Mathematical Induction

Part One

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 predicate. The ***principle of mathematical induction*** states that if

If it starts true…

$P(0)$ is true

and

…and it stays true…

$\forall k \in \mathbb{N}. (P(k) \to P(k+1))$

then

$\forall n \in \mathbb{N}. P(n)$

…then it's always true.

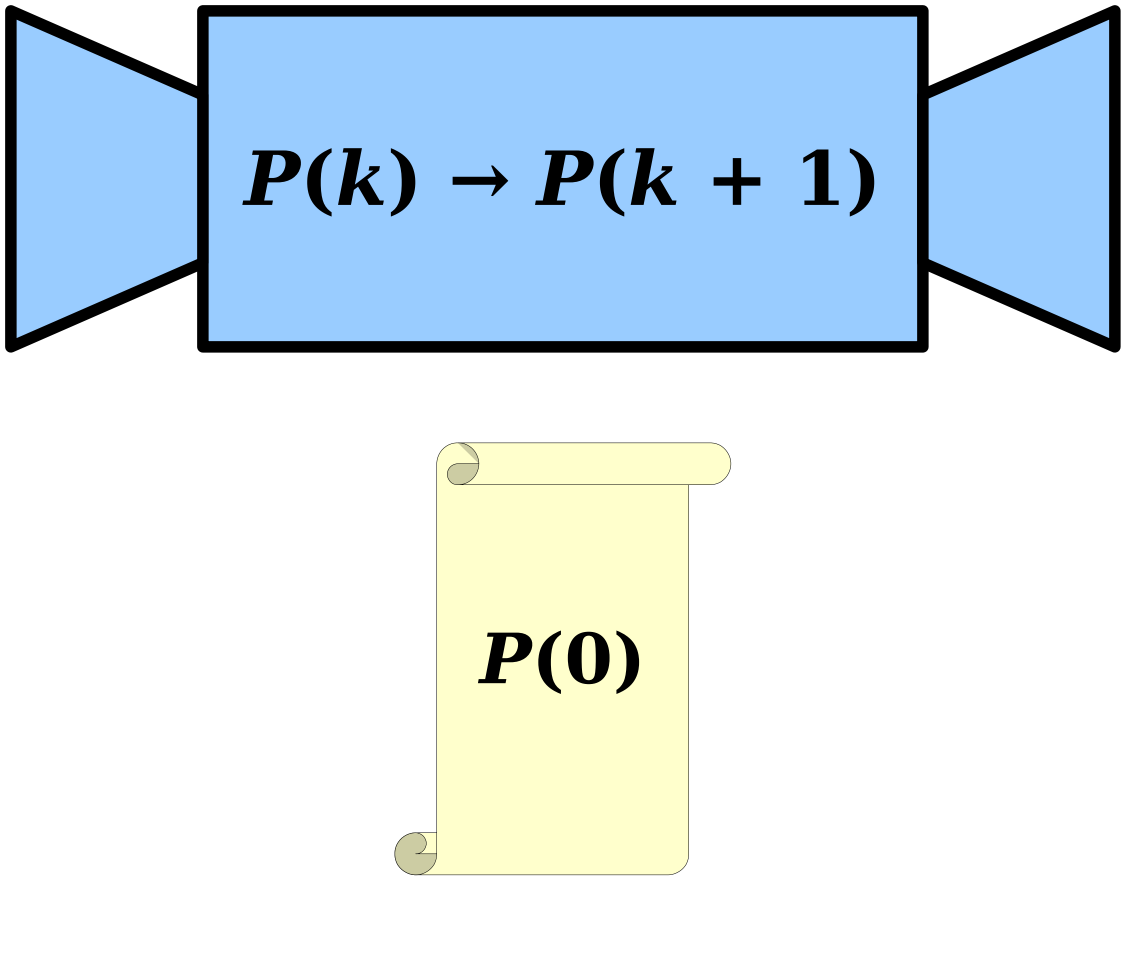
Induction, Intuitively

$$\boldsymbol{P(0)}$$

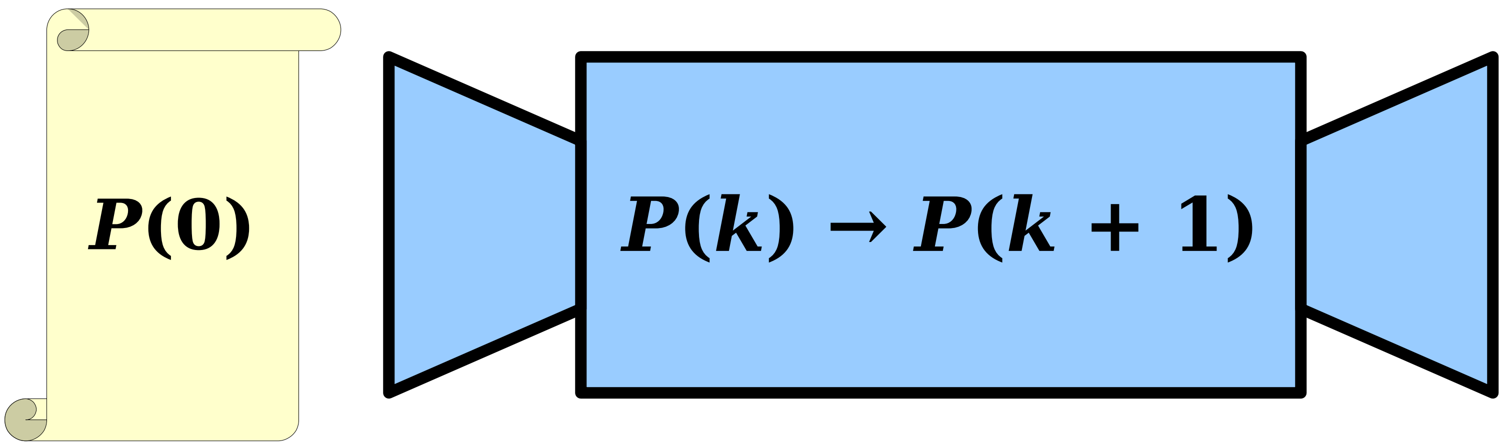
$$\boldsymbol{\forall k \in \mathbb{N}.\ (P(k) \rightarrow P(k+1))}$$

- 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.
- …

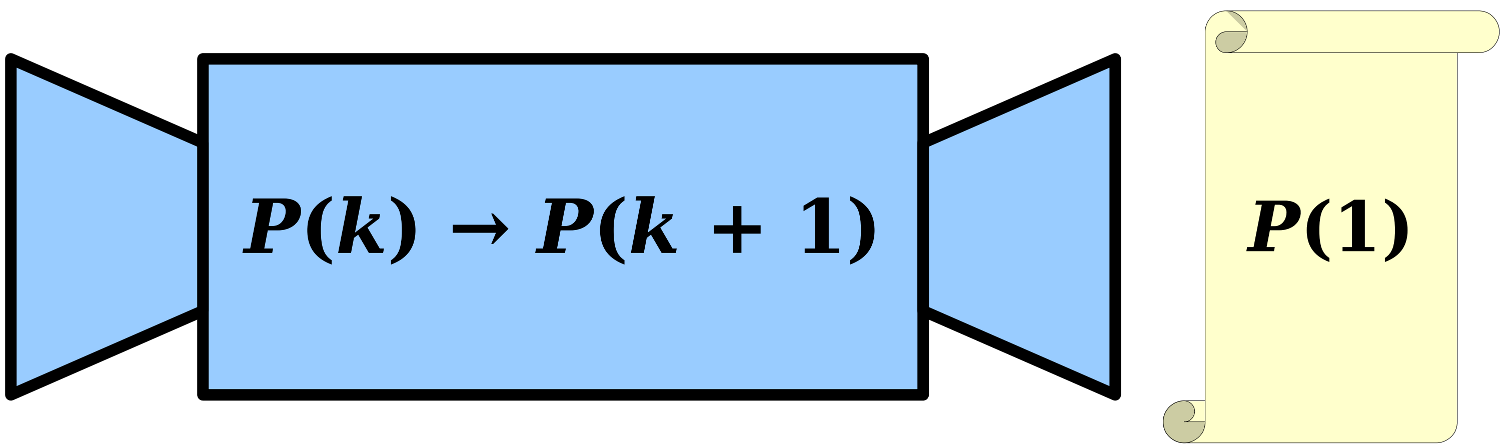
Why Induction Works



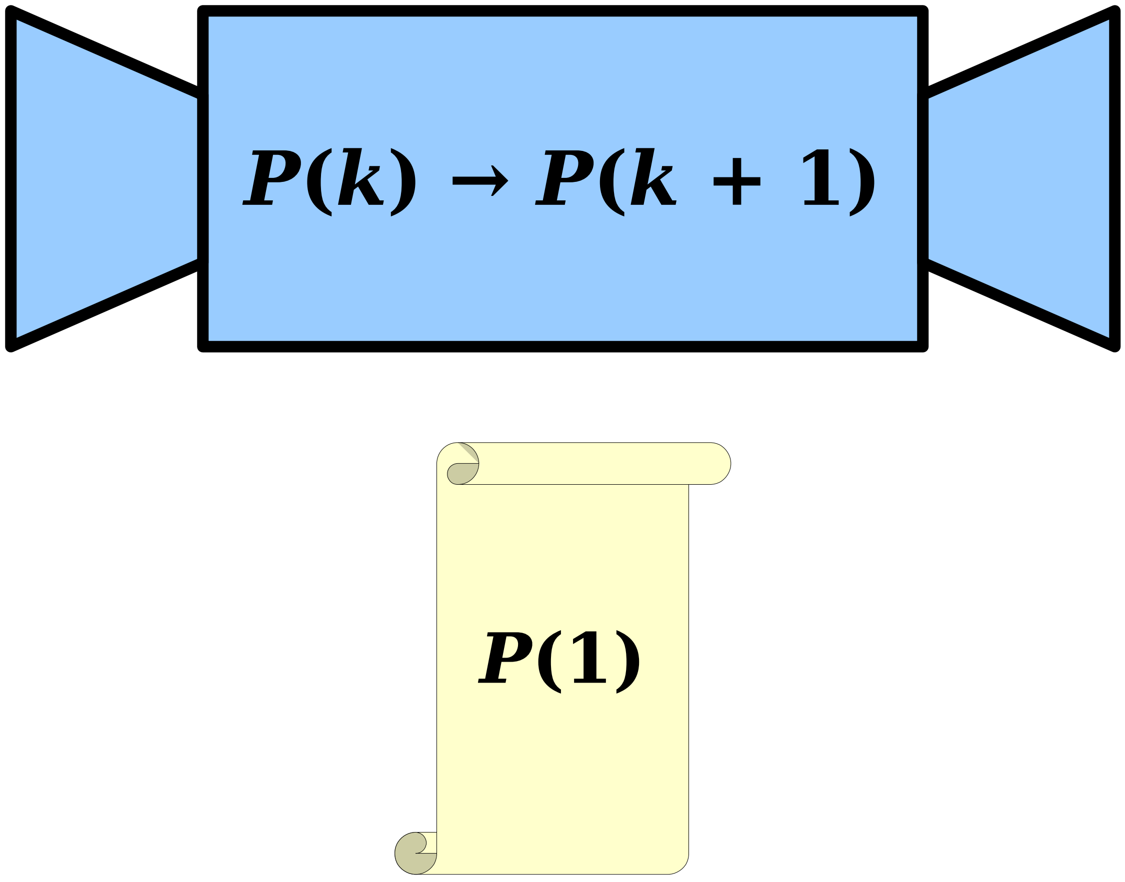
Why Induction Works



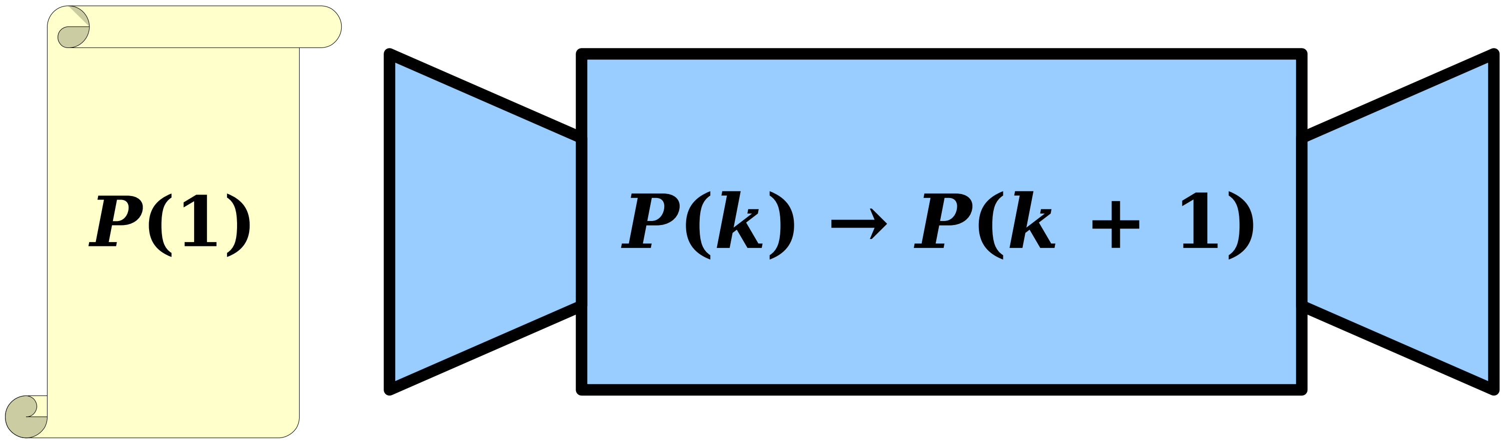
Why Induction Works



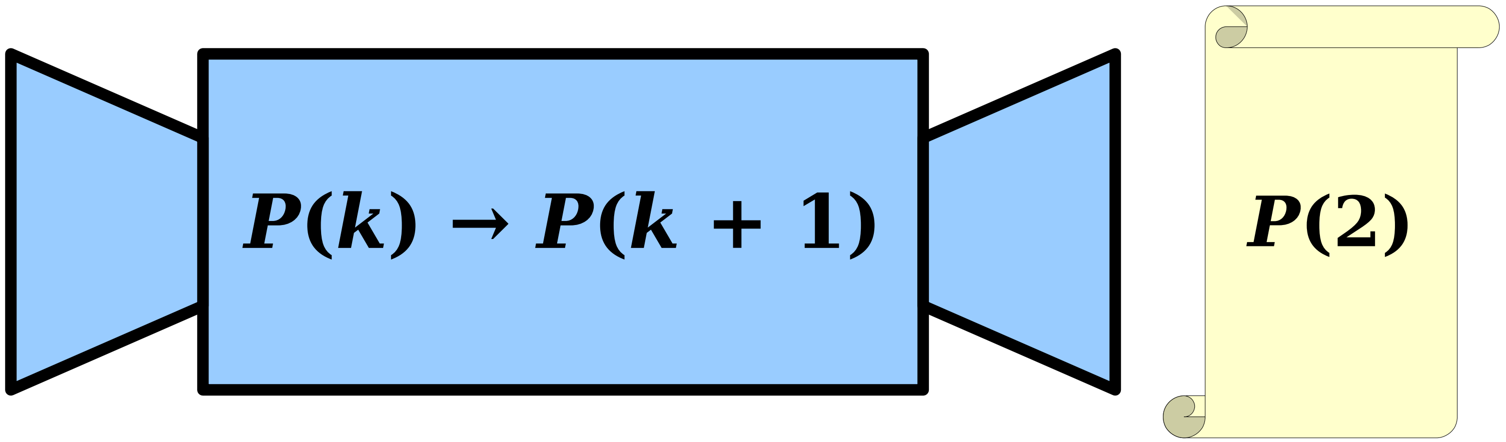
Why Induction Works



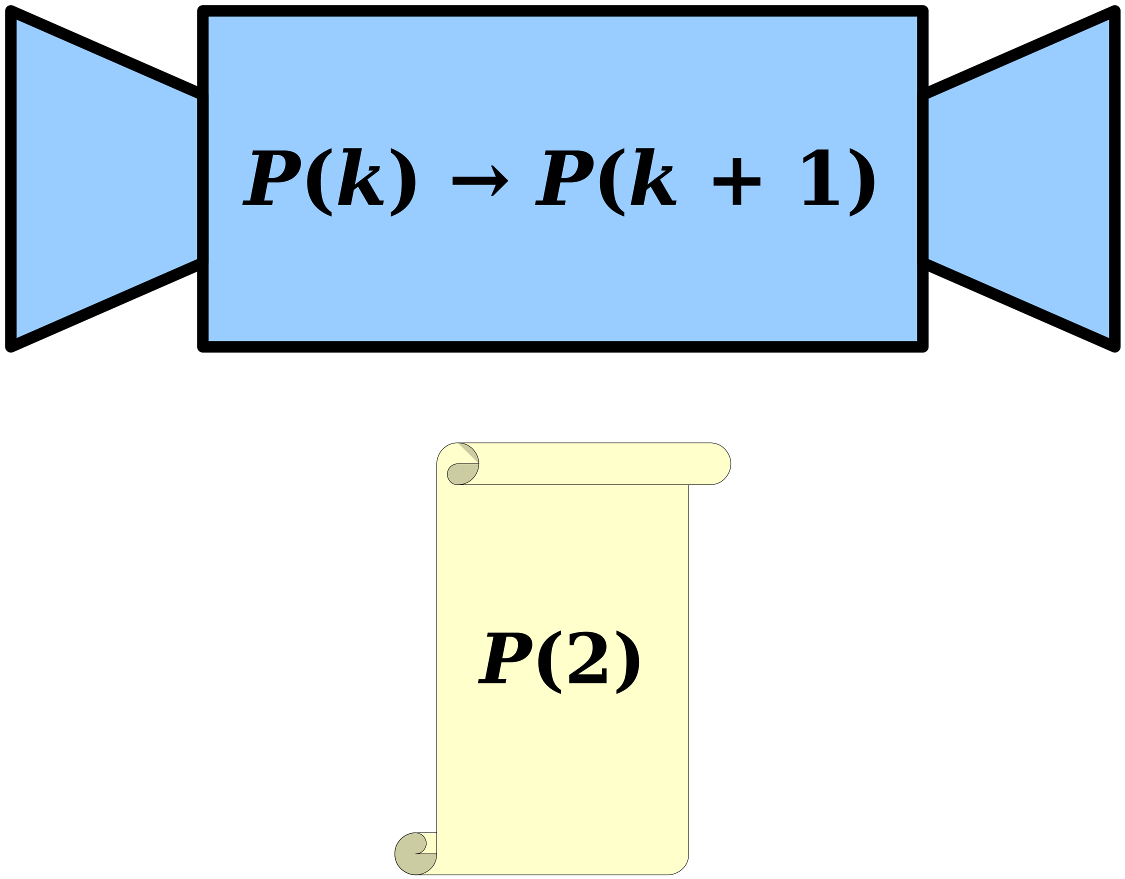
Why Induction Works



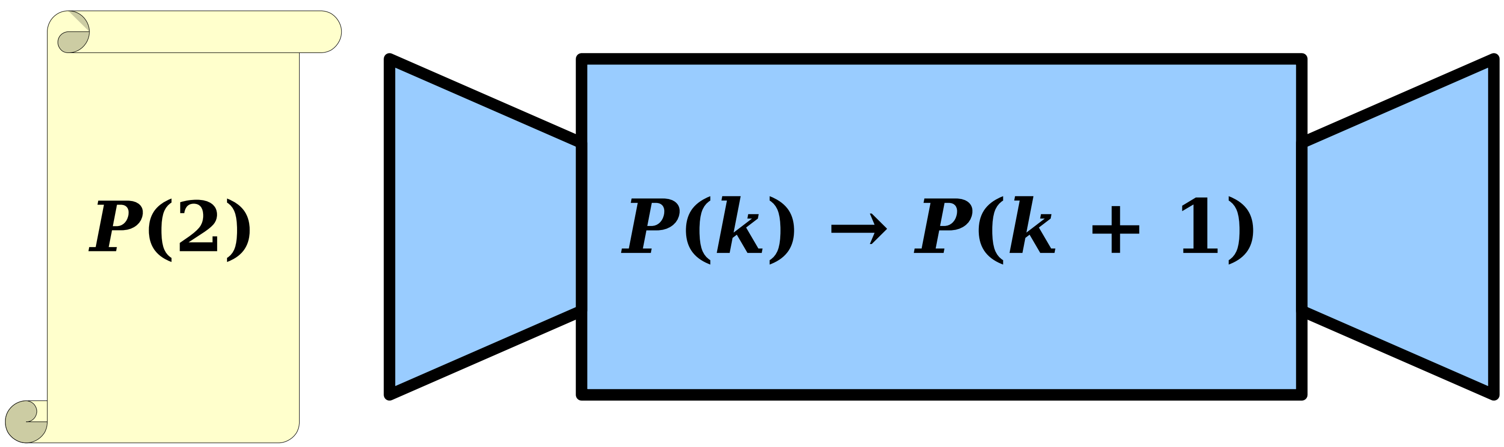
Why Induction Works



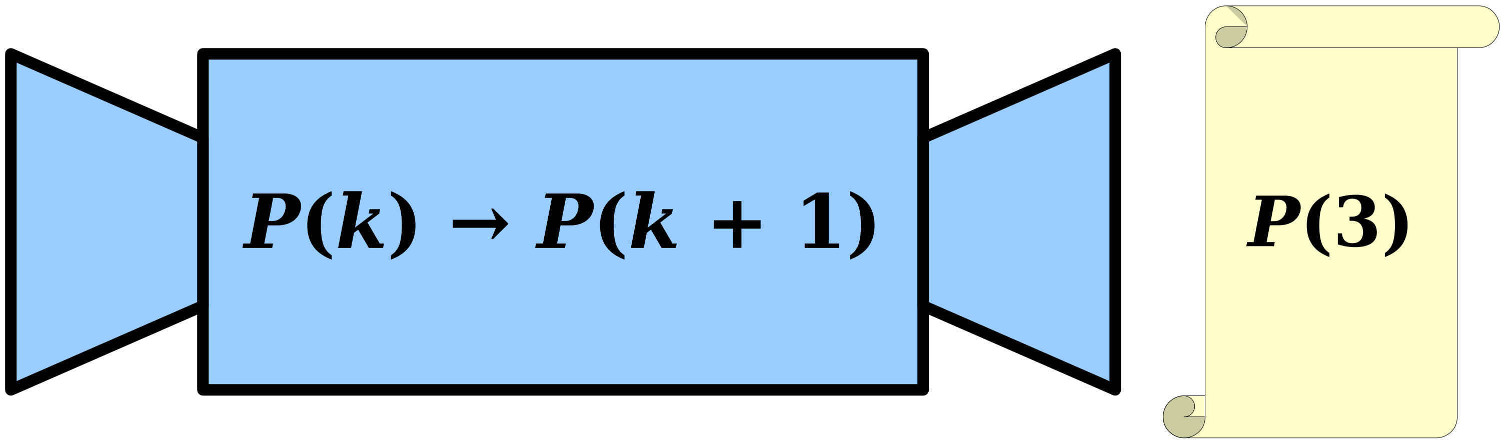
Why Induction Works



Why Induction Works



Why Induction Works



Proof by Induction

- A ***proof by induction*** is a way to use the principle of 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 $P(0)$ is true.
    - This is called the ***basis step*** or the ***base case***.
  - Prove that for all naturals k, if $P(k)$ is true, then $P(k+1)$ is true.
    - This is called the ***inductive step***. (This part is generally done as a direct proof of a universal implication.)
    - The assumption that $P(k)$ is true is called the ***inductive hypothesis***.
  - Conclude, by induction, that $P(n)$ is true for all $n \in \mathbb{N}$.

Some Sums

$$2^0$$

$$2^0 + 2^1$$

$$2^0 + 2^1 + 2^2$$

$$2^0 + 2^1 + 2^2 + 2^3$$

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4$$

$$\mathbf{2^0} = 1$$

$$\mathbf{2^0 + 2^1} = 1 + 2 = 3$$

$$\mathbf{2^0 + 2^1 + 2^2} = 1 + 2 + 4 = 7$$

$$\mathbf{2^0 + 2^1 + 2^2 + 2^3} = 1 + 2 + 4 + 8 = 15$$

$$\mathbf{2^0 + 2^1 + 2^2 + 2^3 + 2^4} = 1 + 2 + 4 + 8 + 16 = 31$$

$$2^0 = 1$$

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

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

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

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

Hmm, 3 is close to 4
and 7 is close to 8,
and 15 is close to 1
And 31 is close to 32

$$\mathbf{2^0} = 1$$

$$\mathbf{2^0 + 2^1} = 1 + 2 = 3$$

$$\mathbf{2^0 + 2^1 + 2^2} = 1 + 2 + 4 = 7$$

$$\mathbf{2^0 + 2^1 + 2^2 + 2^3} = 1 + 2 + 4 + 8 = 15$$

$$\mathbf{2^0 + 2^1 + 2^2 + 2^3 + 2^4} = 1 + 2 + 4 + 8 + 16 = 31$$

Hmm, 3 is close to 4
and 7 is close to 8,
and 15 is close to 1
And 31 is close to 32

Quick check: What is the pattern? The sum of first *n* powers of 2 is ...

P

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

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

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

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

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

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

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 $2^n - 1$."

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.

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.

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 predicate 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.

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
- ☐ For all naturals k, 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 $2^0 - 1$.

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 $2^0 - 1$.

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 technique!

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.

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
- ☐ For all naturals k, 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.

In a proof by induction, we need to prove that

- ✓ $P(0)$ is true
- ☐ For all naturals k, 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
of two is $2^n - 1$." We will prove, by
true for all $n \in \mathbb{N}$, from which the

For our base case, we need to sho
that the sum of the first zero powe
the sum of the first zero powers o
is zero as well, we see that $P(0)$ is

Quick check: Ignore tha
kind of proof for us for a s
were proving the theore
direct proof, what wou
sentence be?

In a proof by induction, we need to prove that

- ✓ $P(0)$ is true
- ☐ For all naturals k, 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, pick an arbitrary $k \in \mathbb{N}$ and assume that $P(k)$ holds, meaning that

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

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, pick an arbitrary $k \in \mathbb{N}$ and assume 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 $2^{k+1} - 1$.

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, pick an arbitrary k ∈ ℕ and assume 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 $2^{k+1} - 1$.

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, pick an arbitrary $k \in \mathbb{N}$ and assume 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

"For all $k \in \mathbb{N}$, if $P(k)$, then $P(k+1)$."

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, pick an arbitrary $k \in \mathbb{N}$ and assume 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 $2^{k+1} - 1$.

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, pick an arbitrary $k \in \mathbb{N}$ and assume 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 state $P(k+1)$, which is what we want to prove. Now, we can use any proof technique we want 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 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, pick an arbitrary $k \in \mathbb{N}$ and assume 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 fo… s.

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

> Here, we'll 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, pick an arbitrary $k \in \mathbb{N}$ and assume 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, pick an arbitrary $k \in \mathbb{N}$ and assume 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

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

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, pick an arbitrary $k \in \mathbb{N}$ and assume 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

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

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, pick an arbitrary $k \in \mathbb{N}$ and assume that P(k) holds, meaning thathat

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

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

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

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, pick an arbitrary $k \in \mathbb{N}$ and assume 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.

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, pick an arbitrary k ∈ ℕ and assume that P(k) holds, meaning that

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

> In a proof by induction, we need to prove that
>
> ✓ $P(0)$ is true
>
> ✓ For all k $\in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

We n … um

of th …

notic …

2^0 …

$$= 2^k - 1 + 2^k \qquad (\text{via } (1))$$

$$= 2(2^k) - 1$$

$$= 2^{k+1} - 1.$$

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

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, pick an arbitrary k ∈ ℕ and assume 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

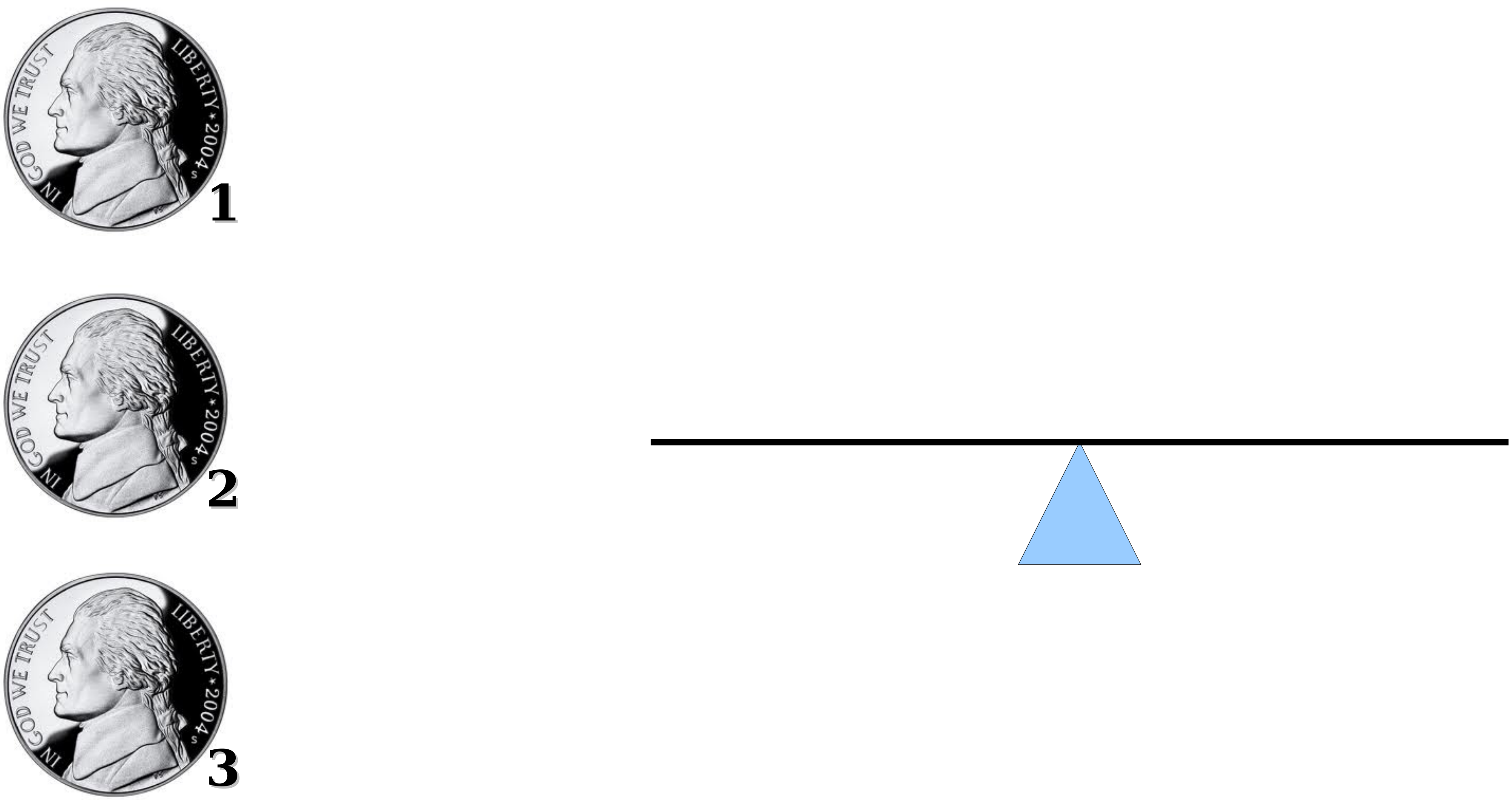
- This result helps explain the range of numbers that can be stored in an **`int`**.
- If you have an unsigned 32-bit integer, the largest value you can store is given by $1 + 2 + 4 + 8 + \ldots + 2^{31} = 2^{32} - 1$.
- This formula for sums of powers of two has many other uses as well. You'll see one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

The Counterfeit Coin Problem

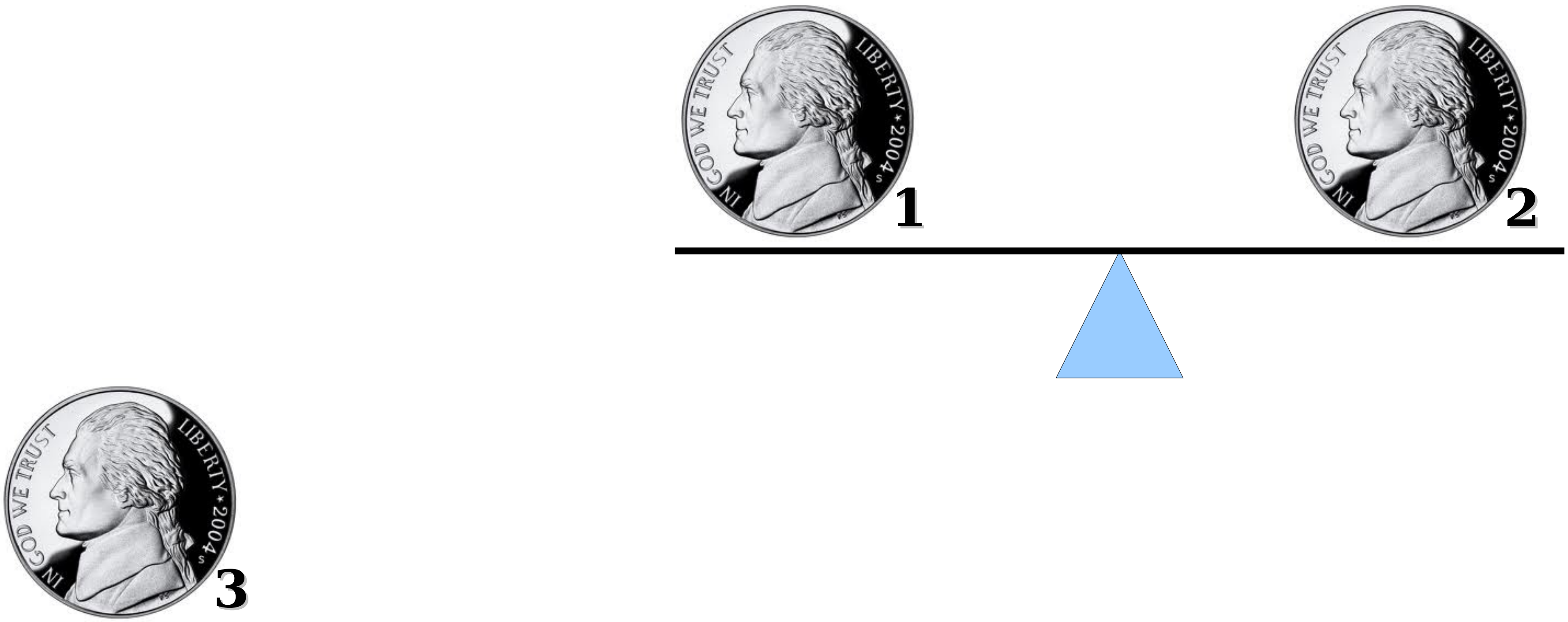
Problem Statement

- 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.

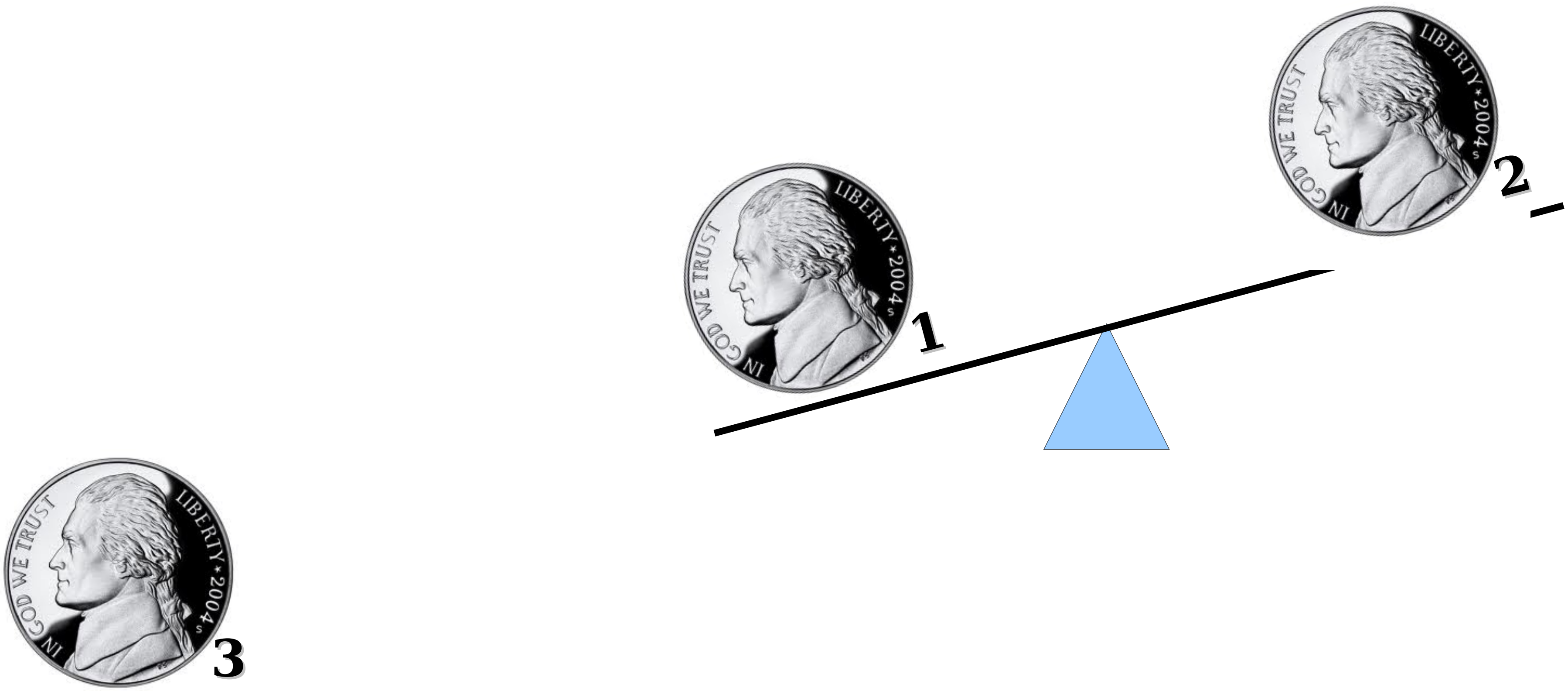
Finding the Counterfeit Coin



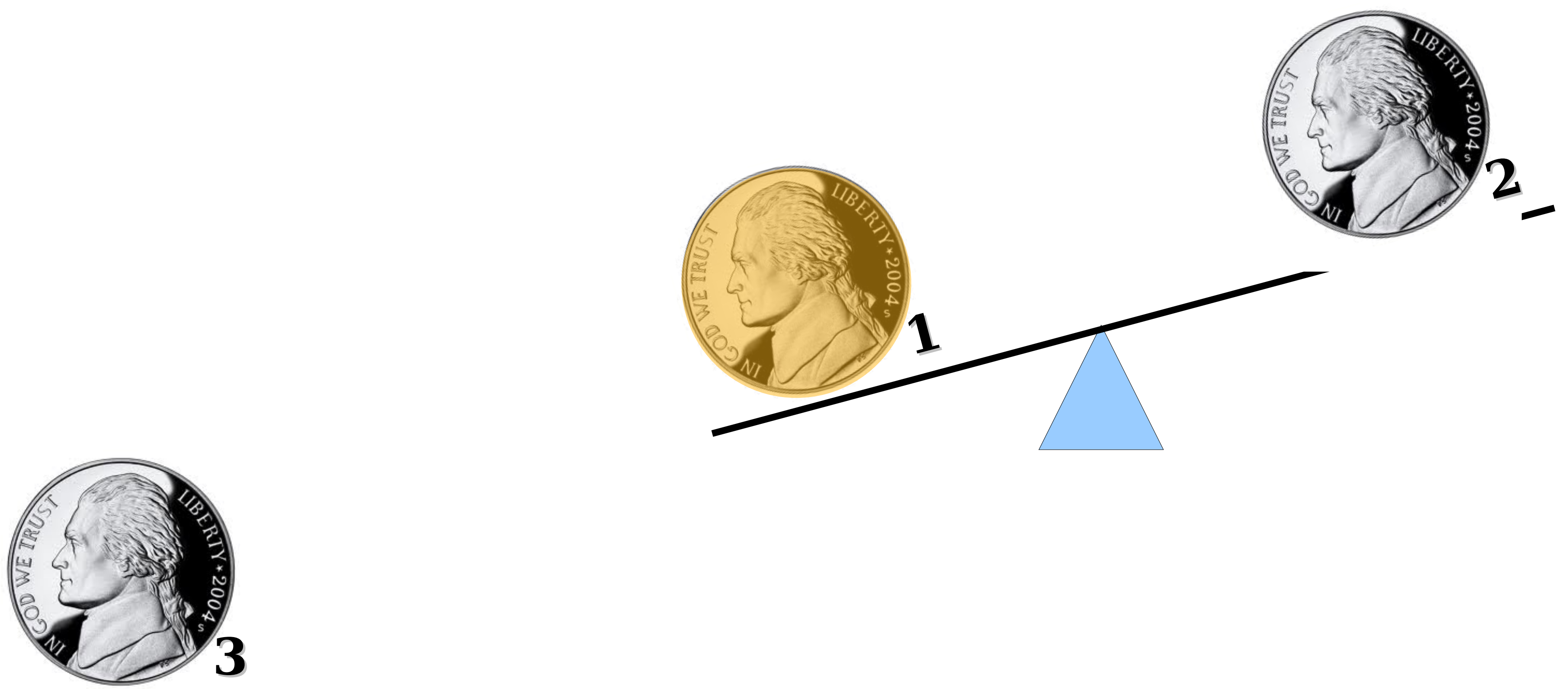
Finding the Counterfeit Coin



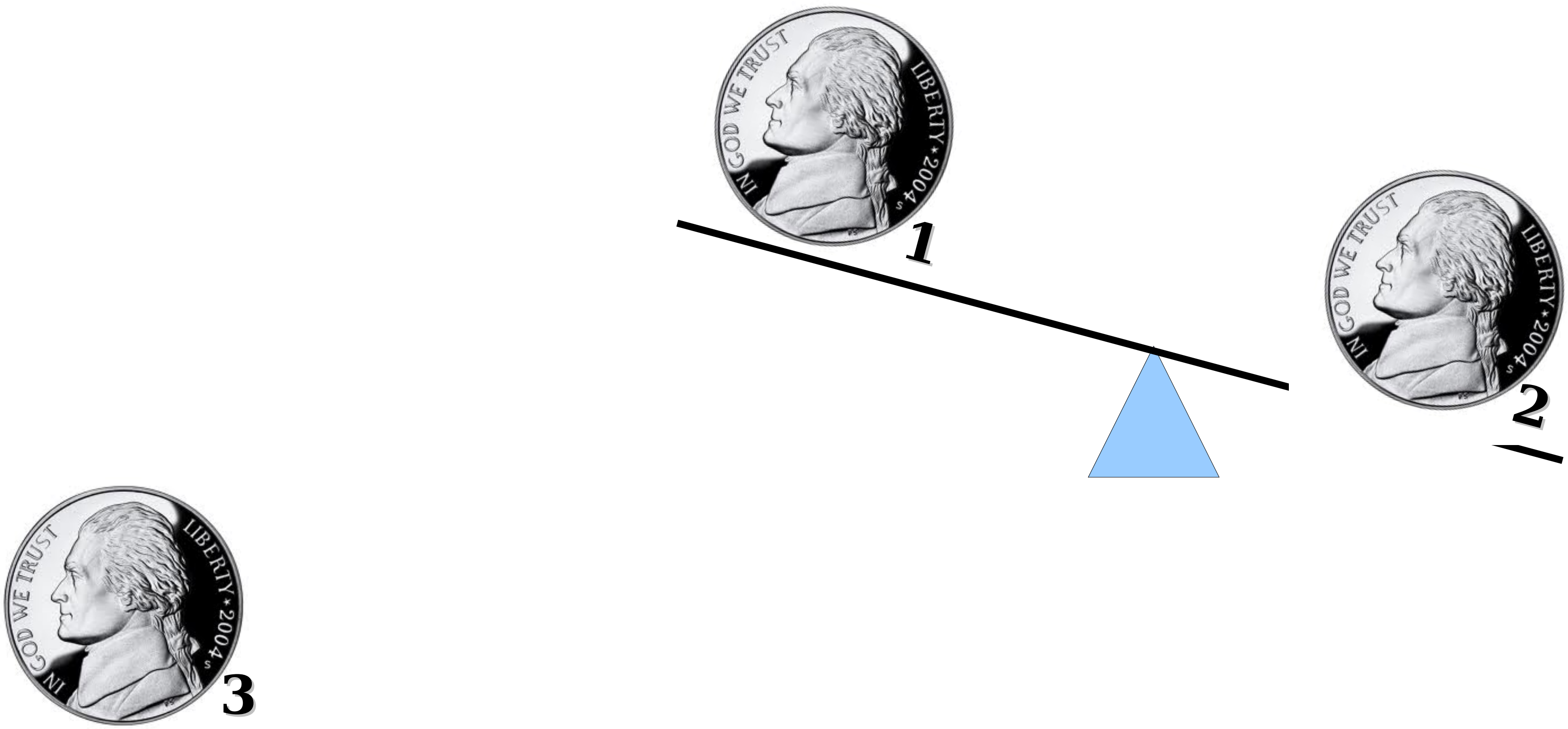
Finding the Counterfeit Coin



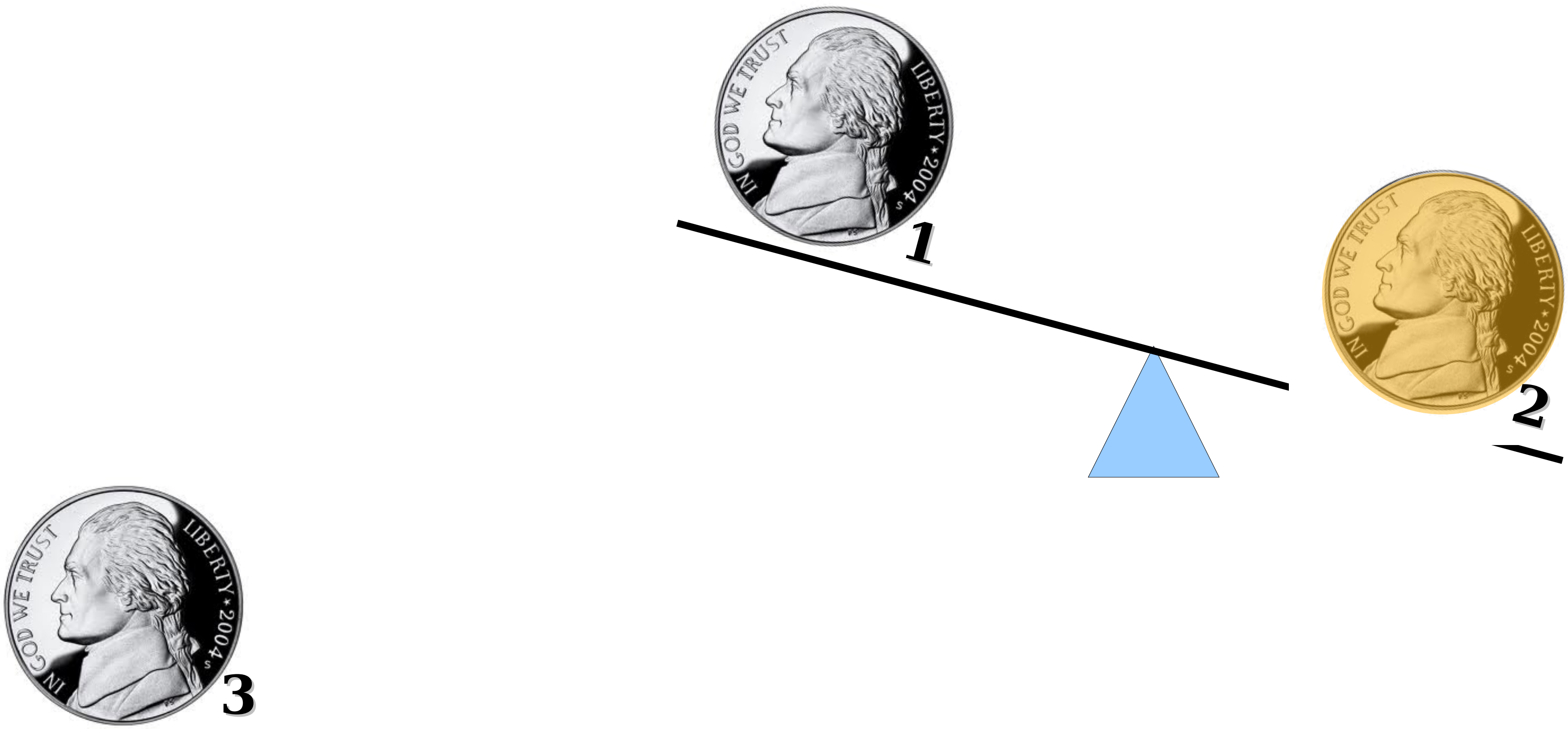
Finding the Counterfeit Coin



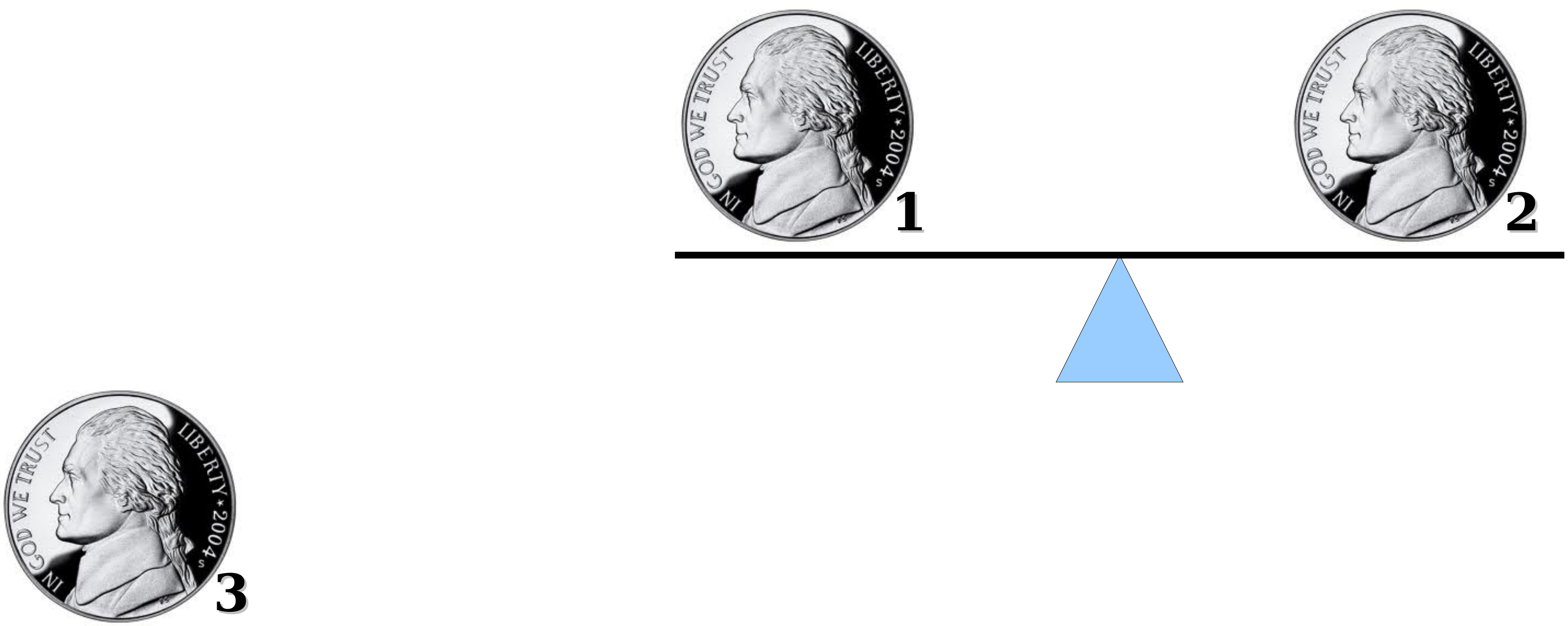
Finding the Counterfeit Coin



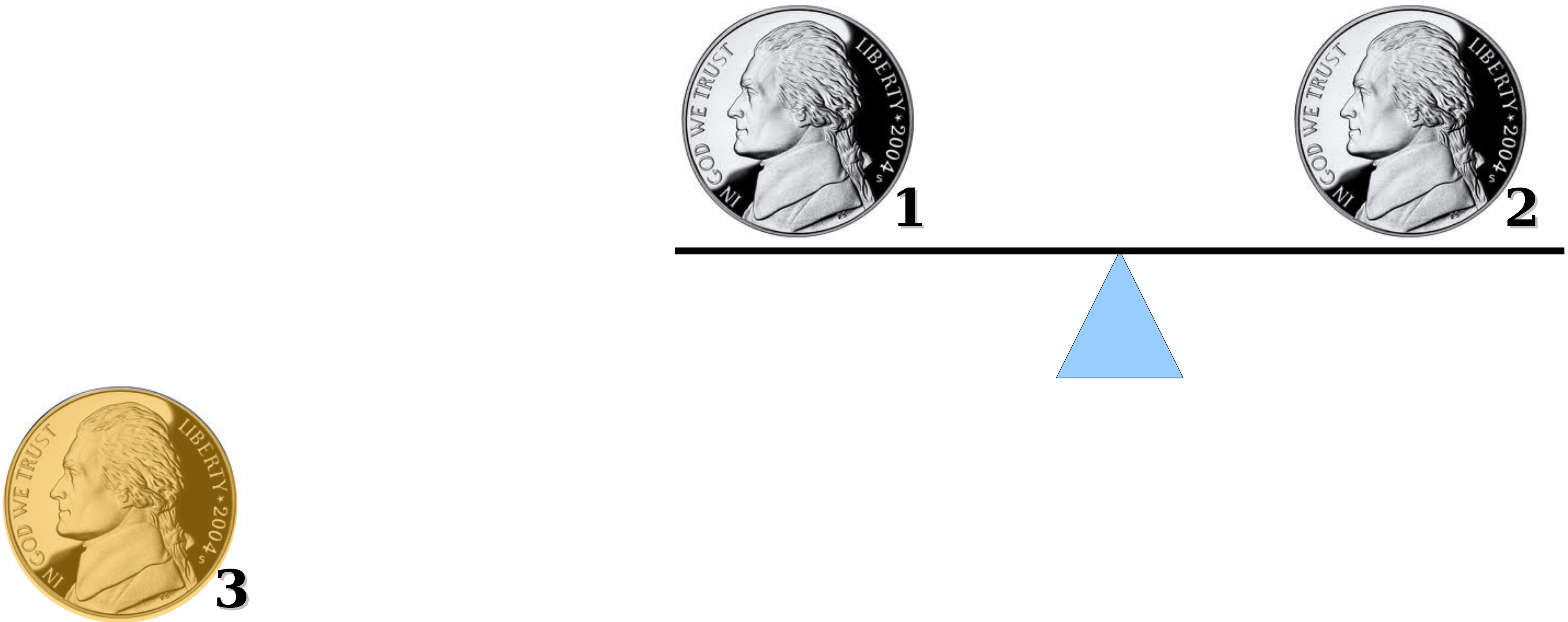
Finding the Counterfeit Coin



Finding the Counterfeit Coin



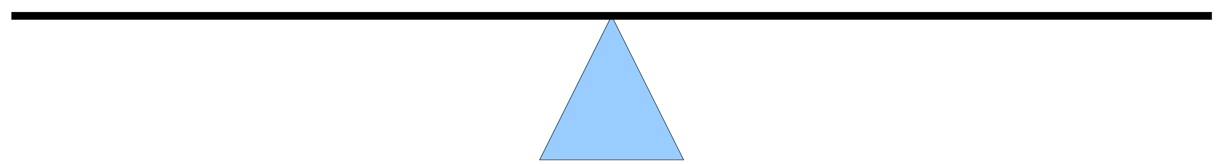
Finding the Counterfeit Coin



A Harder Problem

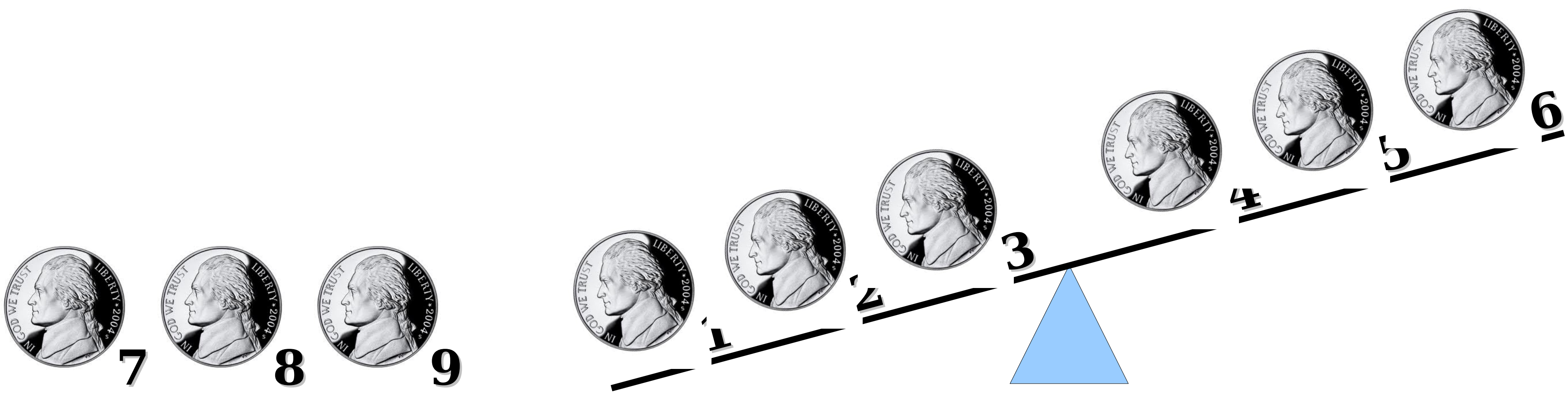
- You are given a set of ***nine*** seemingly identical coins, eight of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only ***two*** weighings on the balance, find the counterfeit coin.

Finding the Counterfeit Coin

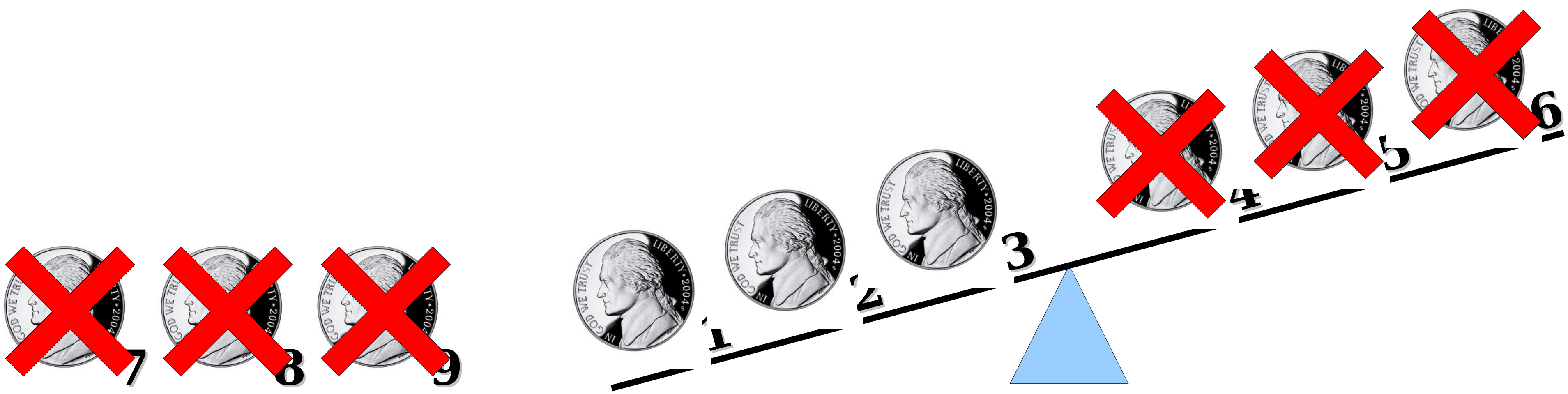


Finding the Counterfeit Coin

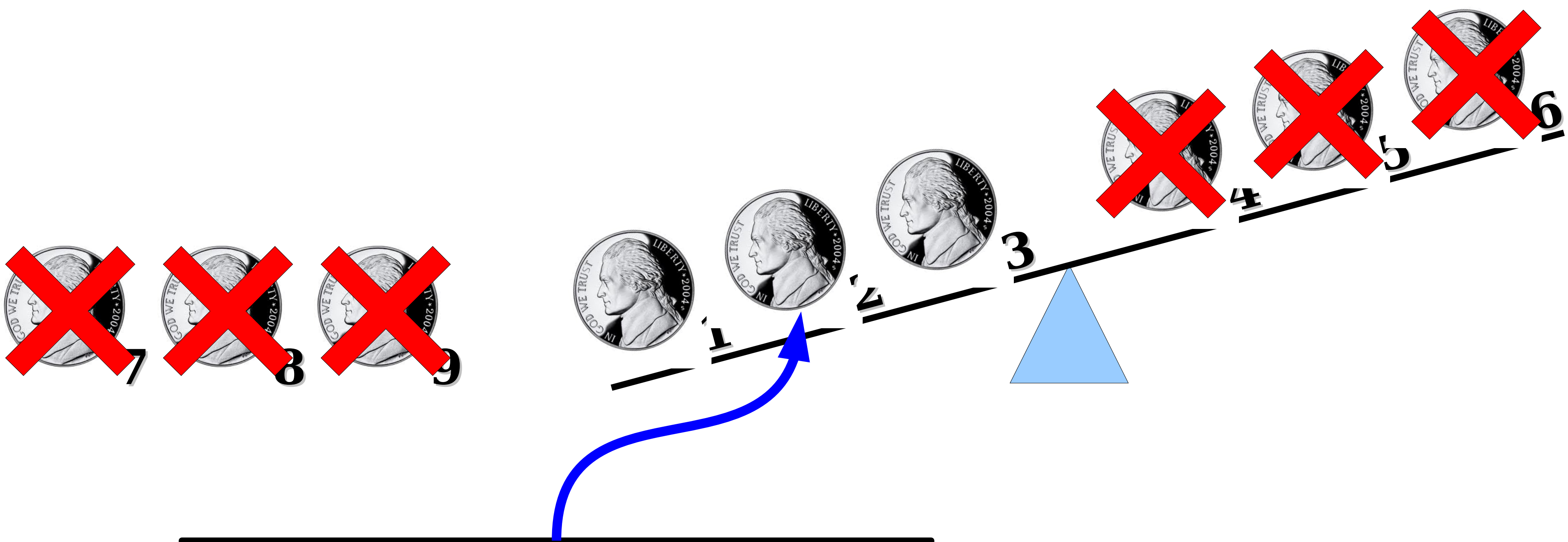
Finding the Counterfeit Coin



Finding the Counterfeit Coin



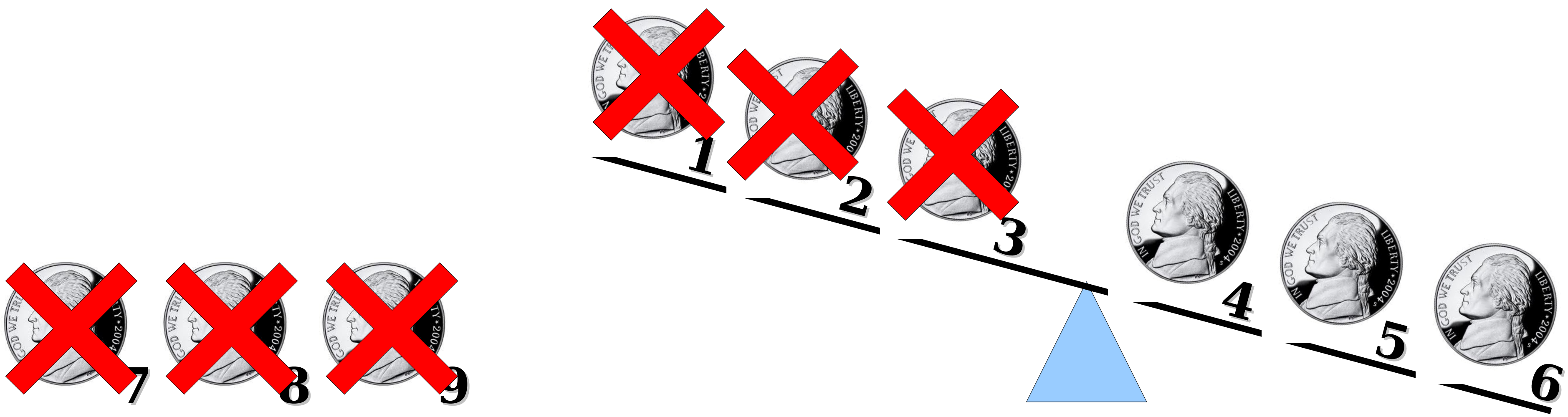
Finding the Counterfeit Coin



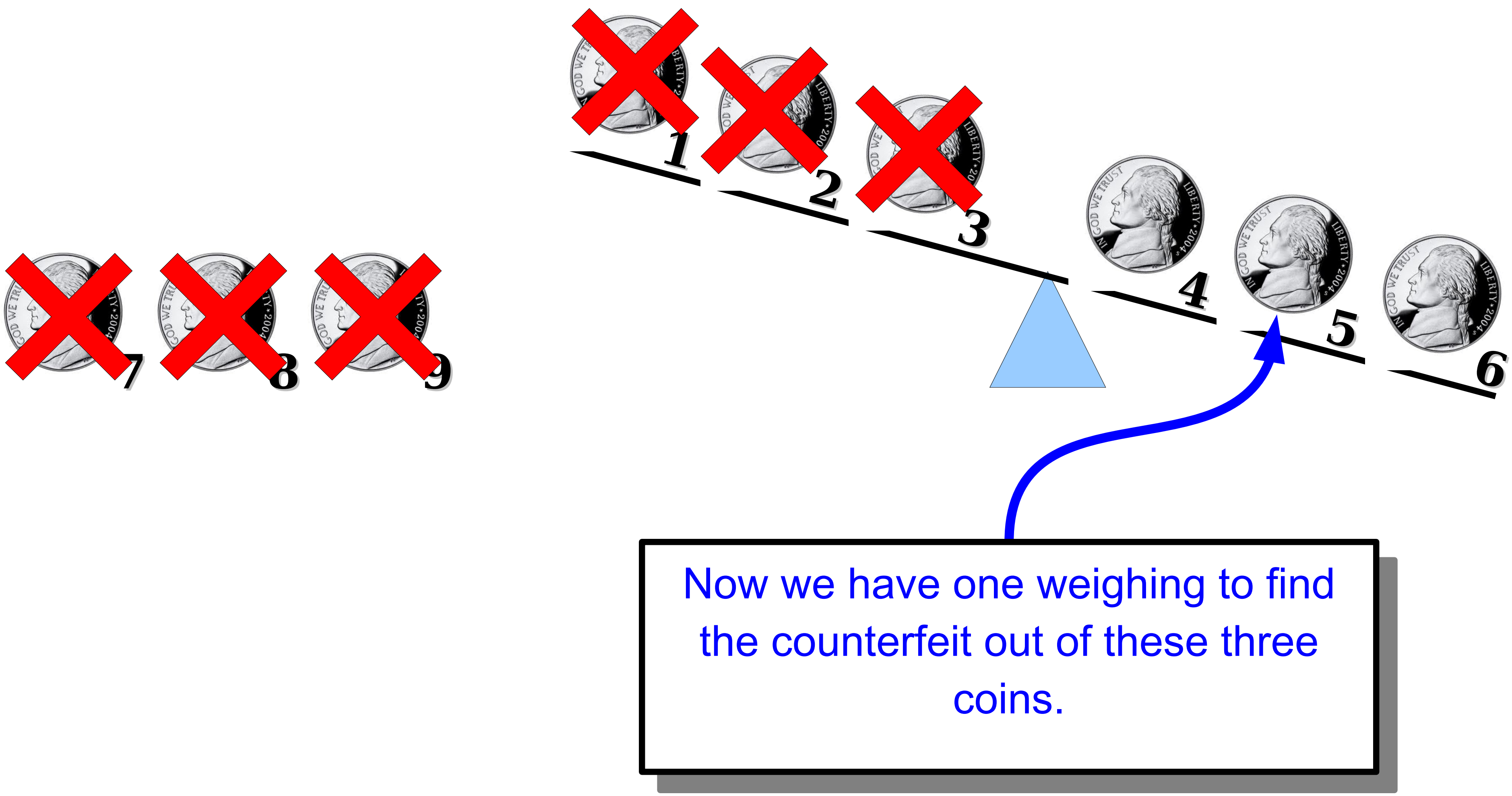
Now we have one weighing to find the counterfeit out of these three coins.

Finding the Counterfeit Coin

Finding the Counterfeit Coin

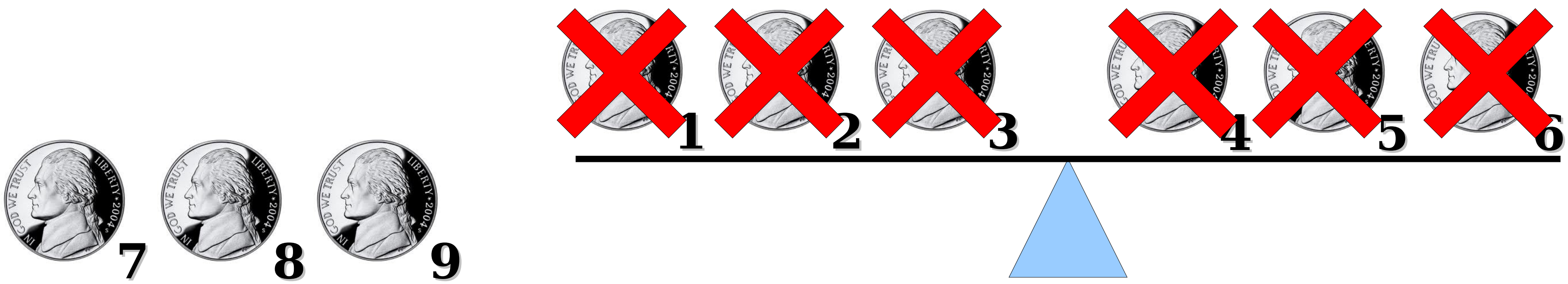


Finding the Counterfeit Coin

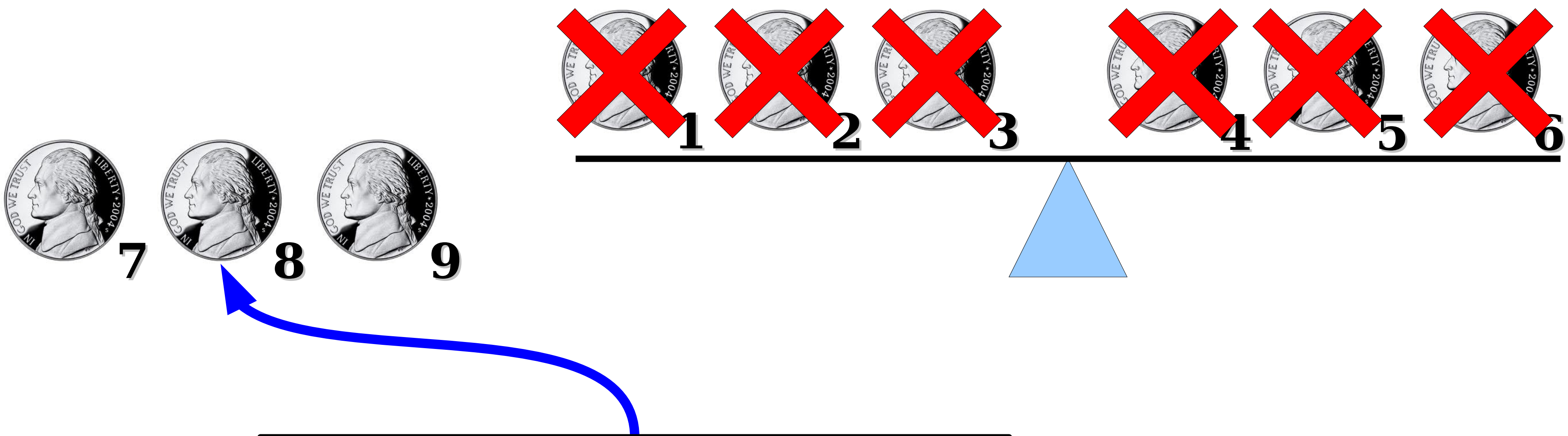


Finding the Counterfeit Coin

Finding the Counterfeit Coin



Finding the Counterfeit Coin



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

Can we generalize this?

Can we generalize this?

1 coin : _?_ weighings
3 coins: 1 weighing
9 coins: 2 weighings

Quick check: What is the pattern? The number of weighings we need to find a counterfeit in 3^n coins is…

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

$1, 3, 9 = 3^0, 3^1, 3^2$

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.

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.

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.

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.

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.

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

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.

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.

In a proof by induction, we need to prove that

- ☐ $P(0)$ is true
- ☐ For all k $\in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

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.

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.

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.

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

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.

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.

In a proof by induction, we need to prove that

- ✓ $P(0)$ is true
- ☐ For all k $\in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, so we can find the heavier of 3^k coins in k weighings.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

The goal of this step is to prove

"For all k ∈ $\mathbb{N}$, 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: 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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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

Theorem: 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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 exact … rest,
that c … ce.

We'll use i … om which
the theore …

As our bas … we have
a set of 3^0 … find that
coin with z … one coin,
it's vacuously heavier than all the others, and no weighings are needed.

Here, we use our **inductive hypothesis** (the assumption that $P(k)$ is true) to solve this simpler version of the overall problem.

For the inductive step, suppose $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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.

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 wi … n,
it's vac … ed.

For the … so
we can … :
that we

In a proof by induction, we need to prove that

✓ $P(0)$ is true

✓ For all k $\in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

Suppos … e
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.

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 $P(k)$ is true for some arbitrary $k \in \mathbb{N}$, 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

- Here's some nifty variants of this problem that you can work through:
  - 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?
  - Can you find the counterfeit out of a group of more than 3^k coins with k weighings?
  - Can you find the counterfeit out of any group of at most 3^k coins with k weighings?

How Not To Induct

Something's Wrong...

Something's Wrong...

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

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."

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.

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 arbitrary $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

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

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 arbitrary $k \in \mathbb{N}$ 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}.

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 arbitrary $k \in \mathbb{N}$ 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

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

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 arbitrary $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

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

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

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

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 arbitrary $k \in \mathbb{N}$ 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

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

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 arbitrary $k \in \mathbb{N}$ 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

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

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 arbitrary $k \in \mathbb{N}$ 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 Wro

Quick check: Whe

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 arbitrary $k \in \mathbb{N}$ that $P(k)$ holds, meaning that

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

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

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

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 arbitrary $k \in \mathbb{N}$ 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 prove the base case!

Otherwise, your proof is incomplete!

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 arbitrary $k \in \mathbb{N}$ 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. ■

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 arbitrary $k \in \mathbb{N}$ 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. ■

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 arbitrary $k \in \mathbb{N}$ 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 ... that

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

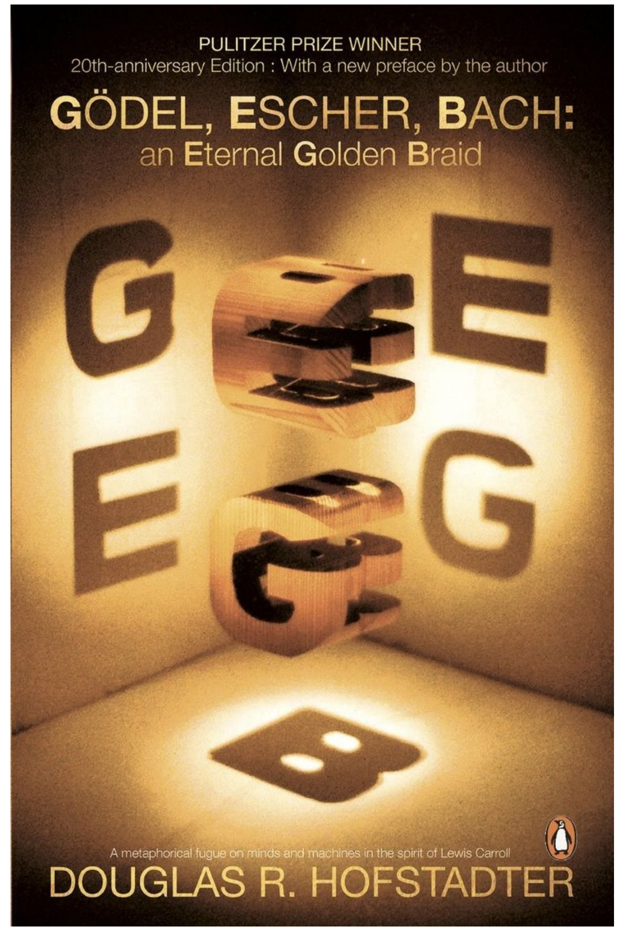
You can prove ***anything*** from a faulty assumption. This is called the **principle of explosion**.

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

The MU Puzzle

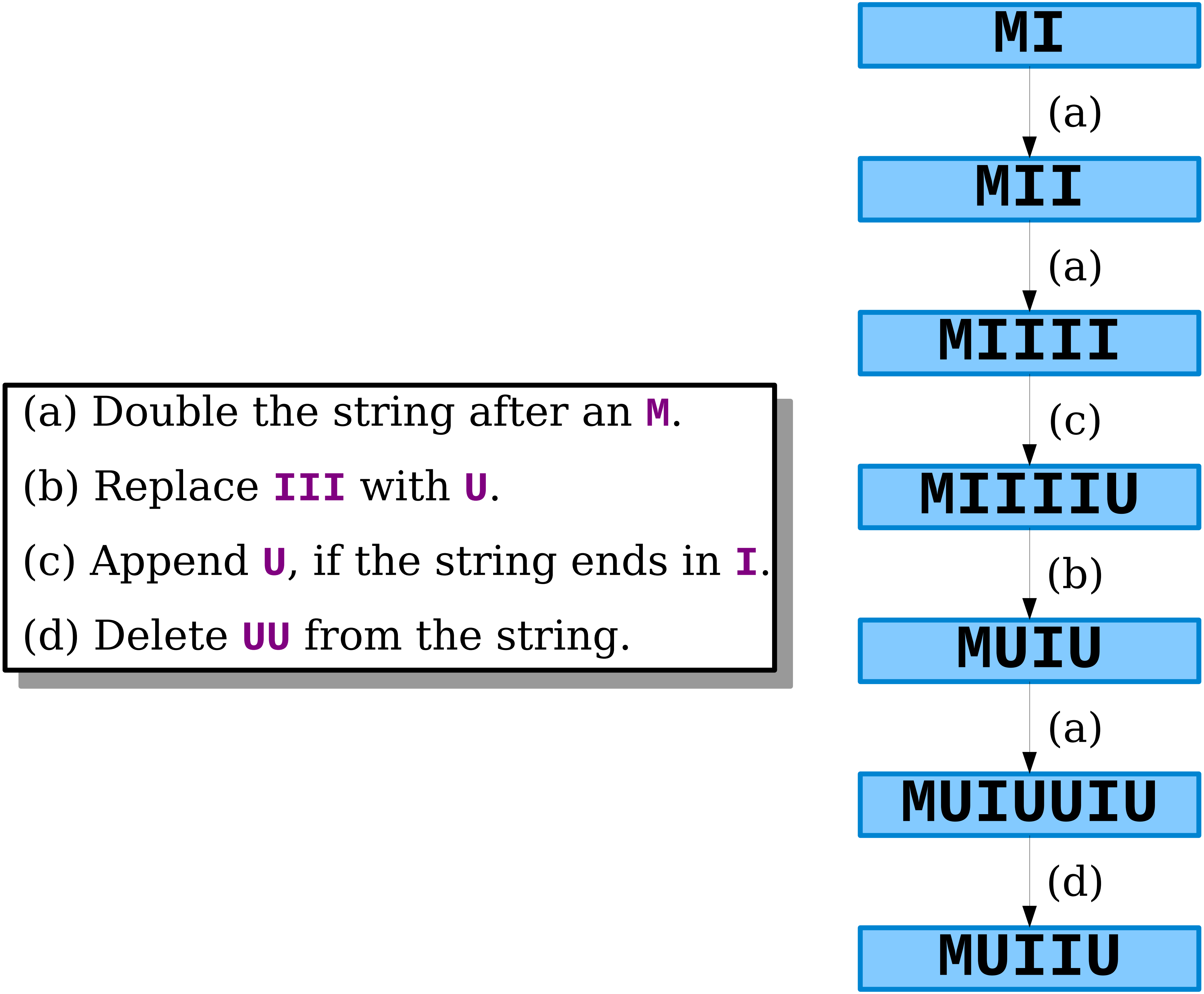
Gödel, Escher Bach: An Eternal Golden Braid

- Douglas Hofstadter, cognitive scientist at the University of Indiana, wrote this Pulitzer-Prize-winning mind trip of a book.
- It's a great read after you've finished CS103 – you'll see so many of the ideas we'll cover presented in a totally different way!



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`**?


MI
(a)
MII
(a)
MIIII
(c)
MIIIIU
(b)
MUIU
(a)
MUIUUIU
(d)
MUIIU
(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.

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

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."

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.

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.

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.

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.

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 arbitrary $k \in \mathbb{N}$.

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 arbitrary $k \in \mathbb{N}$. We'll prove $P(k+1)$ is also true.

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 arbitrary $k \in \mathbb{N}$. We'll prove $P(k+1)$ is also true. Consider any sequence of $k+1$ moves.

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 arbitrary $k \in \mathbb{N}$. 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.

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 arbitrary $k \in \mathbb{N}$. 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.

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 arbitrary $k \in \mathbb{N}$. 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 $k+1^{st}$ move:

Case 1: Double the string after the **M**.

Case 2: Replace **III** with **U**.

Case 3: Either append **U** or delete **UU**.

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 arbitrary $k \in \mathbb{N}$. 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 $k+1^{st}$ 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`**.

Case 3: Either append **`U`** or delete **`UU`**.

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 arbitrary $k \in \mathbb{N}$. 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 $k+1^{st}$ 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**.

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 on e isn't a multiple of three, $P(0)$ is true.

For our inductive step, suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$. 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 $k+1^{st}$ 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.

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 arbitrary $k \in \mathbb{N}$. 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.

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 arbitrary $k \in \mathbb{N}$. 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 $k+1^{st}$ 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.

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 arbitrary $k \in \mathbb{N}$. 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 $k+1^{st}$ 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.