Mathematical Proofs

Announcements

- ***Pset 0***
  - Due ~~Friday~~ Monday
- ***Pset 1***
  - Goes out Friday, due following Friday
  - LaTeX Beginner's Quick Start Tutorial (LaTeX is the preferred tool for writing homework in this class)
- ***Office Hours***
  - They start Monday! Schedule will be on the course website by Friday. They will be accessible in person (or by Zoom for CGOE students).

Outline for Today

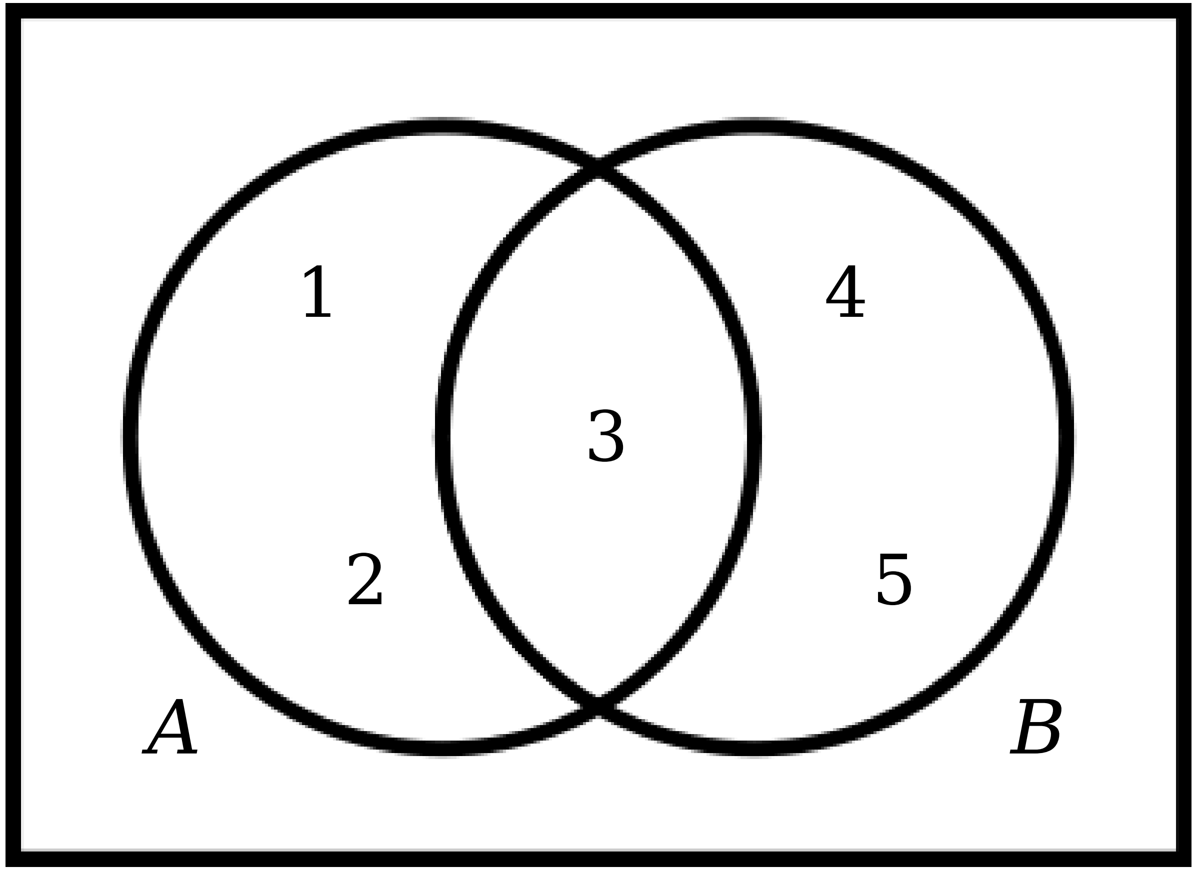
- ***How to Write a Proof***
    - Synthesizing definitions, intuitions, and conventions.
- ***Proofs on Numbers***
    - Working with odd and even numbers.
- ***Universal and Existential Statements***
    - Two important classes of statements.
- ***Variable Ownership***
    - Who owns what?

Quick Addendum to Monday's

Set Theory Lecture:

Combining Sets

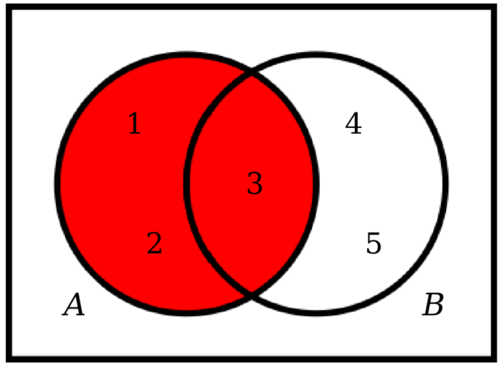
Venn Diagrams



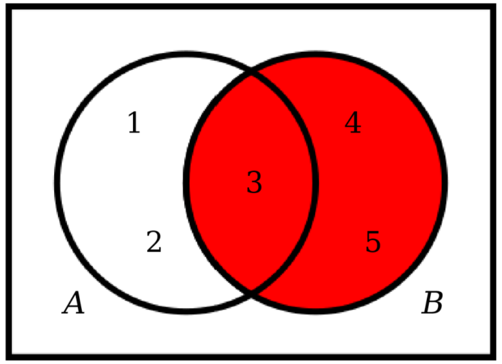
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

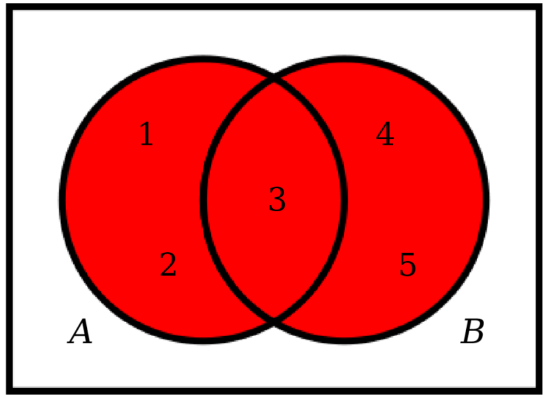
Venn Diagrams

A



B

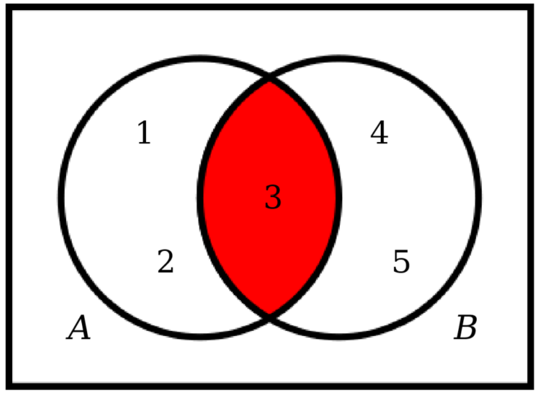




Union

$A \cup B$

{ 1, 2, 3, 4, 5 }



Intersection

$A \cap B$

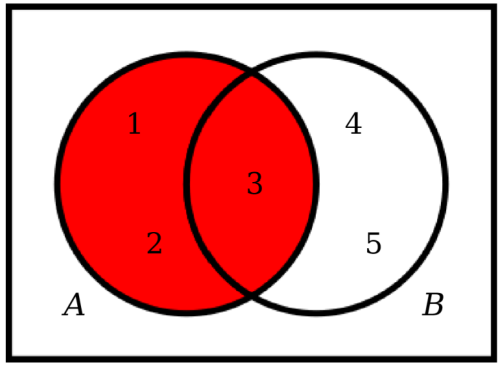
{ 3 }

$A = \{ 1, 2, 3 \}$

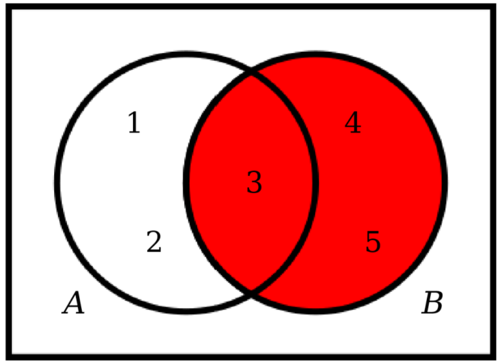
$B = \{ 3, 4, 5 \}$

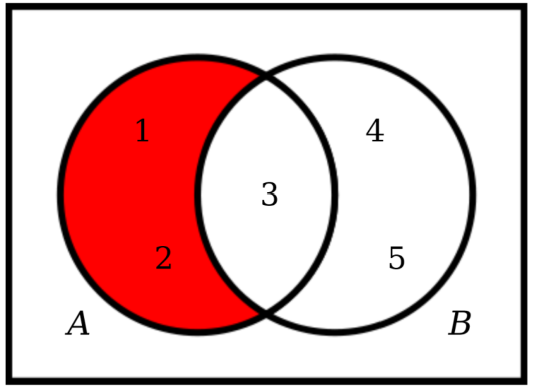
Venn Diagrams

A



B



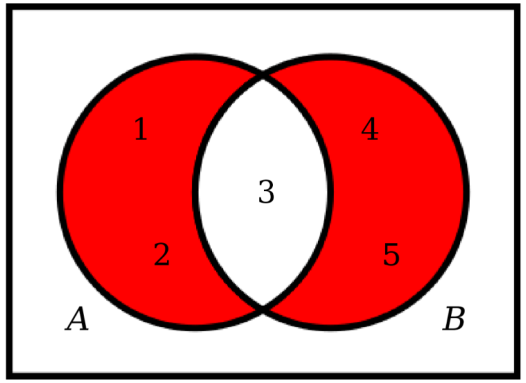


Difference

$A - B$

$A \setminus B$

$\{ 1, 2 \}$



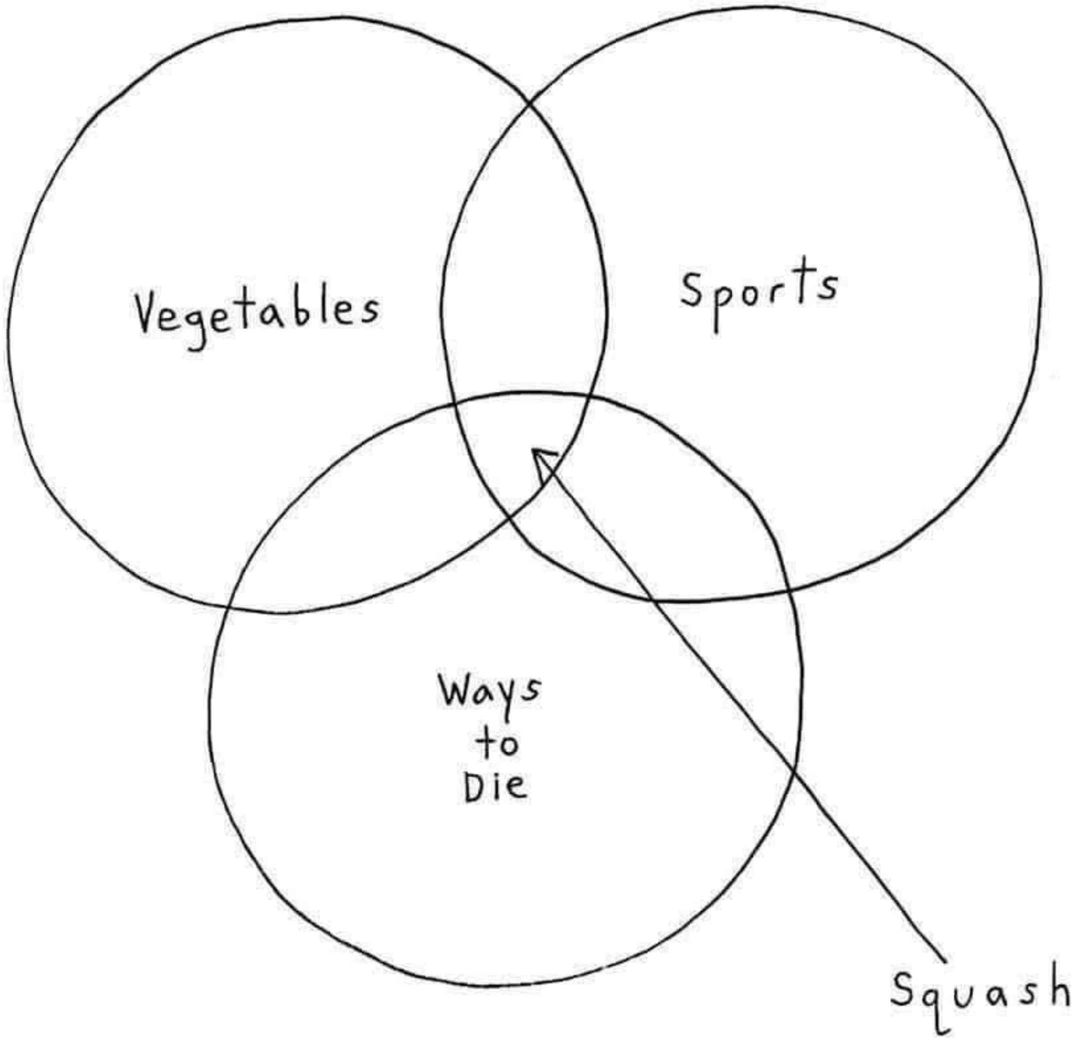
Symmetric Difference

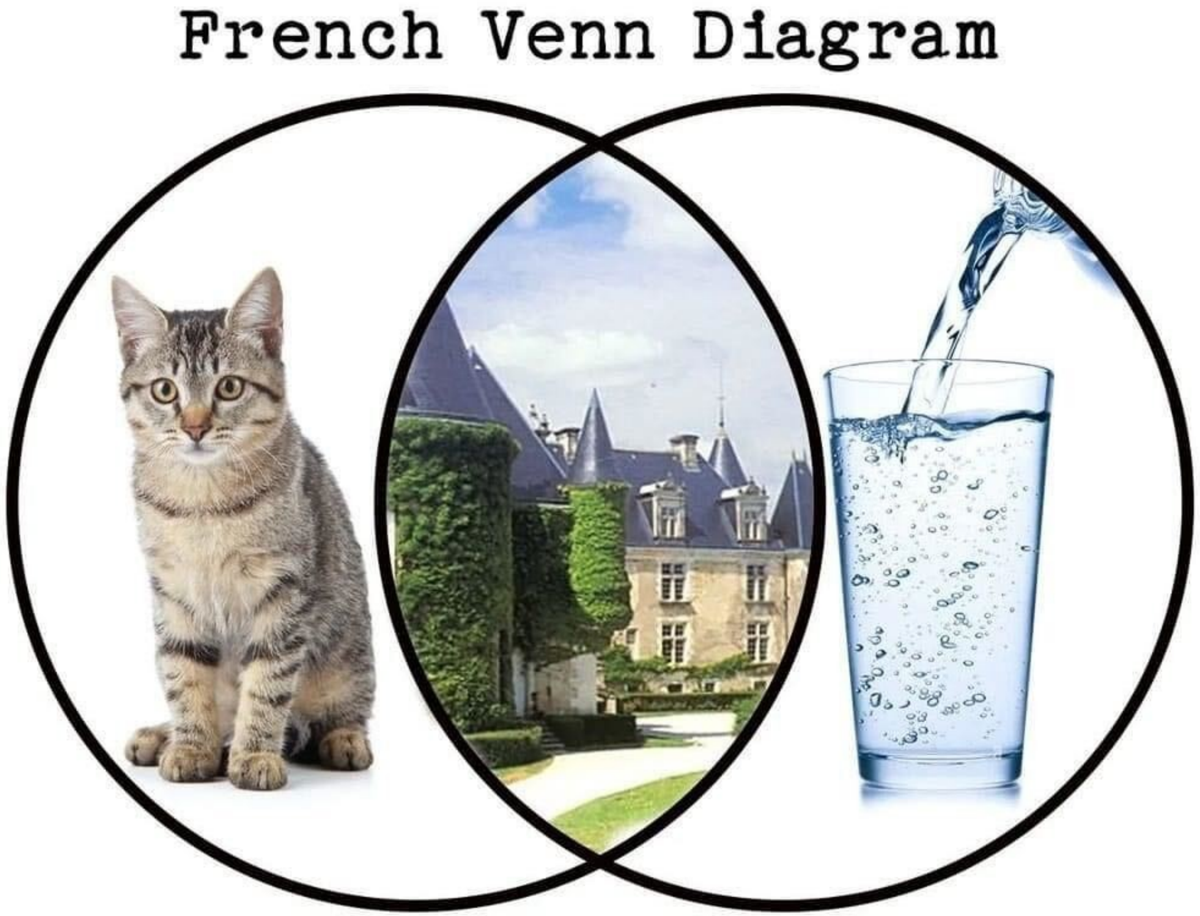
$A \Delta B$

$\{ 1, 2, 4, 5 \}$

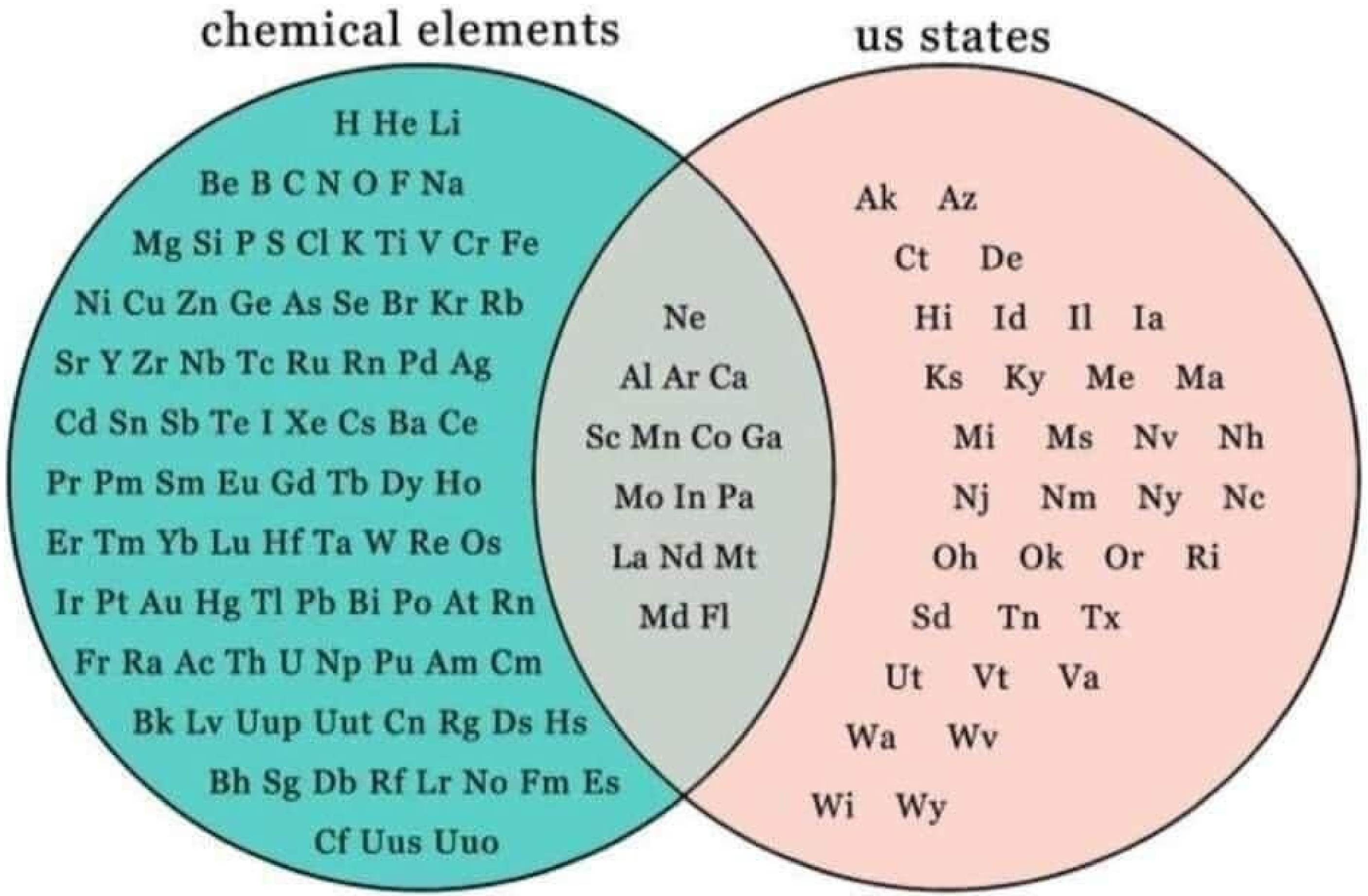
$$A = \{ 1, 2, 3 \}$$
$$B = \{ 3, 4, 5 \}$$

Venn Diagrams





Venn Diagrams



What is a Proof?

A ***proof*** is an argument that demonstrates why a conclusion is true, subject to certain standards of truth.

A ***mathematical proof*** is an argument that demonstrates why a mathematical statement is true, following the rules of mathematics.

Proofwriting is not like other forms of writing, or even other forms of math problems, and we understand this can be a big adjustment!

Here is some advice from years of teaching proofwriting.

Rule: Proofs are meant to argue something precisely and completely.

Advice: Well trained readers should find this persuasive, however *precision* and *completeness* are the goals you should have in mind, <u>not</u> *persuasion* in the usual social-emotional-rhetorical way that we think of persuasion.

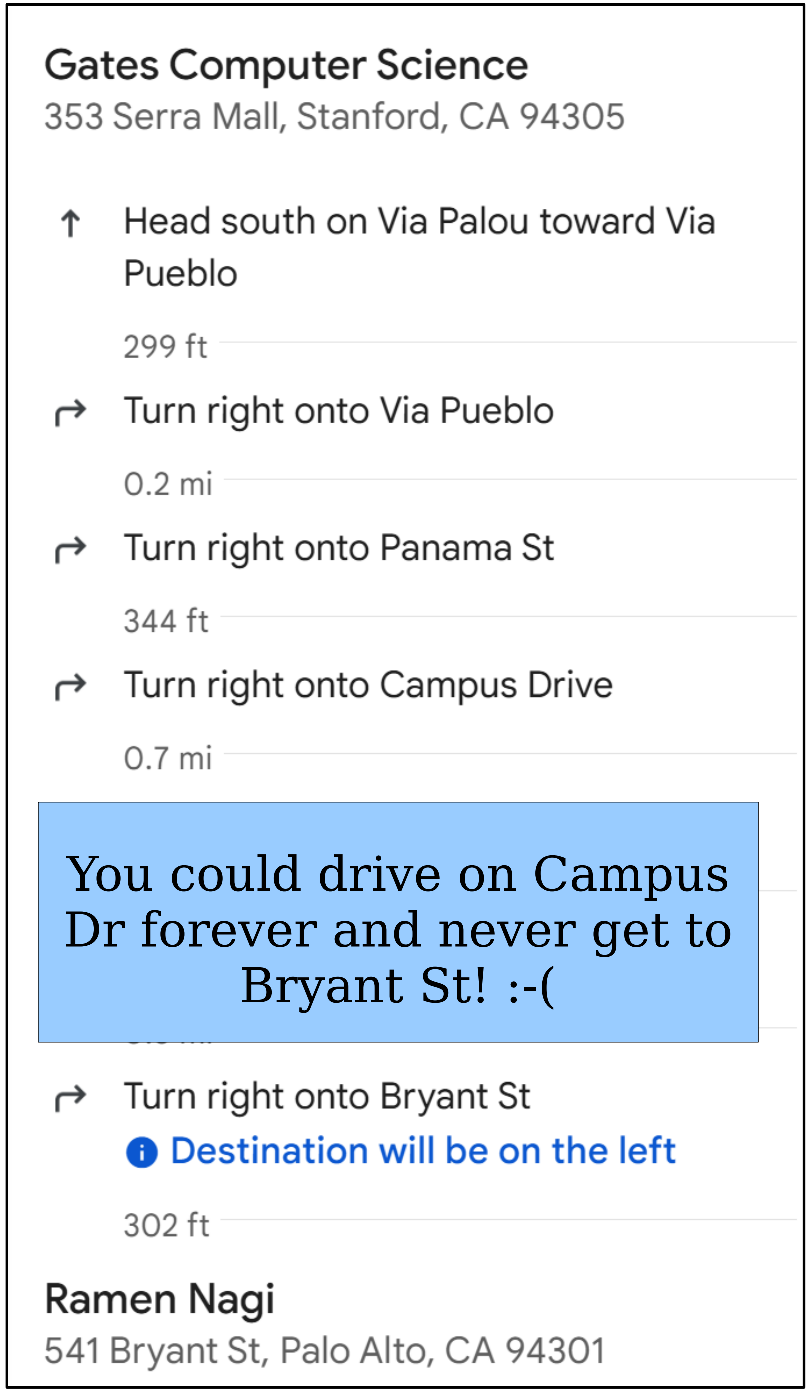
Rule: Proofs are structured, mechanical, functional. They describe precise processes (algorithms) on formally introduced variables.

Advice: Think of a proof less as storytelling and more like programming (or driving directions, as we'll see next). Though, it can be very helpful as a proofwriter to have a vision of the story you want to tell in your mind and, as you write, translate that story into proof structure.

Rule: Skipping even one step of a proof is a big deal—it makes the proof logically invalid.

Advice: Think of a proof as written driving directions from Point A to Point B, for someone who has never been, and who doesn't have a GPS/phone. If you leave out one step, the driver will never get to the next street name in the sequence. They simply can't continue, and will be permanently lost!

Proofs are powerful, but their correctness is quite fragile.



Writing our First Proof

Definitions:

An integer n is called ***even*** if
there is an integer k where $n = 2k$.

An integer n is called ***odd*** if
there is an integer k where $n = 2k + 1$.

Additionally, in this class, we will assume the following:
1. Every integer is either even or odd.
2. No integer is both even and odd.

Theorem: For all integers n, if n is even, then n^2 is even.

Theorem: For all integers n, if n is **even**, then n^2 is **even**.

Step 1: find the formal definitions for any terms in the theorem. (Not just what you intuitively understand the concept of “even” to mean.)

Theorem: For all integers n, if n is **even**, then n^2 is **even**.

Step 1: find the formal definitions for any terms in the theorem. (Not just what you intuitively understand the concept of "even" to mean.)

Definition:

An integer n is called ***even*** if there is an integer k where $n = 2k$.

Theorem: For all integers n, if n is even, then n^2 is even.

Step 2: examine the grammatical structure of the theorem, because this dictates how we will structure our proof.

Theorem: **For all** integers n, **if** n is even, **then** n^2 is even.

Step 2: examine the grammatical structure of the theorem, because this dictates how we will structure our proof.

“For all” means we need this to be true for all examples of elements of the set integers. So we challenge our reader: “pick ANY integer!!”

***Theorem:* For all** integers n, **if** n is even, **then** n^2 is even.

Step 2: examine the grammatical structure of the theorem, because this dictates how we will structure our proof.

The “if...then...” means that the “then” part is only guaranteed to hold when the “if” part is true. So we are going to tell our reader to pick any integer **assuming** that the “if” condition is true of it. In other words, only pick even integers.

Theorem: **For all** integers n, **if** n is even, **then** n^2 is even.

Step 2: examine the grammatical structure of the theorem, because this dictates how we will structure our proof.

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof:

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n.

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$.

Definition:

An integer n is called ***even*** if there is an integer k where $n = 2k$.

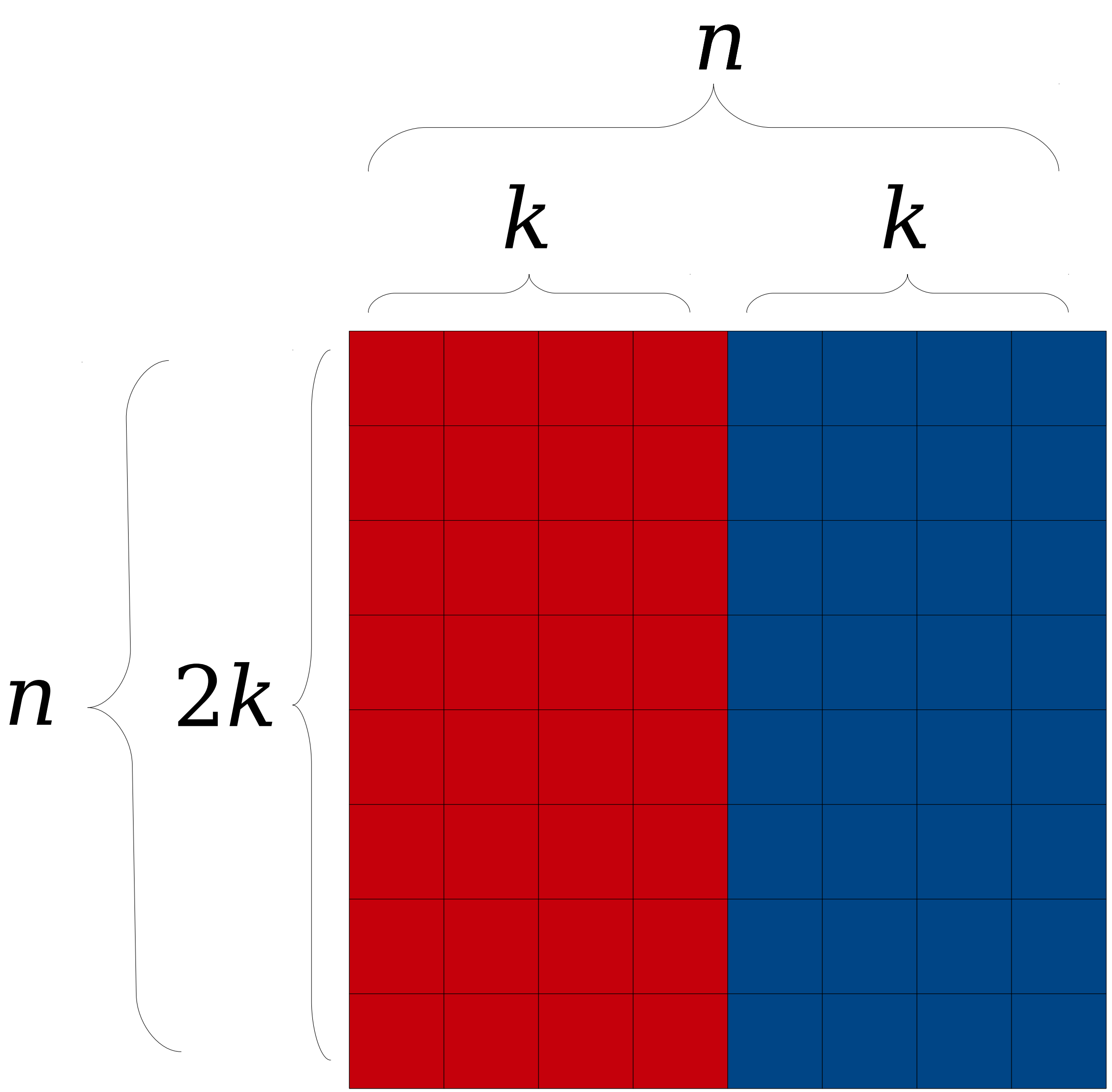
You Could Try Some Examples

$$
\begin{aligned}
2^2 &= 4 &&= 2 \cdot \mathbf{2} \\
10^2 &= 100 &&= 2 \cdot \mathbf{50} \\
0^2 &= 0 &&= 2 \cdot \mathbf{0} \\
(-8)^2 &= 64 &&= 2 \cdot \mathbf{32} \\
n^2 & &&= 2 \cdot \mathbf{?}
\end{aligned}
$$

What’s the pattern? How do we predict this?

Theorem: For all integers n, if n is even, then n2 is even.

🤔 You Could Draw Some Pictures



$$n^2 = 2(2k^2)$$

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$n^2 = (2k)^2$$

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$n^2 = (2k)^2$$
$$= 4k^2$$

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$
\begin{aligned}
n^2 &= (2k)^2 \\
&= 4k^2 \\
&= 2(2k^2).
\end{aligned}
$$

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show.

> ***Definition:***
>
> An integer n is called ***even*** if there is an integer k where $n = 2k$.

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$n^2 = (2k)^2$$
$$= 4k^2$$
$$= 2(2k^2).$$

This symbol means “end of proof.” It’s basically math nerd “mic drop.”

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

…teger k such

…is an int…
(namely, $2k^2$) where $n^2 = 2m$. Therefo…
is even, which is what we wanted to…

To prove a statement of the form

"For all x…"

Pick an arbitrary x.

To prove a statement of the form

"If *P*, then *Q*."

Start by assuming ***P***, then state "We want to show that ***Q***."

Our First Proof!

Theorem: For all integers n, if n is even, th

even.

"**Assume**"

Proof: Pick an arbitrary even integer n. We want to show that n^2 is even.

Since n is even, there is some integer

that $n = 2k$. This means that

"**Want to Show**"
(nickname "WTS" for short)

These first two sentences of setup for the proof are so critical that they have their own names to refer to them!

integer m

(namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our First Proof!

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Pick an arbitrary even integer n. We need to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our Next Proof

Theorem: For all integers m and n,
if m and n are odd, then $m + n$ is even.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof:

To prove a statement of the form

"For all x…"

Pick an arbitrary x.

To prove a statement of the form

"If *P*, then *Q*."

Start by assuming ***P***, then state "We want to show that ***Q***."

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof:

NOT FOR CREDIT TODAY
(just dry run)

PollEv.com/cs103spr26

Your Turn: How many of these would be a good first sentence of our proof? (the "Assume" step)

- We want to show that if m and n are odd, then m + n is even.
- Pick arbitrary odd integers n and m.
- Consider n=7 and m=3.
- Let n and m be arbitrary integers.
- Since n and m are odd, there are integers k and r such that n=2k + 1 and m = 2r + 1.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary odd integers m and n.

To prove a statement of the form

"For all x…"

Pick an arbitrary x.

To prove a statement of the form

"If *P*, then *Q*."

Start by assuming ***P***, then state "We want to show that ***Q***."

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary odd integers m and n. We want to show that $m + n$ is even.

Assume	**Want to Show** (nickname "WTS" for short)

To prove a statement of the form

"For all x…"

Pick an arbitrary x.

To prove a statement of the form

"If *P*, then *Q*."

Start by assuming ***P***, then state "We want to show that ***Q***."

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Definition:

An integer n is called ***odd*** if there is an integer k where $n = 2k + 1$.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \quad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \quad (2)$$

Definition:

An integer n is called ***odd*** if there is an integer k where $n = 2k + 1$.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \qquad (2)$$

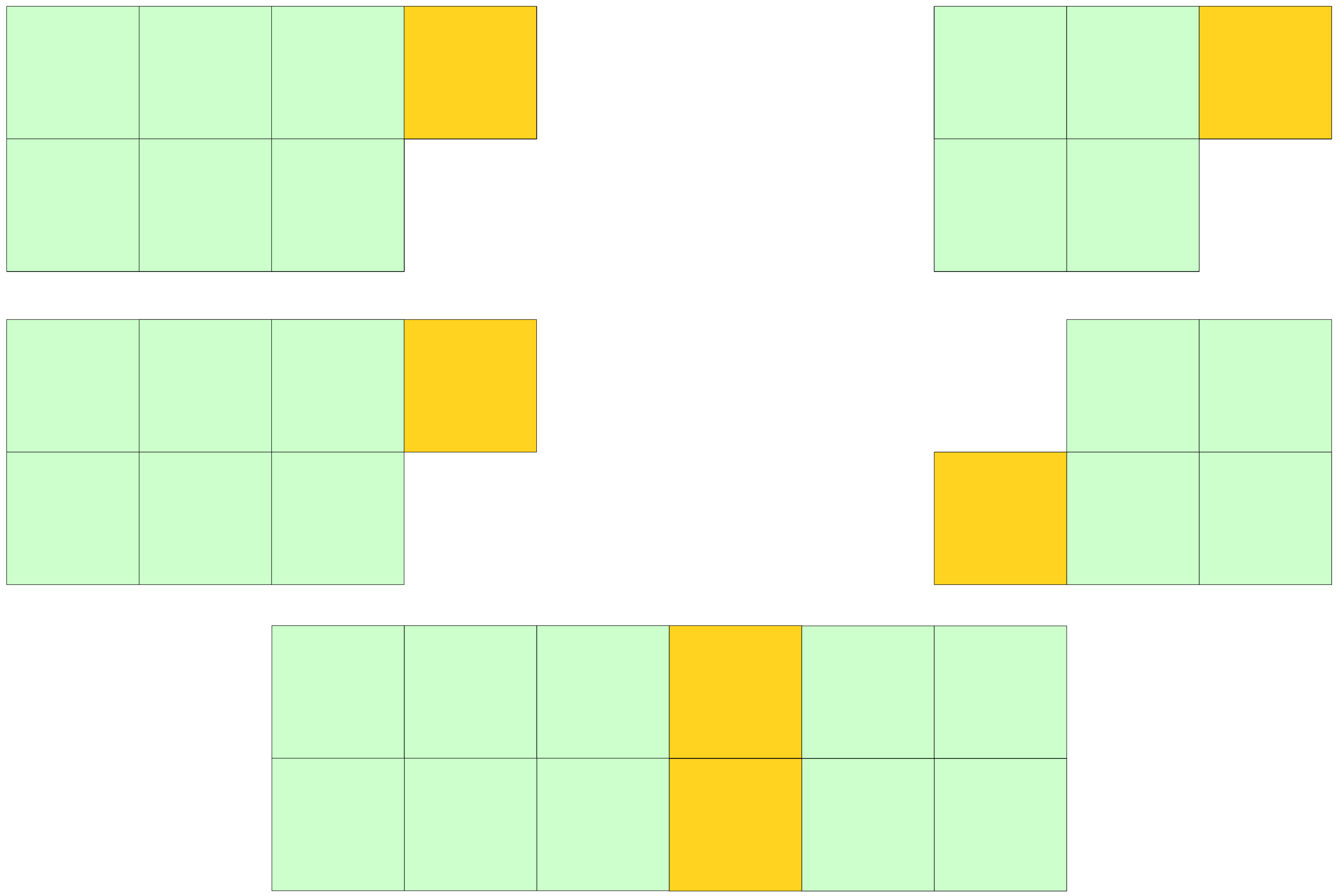
By adding equations (1) and (2) we learn that

$$m + n = 2k + 1 + 2r + 1$$

🤔 You Could Draw Some Pictures

$2k+1$

$2r+1$



$$(2k+1) + (2r+1) = 2(k + r + 1)$$

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \quad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \quad (2)$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \end{aligned}$$

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned}$$

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd,

Similarly, becau
that

By adding equa

We ask the reader to make an ***arbitrary choice***. Rather than specifying what m and n are, we're signaling to the reader that they could, in principle, supply any choices of m and n that they'd like.

By letting the reader pick m and n arbitrarily, anything we prove about m and n will <u>generalize</u> to all possible choices for those values.

This bold challenge to take on any choice of values makes our proof strong!

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrar
odd. We want to s

Style note: *(optional)* Numbering these equalities lets us refer back to them later on, making the flow of the proof a bit easier to understand.

Since m is odd, w

$$m = 2k + 1. \quad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \quad (2)$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \quad (3) \end{aligned}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Similarly, becaus… is odd there must be some integer r such

(2)

…earn that

$$+ 2r + 1$$

$$= 2k + 2r + 2$$

$$= 2(k + r + 1). \qquad (3)$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Style note: *(required)* This is a complete sentence! Proofs are expected to be written in complete sentences, so you'll often use punctuation at the end of formulas.

Theorem: For all integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Pick arbitrary integers m and n where m and n are odd. We want to show that $m + n$ is even.

Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \qquad (2)$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \qquad (3) \end{aligned}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Some Little Exercises

- Here’s a list of other theorems that are true about odd and even numbers:
  - ***Theorem:*** The sum and difference of any two even numbers is even.
  - ***Theorem:*** The sum and difference of an odd number and an even number is odd.
  - ***Theorem:*** The product of any integer and an even number is even.
  - ***Theorem:*** The product of any two odd numbers is odd.
- Going forward, we’ll just take these results for granted. Feel free to use them in the problem sets.
- If you’d like to practice the techniques from today, try your hand at proving these results!

Universal and Existential Statements

Theorem: For all odd integers n,
there exist integers r and s where $r^2 - s^2 = n$.

Theorem: For all odd integers n, there exist integers r and s where $r^2 - s^2 = n$.

This result is true for every possible choice of odd integer n. It'll work for $n = 1$, $n = 137$, $n = 103$, etc.

Theorem: For all odd integers n, there exist integers r and s where $r^2 - s^2 = n$.

We aren't saying this is true for every choice of r and s. Rather, we're saying that ***somewhere out there*** are (one or more) choices of r and s where this works.

Universal vs. Existential Statements

- A ***universally-quantified statement*** is a statement of the form

  For all *x*, `[some-property]` holds for *x*.

- We've seen how to prove these statements.
- An ***existentially-quantified statement*** is a statement of the form

  There is some *x* where `[some-property]` holds for *x*.

- How do you prove an existentially-quantified statement?

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof:

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof:

Your Turn:

- Write the first sentence of the proof (Assume step).

To prove a statement of the form

"For all x…"

Pick an arbitrary x.

To prove a statement of the form

"If *P*, then *Q*."

Start by assuming ***P***, then state "We want to show that ***Q***."

NOT FOR CREDIT TODAY
(just dry run)

PollEv.com/cs103spr26

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n.

Your Turn:

- Write the second sentence of the proof (WTS step).

To prove a statement of the form

"For all x…"

Pick an arbitrary x.

To prove a statement of the form

"If *P*, then *Q*."

Start by assuming ***P***, then state "We want to show that ***Q***."

NOT FOR CREDIT TODAY
(just dry run)

PollEv.com/cs103spr26

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$.

Proving an Existential Statement

- Over the course of the quarter, we will see several different ways to prove an existentially-quantified statement of the form

  There is an *x* where `[some-property]` holds for *x*.

- ***Approach:*** Search far and wide, find a *concrete example value* for *x* that has the right property. In the proof, (1) announce the find to your reader, *then* (2) show why your choice is correct.

🤔 You Could Draw Some Pictures

$$1 = \_\_\_^2 - \_\_\_^2$$

$$3 = \_\_\_^2 - \_\_\_^2$$

$$5 = \_\_\_^2 - \_\_\_^2$$

$$7 = \_\_\_^2 - \_\_\_^2$$

$$9 = \_\_\_^2 - \_\_\_^2$$

Theorem: For all odd integers n,
there exist integers r and s where $r^2 - s^2 = n$.

🤔 You Could Try Some Examples

$$1 = \mathbf{1}^2 - \mathbf{0}^2$$

$$3 = \mathbf{2}^2 - \mathbf{1}^2$$

$$5 = \mathbf{3}^2 - \mathbf{2}^2$$

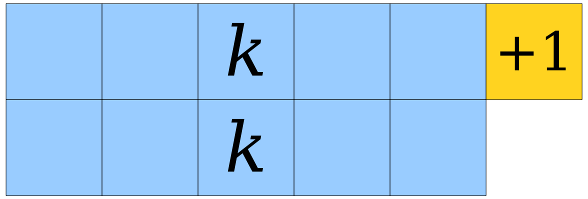
$$7 = \mathbf{4}^2 - \mathbf{3}^2$$

$$9 = \mathbf{5}^2 - \mathbf{4}^2$$

We've got a pattern – but why does this work?

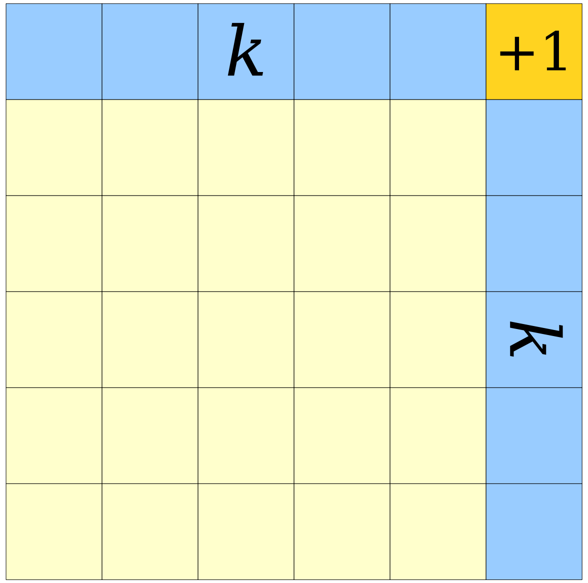
Theorem: For all odd integers n,
there exist integers r and s where $r^2 - s^2 = n$.

🤔 You Could Draw Some Pictures



Theorem: For all odd integers n,
there exist integers r and s where $r^2 - s^2 = n$.

🤔 You Could Draw Some Pictures



$$(k+1)^2 - k^2 = 2k+1$$

Theorem: For all odd integers n,
there exist integers r and s where $r^2 - s^2 = n$.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$r^2 - s^2 = (k+1)^2 - k^2$$

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \end{aligned}$$

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \end{aligned}$$

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 – s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 – s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$
\begin{aligned}
r^2 - s^2 &= (k+1)^2 - k^2 \\
&= k^2 + 2k + 1 - k^2 \\
&= 2k + 1 \\
&= n.
\end{aligned}
$$

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Assume

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Want to Show

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. **Now, let $r = k+1$ and $s = k$.** Then see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Our WTS is an existential statement, so we followed that pattern:

First we announce concrete choices of the objects being sought out.

Second, we demonstrate correctness of the choice.

Theorem: For all integers n, if n is odd, then there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick an arbitrary odd integer n. We will show that there exist integers r and s where $r^2 - s^2 = n$.

Since n is odd, we know there is an integer k where $n = 2k + 1$. Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: If n is an integer, then $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$.

Floors and Ceilings

- The notation $\lceil x \rceil$ represents the ***ceiling*** of x, the smallest integer greater than or equal to x.

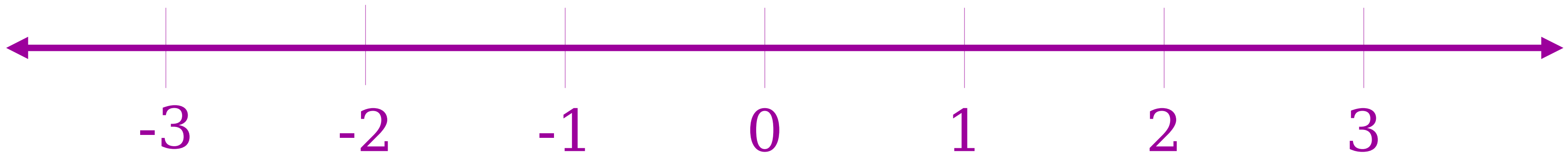
$$\lceil 1 \rceil = 1 \qquad \lceil 1.5 \rceil = 2$$

$$\lceil -1 \rceil = -1 \qquad \lceil -1.5 \rceil = -1$$

- The notation $\lfloor x \rfloor$ represents is the ***floor*** of x, the largest integer less than or equal to x.

$$\lfloor 1 \rfloor = 1 \qquad \lfloor 1.5 \rfloor = 1$$

$$\lfloor -1 \rfloor = -1 \qquad \lfloor -1.5 \rfloor = -2$$



Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Your Turn:

- Write the first sentence of the proof (Assume step).

NOT FOR CREDIT TODAY
(just dry run)

PollEv.com/cs103spr26

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer.

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer.

Your Turn:

- Write the second sentence of the proof (WTS step).

NOT FOR CREDIT TODAY
(just dry run)

PollEv.com/cs103spr26

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer. We want to show that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer. We want to show that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Hmmm...are we stuck? Typically, our third sentence (after the Assume and WTS sentences) is an expansion of a definition word, such as “even” or “odd.” Here we just have an integer, so there’s no definition to expand.

Let’s take a moment to do some work on scratch paper and see if we can find a way forward?

🤔 You Could Try Some Examples

Scratch paper work.

$$\lceil 0/2 \rceil + \lfloor 0/2 \rfloor = 0 + 0 = 0$$

$$\lceil 1/2 \rceil + \lfloor 1/2 \rfloor = 1 + 0 = 1$$

$$\lceil 2/2 \rceil + \lfloor 2/2 \rfloor = 1 + 1 = 2$$

$$\lceil 3/2 \rceil + \lfloor 3/2 \rfloor = 2 + 1 = 3$$

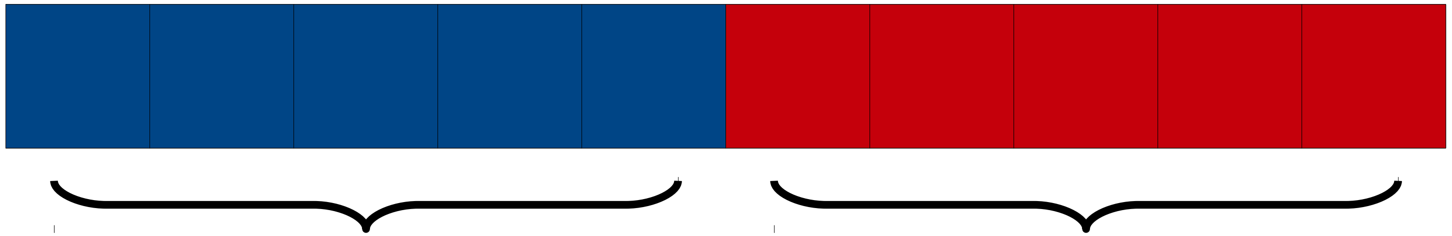
$$\lceil 4/2 \rceil + \lfloor 4/2 \rfloor = 2 + 2 = 4$$

Theorem: If n is an integer, then $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$.

You Could Draw Some Pictures

Scratch paper work.

Hm, too bad we weren’t asked to this proof for a theorem that says that *n* is even—that looks easy!

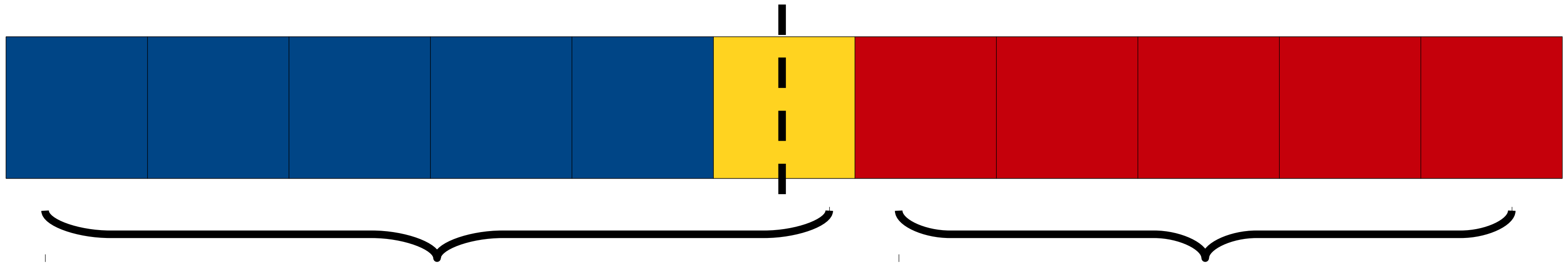


$$\lceil n/2 \rceil \qquad \lfloor n/2 \rfloor$$

$$n = 2k$$

Theorem: If n is an integer, then $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$.

You Could Draw Some Pictures



$\lceil n/2 \rceil$ $\lfloor n/2 \rfloor$

Scratch paper work.

Hm, too bad we weren't asked to this proof for a theorem that says that *n* is odd—a little harder than even, but we can still find a way.

$$n = 2k + 1$$

Theorem: If n is an integer, then $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$.

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer. We want to show that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$. To do so, we consider two cases:

Case 1: n is even.

Turns out that we can just smash our two proofs together—the odd one and the even one—and that counts as a proof for *all* integers—yay!!

Thanks, **Proof by Cases**!

Case 2: n is odd.

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer. We want to show that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$. To do so, we consider two cases:

Case 1: n is even. This means there is an integer k such that $n = 2k$. Some algebra then tells us that

$$\begin{aligned} \left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor &= \left\lceil \frac{2k}{2} \right\rceil + \left\lfloor \frac{2k}{2} \right\rfloor \\ &= \lceil k \rceil + \lfloor k \rfloor \\ &= 2k \\ &= n. \end{aligned}$$

Case 2: n is odd. Then there's an integer k where $n = 2k + 1$, and

$$\begin{aligned} \left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor &= \left\lceil \frac{2k+1}{2} \right\rceil + \left\lfloor \frac{2k+1}{2} \right\rfloor \\ &= \left\lceil k + \frac{1}{2} \right\rceil + \left\lfloor k + \frac{1}{2} \right\rfloor \\ &= (k+1) + k \\ &= 2k+1 \\ &= n. \end{aligned}$$

The case labels in effect introduce the new assumptions you wish you had, to make the proof solvable. Then you proceed to show your work from there.

In either case, we see that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$, as required. ∎

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer. We want to show that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$. To do so, we consider two cases:

Case 1: n is even. This means there is an integer k such that $n = 2k$. Some algebra then tells us that

$$\left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor = \left\lceil \frac{2k}{2} \right\rceil + \left\lfloor \frac{2k}{2} \right\rfloor$$

$$= \lceil k \rceil + \lfloor k \rfloor$$

$$= 2k$$

$$= n.$$

Case 2: n is odd. Then there's an integer k where $n = 2k + 1$, and

$$\left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor = \left\lceil \frac{2k+1}{2} \right\rceil + \left\lfloor \frac{2k+1}{2} \right\rfloor$$

At the end of a split into cases, it's a nice courtesy to explain to the reader what it was that you established in each case.

$$= n.$$

In either case, we see that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$, as required. ∎

Theorem: If n is an integer, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

Proof: Let n be an integer. We want to show that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$. To do so, we consider two cases:

Case 1: n is even. This means there is an integer k such that $n = 2k$.
Some algebra then tells us that

$$\begin{aligned} \left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor &= \left\lceil \frac{2k}{2} \right\rceil + \left\lfloor \frac{2k}{2} \right\rfloor \\ &= \lceil k \rceil + \lfloor k \rfloor \\ &= 2k \\ &= n. \end{aligned}$$

Case 2: n is odd. Then there's an integer k where $n = 2k + 1$, and

$$\begin{aligned} \left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor &= \left\lceil \frac{2k+1}{2} \right\rceil + \left\lfloor \frac{2k+1}{2} \right\rfloor \\ &= \left\lceil k + \frac{1}{2} \right\rceil + \left\lfloor k + \frac{1}{2} \right\rfloor \\ &= (k+1) + k \\ &= 2k+1 \\ &= n. \end{aligned}$$

In either case, we see that $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$, as required. ■

Reviewing What We Learned Today

Proofwriting Rules We Learned Today

- **Direct proof:** A proof pattern/technique where the first two sentences of the proof are (1) assume the “if” part of theorem, (2) “want to show” the “then” part of the theorem.
- To prove a **universal**, “pick an arbitrary.”
- To prove an **existential**, (1) announce a concrete value that works, then (2) justify that it works.
- Pay attention to and use **formal definitions** of terms.
- Write in **complete sentences**.
- Clearly **introduce variable names** using prescribed language. Don’t reuse/overlap variable names.
- **Proof by Cases:** A proof technique where you divide a situation into all possible cases, and prove each one separately, to prove the whole. Give clear case labels, which act as assumptions.
- *For these and more rules, see the* ***Proofwriting Checklist!***

Ways of thinking about Proofwriting

Proofs as a Dialog

Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

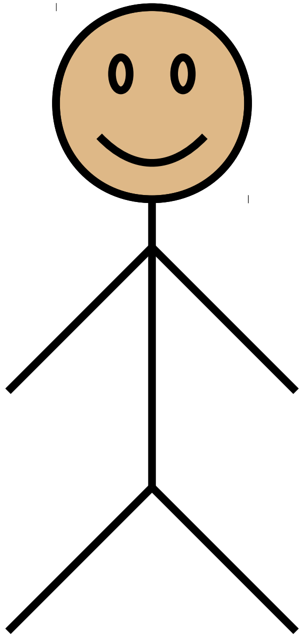
Now, let $z = k - 34$.

Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.



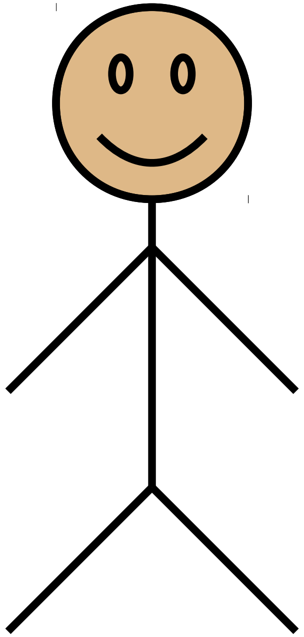
Proof Writer (You)

Proofs as a Dialog

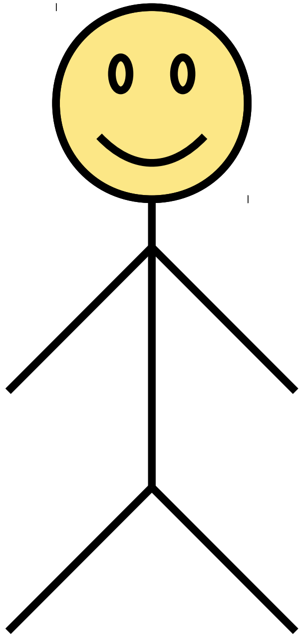
Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.



Proof Writer (You)



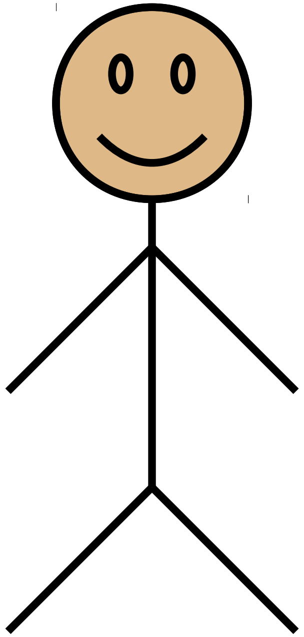
Proof Reader

Proofs as a Dialog

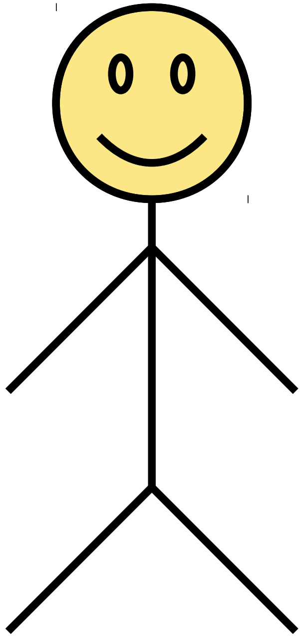
Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.



Proof Writer (You)



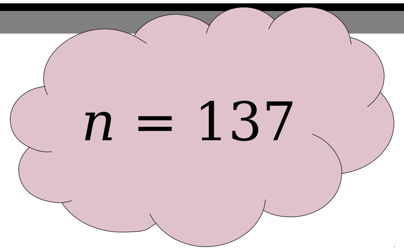
Proof Reader

Proofs as a Dialog

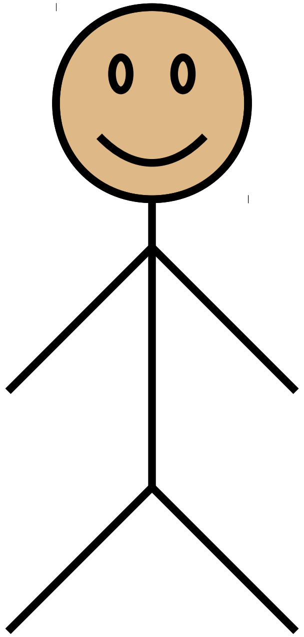
Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

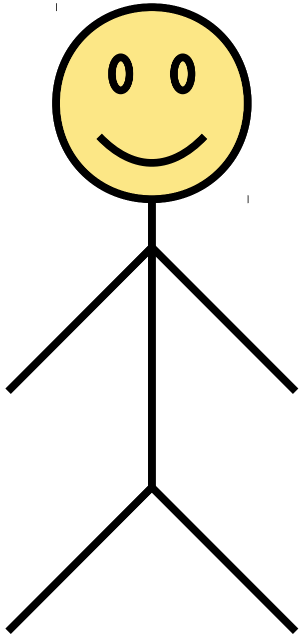
Now, let $z = k - 34$.



Reader *Picks*



Proof Writer (You)



Proof Reader

Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

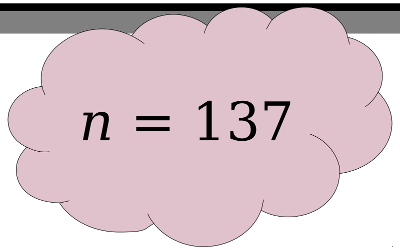
Now, let $z = k - 34$.

Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

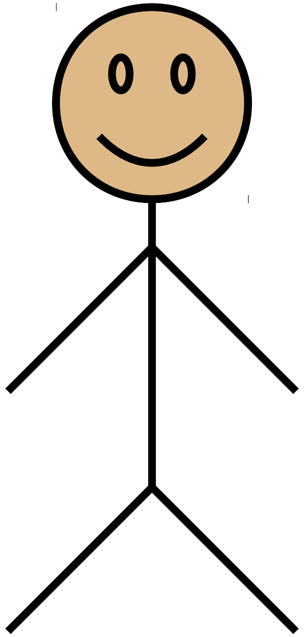
Now, let $z = k - 34$.



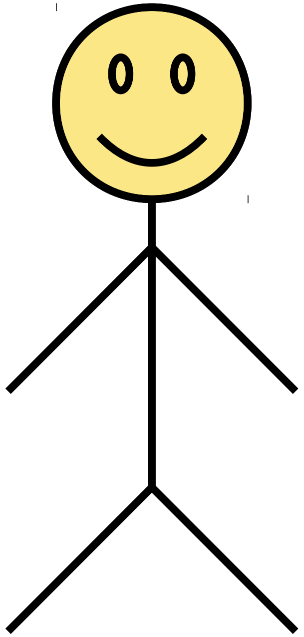
Reader *Picks*

$k = 68$

Neither *Picks*
(just a consequence of prior Reader Pick)



Proof Writer (You)



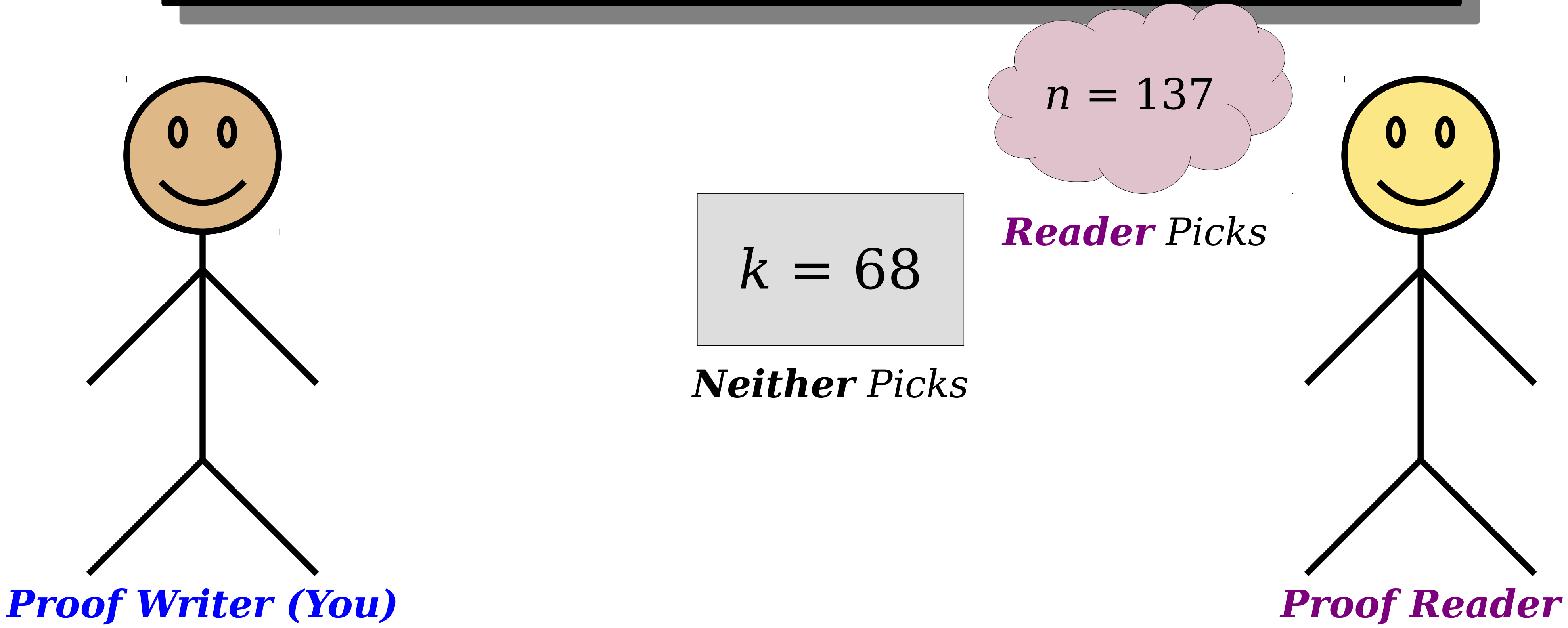
Proof Reader

Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.

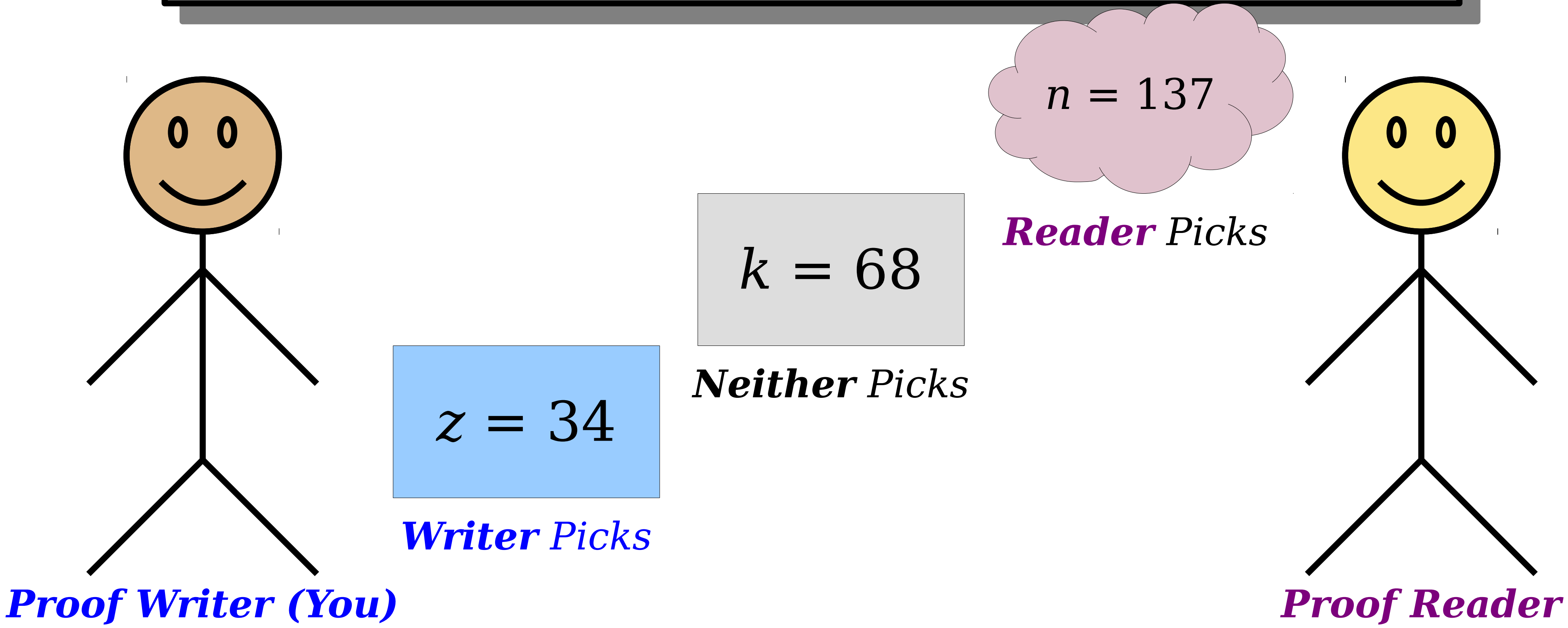


Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.

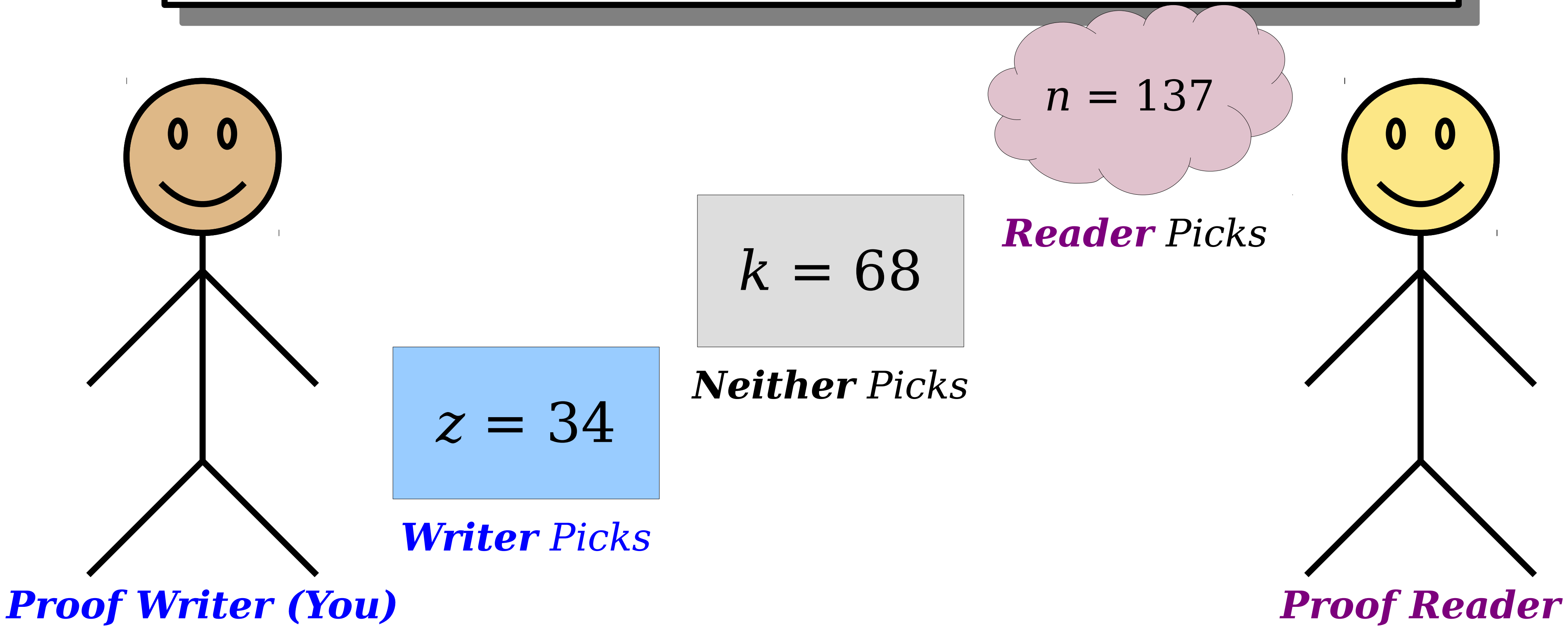


Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.

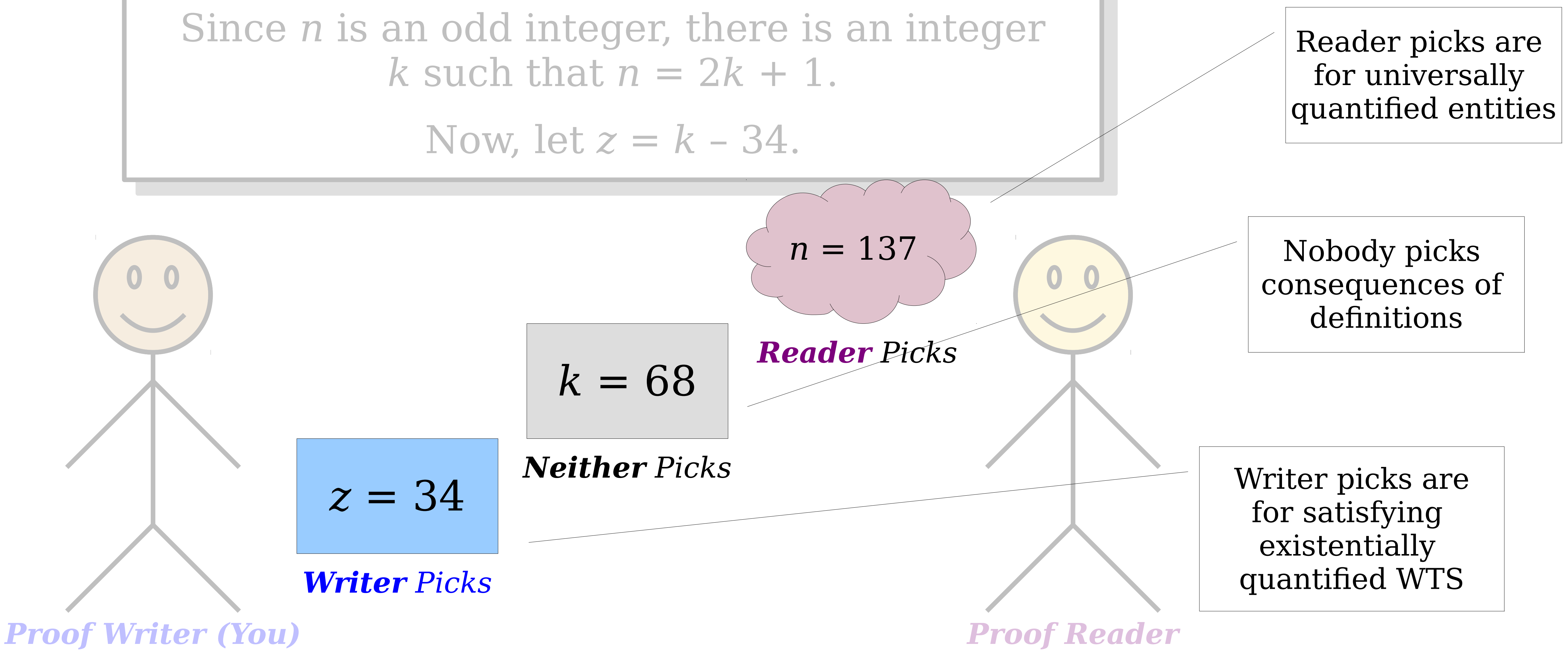


Proofs as a Dialog

Pick an arbitrary odd integer n.

Since n is an odd integer, there is an integer k such that $n = 2k + 1$.

Now, let $z = k - 34$.



Who Owns What?

- The ***reader*** chooses and owns a value if you use wording like this:
  - Pick an arbitrary natural number n.
  - Consider some $n \in \mathbb{N}$.
  - Let n be a natural number.
  - Let n be an arbitrary $n \in \mathbb{N}$.
- The ***writer*** (you) chooses and owns a value if you use wording like this:
  - We choose $r = n + 1$.
  - Pick $s = n$.
- ***Neither*** of you chooses a value if you use wording like this:
  - Since n is even, we know there is some $k \in \mathbb{Z}$ where $n = 2k$.
  - Because n is odd, there must be some integer k where $n = 2k + 1$.

Next Time

- ***Indirect Proofs***
  - How do you prove something without actually proving it?
- ***Mathematical Implications***
  - What exactly does "if *P*, then *Q*" mean?
- ***Proof by Contrapositive***
  - A helpful technique for proving implications.
- ***Proof by Contradiction***
  - Proving something is true by showing it can't be false.