Last time... we proved

- $\forall n \in \mathbb{N},\ Prime(n) \Rightarrow n > 1 \wedge Atomic(n)$
- $\forall n \in \mathbb{N},\ n > 1 \wedge Atomic(n) \Rightarrow Prime(n)$

Conclusion: $\forall n \in \mathbb{N},\ Prime(n) \Leftrightarrow n > 1 \wedge Atomic(n)$

Proof techniques:

direct, indirect (contrapositive), by cases

Today:
- by contradiction
- by induction

Proof by contradiction

Want to prove proposition P

- instead of proving "P is true"
- try to prove "P cannot be false"
- Assume (for a contradiction) that $\neg P$.

... try to prove something false...

Example: Prove there exist infinitely many prime numbers.

In predicate notation:

$$\forall n_0 \in \mathbb{N}, \exists n \in \mathbb{N}, n > n_0 \wedge \text{Prime}(n)$$

Proof: Let $n_0 \in \mathbb{N}$

Let $n =$ ____?____ ← hard!

Instead...

For a contradiction, assume there are finitely many primes.

High level intuition

- $\text{Primes} = \{p_1, p_2, \dots, p_n\}$ for some $n \in \mathbb{N}$

  ALL prime numbers

- Consider $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

  Eiter N is prime, or it isn't

- Case 1: if N is prime, then $N \notin \text{Primes}$

  $(N \neq p_1, N \neq p_2, \dots, N \neq p_n)$. contradiction!

- Case 2: if N is not prime, it must have some prime divisor q (Why?)

(q is prime and $q \mid N$)

Note: $q \neq p_1, q \neq p_2, \ldots, q \neq p_n$

- because N divided by p_i leaves a remainder of 1

Contradiction: $q \notin$ Primes

alternatively we can show $\gcd(N, p_i) = 1$

Proof by induction

Basic induction:

Want to prove $\forall n \in \mathbb{N}, P(n)$

(for some predicate $P: \mathbb{N} \to \{\text{True}, \text{False}\}$)

- **Base Case**: Prove $P(0)$.
- **Induction Hypothesis**: Let $n \in \mathbb{N}$. Assume $P(n)$.
- **Induction Step**: Prove $P(n+1)$.

What have we proved?

$$\boxed{P(0) \land \forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)}$$

induction allows us to make this "jump"

BY INDUCTION, $\forall n \in \mathbb{N},\ P(n)$

$\mathbb{N}$: 0 1 2 3 ... k k+1 k+2 ...

P is true ✓ ✓ ✓ ✓ ... ✓ ✓ ✓ ...

$$\Big(P(0) \land \forall n \in \mathbb{N},\ P(n)\Big) \Rightarrow P(n+1)$$ ✗

parentheses go around $(\forall \ldots \Rightarrow \ldots)$

Example: Prove $\forall n \in \mathbb{N},\ n \geq 3 \Rightarrow 2n+1 < 2^n$

- First, define predicate $P(n)$:
  - $P_1(n)$: $n \geq 3 \Rightarrow 2n+1 < 2^n$
  - $\boxed{P_2(n):\ 2n+1 < 2^n}$

    ↳ prove only for $n \geq 3$

- B.C.: Prove $P(3)$:

$$2 \cdot 3 + 1 = 7 < 8 = 2^3 \quad ✓$$

- I.H.: Let $n \in \mathbb{N}$ and assume $n \geq 3$.

  Assume $P(n)$: $2n+1 < 2^n$

• I.S.: (WTS $P(n+1)$: $2(n+1)+1 < 2^{n+1}$) goal

Proof of $P(n+1)$ — exercise!

Proof of I.S. (for reference, not covered during lecture):

$$\begin{aligned} 2(n+1)+1 &= \underbrace{2n+1}+2 \\ &< 2^n + 2 \quad \text{(by I.H.)} \\ &< 2^n + 2^n \quad (n \geq 3 \Rightarrow 2^n \geq 2^3 > 2^1) \\ &= 2^{n+1}. \quad \square \end{aligned}$$