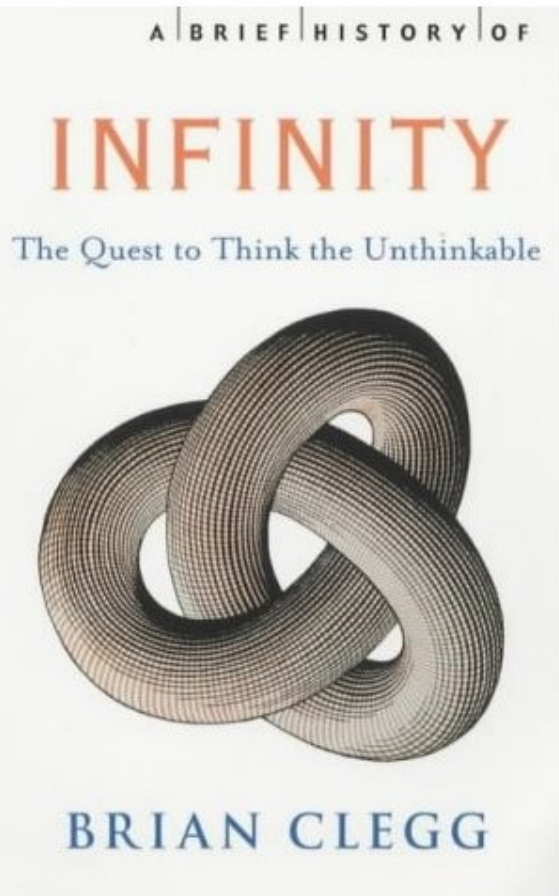
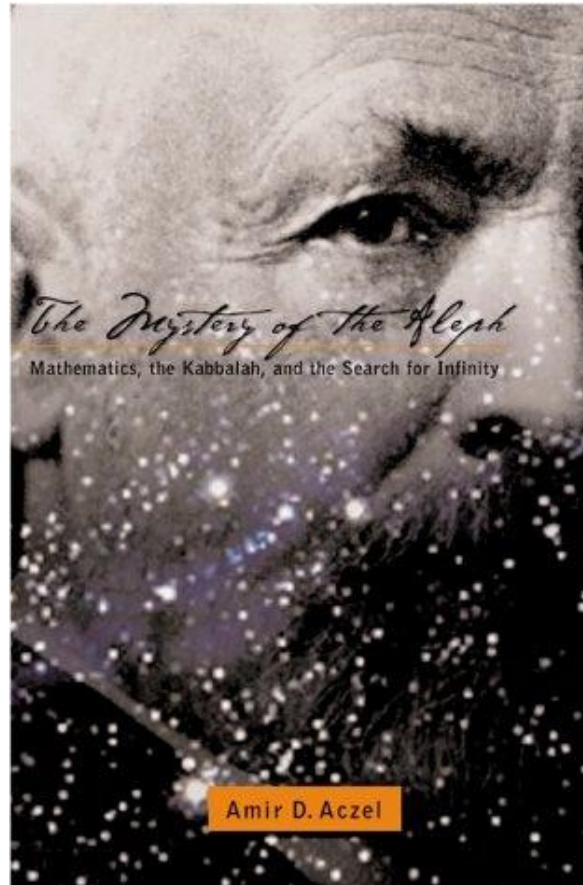


Direct Proofs

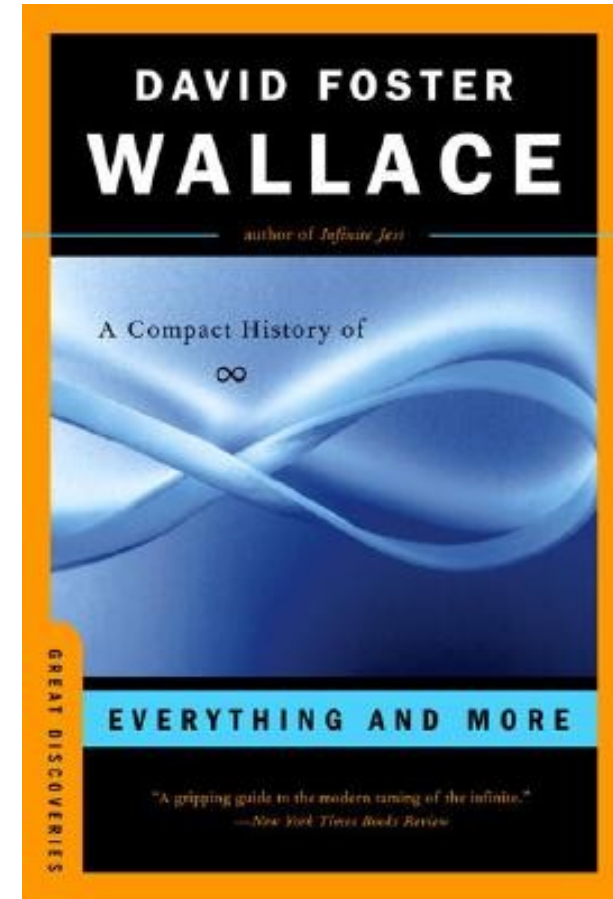
Recommended Reading



A Brief History of Infinity



The Mystery of the Aleph



Everything and More

What is a Proof?

Induction and Deduction

- In the sciences, much reasoning is done **inductively**.
 - Conduct a series of experiments and find a rule that explains all the results.
 - Conclude that there is a general principle explaining the results.
 - Even if all data are correct, the conclusion might be incorrect.
- In mathematics, reasoning is done **deductively**.
 - Begin with a series of statements assumed to be true.
 - Apply logical reasoning to show that some conclusion necessarily follows.
 - If all the starting assumptions are correct, the conclusion necessarily must be correct.

Structure of a Mathematical Proof

- Begin with a set of initial assumptions called **hypotheses**.
- Apply logical reasoning to derive the final result (the **conclusion**) from the hypotheses.
- Assuming that all intermediary steps are sound logical reasoning, the conclusion follows from the hypotheses.

Direct Proofs

Direct Proofs

- A **direct proof** is the simplest type of proof.
- Starting with an initial set of hypotheses, apply simple logical steps to prove the conclusion.
 - *Directly* proving that the result is true.
- Contrasts with **indirect proofs**, which we'll see on Friday.

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.

A Simple Direct Proof

Theorem: If n is even, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof


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

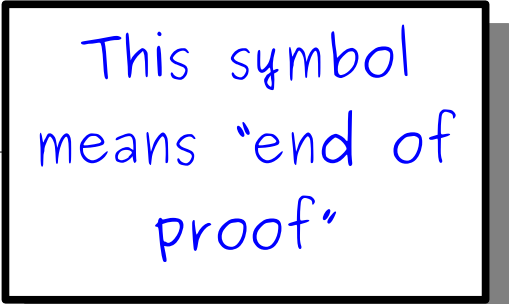
Proof: Let n be an even integer.

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

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

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. 



This symbol means "end of proof"

A Simple Direct Proof

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

Proof: Let n be an even integer.

Since
such

To prove a statement of the
form

for k

This

“If P , then Q ”

$2(2k^2)$.

Since
the

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

that
 2) such

that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, 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

Since $2k$
there is
that $n^2 =$

Thus n^2 is even. ■

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

ch

A Simple Direct Proof

Theorem: If n is even, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, there is an integer m such that $n^2 = 2m$.

Thus n^2 is even.

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.

uch

A Simple Direct Proof

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

Proof: Let n be an even integer.

Since n is even,
such that

This means

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.

n^2).

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2(2k^2)$ is even, there is some integer m such that $n^2 = 2m$.
Hey, that's what we were trying to show! We're done now.

Thus n^2 is even. ■

Another Direct Proof

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

Another Direct Proof

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

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 , $P(X)$ is true.

- Examples:

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

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

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

- How do we prove these statements when there are 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 .
- Conclude that since the choice of x was arbitrary, $P(x)$ must hold true for all choices of x .

Another Direct Proof

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

Another Direct Proof

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

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

Another Direct Proof

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

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

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

Another Direct Proof

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

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

To prove a statement of the form

“If P , then Q ”

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

Another Direct Proof

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

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

By definition, since $A \subseteq B$, every $x \in A$ also satisfies $x \in B$.

By definition, since $B \subseteq C$, every $x \in B$ also satisfies $x \in C$.

Consequently, any $x \in A$ satisfies $x \in C$.

Thus $A \subseteq C$. ■

An Incorrect Proof

Theorem: For any integer n , if n is even, n has no odd divisors.

Proof: Consider an arbitrary even natural number, say, 16. 16 is even, and it has no odd divisors. Since our choice was arbitrary, for any arbitrary n , if n is even, n has no odd divisors. ■

An Incorrect Proof

Theorem: For any integer n , if n is even, n has no odd divisors.

Proof: Consider an arbitrary even natural number, say, 16. 16 is even, and it has no odd divisors. Since our choice was arbitrary, for any arbitrary n , if n is even, n has no odd divisors. ■

ar·bi·trar·y

adjective /'ärbi,trerē/

Not this
one!

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Use this
definition

To prove something is true for all x , **do not** choose an x and base the proof off of your choice!

Instead, leave x unspecified and show that no matter what x is, the specified property must hold.

Another Incorrect Proof

Theorem: For any sets A and B , $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well.

Consider any arbitrary $x \in A \cap B$. This means that $x \in A$ and $x \in B$, so $x \in A$ as required. ■

Another Incorrect Proof

Theorem: For any sets A and B , $A \subseteq A \cap B$.

Proof: We need to show that **if $x \in A$, then $x \in A \cap B$ as well.**

Consider any arbitrary $x \in A \cap B$. This means that $x \in A$ and $x \in B$, so $x \in A$ as required. ■

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 .

This is a fundamentally different type of proof that what we've done before. Instead of showing that every object has some property, we want to show that some 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.
- 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 .

Proof: Take $n = 3$.

There are three natural numbers smaller than 3: 0, 1, and 2.

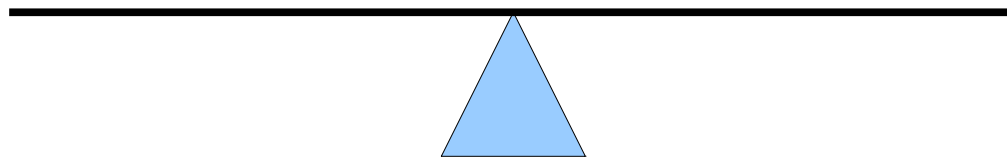
We have $0 + 1 + 2 = 3$.

Thus 3 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.



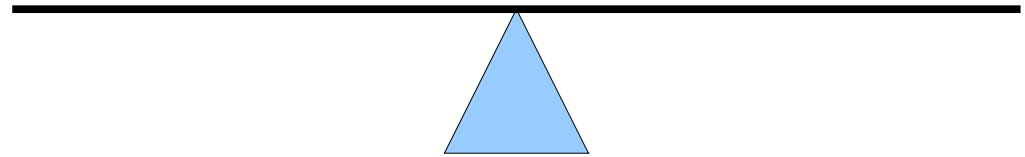
Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

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.

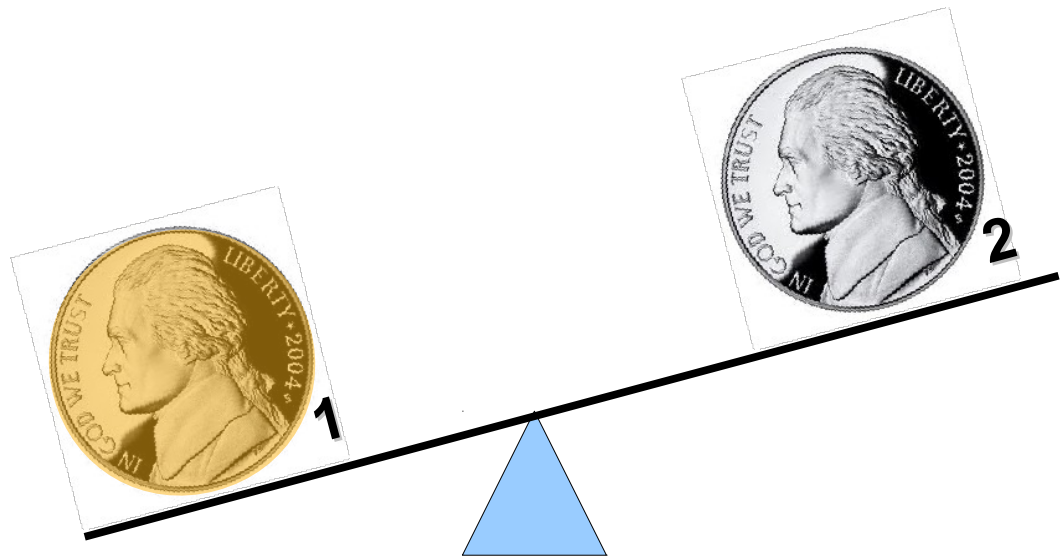
This is an existential statement.

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

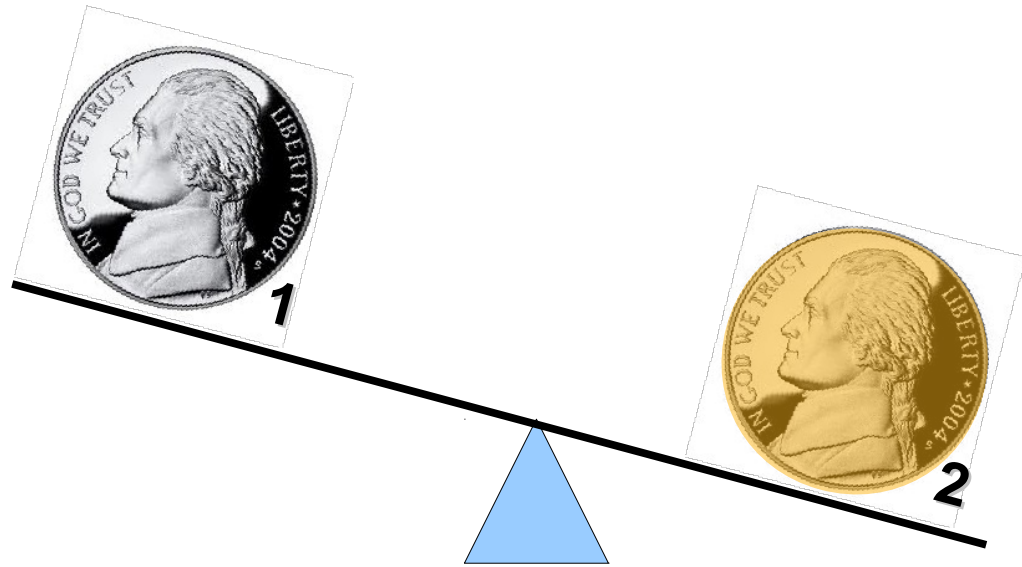
Finding the Counterfeit Coin



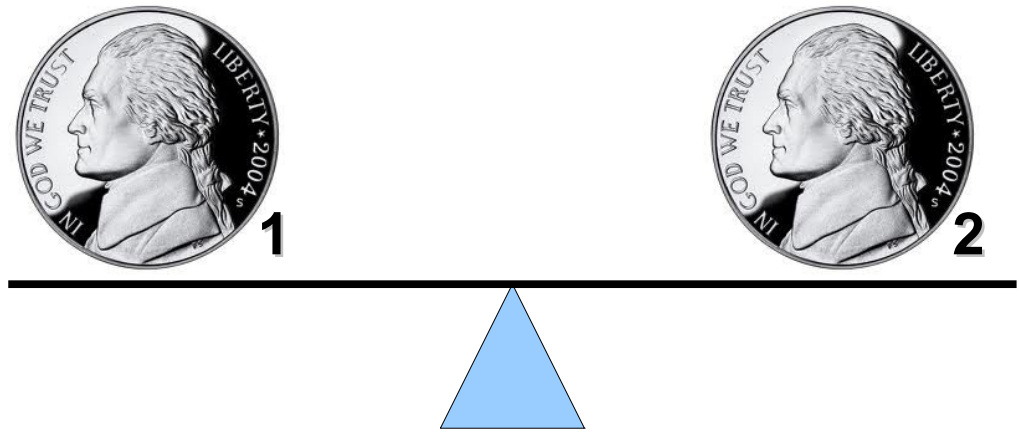
Finding the Counterfeit Coin



Finding the Counterfeit Coin



Finding the Counterfeit Coin



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 heavier 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 heavier 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 heavier 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 heavier than coin A. Then coin B is counterfeit.

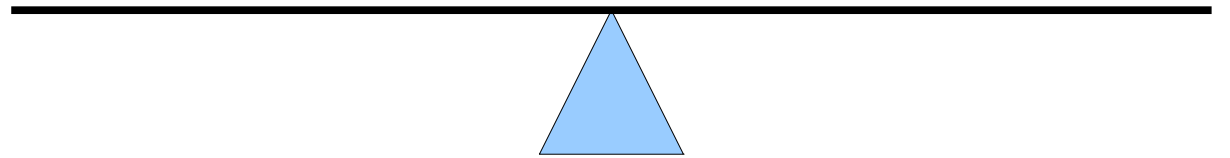
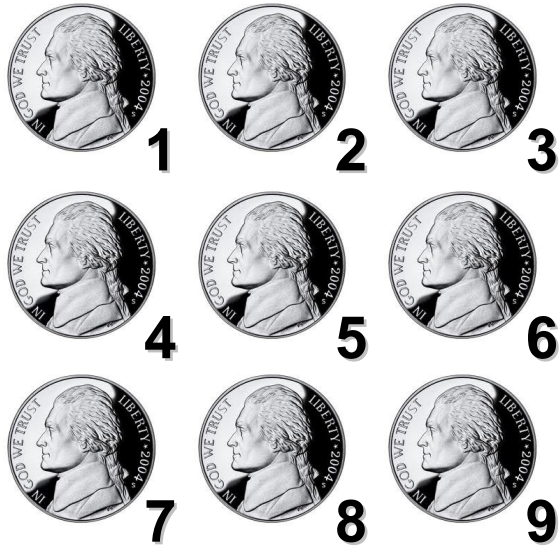
Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

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

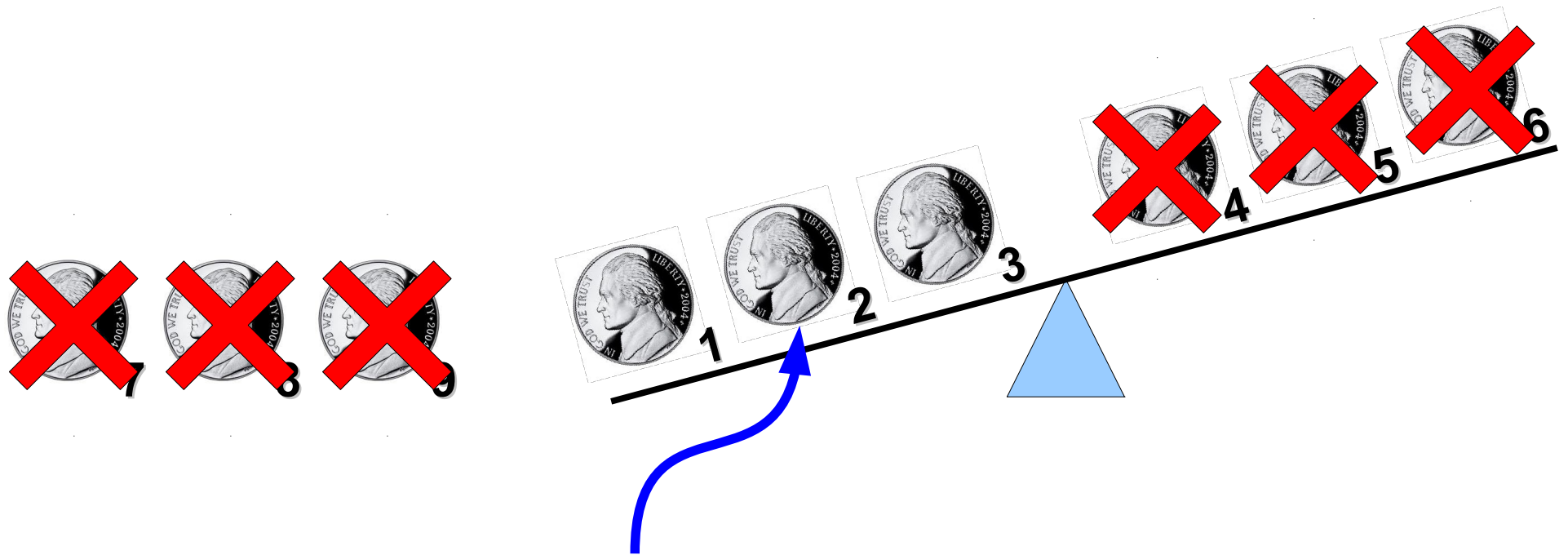
A Harder Problem

- 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

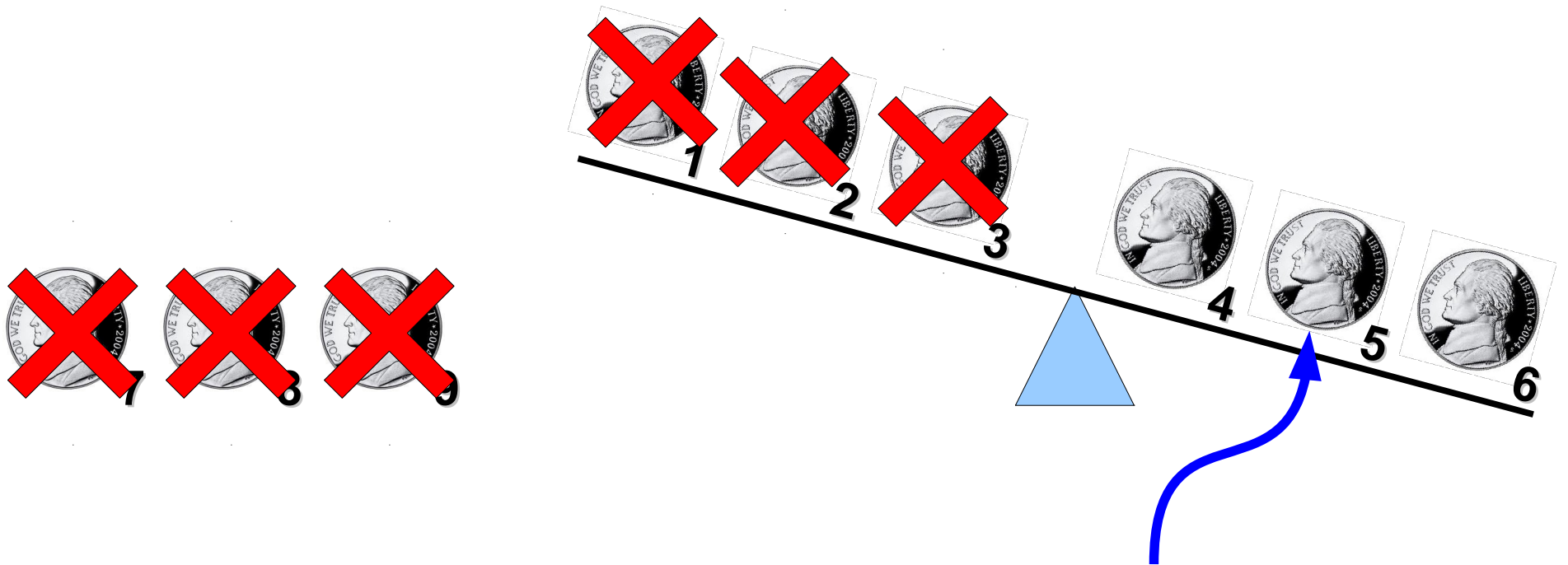


Finding the Counterfeit Coin



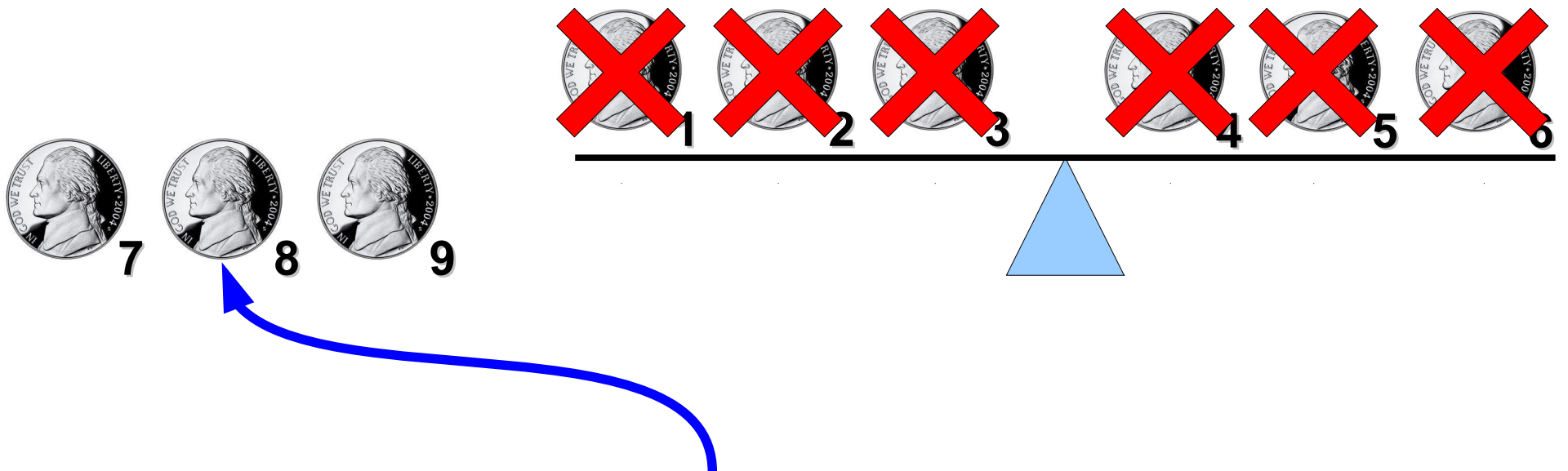
Now we have one weighing to find the counterfeit out of these three.

Finding the Counterfeit Coin



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

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.

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. 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 $A = B$.

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 $x \in A$, $x \in B$.

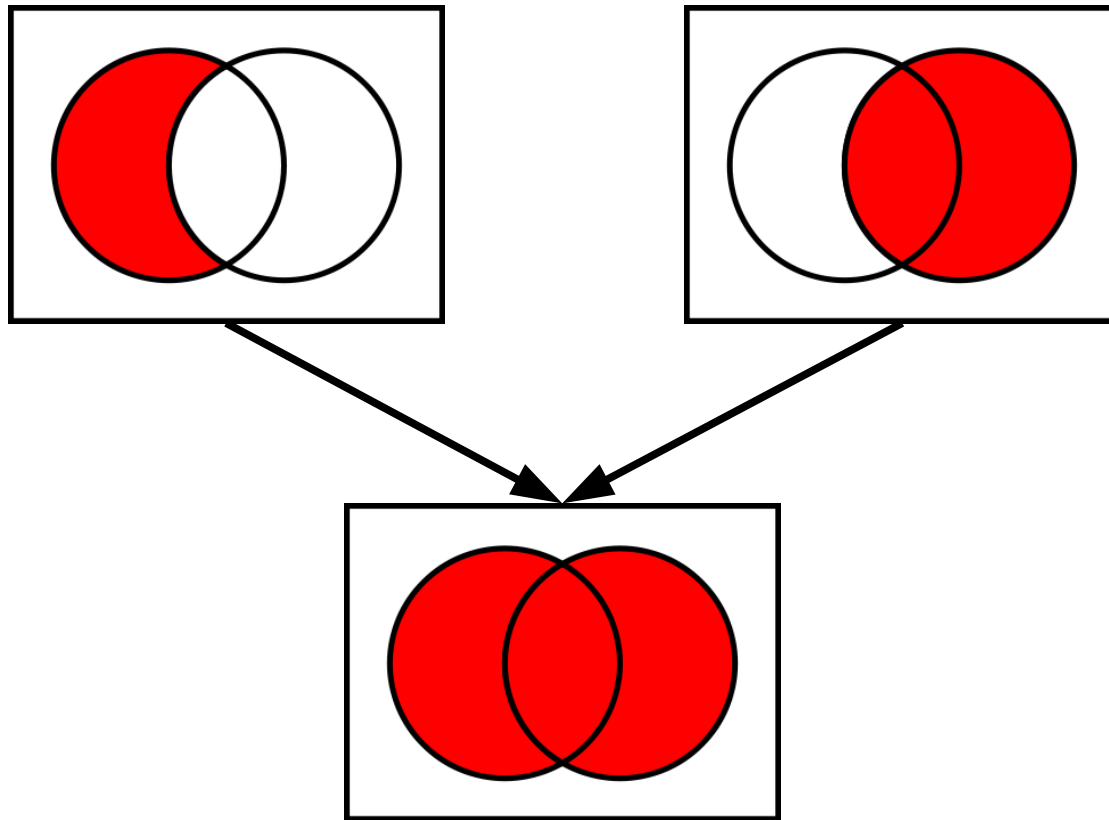
By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

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 $(A - B) \cup B = A \cup B$.
- Proof idea: Show that each set is a subset of the other.

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

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 , $A \cup B \subseteq (A - B) \cup B$.

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,
 $(A - B) \cup B = A \cup B$. ■

Next Time

- Indirect Proofs
 - Proof by contradiction.
 - Proof by contrapositive.