Direct Proofs

Outline for Today

- ***Mathematical Proof***
  - What is a mathematical proof? What does a proof look like?
- ***Direct Proofs***
  - A versatile, powerful proof technique.
- ***Universal and Existential Statements***
  - What exactly are we trying to prove?
- ***Proofs on Set Theory***
  - Formalizing our reasoning.

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.

***54·43.** $\vdash :. \alpha, \beta$ [illegible] $2 = \Lambda . \equiv . \alpha \cup \beta \epsilon 2$

Dem.

$\vdash . *54$ [illegible] $\vdash :. \alpha =$ [illegible] $\iota`y . \supset : \alpha \cup \beta \epsilon 2 . \equiv . x$ [illegible]

[*51·2 [illegible] $\equiv . \iota`x$ [illegible] $= \Lambda .$

[*13· [illegible] $\equiv . \alpha \cap$ [illegible] (1)

$\vdash . (1)$ [illegible] 11·35 . $\supset$

$\vdash$ [illegible] $y) . \alpha = \iota`x . \beta = \iota`y .$ [illegible] $\epsilon 2 . \equiv . \alpha \cap$ [illegible] (2)

$\vdash . (2) .$ [illegible] $. *52·1 . \supset \vdash .$ Prop

From this p[illegible]on it will follow, when a[illegible]tion has been defined, that 1 + [illegible]

Modern Proofs

Thinking about proofs as an adversarial exchange

- It is helpful to think about proofs as an exchange between two parties:
  1. someone who is trying to prove something is true
  2. someone who is trying their best thwart that effort by choosing “hard” cases for you to address, and being generally skeptical of the argument

Two Quick Definitions

- An integer n is ***even*** if there is some integer k such that $n = 2k$.
  - This means that 0 is even.
- An integer n is ***odd*** if there is some integer k such that $n = 2k + 1$.
  - This means that 0 is not odd.
- We'll assume the following for now:
  - Every integer is either even or odd.
  - No integer is both even and odd.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Pick an arbitrary even integer n.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2$

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2$

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

This symbol means "end of proof"

Our First Dire

Theorem: If n is an even inte

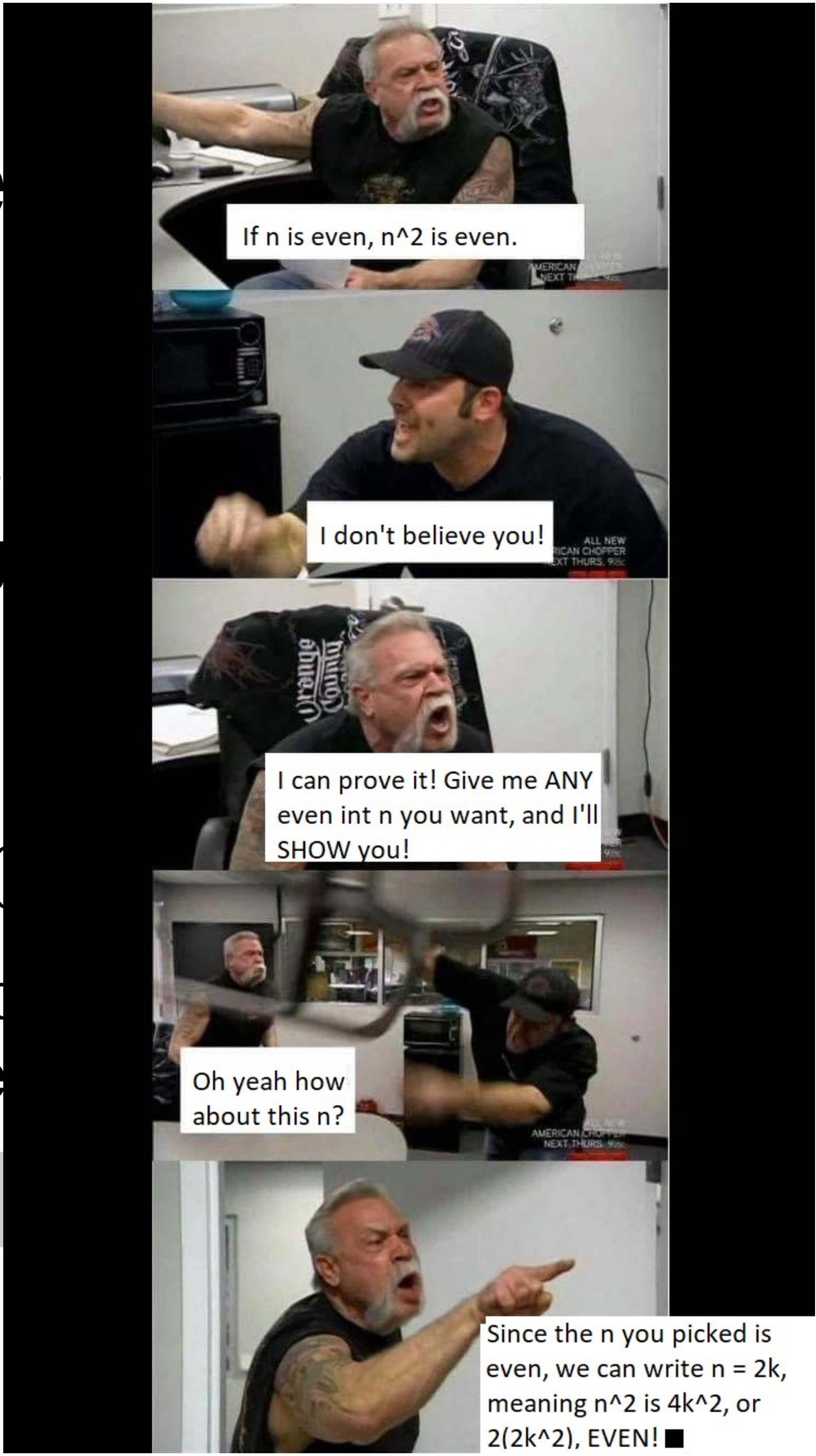
Proof: Let n be an even integ

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

This means that $n^2 = ($

From this, we see that
m (namely, $2k^2$) where

Therefore, n^2 is even.



Our First Direct Proof

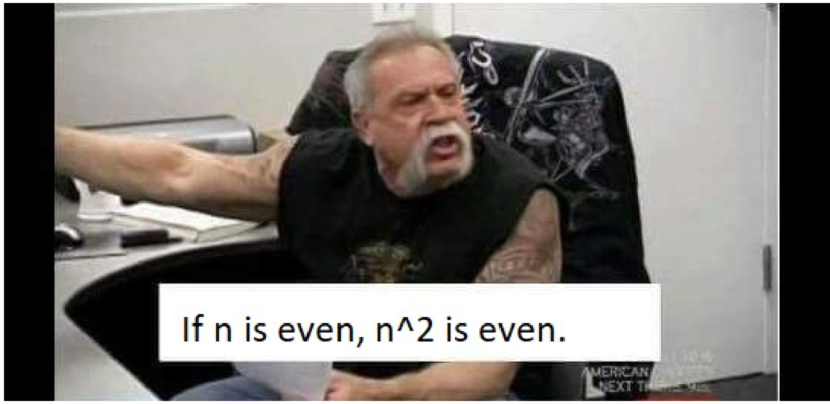
Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■



st Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integ

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

Since n i
such tha

This mea

From thi
m (name

Therefor

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Our First Direc

Theorem: If n is an even integ

Proof: Pick an arbitrary even integer n.

- This “pick any” step is really important!

- TAs will tell you, improper introduction of variables is one of the most common deductions for proofs on psets and exams!

Our First Direc

Theorem: If n is an even integ

Proof: Pick an arbitrary even integer n.

- Once you finish this step, think of the value picked as fixed for the rest of the proof.

- So it's important to specify any conditions or limitations *now,* in this step where you instruct the "adversarial" person on how to make the pick.

Our First Direc

Theorem: If n is an even integ

Proof: Pick an arbitrary even integer n.

Acceptable wording for this step:

- "**Pick** an arbitrary even integer n."
- "**Consider** any even integer n."
- "**Choose** an arbitrary even integer n."
- "**Let** n be an even integer."

Unacceptable wording for this step:

- "**For all** even integers n." ("For any" is better but not ideal.)
- "Let n be **an integer**. Since n is **even**, it must have…"
- [just start talking about n]

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

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

This means th ... ^{2}).

From this, we ... er m (namely, $2k$ ...

Therefore, n^2 ...

This is the definition of an even integer. When writing a mathematical proof, it's common to call back to the definitions.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Fr
m

Th

Notice how we use the value of ***k*** that we obtained above. Giving names to quantities, even if we aren't fully sure what they are, allows us to manipulate them. This is similar to variables in programs.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n … en.
Proof: Let n b…

Since n …
such th…

Our ultimate goal is to prove that $\boldsymbol{n^2}$ is even. This means that we need to find some $\boldsymbol{m}$ such that $\boldsymbol{n^2 = 2m}$. Here, we're explicitly showing how we can do that.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

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

This mea…).

From thi… r
m (name…

Hey, that's what we were trying to show! We're done now.

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

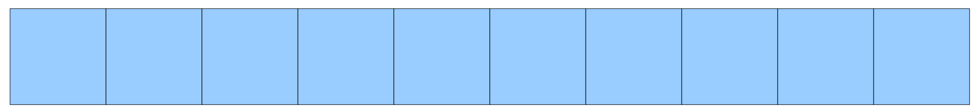
Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

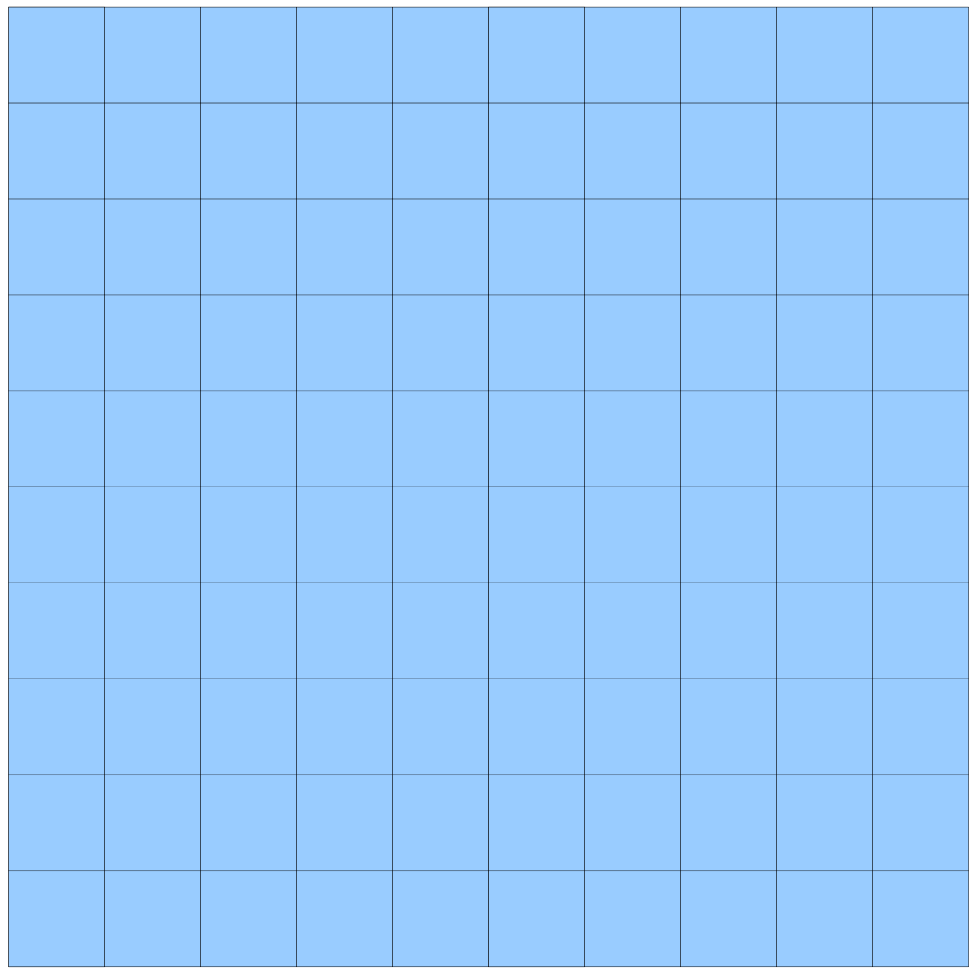
From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

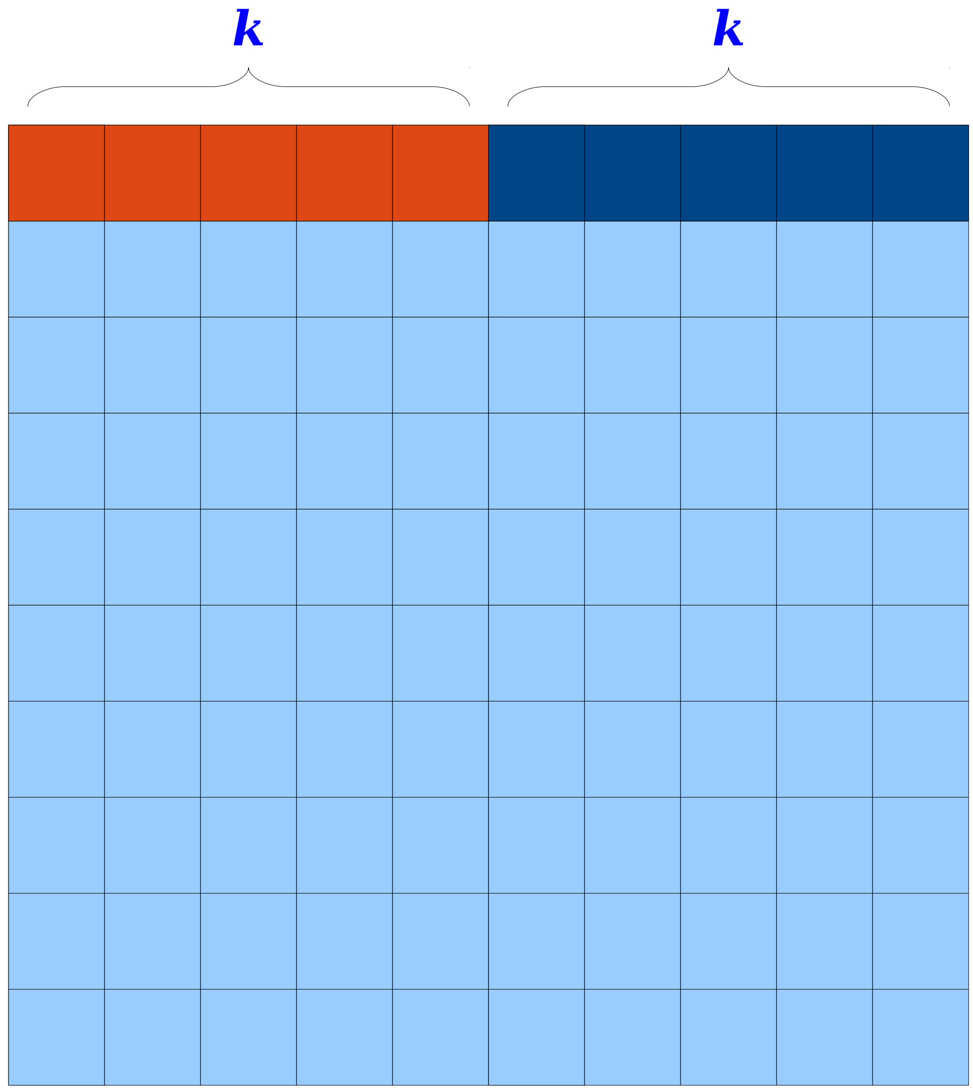
A Visual Intuition



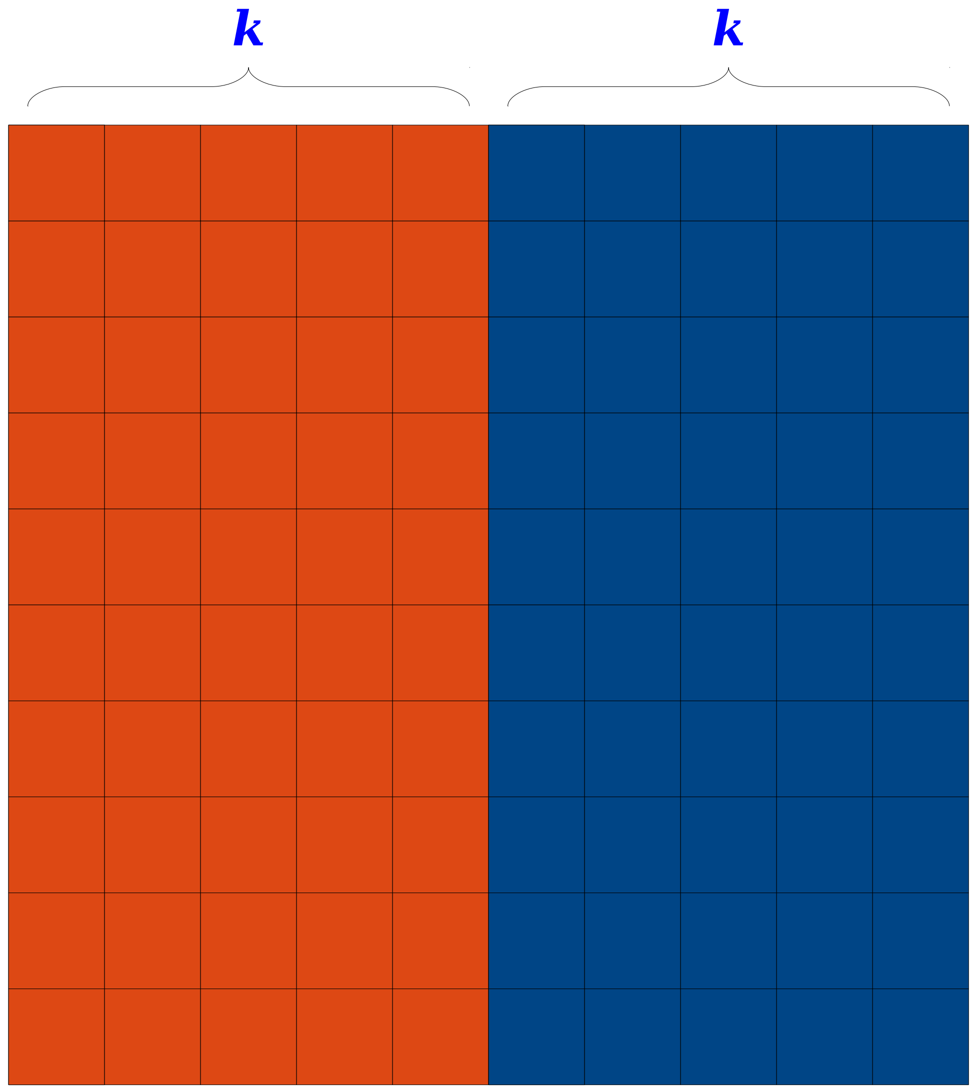
A Visual Intuition



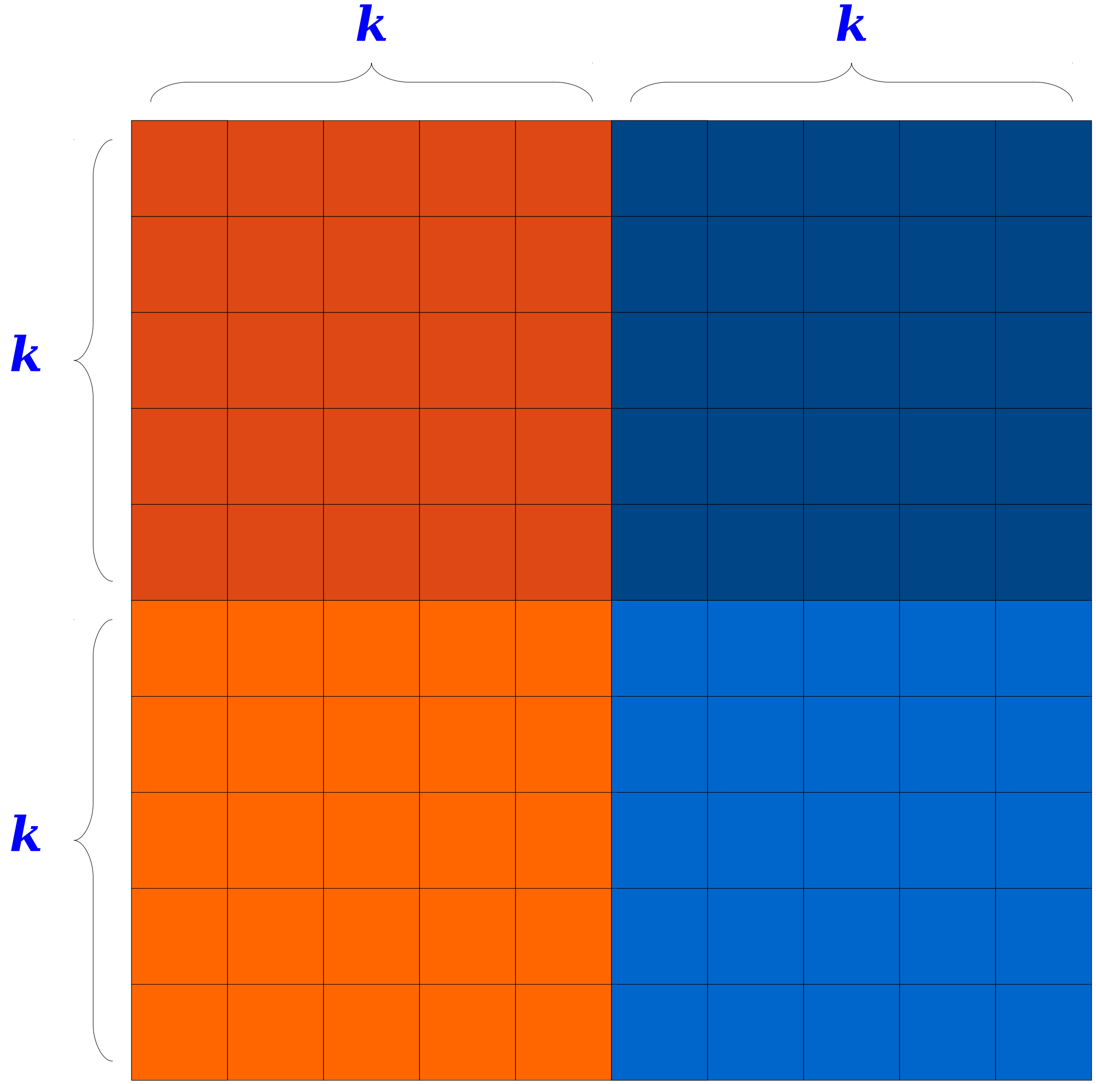
A Visual Intuition



A Visual Intuition



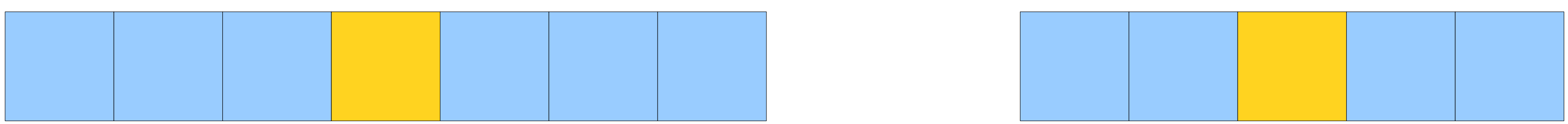
A Visual Intuition



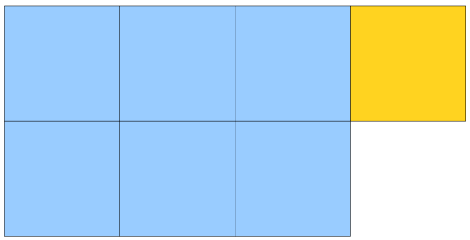
That wasn't so bad! Let's do another one.

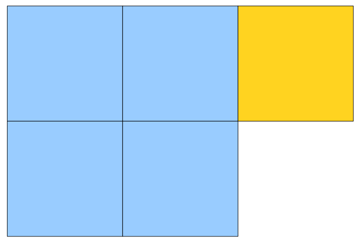
Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

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



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





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

Proof:

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

Proof:

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

Proof:

How do we prove that this is true for ***any*** integers?

Proving Something Always Holds

- Many statements have the form

For any *x*, `[some-property]` holds of *x*.

- Examples:

For all integers n, if n is even, n^2 is even.

For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

For all sets S, $|S| < |\wp(S)|$.

- How do we prove these statements when there are (potentially) infinitely many cases to check?
  - This is where the arbitrary choice comes in—our proof is essentially a template of what we would do for any choice the adversarial person could make for n.

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

Proof:

Theorem: For any 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.

Theorem: For any 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.

By picking ***m*** and ***n*** arbitrarily, anything we prove about ***m*** and ***n*** will generalize to all possible choices we could have made.

Theorem: For any 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.

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Theorem: For any 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.

Theorem: For any 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. Since m is odd, we know that there is an integer k where

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

Theorem: For any 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. 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

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

Theorem: For any 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. 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

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

Theorem: For any 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. 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

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

Theorem: For any 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. 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 any 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. 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 any 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. 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

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

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 any 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. 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. ■

Numbering these equalities lets us refer back to them later on, making the flow of the proof a bit easier to understand.

Theo … d n are odd, then m …

Proo … d n, where m and n are od … s 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. ■

Theorem: For any 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. 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

Notice that we use k in the first equality and r in the second equality. That's because we know that n is twice something plus one, but we can't say for sure that it's k specifically.

Equation (3) te… $k + r + 1)$
such that $m +$ … even, as
required. ■

Theorem: For any 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. 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

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

hat

1

(3)

er s (namely, $k + r + 1$)

hat $m + n$ is even, as

This is a grammatically correct and complete sentence! Proofs are expected to be written in complete sentences, so you'll often use punctuation at the end of formulas.

We recommend using the "mugga mugga" test – if you read a proof and replace all the mathematical notation with "mugga mugga," what comes back should be a valid sentence.

Theorem: For any 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. 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 any 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. 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

$$n = 2r + 1.$$

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

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

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. ■

Trace through this proof if $m = 7$ and $n = 9$. What is the resulting value of s?

A. 3
B. 8
C. 17

Answer at **PollEv.com/cs103** or text **CS103** to **22333** once to join, then **A**, **B**, or **C**.

Proof by Exhaustion

Theorem: The product of any two consecutive integers is even.

Theorem: The product of any two consecutive integers is even.

… -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 …

Theorem: The product of any two consecutive integers is even.

… -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 …

Theorem: The product of any two consecutive integers is even.

... -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 ...

Theorem: The product of any two consecutive integers is even.

... -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 ...

Theorem: The product of any two consecutive integers is even.

... -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 ...

Theorem: The product of any two consecutive integers is even.

Proof:

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even.

Case 2: n is odd.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even.

Case 2: n is odd.

This is called a **proof by cases** (alternatively, a **proof by exhaustion**) and works by showing that the theorem is true regardless of what specific outcome arises.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even.

Case 2: n is odd.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$.

Case 2: n is odd.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

$$n(n+1) \;=\; 2k(n+1)$$

Case 2: n is odd.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Case 2: n is odd.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

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

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$. We then see that

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

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$. We then see that

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

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$. We then see that

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

This means there is an integer m (namely, $n(k+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$. We then see that

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

This means there is an integer m (namely, $n(k+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

In either case, we find that $n(n+1)$ is even, which is what we needed to show.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$. We then see that

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

This means there is an integer m (namely, $n(k+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

In either case, we find that $n(n+1)$ is even, which is what we needed to show. ■

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there

This tells us $n+1 = 2k+2$

$$\begin{aligned} n(n+1) &= \\ &= \end{aligned}$$

After splitting into cases, it's a good idea to summarize what you just did so that the reader knows what to take away from it.

This means there is an integer m (namely, $n(k+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

In either case, we find that $n(n+1)$ is even, which is what we needed to show.

Theorem: The product of any two consecutive integers is even.

Proof: Pick any two consecutive integers n and $n+1$. We'll prove that their product $n(n+1)$ is even. Let's consider two cases:

Case 1: n is even. This means there exists an integer k such that $n = 2k$. Therefore, we learn that

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

Therefore, there is an integer m (namely, $k(n+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

Case 2: n is odd. Then there is an integer k where $n = 2k+1$. This tells us $n+1 = 2k+2$. We then see that

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

This means there is an integer m (namely, $n(k+1)$) such that $n(n+1) = 2m$, so $n(n+1)$ is even.

In either case, we find that $n(n+1)$ is even, which is what we needed to show. ■

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.
- Feel free to use these results going forward.
- If you'd like to practice the techniques from today, try your hand at proving some of these results!

Universal and Existential Statements

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

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

Proof:

Which of the following should be the next sentence of this proof?

A. "Pick any odd integer, $n = 137$."
B. "Pick any odd integer n."
C. "Pick any odd integer n and arbitrary integers r and s where $r^2 - s^2 = n$."

Answer at **PollEv.com/cs103** or text **CS103** to **22333** once to join, then **A**, **B**, or **C**.

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

Proof: Pick any odd integer n.

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

Proof: Pick any odd integer n.

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

Proof: Pick any odd integer n.

This is a very different sort of request than what we've seen in the past. How on earth do we go about proving something like this?

Universal vs. Existential Statements

- A ***universal statement*** is a statement of the form

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

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

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

- How do you prove an existential statement?

Proving an Existential Statement

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

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

- ***Simplest approach:*** Search far and wide, find an *x* that has the right property, then show why your choice is correct.

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

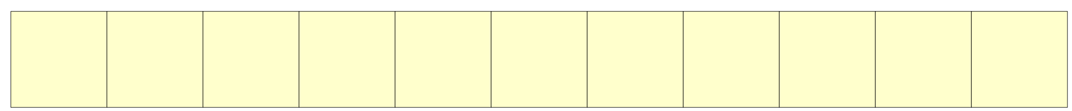
Proof: Pick any odd integer n.

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

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

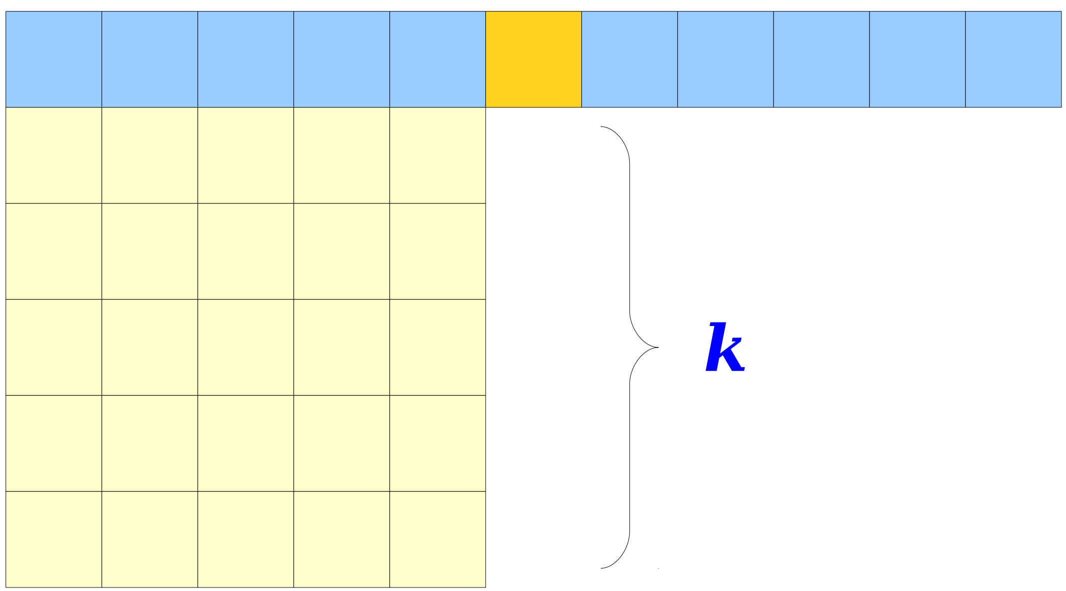
Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.



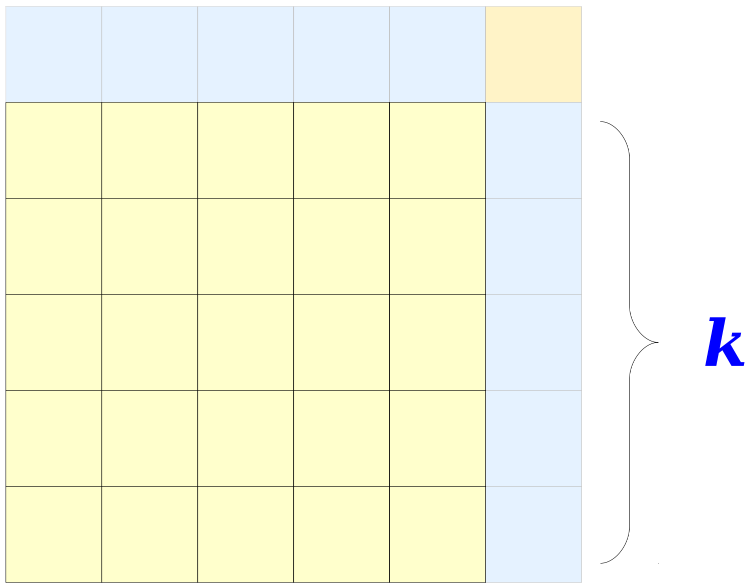
Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.



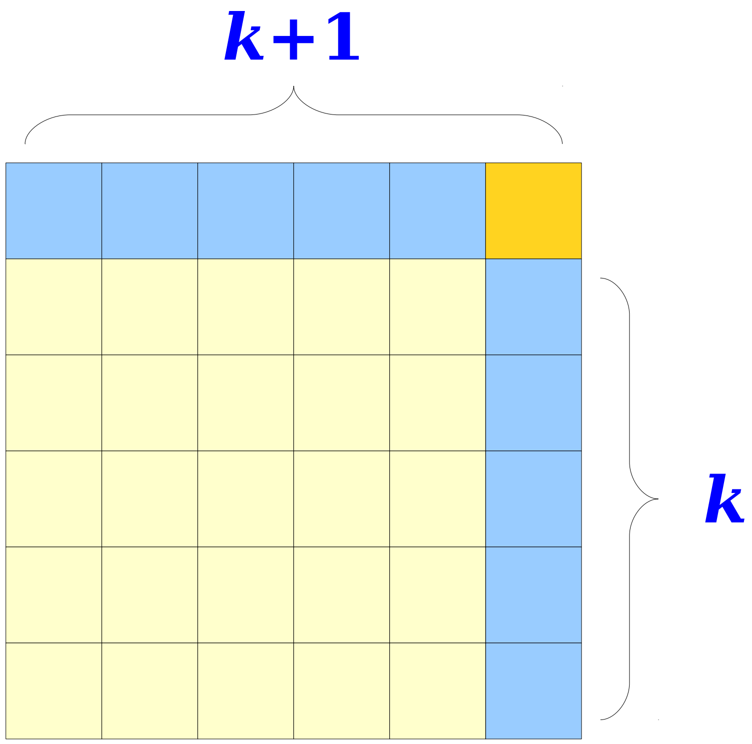
Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.



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

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.



Our guess:

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

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

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$.

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

Proof: Pick any odd integer n. Since n is odd, we know there is some 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 any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some 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 any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some 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 any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some 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 any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some 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 any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some 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. ■

Follow-Up Question: There are some integers that can't be written as $r^2 - s^2$ for any integers r and s.

Can you prove that every integer can be formed by adding and subtracting some combination of at most *three* perfect squares?

Reading Recommendations

- We’ve released two handouts online that you should read over:
  - Handout 06: How to Succeed in CS103
  - Handout 07: Set Theory Definitions.
- Additionally, if you haven’t yet read over the Guide to Elements and Subsets, we’d recommend doing so.
- Finally, we strongly recommend reading over Chapter 1 and Chapter 2 of the online course reader to get some more background with proofs and set theory.

Problem Set 0

- Problem Set 0 went out on Monday. It's due this Friday at 2:30PM.
  - Even though this just involves setting up your compiler and submitting things, please start this one early. If you start things on Friday morning, we can't help you troubleshoot Qt Creator issues!
  - There's a very detailed troubleshooting guide up on the CS103 website and a Piazza post detailing common fixes. If you're still having trouble, please feel free to ask on Piazza!

Back to CS103!

Proofs on Sets

Set Theory Review

- Recall from last time that we write $x \in S$ if x is an element of set S and $x \notin S$ if x is not an element of set S.
- If S and T are sets, we say that S is a subset of T (denoted $S \subseteq T$) if the following statement is true:

  For every object x, if $x \in S$, then $x \in T$.

- Let's explore some properties of the subset relation.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$.

We're showing here that regardless of what ***A***, ***B***, *and* ***C*** you pick, the result will still be true.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$.

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

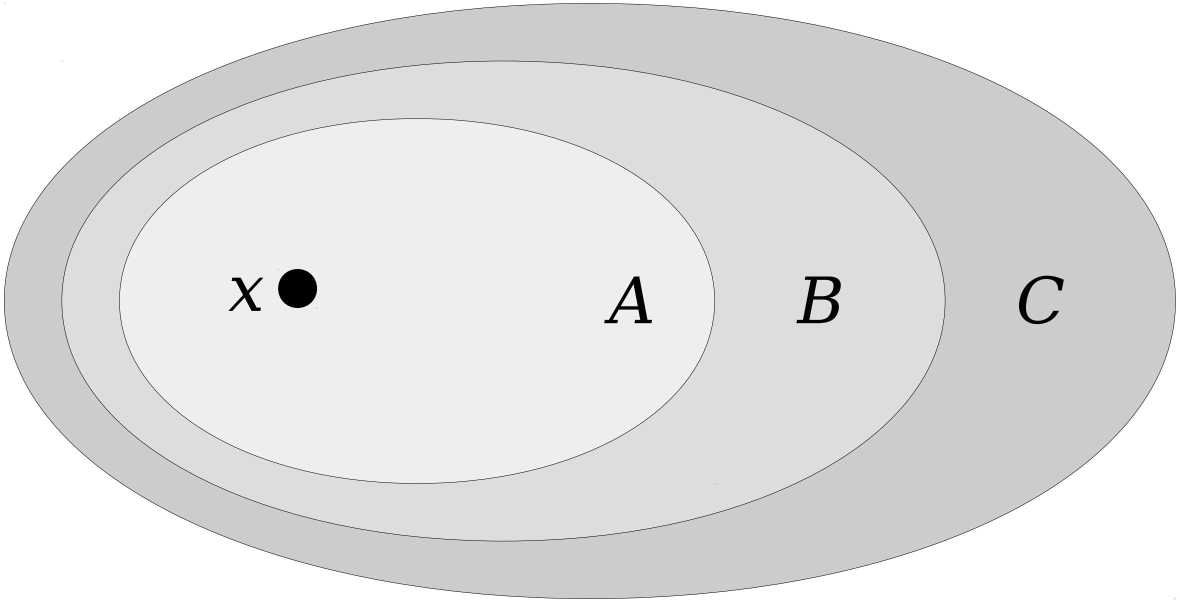
Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

This is, by definition, what it means for $A \subseteq C$ to be true. Our job will be to prove this statement.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.



Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$.

We're showing here that regardless of what x you pick, the result will still be true.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$.

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$. Similarly, since $B \subseteq C$ and $x \in B$, we see that $x \in C$, which is what we needed to show.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$. Similarly, since $B \subseteq C$ and $x \in B$, we see that $x \in C$, which is what we needed to show. ■

This property of the subset relation is called ***transitivity***. We'll revisit transitivity in a couple of weeks.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Question to ponder: is this theorem still true if we replace $\subseteq$ with $\in$?

Proof: Let A, B, and C b… B
and $B \subseteq C$. We need t… ,
we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$. Similarly, since $B \subseteq C$ and $x \in B$, we see that $x \in C$, which is what we needed to show. ■

Set Equality and Lemmas

Set Equality

- As we mentioned on Monday, two sets A and B are equal when they have exactly the same elements.
- Here's a little theorem that's very useful for showing that two sets are equal:

  Theorem: If A and B are sets where $A \subseteq B$ and $B \subseteq A$, then $A = B$.

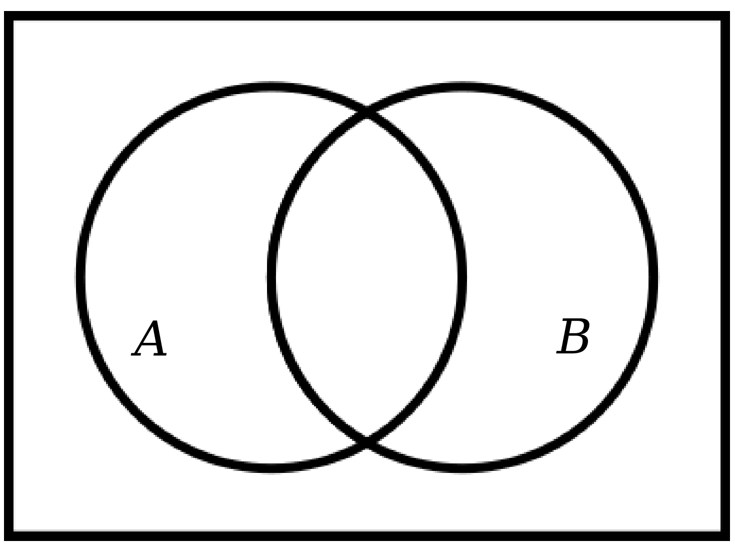
- We've included a proof of this result as an appendix to this slide deck. You should read over it on your own time.

A Trickier Theorem

- Our last theorem for today is this one, which comes to us from the annals of set theory:

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

- Unlike our previous theorem, this one is a lot harder to see using Venn diagrams alone.



Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

- Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

- We're going to pick arbitrary sets A and B.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

- Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.
  - We're going to pick arbitrary sets A and B.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

We're going to pick arbitrary sets A and B.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

- We're going to pick arbitrary sets A and B.
- We're going to assume $A \cup B \subseteq A \cap B$.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

- Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.
  - We're going to pick arbitrary sets A and B.
  - We're going to assume $A \cup B \subseteq A \cap B$.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

We're going to pick arbitrary sets A and B.

We're going to assume $A \cup B \subseteq A \cap B$.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.

- We're going to pick arbitrary sets A and B.
- We're going to assume $A \cup B \subseteq A \cap B$.
- We're going to prove that $A = B$.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

- Before we Flail and Panic, let's see if we can tease out some info about what this proof might look like.
  - We're going to pick arbitrary sets A and B.
  - We're going to assume $A \cup B \subseteq A \cap B$.
  - We're going to prove that $A = B$.

Tackling our Theorem

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Before we Flail and Panic, let's see if we can tease out som

proof might look

- We're going to pi
- We're going to assume $A \cup B \subseteq A \cap B$.
- We're going to prove that $A = B$.

Reasonable guess: let's try proving that $A \subseteq B$ and that $B \subseteq A$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

A ***lemma*** is a smaller proof that's designed to build into a larger one. Think of it like program decomposition, except for proofs!

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof:

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Since $x \in S$, we know that $x \in S \cup T$ because x belongs to at least one of S and T.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Since $x \in S$, we know that $x \in S \cup T$ because x belongs to at least one of S and T. We then see that $x \in S \cap T$ because $x \in S \cup T$ and $S \cup T \subseteq S \cap T$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Since $x \in S$, we know that $x \in S \cup T$ because x belongs to at least one of S and T. We then see that $x \in S \cap T$ because $x \in S \cup T$ and $S \cup T \subseteq S \cap T$. Finally, since $x \in S \cap T$, we learn that $x \in T$, since x belongs to both S and T.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Since $x \in S$, we know that $x \in S \cup T$ because x belongs to at least one of S and T. We then see that $x \in S \cap T$ because $x \in S \cup T$ and $S \cup T \subseteq S \cap T$. Finally, since $x \in S \cap T$, we learn that $x \in T$, since x belongs to both S and T.

Overall, we've started with an arbitrary choice of $x \in S$ and concluded that $x \in T$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Since $x \in S$, we know that $x \in S \cup T$ because x belongs to at least one of S and T. We then see that $x \in S \cap T$ because $x \in S \cup T$ and $S \cup T \subseteq S \cap T$. Finally, since $x \in S \cap T$, we learn that $x \in T$, since x belongs to both S and T.

Overall, we've started with an arbitrary choice of $x \in S$ and concluded that $x \in T$. Therefore, we see that $S \subseteq T$ holds, which is what we needed to prove.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Proof: Let S and T be any sets where $S \cup T \subseteq S \cap T$. We will prove that $S \subseteq T$. To do so, consider any $x \in S$. We will prove that $x \in T$.

Since $x \in S$, we know that $x \in S \cup T$ because x belongs to at least one of S and T. We then see that $x \in S \cap T$ because $x \in S \cup T$ and $S \cup T \subseteq S \cap T$. Finally, since $x \in S \cap T$, we learn that $x \in T$, since x belongs to both S and T.

Overall, we've started with an arbitrary choice of $x \in S$ and concluded that $x \in T$. Therefore, we see that $S \subseteq T$ holds, which is what we needed to prove. ■

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof:

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Next, since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, from $A \cup B \subseteq A \cap B$ we learn that $B \cup A \subseteq B \cap A$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Next, since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, from $A \cup B \subseteq A \cap B$ we learn that $B \cup A \subseteq B \cap A$. Applying our lemma again in this case tells us that $B \subseteq A$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Next, since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, from $A \cup B \subseteq A \cap B$ we learn that $B \cup A \subseteq B \cap A$. Applying our lemma again in this case tells us that $B \subseteq A$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Next, since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, from $A \cup B \subseteq A \cap B$ we learn that $B \cup A \subseteq B \cap A$. Applying our lemma again in this case tells us that $B \subseteq A$.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Next, since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, from $A \cup B \subseteq A \cap B$ we learn that $B \cup A \subseteq B \cap A$. Applying our lemma again in this case tells us that $B \subseteq A$.

Since both $A \subseteq B$ and $B \subseteq A$, we conclude that $A = B$, which is what we needed to show.

Lemma: If S and T are sets and $S \cup T \subseteq S \cap T$, then $S \subseteq T$.

Theorem: If A and B are sets and $A \cup B \subseteq A \cap B$, then $A = B$.

Proof: Let A and B be any sets where $A \cup B \subseteq A \cap B$. We will prove that $A = B$ by showing $A \subseteq B$ and $B \subseteq A$.

First, notice that by our lemma, since $A \cup B \subseteq A \cap B$, we know that $A \subseteq B$.

Next, since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, from $A \cup B \subseteq A \cap B$ we learn that $B \cup A \subseteq B \cap A$. Applying our lemma again in this case tells us that $B \subseteq A$.

Since both $A \subseteq B$ and $B \subseteq A$, we conclude that $A = B$, which is what we needed to show. ■

What We've Covered

- ***What is a mathematical proof?***
  - An argument – mostly written in English – outlining a mathematical argument.
- ***What is a direct proof?***
  - It's a proof where you begin from some initial assumptions and reason your way to the conclusion.
- ***What are universal and existential statements?***
  - Universal statements make a claim about all objects of one type. Existential statements make claims about at least one object of some type.
- ***How do we write proofs about set theory?***
  - By calling back to definitions! Definitions are key.

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.

Appendix: Set Equality

Set Equality

- If A and B are sets, we say that $A = B$ precisely when the following statement is true:

For any object x, $x \in A$ if and only if $x \in B$.

- (This is called the ***axiom of extensionality***.)
- In practice, this definition is tricky to work with.
- It's often easier to use the following result to show that two sets are equal:

For any sets A and B,
if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof:

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Next, we'll prove that if $x \in B$, then $x \in A$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Next, we'll prove that if $x \in B$, then $x \in A$. Consider an arbitrary $x \in B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Next, we'll prove that if $x \in B$, then $x \in A$. Consider an arbitrary $x \in B$. Since $B \subseteq A$ and $x \in B$, we see that $x \in A$, which is what we needed to show.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Next, we'll prove that if $x \in B$, then $x \in A$. Consider an arbitrary $x \in B$. Since $B \subseteq A$ and $x \in B$, we see that $x \in A$, which is what we needed to show.

Since we've proven both directions of implication, we see that $A = B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We need to prove $A = B$. To do so, we will prove for all x that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. To do so, take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Next, we'll prove that if $x \in B$, then $x \in A$. Consider an arbitrary $x \in B$. Since $B \subseteq A$ and $x \in B$, we see that $x \in A$, which is what we needed to show.

Since we've proven both directions of implication, we see that $A = B$. ■