Discrete Mathematics

Mathematical Proofs

Theorem

A **theorem** (**fact** or **result**) is a statement that can be shown to be true.

Proposition

Less important theorem

Proof

A **proof** is a valid argument that establishes the truth of a theorem.

The statements used in a proof can include:

- axioms (postulates) – statements assumed to be true
- proven theorems

Lemma

A less important theorem that is helpful in the proof of other results

Corollary

A theorem that can be established directly from a theorem that has been proof.

Conjecture

A conjecture is a statement that is **being proposed to be true**.

A conjecture becomes a theorem when we can find a proof of it.

Only Prime Numbers?

Let $p(n) ::= n^2 + n + 41.$

Hypothesis:

$\forall n \epsilon N$ P(n) is a prime number

Only Prime Numbers?

Evidence:

$p(0) = 41$ prime

$p(1) = 43$ prime

$p(2) = 47$ prime

$p(3) = 53$ prime

$p(20) = 461$ prime **looking good!**

$p(39) = 1601$ prime **enough already!**

Only Prime Numbers?

$\forall n \epsilon N \; P(n) ::= n^2 + n + 41$
is a prime number

This can't be a coincidence.
The hypothesis must be true.

BUT IT'S NOT:

$p(40) = 1681$ is NOT PRIME.

Further Extreme Example

EULER'S CONJECTURE (1769)

$$a^4 + b^4 + c^4 = d^4$$

has no solution for a, b, c ,d positive integers:

$$a^4 + b^4 + c^4 \neq d^4$$

Further Extreme Example

Counterexample: 218 years later by Noam Elkies

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

Further Extreme Example

Hypothesis: $313 \cdot (x^3 + y^3) = z^3$

has no positive integer solution.

False. But smallest counterexample has

MORE THAN 1000 digits!

Goldbach Conjecture

Every even integer greater than 2 is the sum of two primes.

Evidence:

$4 = 2 + 2$

$6 = 3 + 3$

$8 = 5 + 3$

:

$20 = 13 + 7$

True for all even numbers with up to 13 digits.

It remains an OPEN problem:

No counterexample, no proof.

Direct Proofs

A direct proof shows that conditional statement $p \rightarrow q$ is true by showing that if p is true then q must also be true, so that the combination of p true and q false never occurs.

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 $n = 2k + 1$.
- 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: Let n be an even integer.

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. ■

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 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 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 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 i … n.

Proof: Let n b …

Since n …

such th …

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

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

Therefore, n^2 is even. ■

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

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

m (name

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

Therefore, n^2 is even. ■

An Important Result

- Set equality is defined as follows

Two sets A and B are equal if every element of A is an element of B and every element of B is an element of A.

- In practice, this definition is a bit 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 $A = B$.

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

How do we prove that this is true for *any* choice of sets?

Proving Something Always Holds

- Many statements have the form

  For any x, some property $P(x)$ holds

- Examples:

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

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

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

  Everything that drowns me makes me wanna fly.

- How do we prove these statements when there are (potentially) infinitely many cases to check?

Arbitrary Choices

- To prove that $P(x)$ is true for all possible x, show that no matter what choice of x you make, $P(x)$ must be true.
- Start the proof by making an **arbitrary choice** of x:
  - "Let x be chosen arbitrarily."
  - "Let x be an arbitrary even integer."
  - "Let x be an arbitrary set containing 137."
  - "Consider any x."
- Demonstrate that $P(x)$ holds true for this choice of x.

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: 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 $B \subseteq A$.

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

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 $B \subseteq A$**.

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 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 $B \subseteq A$. Because $A \subseteq B$, if we take an arbitrary $x \in A$, we know that $x \in B$.

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 $B \subseteq A$. Because $A \subseteq B$, if we take an arbitrary $x \in A$, we know that $x \in B$. Similarly, since $B \subseteq A$, if we take an arbitrary $x \in B$, we'll see that $x \in A$ as well.

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 $B \subseteq A$.

Because $A \subseteq B$, if we take an arbitrary $x \in A$, we know that $x \in B$. Similarly, since $B \subseteq A$, if we take an arbitrary $x \in B$, we'll see that $x \in A$ as well.

Therefore, whenever $x \in A$ we have $x \in B$, and whenever $x \in B$ we have $x \in A$.

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 $B \subseteq A$.

Because $A \subseteq B$, if we take an arbitrary $x \in A$, we know that $x \in B$. Similarly, since $B \subseteq A$, if we take an arbitrary $x \in B$, we'll see that $x \in A$ as well.

Therefore, whenever $x \in A$ we have $x \in B$, and whenever $x \in B$ we have $x \in A$.

Consequently, 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: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. Because $A \subseteq B$, if we take an arbitrary $x \in A$, we know that $x \in B$. Similarly, since $B \subseteq A$, if we take an arbitrary $x \in B$, we'll see that $x \in A$ as well.

Therefore, whenever $x \in A$ we have $x \in B$, and whenever $x \in B$ we have $x \in A$.

Consequently, if $A \subseteq B$ and $B \subseteq A$, then $A = B$. ■

If you want to prove that P implies Q,
assume P and prove Q.

Don't assume Q and then prove P!

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

An Entirely Different Proof

Theorem: **There exists** a natural number $n > 0$ **such that** the sum of all natural numbers less than n is equal to n.

This is a fundamentally different type of proof that what we've done before. Instead of showing that <u>*every*</u> object has some property, we want to show that <u>*some*</u> object has a given property.

Universal vs. Existential Statements

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

  For all x, $P(x)$ is true.

- We've seen how to prove these statements.

Universal vs. Existential Statements

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

  For all x, P(x) is true.

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

  There exists an x for which P(x) is true.

- How do you prove an existential statement?

Proving an Existential Statement

- We will see several different ways to prove "there is some x for which $P(x)$ is true."
- Simple approach: Just go and find some x for which $P(x)$ is true!
  - In our case, we need to find a positive natural number n such that that sum of all smaller natural numbers is equal to n.
  - Can we find one?

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

Proof: Take $n = 3$.

The three natural numbers smaller than three are 0, 1, and 2.

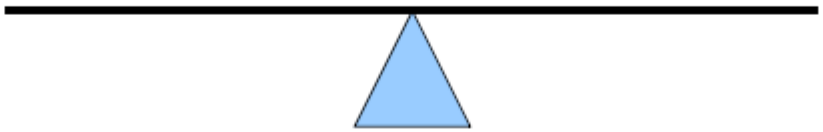
Notice that $0 + 1 + 2 = 3$.

Therefore, three is a natural number greater than zero equal to the sum of all smaller natural numbers. ■

The Counterfeit Coin Problem

Problem Statement

- You are given a set of three seemingly identical coins, two of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only one weighing on the balance, find the counterfeit coin.



Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

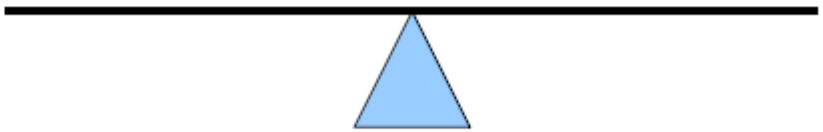
Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

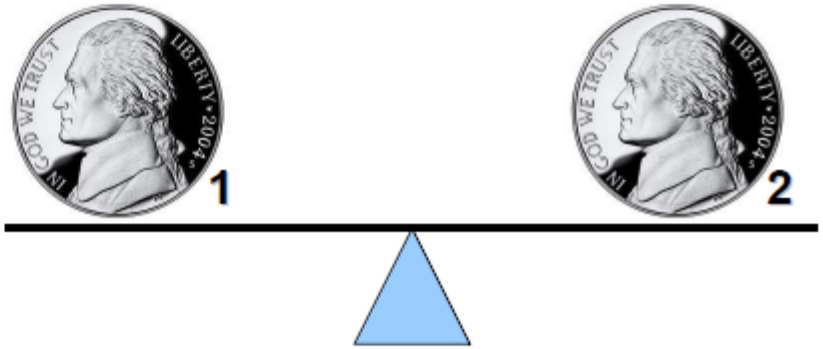
This is an existential statement.

We should try to look for an actual way to do this.

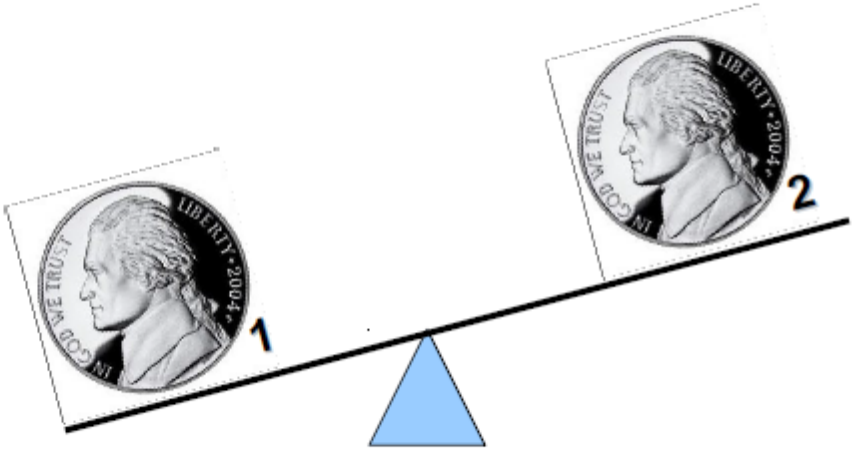
Finding the Counterfeit Coin



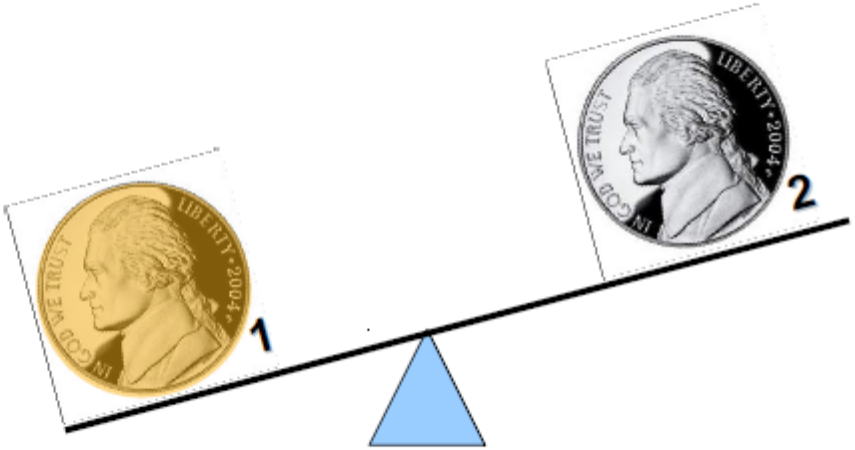
Finding the Counterfeit Coin



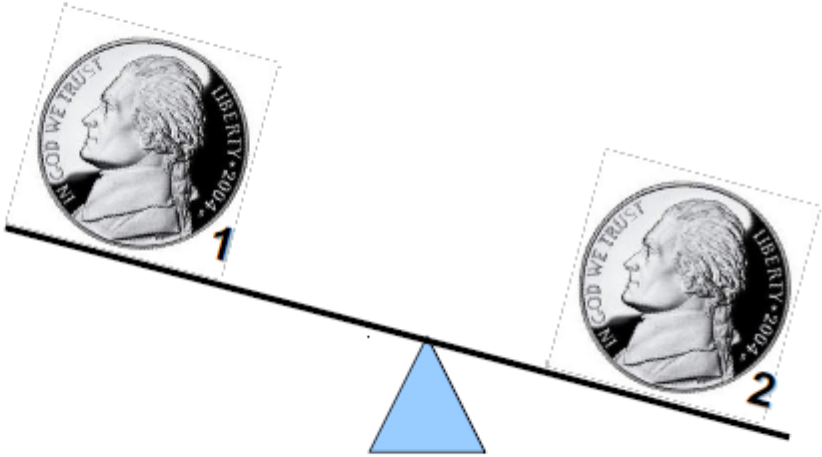
Finding the Counterfeit Coin



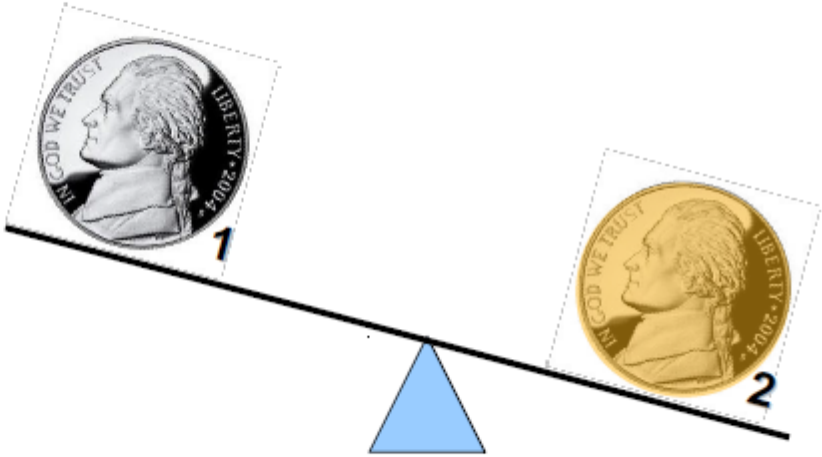
Finding the Counterfeit Coin



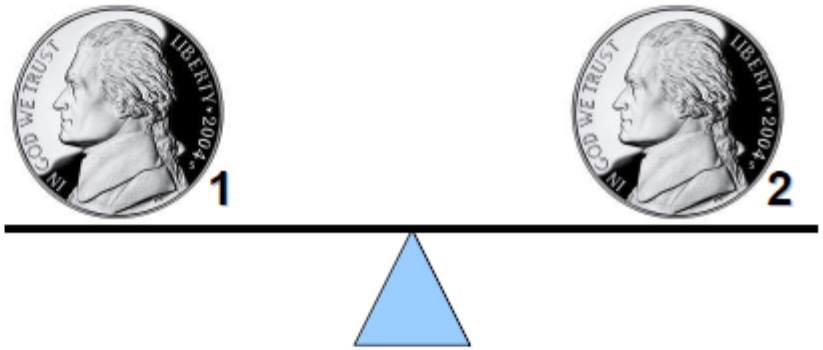
Finding the Counterfeit Coin



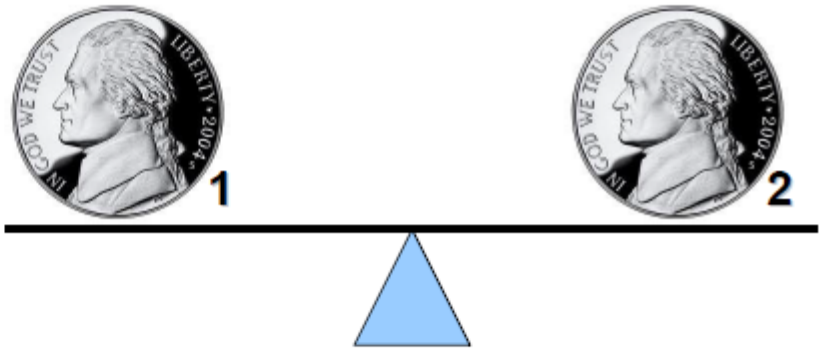
Finding the Counterfeit Coin



Finding the Counterfeit Coin



Finding the Counterfeit Coin



Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B.

Case 2: Coin B is heaver than coin A.

Case 3: Coins A and B have the same weight.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B.

Case 2: Coin B is heaver than coin A.

Case 3: C

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: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A.

Case 3: Coins A and B have the same weight.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

In a proof by cases, after demonstrating each case, you should summarize the cases afterwards to make your point clearer.

is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

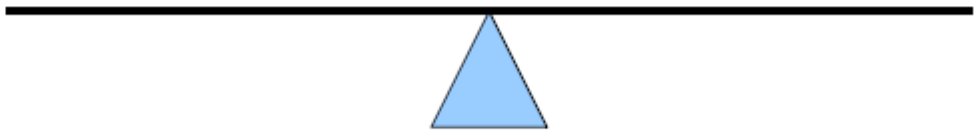
Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin. ■

A Harder Problem

- You are given a set of **nine** seemingly identical coins, eight of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only **two** weighings on the balance, find the counterfeit coin.

Finding the Counterfeit Coin

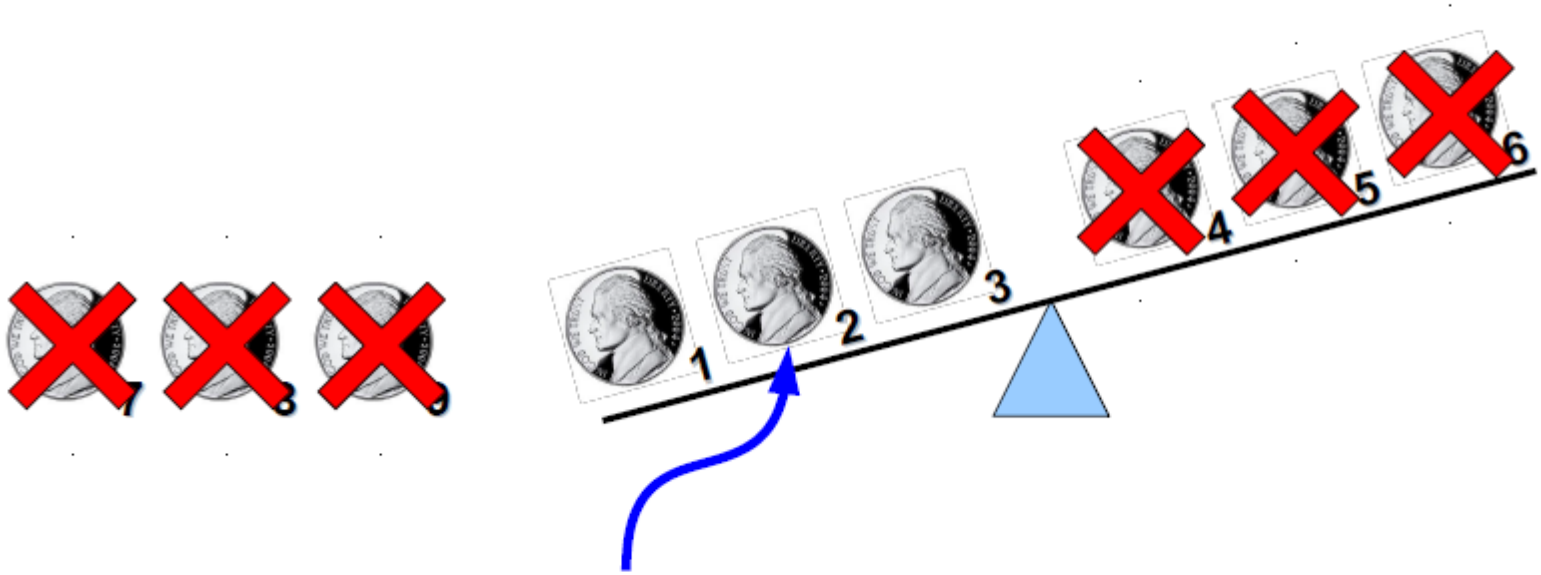


Finding the Counterfeit Coin

Finding the Counterfeit Coin

Finding the Counterfeit Coin

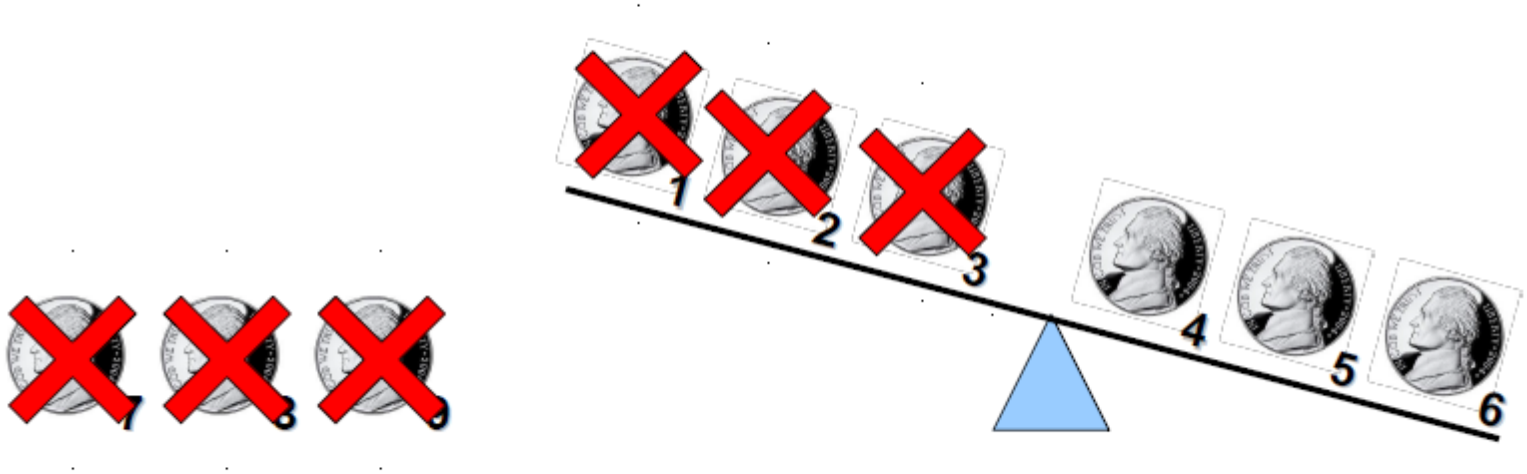
Finding the Counterfeit Coin



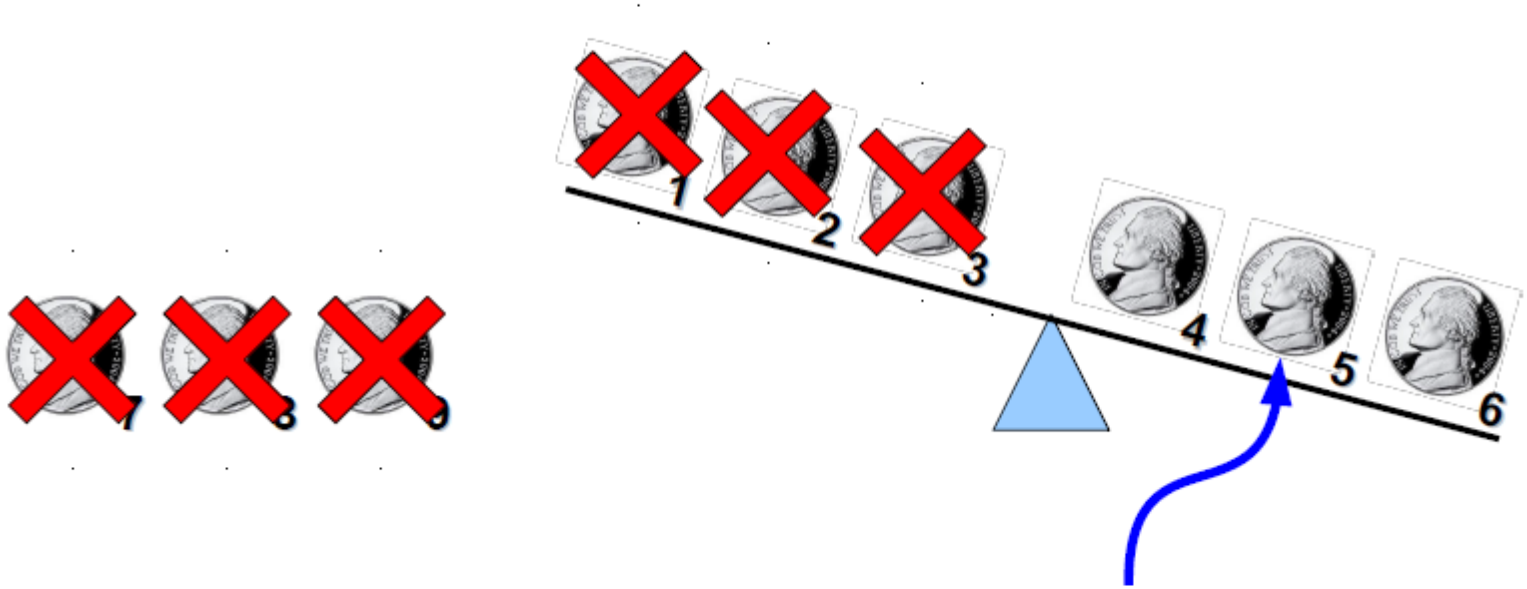
Now we have one weighing to find the counterfeit out of these three.

Finding the Counterfeit Coin

Finding the Counterfeit Coin



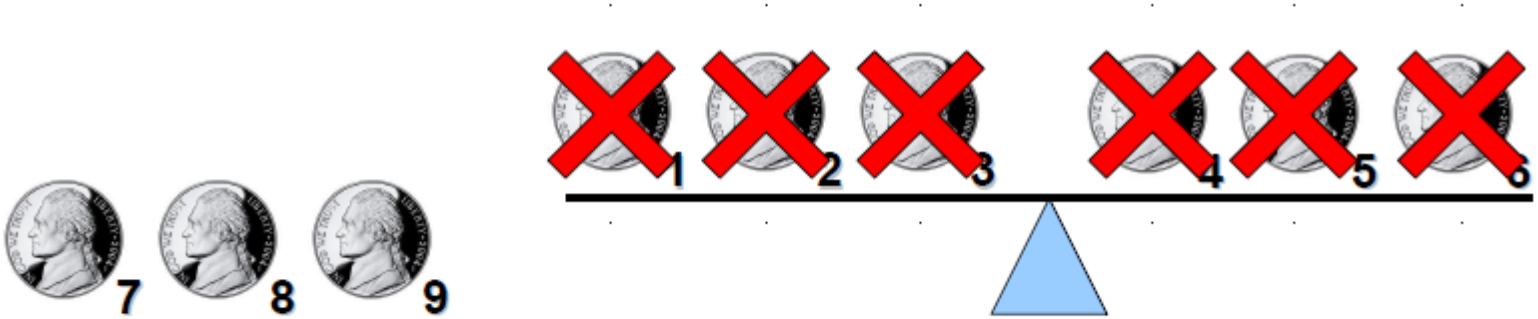
Finding the Counterfeit Coin



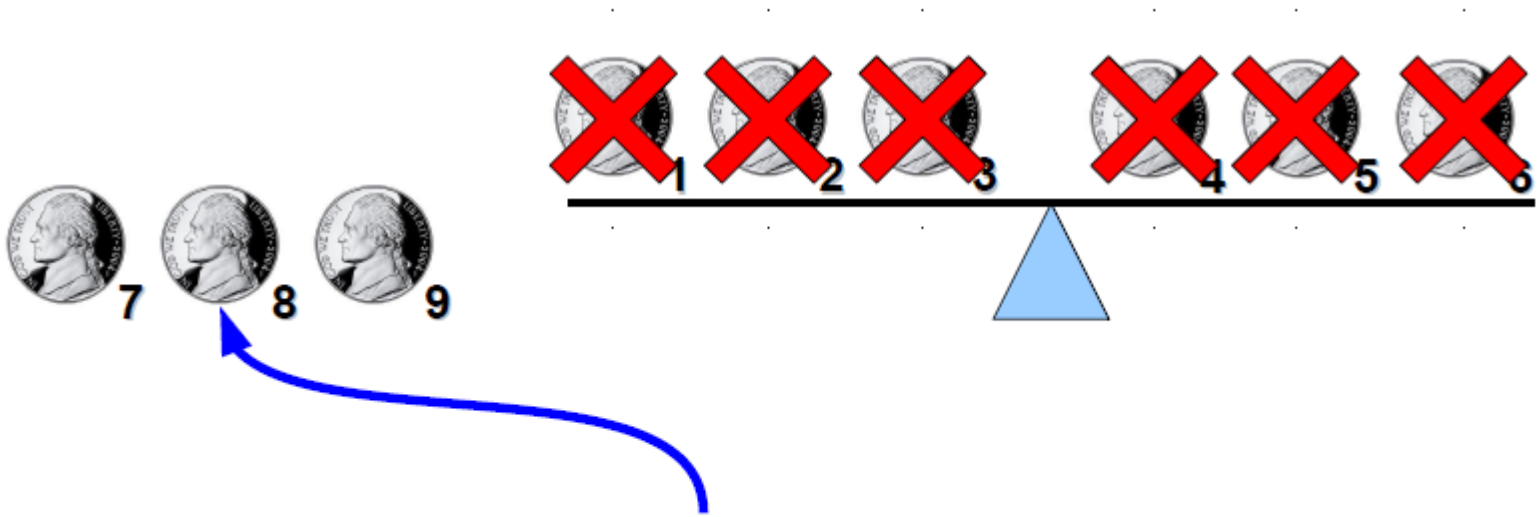
Now we have one weighing to find the counterfeit out of these three.

Finding the Counterfeit Coin

Finding the Counterfeit Coin



Finding the Counterfeit Coin



Now we have one weighing to find the counterfeit out of these three.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B.

Case 2: Group B is heavier than group A.

Case 3: Groups A and B have the same weight.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A.

Case 3: Groups A and B have the same weight.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

When proving a result, it's perfectly fine to refer to theorems you've proven earlier! Here, we cite our theorem from before and say it's possible to find which of three coins is the counterfeit.

In this course, feel free to refer to any theorem that we've proven in lecture, in the course notes, in the book, in section, or in previous problem sets when writing your proofs.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing. Consequently, it's possible to find which of the nine coins is counterfeit in just two weighings.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing. Consequently, it's possible to find which of the nine coins is counterfeit in just two weighings. ■

Relations Between Proofs

- Proofs often build off of one another: large results are almost often accomplished by building off of previous work.
  - Like writing a large program – split the work into smaller methods, across different classes, etc. instead of putting the whole thing into `main`.
- A result that is proven specifically as a stepping stone toward a larger result is called a **lemma**.
- We can treat the proof of the three-coin case as a lemma in the larger proof about nine coins.
  - The result in itself isn't particularly impressive, but it helps us prove a more advanced result.

Our Very Second Lemma

- Set equality is defined as follows

$A = B$ precisely when
for every $x \in A$, $x \in B$ and vice-versa.

- This definition makes it a bit tricky to prove that two sets are equal.
- Instead, we will prove the following result:

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

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

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

Proof:

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Thus whenever $x \in A$, $x \in B$ and whenever $x \in B$, $x \in A$ as well.

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Thus whenever $x \in A$, $x \in B$ and whenever $x \in B$, $x \in A$ as well.

Consequently, A = B.

Lemma: 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 such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Thus whenever $x \in A$, $x \in B$ and whenever $x \in B$, $x \in A$ as well.

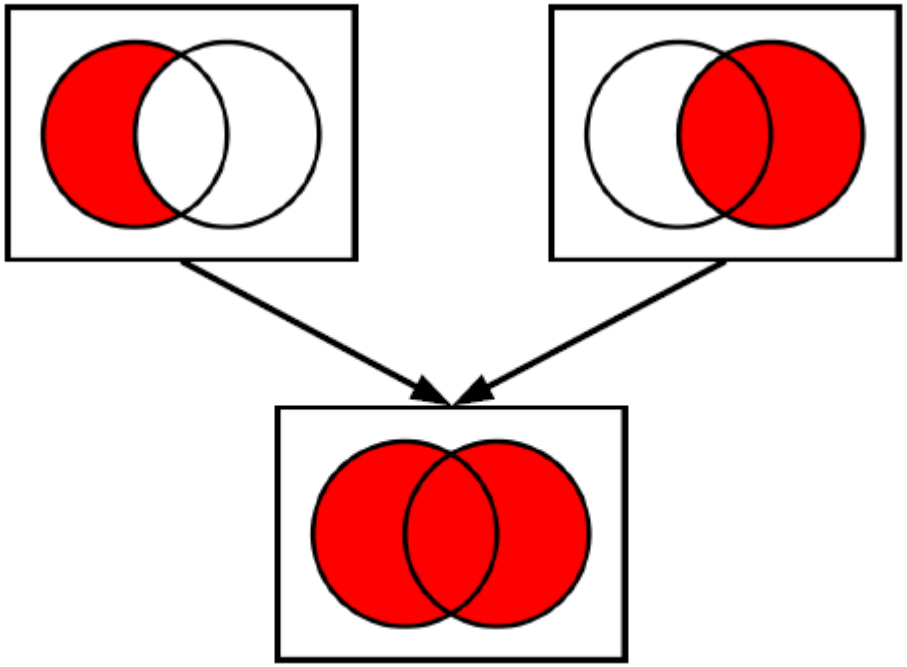
Consequently, A = B. ■

Using Our Lemma

- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.

Using Our Lemma

- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.



Using Our Lemma

- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.
- Proof idea: Show that each set is a subset of the other.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$.

Case 2: $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$.

Case 2: $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$. This means that $x \in A$, and so $x \in A \cup B$ as well.

Case 2: $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$. This means that $x \in A$, and so $x \in A \cup B$ as well.

Case 2: $x \in B$. Then $x \in A \cup B$ as well.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$. This means that $x \in A$, and so $x \in A \cup B$ as well.

Case 2: $x \in B$. Then $x \in A \cup B$ as well.

In either case, any $x \in (A - B) \cup B$ also satisfies $x \in A \cup B$, so $(A - B) \cup B \subseteq A \cup B$ as required. ■

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$.

Case 2: $x \in A$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

We're already doing a proof by cases, but inside this particular case there's two more cases to consider. There's nothing wrong with that; just like nested loops in a program, we can have nested cases.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$. Thus $x \in A - B$, and therefore $x \in (A - B) \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$. Thus $x \in A - B$, and therefore $x \in (A - B) \cup B$.

In either case, any $x \in (A - B) \cup B$ also satisfies $x \in A \cup B$, so $(A - B) \cup B \subseteq A \cup B$ as required.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$. Thus $x \in A - B$, and therefore $x \in (A - B) \cup B$.

In either case, any $x \in (A - B) \cup B$ also satisfies $x \in A \cup B$, so $(A - B) \cup B \subseteq A \cup B$ as required. ■

Theorem: For any sets A and B, $(A - B) \cup B = A \cup B$.

Proof: Let A and B be arbitrary sets.

By Lemma 1, $(A - B) \cup B \subseteq A \cup B$.

By Lemma 2, $A \cup B \subseteq (A - B) \cup B$.

Consequently, by our earlier lemma,
$(A - B) \cup B = A \cup B$. ■

Disproving Statements

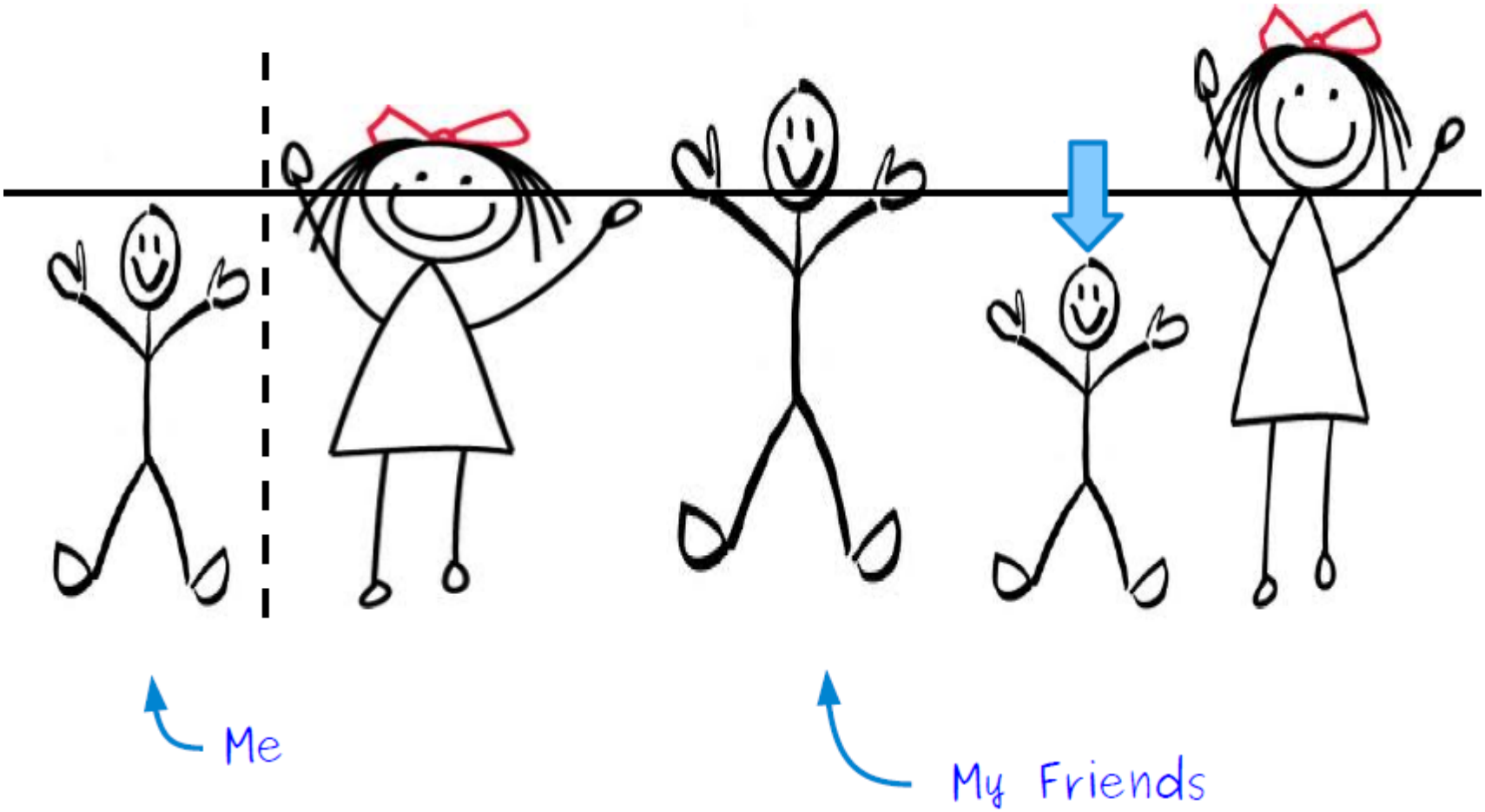
Proofs and Disproofs

- A proof is an argument establishing why a statement is true.
- A ***disproof*** is an argument establishing why a statement is *false*.
- Although proofs generally are more famous than disproofs, mathematics heavily relies on disproofs of conjectures that have turned out to be false.

Writing a Disproof

- The easiest way to disprove a statement is to write a proof of the opposite of that statement.
  - The opposite of a statement X is called the ***negation*** of statement X.
- A typical disproof is structured as follows:
  - Start by stating that you're going to disprove some statement X.
  - Write out the negation of statement X.
  - Write a normal proof that statement X is false.

“All My Friends Are Taller Than Me”



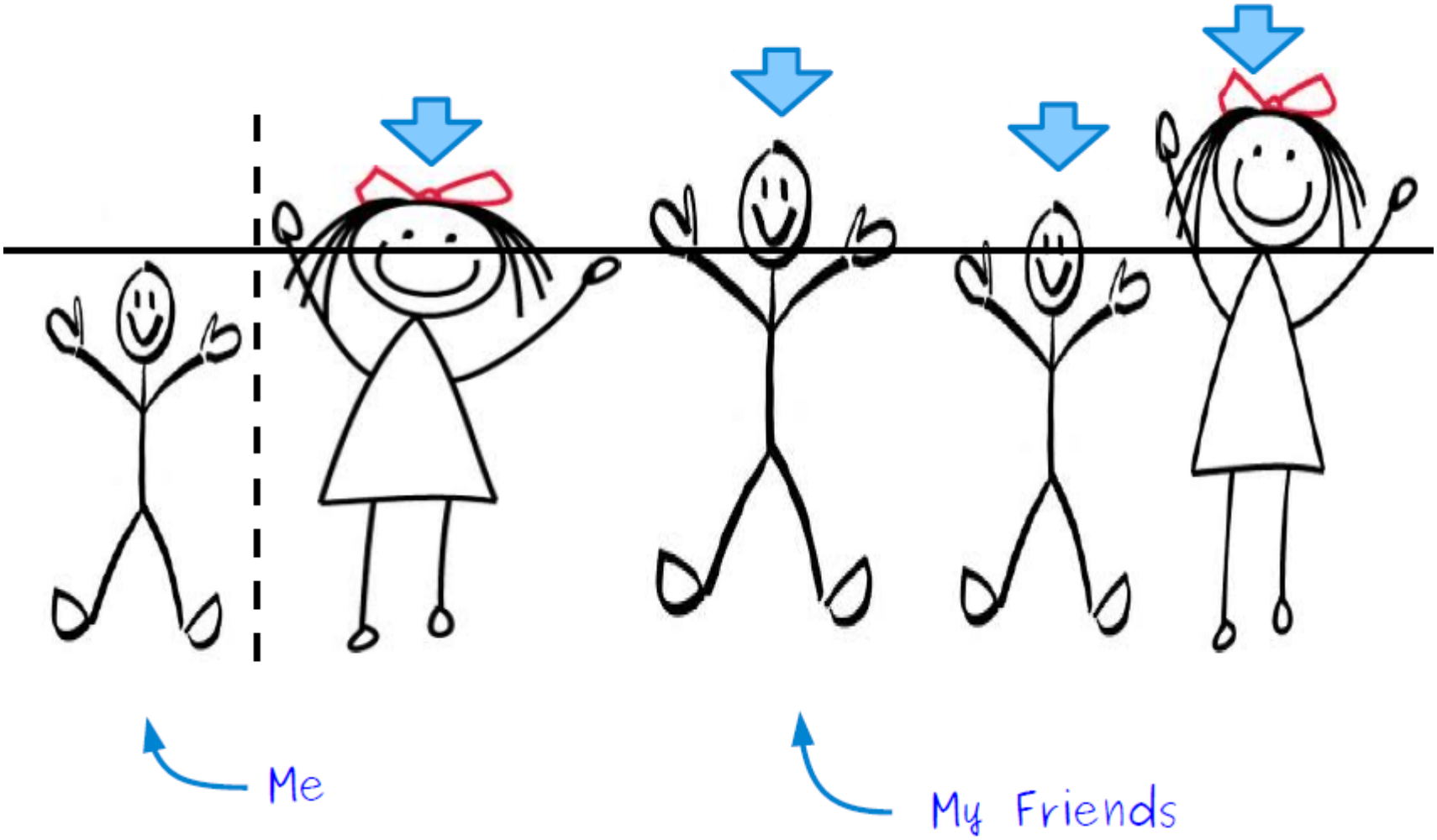
The negation of the *universal* statement

For all x, $P(x)$ is true.

is the *existential* statement

There exists an x where $P(x)$ is false.

“Some Friend Is Shorter Than Me”



The negation of the *existential* statement

There exists an x where $P(x)$ is true.

is the *universal* statement

For all x, $P(x)$ is false.

What would we have to show to disprove the following statement?

"Some set is the same size as its power set."

First, is this an existential statement or a universal statement?

"Some set is the same size as its power set."

First, is this an existential statement or a universal statement?

"Some set is the same size as its power set."

First, is this an existential statement or a universal statement?

"There is a set S where S is the same size as its power set."

What happens when you negate an existential statement?

"There is a set S where S is the same size as its power set."

What happens when you negate an existential statement?

"For any set S, the set S is ***not*** the same size as its power set."

This is what we need to prove
to disprove the original statement.

"For any set S, the set S is ***not*** the same size as its power set."

Proof by Contrapositive

Proofs by contraposition of $p \rightarrow q$ make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$.

The Contrapositive

- The ***contrapositive*** of the implication "If P, then Q" is the implication "If ***not*** Q, then ***not*** P."
- For example:
  - "If I store the cat food inside, then the raccoons will not steal my cat food."
  - Contrapositive: "If the raccoons stole my cat food, then I didn't store it inside."
- Another example:
  - "If Harry had opened the right book, then Harry would have learned about Gillyweed."
  - Contrapositive: "If Harry didn't learn about Gillyweed, then Harry didn't open the right book."

To prove the statement

If P is true, then Q is true

You may instead prove the statement

If Q is false, then P is false.

This is called a ***proof by contrapositive***.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

We're starting this proof by telling the reader that it's a proof by contrapositive. This helps cue the reader into what's about to come next.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Here, we're explicitly writing out the contrapositive. This tells the reader what we're going to prove. It also acts as a sanity check by forcing us to write out what we think the contrapositive is.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

We've said that we're going to prove this new implication, so let's go do it! The rest of this proof will look a lot like a standard direct proof.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

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

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

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

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. Therefore, n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. Therefore, n^2 is odd. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. Therefore, n^2 is odd. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that
$n = 2$
and s

From
(nam
There

The general pattern here is the following:

1. Start by announcing that we're going to use a proof by contrapositive so that the reader knows what to expect.

2. Explicitly state the contrapositive of what we want to prove.

3. Go prove the contrapositive.

Biconditionals

- Combined with what we saw
  we have proven that, if n is an integer:

  If n is even, then n^2 is even.

  If n^2 is even, then n is even.

- Therefore, if n is an integer:

  n is even if and only if n^2 is even.

- "If and only if" is often abbreviated **iff**:

  n is even iff n^2 is even.

- This is called a **biconditional**.

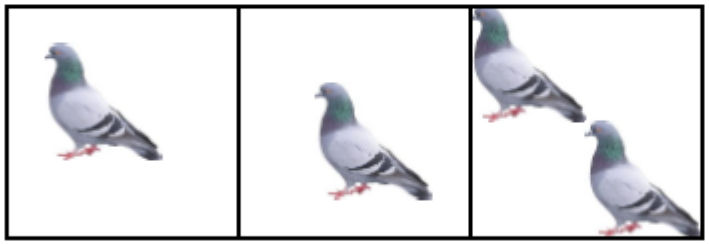
Proving Biconditionals

- To prove ***P* iff *Q***, you need to prove that P implies Q and that Q implies P.
- You can any proof techniques you'd like to show each of these statements.
  - In our case, we used a direct proof and a proof by contrapositive.

The Pigeonhole Principle

The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have $m > n$ pigeons.
- If you put the pigeons into the pigeonholes, some pigeonhole will have more than one pigeon in it.



The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.
- What is the contrapositive of this statement?

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.
- What is the contrapositive of this statement?

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

  If "some bin contains at least two objects" is false, then "$m > n$" is false.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then "$m > n$" is false.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

  If "some bin contains at least two objects" is false, then $m \leq n$.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

Is this a universal statement or an existential statement?

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

How do you take the negation of an existential statement?

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If every bin contains at most one object,
then $m \leq n$.

How do you take the negation of an existential statement?

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

  If every bin contains at most one object, then $m \leq n$.

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.
- What is the contrapositive of this statement?

  If every bin contains at most one object, then $m \leq n$.

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.
- What is the contrapositive of this statement?

  If every bin contains at most one object, then $m \leq n$.
- Look at the definitions of m and n. Does this make sense?

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains at least two objects.

Proof: By contrapositive; we prove that if every bin contains at most one object, then $m \leq n$.

Let x_i denote the number of objects in bin i. Since m is the number of total objects, we see that

$$m = x_1 + x_2 + \ldots + x_n.$$

We're assuming every bin has at most one object. In our notation, this means that $x_i \leq 1$ for all i. Using this inequalities, we get the following:

$$\begin{aligned} m &= x_1 + x_2 + \ldots + x_n \\ &\leq 1 + 1 + \ldots + 1 \qquad (n \textit{ times}) \\ &= n. \end{aligned}$$

So $m \leq n$, as required. ■

Some Simple Applications

- Any group of 367 people must have a pair of people that share a birthday.
  - 366 possible birthdays (pigeonholes)
  - 367 people (pigeons)
- Two people in San Francisco have the exact same number of hairs on their head.
  - Maximum number of hairs ever found on a human head is no greater than 500,000.
  - There are over 800,000 people in San Francisco.
- Each day, two people in New York City drink the same amount of water, to the thousandth of a fluid ounce.
  - No one can drink more than 50 gallons of water each day.
  - That's 6,400 fluid ounces. This gives 6,400,000 possible numbers of thousands of fluid ounces.
  - There are about 8,000,000 people in New York City proper.

Proving a statement P

Proof by Contradiction

Proofs by contradiction of p make use of the fact that

$(-p \rightarrow F) \rightarrow P$ is a tautology.

Therefore,

it is sufficient to prove $-p \rightarrow F$.

Proof by Contradiction

- A **proof by contradiction** is a proof that works as follows:
  - To prove that P is true, assume that P is *not* true.
  - Based on the assumption that P is not true, conclude something impossible.
  - Assuming the logic is sound, the only valid explanation is that the original assumption must have been wrong.
  - Therefore, P can't be false, so it must be true.

Theorem: No integer is both even and odd.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Because r and s are integers, their difference must also be an integer.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \frac{1}{2}$, which is not an integer.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \frac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \frac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \frac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \tfrac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Rational and Irrational Numbers

Rational and Irrational Numbers

- A number r is called a ***rational number*** if it can be written as

$$r = \frac{p}{q}$$

  where p and q are integers and $q \neq 0$.
- A number that is not rational is called ***irrational***.
- Useful theorem: If r is rational, r can be written as p / q where $q \neq 0$ and where p and q have no common factors other than ± 1.

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

Theorem: $\sqrt{2}$ is irrational.
Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

These floating numbers are labels on equations. We can use them to more easily refer to equations in the body of the proof.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$p^2 = 2q^2$$

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$p^2 = 2q^2$$
$$(2k)^2 = 2q^2$$

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$p^2 = 2q^2$$
$$(2k)^2 = 2q^2$$
$$4k^2 = 2q^2$$

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong. Therefore, $\sqrt{2}$ is irrational.

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

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong. Therefore, $\sqrt{2}$ is irrational. ■

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

Proof: **Assume for the sake of contradiction that $\sqrt{2}$ is rational.** This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides

The three key pieces:

1. State that the proof is by contradiction.
2. State what you are assuming is the negation of the statement to prove.
3. State you have reached a contradiction and what the contradiction entails.

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. **But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.**

We have reached a contradiction, so our original assumption must have been wrong. Therefore, $\sqrt{2}$ is irrational. ■

Proving Implications

- To prove the implication

  “If P is true, then Q is true.”

- you can use these three techniques:
  - **Direct Proof.**
    - Assume P and prove Q.
  - **Proof by Contrapositive**
    - Assume not Q and prove not P.
  - **Proof by Contradiction**
    - ... what does this look like?

Negating Implications

- To prove the statement

  "If P is true, then Q is true"

  by contradiction, we do the following:

  - Assume this statement is false.
  - Derive a contradiction.
  - Conclude that the statement is true.
- What is the negation of this statement?

  "P is true and Q is false"

Contradictions and Implications

- To prove the statement

  "If *P* is true, then *Q* is true"

  using a proof by contradiction, do the following:

  - Assume that P is true and that Q is false.
  - Derive a contradiction.
  - Conclude that if P is true, Q must be as well.

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

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

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

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \qquad (2) \end{aligned}$$

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect.

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well.

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

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

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

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

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

The three key pieces:

1. State that the proof is by contradiction.
2. State what the negation of the original statement is.
3. State you have reached a contradiction and what the contradiction entails.

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■