n)$ is true for all $n \geq$ b.c.
(b.c. = base case)

Base-case

Base-case: We prove $P($b.c.$)$ is true. ... (Sometimes multiple b.c.) $P(0)$, $P(1)$)

Inductive case

Inductive case: Assume for strong induction that $P(k)$ is true

$\forall k \in \mathbb{Z}$, b.c. $\leq k \leq k$

⋮

Therefore $P(k+1)$ is true

Conclusion

By strong induction, we conclude $P(n)$ is true for all $n \geq$ b.c.

Metaphor: