

# Strong Induction

CSE 311 Autumn 2025  
Lecture 17

# How do we know recursion works?

```
//Assume i is a nonnegative integer
//returns 2^i.
public int CalculatesTwoToTheI(int i) {
    if(i == 0)
        return 1;
    else
        return 2*CaclulatesTwoToTheI(i-1);
}
```

Why does `CalculatesTwoToTheI(4)` calculate  $2^4$ ?

Convince the other people in your room

# Making Induction Proofs Pretty (v1)

All of our induction proofs will come in 5 easy(?) steps!

1. Define  $P(n)$ . State that your proof is by induction on  $n$ .
2. Base Case: Show  $P(0)$  i.e. show the base case
3. Inductive Hypothesis: Suppose  $P(k)$  for an arbitrary  $k$ .
4. Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )
5. Conclude by saying  $P(n)$  is true for all  $n$  by the principle of induction.

# More Induction (goal)

Induction doesn't **only** work for code!

Show that  $\sum_{i=0}^n 2^i = 1 + 2 + 4 + \dots + 2^n = 2^{n+1} - 1$ .

# More Induction (setup)

Induction doesn't **only** work for code!

Show that  $\sum_{i=0}^n 2^i = 1 + 2 + 4 + \dots + 2^n = 2^{n+1} - 1$ .

Let  $P(n)$  be " $\sum_{i=0}^n 2^i = 2^{n+1} - 1$ ."

We show  $P(n)$  holds for all  $n$  by induction on  $n$ .

Base Case ( )

Inductive Hypothesis:

Inductive Step:

$P(n)$  holds for all  $n \geq 0$  by the principle of induction.

# More Induction (complete)

Induction doesn't **only** work for code!

Show that  $\sum_{i=0}^n 2^i = 1 + 2 + 4 + \dots + 2^n = 2^{n+1} - 1$ .

Let  $P(n)$  be " $\sum_{i=0}^n 2^i = 2^{n+1} - 1$ ."

We show  $P(n)$  holds for all natural numbers  $n$  by induction on  $n$ .

Base Case ( $n = 0$ )  $\sum_{i=0}^0 2^i = 1 = 2 - 1 = 2^{0+1} - 1$ .

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq 0$ .

Inductive Step: We show  $P(k + 1)$ . Consider the summation  $\sum_{i=0}^{k+1} 2^i = 2^{k+1} + \sum_{i=0}^k 2^i = 2^{k+1} + 2^{k+1} - 1$ , where the last step is by IH.

Simplifying, we get:  $\sum_{i=0}^{k+1} 2^i = 2^{k+1} + 2^{k+1} - 1 = 2 \cdot 2^{k+1} - 1 = 2^{(k+1)+1} - 1$ .

$P(n)$  holds for all  $n \geq 0$  by the principle of induction.

# Algebra Block Formatting

In an English proof it's very common to have algebra broken out (instead of separate sentences); this is often easier to read.

Inductive Step: We show  $P(k + 1)$ . Consider the summation

$$\begin{aligned}\sum_{i=0}^{k+1} 2^i &= 2^{k+1} + \sum_{i=0}^k 2^i \text{ breaking off final term} \\ &= 2^{k+1} + 2^{k+1} - 1 \text{ by IH} \\ &= 2 \cdot 2^{k+1} - 1 \text{ combining two copies of } 2^{k+1} \\ &= 2^{(k+1)+1} - 1.\end{aligned}$$

$P(n)$  holds for all  $n \geq 0$  by the principle of induction.

# Let's Try Another Induction Proof

$$\text{Let } g(n) = \begin{cases} 2 & \text{if } n = 2 \\ g(n-1)^2 + 3g(n-1) & \text{if } n > 2 \end{cases}$$

Prove  $g(n)$  is even for all  $n \geq 2$  by induction on  $n$ .

Let's just set this one up, we'll leave the individual pieces as exercises.

# Setup scratchwork

Let  $P(n)$  be " $g(n)$  is even."

HEY WAIT --  $P(0)$  isn't true  $g(0)$  isn't even defined!

We can move the "starting line"

Change the base case, and then update the IH to have the smallest value of  $k$  assume just the base case.

# Setup

$$g(n) = \begin{cases} 2 & \text{if } n = 2 \\ g(n-1)^2 + 3g(n-1) & \text{if } n > 2 \end{cases}$$

Let  $P(n)$  be " $g(n)$  is even."

We show  $P(n)$  for all integers  $n \geq 2$  by induction on  $n$ .

**Base Case ( $n = 2$ ):** <todo>

**Inductive Hypothesis:** Suppose  $P(k)$  holds for an arbitrary  $k \geq 2$ .

**Inductive Step:**

<todo>

We conclude  $P(k + 1)$ . Therefore,  $P(n)$  holds for all  $n \geq 2$  by the principle of induction.

# "Another Induction Proof" Complete!

Let  $P(n)$  be " $g(n)$  is even."

We show  $P(n)$  for all integers  $n \geq 2$  by induction on  $n$ .

**Base Case ( $n = 2$ ):**  $g(n) = 2$  by definition. 2 is even, so we have  $P(2)$ .

**Inductive Hypothesis:** Suppose  $P(k)$  holds for an arbitrary  $k \geq 2$ .

**Inductive Step:** We show  $P(k + 1)$ . Consider  $g(k + 1)$ . By definition of  $g(\cdot)$ ,  $g(k + 1) = g(k)^2 + 3g(k)$ . By inductive hypothesis,  $g(k)$  is even, so it equals  $2j$  for some integer  $j$ . Plugging in we have:

$$g(k + 1) = (2j)^2 + 3(2j) = 2(2j^2) + 2(3j) = 2(2j^2 + 3j).$$

Since  $j$  is an integer,  $2j^2 + 3j$  is also an integer, and  $g(k + 1)$  is even.

Therefore,  $P(n)$  holds for all  $n \geq 2$  by the principle of induction.

# Making Induction Proofs Pretty (v2)

All of our induction proofs will come in 5 easy(?) steps!

1. Define  $P(n)$ . State that your proof is by induction on  $n$ .
2. Base Case: Show  $P(b)$  i.e. show the base case
3. Inductive Hypothesis: Suppose  $P(k)$  for an arbitrary  $k \geq b$ .
4. Inductive Step: Show  $P(k + 1)$  (i.e. get  $P(k) \rightarrow P(k + 1)$ )
5. Conclude by saying  $P(n)$  is true for all  $n \geq b$  by the principle of induction.

# Let's Try Yet Another Induction Proof

## Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization.

Uniqueness is hard. Let's just show existence.

I.e.

Claim: Every positive integer greater than 1 can be written as a product of primes.

# Prime Factorizations

Some examples

$$12 = 2^2 \cdot 3$$

$$35 = 5 \cdot 7$$

$$36 = 2^2 \cdot 3^2$$

$$7 = 7$$

Notice, for prime numbers the product is just the one number.

# Induction on Primes (first try)

Let  $P(n)$  be " $n$  can be written as a product of primes."

We show  $P(n)$  for all integers  $n \geq 2$  by induction on  $n$ .

**Base Case ( $n = 2$ ):** 2 is a product of just itself. Since 2 is prime, it is written as a product of primes.

**Inductive Hypothesis:** Suppose  $P(k)$  holds for an arbitrary integer  $k \geq 2$ .

**Inductive Step:**

Case 1,  $k + 1$  is prime: then  $k + 1$  is automatically written as a product of primes.

Case 2,  $k + 1$  is composite:

Therefore  $P(k + 1)$ .

$P(n)$  holds for all  $n \geq 2$  by the principle of induction.

# We're Stuck

We can divide  $k + 1$  up into smaller pieces (say  $s, t$  such that  $st = k + 1$  with  $2 \leq s < k + 1$  and  $2 \leq t < k + 1$ )

Is  $P(s)$  true? Is  $P(t)$  true?

I mean...it would be...

But in the inductive step we don't have it...

Let's add it to our inductive hypothesis.

# Induction on Primes (revised)

Let  $P(n)$  be " $n$  can be written as a product of primes."

We show  $P(n)$  for all integers  $n \geq 2$  by induction on  $n$ .

**Base Case ( $n = 2$ ):** 2 is a product of just itself. Since 2 is prime, it is written as a product of primes.

**Inductive Hypothesis:**

**Inductive Step:**

Case 1,  $k + 1$  is prime: then  $k + 1$  is automatically written as a product of primes.

Case 2,  $k + 1$  is composite:

Therefore  $P(k + 1)$ .

$P(n)$  holds for all  $n \geq 2$  by the principle of induction.

# Induction on Primes (complete)

Let  $P(n)$  be " $n$  can be written as a product of primes."

We show  $P(n)$  for all integers  $n \geq 2$  by induction on  $n$ .

**Base Case ( $n = 2$ ):** 2 is a product of just itself. Since 2 is prime, it is written as a product of primes.

**Inductive Hypothesis:** Suppose  $P(2), \dots, P(k)$  hold for an arbitrary integer  $k \geq 2$ .

**Inductive Step:**

Case 1,  $k + 1$  is prime: then  $k + 1$  is automatically written as a product of primes.

Case 2,  $k + 1$  is composite: We can write  $k + 1 = st$  for  $s, t$  nontrivial divisors (i.e.  $2 \leq s < k + 1$  and  $2 \leq t < k + 1$ ). By inductive hypothesis, we can write  $s$  as a product of primes  $p_1 \cdot \dots \cdot p_j$  and  $t$  as a product of primes  $q_1 \cdot \dots \cdot q_\ell$ . Multiplying these representations,  $k + 1 = p_1 \cdot \dots \cdot p_j \cdot q_1 \cdot \dots \cdot q_\ell$ , which is a product of primes.

Therefore  $P(k + 1)$ .

$P(n)$  holds for all  $n \geq 2$  by the principle of induction.

# Strong Induction

That hypothesis where we assume  $P(\text{base case}), \dots, P(k)$  instead of just  $P(k)$  is called a strong inductive hypothesis.

Strong induction is the same fundamental idea as weak ("regular") induction.

$P(0)$  is true.

And  $P(0) \rightarrow P(1)$ , so  $P(1)$ .

And  $P(1) \rightarrow P(2)$ , so  $P(2)$ .

And  $P(2) \rightarrow P(3)$ , so  $P(3)$ .

And  $P(3) \rightarrow P(4)$ , so  $P(4)$ .

...

$P(0)$  is true.

And  $P(0) \rightarrow P(1)$ , so  $P(1)$ .

And  $[P(0) \wedge P(1)] \rightarrow P(2)$ , so  $P(2)$ .

And  $[P(0) \wedge \dots \wedge P(2)] \rightarrow P(3)$ , so  $P(3)$ .

And  $[P(0) \wedge \dots \wedge P(3)] \rightarrow P(4)$ , so  $P(4)$ .

...

# Making **Strong** Induction Proofs Pretty

All of our **strong** induction proofs will come in 5 easy(?) steps!

1. Define  $P(n)$ . State that your proof is by induction on  $n$ .
2. Base Case: Show  $P(b)$  i.e. show the base case
3. Inductive Hypothesis: Suppose  $P(b) \wedge \dots \wedge P(k)$  for an arbitrary  $k \geq b$ .
4. Inductive Step: Show  $P(k + 1)$  (i.e. get  $[P(b) \wedge \dots \wedge P(k)] \rightarrow P(k + 1)$ )
5. Conclude by saying  $P(n)$  is true for all  $n \geq b$  by the principle of induction.

# Strong Induction vs. Weak Induction

Think of strong induction as “my recursive call might be on LOTS of smaller values” (like mergesort – you cut your array in half)

Think of weak induction as “my recursive call is always on one step smaller.”

Practical advice:

A strong hypothesis isn't wrong when you only need a weak one (but a weak one is wrong when you need a strong one). Some people just always write strong hypotheses. But it's easier to typo a strong hypothesis.

Robbie leaves a blank spot where the IH is, and fills it in after the step.

# Let's Try Another! Stamp Collecting

I have 4 cent stamps and 5 cent stamps (as many as I want of each).  
Prove that I can make exactly  $n$  cents worth of stamps for all  $n \geq 12$ .

Try for a few values.

Then think...how would the inductive step go?



# Stamp Collection (attempt)

Define  $P(n)$  "I can make  $n$  cents of stamps with just 4 and 5 cent stamps."

We prove  $P(n)$  is true for all integers  $n \geq 12$  by induction on  $n$ .

Base Case:

12 cents can be made with three 4 cent stamps.

Inductive Hypothesis Suppose [maybe some other stuff and]  $P(k)$ , for an arbitrary  $k \geq 12$ .

Inductive Step:

We want to make  $k + 1$  cents of stamps. By IH we can make  $k - 3$  cents exactly with stamps. Adding another 4 cent stamp gives exactly  $k + 1$  cents.

# Stamp Collection...wait a second...

Is the proof right?

How do we know  $P(13)$

We're not the base case, so our inductive hypothesis assumes  $P(12)$ , and then we say if  $P(9)$  then  $P(13)$ .

Wait a second....

If you go back  $s$  steps every time, you need  $s$  base cases.

Or else the first few values aren't proven.

# Stamp Collection (corrected)

Define  $P(n)$  to be "I can make  $n$  cents of stamps with just 4 and 5 cent stamps."

We prove  $P(n)$  is true for all integers  $n \geq 12$  by induction on  $n$ .

Base Case:

12 cents can be made with three 4 cent stamps.

13 cents can be made with two 4 cent stamps and one 5 cent stamp.

14 cents can be made with one 4 cent stamp and two 5 cent stamps.

15 cents can be made with three 5 cent stamps.

Inductive Hypothesis Suppose  $P(12) \wedge P(13) \wedge \dots \wedge P(k)$ , for an arbitrary  $k \geq 15$ .

Inductive Step:

We want to make  $k + 1$  cents of stamps. By IH we can make  $k - 3$  cents exactly with stamps. Adding another 4 cent stamp gives exactly  $k + 1$  cents.

# A good last check

After you've finished writing an inductive proof, pause.

If your inductive step always goes back  $s$  steps, you need  $s$  base cases (otherwise  $b + 1$  will go back before the base cases you've shown). And make sure your inductive hypothesis is strong enough.

If your inductive step is going back a varying (unknown) number of steps, check the first few values above the base case, make sure your cases are really covered. And make sure your IH is strong.

# Practical Advice

How many base cases do you need?

Always at least one.

If you're analyzing recursive code or a recursive function, at least one for each base case of the code/function.

If you always go back  $s$  steps, at least  $s$  consecutive base cases.

Enough to make sure every case is handled.

# Making **Strong** Induction Proofs Pretty (with multiple base cases)

All of our induction proofs will come in 5 easy(?) steps!

1. Define  $P(n)$ . State that your proof is by induction on  $n$ .
2. Base Cases: Show  $P(b_{min}), P(b_{min+1}) \dots P(b_{max})$  i.e. show the base cases
3. Inductive Hypothesis: Suppose  $P(b_{min}) \wedge P(b_{min} + 1) \wedge \dots \wedge P(k)$  for an arbitrary  $k \geq b_{max}$ . (The smallest value of  $k$  assumes **all** bases cases, but nothing else)
4. Inductive Step: Show  $P(k + 1)$  (i.e. get  $[P(b_{min}) \wedge \dots \wedge P(k)] \rightarrow P(k + 1)$ )
5. Conclude by saying  $P(n)$  is true for all  $n \geq b_{min}$  by the principle of induction.

# Stamp Collection, Done Wrong

Define  $P(n)$  to be "I can make  $n$  cents of stamps with just 4 and 5 cent stamps."

We prove  $P(n)$  is true for all integers  $n \geq 12$  by induction on  $n$ .

Base Case:

12 cents can be made with three 4 cent stamps.

Inductive Hypothesis Suppose  $P(k)$ ,  $k \geq 12$ .

Inductive Step:

We want to make  $k + 1$  cents of stamps. By IH we can make  $k$  cents exactly with stamps. Replace one of the 4 cent stamps with a 5 cent stamp.

$P(n)$  holds for all  $n$  by the principle of induction.

# Stamp Collection, Done Wrong

What if the starting point doesn't have any 4 cent stamps?

Like, say, 15 cents =  $5+5+5$ .

Claim:  $3 \mid (2^{2n} - 1)$  for all natural numbers

[Define  $P(n)$ ]

Base Case

Inductive Hypothesis

Inductive Step

[conclusion]

Claim:  $3 \mid (2^{2^n} - 1)$  for all natural numbers

Let  $P(n)$  be " $3 \mid (2^{2^n} - 1)$ ." We show  $P(n)$  holds for all natural numbers  $n$ .

Base Case ( $n = 0$ ) note that  $2^{2^n} - 1 = 2^0 - 1 = 0$ . Since  $3 \cdot 0 = 0$ , and 0 is an integer,  $3 \mid (2^{2 \cdot 0} - 1)$ .

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq 0$

Inductive Step:

Target:  $P(k + 1)$ , i.e.  $3 \mid (2^{2^{(k+1)}} - 1)$

Therefore, we have  $P(n)$  for all  $n \in \mathbb{N}$  by the principle of induction.

# Claim: $3 \mid (2^{2^n} - 1)$ for all natural numbers

Let  $P(n)$  be " $3 \mid (2^{2^n} - 1)$ ." We show  $P(n)$  holds for all natural numbers  $n$ .

Base Case ( $n = 0$ ) note that  $2^{2^n} - 1 = 2^0 - 1 = 0$ . Since  $3 \cdot 0 = 0$ , and 0 is an integer,  $3 \mid (2^{2 \cdot 0} - 1)$ .

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq 0$

Inductive Step: By inductive hypothesis,  $3 \mid (2^{2^k} - 1)$ . i.e. there is an integer  $j$  such that  $3j = 2^{2^k} - 1$ .

$$2^{2^{(k+1)}} - 1 = 4 \cdot 2^{2^k} - 1$$

**FORCE the expression in your IH to appear**

Target:  $P(k + 1)$ , i.e.  $3 \mid (2^{2^{(k+1)}} - 1)$

Therefore, we have  $P(n)$  for all  $n \in \mathbb{N}$  by the principle of induction.

# Claim: $3 \mid (2^{2^n} - 1)$ for all natural numbers

Let  $P(n)$  be " $3 \mid (2^{2^n} - 1)$ ." We show  $P(n)$  holds for all natural numbers  $n$ .

Base Case ( $n = 0$ ) note that  $2^{2^n} - 1 = 2^0 - 1 = 0$ . Since  $3 \cdot 0 = 0$ , and  $0$  is an integer,  $3 \mid (2^{2 \cdot 0} - 1)$ .

Inductive Hypothesis: Suppose  $P(k)$  holds for an arbitrary  $k \geq 0$

Inductive Step: By inductive hypothesis,  $3 \mid (2^{2^k} - 1)$ . i.e. there is an integer  $j$  such that  $3j = 2^{2^k} - 1$ .

$$2^{2^{(k+1)}} - 1 = 4(2^{2^k} - 1 + 1) - 1 = 4(2^{2^k} - 1) + 4 - 1$$

By IH, we can replace  $2^{2^k} - 1$  with  $3j$  for an integer  $j$

$$2^{2^{(k+1)}} - 1 = 4(3j) + 4 - 1 = 3(4j) + 3 = 3(4j + 1)$$

Since  $4j + 1$  is an integer, we meet the definition of divides and we have:

Target:  $P(k + 1)$ , i.e.  $3 \mid (2^{2^{(k+1)}} - 1)$

Therefore, we have  $P(n)$  for all  $n \in \mathbb{N}$  by the principle of induction.

# Claim: $3 \mid (2^{2^n} - 1)$ for all natural numbers

That inductive step might still seem like magic.

It sometimes helps to run through examples, and look for patterns:

$$2^{2 \cdot 0} - 1 = 0 = 3 \cdot 0$$

$$2^{2 \cdot 1} - 1 = 3 = 3 \cdot 1$$

$$2^{2 \cdot 2} - 1 = 15 = 3 \cdot 5$$

$$2^{2 \cdot 3} - 1 = 63 = 3 \cdot 21$$

$$2^{2 \cdot 4} - 1 = 255 = 3 \cdot 85$$

$$2^{2 \cdot 5} - 1 = 1023 = 3 \cdot 341$$

The divisor goes from  $k$  to  $4k + 1$

$$0 \rightarrow 4 \cdot 0 + 1 = 1$$

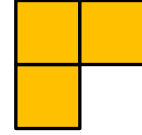
$$1 \rightarrow 4 \cdot 1 + 1 = 5$$

$$5 \rightarrow 4 \cdot 5 + 1 = 21$$

...

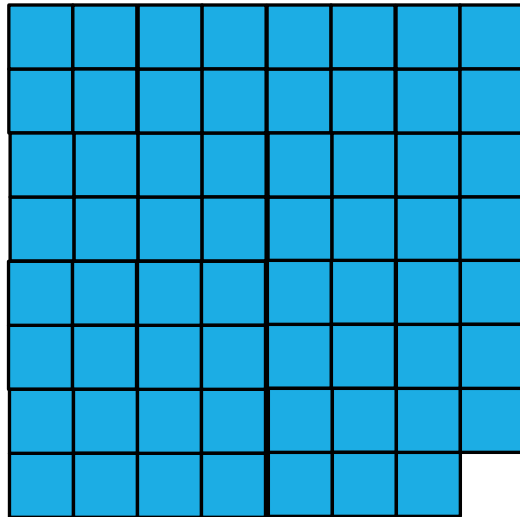
That might give us a hint that  $4k + 1$  will be in the algebra somewhere, and give us another intermediate target.

# Even more practice



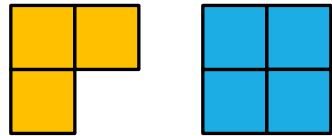
I've got a bunch of these 3 piece tiles.

I want to fill a  $2^n \times 2^n$  grid ( $n \geq 1$ ) with the pieces, except for a  $1 \times 1$  spot in a corner.



# Gridding (not a full proof, just intuition)

Base Case:  $n = 1$



Inductive hypothesis: Suppose you can tile a  $2^k \times 2^k$  grid, except for a corner.

Inductive step:  $2^{k+1} \times 2^{k+1}$ , divide into quarters. By IH can tile...

