

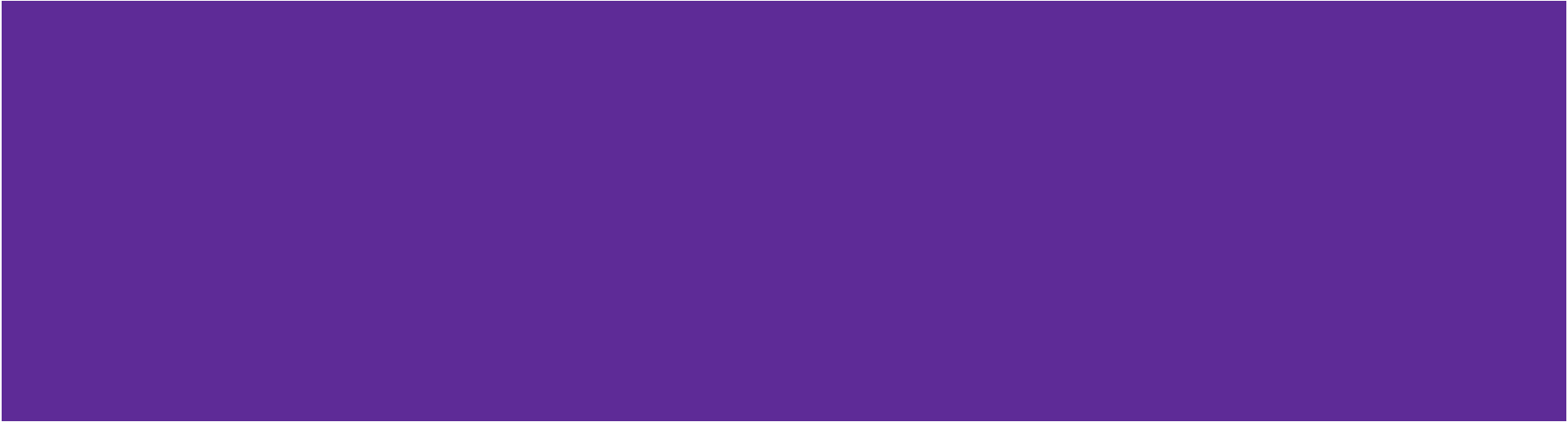
# CSE 311 Section 3

**Number Theory & Induction**

# Announcements & Reminders

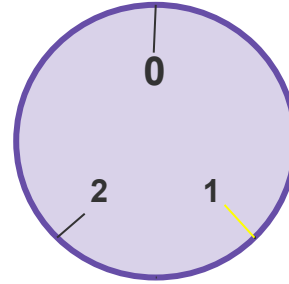
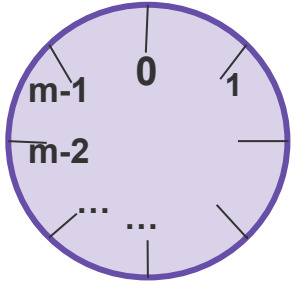
- HW3 due Friday @ 11:00PM on Gradescope
  - Use late days if you need to!
  - Make sure you tagged pages on gradescope correctly
- Quiz next Tuesday
  - Remember to review feedback in homework!

# Mod and Proving Divisibility



# $a \equiv b \pmod{m}$

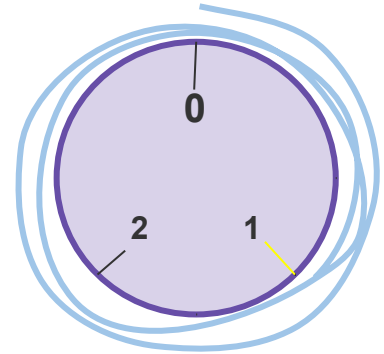
Imagine a clock with  $m$  numbers



$1 \pmod{3}$

$\equiv$

**VS**



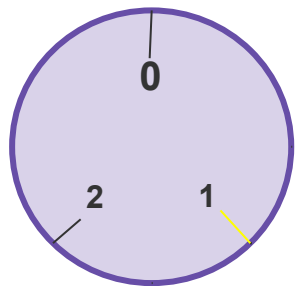
$10 \pmod{3}$

We can say that  $a \equiv b \pmod{m}$  where  $a$  and  $b$  are in the same position in the mod clock

$$1 \equiv 10 \pmod{3}$$

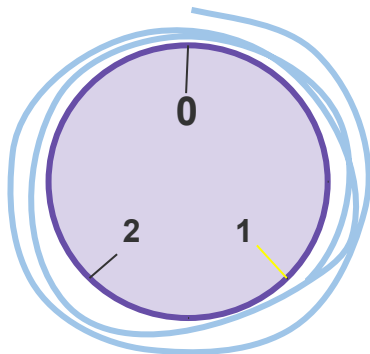
# Divides

What if we “unroll” this clock?



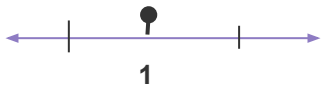
$1 \pmod{3}$

$\equiv$



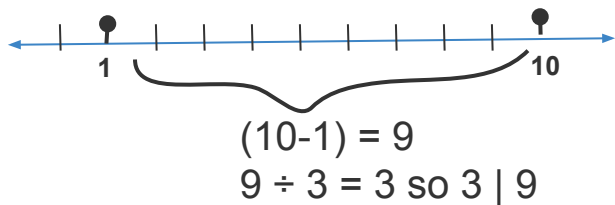
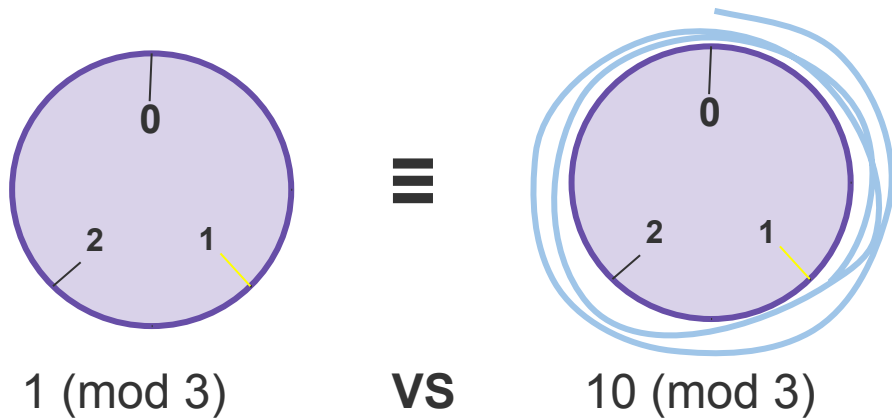
$10 \pmod{3}$

**VS**



# Divides

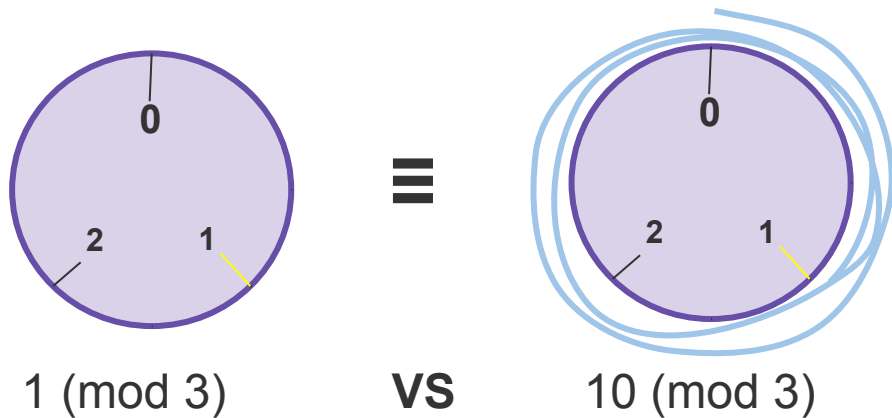
What if we “unroll” this clock?



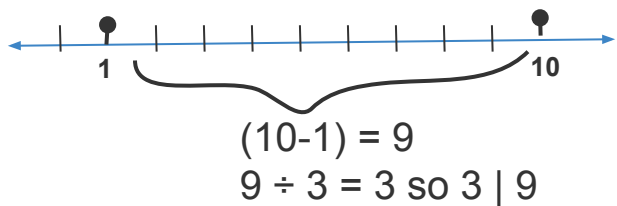
$3 \nmid 10$  and  $3 \nmid 1$  BUT  $3 \mid 9$

# Divides

What if we “unroll” this clock?



So  $m$  divides the difference between  $a$  and  $b$ !



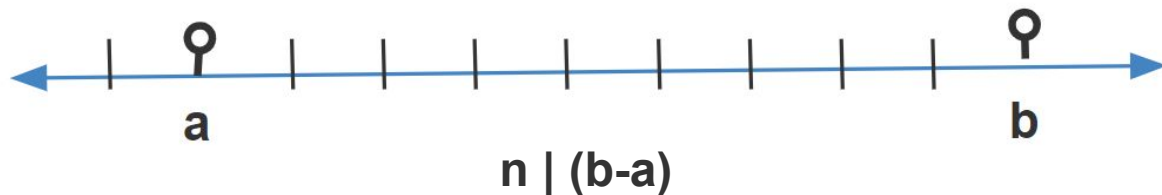
$3 \nmid 10$  and  $3 \nmid 1$  BUT  $3 \mid 9$

# Formalizing Mod and Divides

## Equivalence in modular arithmetic

Let  $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$  and  $n > 0$ .

We say  $a \equiv b \pmod{n}$  if and only if  $n \mid (b - a)$





# “Unwrapping”

*This expression is generally easier to deal with*

$$a \equiv b \pmod{n} \longleftrightarrow n \mid (b-a) \longleftrightarrow (b-a) = n * k$$

## Equivalence in modular arithmetic

Let  $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$  and  $n > 0$ .  
We say  $a \equiv b \pmod{n}$  if and only if  $n \mid (b - a)$

## Divides

For integers  $x, y$  we say  $x \mid y$  (“ $x$  divides  $y$ ”) iff there is an integer  $z$  such that  $xz = y$ .



**Divides is an operation that outputs true/false! It is not the same as divided by!**

# Extended Euclid



## Problem 2 – Extended Euclidean Algorithm

- a) Find the multiplicative inverse  $y$  of  $7 \bmod 33$ . That is, find  $y$  such that  $7y \equiv 1 \pmod{33}$ . You should use the extended Euclidean Algorithm. Your answer should be in the range  $0 \leq y < 33$ .

## Problem 2 – Extended Euclidean Algorithm

- a) Find the multiplicative inverse  $y$  of  $7 \bmod 33$ . That is, find  $y$  such that  $7y \equiv 1 \pmod{33}$ . You should use the extended Euclidean Algorithm. Your answer should be in the range  $0 \leq y < 33$ .

First, we find the gcd:

$$\begin{aligned} \gcd(33, 7) &= \gcd(7, 5) & 33 &= 4 \cdot 7 + 5 \\ &= \gcd(5, 2) & 7 &= 1 \cdot 5 + 2 \\ &= \gcd(2, 1) & 5 &= 2 \cdot 2 + 1 \\ &= \gcd(1, 0) & 2 &= 2 \cdot 1 + 0 \end{aligned}$$

## Problem 2 – Extended Euclidean Algorithm

- a) Find the multiplicative inverse  $y$  of  $7 \bmod 33$ . That is, find  $y$  such that  $7y \equiv 1 \pmod{33}$ . You should use the extended Euclidean Algorithm. Your answer should be in the range  $0 \leq y < 33$ .

First, we find the gcd:

$$\begin{aligned}\gcd(33, 7) &= \gcd(7, 5) \\ &= \gcd(5, 2) \\ &= \gcd(2, 1) \\ &= \gcd(1, 0)\end{aligned}$$

$$\begin{aligned}33 &= 4 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0\end{aligned}$$

Next, we re-arrange the equations by solving for the remainder:

$$\begin{aligned}1 &= 5 - 2 \cdot 2 \\ 2 &= 7 - 1 \cdot 5 \\ 5 &= 33 - 4 \cdot 7\end{aligned}$$

# Problem 2 – Extended Euclidean Algorithm

- a) Find the multiplicative inverse  $y$  of  $7 \bmod 33$ . That is, find  $y$  such that  $7y \equiv 1 \pmod{33}$ . You should use the extended Euclidean Algorithm. Your answer should be in the range  $0 \leq y < 33$ .

First, we find the gcd:

$$\begin{aligned}\gcd(33, 7) &= \gcd(7, 5) \\ &= \gcd(5, 2) \\ &= \gcd(2, 1) \\ &= \gcd(1, 0)\end{aligned}$$

$$\begin{aligned}33 &= 4 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0\end{aligned}$$

Next, we re-arrange the equations by solving for the remainder:

$$\begin{aligned}1 &= 5 - 2 \cdot 2 \\ 2 &= 7 - 1 \cdot 5 \\ 5 &= 33 - 4 \cdot 7\end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned}1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 33 + -14 \cdot 7\end{aligned}$$

# Problem 2 – Extended Euclidean Algorithm

- a) Find the multiplicative inverse  $y$  of  $7 \bmod 33$ . That is, find  $y$  such that  $7y \equiv 1 \pmod{33}$ . You should use the extended Euclidean Algorithm. Your answer should be in the range  $0 \leq y < 33$ .

First, we find the gcd:

$$\begin{aligned}\gcd(33, 7) &= \gcd(7, 5) \\ &= \gcd(5, 2) \\ &= \gcd(2, 1) \\ &= \gcd(1, 0)\end{aligned}$$

$$\begin{aligned}33 &= 4 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0\end{aligned}$$

Next, we re-arrange the equations by solving for the remainder:

$$\begin{aligned}1 &= 5 - 2 \cdot 2 \\ 2 &= 7 - 1 \cdot 5 \\ 5 &= 33 - 4 \cdot 7\end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned}1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 33 + -14 \cdot 7\end{aligned}$$

So,  $1 = 3 \cdot 33 + -14 \cdot 7$ . Thus,  $33 - 14 = 19$  is the multiplicative inverse of  $7 \bmod 33$

## Problem 2 – Extended Euclidean Algorithm

- a) Find the multiplicative inverse  $y$  of  $7 \bmod 33$ . That is, find  $y$  such that  $7y \equiv 1 \pmod{33}$ . You should use the extended Euclidean Algorithm. Your answer should be in the range  $0 \leq y < 33$ .
- b) Now, solve  $7z \equiv 2 \pmod{33}$  for all of its integer solutions  $z$ .

Try this problem with the people around you, and then we'll go over it together!



## Problem 2 – Extended Euclidean Algorithm

b) Now, solve  $7z \equiv 2 \pmod{33}$  for all of its integer solutions  $z$ .

## Problem 2 – Extended Euclidean Algorithm

b) Now, solve  $7z \equiv 2 \pmod{33}$  for all of its integer solutions  $z$ .

If we have  $7z \equiv 2 \pmod{33}$ , multiplying both sides by 19, we get:

$$\begin{aligned} 19 \cdot 7z &\equiv 19 \cdot 2 \pmod{33} \\ z &\equiv 5 \pmod{33} \end{aligned}$$

Thus  $z = 5 + 33k$

This means that the set of solutions is  $\{5 + 33k \mid k \in \mathbb{Z}\}$

# Introducing Induction (kind of)



# Climb the ladder!

You are scared of heights and there is a prize at the top of a very very tall ladder.

You do not want to climb this ladder...



# Climb the ladder!

You are scared of heights and there is a prize at the top of a very very tall ladder.

You do not want to climb this ladder...

Lets convince your friend to climb it instead!!!



# Climb the ladder!

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$



# Climb the ladder!

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

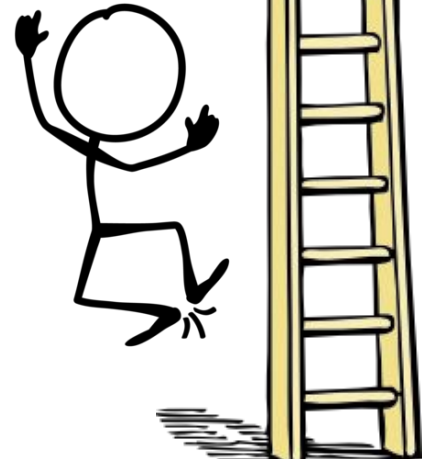


# Climb the ladder!

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with  $k$  steps ( $k$  is arbitrary).”





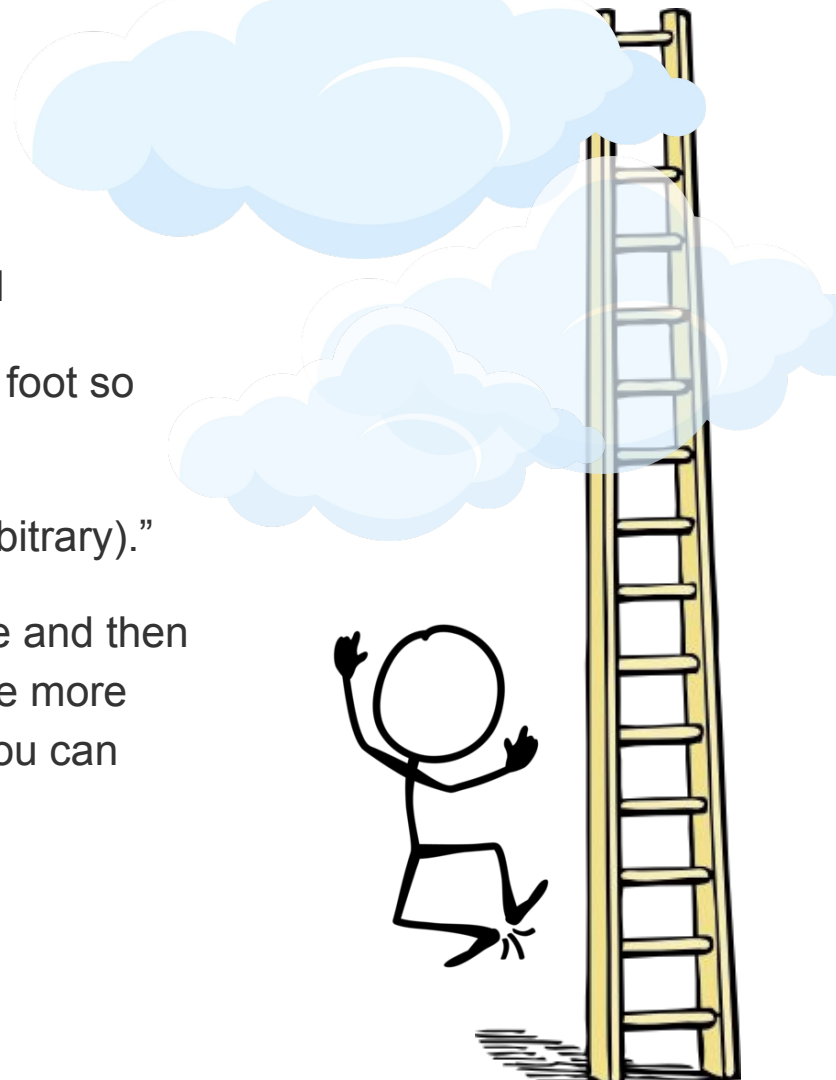
# Climb the ladder!

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with  $k$  steps ( $k$  is arbitrary).”

“Since you can climb to the  $k$ th step, climb up to there and then after you reach the  $k$ th step, you can lift your foot one more step to reach the  $k+1$  step of the ladder. Therefore, you can climb a ladder with  $k+1$  steps.”



# Climb the ladder!

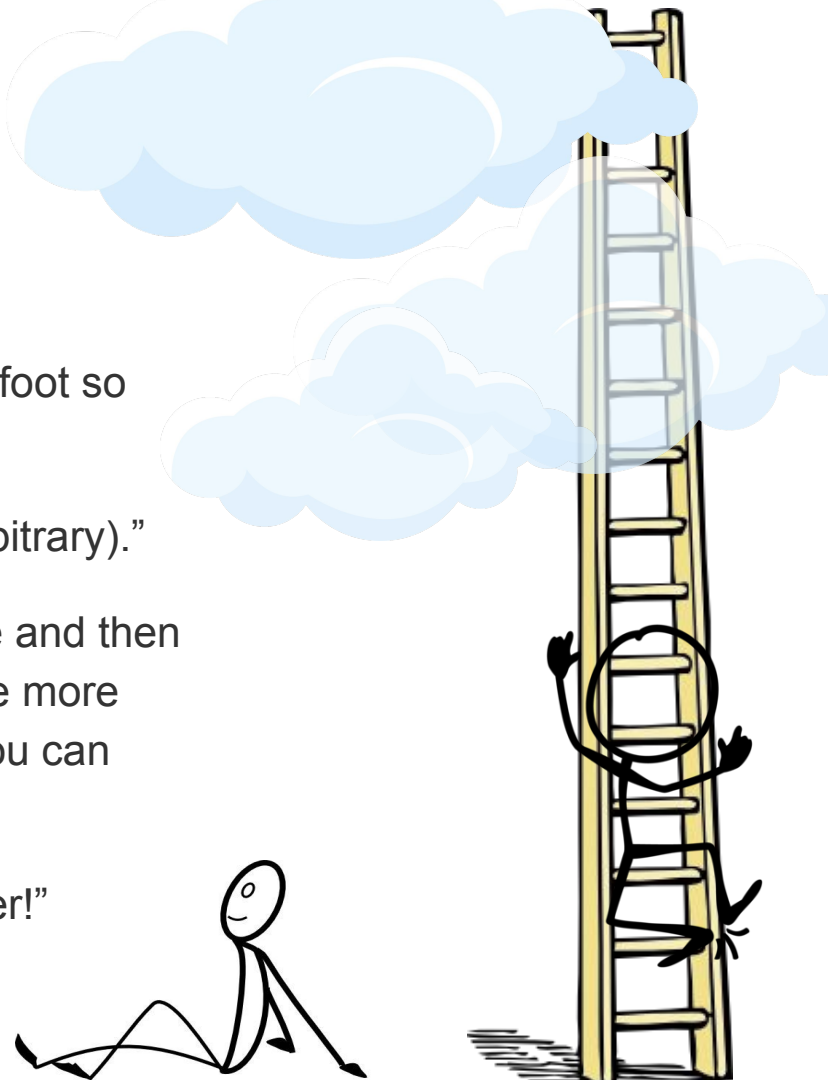
Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with  $k$  steps ( $k$  is arbitrary).”

“Since you can climb to the  $k$ th step, climb up to there and then after you reach the  $k$ th step, you can lift your foot one more step to reach the  $k+1$  step of the ladder. Therefore, you can climb a ladder with  $k+1$  steps.”

“By the principle of induction, you can climb any ladder!”



# Why does it work?

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with  $k \geq 1$  steps ( $k$  is arbitrary).”

“Since you can climb to the  $k$ th step, climb up to there and then after you reach the  $k$ th step, you can lift your foot one more step to reach the  $k+1$  step of the ladder. Therefore, you can climb a ladder with  $k+1$  steps.”

“By the principle of induction, you can climb any ladder!”

**Base Case:** You were able to start climbing at some point

**Inductive Step:**  $k$  was arbitrary, so no matter how far you go, you can always go one step higher



# Induction Proof Structure

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with  $k \geq 1$  steps ( $k$  is arbitrary).”

“Since you can climb to the  $k$ th step, climb up to there and then after you reach the  $k$ th step, you can lift your foot one more step to reach the  $k+1$  step of the ladder. Therefore, you can climb a ladder with  $k+1$  steps.”

“By the principle of induction, you can climb any ladder!”

**$P(n)$**

**Base Case**

**Inductive Hypothesis:**  
Suppose  $P(k)$  holds

**Inductive Step:**  
Show  $P(k+1)$  holds

**Conclusion:**  
 $P(n)$  holds for all  $n$ !



# Why $k \geq 1$ ? Why not just $k > 1$ ?

Claim: “You can climb a ladder with  $n$  steps” for  $n \geq 1$

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with  $k \geq 1$  steps ( $k$  is arbitrary).”

“Since you can climb to the  $k$ th step, climb up to there and then after you reach the  $k$ th step, you can lift your foot one more step to reach the  $k+1$  step of the ladder. Therefore, you can climb a ladder with  $k+1$  steps.”

“By the principle of induction, you can climb any ladder!”



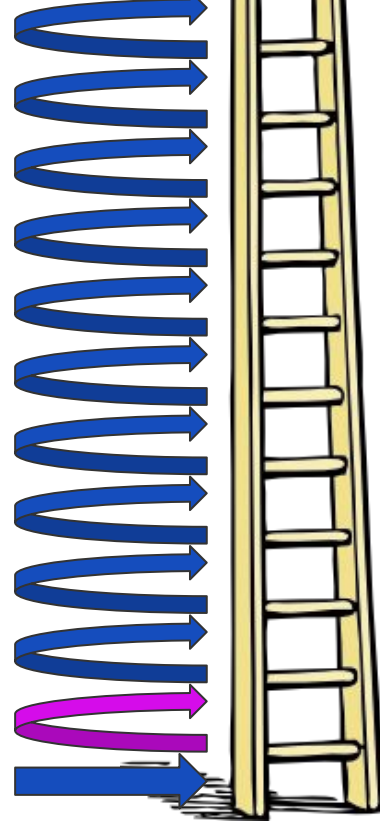
Why  $k \geq 1$ ? Why not just  $k > 1$ ?

Base Case: You  
can climb to the  
first rung



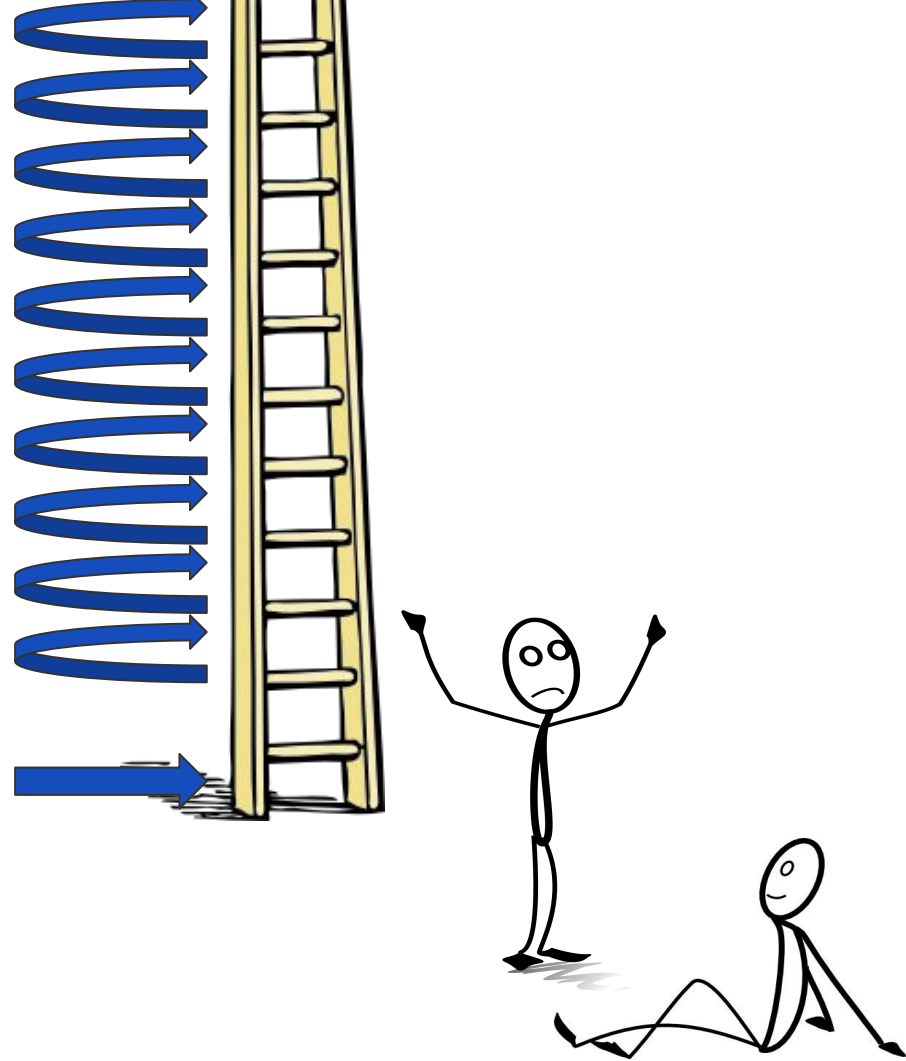
Why  $k \geq 1$ ? Why not just  $k > 1$ ?

Inductive Step: If you can climb to rung  $k \geq 1$ , then you can climb to rung  $k+1$ .  $k$  can be as small as 1, so inductive step handles the case of going from rung 1 to rung 2



Why  $k \geq 1$ ? Why not just  $k > 1$ ?

If  $k > 1$ , then the smallest  $k$  can be is 2. So if you can climb to rung 2, then you can climb to rung 3. But how can you climb to rung 2?





# Induction: How it actually works



# (Weak) Induction Template

Let  $P(n)$  be “(whatever you’re trying to prove)”.

We show  $P(n)$  holds for all  $n \in \mathbb{N}$  by induction on  $n$

Base Case: Show  $P(b)$  is true.

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq b$ .

Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )

Conclusion: Therefore,  $P(n)$  holds for all  $n$  by the principle of induction.

# (Weak) Induction Template

Let  $P(n)$  be “(whatever you’re trying to prove)”.

We show  $P(n)$  holds **for all  $n \in \mathbb{N}$**  by induction on  $n$

Note: often you will condition  $n$  here, like “all natural numbers  $n$ ” or “ $n \geq 0$ ”

Base Case: Show  $P(b)$  is true.

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq b$ .

Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )

Conclusion: Therefore,  $P(n)$  holds **for all  $n$**  by the principle of induction.

Match the earlier condition on  $n$  in your conclusion!



P(n) IS A PREDICATE, IT  
HAS A BOOLEAN VALUE  
NOT A NUMERICAL ONE

# (Weak) Induction Template

Let  $P(n)$  be “(whatever you’re trying to prove)”.

We show  $P(n)$  holds **for all  $n$**   $\in \mathbb{N}$  by induction on  $n$

Base Case: Show  $P(b)$  is true.

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq b$ .

Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )

Conclusion: Therefore,  $P(n)$  holds **for all  $n$**  by the principle of induction.

# (Weak) Induction Template

Let  $P(n)$  be “(whatever you’re trying to prove)”.

We show  $P(n)$  holds **for all  $n$**   $\in \mathbb{N}$  by induction on  $n$



$P(n)$  IS A PREDICATE, IT HAS A BOOLEAN VALUE NOT A NUMERICAL ONE



YOU MUST INTRODUCE AN ARBITRARY VARIABLE IN YOUR IH

Base Case: Show  $P(b)$  is true.

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq b$ .

Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )

Conclusion: Therefore,  $P(n)$  holds **for all  $n$**  by the principle of induction.

# (Weak) Induction Template

Let  $P(n)$  be “(whatever you’re trying to prove)”.

We show  $P(n)$  holds **for all  $n$**   $\in \mathbb{N}$  by induction on  $n$

Base Case: Show  $P(b)$  is true.

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq b$ .

Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )

Conclusion: Therefore,  $P(n)$  holds **for all  $n$**  by the principle of induction.



$P(n)$  IS A PREDICATE, IT HAS A BOOLEAN VALUE NOT A NUMERICAL ONE



YOU MUST INTRODUCE AN ARBITRARY VARIABLE IN YOUR IH



START WITH LHS OF EXPRESSION AND END WITH RHS (FOR BASE CASE AND IS)

# Weak Induction



## Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .



## Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement “ $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ ” defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement “ $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ ” defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

**Base Case.**

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

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement " $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ " defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

**Base Case.**

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

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement “ $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ ” defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

**Base Case.**

$$\begin{aligned}\sum_{i=0}^n i^2 &= 0^2 \\ &= \frac{1}{6}(0)(0+1)(2(0)+1)\end{aligned}$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement “ $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ ” defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

**Base Case.**

$$\begin{aligned}\sum_{i=0}^n i^2 &= 0^2 \\ &= \frac{1}{6}(0)(0+1)(2(0)+1)\end{aligned}$$

Thus  $P(0)$  is true.

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement “ $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ ” defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

**Base Case.**

$$\begin{aligned}\sum_{i=0}^n i^2 &= 0^2 \\ &= \frac{1}{6}(0)(0+1)(2(0)+1)\end{aligned}$$

Thus  $P(0)$  is true.

**Inductive Hypothesis.** Suppose that  $P(k)$  is true for some arbitrary  $k \in \mathbb{N}$  (i.e.  $\sum_{i=0}^k i^2 = \frac{1}{6}k(k+1)(2(k)+1)$ .)

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

Let  $P(n)$  be the statement " $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ " defined for all  $n \in \mathbb{N}$ . We prove that  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction on  $n$ .

**Base Case.**

$$\begin{aligned}\sum_{i=0}^n i^2 &= 0^2 \\ &= \frac{1}{6}(0)(0+1)(2(0)+1)\end{aligned}$$

Thus  $P(0)$  is true.

**Inductive Hypothesis.** Suppose that  $P(k)$  is true for some arbitrary  $k \in \mathbb{N}$  (i.e.  $\sum_{i=0}^k i^2 = \frac{1}{6}k(k+1)(2(k)+1)$ .)

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Hypothesis.** Suppose that  $P(k)$  is true for some arbitrary  $k \in \mathbb{N}$  (i.e.  $\sum_{i=0}^k i^2 = \frac{1}{6}k(k+1)(2(k)+1)$ ).

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^k i^2 + (k+1)^2 \quad \text{by definition}$$



# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Hypothesis.** Suppose that  $P(k)$  is true for some arbitrary  $k \in \mathbb{N}$  (i.e.  $\sum_{i=0}^k i^2 = \frac{1}{6}k(k+1)(2(k)+1)$ ).

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^k i^2 + (k+1)^2 \quad \text{by definition}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Hypothesis.** Suppose that  $P(k)$  is true for some arbitrary  $k \in \mathbb{N}$  (i.e.  $\sum_{i=0}^k i^2 = \frac{1}{6}k(k+1)(2(k)+1)$ ).

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^k i^2 + (k+1)^2 \quad \text{by definition}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Hypothesis.** Suppose that  $P(k)$  is true for some arbitrary  $k \in \mathbb{N}$  (i.e.  $\sum_{i=0}^k i^2 = \frac{1}{6}k(k+1)(2k+1)$ ).

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.}\end{aligned}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\ &= (k+1) \left( \frac{1}{6}k(2k+1) + (k+1) \right) && \text{using common factor } (k+1)\end{aligned}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\ &= (k+1) \left( \frac{1}{6}k(2k+1) + (k+1) \right) && \text{using common factor } (k+1) \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1))\end{aligned}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\ &= (k+1) \left( \frac{1}{6}k(2k+1) + (k+1) \right) && \text{using common factor } (k+1) \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)\end{aligned}$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\ &= (k+1) \left( \frac{1}{6}k(2k+1) + (k+1) \right) && \text{using common factor } (k+1) \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3) && \text{factoring the quadratic term} \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)\end{aligned}$$

# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\ &= (k+1) \left( \frac{1}{6}k(2k+1) + (k+1) \right) && \text{using common factor } (k+1) \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3) && \text{factoring the quadratic term} \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)\end{aligned}$$

Thus, we can conclude that  $P(k+1)$  is true.



# Task 4

For all  $n \in \mathbb{N}$ , prove that  $\sum_{i=0}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Inductive Step.** Goal:  $P(k+1)$  i.e.  $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^k i^2 + (k+1)^2 && \text{by definition} \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\ &= (k+1) \left( \frac{1}{6}k(2k+1) + (k+1) \right) && \text{using common factor } (k+1) \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3) && \text{factoring the quadratic term} \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)\end{aligned}$$

Thus, we can conclude that  $P(k+1)$  is true.

**Conclusion:** Therefore,  $P(n)$  is true for all  $n \in \mathbb{N}$  by induction.

# Strong Induction



# Why Strong Induction?

In **weak induction**, the inductive hypothesis only assumes that  $P(k)$  is true and uses that in the inductive step to prove the implication  $P(k) \rightarrow P(k + 1)$ .

In **strong induction**, the inductive hypothesis assumes the predicate holds for every step from the base case(s) up to  $P(k)$ . This usually looks something like  $P(b_1) \wedge P(b_2) \wedge \cdots \wedge P(k)$ . Then it uses this stronger inductive hypothesis in the inductive step to prove the implication  $P(b_1) \wedge \cdots \wedge P(k) \rightarrow P(k + 1)$ .

Strong induction is necessary when we have multiple base cases, or when we need to go back to a smaller number than  $k$  in our inductive step.

# Strong Induction Template

Let  $P(n)$  be “(whatever you’re trying to prove)”.

We show  $P(n)$  holds for all  $n \geq b_{min}$  by induction on  $n$ .

Base Case: Show  $P(b_{min}), P(b_{min+1}), \dots, P(b_{max})$  are all true.

Inductive Hypothesis: Suppose  $P(b_{min}) \wedge \dots \wedge P(k)$  hold for an arbitrary  $k \geq b_{max}$ .

Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(b_{min}) \wedge \dots \wedge P(k) \rightarrow P(k + 1)$ )

Conclusion: Therefore,  $P(n)$  holds for all  $n \geq b_{min}$  by the principle of induction.

## Task 5: Strong Induction

Consider the function  $a(n)$  defined for  $n \geq 1$  recursively as follows.

$$a(1) = 1$$

$$a(2) = 3$$

$$a(n) = 2a(n-1) - a(n-2) \text{ for } n \geq 3$$

Use strong induction to prove that  $a(n) = 2n - 1$  for all  $n \geq 1$ .

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .



# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .

**Inductive Step:**

We will show  $P(k + 1)$  holds.

$$a(k + 1) =$$

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .

**Inductive Step:**

We will show  $P(k + 1)$  holds.

$$a(k + 1) = 2a(k) - a(k - 1)$$

[Definition of  $a$ ]

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

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .

**Inductive Step:**

We will show  $P(k + 1)$  holds.

$$\begin{aligned} a(k + 1) &= 2a(k) - a(k - 1) \\ &= 2(2k - 1) - (2(k - 1) - 1) \end{aligned}$$

[Definition of  $a$ ]

[Inductive Hypothesis]

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

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .

**Inductive Step:**

We will show  $P(k + 1)$  holds.

$$\begin{aligned} a(k + 1) &= 2a(k) - a(k - 1) \\ &= 2(2k - 1) - (2(k - 1) - 1) \\ &= 2k + 1 \end{aligned}$$

[Definition of  $a$ ]  
[Inductive Hypothesis]  
[Algebra]

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

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

( $n = 1$ )

$$a(1) = 1 = 2 \cdot 1 - 1$$

( $n = 2$ )

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .

**Inductive Step:**

We will show  $P(k + 1)$  holds.

$$\begin{aligned} a(k + 1) &= 2a(k) - a(k - 1) \\ &= 2(2k - 1) - (2(k - 1) - 1) \\ &= 2k + 1 \\ &= 2(k + 1) - 1 \end{aligned}$$

[Definition of  $a$ ]

[Inductive Hypothesis]

[Algebra]

[Algebra]

# Strong Induction

Let  $P(n)$  be “ $a(n) = 2n - 1$ ”. We will show that  $P(n)$  is true for all  $n \geq 1$  by strong induction.

**Base Cases** ( $n = 1, n = 2$ ):

$$(n = 1)$$

$$a(1) = 1 = 2 \cdot 1 - 1$$

$$(n = 2)$$

$$a(2) = 3 = 2 \cdot 2 - 1$$

So,  $P(1)$  and  $P(2)$  hold.

**Inductive Hypothesis:**

Suppose that  $P(j)$  is true for all integers  $1 \leq j \leq k$  for some arbitrary  $k \geq 2$ .

**Inductive Step:**

We will show  $P(k + 1)$  holds.

$$a(k + 1) = 2a(k) - a(k - 1)$$

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

$$= 2k + 1$$

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

So,  $P(k + 1)$  holds.

[Definition of  $a$ ]

[Inductive Hypothesis]

[Algebra]

[Algebra]

**Conclusion:**

Therefore,  $P(n)$  holds for all integers  $n \geq 1$  by the principle of strong induction.

# **That's All, Folks!**

**Thanks for coming to section this week!**  
**Any questions?**