L3: Proof Styles

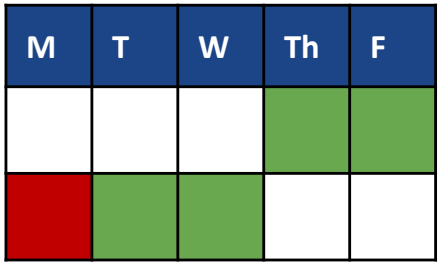
Please grab a handout.

Announcements

- Homework 1 posts tonight! Due in **1 week (Thursday 1/20)**.

- Find a group for the groupwork portion
  - **Max group size 5, suggested group size 3**
  - You can form your own group
  - You can use the Piazza group-finding thread to find a group
  - You can use the **group request form** if you'd like course staff to help with group matchmaking

- Reminder: Monday = MLK Day = No Discussions
  - If you usually have Monday discussion:
    - attend a different discussion this week:
      today, tomorrow, next Tuesday or Wednesday
  - OR watch a discussion recording



Summary: Algebra vs. Modular Arithmetic

	Algebra	**Modular Arithmetic**
Domain	real numbers	integers
We care about	Equality ex: x = y	Equivalence with respect to a modulus m ex: $x \equiv y \pmod{m}$
How many unique numbers?	Infinitely many ex: -153.21, 76, $\sqrt{2}$	There are only m unique numbers in (mod m): $\{0, \ldots, m-1\}$
Multiplicative Inverse, a^{-1} Defn: $a^{-1}a \equiv 1$	For $a \neq 0$, $a^{-1} = 1/a$	Even for $a \neq 0$, $\mathbf{a^{-1}}$ may or may not exist

Summary: Algebra vs. Modular Arithmetic

	Algebra	Modular Arithmetic
Domain	real numbers	**integers**
We care about	Equality ex: x = y	**Equivalence** with respect to a modulus **m** ex: **x ≡ y (mod m)**
How many unique numbers?	Infinitely many ex: -153.21, 76, $\sqrt{2}$	There are *only* **m** numbers with all pairs non-equivalent in **(mod m)**: **{0, 1, 2, …., m-1}**
Multiplicative Inverse	For $a \neq 0$, $a^{-1} = 1/a$	Even for $a \neq 0$, $\mathbf{a^{-1}}$ **may or may not exist**

Modular Inverses

- "Division by a" is really multiplying by a^{-1}.
  - But a^{-1} is **not** $\frac{1}{a}$, like in algebra.
  - a^{-1} is an integer in $\{0,1,\ldots,m-1\}$, such that $(a^{-1})(a) \equiv 1 \ (mod\ m)$

Beware: a^{-1} may or may not exist!

- **If it doesn't exist**, $ax + b \equiv c \ (mod\ m)$ won't have a **unique** solution
  - Either no solutions or multiple solutions with x in $\{0,\ldots,m-1\}$.
- **If it does exist**: $\mathbf{a^{-1}}$ is unique we will have a unique solution.

Theorem (but we won't prove it):

a has an inverse (mod m) if and only if a, m are **relatively prime**.

(meaning they have no common factor > 1)

Modular Inverses

Beware: a^{-1} may or may not exist!

- **If it doesn't exist**, $ax + b \equiv c \ (mod\ m)$ won't have a **unique** solution
  - Either no solutions or multiple solutions.
- **If it does exist**: **a^{-1}** is unique we will have a unique solution.

Theorem:

a has an inverse (mod m) if and only if a, m are

_____.

(meaning _____)

Examples: Finding a^{-1} "By Observation"

$\boldsymbol{a^{-1}}$ is the value that makes $\boldsymbol{a \cdot a^{-1} \equiv 1 \pmod{m}}$

- For example: $7^{-1} \equiv 4 \pmod{9}$
  because $7 \cdot 7^{-1} \equiv 7 \cdot 4 \equiv 28 \equiv \mathbf{1} \pmod{9}$

- Find the following inverses, if they exist:

$1^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$2^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$3^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$4^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$5^{-1} \equiv \_\_\_\_\_ \pmod{5}$

$1^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$2^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$3^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$4^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$5^{-1} \equiv \_\_\_\_\_ \pmod{6}$

Finding a^{-1} "By Observation"

Handout

1. Find the following inverses, if they exist:

$1^{-1} \equiv \_\_\_\_\_ \pmod 5$

$2^{-1} \equiv \_\_\_\_\_ \pmod 5$

$3^{-1} \equiv \_\_\_\_\_ \pmod 5$

$4^{-1} \equiv \_\_\_\_\_ \pmod 5$

$5^{-1} \equiv \_\_\_\_\_ \pmod 5$

$1^{-1} \equiv \_\_\_\_\_ \pmod 6$

$2^{-1} \equiv \_\_\_\_\_ \pmod 6$

$3^{-1} \equiv \_\_\_\_\_ \pmod 6$

$4^{-1} \equiv \_\_\_\_\_ \pmod 6$

$5^{-1} \equiv \_\_\_\_\_ \pmod 6$

Finding a^{-1} "By Observation" Handout

1. Find the following inverses, if they exist:

$1^{-1} \equiv \underline{\quad 1 \quad} \pmod 5$	$1^{-1} \equiv \underline{\qquad} \pmod 6$
$2^{-1} \equiv \underline{\quad 3 \quad} \pmod 5$	$2^{-1} \equiv \underline{\qquad} \pmod 6$
$3^{-1} \equiv \underline{\quad 2 \quad} \pmod 5$	$3^{-1} \equiv \underline{\qquad} \pmod 6$
$4^{-1} \equiv \underline{\quad 4 \quad} \pmod 5$	$4^{-1} \equiv \underline{\qquad} \pmod 6$
$5^{-1} \equiv \underline{\quad DNE \quad} \pmod 5$	$5^{-1} \equiv \underline{\qquad} \pmod 6$

Try $aj \equiv \mathbf{1} \pmod 5$, for $j = 1, \ldots, 4$.

$\boldsymbol{a = 1}$: $1 \cdot 1 \equiv 1 \pmod 5$ → $1^{-1} \equiv 1 \pmod 5$

$\boldsymbol{a = 2}$: $2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$ → $2^{-1} \equiv 3 \pmod 5$

$\boldsymbol{a = 3}$: $3 \cdot 2 \equiv 6 \equiv 1 \pmod 5$ → $3^{-1} \equiv 2 \pmod 5$

$\boldsymbol{a = 4}$: $4 \cdot 4 \equiv 16 \equiv 1 \pmod 5$ → $4^{-1} \equiv 4 \pmod 5$

$\boldsymbol{a = 5}$: $5 \cdot j \equiv 1 \pmod 5$; But $5j \equiv 0 \pmod 5$ always, so 5^{-1} DNE

Finding a^{-1} "By Observation"

Handout

1. Find the following inverses, if they exist:

$1^{-1} \equiv \underline{\quad 1 \quad} \pmod 5$ $\qquad$ $1^{-1} \equiv \underline{\quad 1 \quad} \pmod 6$

$2^{-1} \equiv \underline{\quad 3 \quad} \pmod 5$ $\qquad$ $2^{-1} \equiv \underline{\quad DNE \quad} \pmod 6$

$3^{-1} \equiv \underline{\quad 2 \quad} \pmod 5$ $\qquad$ $3^{-1} \equiv \underline{\quad DNE \quad} \pmod 6$

$4^{-1} \equiv \underline{\quad 4 \quad} \pmod 5$ $\qquad$ $4^{-1} \equiv \underline{\quad DNE \quad} \pmod 6$

$5^{-1} \equiv \underline{\quad DNE \quad} \pmod 5$ $\qquad$ $5^{-1} \equiv \underline{\quad 5 \quad} \pmod 6$

Try $aj \equiv \mathbf{1} \pmod 6$, for $j = 1, \ldots, 5$.

$\boldsymbol{a = 1}$: $1 \cdot 1 \equiv 1 \pmod 6$ $\rightarrow$ $1^{-1} \equiv 1 \pmod 6$

$\boldsymbol{a = 2}$: $2 \cdot j \equiv 1 \pmod 6$; But $2j \bmod 6$ is in $\{0,2,4\}$, so 2^{-1} DNE

$\boldsymbol{a = 3}$: $3 \cdot j \equiv 1 \pmod 6$; But $3j \bmod 6$ is in $\{0,3\}$, so 3^{-1} DNE

$\boldsymbol{a = 4}$: $4 \cdot j \equiv 1 \pmod 6$; But $4j \bmod 6$ is in $\{0,2,4\}$, so 4^{-1} DNE

$\boldsymbol{a = 5}$: $5 \cdot 5 \equiv 25 \equiv 1 \pmod 6$ $\rightarrow$ $5^{-1} \equiv 5 \pmod 6$

$2j \bmod 6$ is **never** 1

"Is there a unique solution" Blitz

Handout

Determine whether there is a unique solution (mod m) for each of the following.

$ax + b \equiv c \pmod{m}$

– **Don't find the solution**, just decide if there **is** a unique solution

a) $6x - 10 \equiv 2 \pmod{13}$ ✓

b) $11x + 3 \equiv 14 \pmod{16}$ ✓

c) $15x + 3 \equiv 14 \pmod{16}$ ✓

d) $15x + 3 \equiv 14 \pmod{18}$ ✗

both have a factor of 3

Hint:
Does $\mathbf{a^{-1}}$ exist **(mod m)** for the given equivalence? If so, there is a unique solution.

$6x - 10 \equiv 2 \pmod{13}$

$6x \equiv 12 \pmod{13}$

$6^{-1} \cdot 6x \equiv 6^{-1} \cdot 12 \pmod{13}$

1

$x \equiv \_\_\_\_ \pmod{13}$

"Is there a unique solution" Blitz

Handout

Determine whether there is a unique solution (mod m) for each of the following.

- **Don't find the solution**, just decide if there **is** a unique solution

a) $6x - 10 \equiv 2 \pmod{13}$

b) $11x + 3 \equiv 14 \pmod{16}$

c) $15x + 3 \equiv 14 \pmod{16}$

d) $15x + 3 \equiv 14 \pmod{18}$

Solution:

a) a = 6: factors are 1, 2, 3, 6
m = 13: factors are 1, 13
no common factors > 1, so unique solution

b) a = 11: factors are 1, 11
m = 16: factors are 1, 2, 4, 8, 16
no common factors > 1, so unique solution

c) a = 15: factors are 1, 3, 5, 15
m = 16: factors are 1, 2, 4, 8, 16
no common factors > 1, so unique solution

d) a = 15: factors are 1, 3, 5, 15
m = 18: factors are 1, 2, 3, 6, 9, 18
common factor of 3, so **no** unique solution

Learning Objectives: Lec 3

After today's lecture (and the associated readings, discussion, & homework), you should be able to:

- **Know Technical Vocab:** direct proof, (proof by) contrapositive, proof by contradiction, proof by cases, lemma
- Find the contrapositive of if-then propositions
- Prove simple statements using proof-by-contrapositive, and follow more complex proofs-by-contrapositive
- Prove simple statements using proof-by-contradiction, and follow more complex proofs-by-contradiction
- Prove simple statements using proof-by-cases, and follow more complex proofs-by-cases

Outline

- **Proof Recap and Overview**
- Proof by Contrapositive
  - Finding the contrapositive
  - Overview of proof technique
- Proof by Contradiction
  - Overview of proof technique
  - $\sqrt{2}$ is irrational
- Proof by Cases
  - Overview of proof technique
  - Irrational powers
- Conceptual Proofs
  - Checkerboard Tiling
  - Infinite Primes

Proof Recap

Proposition:
For all integers x, if x is even, then x^2 is even.

To **prove** a true for-all statement:

Proposition:
There exists an integer x such that $(x+1)^2 = x+7$

To **prove** a true there-exists statement:

Proposition:
For all integers x, $\frac{x^2+2x+1}{x+1} = \mathrm{x} + 1.$

To **disprove** a false for-all statement:

Proposition:
There exists an integer x such that $x^2 + x$ is odd

To **disprove** a false there exists statement:

Proof Recap

Proposition:
For all integers x, if x is even, then x^2 is even.

To **prove** a true for-all statement:
- Let x be an **arbitrary** integer
- (Prove that x has the named property)

Proposition:
There exists an integer x such that $(x+1)^2 = x+7$

To **prove** a true there-exists statement:
- Name a **specific** integer:
  - "Consider $x = 2$…"
- (Prove that this x has the named property)

Proposition:
For all integers x, $\frac{x^2+2x+1}{x+1} = x+1$.

To **disprove** a false for-all statement:
- Name a **specific** integer
  - "Consider $x = -1$…"
- (Prove that x does not have the named property)

Proposition:
There exists an integer x such that $x^2 + x$ is odd

To **disprove** a false there exists statement:
- Let x be an **arbitrary** integer
- (Prove that x does not have the named property)

Proof Recap

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

Proposition:
For all integers x, if x is even, then x^2 is even.

We can **"directly"** prove these statements by stepping through their text.

- The statement is not too surprising – not much work to understand **why** it's true.
- If you step through the parts of the proposition, you wind up with a successful proof.

Proof:

- Let x be an arbitrary integer.

Proof Recap

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

Proposition:
For all integers x, if x is even, then x^2 is even.

We can **"directly"** prove these statements by stepping through their text.

- The statement is not too surprising – not much work to understand **why** it's true.
- If you step through the parts of the proposition, you wind up with a successful proof.

Proof:

- Let x be an arbitrary integer.
- Assume that x is even. So there exists an integer k with $x = 2k$.

Proof Recap

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

Proposition:
For all integers x, if x is even, then x^2 is even.

We can **"directly"** prove these statements by stepping through their text.

- The statement is not too surprising – not much work to understand **why** it's true.
- If you step through the parts of the proposition, you wind up with a successful proof.

Proof:

- Let x be an arbitrary integer.
- Assume that x is even. So there exists an integer k with $x = 2k$.
- So $x^2 = (2k)^2 = 2(2k^2)$.

Proof Recap

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

Proposition:
For all integers x, if x is even, then x^2 is even.

We can **"directly"** prove these statements by stepping through their text.

- The statement is not too surprising – not much work to understand **why** it's true.
- If you step through the parts of the proposition, you wind up with a successful proof.

Proof:

- Let x be an arbitrary integer.
- Assume that x is even. So there exists an integer k with $x = 2k$.
- So $x^2 = (2k)^2 = 2(2k^2)$.
- Since k is an integer, $2k^2$ is also an integer. So x^2 is even.

Proof Recap

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

Proposition:
For all integers x, if x is even, then x^2 is even.

We can **"directly"** prove these statements by stepping through their text.

- The statement is not too surprising – not much work to understand **why** it's true.
- If you step through the parts of the proposition, you wind up with a successful proof.

Proof:

- Let x be an arbitrary integer.
- Assume that x is even. So there exists an integer k with $x = 2k$.
- So $x^2 = (2k)^2 = 2(2k^2)$.
- Since k is an integer, $2k^2$ is also an integer. So x^2 is even.
- So we have proved that if x is even, then x^2 is even.

Proof Recap

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

Proposition:
For all integers x, if x is even, then x^2 is even.

We can **"directly"** prove these statements by stepping through their text.

- The statement is not too surprising – not much work to understand **why** it's true.
- If you step through the parts of the proposition, you wind up with a successful proof.

Proof:

- Let x be an arbitrary integer.
- Assume that x is even. So there exists an integer k with $x = 2k$.
- So $x^2 = (2k)^2 = 2(2k^2)$.
- Since k is an integer, $2k^2$ is also an integer. So x^2 is even.
- So we have proved that if x is even, then x^2 is even.
- Since x was arbitrary, we have shown that for all integers x, if x is even, then x^2 is even

Proof Strategizing

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

New Proposition:

For all integers x, if x^2 is even, then x is even.

(We switched the order: last one was "if x is even, then x^2 is even.")

Most proofs require **strategy**.

- Maybe the proposition is not clearly true – you have to understand **conceptually why it's true** before you convert your understanding to a proof.
- **Maybe "directly" stepping through the statement gets stuck somewhere.**

Proof Attempt:

- Let x be an arbitrary integer.

Proof Strategizing

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

New Proposition:

For all integers x, if x^2 is even, then x is even.

(We switched the order: last one was "if x is even, then x^2 is even.")

Most proofs require **strategy**.

- Maybe the proposition is not clearly true – you have to understand **conceptually why it's true** before you convert your understanding to a proof.
- **Maybe "directly" stepping through the statement gets stuck somewhere.**

Proof Attempt:

- Let x be an arbitrary integer.
- Assume that x^2 is even. So there exists an integer k with $x^2 = 2k$.

Proof Strategizing

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

New Proposition:

For all integers x, if x^2 is even, then x is even.

(We switched the order: last one was "if x is even, then x^2 is even.")

Most proofs require **strategy**.

- Maybe the proposition is not clearly true – you have to understand **conceptually why it's true** before you convert your understanding to a proof.
- **Maybe "directly" stepping through the statement gets stuck somewhere.**

Proof Attempt:

- Let x be an arbitrary integer.
- Assume that x^2 is even. So there exists an integer k with $x^2 = 2k$.
- So $x = \sqrt{2k}$…

Proof Strategizing

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

New Proposition:

For all integers x, if x^2 is even, then x is even.

(We switched the order: last one was "if x is even, then x^2 is even.")

Most proofs require **strategy**.

- Maybe the proposition is not clearly true – you have to understand **conceptually why it's true** before you convert your understanding to a proof.
- **Maybe "directly" stepping through the statement gets stuck somewhere.**

Proof Attempt:

- Let x be an arbitrary integer.
- Assume that x^2 is even. So there exists an integer k with $x^2 = 2k$.
- So $x = \sqrt{2k}$…
- *Then what? Why would this mean x is even?*

Proof Strategizing

Definition: Int **x** is **"even"** if there exists an int **k** such that **x = 2k**.

New Proposition:

For all integers x, if x^2 is even, then x is even.

(We switched the order: last one was "if x is even, then x^2 is even.")

Most proofs require **strategy**.

- Maybe the proposition is not clearly true – you have to understand **conceptually why it's true** before you convert your understanding to a proof.
- **Maybe "directly" stepping through the statement gets stuck somewhere.**
- **This is a good thing!** The hard, interesting, fun part of proofs is coming up with a strategy.
- **Today's lecture:** how to strategize.

Proof Strategizing

Definition: A number $\boldsymbol{x}$ is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x = \frac{a}{b}}$. Otherwise, x is **"irrational."**

Proposition:
There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

Most proofs require **strategy**.

- **Maybe the proposition is not clearly true – you have to understand conceptually why it's true before you convert your understanding to a proof.**
- Maybe "directly" stepping through the statement gets stuck somewhere.

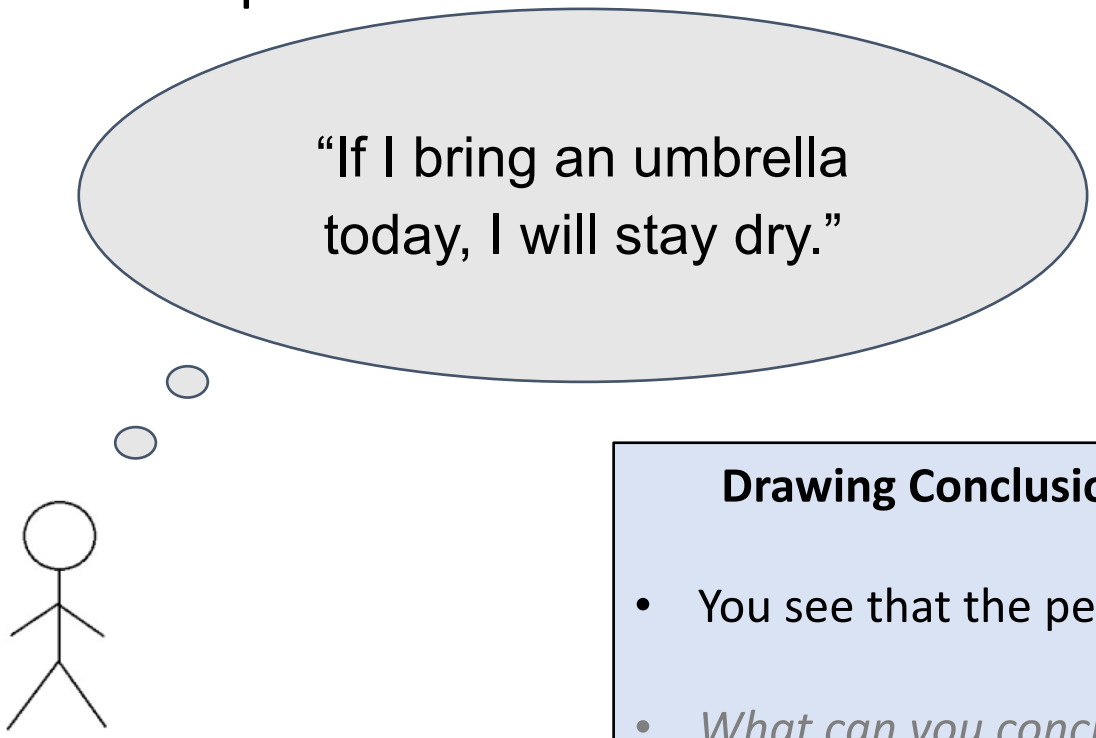
What do you think? (A) Proposition is true (B) Proposition is false

By the end of lecture, we will either prove or refute this proposition!
No spoilers yet

Outline

- Proof Recap and Overview
- **Proof by Contrapositive**
  - Finding the contrapositive
  - Overview of proof technique
- Proof by Contradiction
  - Overview of proof technique
  - $\sqrt{2}$ is irrational
- Proof by Cases
  - Overview of proof technique
  - Irrational powers
- Conceptual Proofs
  - Checkerboard Tiling
  - Infinite Primes

Contrapositives



Drawing Conclusions from *if-then* Statements

- You see that the person has their umbrella.
- *What can you conclude?*
- This person will stay dry.

Contrapositives

Drawing Conclusions from *if-then* Statements

Are there any other situations where we could conclude something?

- What if they don't bring their umbrella?
  - They might have stayed inside, have a raincoat, or maybe it didn't even rain.

we can't conclude anything

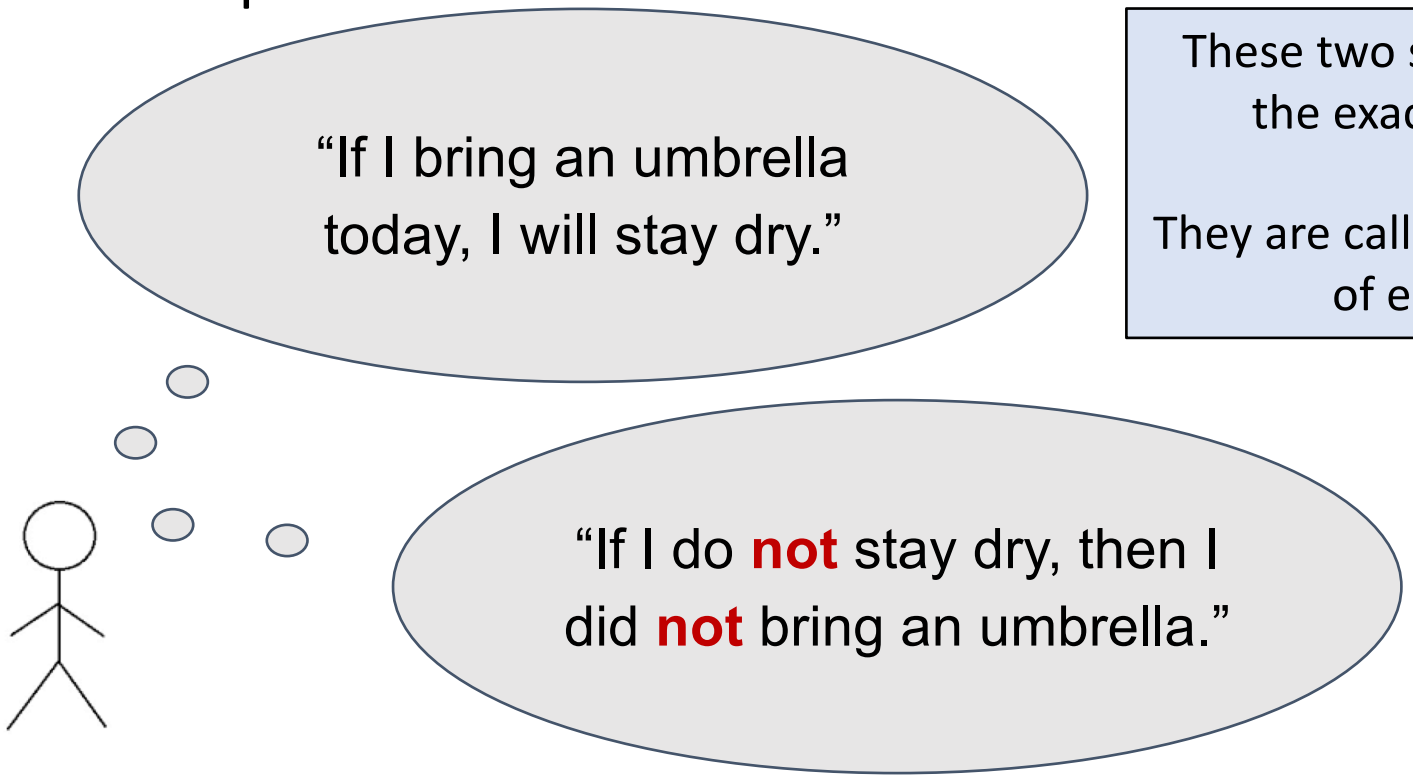
- What if they stay dry all day?
  - Bringing an umbrella might not be the only way they can stay dry

we can't conclude anything.

- What if they show up wet?
  - If they had brought their umbrella, they would not have gotten wet, so:
    - **They must not have brought their umbrella**

she didn't bring an umbrella

Contrapositives



These two statements mean the exact same thing!

They are called **contrapositives** of each other.

Contrapositives

- Any time you have an *if-then* proposition,

"If ***[proposition 1]***, then ***[proposition 2]***"

- The **contrapositive** is the statement

"If ***[negation of proposition 2]***, then ***[negation of proposition 1]***"

- Any statement and its contrapositive have the same truth value
- Contrapositive of contrapositive is the original statement again.

Contrapositives

Original statement: "If ***[prop 1]***, then ***[prop 2]***"
Contrapositive: "If ***[not prop 1]***, then ***[not prop 2]***"

- If it's Tuesday, then we have EECS 203 class.

- If you don't live in Michigan, then you don't live in Ann Arbor.

- If $not\ p$, then q. *(Here p, q can stand for any propositions.)*

Proof by Contrapositive

We can also take contrapositives of "if-then" statements **inside** longer propositions, without changing the meaning

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if x^2 is even, then **x** is even.

If **x** is odd, then x^2 is odd.

Uses Axiom: every integer is even or odd, but not both.
So we can replace "not even" with "odd."

Proof by Contrapositive

Definitions:
- Integer **x** is **"odd"** if $x \equiv 1 \pmod 2$
- Integer **x** is **"even"** if $x \equiv 0 \pmod 2$

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if $\mathbf{x^2}$ is even, then **x** is even.

- **We use a proof by contrapositive.** Our goal is to prove:
  "For all integers **x**, if **x** is odd, then $\mathbf{x^2}$ is odd."

New First Step: ANNOUNCE YOUR PROOF STYLE! So that the reader knows what's happening.

Proof by Contrapositive

Definitions:
- Integer **x** is **"odd"** if $x \equiv 1 \pmod 2$
- Integer **x** is **"even"** if $x \equiv 0 \pmod 2$

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if **x²** is even, then **x** is even.

- **We use a proof by contrapositive.** Our goal is to prove:
  "For all integers **x**, if **x** is odd, then **x²** is odd."
- Let x be an arbitrary integer.

Now we're continuing like usual.
"For all" → start by considering an arbitrary value

Proof by Contrapositive

Definitions:
- Integer **x** is **"odd"** if $x \equiv 1 \pmod 2$
- Integer **x** is **"even"** if $x \equiv 0 \pmod 2$

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if **x²** is even, then **x** is even.

- **We use a proof by contrapositive.** Our goal is to prove:
  "For all integers **x**, if **x** is odd, then **x²** is odd."
- Let x be an arbitrary integer.
- Assume that x is odd. So $x \equiv 1 \ (mod\ 2)$.

Use the formal definition each time it appears.

Proof by Contrapositive

Definitions:
- Integer **x** is **"odd"** if $x \equiv 1 \pmod 2$
- Integer **x** is **"even"** if $x \equiv 0 \pmod 2$

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if **x²** is even, then **x** is even.

- **We use a proof by contrapositive.** Our goal is to prove:
  "For all integers **x**, if **x** is odd, then **x²** is odd."

- Let x be an arbitrary integer.
- Assume that x is odd. So $x \equiv 1 \ (mod\ 2)$.
- So $x^2 \equiv 1^2 \equiv 1 \ (mod\ 2)$.

Rules of modular arithmetic

Proof by Contrapositive

Definitions:
- Integer **x** is **"odd"** if $x \equiv 1 \pmod 2$
- Integer **x** is **"even"** if $x \equiv 0 \pmod 2$

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if **x²** is even, then **x** is even.

- **We use a proof by contrapositive.** Our goal is to prove:

  "For all integers **x**, if **x** is odd, then **x²** is odd."

- Let x be an arbitrary integer.
- Assume that x is odd. So $x \equiv 1 \ (mod\ 2)$.
- So $x^2 \equiv 1^2 \equiv 1 \ (mod\ 2)$.
- So x^2 is odd.

Proof by Contrapositive

Definitions:
- Integer **x** is **"odd"** if $x \equiv 1 \pmod 2$
- Integer **x** is **"even"** if $x \equiv 0 \pmod 2$

Proposition: *this was the one we failed to prove directly*

For all integers **x**, if **x²** is even, then **x** is even.

- **We use a proof by contrapositive.** Our goal is to prove:
  "For all integers **x**, if **x** is odd, then **x²** is odd."
- Let x be an arbitrary integer.
- Assume that x is odd. So $x \equiv 1 \ (mod\ 2)$.
- So $x^2 \equiv 1^2 \equiv 1 \ (mod\ 2)$.
- So x^2 is odd.
- So we have proved that, if x is odd, then x^2 is odd.

Terminology

- **"Proof By Contrapositive:"**
  - Any proof that starts out by modifying the given proposition, replacing all or part of it with its contrapositive.

- **"Direct Proof:"**
  - A proof that does **not** use this contrapositive strategy, nor any of the other new proof styles we're about to see.
  - Before this lecture, all proofs we'd seen were direct proofs.

Outline

- Proof Recap and Overview
- Proof by Contrapositive
  - Finding the contrapositive
  - Overview of proof technique
- **Proof by Contradiction**
  - Overview of proof technique
  - $\sqrt{2}$ is irrational
- Proof by Cases
  - Overview of proof technique
  - Irrational powers
- Conceptual Proofs
  - Checkerboard Tiling
  - Infinite Primes

Another Proof We Can't Do Yet

Proposition:
There do not exist integers **a, b** such that $\mathbf{18}\boldsymbol{a} + \mathbf{6}\boldsymbol{b} = \mathbf{1}$.

- We've seen direct proofs for *"For all"* or *"There exist"* propositions.
- But how would we begin a proof of a *"There do not exist"* proposition?

Proofs by Contradiction

Proposition:

There do not exist integers **a, b** such that $\mathbf{18}\boldsymbol{a} + \mathbf{6}\boldsymbol{b} = \mathbf{1}$.

Strategy: assume the *negation*, and try to find a contradiction

- So the assumption (negation of original statement) must have been wrong
- Thus, we've proven the original statement by *disproving* its negation!

Negated Proposition:

There exist integers **a, b** such that $\mathbf{18}\boldsymbol{a} + \mathbf{6}\boldsymbol{b} = \mathbf{1}$.

Proofs by Contradiction

Proposition:
There do not exist integers **a, b** such that $\boldsymbol{18a + 6b = 1}$.

- **We will use a proof by contradiction. Seeking contradiction,**
- Assume there exist integers a, b such that $18a + 6b = 1$.

First step: ANNOUNCE YOUR PROOF STYLE!

Proofs by Contradiction

Proposition:
There do not exist integers **a, b** such that $\boldsymbol{18a + 6b = 1}$.

- **We will use a proof by contradiction. Seeking contradiction,**
- Assume there exist integers a, b such that $18a + 6b = 1$.
- So $3a + b = \frac{1}{6}$

Rules of algebra

Proofs by Contradiction

Proposition:
There do not exist integers **a, b** such that $\boldsymbol{18a + 6b = 1}$.

- **We will use a proof by contradiction. Seeking contradiction,**
- Assume there exist integers a, b such that $18a + 6b = 1$.
- So $3a + b = \frac{1}{6}$
- Since a, b are integers, $3a + b$ is an integer

Closure of integers

Proofs by Contradiction

Proposition:
There do not exist integers **a, b** such that $\boldsymbol{18a + 6b = 1}$.

- **We will use a proof by contradiction. Seeking contradiction,**
- Assume there exist integers a, b such that $18a + 6b = 1$.
- So $3a + b = \frac{1}{6}$
- Since a, b are integers, $3a + b$ is an integer
- So $\frac{1}{6}$ is an integer. *(Our assumption led to something false!)*

Proofs by Contradiction

Proposition:
There do not exist integers **a, b** such that $\boldsymbol{18a + 6b = 1}$.

- **We will use a proof by contradiction. Seeking contradiction,**
- Assume there exist integers a, b such that $18a + 6b = 1$.
- So $3a + b = \frac{1}{6}$
- Since a, b are integers, $3a + b$ is an integer
- So $\frac{1}{6}$ is an integer. *(Our assumption led to something false!)*
- **This completes the contradiction.**

Acknowledge that the last statement was actually false, so the initial assumption was wrong

Definition: A number x is **"positive"** if $x > 0$.

Proofs by Contradiction

Proposition:
There does not exist a smallest positive real number.

Exercise in handout – try this out (if time)

Irrationality

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

Proposition:
$\sqrt{2}$ is irrational.

Expanded Proposition:
There do not exist two integers a, b with $\frac{a}{b} = \sqrt{2}$.

"There do not exist" proposition – think proof by contradiction!

This proof will be harder in two ways than what we're used to:

- More steps in the logic
- We will use a **lemma:** reuse a statement proved previously (without redoing the proof)

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.
- $\frac{a}{b} = \sqrt{2}$, so $a^2 = 2b^2$, so a^2 is even

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.
- $\frac{a}{b} = \sqrt{2}$, so $a^2 = 2b^2$, so a^2 is even
- By Lemma, ***a* is even**

Lemma:
For all integers **x**, if $\mathbf{x^2}$ is even, then **x** is even.

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.
- $\frac{a}{b} = \sqrt{2}$, so $a^2 = 2b^2$, so a^2 is even
- By Lemma, ***a* is even**
- There exists an integer k for which $a = 2k$, so $a^2 = 4k^2$

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.
- $\frac{a}{b} = \sqrt{2}$, so $a^2 = 2b^2$, so a^2 is even
- By Lemma, ***a* is even**
- There exists an integer k for which $a = 2k$, so $a^2 = 4k^2$
- We have $2b^2 = a^2 = 4k^2$

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:
- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.
- $\frac{a}{b} = \sqrt{2}$, so $a^2 = 2b^2$, so a^2 is even
- By Lemma, ***a* is even**
- There exists an integer k for which $a = 2k$, so $a^2 = 4k^2$
- We have $2b^2 = a^2 = 4k^2$
- So $2k^2 = b^2$, so by Lemma, ***b* is even**

Lemma:
For all integers **x**, if $\mathbf{x^2}$ is even, then **x** is even.

Irrationality

Proposition: $\sqrt{2}$ is irrational.

Definition:

- A number **x** is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x} = \frac{\boldsymbol{a}}{\boldsymbol{b}}$.
- Otherwise, it is **"irrational."**

- **We will use a proof by contradiction. Seeking contradiction,**

- **Assume that $\sqrt{2}$ is rational**. So there exist integers a, b with **no common factors** and $\frac{a}{b} = \sqrt{2}$.
- $\frac{a}{b} = \sqrt{2}$, so $a^2 = 2b^2$, so a^2 is even
- By Lemma, ***a* is even**
- There exists an integer k for which $a = 2k$, so $a^2 = 4k^2$
- We have $2b^2 = a^2 = 4k^2$
- So $2k^2 = b^2$, so by Lemma, ***b* is even**

If the contradiction is at all non-obvious, or the pieces are scattered around the proof, explain it a little.

- **This completes the contradiction**, since we have proved that **a** is even, **b** is even, and **a, b** have no common factors.

Outline

- Proof Recap and Overview
- Proof by Contrapositive
  - Finding the contrapositive
  - Overview of proof technique
- Proof by Contradiction
  - Overview of proof technique
  - $\sqrt{2}$ is irrational
- **Proof by Cases**
  - Overview of proof technique
  - Irrational powers
- Conceptual Proofs
  - Checkerboard Tiling
  - Infinite Primes

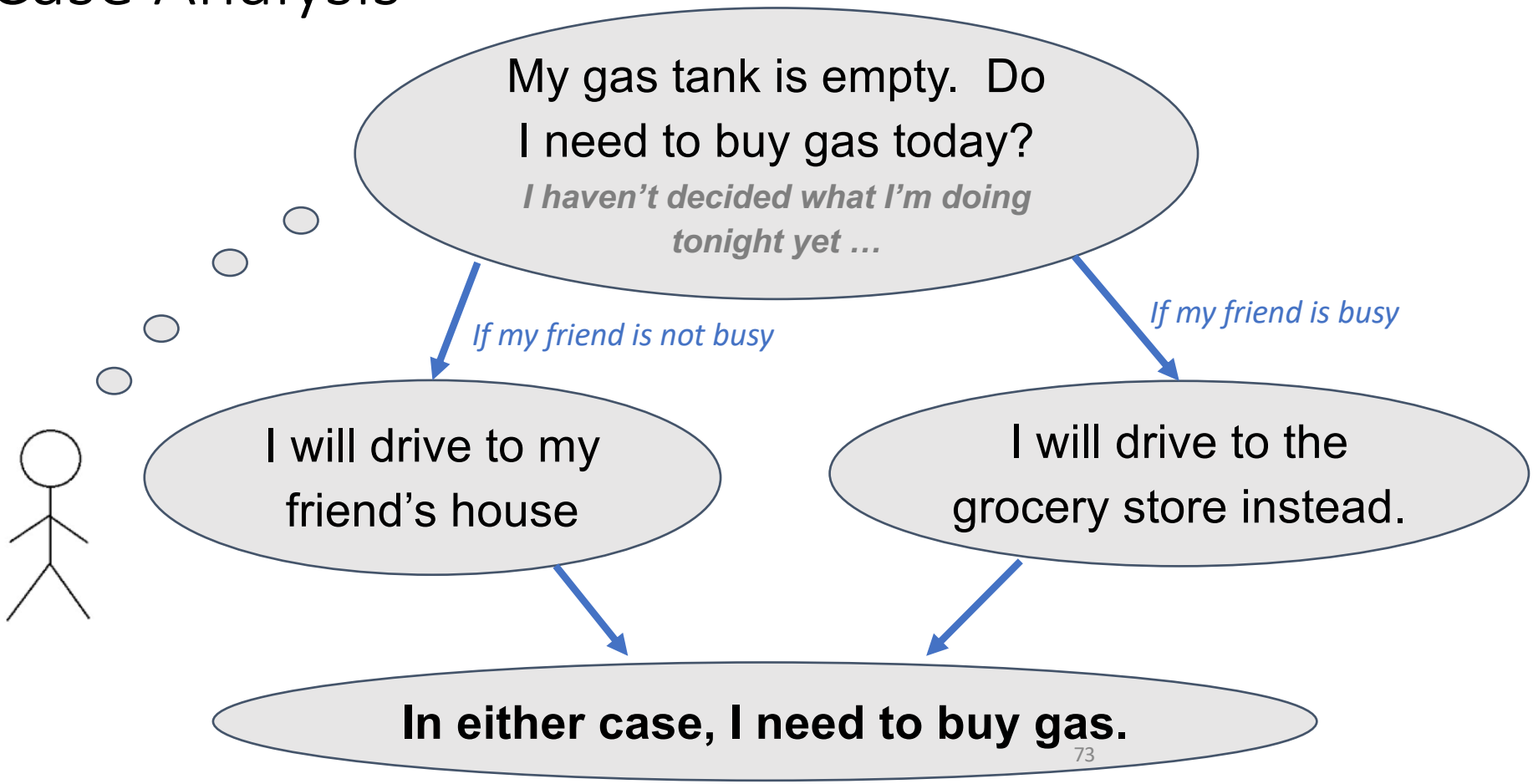
Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

- None of the previous proof methods are very helpful.
- If **x** is an arbitrary integer, we can't say much about $\mathbf{x^2}$.

Strategy:
- Instead of considering arbitrary **x**, split into **cases**, where you assume various things about **x**.
- Make sure **at least one** of our cases is true for any x!
- Prove the proposition in **every** possible case.

Case Analysis



Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

- Let **x** be an arbitrary integer.
- **We will use a proof by cases**. By rules of modular arithmetic, we have:

$$x \equiv 0,\ x \equiv 1, \text{ or } x \equiv 2 \pmod 3$$

Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

- Let **x** be an arbitrary integer.
- **We will use a proof by cases**. By rules of modular arithmetic, we have:

$$x \equiv 0,\ x \equiv 1, \text{ or } x \equiv 2 \pmod 3$$

- **Case 1:** Assume $x \equiv 0$.
- Then $x^2 \equiv 0$, and the proposition is true.

Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

- Let **x** be an arbitrary integer.
- **We will use a proof by cases**. By rules of modular arithmetic, we have:

$$x \equiv 0,\ x \equiv 1, \text{ or } x \equiv 2 \pmod 3$$

- **Case 1:** Assume $x \equiv 0$.
- Then $x^2 \equiv 0$, and the proposition is true.

- **Case 2:** Assume $x \equiv 1$.
- Then $x^2 \equiv 1$, and the proposition is true.

Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

- Let **x** be an arbitrary integer.
- **We will use a proof by cases**. By rules of modular arithmetic, we have:

$$x \equiv 0,\ x \equiv 1, \text{ or } x \equiv 2 \pmod 3$$

- **Case 1:** Assume $x \equiv 0$.
- Then $x^2 \equiv 0$, and the proposition is true.

- **Case 2:** Assume $x \equiv 1$.
- Then $x^2 \equiv 1$, and the proposition is true.

- **Case 3:** Assume $x \equiv 2$.
- Then $x^2 \equiv 4 \equiv 1$, and the proposition is true.

Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

- Let **x** be an arbitrary integer.
- **We will use a proof by cases**. By rules of modular arithmetic, we have:

$$x \equiv 0,\ x \equiv 1, \text{ or } x \equiv 2 \pmod 3$$

- **Case 1:** Assume $x \equiv 0$.
- Then $x^2 \equiv 0$, and the proposition is true.

- **Case 2:** Assume $x \equiv 1$.
- Then $x^2 \equiv 1$, and the proposition is true.

- **Case 3:** Assume $x \equiv 2$.
- Then $x^2 \equiv 4 \equiv 1$, and the proposition is true.

- **Since the proposition is true in any case, it is true.**

Proof by Cases

Proposition:
For all integers x, we have $x^2 \equiv 0$ or $x^2 \equiv 1 \pmod 3$

Proving that **one of several** possible conditions holds sometimes signals that proof-by-cases will be useful

(But proof-by-cases is still sometimes useful even for propositions without this "**or**" flag…)

Proof Styles

Handout

The 4 proof styles discussed today:

1. **Direct Proofs**: Proceed without any of the following styles

2. **Proof by** Contrapositive: To prove "if p, then q", instead prove the logically equivalent statement "if not q, then not p"

3. **Proof by** Contraction : Assume the **negation**, and try to prove something false. is true ; i.e. try to find a contradiction.

4. **Proof by** Cases **:** Break the situation down into cases, and show that each case leads to the desired conclusion.

Which Style Should I Use?

Handout

1. **Proof by Contrapositive**: Flagged by an "if p , then q" piece of the proposition that you find difficult to prove directly.

2. **Proof by Contradiction**: Often (but not always) flagged by "there do not exist…" at beginning of proposition

3. **Proof by Cases:** Often (but not always) flagged by a "p or q" piece of the proposition

The Reveal

Definition: A number $\boldsymbol{x}$ is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x = \frac{a}{b}}$. Otherwise, x is **"irrational."**

Proposition:
There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

What do you think? (A) Proposition is true (B) Proposition is false

The Reveal

Definition: A number $\boldsymbol{x}$ is **"rational"** if there exist two integers $\boldsymbol{a}, \boldsymbol{b}$ with $\boldsymbol{x = \frac{a}{b}}$. Otherwise, x is **"irrational."**

Proposition:
There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

What do you think? **(A) Proposition is true** (B) Proposition is false

- Strategy: **proof by cases**
- The magic of the proof is picking a clever case breakdown - after that, it's easy!

The Reveal

Theorem: There exist irrational numbers x, y such that x^y is rational.

Lemma: $\sqrt{2}$ is irrational.

The Reveal

Theorem: There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

- Consider the number $\sqrt{2}^{\sqrt{2}}$.  This number is either rational or irrational.
- **We split into two cases accordingly.**

- **Case 1: Assume that $\sqrt{2}^{\sqrt{2}}$ is rational.**
  - In this case, consider $x = y = \sqrt{2}$.
  - By **Lemma**, both x, y are irrational

Lemma: $\sqrt{2}$ is irrational.

The Reveal

Theorem: There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

- Consider the number $\sqrt{2}^{\sqrt{2}}$.  This number is either rational or irrational.
- **We split into two cases accordingly.**

- **Case 1: Assume that $\sqrt{2}^{\sqrt{2}}$ is rational.**
  - In this case, consider $x = y = \sqrt{2}$.
  - By **Lemma**, both x, y are irrational
  - By **assumption, $\boldsymbol{x^y}$** is rational.
  - So the theorem holds.

Lemma: $\sqrt{2}$ is irrational.

The Reveal

Theorem: There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

- Consider the number $\sqrt{2}^{\sqrt{2}}$. This number is either rational or irrational.
- **We split into two cases accordingly.**

- **Case 1: Assume that $\sqrt{2}^{\sqrt{2}}$ is rational.**
  - In this case, consider $x = y = \sqrt{2}$.
  - By **Lemma**, both x, y are irrational
  - By **assumption, $\boldsymbol{x^y}$** is rational.
  - So the theorem holds.

- **Case 2: Assume that $\sqrt{2}^{\sqrt{2}}$ is irrational.**
  - In this case, consider $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$.

The Reveal

Theorem: There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

- Consider the number $\sqrt{2}^{\sqrt{2}}$.  This number is either rational or irrational.
- **We split into two cases accordingly.**

- **Case 1: Assume that $\sqrt{2}^{\sqrt{2}}$ is rational.**
  - In this case, consider $x = y = \sqrt{2}$.
  - By **Lemma**, both x, y are irrational
  - By **assumption,** $\boldsymbol{x^y}$ is rational.
  - So the theorem holds.

- **Case 2: Assume that $\sqrt{2}^{\sqrt{2}}$ is irrational.**
  - In this case, consider $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$.
  - By **assumption, x** is irrational.
  - By **lemma**, y is irrational

Lemma: $\sqrt{2}$ is irrational.

The Reveal

Theorem: There exist irrational numbers $\boldsymbol{x}, \boldsymbol{y}$ such that $\boldsymbol{x^y}$ is rational.

- Consider the number $\sqrt{2}^{\sqrt{2}}$.  This number is either rational or irrational.
- **We split into two cases accordingly.**

- **Case 1: Assume that $\sqrt{2}^{\sqrt{2}}$ is rational.**
  - In this case, consider $x = y = \sqrt{2}$.
  - By **Lemma**, both x, y are irrational
  - By **assumption, x^y** is rational.
  - So the theorem holds.

- **Case 2: Assume that $\sqrt{2}^{\sqrt{2}}$ is irrational.**
  - In this case, consider $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$.
  - By **assumption, x** is irrational.
  - By **lemma**, y is irrational
  - By algebra: $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^{2} = 2.$
  - 2 is rational, so the theorem holds.

Since the theorem holds in either case, it is proved.

Outline

- Proof Recap and Overview
- Proof by Contrapositive
  - Finding the contrapositive
  - Overview of proof technique
- Proof by Contradiction
  - Overview of proof technique
  - $\sqrt{2}$ is irrational
- Proof by Cases
  - Overview of proof technique
  - Irrational powers
- **Conceptual Proofs**
  - Checkerboard Tiling
  - Infinite Primes

Strategizing

Most proofs require **strategy**.

- Maybe the proposition is not clearly true – you have to understand **conceptually why it's true** before you convert your understanding to a proof.
- **Maybe "directly" stepping through the statement gets stuck somewhere.**

Usually solved by **choosing a good proof style** to reframe the proposition

- Proof by contrapositive
- Proof by contradiction
- Proof by cases

- **More proof styles coming**, but not until ≈ Lecture 10

Strategizing

Most proofs require **strategy**.

- **Maybe the proposition is not clearly true – you have to understand conceptually why it's true before you convert your understanding to a proof.**
- Maybe "directly" stepping through the statement gets stuck somewhere.

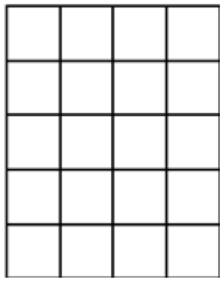
Coming up with a proof generally takes two steps:

Find a **way to look at the problem** that helps you understand why the proposition is true

If your understanding is correct, the universe will let you write a **receipt** of your understanding by a step-by-step proof.

A pure  proof

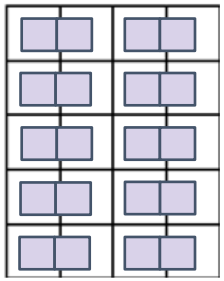
Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.



A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

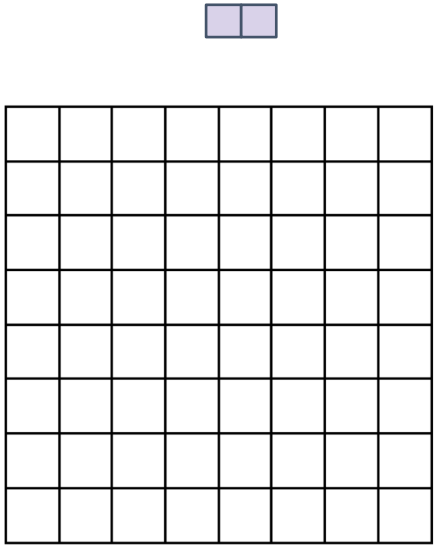
Example



A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

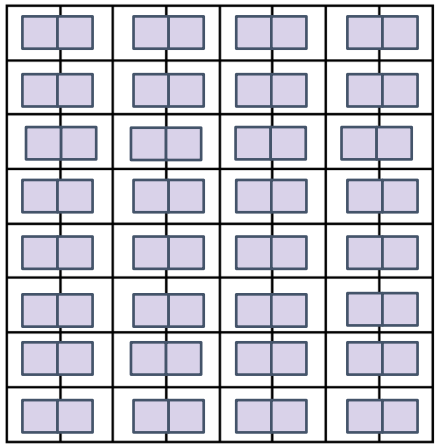
Proposition:
There exists a way to **tile** an 8x8 grid with **2x1** dominoes.



A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

Proposition:
There exists a way to **tile** an 8x8 grid with **2x1** dominoes.



Proof:

- Consider the following valid tiling.
- (Done!)

A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

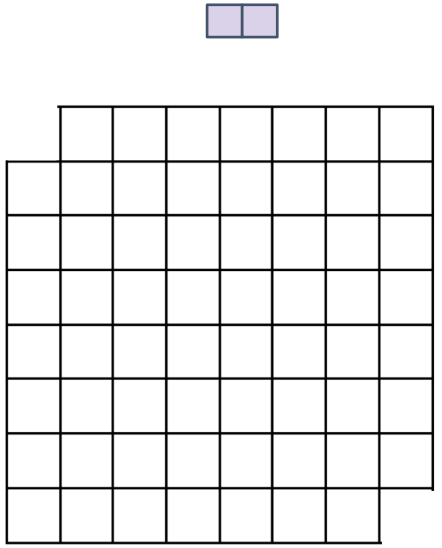
Proposition:

There exists a way to **tile** an **8x8** grid **with the two opposite corners removed** with **2x1** dominoes.

What do you think?

(A) Proposition is true

(B) Proposition is false



A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

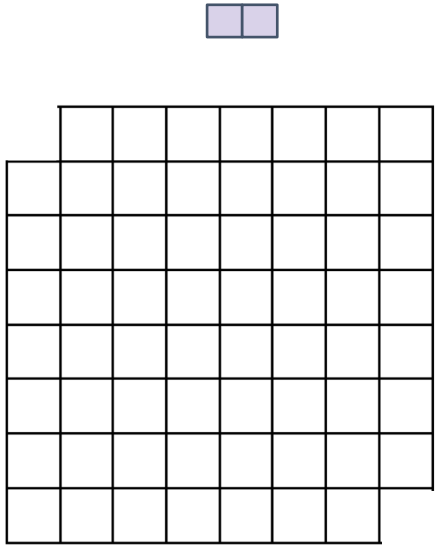
Proposition:

There exists a way to **tile** an **8x8** grid **with the two opposite corners removed** with **2x1** dominoes.

What do you think?

(A) Proposition is true

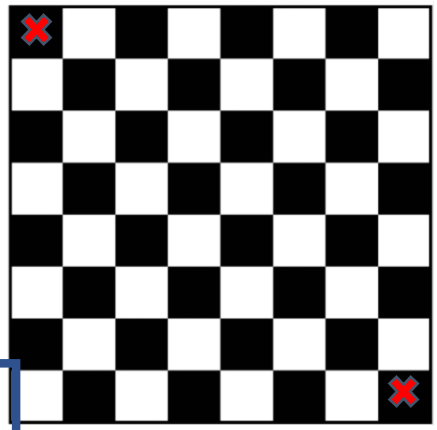
(B) Proposition is false



A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

Proposition:
There exists a way to **tile** an **8x8** grid **with the two opposite corners removed** with **2x1** dominoes.



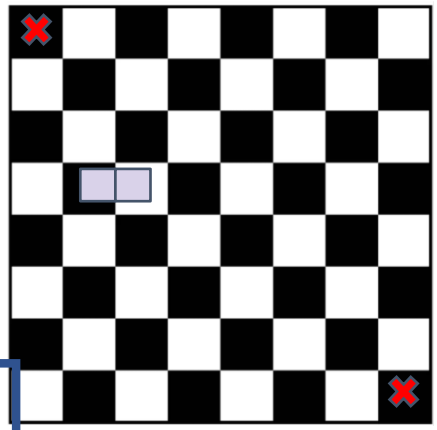
Disproof:

- **We use a proof by contradiction. Seeking contradiction,**
- Assume that a tiling exists.
- Color the cells in a checkerboard pattern.

A pure  proof

Definition: A **"tiling"** of a grid by 2x1 dominoes is a placement of dominoes on the grid so that every square has exactly one domino.

Proposition:
There exists a way to **tile** an **8x8** grid **with the two opposite corners removed** with **2x1** dominoes.



Disproof:

- **We use a proof by contradiction. Seeking contradiction,**
- Assume that a tiling exists.
- Color the cells in a checkerboard pattern. 
- Every domino covers one black square and one white square.
- We count 30 black squares remaining
- We count 32 white squares remaining.
- **This completes the contradiction**

Infinite Primes

Definition: An integer $k \geq 2$ is **"prime"** if there do not exist two integers $a, b \geq 2$ with $k = ab$.

Axiom:
Every integer $k \geq 2$ is a multiple of a prime number p.
(Meaning there exists prime p such that $k \equiv 0 \ (mod\ p)$)

Proposition:
There are infinitely many prime numbers.

Rephrased Proposition:
There does not exist a finite list $\{p_1, \dots, p_c\}$ that contains all the prime numbers.

No "there exists" or "for all" or "there does not exist" – how do we begin?

Style: proof by contradiction
- Assume this list $\{p_1, \dots, p_c\}$ exists…

The integer $Q = p_1 p_2 p_3 \dots p_c + 1$ is not a multiple of any of $\{p_1, \dots, p_c\}$.
Contradicts **axiom!**

Infinite Primes

Theorem: There are infinitely many prime numbers.

- **We will use a proof by contradiction. Seeking contradiction,**

- Assume there exists a complete, finite list of prime numbers $\{p_1, \dots, p_c\}$.
- Let Q be one more than the product of all primes in the list: $Q = p_1 p_2 p_3 \dots p_c + 1$

Infinite Primes

Theorem: There are infinitely many prime numbers.

- **We will use a proof by contradiction. Seeking contradiction,**

- Assume there exists a complete, finite list of prime numbers $\{p_1, \dots, p_c\}$.
- Let Q be one more than the product of all primes in the list: $Q = p_1 p_2 p_3 \dots p_c + 1$
- For any prime p_i in the list, $p_1 p_2 p_3 \dots p_c$ is a multiple of p_i.
- Q is 1 more than this product, so $Q \equiv 1 \ (mod \ p_i)$

Infinite Primes

Theorem: There are infinitely many prime numbers.

- **We will use a proof by contradiction. Seeking contradiction,**

- Assume there exists a complete, finite list of prime numbers $\{p_1, \dots, p_c\}$.
- Let Q be one more than the product of all primes in the list: $Q = p_1 p_2 p_3 \dots p_c + 1$
- For any prime p_i in the list, $p_1 p_2 p_3 \dots p_c$ is a multiple of p_i.
- Q is 1 more than this product, so $Q \equiv 1 \ (mod\ p_i)$
- By **Axiom**, there must exist a prime p_i with $Q \equiv 0 \ (mod\ p_i)$.

Axiom:
Every integer $k \geq 2$ is a multiple of a prime number p.
(Meaning there exists prime p such that $k \equiv 0 \ (mod\ p)$)

Infinite Primes

Theorem: There are infinitely many prime numbers.

- **We will use a proof by contradiction. Seeking contradiction,**

- Assume there exists a complete, finite list of prime numbers $\{p_1, \dots, p_c\}$.
- Let Q be one more than the product of all primes in the list: $Q = p_1 p_2 p_3 \dots p_c + 1$

- For any prime p_i in the list, $p_1 p_2 p_3 \dots p_c$ is a multiple of p_i.
- Q is 1 more than this product, so $Q \equiv 1 \ (mod\ p_i)$
- By **Axiom**, there must exist a prime p_i with $Q \equiv 0 \ (mod\ p_i)$.

- **This completes the contradiction.**

Wrapup

- **Proof Styles** can help you prove propositions, especially when "stepping through the proposition" doesn't seem to work.
  - Contrapositive, contradiction, and cases covered today

- Many proofs aren't straightforward even with a style: they require a clever way to reframe the problem

- **Next Few Lectures:** Revisiting truth values, propositions, etc. from the standpoint of logic. (Why do all these proof ideas really work?)