- PS1 FAQ now available on course website
- Course notes available in bookstore

- This week: PROOFS!
  Proof = convincing argument

- In general
  English statement
  ↓
  Predicate statement
  ↓
  Rough work
  (“discussion" in the notes)
  ↓
  Proof header
  ↓
  Proof body: deductions with justifications

\[ \forall x \in D, P(x) \]

Proof header
Let \( x \in D \)
(let \( x \) be an arbitrary but fixed element of \( D \))
$\exists x \in D, P(x)$  

Let $x =$ (some specific value)

$P \Rightarrow Q$  

Assume $P$  

(try to prove $Q$)

---

**Ex:** Prove that every natural number $n$ greater than 20 satisfies $1.5n - 4 \geq 3$.

1. \( \forall n \in \mathbb{N}, \ n > 20 \Rightarrow 1.5n - 4 \geq 3 \)

2. Proof headers:

   Let $n \in \mathbb{N}$, and assume $n > 20$.

---

**PAUSE! Rough work...**

\[ 1.5n - 4 \geq 3 \iff 1.5n \geq 7 \]

\[ \iff n \geq \frac{7}{1.5} \]

---

3. Complete proof:
* Let \( n \in \mathbb{N} \), assume \( n > 20 \).

Then \( n \geq 5 \)

**optional**

So \( 1.5n \geq 7.5 \)  
(mult. both sides by 1.5)

Then \( 1.5n - 4 \geq 3.5 \geq 3 \)

- justification is optional for simple arithmetic and algebraic manipulation

\[ S_1: \forall n \in \mathbb{N}, \ n > 20 \ \Rightarrow \ 1.5n - 4 \geq 3 \]

\[ S_2: \forall n \in \mathbb{N}, \ n > 20 \ \Rightarrow \ 1.5n - 4 \geq 3 \]

\[ S_3: \forall n \in \mathbb{N}, \ n > 20 \ \Rightarrow \ 1.5n - 4 \geq 3 \]

syntax error: does not have a meaning

\( S_2 \) means "every natural number is >20 and satisfies \( 1.5n - 4 \geq 3 \)"

Exercise: To prove \( S_2 \) is False, simply prove \( \neg S_2 \) is True.

\[ S_4: \exists n \in \mathbb{N}, \ n > 20 \land 1.5n - 4 \geq 3 \]

\[ S_5: \exists n \in \mathbb{N}, \ n > 20 \ \Rightarrow \ 1.5n - 4 \geq 3 \]

\( \times \)

does not have a natural English meaning
Proof example 2: Prove that for all integers \( x \), if \( x \mid x+5 \), then \( x \mid 5 \).

1. Translation:
   \[
   \forall x \in \mathbb{Z}, \ (x \mid x+5) \Rightarrow (x \mid 5)
   \]

   EXPAND
   DEFINITION

   \[
   \forall x \in \mathbb{Z}, \ (\exists k_1 \in \mathbb{Z}, x+5 = k_1 x) \\
   \Rightarrow (\exists k_2 \in \mathbb{Z}, \ 5 = k_2 x)
   \]

2. Proof headers
   Let \( x \in \mathbb{Z} \). Assume \( \exists k_1 \in \mathbb{Z}, x+5 = k_1 x \).

   convention: "assume \( \exists \)" introduces a new variable (\( k_1 \)). At this point, we can use
   - \( x \in \mathbb{Z} \)
   - \( k_1 \in \mathbb{Z}, \ x+5 = k_1 x \)

   We want to prove \( \exists k_2 \in \mathbb{Z}, \ 5 = k_2 x \).

   Let \( k_2 = \frac{k_1 - 1}{x} \)

   We want to show \( 5 = k_2 x \).

Time to think! (Rough work)
NOT PART OF PROOF
Consider \( 5 = k_2 x \) \( \Rightarrow \) \( k_2 = \frac{5}{x} \)

PROBLEM: \( \frac{5}{x} \) may not be an integer!
Instead, consider \( x+5 = k_1x \)

pick \( k_2 = k_1 - 1 \) \( \leq \)
\[
5 = k_1x - x \\
5 = (k_1 - 1)x
\]

(back to proof)

Then,
(by assumption) \( x + 5 = k_1x \)
\[
5 = k_1x - x \\
5 = (k_1 - 1)x
\]
(by def.) \( 5 = k_2x \)

Q.E.D.

Then,
\[
5 = k_2x \\
5 = (k_1 - 1)x
\]
\[
5 = k_1x - x \\
x + 5 = k_1x
\]

BACKWARDS

Note: in general, justifying why \( k_2 \in \mathbb{Z} \) is important — here, okay to leave out because it is so simple.

Generalization:

For all integers \( d, x \),
if \( x | (x+d) \), then \( x | d \) ?

Proof generalization:

* substitute \( d \) for \( 5 \) in previous proof;
  does it still work?

Further: \( x | ax + d \Rightarrow x | d \) ?