Mathematical Induction

A Note to CS106B Students

- Since CS106B and CS103 overlap, I'll be repeating the last 15 minutes of lecture every M/W/F from 4:15ish to 4:30ish in my office (Gates 178).
- Stop by if you're interested!

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.

The **principle of mathematical induction** states that if for some property $P(n)$, we have that

$P(0)$ is true

If it starts …

… and it keeps going …

and

For any $n \in \mathbb{N}$, we have $P(n) \rightarrow P(n+1)$

Then

… then it's always true.

For any $n \in \mathbb{N}$, $P(n)$ is true.

Another Example of Induction

Video: Human Dominoes

Human Dominoes

- Everyone (except that last guy) eventually fell over.
- Why is that?
  - Someone fell over.
  - Once someone fell over, the next person fell over as well.

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.
- …

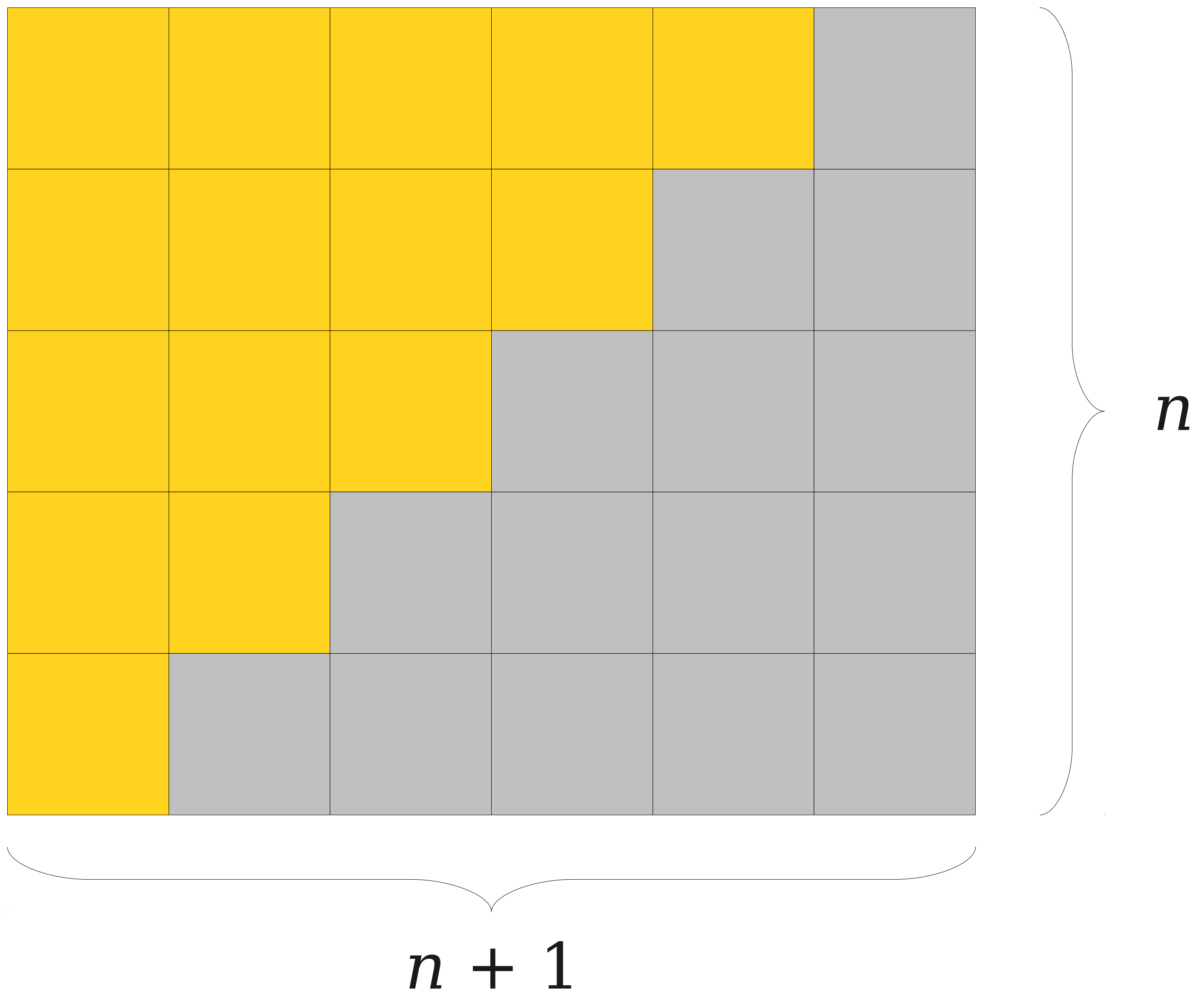
Proof by Induction

- Suppose that you want to prove that some property $P(n)$ holds of all natural numbers. To do so:
  - Prove that $P(0)$ is true.
    - This is called the **basis** or the **base case**.
  - Prove that for all $n \in \mathbb{N}$, that if $P(n)$ is true, then $P(n + 1)$ is true as well.
    - This is called the **inductive step**.
    - $P(n)$ is called the **inductive hypothesis**.
  - Conclude by induction that $P(n)$ holds for all n.

Some Sums

$1 = 1$
$1 + 2 = 3$
$1 + 2 + 3 = 6$
$1 + 2 + 3 + 4 = 10$
$1 + 2 + 3 + 4 + 5 = 15$

$$1 + 2 + \ldots + (n - 1) + n = n(n + 1) / 2$$



Some Sums

$1 = 1$ **$= 1(1 + 1) / 2$**

$1 + 2 = 3$ **$= 2(2 + 1) / 2$**

$1 + 2 + 3 = 6$ **$= 3(3 + 1) / 2$**

$1 + 2 + 3 + 4 = 10$ **$= 4(4 + 1) / 2$**

$1 + 2 + 3 + 4 + 5 = 15$ **$= 5(5 + 1) / 2$**

Theorem: The sum of the first n positive natural numbers is $n(n + 1)/2$.

Proof: By induction. Let $P(n)$ be "the sum of the first n positive natural numbers is $n(n + 1) / 2$." We show that $P(n)$ is true for all $n \in \mathbb{N}$.

For our base case, we need to show $P(0)$ is true, meaning that the sum of the first zero positive natural numbers is $0(0 + 1)/2$. Since the sum of the first zero positive natural numbers is $0 = 0(0 + 1)/2$, $P(0)$ is true.

For the inductive step, assume that for some $n \in \mathbb{N}$ that $P(n)$ holds, meaning that $1 + 2 + \ldots + n = n(n + 1) / 2$. We need to show that $P(n + 1)$ holds, meaning that the sum of the first $n + 1$ natural numbers is $(n + 1)(n + 2)/2$.

Consider the sum of the first $n + 1$ positive natural numbers. This is the sum of the first n positive natural numbers, plus $n + 1$. By the inductive hypothesis, this is given by

$$1+\ldots+n+(n+1)=\frac{n(n+1)}{2}+n+1=\frac{n(n+1)+2(n+1)}{2}=\frac{(n+1)(n+2)}{2}$$

Thus $P(n + 1)$ is true, completing the induction. ■

Structuring a Proof by Induction

- State that your proof works by induction.
- State your choice of $P(n)$.
- Prove the base case:
  - State what $P(0)$ is, then prove it using any technique you'd like.
- Prove the inductive step:
  - State that for some arbitrary $n \in \mathbb{N}$ that you're assuming $P(n)$ and mention what $P(n)$ is.
  - State that you are trying to prove $P(n + 1)$ and what $P(n + 1)$ means.
  - Prove $P(n + 1)$ using any technique you'd like.
- This is very rigorous, so as we gain more familiarity with induction we will start being less formal in our proofs.

Notation: Summations

- Instead of writing 1 + 2 + 3 + … + n, we write

Sum from i = 1 to n

$$\boxed{\sum_{i=1}^{n} i}$$

of i

Summation Examples

$$\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15$$

$$\sum_{i=1}^{3} i^2 = 1^2 + 2^2 + 3^2 = 1 + 4 + 9 = 14$$

$$\sum_{i=0}^{2} \left(i^2 - i\right) = \left(0^2 - 0\right) + \left(1^2 - 1\right) + \left(2^2 - 2\right) = 2$$

The Empty Sum

- A sum of no numbers is called the **empty sum** and is defined to be zero.
- Examples:

$$\sum_{i=1}^{0} 2^i = 0 \qquad \sum_{i=137}^{42} i^i = 0 \qquad \sum_{i=0}^{-1} i = 0$$

Theorem: For any natural number n, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof: By induction. Let $P(n)$ be

$$P(n) \equiv \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

For our base case, we need to show $P(0)$ is true, meaning that

$$\sum_{i=1}^{0} i = \frac{0(0+1)}{2}$$

Since the empty sum is defined to be 0, this claim is true.

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

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

We need to show that $P(n + 1)$ holds, meaning that

$$\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

To see this, note that

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Thus $P(n + 1)$ is true, completing the induction. ■

Sums of Powers of Two

(empty sum) $= 0$ **$= 2^0 - 1$**

$2^0 = 1 = 1$ **$= 2^1 - 1$**

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

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

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

$$\sum_{i=0}^{n-1} 2^i = 2^n - 1$$

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. We'll see one in a week.

Theorem: For any natural number n, $\sum_{i=0}^{n-1} 2^i = 2^n - 1$

Proof: By induction. Let $P(n)$ be

$$P(n) \equiv \sum_{i=0}^{n-1} 2^i = 2^n - 1$$

For our base case, we need to show $P(0)$ is true, meaning that

$$\sum_{i=0}^{-1} 2^i = 2^0 - 1$$

Since $2^0 - 1 = 0$ and the left-hand side is the empty sum, $P(0)$ holds.

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

$$\sum_{i=0}^{n-1} 2^i = 2^n - 1$$

We need to show that $P(n + 1)$ holds, meaning that

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

To see this, note that

$$\sum_{i=0}^{n} 2^i = \left(\sum_{i=0}^{n-1} 2^i\right) + 2^n = 2^n - 1 + 2^n = 2(2^n) - 1 = 2^{n+1} - 1$$

Thus $P(n + 1)$ holds, completing the induction. ■

Problem Session Tonight

- Problem Session tonight, 7:00 – 7:50PM in 380-380X
- Purely optional, but should be a lot of fun!
- We'll try to get it recorded and posted online as soon as possible.

An Incorrect Proof

Theorem: For any $n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{1}{2}(n + \frac{1}{2})^2$

Proof: By induction. Let $P(n)$ be defined as $P(n) \equiv \sum_{i=1}^{n} i = \frac{1}{2}(n + \frac{1}{2})^2$

Now, assume that for some $n \in \mathbb{N}$ that $P(n)$ holds, so

$$\sum_{i=1}^{n} i = \frac{1}{2}(n + \frac{1}{2})^2$$

We want to show that $P(n + 1)$ is true, which means that we want to show

$$\sum_{i=1}^{n+1} i = \frac{1}{2}(n + 1 + \frac{1}{2})^2 = \frac{1}{2}(n + \frac{3}{2})^2$$

To see this, note that

$$\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + n + 1 = \frac{1}{2}(n + \frac{1}{2})^2 + n + 1 = \frac{(n + \frac{1}{2})^2}{2} + \frac{2(n+1)}{2} = \frac{(n + \frac{1}{2})^2 + 2(n+1)}{2}$$

$$= \frac{n^2 + n + \frac{1}{4} + 2\mathrm{n} + 2}{2} = \frac{n^2 + 3\mathrm{n} + \frac{9}{4}}{2} = \frac{(n + \frac{3}{2})^2}{2}$$

So $P(n + 1)$ holds, completing the induction. ■

An Incorrect Proof

Theorem: For any $n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{1}{2}\left(n + \frac{1}{2}\right)^2$

Proof: By induction. Let $P(n)$ be defined as $P(n) \equiv \sum_{i=1}^{n}$

Where did we prove the base case?

Now, assume that for some $n \in \mathbb{N}$ that $P(n)$ holds,

$$\sum_{i=1}^{n} i = \frac{1}{2}\left(n + \frac{1}{2}\right)^2$$

We want to show that $P(n + 1)$ is true, which means that we want to show

$$\sum_{i=1}^{n+1} i = \frac{1}{2}\left(n + 1 + \frac{1}{2}\right)^2 = \frac{1}{2}\left(n + \frac{3}{2}\right)^2$$

To see this, note that

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + n + 1 = \frac{1}{2}\left(n + \frac{1}{2}\right)^2 + n + 1 = \frac{\left(n + \frac{1}{2}\right)^2}{2} + \frac{2(n+1)}{2} = \frac{\left(n + \frac{1}{2}\right)^2 + 2(n+1)}{2}$$

$$= \frac{n^2 + n + \frac{1}{4} + 2n + 2}{2} = \frac{n^2 + 3n + \frac{9}{4}}{2} = \frac{\left(n + \frac{3}{2}\right)^2}{2}$$

So $P(n + 1)$ holds, completing the induction. ■

When proving $P(n)$ is true
for all $n \in \mathbb{N}$ by induction,

make sure to show the base case!

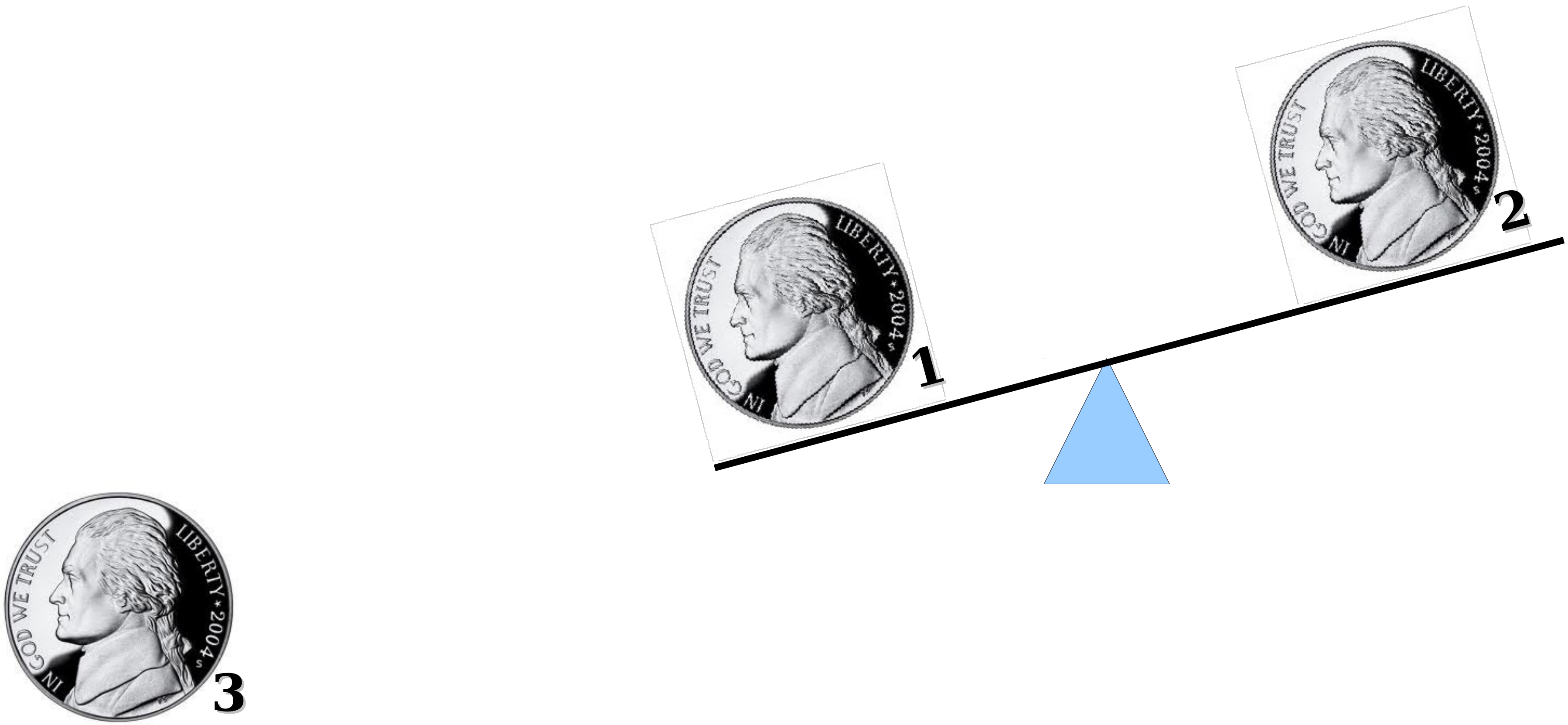
Otherwise, your argument is invalid!

The Counterfeit Coin Problem, Take Two

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.

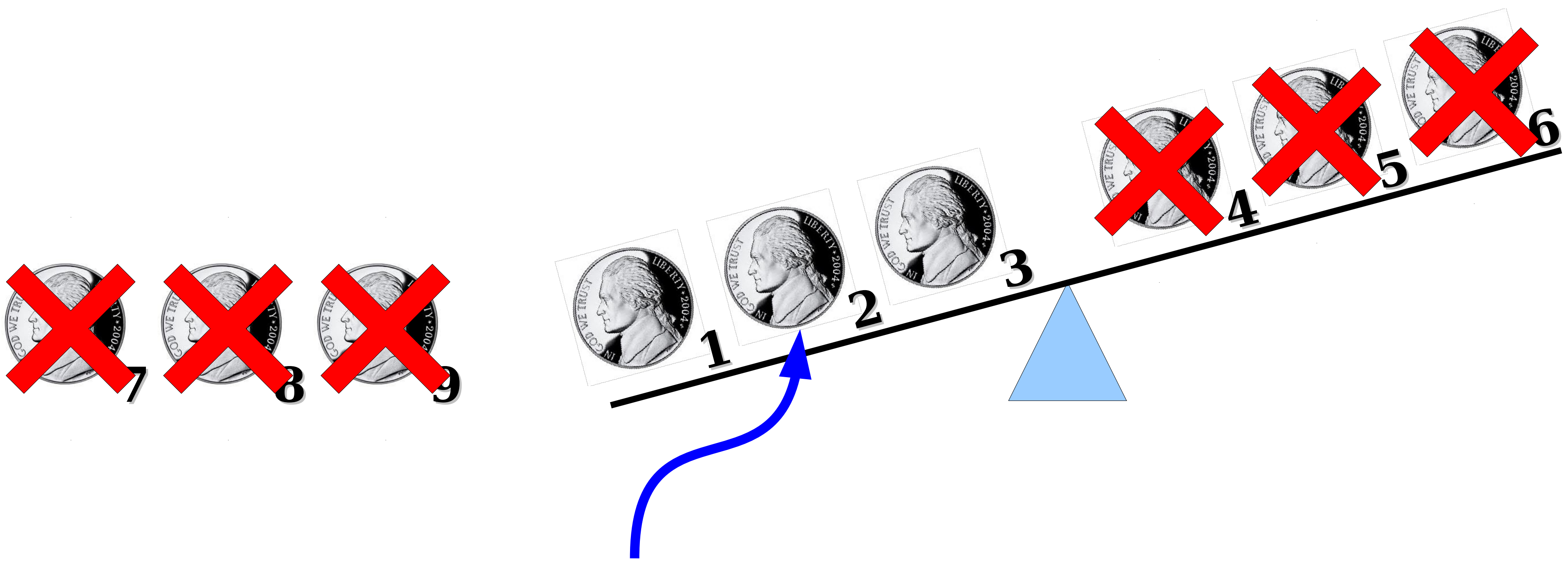
Finding the Counterfeit Coin



A Harder Problem

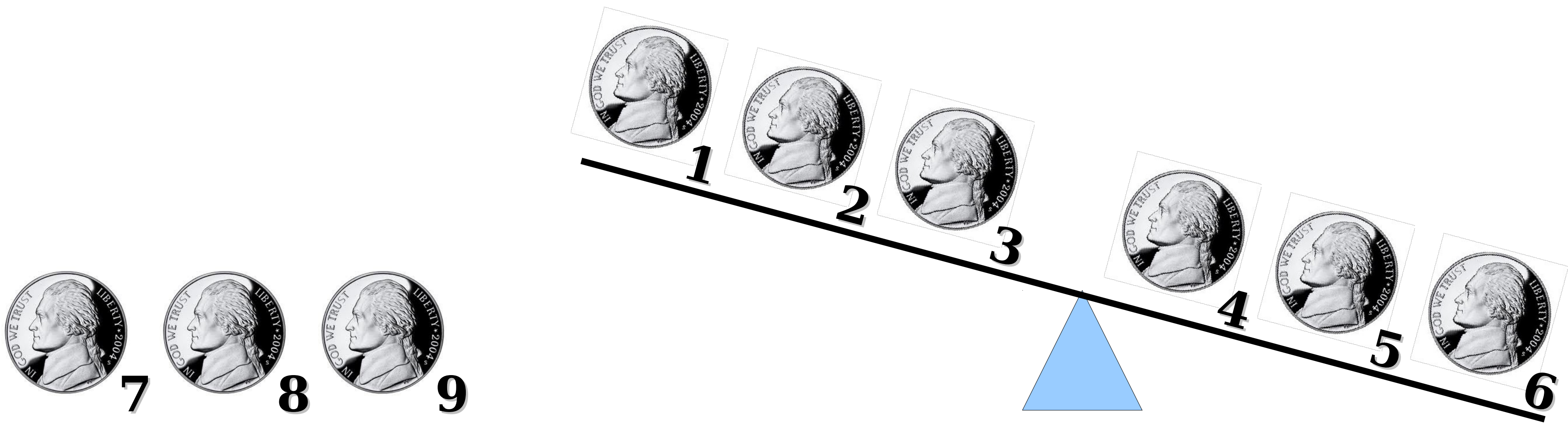
- You are given a set of **nine** seemingly identical coins, eight of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only **two** weighings on the balance, find the counterfeit coin.

Finding the Counterfeit Coin

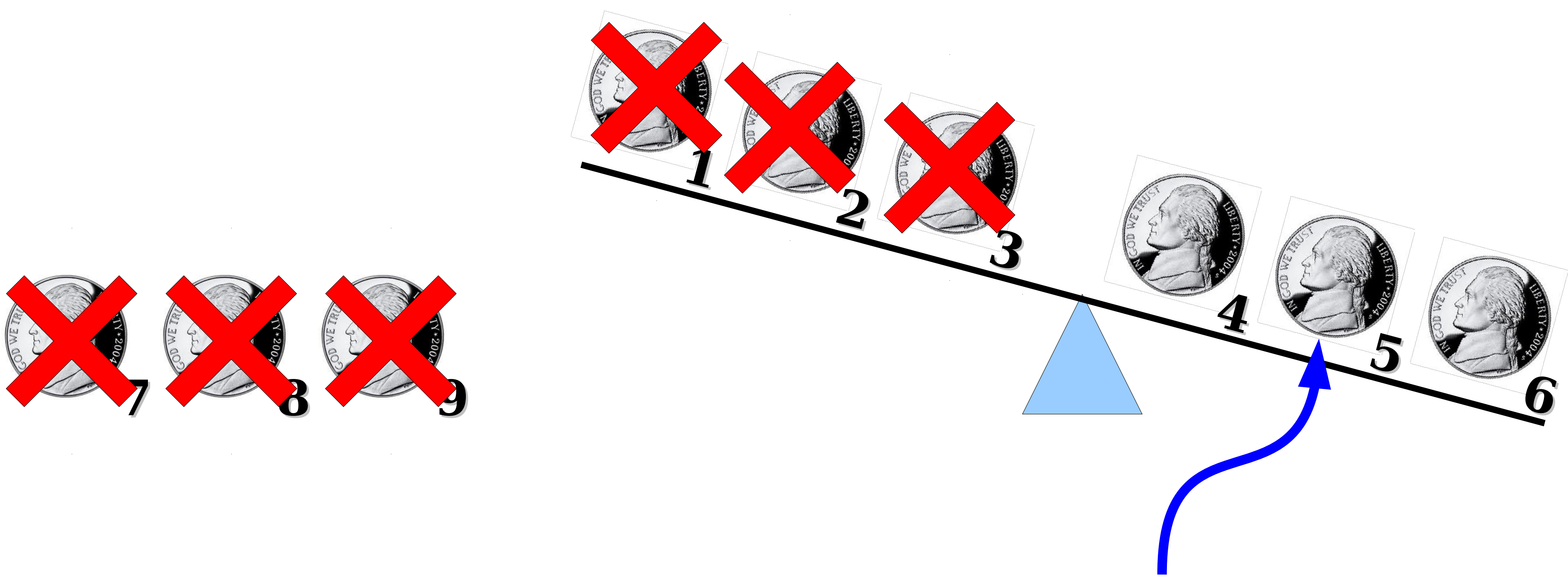


Now we have one weighing to find
the counterfeit out of these three

Finding the Counterfeit Coin

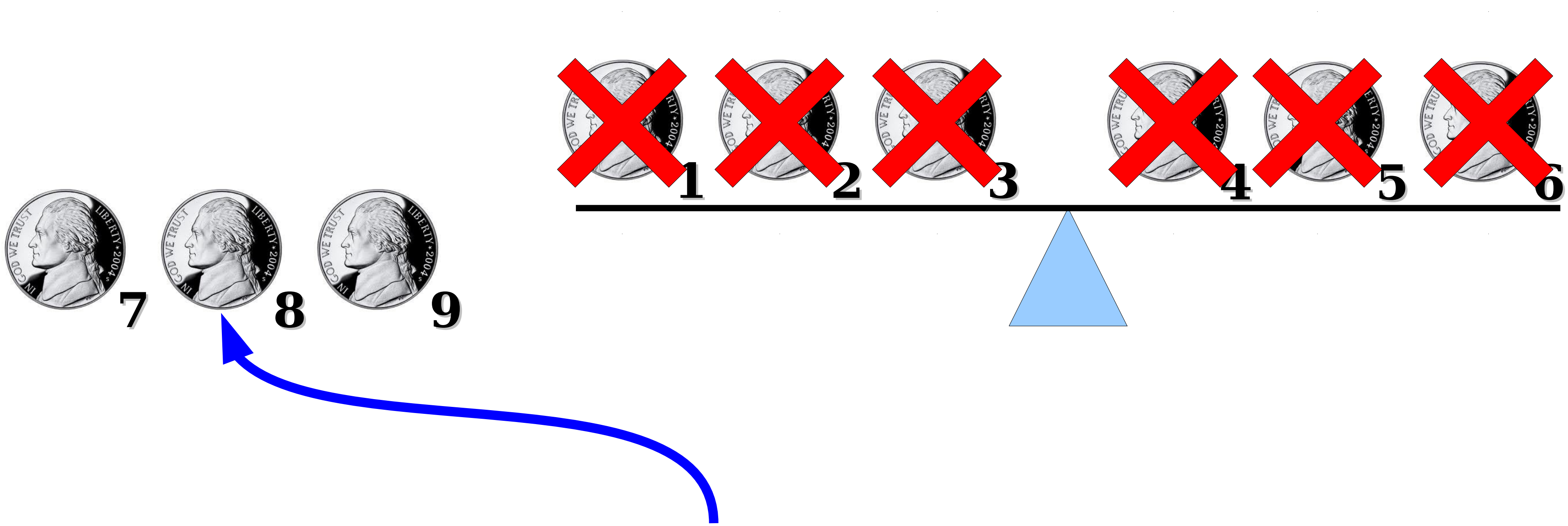


Finding the Counterfeit Coin



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

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

- 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: Given n weighings, we can detect which of 3^n coins is counterfeit.

Proof: By induction. Let $P(n)$ be "Given n weighings, we can detect which of the 3^n coins is counterfeit." We prove that $P(n)$ is true for all $n \in \mathbb{N}$.

For the base case, we show $P(0)$ holds, which means that we can detect which of $3^0 = 1$ coins is counterfeit in no weighings. This is trivial – if there is only one coin, it must be the counterfeit.

For the inductive step, suppose that for some n, $P(n)$ holds, so we can detect which of 3^n coins is counterfeit using n weighings. We will show $P(n + 1)$ holds, meaning we can detect which of 3^{n+1} coins is counterfeit using $n + 1$ weighings.

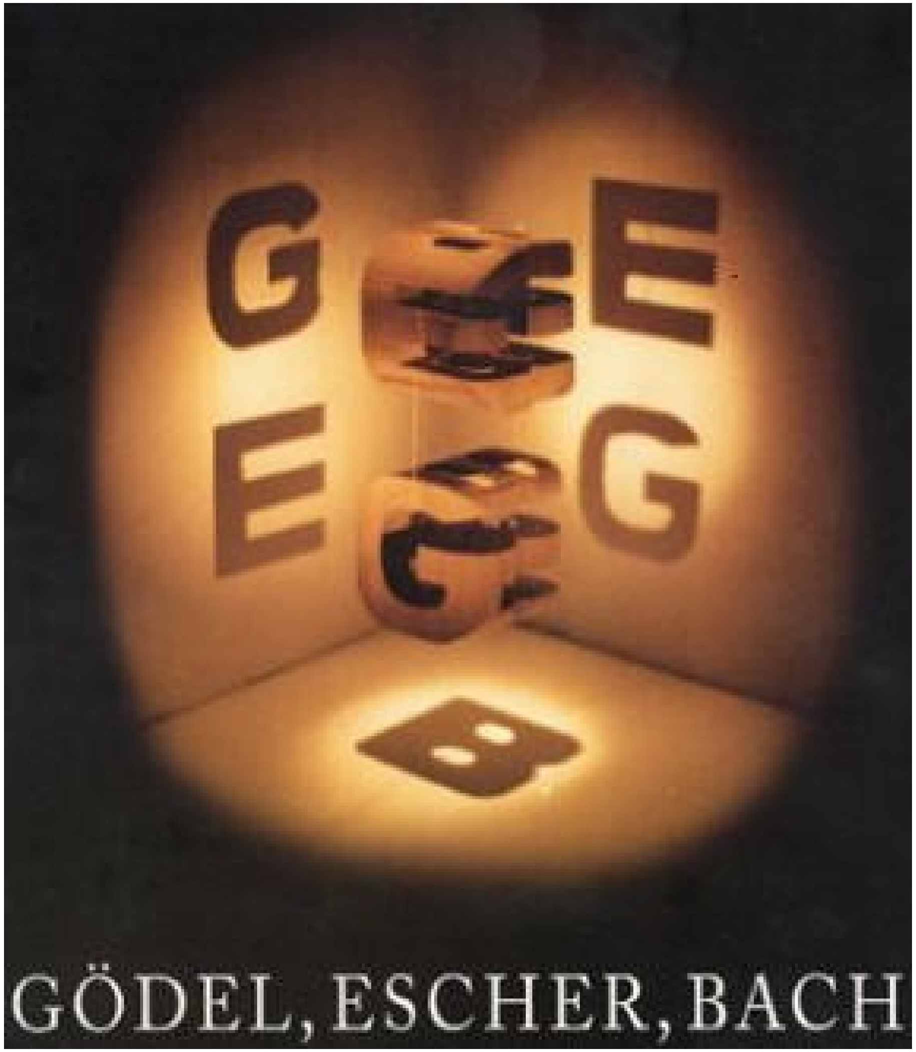
Given 3^{n+1} coins, split them into three equal groups of size 3^n; call the groups A, B, and C. Put the coins in set A on one side of the scale and the coins in set B on the other side. There are three cases to consider:

Case 1: Side A is heavier. Then the counterfeit coin must be in group A.
Case 2: Side B is heavier. Then the counterfeit coin must be in group B.
Case 3: The scale is balanced. Then the counterfeit coin must be in group C, since it isn't in groups A or B.

In any case, we can use one weighing to find a group of 3^n coins that contains the counterfeit coin. By the inductive hypothesis, we can use n more weighings to find which of these 3^n coins is counterfeit. Combined with our original weighing, this means that we can find the counterfeit of 3^{n+1} coins in $n + 1$ weighings. Thus $P(n + 1)$ holds, completing the induction. ■

The **MU** Puzzle

Gödel, Escher Bach: An Eternal Golden Braid



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

The **`MU`** Puzzle

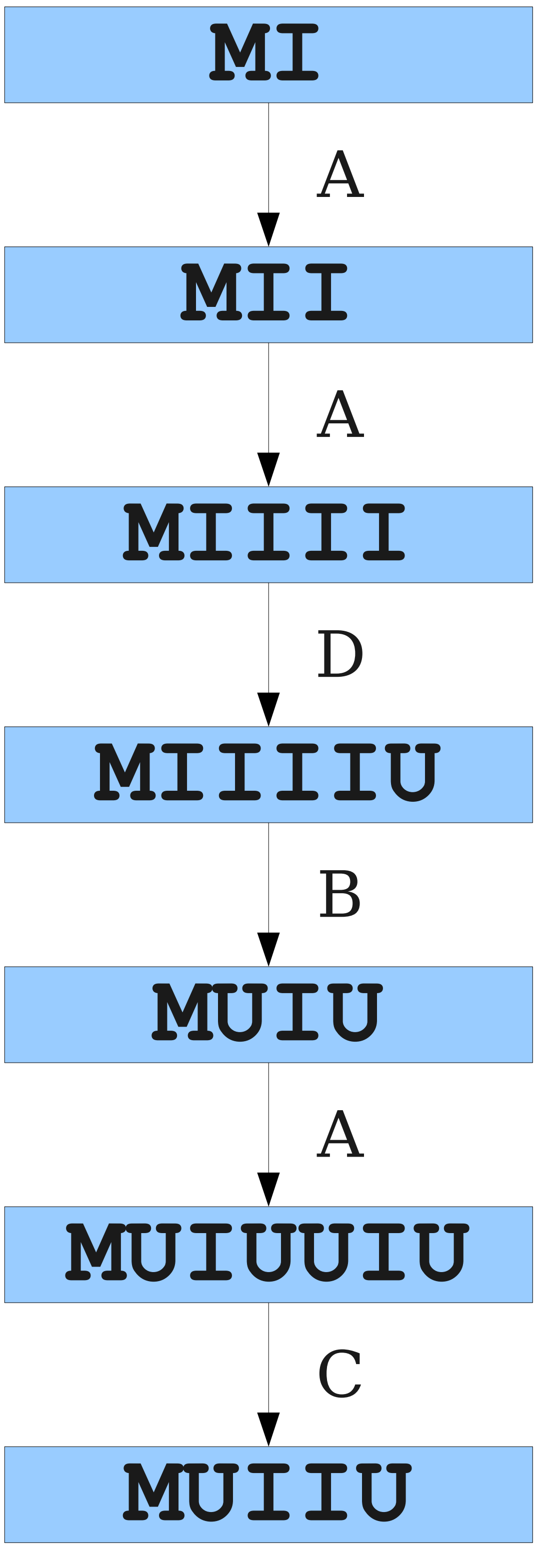
- Begin with the string **`MI`**.
- Repeatedly apply one of the following operations:
  - Double the contents of the string after the **`M`**: for example, **`MIIU`** becomes **`MIIUIIU`** or **`MI`** becomes **`MII`**.
  - Replace **`III`** with **`U`**: **`MIIII`** becomes **`MUI`** or **`MIU`**
  - 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 contents of the string after **M**.

B) Replace **III** with **U**.

C) Remove **UU**

D) Append **U** if the string ends in **I**.



Try It!

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

A) Double the contents of the string after **`M`**.

B) Replace **`III`** with **`U`**.

C) Remove **`UU`**

D) Append **`U`** if the string ends in **`I`**.

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

None of these are multiples of three...

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: Beginning with **MI** and applying any legal sequence of moves, the number of **I**'s is never a multiple of 3.

Proof: By induction. Let $P(n)$ be "After making n legal moves starting with string **MI**, the number of **I**'s is not a multiple of 3." We prove $P(n)$ holds for all $n \in \mathbb{N}$.

As a base case, to prove $P(0)$, we show that after making no moves the number of **I**'s is not a multiple of 3. **MI** has one **I** in it, which is not a multiple of 3.

For the inductive step, assume for some $n \in \mathbb{N}$ that $P(n)$ holds and that after any sequence of n operations, the number of **I**'s is not a multiple of 3. We prove $P(n + 1)$, that after $n + 1$ operations, the number of **I**'s is not a multiple of 3.

To see this, note that any sequence of $n + 1$ operations is formed from a sequence of n operations followed by one final operations. By the inductive hypothesis, after the first n operations, the number of **I**'s is not a multiple of 3. Thus before performing the $(n + 1)$st operation, the number of **I**'s either has the form $3k + 1$ or $3k + 2$ for some $k \in \mathbb{N}$. Now, consider the $(n + 1)$st operation:

Case 1: It's "double the string after the **M**." Then we either end up with either $2(3k + 1) = 6k + 2 = 3(2k) + 2$ or $2(3k + 2) = 6k + 4 = 3(2k + 1) + 1$ copies of **I**, neither of which is a multiple of 3.

Case 2: It's "delete **UU**" or "append **U**." Then the number of **I**'s is unchanged.

Case 3: It's "delete **III**." Then we either go from $3k + 1$ to $3k + 1 - 3 = 3(k - 1) + 1$ **I**'s, or from $3k + 2$ to $3k + 2 - 3 = 3(k - 1) + 2$ **I**'s, neither of which is a multiple of 3.

Thus any sequence of $n + 1$ moves starting with **MI** ends with the number of **I**'s not a multiple of three. Thus $P(n + 1)$ holds, completing the induction. ■

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

Proof: By contradiction; assume it has a solution. By our lemma, the number of **`I`**'s in the final string must not be a multiple of 3. However, for the solution to be valid, the number of **`I`**'s must be 0, which is a multiple of 3. We have reached a contradiction, so our assumption was wrong and 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!