CS103
Winter 2025

Lecture 12:

Mathematical Induction

Part 1 of 2

Okay, let’s kick off our exploration of today’s material with some kinetic activity.

Let’s do the wave!

The Wave

- If done properly, everyone will eventually end up joining in.
- Why is that? There are two primary components:
  - 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…

$$\boldsymbol{P(0)} \textbf{ is true}$$

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.

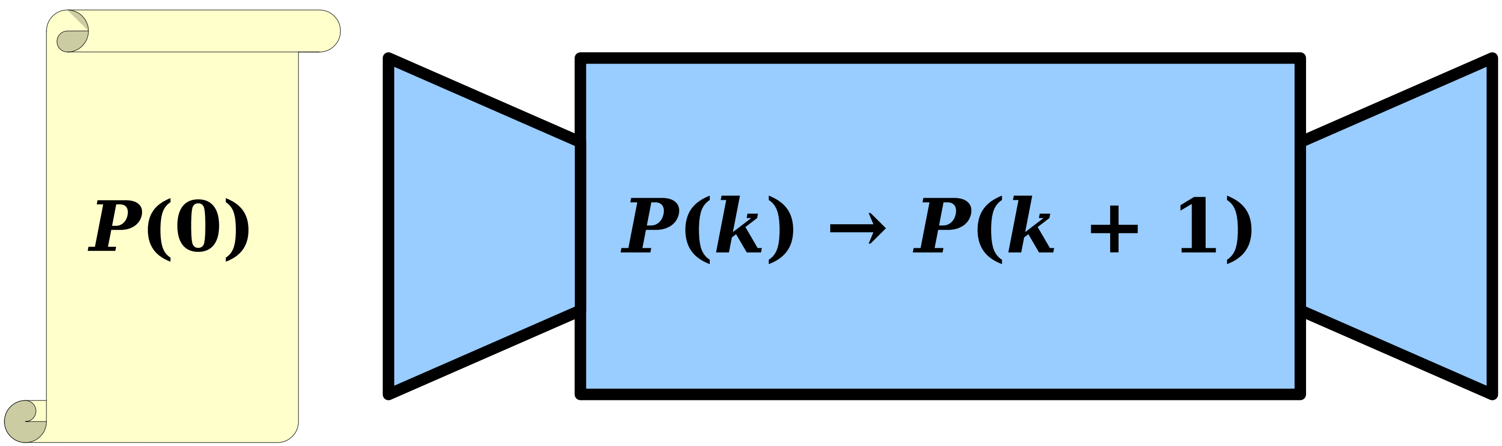
Induction, Intuitively

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

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

- 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



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*** or the ***base case***.
  - Prove that if $P(k)$ is true, then $P(k+1)$ is true.
    - This is called the ***inductive step***.
    - 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

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

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

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

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

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

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

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

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

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

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

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

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

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

A Quick Aside

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

Structuring a Proof by Induction

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

The Counterfeit Coin Problem

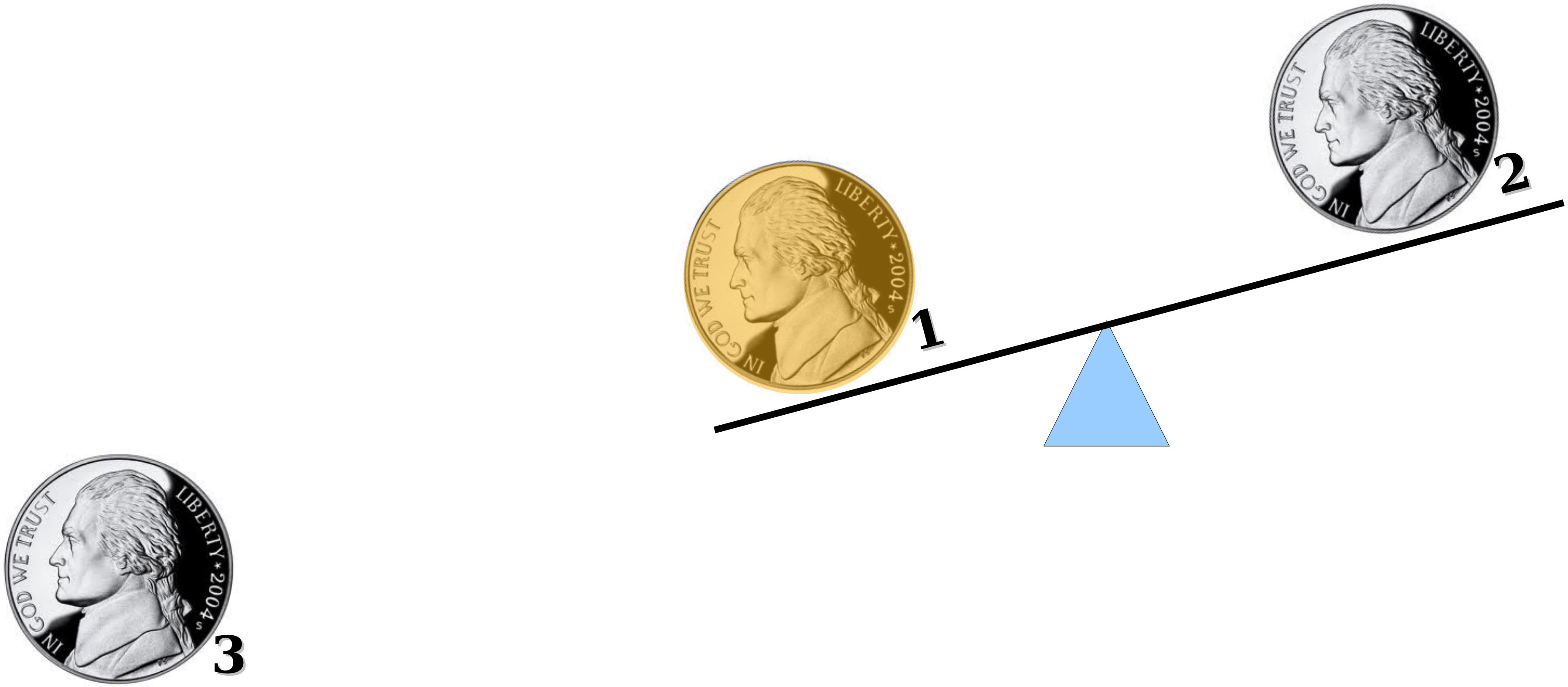
Problem Statement

- 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.

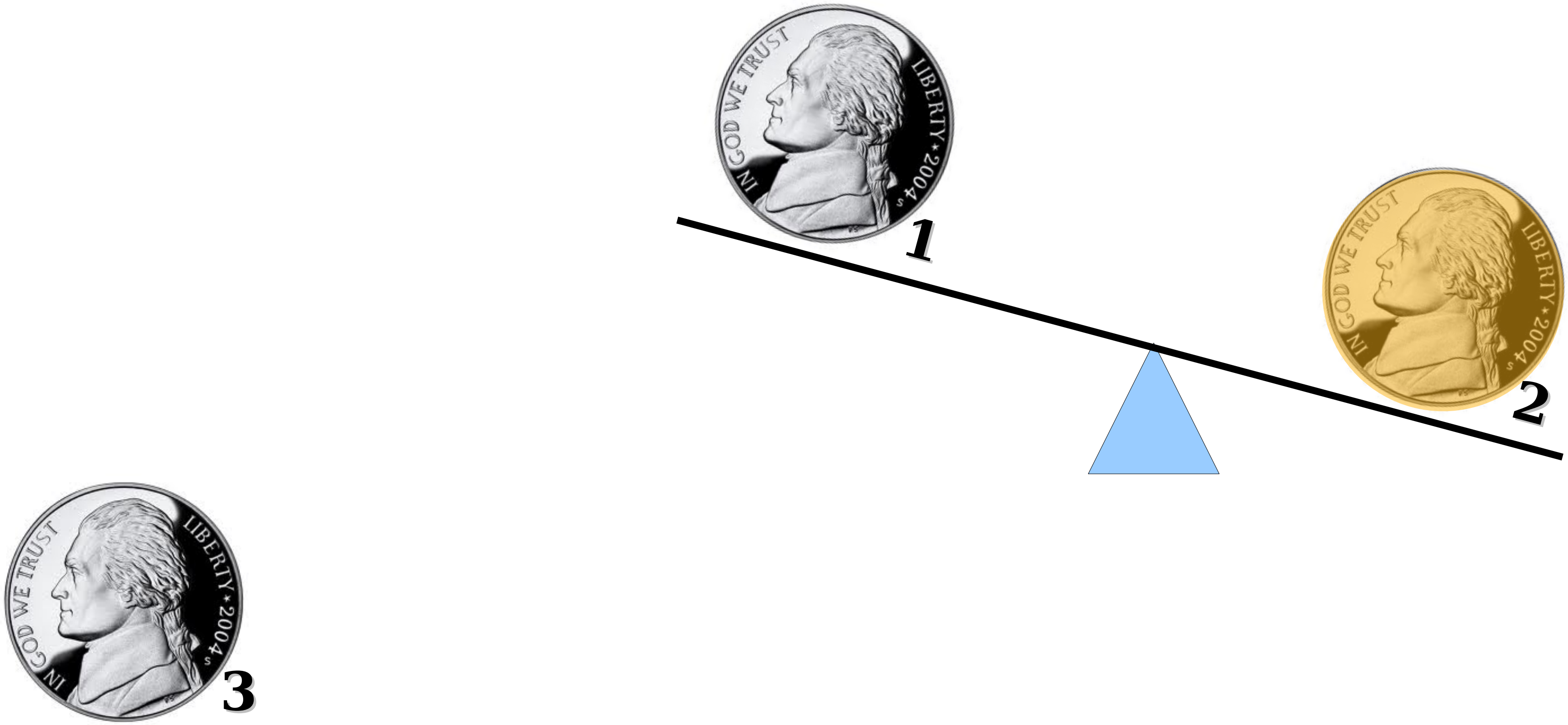
How?

Answer at
https://cs103.stanford.edu/pollev

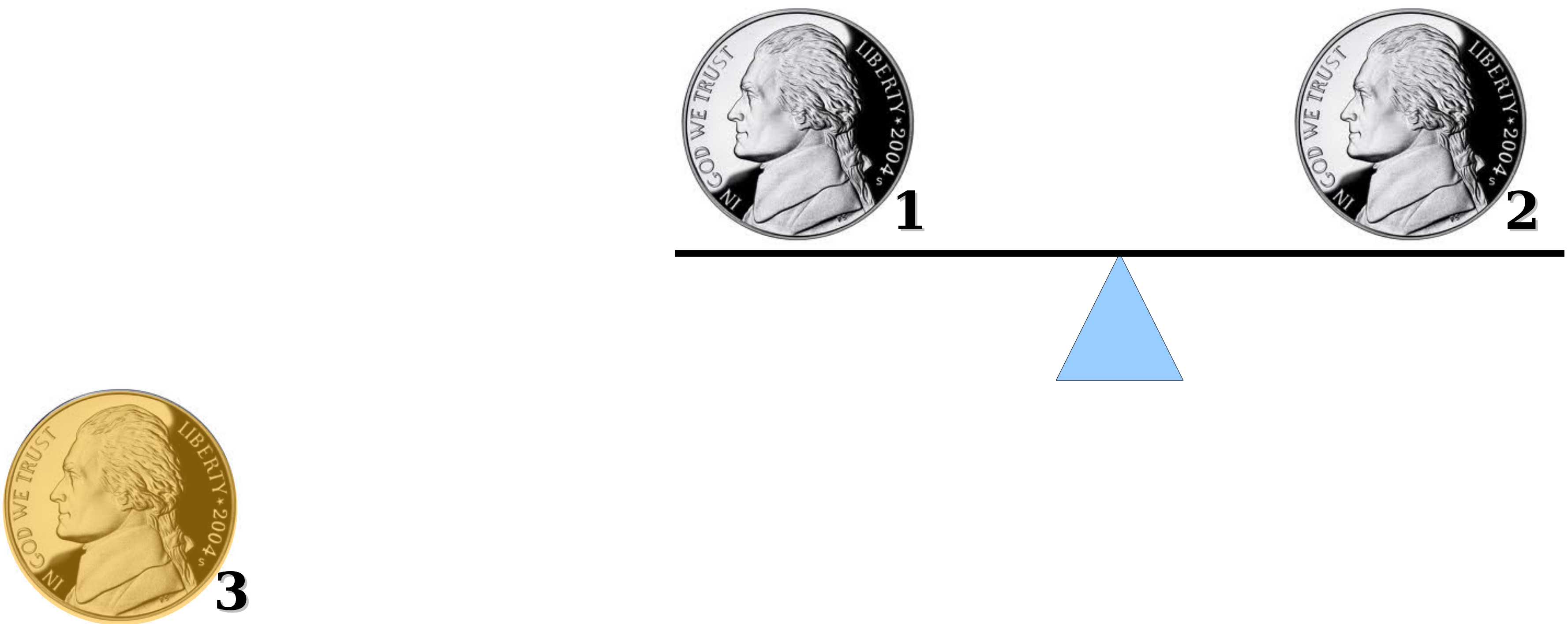
Finding the Counterfeit Coin



Finding the Counterfeit Coin



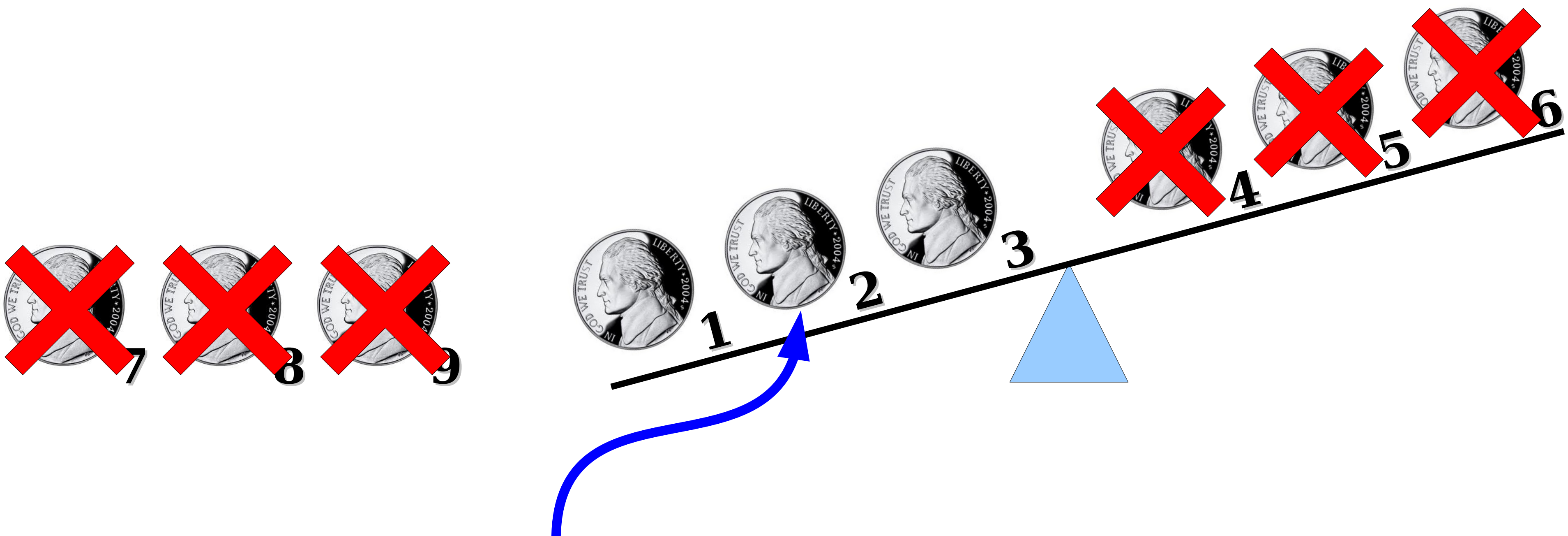
Finding the Counterfeit Coin



A Harder Problem

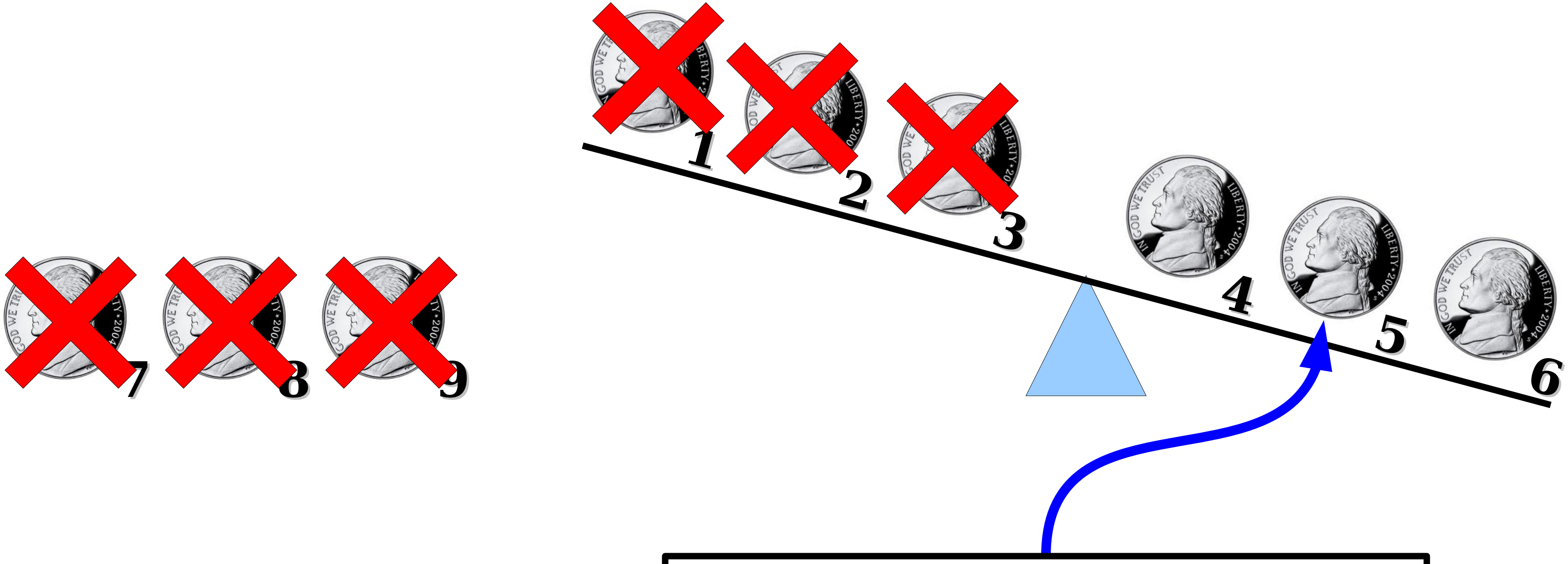
- You are given a set of ***nine*** seemingly identical coins, eight of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only ***two*** weighings on the balance, find the counterfeit coin.

Finding the Counterfeit Coin



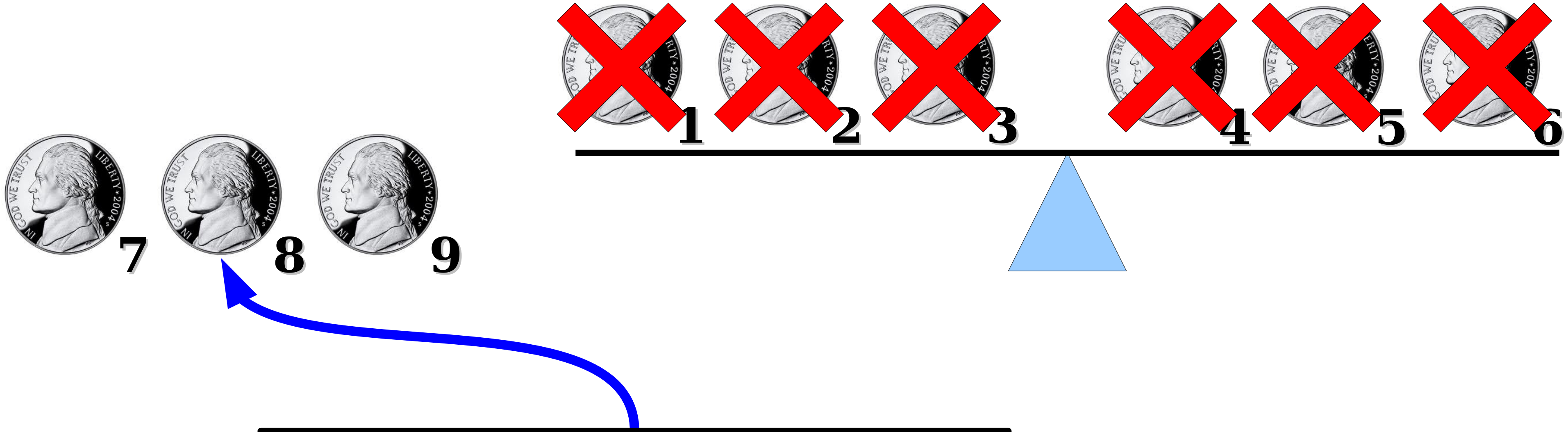
Now we have one weighing to find the counterfeit out of these three coins.

Finding the Counterfeit Coin



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

Finding the Counterfeit Coin



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

Can we generalize this?

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.

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?

From Cynthia’s Slide Deck

- See today’s lecture video for two additional examples not included in this slide deck:
  - “**Something’s Wrong**” – An example of how induction can be used to “prove” things that are untrue if we’re not careful to include all required components (the base case and the inductive step).
  - “**The MU Puzzle**” – Another example of an inductive proof revolving around string mutation operations.
  - Comments about proofs on algorithms.

Generalizing Induction

- When doing a proof by induction,
  - feel free to use multiple base cases [**see appendix!**], and
  - feel free to take steps of sizes other than one.
- If you do, make sure that…
  - … you actually need all your base cases. Avoid redundant base cases that are already covered by a mix of other base cases and your inductive step.
  - … you cover all the numbers you need to cover. Trace out your reasoning and make sure all the numbers you need to cover really are covered.
- As with a proof by cases, you don’t need to separately prove you’ve covered all the options. We trust you.

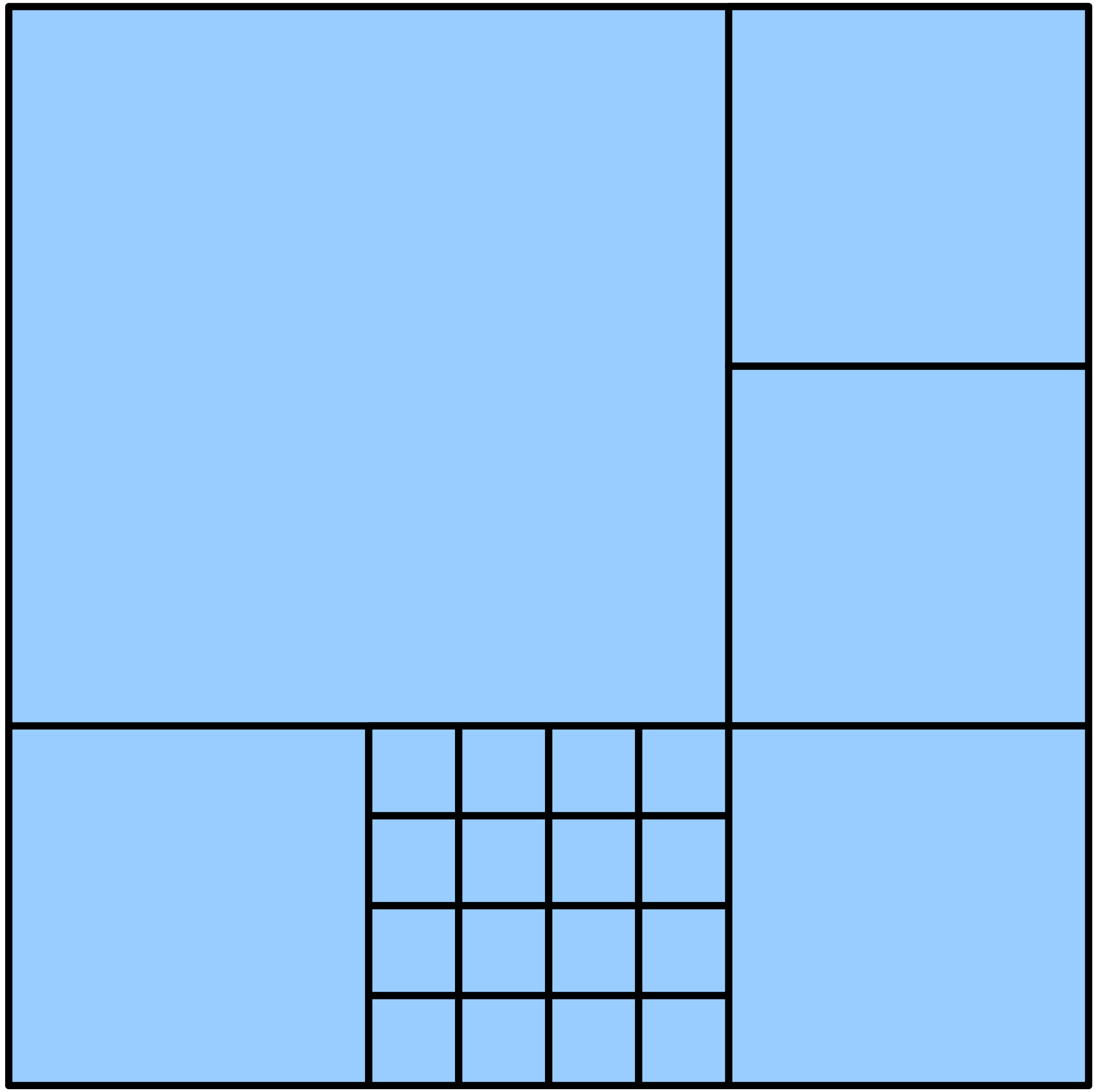
Next Time

- ***"Build Up" vs "Build Down"***
  - A subtle but key point in induction proofs.
- ***Complete Induction***
  - Expanding our inductive hypothesis.

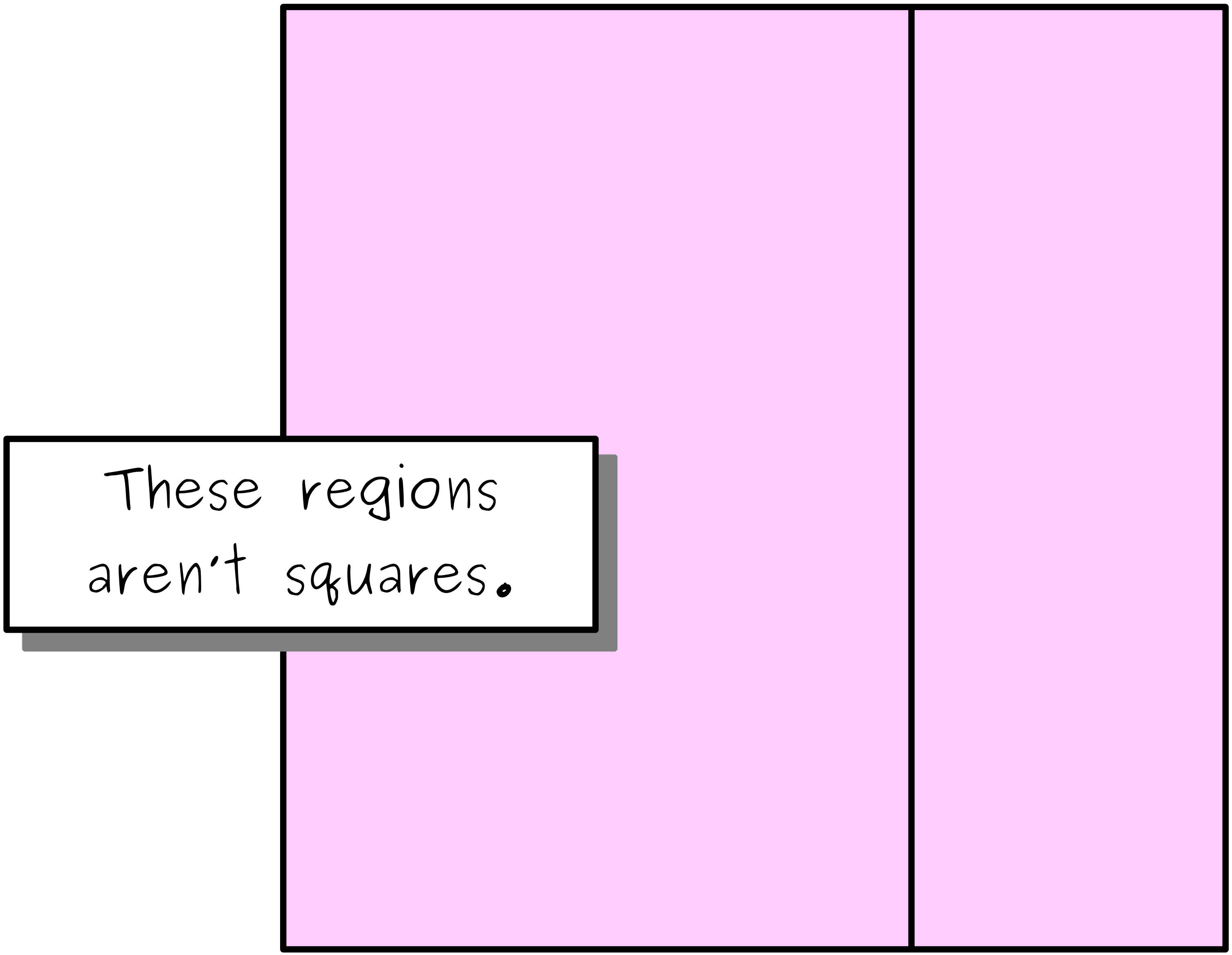
Appendix

Variations on Induction

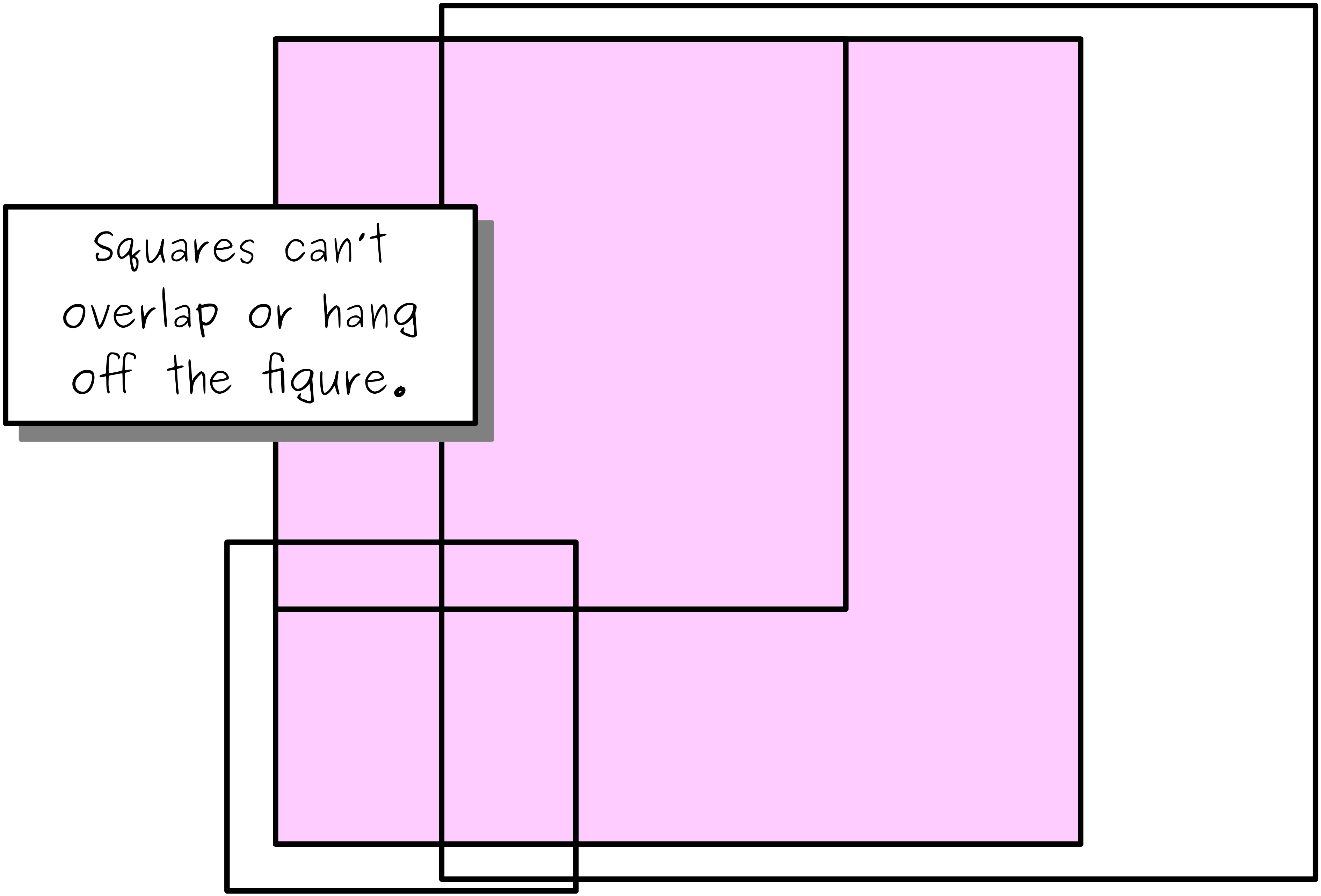
Subdividing a Square



Subdividing a Square



Subdividing a Square

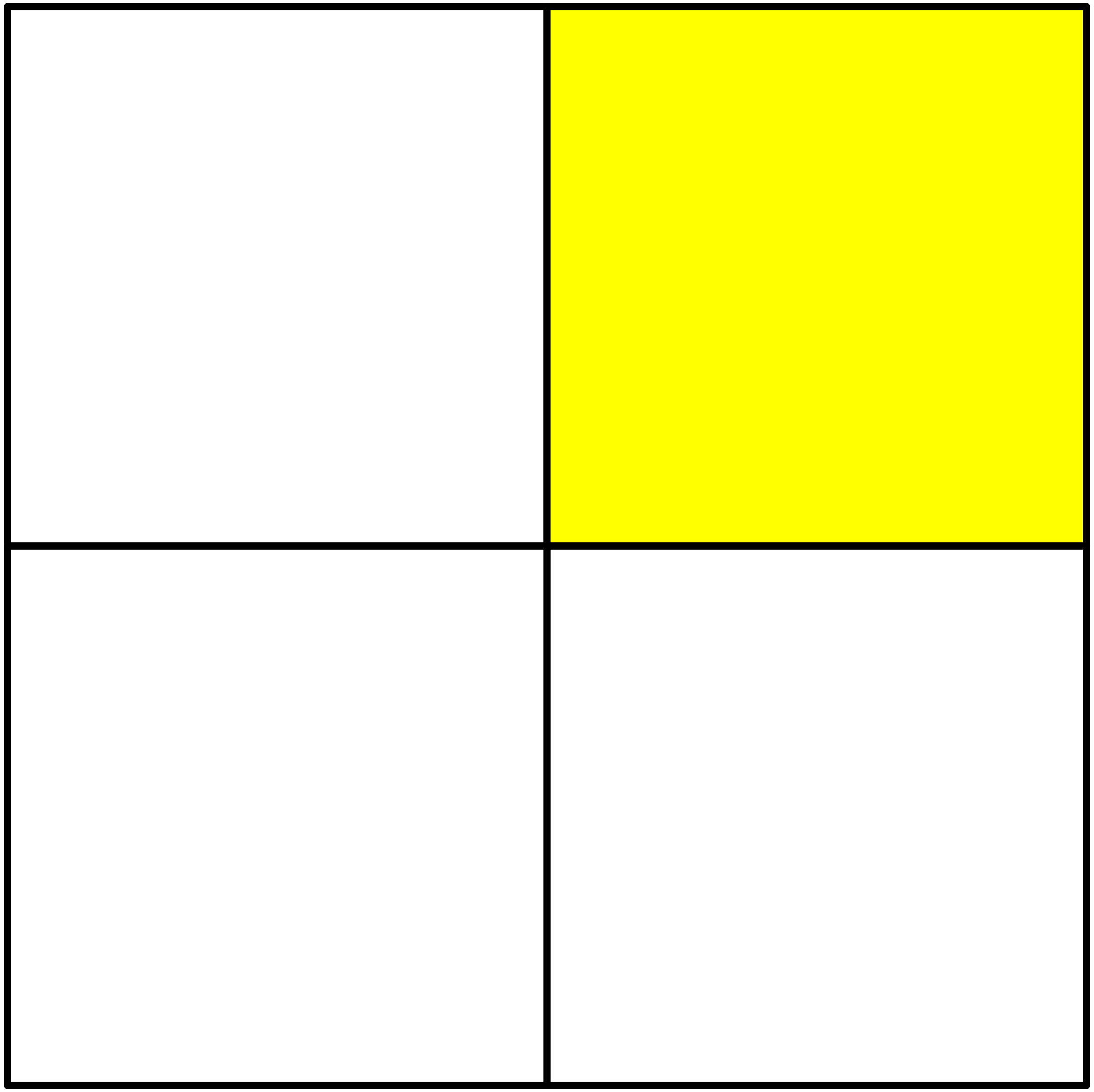


For what values of n can a square be subdivided into n squares?

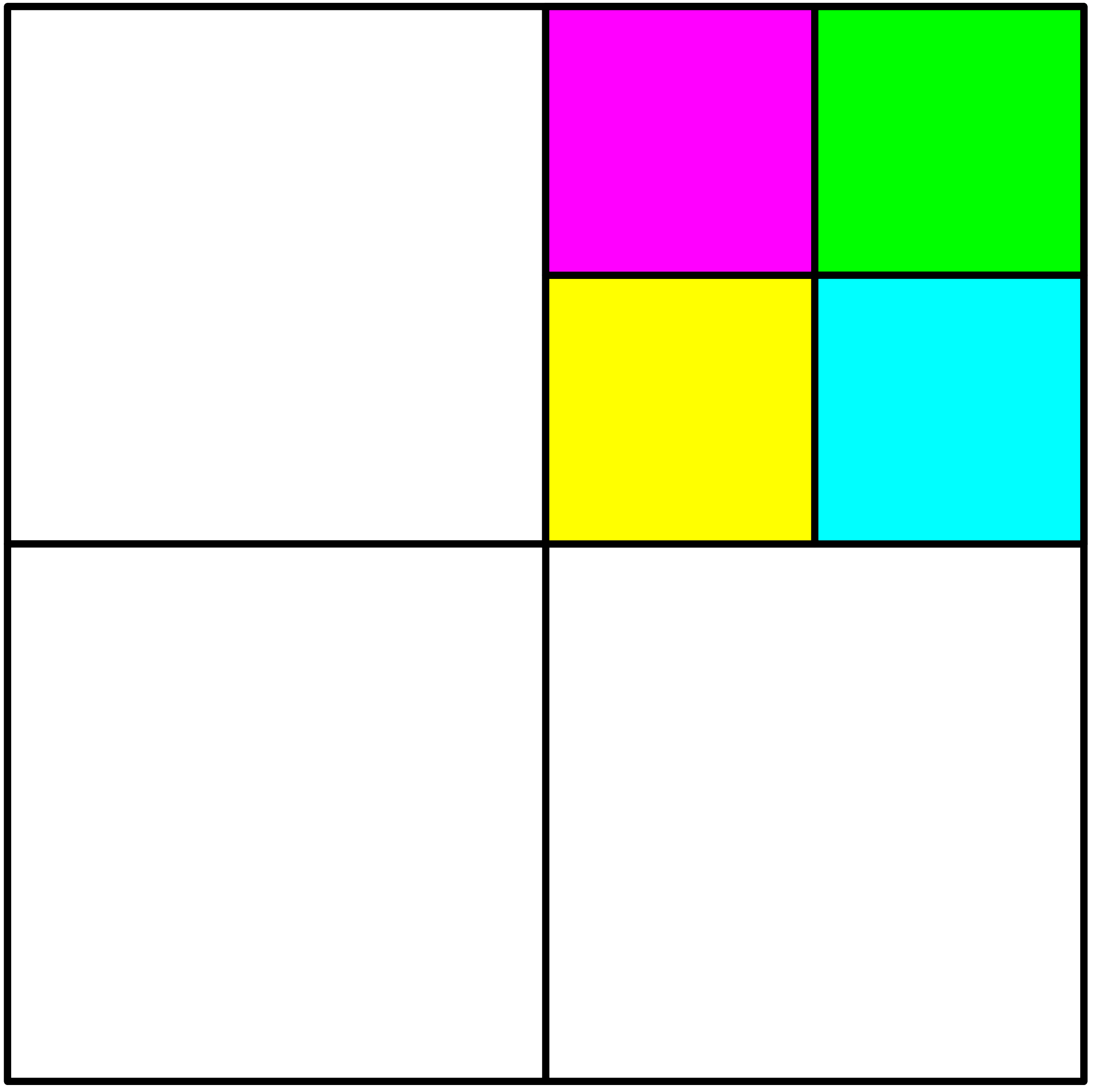
Try out some numbers n from 1 to 12. Which values of n work?

Answer at ***https://cs103.stanford.edu/pollev***

An Insight



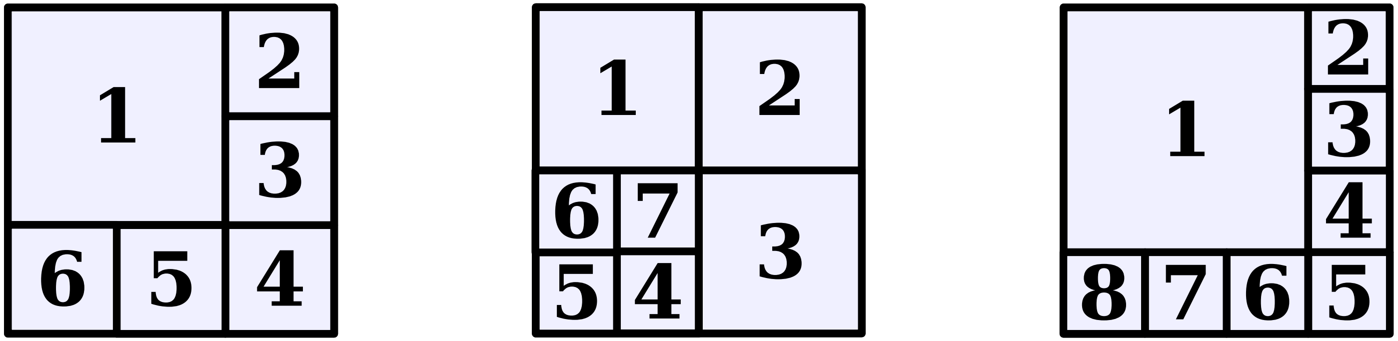
An Insight



Theorem: For any $n \geq 6$, there is a way to subdivide a square into n smaller squares.

Proof: Let $P(n)$ be the statement "there is a way to subdivide a square into n smaller squares." We will prove by induction that $P(n)$ holds for all $n \geq 6$, from which the theorem follows.

As our base cases, we prove $P(6)$, $P(7)$, and $P(8)$, that a square can be subdivided into 6, 7, and 8 squares. This is shown here:



For the inductive step, assume that for some arbitrary $k \geq 6$ that $P(k)$ is true and that there is a way to subdivide a square into k squares. We prove $P(k+3)$, that there is a way to subdivide a square into $k+3$ squares. To see this, start by obtaining (via the inductive hypothesis) a subdivision of a square into k squares. Then, choose any of the squares and split it into four equal squares. This removes one of the k squares and adds four more, so there will be a net total of $k+3$ squares. Thus $P(k+3)$ holds, completing the induction. ■

More on Square Subdivisions

- There are a ton of interesting questions that come up when trying to subdivide a rectangle or square into smaller squares.
- In fact, one of the major players in early graph theory (William Tutte) got his start playing around with these problems.
- Good starting resource: this Numberphile video on ***Squaring the Square***.