Mathematical Induction

Everybody – do the wave!

The Wave

- If done properly, everyone will eventually end up joining in.
- Why is that?
  - Someone (me!) started everyone off.
  - Once the person before you did the wave, you did the wave.

Let P be some property. The ***principle of mathematical induction*** states that if

If it starts true…

P is true for 0

…and it stays true…

and

For any $k \in \mathbb{N}$, if P is true for k, then P is true for $k + 1$

then

P is true for every $n \in \mathbb{N}$.

…then it's always true.

Induction, Intuitively

- It's true for 0.
- Since it's true for 0, it's true for 1.
- Since it's true for 1, it's true for 2.
- Since it's true for 2, it's true for 3.
- Since it's true for 3, it's true for 4.
- Since it's true for 4, it's true for 5.
- Since it's true for 5, it's true for 6.
- …

Proof by Induction

- A ***proof by induction*** is a way to use mathematical induction to show that some result is true for all natural numbers n.
- In a proof by induction, there are three steps:
  - Prove that P is true for 0.
    - This is called the ***basis*** or the ***base case***.
  - Prove that if P is true for some arbitrary natural number k, then P must also be true for $k+1$.
    - This is called the ***inductive step***.
    - The assumption that P is true for k is called the ***inductive hypothesis***.
  - Conclude, by induction, that P is true for all natural numbers n.

Some Summations

$$2^0 = 1 \quad = 2^1 - 1$$

$$2^0 + 2^1 = 1 + 2 = 3 = 2^2 - 1$$

$$2^0 + 2^1 + 2^2 = 1 + 2 + 4 = 7 = 2^3 - 1$$

$$2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = 15 = 2^4 - 1$$

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 1 + 2 + 4 + 8 + 16 = 31 = 2^5 - 1$$

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

At the start of the proof, we tell the reader what property we're going to show is true for all natural numbers n, then tell them we're going to prove it by induction.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

In a proof by induction, we need to prove that

- ☐ $P(0)$ is true
- ☐ If $P(k)$ is true, then $P(k+1)$ is true.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero powers of two is $2^0 - 1$.

Here, we state what $P(0)$ actually says. Now, can go prove this using any proof techniques we'd like!

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero powers of two is $2^0 - 1$. Since the sum of the first zero powers of two is zero and $2^0 - 1$ is zero as well, we see that $P(0)$ is true.

In a proof by induction, we need to prove that

✓ $P(0)$ is true

☐ If $P(k)$ is true, then $P(k+1)$ is true.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero powers of two is $2^0 - 1$. Since the sum of the first zero powers of two is zero and $2^0 - 1$ is zero as well, we see that $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k - 1. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is $2^{k+1} - 1$.

The goal of this step is to prove

"If $P(k)$ is true, then $P(k+1)$ is true."

To do this, we'll choose an arbitrary k, assume that $P(k)$ is true, then try to prove $P(k+1)$.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero powers of two is $2^0 - 1$. Since the sum of the first zero powers of two is zero and $2^0 - 1$ is zero as well, we see that $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k - 1. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is $2^{k+1} - 1$.

Here, we explicitly stating $P(k+1)$, which is what we want to prove. Now, we can use any proof technique we want to try to prove it.

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true fo … s.

For ou … meaning that th … 1. Since the su … d $2^0 - 1$ is zero …

Here, we use our inductive hypothesis (the assumption that $P(k)$ is true) to simplify a complex expression. This is a common theme in inductive proofs.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k - 1. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is $2^{k+1} - 1$. To see this, notice that

$$2^0 + 2^1 + \ldots + 2^{k-1} + 2^k = (2^0 + 2^1 + \ldots + 2^{k-1}) + 2^k$$

Theorem: The sum of the first n powers of two is $2^n - 1$.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is $2^n - 1$." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero powers of two is $2^0 - 1$. Since the sum of the first zero powers of two is zero and $2^0 - 1$ is zero as well, we see that $P(0)$ is true.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k - 1. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is $2^{k+1} - 1$. To see this, notice that

$$\begin{aligned} 2^0 + 2^1 + \ldots + 2^{k-1} + 2^k &= (2^0 + 2^1 + \ldots + 2^{k-1}) + 2^k \\ &= 2^k - 1 + 2^k \qquad \textit{(via (1))} \\ &= 2(2^k) - 1 \\ &= 2^{k+1} - 1. \end{aligned}$$

Therefore, $P(k + 1)$ is true, completing the induction. ■

A Quick Aside

- This result helps explain the range of numbers that can be stored in an **`int`**.
- If you have an unsigned 32-bit integer, the largest value you can store is given by $1 + 2 + 4 + 8 + \ldots + 2^{31} = 2^{32} - 1$.
- This formula for sums of powers of two has many other uses as well. You'll see a few over the course of this quarter.

Structuring a Proof by Induction

- Define some property P that you'll show, by induction, is true for all natural numbers.
- Prove the base case:
  - State that you're going to prove the property holds for 0, then go prove it.
- Prove the inductive step:
  - Say that you're assuming P is true for some natural number k, then write out exactly what that means.
  - Say that you're going to prove P is true for $k+1$, then write out exactly what that means.
  - Prove that P is true for $k+1$ using any proof technique you'd like.
- This is a rather verbose way of writing inductive proofs. As we get more experience with induction, we'll start leaving out some details from our proofs.

Induction, Intuitively

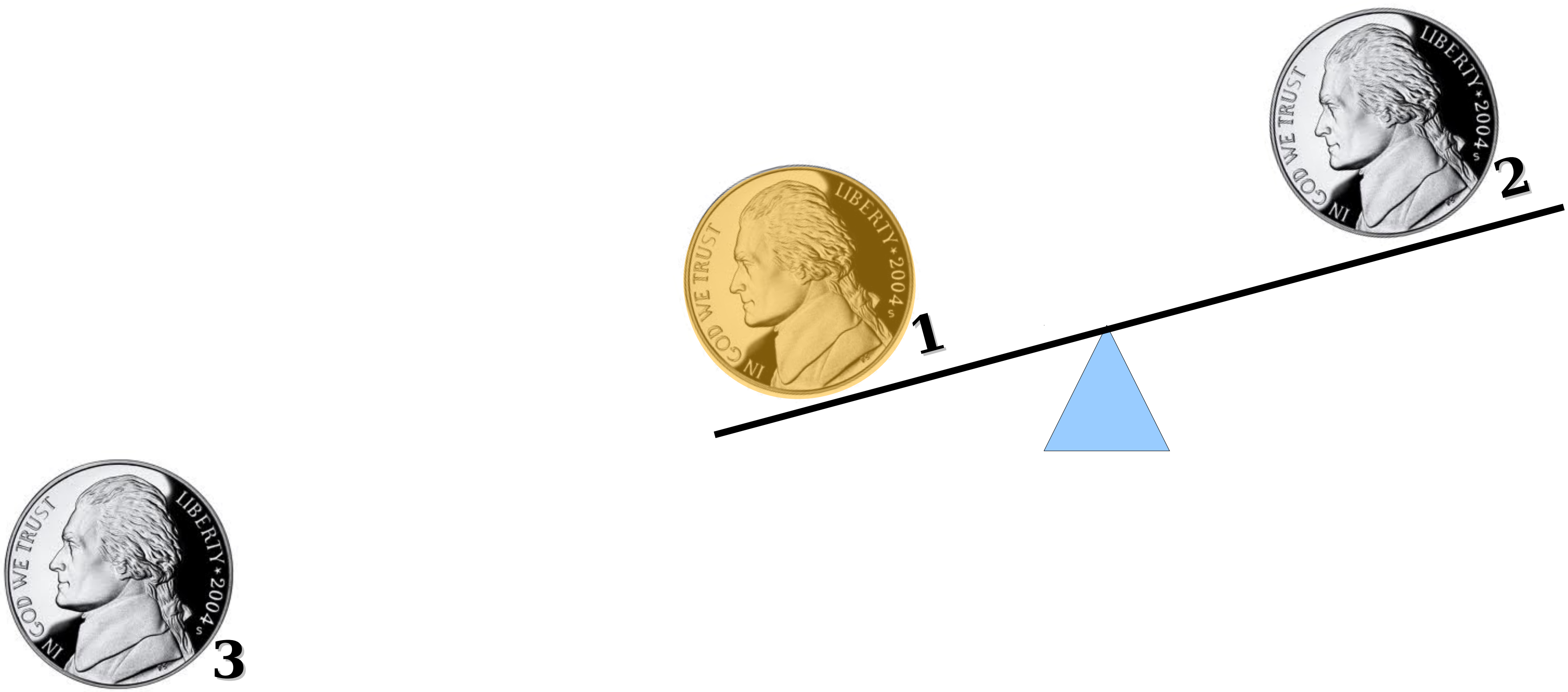
- You can imagine an “machine” that turns proofs that the property holds for k into proofs that the property holds for $k + 1$.
- Starting with a proof that the property holds for 0, we can run the machine as many times as we'd like to get proofs for 1, 2, 3, … .
- The principle of mathematical induction says that this style of reasoning is a rigorous argument.

The Counterfeit Coin Problem

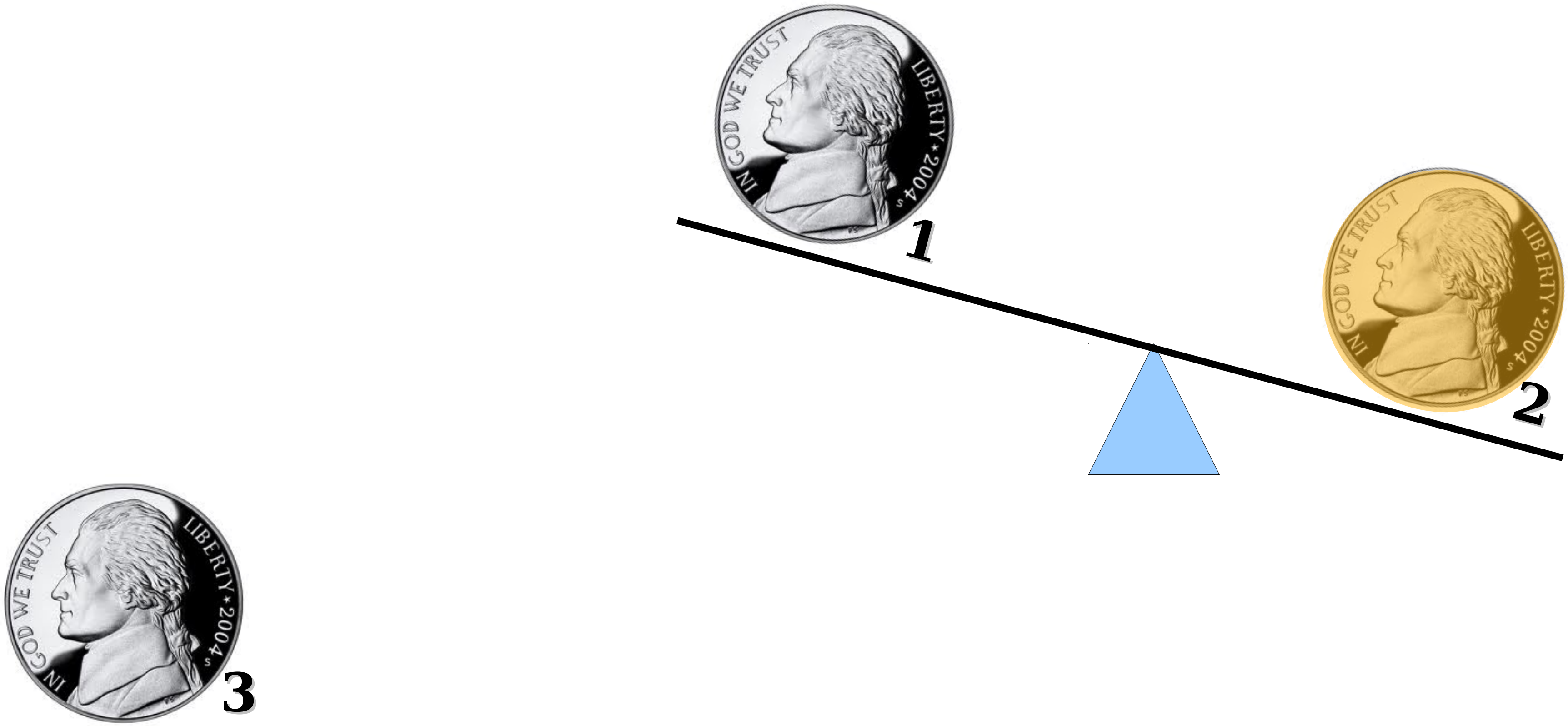
Problem Statement

- 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.

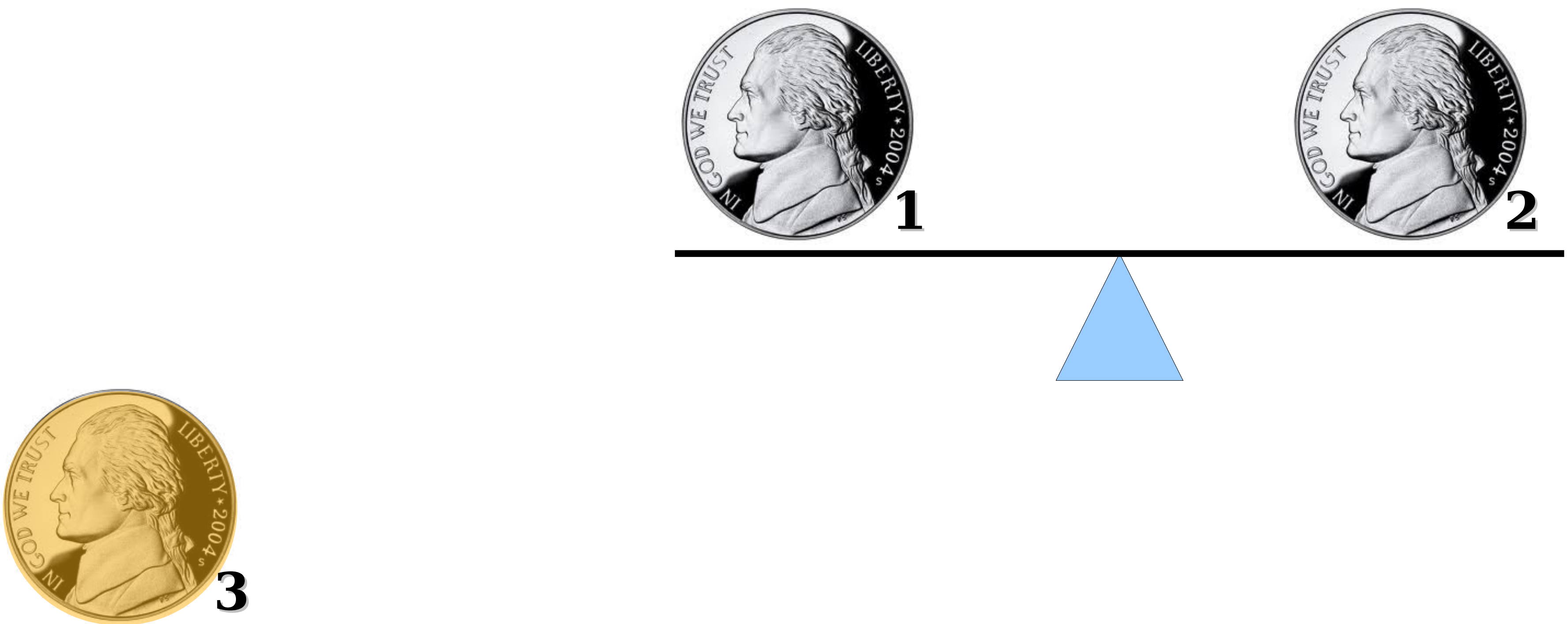
Finding the Counterfeit Coin



Finding the Counterfeit Coin



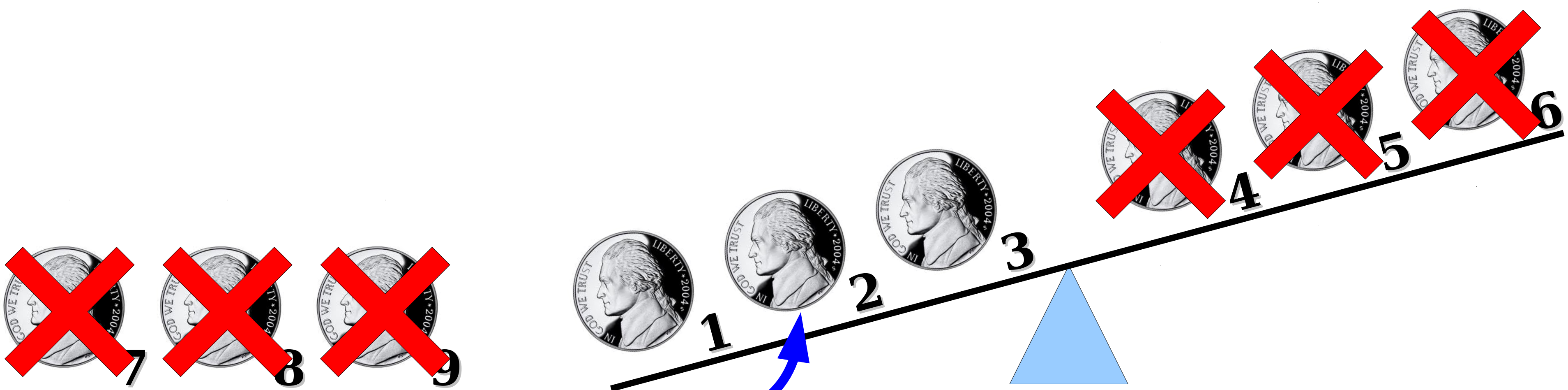
Finding the Counterfeit Coin



A Harder Problem

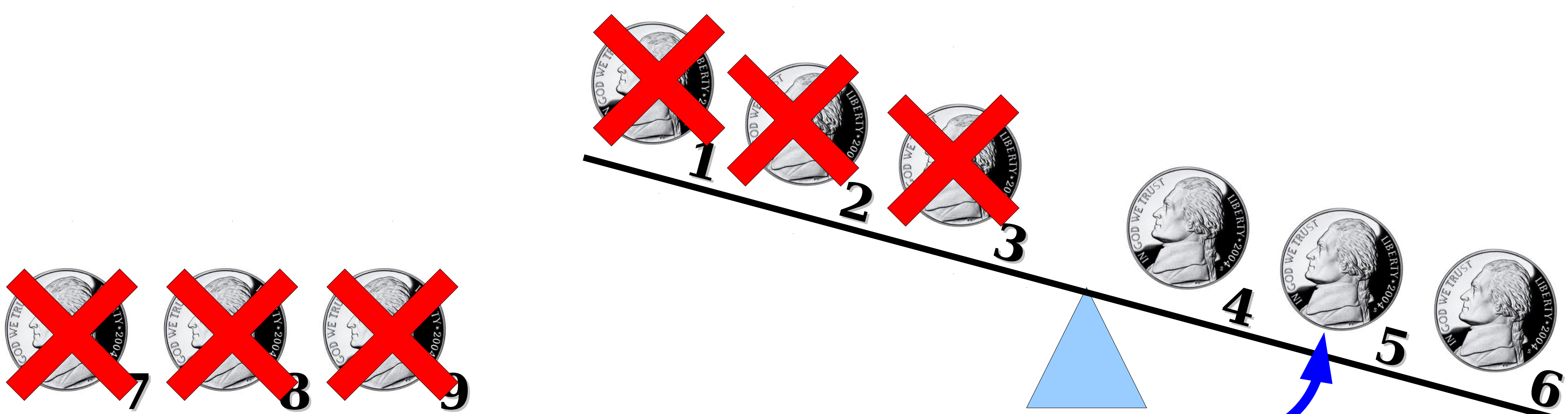
- You are given a set of ***nine*** seemingly identical coins, eight of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only ***two*** weighings on the balance, find the counterfeit coin.

Finding the Counterfeit Coin



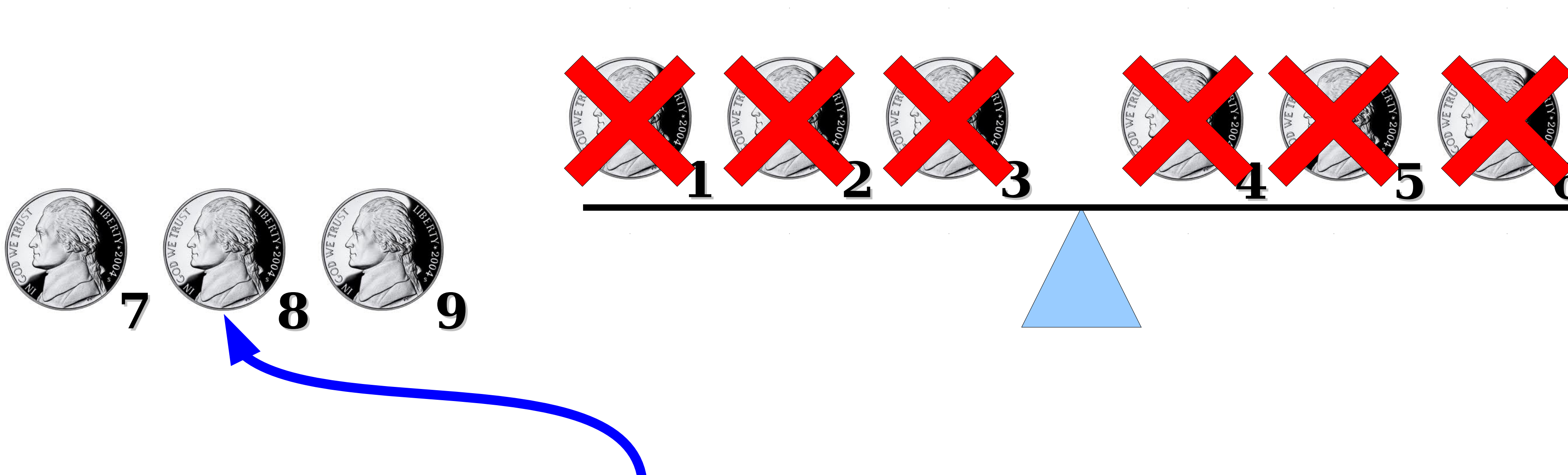
Now we have one weighing to find the counterfeit out of these three coins.

Finding the Counterfeit Coin



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

Finding the Counterfeit Coin



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

If we have n weighings on the scale, what is the largest number of coins out of which we can find the counterfeit?

A Pattern

- Assume out of the coins that are given, exactly one is counterfeit and weighs more than the other coins.
- If we have no weighings, how many coins can we have while still being able to find the counterfeit?
  - **One coin**, since that coin has to be the counterfeit!
- If we have one weighing, we can find the counterfeit out of **three** coins.
- If we have two weighings, we can find the counterfeit out of **nine** coins.

So far, we have

$$\mathbf{1, 3, 9 = 3^0, 3^1, 3^2}$$

Does this pattern continue?

Theorem: If exactly one coin in a group of 3^n coins is heavier than the rest, that coin can be found using only n weighings on a balance.

Proof: Let $P(n)$ be the following statement:

> If exactly one coin in a group of 3^n coins is heavier than the rest, that coin can be found using only n weighings on a balance.

We'll use induction to prove that $P(n)$ holds for every $n \in \mathbb{N}$, from which the theorem follows.

As our base case, we'll prove that $P(0)$ is true, meaning that if we have a set of $3^0=1$ coins with one coin heavier than the rest, we can find that coin with zero weighings. This is true because if we have just one coin, it's vacuously heavier than all the others, and no weighings are needed.

For the inductive step, suppose that $P(k)$ is true for some $k \in \mathbb{N}$, so we can find the heavier of 3^k coins in k weighings. We'll prove $P(k+1)$: that we can find the heavier of 3^{k+1} coins in $k+1$ weighings.

Suppose we have 3^{k+1} coins with one heavier than the others. Split the coins into three groups of 3^k coins each. Weigh two of the groups against one another. If one group is heavier than the other, the coins in that group must contain the heavier coin. Otherwise, the heavier coin must be in the group we didn't put on the scale. Therefore, with one weighing, we can find a group of 3^k coins containing the heavy coin. We can then use k more weighings to find the heavy coin in that group.

We've given a way to use $k+1$ weighings and find the heavy coin out of a group of 3^{k+1} coins. Thus $P(k+1)$ is true, completing the induction. ■

Some Fun Problems

- Suppose that you have a group of coins where there's either exactly one heavier coin, or all coins weigh the same amount. If you only get k weighings, what's the largest number of coins where you can find the counterfeit or determine none exists?
- What happens if the counterfeit can be either heavier or lighter than the other coins? What's the maximum number of coins where you can find the counterfeit if you have k weighings?

Time-Out for Announcements!

Office Hours

- Office hours start today! A schedule is available online.
- Come with questions, leave with answers.
- You can also ask questions on Piazza or by emailing the staff list.

Problem Set Clarification

- All problem sets are designed to use only the material up to and include the lecture in which they are released.
- We'll explicitly mark any problems for which we won't have covered the requisite material.
- (In particular, you shouldn't need induction for any of the current problem set questions.)

Checkpoint Feedback

Alternate Exams

- We've slightly relaxed our alternate exam policy.
- We will be offering alternate midterm exams from 4PM – 7PM on the nights of the normal exams.
- We will not offer alternate final exam times.
- If you have documentation from the OAE, we will absolutely arrange for an alternate exam time.

Want to join WiCS Core?

Come to our informational meeting to learn about the different roles and the impact you could have in the CS community

We put on programs like HackOverflow, WiCS Industry Mentorship, eCSplore & more

WEDNESDAY, APRIL 8TH
7:30P @ GATES 219

+ snag some free WiCS swag!

WICS
STANFORD WOMEN IN COMPUTER SCIENCE

Board applications go live on wics.stanford.edu after the meeting!

Applications due Friday, April 17th @ 11:59p

CS + Social Good Mixer

- Interested in learning more about applying CS skills for social good? Stop by the CS + Social Good mixer.
- Thursday, 5:30PM – 7:00PM on the Gates Fifth Floor.
- RSVP at https://www.facebook.com/events/408560675991922/

Your Questions

"Since there are many ways to prove and disprove something, what is the best approach to choosing a particular technique? Is this an intuition we will gain in practice?"

Some of this is experience, but some of this is just having a bag of tricks to use. Try out one approach and see if it works. If so, great! If not, try something else. Usually, you'll find something that works.

"Do we need to prove basic math ideas if we're using them in the psets (for example, that a negative number times a positive number equals a negative number)?"

Good rule of thumb – assume your audience is another CS103 student. You can assume basic facts about numbers and results from high school algebra, since we'll assume everyone has seen them. If it's more complex than that, try proving it!

"Which area of CS do you believe does the most net good for humanity, and why?"

Tough question! I'm not sure about how to approach the "net" part. I'm going to go with biocomputation if you include "net" and artificial intelligence if you don't.

"What technology do you suggest for digitally writing these proofs? Latex? Sublime? Word?"

The "correct" answer I should give is LaTeX, since it's the standard typesetting system for academic mathematics. If you have the time to learn it, go for it! If not, use anything that works and doesn't have awful formatting.

Back to our regularly scheduled ~~programming~~...

math

How Not To Induct

Something's Wrong...

Theorem: The sum of the first n powers of two is 2^n.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is 2^n." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is 2^{k+1}. To see this, notice that

$$\begin{aligned} 2^0 + 2^1 + \ldots + 2^{k-1} + 2^k &= (2^0 + 2^1 + \ldots + 2^{k-1}) + 2^k \\ &= 2^k + 2^k \qquad \textit{(via (1))} \\ &= 2(2^k) \\ &= 2^{k+1}. \end{aligned}$$

Therefore, $P(k + 1)$ is true, completing the induction. ■

Something's Wrong...

Theorem: The sum of the first n powers of two is 2^n.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is 2^n." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is 2^{k+1}. To see this, notice that

$$\begin{aligned} 2^0 + 2^1 + \ldots + 2^{k-1} + 2^k &= (2^0 + 2^1 + \ldots \\ &= 2^k + 2^k \\ &= 2(2^k) \\ &= 2^{k+1}. \end{aligned}$$

Where did we prove the base case?

Therefore, $P(k + 1)$ is true, completing the induction. ■

When writing a proof by induction,

make sure to show the base case!

Otherwise, your argument is invalid!

Why did this work?

Theorem: The sum of the first n powers of two is 2^n.

Proof: Let $P(n)$ be the statement "the sum of the first n powers of two is 2^n." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

For the inductive step, assume that for some $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

$$2^0 + 2^1 + \ldots + 2^{k-1} = 2^k. \qquad (1)$$

We need to show that $P(k + 1)$ holds, meaning that the sum of the first $k + 1$ powers of two is 2^{k+1}. To see this, notice that

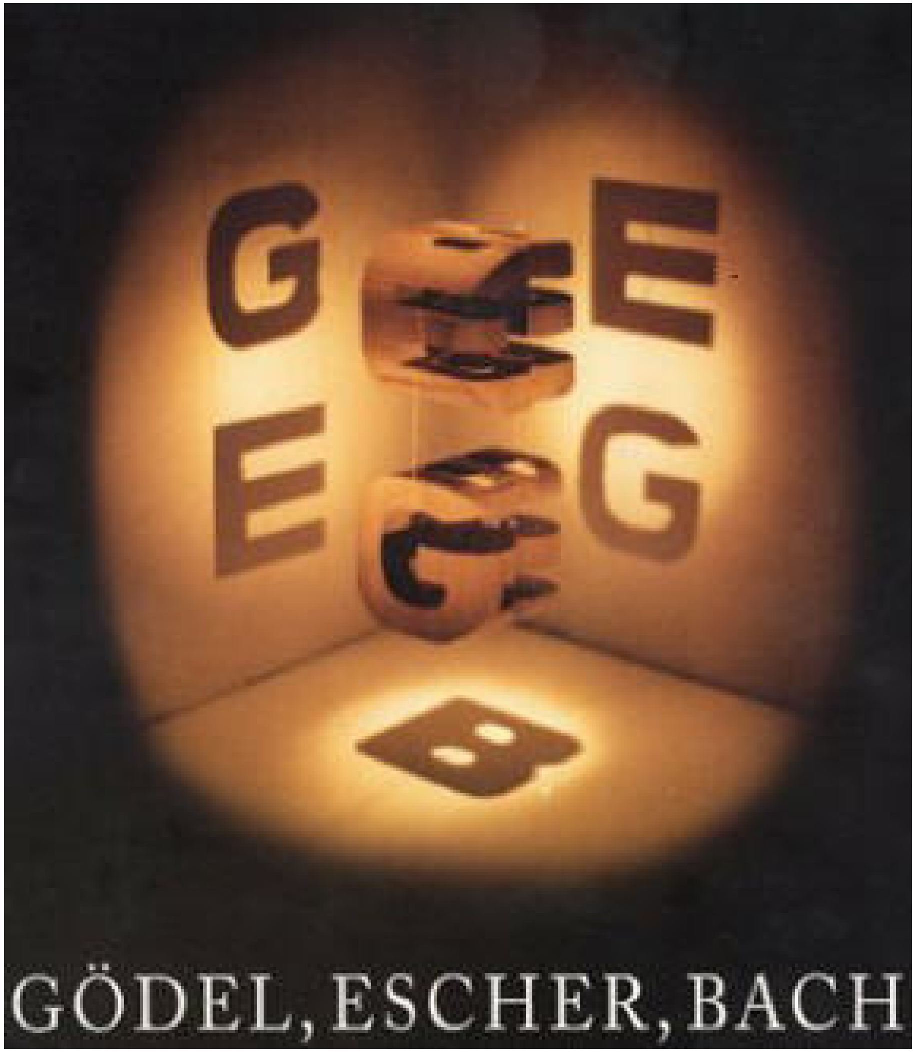
$$2^0 + 2^1 + \ldots + 2^{k-1} + 2^k = (2^0 + 2^1 + \ldots + 2^{k-1}) + 2^k$$

Therefore, $P(k + 1)$

You can prove **anything** from a faulty assumption. This is called the **principle of explosion.**

The **MU** Puzzle

Gödel, Escher Bach: An Eternal Golden Braid



- Pulitzer-Prize winning book exploring recursion, computability, and consciousness.
- Written by Douglas Hofstadter, cognitive scientist at Indiana University.
- A great (but dense!) read.

The `MU` Puzzle

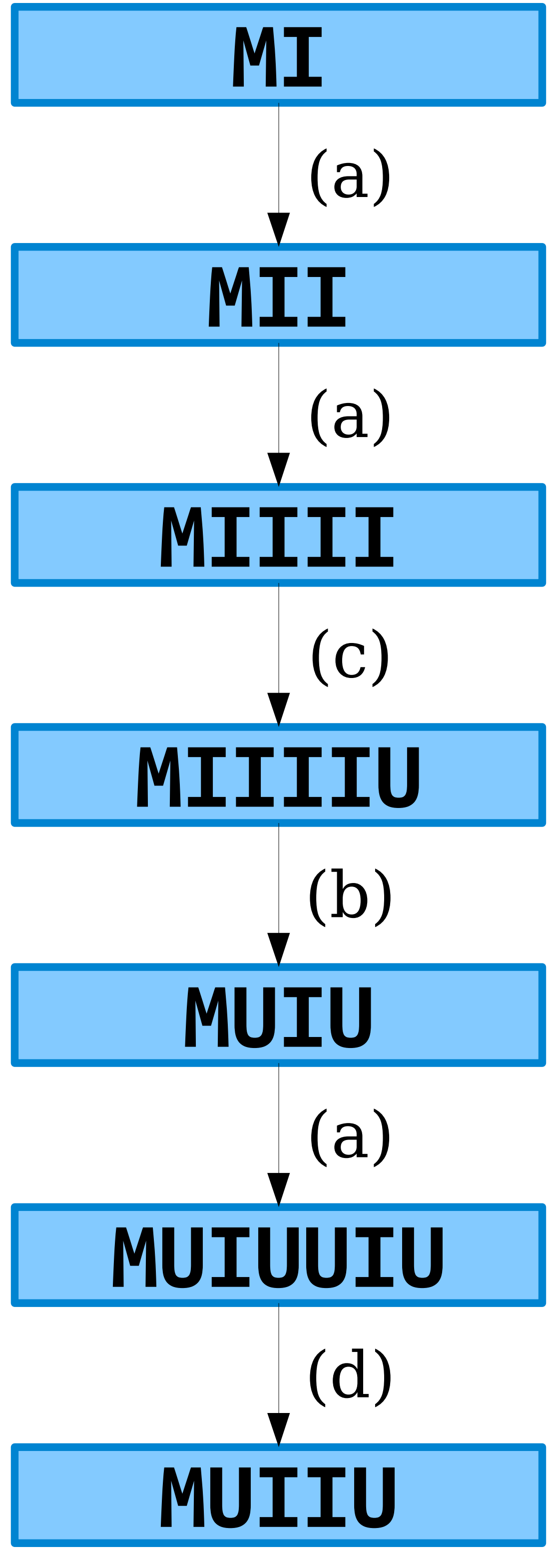
- Begin with the string `MI`.
- Repeatedly apply one of the following operations:
  - Double the contents of the string after the `M`: for example, `MIIU` becomes `MIIUIIU`, or `MI` becomes `MII`.
  - Replace `III` with `U`: `MIIII` becomes `MUI` or `MIU`.
  - Append `U` to the string if it ends in `I`: `MI` becomes `MIU`.
  - Remove any `UU`: `MUUU` becomes `MU`.
- ***Question***: How do you transform `MI` to `MU`?

(a) Double the string after an `M`.

(b) Replace `III` with `U`.

(c) Append `U`, if the string ends in `I`.

(d) Delete `UU` from the string.



Try It!

Starting with `MI`, apply these operations to make `MU`:

(a) Double the string after an `M`.

(b) Replace `III` with `U`.

(c) Append `U`, if the string ends in `I`.

(d) Delete `UU` from the string.

Not a single person in this room
was able to solve this puzzle.

Are we even sure that there is a solution?

Counting **I**'s

MI
1
MII
2
MIIII
4
MIIIIU
4
MIIIIUIIIIU
8
MIIIIUUIU
5
MIIIIUUIUIIIIUUIU
10
MUIUUIUIIIIUUIU
7

The Key Insight

- Initially, the number of **`I`**'s is *not* a multiple of three.
- To make **`MU`**, the number of **`I`**'s must end up as a multiple of three.
- Can we *ever* make the number of **`I`**'s a multiple of three?

Lemma 1: If n is an integer that is not a multiple of three, then $n – 3$ is not a multiple of three.

Proof: By contrapositive; we'll prove that if $n – 3$ is a multiple of three, then n is also a multiple of three. Because $n – 3$ is a multiple of three, we can write $n – 3 = 3k$ for some integer k. Then $n = 3(k+1)$, so n is also a multiple of three, as required. ■

Lemma 2: If n is an integer that is not a multiple of three, then $2n$ is not a multiple of three.

Proof: Let n be a number that isn't a multiple of three. If n is congruent to one modulo three, then $n = 3k + 1$ for some integer k. This means $2n = 2(3k+1) = 6k + 2 = 3(3k) + 2$, so $2n$ is not a multiple of three. Otherwise, n must be congruent to two modulo three, so $n = 3k + 2$ for some integer k. Then $2n = 2(3k+2) = 6k+4 = 3(2k+1) + 1$, and so $2n$ is not a multiple of three. ■

Lemma: No matter which moves are made, the number of **I**'s in the string never becomes multiple of three.

Proof: Let $P(n)$ be the statement "After any n moves, the number of **I**'s in the string will not be multiple of three." We will prove, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$, from which the theorem follows.

As a base case, we'll prove $P(0)$, that the number of **I**'s after 0 moves is not a multiple of three. After no moves, the string is **MI**, which has one **I** in it. Since one isn't a multiple of three, $P(0)$ is true.

For our inductive step, suppose that $P(k)$ is true for some $k \in \mathbb{N}$. We'll prove $P(k+1)$ is also true. Consider any sequence of $k+1$ moves. Let r be the number of **I**'s in the string after the kth move. By our inductive hypothesis (that is, $P(k)$), we know that r is not a multiple of three. Now, consider the four possible choices for the $k+1^{\text{st}}$ move:

Case 1: Double the string after the **M**. After this, we will have $2r$ **I**'s in the string, and from our lemma $2r$ isn't a multiple of three.

Case 2: Replace **III** with **U**. After this, we will have $r - 3$ **I**'s in the string, and by our lemma $r - 3$ is not a multiple of three.

Case 3: Either append **U** or delete **UU**. This preserves the number of **I**'s in the string, so we don't have a multiple of three **I**'s at this point.

Therefore, no sequence of $k+1$ moves ends with a multiple of three **I**'s. Thus $P(k+1)$ is true, completing the induction. ■

Theorem: The **MU** puzzle has no solution.

Proof: Assume for the sake of contradiction that the **MU** puzzle has a solution and that we can convert **MI** to **MU**. This would mean that at the very end, the number of **I**'s in the string must be zero, which is a multiple of three. However, we've just proven that the number of **I**'s in the string can never be a multiple of three.

We have reached a contradiction, so our assumption must have been wrong. Thus the **MU** puzzle has no solution. ■

Algorithms and Loop Invariants

- The proof we just made had the form
  - "If P is true before we perform an action, it is true after we perform an action."
- We could therefore conclude that after any series of actions of any length, if P was true beforehand, it is true now.
- In algorithmic analysis, this is called a ***loop invariant***.
- Proofs on algorithms often use loop invariants to reason about the behavior of algorithms.
  - Take CS161 for more details!

Next Time

- **Variations on Induction**
  - Starting induction later.
  - Taking larger steps.
  - Complete induction.