Proof:

header: introduce variables + assumptions

. A quant. stmt.
   Let \( x \) be an arbitrary ... 
   or Let \( x \in \ldots \)

. \( \exists \) quant stmt.
   Let \( x = \ldots \)
   (a computable value/expression could depend on pre-defined variables)

. universally quant implication.
   Let \( x \in \ldots \) and assume
   \( x \) satisfies ... 

proof body

contains a sequence of True statements, each following logically from previous

how do you know it follows

1. definitions
2. assumptions
3. previous deduction/statements
4. External facts / claims
The last statement should be the statement we are trying to prove.
(often conclusion of implication)

Stuck? Ask “what fact do I know to be True that I have not used yet?”

Don’t start deduction with the conclusion!

\[ \text{Prime}(p): \quad p > 1 \land \left( \forall d \in \mathbb{N}, \ d \mid p \Rightarrow (d = 1 \lor d = p) \right), \]

where \( p \in \mathbb{N} \).

\[ \forall a, b \in \mathbb{Z}, \ odd(a) \land odd(b) \Rightarrow odd(ab) \]

\[ \forall a, b \in \mathbb{Z}, \ 2 \nmid a \land 2 \nmid b \Rightarrow 2 \nmid (ab) \]

Consider
\[ \text{Atomic}(n): \quad \forall a, b \in \mathbb{N}, \ n \nmid a \land n \nmid b \Rightarrow n \nmid (ab), \]

where \( n \in \mathbb{N} \).

It turns out: \[ \forall n \in \mathbb{N}, \ n > 1 \land \text{Atomic}(n) \iff \text{Prime}(n) \]
prove it!

\[ p \Rightarrow q \] means \[ p \Rightarrow q \land q \Rightarrow p \]

Try to prove \[ \forall n \in \mathbb{N}, \ n > 1 \land \text{Atomic}(n) \Rightarrow \text{Prime}(n) \]

( later prove \[ \forall n \in \mathbb{N}, \ \text{Prime}(n) \Rightarrow n \geq 1 \land \text{Atomic}(n) \]

unpack def.:
\[ \forall n \in \mathbb{N}, (n > 1 \land (\forall a, b \in \mathbb{N}, n | a \land n | b \Rightarrow n | ab)) \Rightarrow \text{Prime}(n) \]

complicated!

Structure of problem: \[ \forall n \in \mathbb{N}, \ P(n) \Rightarrow Q(n) \]

recall:
\[ (p \Rightarrow q) \iff (-q \Rightarrow -p) \]

we could equivalently try to prove \[ \forall n \in \mathbb{N}, -Q(n) \Rightarrow -P(n) \]

- Sometimes working with the assumption \[ -Q(n) \] is easier than working with the assumption \[ P(n) \]

Get an "indirect proof" or "proof of the contrapositive"

- Now consider
\[ \forall n \in \mathbb{N}, \ \neg \text{Prime}(n) \Rightarrow \neg (n > 1 \land \text{Atomic}(n)) \]
\[ \forall n \in \mathbb{N}, \neg \text{Prime}(n) \implies (n \leq 1 \lor \neg \text{Atomic}(n)) \]

**Prime** \((n)\): \( n > 1 \land (\forall d \in \mathbb{N}, d \mid n \Rightarrow (d = 1 \lor d = n)) \)

\[ \neg \text{Prime}(n) : n \leq 1 \lor (\exists d \in \mathbb{N}, d \mid n \land d \neq 1 \land d \neq n) \]

**Atomic** \((n)\): \( \forall a, b \in \mathbb{N}, n \mid a \land n \mid b \implies n \mid ab \)

\[ \neg \text{Atomic}(n) : \exists a, b \in \mathbb{N}, n \mid a \land n \mid b \land n \not\mid ab \]

**Claim:** Proving an \( \exists \) may be easier than proving a \( \forall \)

**Discuss:** We will assume \( \neg \text{Prime}(n) \)

\[ \text{we know } n \leq 1 \]

or there is some \( d \neq 1, n \) that divides \( n \)

we will need to find an \( a, b \) such that \( n \mid a, n \mid b \) and \( n \not\mid ab \)

**Suppose** \( n = 6 \) \((\text{not prime})\)

Then \( n = 2 \cdot 3 \)

will need to find \( a, b \) s.t. \( n \mid a \land n \mid b \land n \not\mid ab \)
Let $a = 2$, $b = 3$

Then $6 \parallel 2$, $6 \times 3$, $6 \parallel 6$ !

$n = 12$

$12 = 2 \cdot 6$

$12 = 3 \cdot 4$

both work as $a, b$

Generalizing: Since $\neg \text{Prime}(n)$, we can find $n_1, n_2$ s.t. $1 < n_1, n_2 < n$

and $n = n_1 n_2$

then picking $a = n_1$ and $b = n_2$ gives properties we need.

Proof:

Let $n \in \mathbb{N}$ and assume $n$ is not Prime.

Then by negating the definition of Prime, either $n \leq 1$ or there exists $d \in \mathbb{N}$, $d \mid n \land d \neq 1 \land d \neq n$.

We can divide the rest of the proof into cases, depending whether or not $n \leq 1$.

Case 1: Assume $n \leq 1$.

Then $n \leq 1 \lor \neg \text{Atomic}(n)$ is True, as reg'd.
Case 2: Assume \( \exists d \in \mathbb{N}, d \mid n \land d \neq 1 \land d \neq n \) 

Expanding the divide predicate says 
\[ \exists k \in \mathbb{N}, \; n = d \cdot k. \]

We know \( \exists d, k \in \mathbb{N}, n = d \cdot k \land d \neq 1 \land d \neq n \)

Let \( a = d \) and \( b = k \). We want to show that \( n \nmid a \land n \nmid b \land n \mid ab \)

We know \( n \mid ab \) since \( ab = d \cdot k = n \)

Also since \( n = d \cdot k \), where \( d, n, k \in \mathbb{N} \), and \( d \neq 1 \) and \( d \neq n \), \( n > a \), \( n > b \) and so \( n \nmid a \) and \( n \nmid b \).

We have proven that 
\[ \forall n \in \mathbb{N}, \; n > 1 \land \text{Atomic}(n) \Rightarrow \text{Prime}(n) \]

using an indirect proof.

Does \( \text{Prime}(n) \Rightarrow n > 1 \land \text{Atomic}(n) \)

next week!