Welcome back!

Last times:

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

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

Proof techniques:

How to prove $\forall$, $\exists$, $\Rightarrow$ (direct, indirect),

$\Leftrightarrow$, $\wedge$, $\vee$ (proof by cases)

Today:

- proof by contradiction
- proof by induction

Proof by contradiction

General idea: want to prove proposition P
- if proving "P is true" is too difficult
- instead, try to prove "P cannot be false"

Assume (for a contradiction) $\neg P$

... goal: reach a conclusion that we <u>know</u> is false — a contraction ...

Conclusion: $\underline{\neg P \Rightarrow \text{False}}$

↳ contrapositive: $\text{True} \Rightarrow P$

must be True

Example: Prove that there are infinitely many primes.

$\neg \left(\forall n_0 \in \mathbb{N}, \exists n \in \mathbb{N}, n > n_0 \wedge \mathrm{Prime}(n) \right)$

Proof: Let $n_0 \in \mathbb{N}$. Let $n =$ ___?___

For a contradiction, assume

$\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, \mathrm{Prime}(n) \Rightarrow n \leq n_0$

Insight: try to get a contradiction by finding a prime $> n_0$.

Consider $N = 1 + n_0! = 1 + \prod_{i=1}^{n_0} i$

Fact 1: N has a prime divisor, i.e.,

$\exists q \in \mathbb{N}, \mathrm{Prime}(q) \wedge q \mid N$ (why?)

Fact 2: $\forall d \in \mathbb{N},\ 1 < d \leq n_0 \Rightarrow d \nmid N$

— **Exercise**

(intuition: $\dfrac{N}{d} = \dfrac{(1 \cdot 2 \cdot \ldots \cdot d \cdot (d+1) \cdot \ldots \cdot n_0) + 1}{d}$

$\rightarrow$ always a remainder of 1 ...)

From fact 2, $q > n_0$ (where q is the prime divisor from Fact 1)

This contradicts the assumption!

Induction

- **Basic induction:** want to prove $\forall n \in \mathbb{N}, P(n)$,

  for some predicate $P : \mathbb{N} \rightarrow \{True, False\}$

Proof: by induction

- 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?

$$P(0) \wedge \left(\forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)\right)$$

induction allows us to jump from

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

intuition:

$\mathbb{N}$:	0	1	2	3	4	...
P:	✓	✓	✓	✓	✓	...

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

<u>First</u> define predicate

- $P(n)$: $\underbrace{n \geq 3 \Rightarrow 2n+1 < 2^n}$ — okay but a bit messy

$\Rightarrow$ $\underbrace{n+1 \geq 3 \Rightarrow 2(n+1)+1 < 2^{n+1}}$

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

<u>Proof by induction:</u>

- <u>B.C.</u>: (WTS $P(3)$)

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

• IH: Let $n \in \mathbb{N}$ and assume $n \geq 3$.

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

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

Body? $\boxed{\text{... exercise ...}}$

Conclusion: by induction, $\forall n \in \mathbb{N}$, $n \geq 3 \Rightarrow 2n+1 < 2^n$.

Ind. Step: $2(n+1)+1 = \underbrace{2n+1} + 2$

$< 2^n + 2$ (by Ind. Hyp.)

$< 2^n + 2^n$ $(n \geq 3 \Rightarrow 2^n \geq 2^3 > 2^1)$

$= 2^{n+1}$ $\square$

(NOT COVERED DURING LECTURE)