Foundations of Computer Science Lecture 6

Strong Induction

Strengthening the Induction Hypothesis Strong Induction Many Flavors of Induction



Proving "for all": $P(n): 4^n - 1$ is divisible by 3. $\forall n: P(n)$? $P(n): \sum_{i=1}^n i = \frac{1}{2}n(n+1).$ $\forall n: P(n)$? $P(n): \sum_{i=1}^n i^2 = \frac{1}{6}n(n+1)(2n+1).$ $\forall n: P(n)$?

- **2** Induction.
- Induction and Well-Ordering.

Solving Harder Problems with Induction • $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}$

- 2 Strengthening the Induction Hypothesis
 - $n^2 < 2^n$
 - *L*-tiling.

Many Flavors of Induction

- Leaping Induction
 Postage; n³ < 2ⁿ
- Strong Induction
 - Fundamental Theorem of Arithmetic
 - Games of Strategy

- Proof. $P(n): \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}.$
 - 1: [Base case] P(1) claims that $1 \le 2 \times \sqrt{1}$, which is clearly T.

Proof. $P(n): \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}.$

1: [Base case] P(1) claims that $1 \le 2 \times \sqrt{1}$, which is clearly T.

2: **[Induction step]** Show $P(n) \to P(n+1)$ for all $n \ge 1$ (direct proof) Assume (induction hypothesis) P(n) is T: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \le 2\sqrt{n}$.

Show P(n+1) is T: $\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \le 2\sqrt{n+1}$.

Proof. $P(n): \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}.$

1: [Base case] P(1) claims that $1 \le 2 \times \sqrt{1}$, which is clearly T.

2: **[Induction step]** Show $P(n) \to P(n+1)$ for all $n \ge 1$ (direct proof) Assume (induction hypothesis) P(n) is T: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \le 2\sqrt{n}$.

Show
$$P(n+1)$$
 is T: $\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \le 2\sqrt{n+1}$.

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{n+1}}$$

Proof. $P(n): \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}.$

1: [Base case] P(1) claims that $1 \le 2 \times \sqrt{1}$, which is clearly T.

2: **[Induction step]** Show $P(n) \to P(n+1)$ for all $n \ge 1$ (direct proof) Assume (induction hypothesis) P(n) is T: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \le 2\sqrt{n}$.

Show
$$P(n+1)$$
 is T: $\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \le 2\sqrt{n+1}$.

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{n+1}}$$

$$\stackrel{\text{\tiny IH}}{\leq} \quad 2\sqrt{n} + \frac{1}{\sqrt{n+1}}$$

Proof. $P(n): \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}.$

1: [Base case] P(1) claims that $1 \le 2 \times \sqrt{1}$, which is clearly T.

2: **[Induction step]** Show $P(n) \to P(n+1)$ for all $n \ge 1$ (direct proof) Assume (induction hypothesis) P(n) is T: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \le 2\sqrt{n}$.

Show P(n+1) is T: $\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \le 2\sqrt{n+1}$.

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{n+1}}$$

$$\stackrel{\text{\tiny IH}}{\leq} 2\sqrt{n} + \frac{1}{\sqrt{n+1}}$$

Lemma. $2\sqrt{n}+1/\sqrt{n+1} \le 2\sqrt{n+1}$
<i>Proof.</i> By contradiction.
$2\sqrt{n} + 1/\sqrt{n+1} > 2\sqrt{n+1}$
$\rightarrow 2\sqrt{n(n+1)} + 1 > 2(n+1)$
$\rightarrow 4n(n+1) > (2n+1)^2$
$\rightarrow 0 > 1$ FISHY !

Proof. $P(n): \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}.$

1: [Base case] P(1) claims that $1 \le 2 \times \sqrt{1}$, which is clearly T.

2: **[Induction step]** Show $P(n) \to P(n+1)$ for all $n \ge 1$ (direct proof) Assume (induction hypothesis) P(n) is T: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \le 2\sqrt{n}$.

Show
$$P(n+1)$$
 is T: $\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \le 2\sqrt{n+1}$.

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{n+1}}$$

$$\stackrel{\text{\tiny IH}}{\leq} \quad 2\sqrt{n} + \frac{1}{\sqrt{n+1}}$$

$$\stackrel{\text{(lemma)}}{\leq} 2\sqrt{n+1}$$

So, P(n+1) is T.

3: By induction, P(n) is $T \forall n \ge 1$.

Lemma.
$$2\sqrt{n} + 1/\sqrt{n+1} \le 2\sqrt{n+1}$$

Proof. By contradiction.
 $2\sqrt{n} + 1/\sqrt{n+1} > 2\sqrt{n+1}$
 $\rightarrow 2\sqrt{n(n+1)} + 1 > 2(n+1)$
 $\rightarrow 4n(n+1) > (2n+1)^2$
 $\rightarrow 0 > 1$ FISHY!

Proving Stronger Claims

$$n^2 \le 2^n$$
 for $n \ge 4$.

$$n^2 \le 2^n$$
 for $n \ge 4$.

$$(n+1)^2 = n^2 + 2n + 1$$

$$n^2 \le 2^n$$
 for $n \ge 4$.

$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + 1$$

$$n^2 \le 2^n$$
 for $n \ge 4$.

$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + 1 \leq 2^n + 2^n = 2^{n+1}$$

What to do with the 2n + 1?

Would be fine if $2n + 1 \leq 2^n$.

$$n^2 \le 2^n$$
 for $n \ge 4$.

$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + 1 \leq 2^n + 2^n = 2^{n+1}$$

What to do with the 2n + 1?

Would be fine if $2n + 1 \leq 2^n$.

With induction, it can be easier to prove a stronger claim.

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

Proof. $Q(n): (i) n^2 \leq 2^n$ AND $(ii) 2n + 1 \leq 2^n$. 1: [Base case] Q(4) claims $(i) 4^2 \leq 2^4$ AND $(ii) 2 \times 4 + 1 \leq 2^4$. Both clearly T.

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

Proof. $Q(n): (i) \ n^2 \le 2^n$ AND $(ii) \ 2n+1 \le 2^n$.

- 1: [Base case] Q(4) claims (i) $4^2 \le 2^4$ AND (ii) $2 \times 4 + 1 \le 2^4$. Both clearly T.
- 2: [Induction step] Show $Q(n) \rightarrow Q(n+1)$ for $n \ge 4$ (direct proof).

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

Proof. $Q(n): (i) \ n^2 \leq 2^n$ AND $(ii) \ 2n+1 \leq 2^n$. 1: [Base case] Q(4) claims $(i) \ 4^2 \leq 2^4$ AND $(ii) \ 2 \times 4 + 1 \leq 2^4$. Both clearly T.

2: **[Induction step]** Show $Q(n) \rightarrow Q(n+1)$ for $n \ge 4$ (direct proof). Assume (induction hypothesis) Q(n) is T: (i) $n^2 \le 2^n$ AND (ii) $2n + 1 \le 2^n$. Show Q(n+1) is T: (i) $(n+1)^2 \le 2^{n+1}$ AND (ii) $2(n+1) + 1 \le 2^{n+1}$.

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

Proof. $Q(n): (i) \ n^2 \leq 2^n$ AND $(ii) \ 2n+1 \leq 2^n$. 1: [Base case] Q(4) claims $(i) \ 4^2 \leq 2^4$ AND $(ii) \ 2 \times 4 + 1 \leq 2^4$. Both clearly T.

2: **[Induction step]** Show $Q(n) \rightarrow Q(n+1)$ for $n \ge 4$ (direct proof). Assume (induction hypothesis) Q(n) is T: (i) $n^2 \le 2^n$ AND (ii) $2n+1 \le 2^n$. Show Q(n+1) is T: (i) $(n+1)^2 \le 2^{n+1}$ AND (ii) $2(n+1)+1 \le 2^{n+1}$.

(i)
$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2^n = 2^{n+1} \checkmark$$

(because from the induction hypothesis $n^2 \leq 2^n$ and $2n+1 \leq 2^n$)

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

Proof. $Q(n): (i) n^2 \leq 2^n$ AND $(ii) 2n + 1 \leq 2^n$. 1: [Base case] Q(4) claims $(i) 4^2 \leq 2^4$ AND $(ii) 2 \times 4 + 1 \leq 2^4$. Both clearly T.

2: **[Induction step]** Show $Q(n) \rightarrow Q(n+1)$ for $n \ge 4$ (direct proof). Assume (induction hypothesis) Q(n) is T: (i) $n^2 \le 2^n$ AND (ii) $2n+1 \le 2^n$. Show Q(n+1) is T: (i) $(n+1)^2 \le 2^{n+1}$ AND (ii) $2(n+1)+1 \le 2^{n+1}$.

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

(because from the induction hypothesis $n^2 \leq 2^n$ and $2n + 1 \leq 2^n$)
(ii) $2(n+1) + 1 = 2 + 2n + 1 \leq 2^n + 2^n = 2^{n+1}$
(because $2 \leq 2^n$ and from the induction hypothesis $2n + 1 \leq 2^n$)

$$Q(n): (i) \ n^2 \le 2^n \qquad \text{AND} \qquad (ii) \ 2n+1 \le 2^n.$$
$$\boxed{Q(4)} \to Q(5) \to Q(6) \to Q(7) \to Q(8) \to Q(9) \to \cdots$$

Proof. $Q(n): (i) \ n^2 \leq 2^n$ AND $(ii) \ 2n+1 \leq 2^n$. 1: [Base case] Q(4) claims $(i) \ 4^2 \leq 2^4$ AND $(ii) \ 2 \times 4 + 1 \leq 2^4$. Both clearly T.

2: **[Induction step]** Show $Q(n) \rightarrow Q(n+1)$ for $n \ge 4$ (direct proof). Assume (induction hypothesis) Q(n) is T: (i) $n^2 \le 2^n$ AND (ii) $2n + 1 \le 2^n$. Show Q(n+1) is T: (i) $(n+1)^2 \le 2^{n+1}$ AND (ii) $2(n+1) + 1 \le 2^{n+1}$.

(i)
$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2^n = 2^{n+1} \checkmark$$

(because from the induction hypothesis $n^2 \leq 2^n$ and $2n + 1 \leq 2^n$)
(ii) $2(n+1) + 1 = 2 + 2n + 1 \leq 2^n + 2^n = 2^{n+1} \checkmark$
(because $2 \leq 2^n$ and from the induction hypothesis $2n + 1 \leq 2^n$)
So, $Q(n+1)$ is T.

3: By induction, Q(n) is $T \forall n \ge 4$.









L-Tile Land

Can you tile a $2^n \times 2^n$ patio missing a center square. You have only \blacksquare – tiles?





















TINKER!



P(n): The $2^n \times 2^n$ grid minus a center-square can be L-tiled.

Suppose P(n) is T. What about P(n+1)?

Suppose P(n) is T. What about P(n+1)?

The $2^{n+1} \times 2^{n+1}$ patio can be decomposed into four $2^n \times 2^n$ patios.



Suppose P(n) is T. What about P(n+1)?

The $2^{n+1} \times 2^{n+1}$ patio can be decomposed into four $2^n \times 2^n$ patios.



Suppose P(n) is T. What about P(n+1)?

The $2^{n+1} \times 2^{n+1}$ patio can be decomposed into four $2^n \times 2^n$ patios.



Problem. Corner squares are missing. P(n) can be used only if center-square is missing.

Suppose P(n) is T. What about P(n+1)?

The $2^{n+1} \times 2^{n+1}$ patio can be decomposed into four $2^n \times 2^n$ patios.



Problem. Corner squares are missing. P(n) can be used only if center-square is missing. **Solution.** Strengthen claim to also include patios missing corner-squares.

Q(n): (i) The $2^n \times 2^n$ grid missing a **center-square** can be *L*-tiled; AND (ii) The $2^n \times 2^n$ grid missing a **corner-square** can be *L*-tiled. Assume $Q(n) : {(i) \text{ The } 2^n \times 2^n \text{ grid missing a center-square can be L-tiled; AND} (ii) \text{ The } 2^n \times 2^n \text{ grid missing a corner-square can be L-tiled.}$

Induction step: Must prove two things for Q(n+1), namely (i) and (ii).

Assume $Q(n) : {(i) \text{ The } 2^n \times 2^n \text{ grid missing a center-square can be L-tiled; AND} (ii) \text{ The } 2^n \times 2^n \text{ grid missing a corner-square can be L-tiled.}$

Induction step: Must prove two things for Q(n+1), namely (i) and (ii).

(i) Center square missing.



use Q(n) with corner squares.
Assume Q(n): (i) The $2^n \times 2^n$ grid missing a **center-square** can be *L*-tiled; AND (ii) The $2^n \times 2^n$ grid missing a **corner-square** can be *L*-tiled.

Induction step: Must prove two things for Q(n+1), namely (i) and (ii).





use Q(n) with corner squares.

(ii) Corner square missing.



use Q(n) with corner squares.

Assume $Q(n) : {(i) \text{ The } 2^n \times 2^n \text{ grid missing a center-square can be L-tiled; AND} (ii) \text{ The } 2^n \times 2^n \text{ grid missing a corner-square can be L-tiled.}$

Induction step: Must prove two things for Q(n+1), namely (i) and (ii).



(i) Center square missing.

use Q(n) with corner squares.

(ii) Corner square missing.



use Q(n) with corner squares.

Your task: Add base cases and complete the formal proof.

Exercise 6.4. What if the missing square is some random square? Strengthen further.

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10.$$
 (Exercise 6.2)

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10. \tag{Exercise 6.2}$$

$$(n+2)^3 = n^3 + 6n^2 + 12n + 8$$

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10. \tag{Exercise 6.2}$$

$$(n+2)^3 = n^3 + 6n^2 + 12n + 8$$

< $n^3 + n \cdot n^2 + n^2 \cdot n + n^3$ ($n \ge 10 \rightarrow 6 < n; \ 12 < n^2; \ 8 < n^3$)

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10. \tag{Exercise 6.2}$$

$$(n+2)^3 = n^3 + 6n^2 + 12n + 8$$

< $n^3 + n \cdot n^2 + n^2 \cdot n + n^3$ $(n \ge 10 \rightarrow 6 < n; 12 < n^2; 8 < n^3)$
= $4n^3$

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10. \tag{Exercise 6.2}$$

$$(n+2)^3 = n^3 + 6n^2 + 12n + 8$$

$$< n^3 + n \cdot n^2 + n^2 \cdot n + n^3 \qquad (n \ge 10 \to 6 < n; \ 12 < n^2; \ 8 < n^3)$$

$$= 4n^3 < 4 \cdot 2^n = 2^{n+2} \qquad (P(n) \text{ gives } n^3 < 2^n)$$

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10. \tag{Exercise 6.2}$$

Suppose P(n) is T. Consider $P(n+2) : (n+2)^3 < 2^{n+2}$?

$$(n+2)^{3} = n^{3} + 6n^{2} + 12n + 8$$

$$< n^{3} + n \cdot n^{2} + n^{2} \cdot n + n^{3}$$

$$= 4n^{3} < 4 \cdot 2^{n} = 2^{n+2}$$

$$(n \ge 10 \to 6 < n; \ 12 < n^{2}; \ 8 < n^{3})$$

$$(P(n) \text{ gives } n^{3} < 2^{n})$$

 $P(n) \rightarrow P(n+2).$

$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10. \tag{Exercise 6.2}$$

Suppose P(n) is T. Consider $P(n+2) : (n+2)^3 < 2^{n+2}$?

$$(n+2)^{3} = n^{3} + 6n^{2} + 12n + 8$$

$$< n^{3} + n \cdot n^{2} + n^{2} \cdot n + n^{3}$$

$$= 4n^{3} < 4 \cdot 2^{n} = 2^{n+2}$$

$$(n \ge 10 \to 6 < n; \ 12 < n^{2}; \ 8 < n^{3})$$

$$(P(n) \text{ gives } n^{3} < 2^{n})$$

$$P(n) \rightarrow P(n+2).$$

Base case. $P(10) : 10^3 < 2^{10}$



$$P(n): n^3 < 2^n, \qquad \text{for } n \ge 10.$$
 (Exercise 6.2)

Suppose P(n) is T. Consider $P(n+2) : (n+2)^3 < 2^{n+2}$?

$$(n+2)^{3} = n^{3} + 6n^{2} + 12n + 8$$

$$< n^{3} + n \cdot n^{2} + n^{2} \cdot n + n^{3}$$

$$= 4n^{3} < 4 \cdot 2^{n} = 2^{n+2}$$

$$(n \ge 10 \to 6 < n; \ 12 < n^{2}; \ 8 < n^{3})$$

$$(P(n) \text{ gives } n^{3} < 2^{n})$$

$$P(n) \to P(n+2).$$

Base cases. $P(10): 10^3 < 2^{10}$ and $P(11): 11^3 < 2^{11}$



Induction. One base case.

$$P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow P(5) \rightarrow \cdots$$

Induction. One base case.

$$P(1) \to P(2) \to P(3) \to P(4) \to P(5) \to \cdots$$

Leaping Induction. More than one base case.

P(1) P(2)
$$P(3)$$
 $P(4)$ $P(5)$ $P(6)$ $P(7)$ $P(8)$ $P(9)$ $P(10)$ $P(11)$ $P(12)$ · · ·

Induction. One base case.

$$P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow P(5) \rightarrow \cdots$$

Leaping Induction. More than one base case.

Example. Postage greater than 5¢ can be made using 3¢ and 4¢ stamps.

3¢	4¢	5¢	6¢	7¢	8¢	9¢	10¢	11¢	12¢	•••
3	4	_	$3,\!3$	$3,\!4$	$4,\!4$	$3,\!3,\!3$	3,3,4	3,4,4	4,4,4	•••

Induction. One base case.

$$P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow P(5) \rightarrow \cdots$$

Leaping Induction. More than one base case.

Example. Postage greater than 5¢ can be made using 3¢ and 4¢ stamps.

3¢	4¢	5¢	6¢	7¢	8¢	9¢	10¢	11¢	12¢	•••
3	4	_	$3,\!3$	$3,\!4$	$4,\!4$	$3,\!3,\!3$	3,3,4	3,4,4	4,4,4	•••

P(n): Postage of n cents can be made using only 3¢ and 4¢ stamps.

Induction. One base case.

$$P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow P(5) \rightarrow \cdots$$

Leaping Induction. More than one base case.

Example. Postage greater than 5¢ can be made using 3¢ and 4¢ stamps.

3¢	4¢	5¢	6¢	7¢	8¢	9¢	10¢	11¢	12c	•••
3	4	_	$3,\!3$	$3,\!4$	$4,\!4$	3,3,3	3,3,4	3,4,4	4,4,4	

P(n): Postage of n cents can be made using only 3¢ and 4¢ stamps. $P(n) \rightarrow P(n+3)$

(add a $3\mathfrak{c}$ stamp to n)

Induction. One base case.

$$P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow P(5) \rightarrow \cdots$$

Leaping Induction. More than one base case.

Example. Postage greater than 5¢ can be made using 3¢ and 4¢ stamps.

3¢	4¢	5¢	6¢	7¢	8¢	9¢	10¢	11¢	12¢	•••
3	4	_	$3,\!3$	$3,\!4$	$4,\!4$	3,3,3	3,3,4	3,4,4	4,4,4	•••

P(n): Postage of n cents can be made using only 3¢ and 4¢ stamps.

 $P(n) \rightarrow P(n+3)$ (add a 3¢ stamp to n) Base cases: 6¢, 7¢, 8¢.

Practice. Exercise 6.6

Fundamental Theorem of Arithmetic

 $2015 = 5 \times 13 \times 31.$

Theorem. (The Primes $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ are the atoms for numbers.)

Suppose $n \ge 2$. Then,



If The representation of n as a product of primes is unique (up to reordering).

P(n): n is a product of primes.

Theorem. (The Primes $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ are the atoms for numbers.)

Suppose $n \ge 2$. Then,

\bigcirc *n* can be written as a product of factors all of which are prime.

The representation of n as a product of primes is unique (up to reordering).

P(n): n is a product of primes.

What's the first thing we do?

Theorem. (The Primes $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ are the atoms for numbers.)

Suppose $n \ge 2$. Then,



The representation of n as a product of primes is unique (up to reordering).

P(n): n is a product of primes.

What's the first thing we do? **TINKER!**

 $2016 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 7.$

Theorem. (The Primes $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ are the atoms for numbers.)

Suppose $n \ge 2$. Then,



The representation of n as a product of primes is unique (up to reordering).

P(n): n is a product of primes.

What's the first thing we do? **TINKER!**

 $2016 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 7.$

Wow! No similarity between the factors of 2015 and those of 2016.

Theorem. (The Primes $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ are the atoms for numbers.)

Suppose $n \ge 2$. Then,



The representation of n as a product of primes is unique (up to reordering).

P(n): n is a product of primes.

What's the first thing we do? **TINKER!**

 $2016 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 7.$

Wow! No similarity between the factors of 2015 and those of 2016.

How will P(n) help us to prove P(n+1)?

Theorem. (The Primes $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ are the atoms for numbers.)

Suppose $n \ge 2$. Then,



The representation of n as a product of primes is unique (up to reordering).

P(n): n is a product of primes.

What's the first thing we do? **TINKER!**

 $2016 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 7.$

Wow! No similarity between the factors of 2015 and those of 2016.

How will P(n) help us to prove P(n+1)?

 $2016 = 32 \times 63$ $P(32) \land P(63) \rightarrow P(2016)$

(like leaping induction)

 $2016 = 32 \times 63$ $P(32) \land P(63) \rightarrow P(2016)$

(like leaping induction)

Much Stronger Claim:

 $Q(n): 2, 3, \ldots, n$ are all products of primes.

 $2016 = 32 \times 63$ $P(32) \land P(63) \rightarrow P(2016)$

(like leaping induction)

Much Stronger Claim:

Q(n): 2, 3, ..., n are all products of primes. P(n): n is a product of primes.

(Compare)

 $Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$

 $2016 = 32 \times 63$ $P(32) \land P(63) \rightarrow P(2016)$

(like leaping induction)

Much Stronger Claim:

 $Q(n): 2, 3, \ldots, n$ are all products of primes. P(n): n is a product of primes.

(Compare)

 $Q(n) = P(2) \wedge P(3) \wedge P(4) \wedge \cdots \wedge P(n).$

Surprise! The much stronger claim is *much* easier to prove. Also, $Q(n) \rightarrow P(n)$.

Fundamental Theorem of Arithmetic: Proof of Part (i)

P(n): n is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.)

Fundamental Theorem of Arithmetic: Proof of Part (i)

P(n): n is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.)

1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

Fundamental Theorem of Arithmetic: Proof of Part (i)

P(n): n is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.)

- 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.
- 2: [Induction step] Show $Q(n) \rightarrow Q(n+1)$ for $n \ge 2$ (direct proof).

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

2: **[Induction step]** Show $Q(n) \to Q(n+1)$ for $n \ge 2$ (direct proof). Assume Q(n) is T: each of $2, 3, \ldots, n$ are a product of primes. Show Q(n+1) is T: each of $2, 3, \ldots, n, n+1$ is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

2: [Induction step] Show Q(n) → Q(n + 1) for n ≥ 2 (direct proof). Assume Q(n) is T: each of 2, 3, ..., n are a product of primes. Show Q(n + 1) is T: each of 2, 3, ..., n, n + 1 is a product of primes. Since we assumed Q(n), we already have that 2, 3, ..., n are products of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

2: **[Induction step]** Show $Q(n) \to Q(n+1)$ for $n \ge 2$ (direct proof). Assume Q(n) is T: each of $2, 3, \ldots, n$ are a product of primes. Show Q(n+1) is T: each of $2, 3, \ldots, n, n+1$ is a product of primes. Since we assumed Q(n), we already have that $2, 3, \ldots, n$ are products of primes. **To prove** Q(n+1), we only need to prove n+1 is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

2: [Induction step] Show Q(n) → Q(n + 1) for n ≥ 2 (direct proof). Assume Q(n) is T: each of 2, 3, ..., n are a product of primes. Show Q(n + 1) is T: each of 2, 3, ..., n, n + 1 is a product of primes. Since we assumed Q(n), we already have that 2, 3, ..., n are products of primes. To prove Q(n + 1), we only need to prove n + 1 is a product of primes.
• n + 1 is prime. Done (nothing to prove).

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

- 2: **[Induction step]** Show $Q(n) \to Q(n+1)$ for $n \ge 2$ (direct proof). Assume Q(n) is T: each of $2, 3, \ldots, n$ are a product of primes. Show Q(n+1) is T: each of $2, 3, \ldots, n, n+1$ is a product of primes. Since we assumed Q(n), we already have that $2, 3, \ldots, n$ are products of primes. **To prove** Q(n+1), we only need to prove n+1 is a product of primes.
 - n + 1 is prime. Done (nothing to prove).
 - n+1 is not prime, $n+1 = k\ell$, where $2 \le k, \ell \le n$.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

- 2: [Induction step] Show Q(n) → Q(n + 1) for n ≥ 2 (direct proof). Assume Q(n) is T: each of 2, 3, ..., n are a product of primes. Show Q(n + 1) is T: each of 2, 3, ..., n, n + 1 is a product of primes. Since we assumed Q(n), we already have that 2, 3, ..., n are products of primes. To prove Q(n + 1), we only need to prove n + 1 is a product of primes.
 • n + 1 is prime. Done (nothing to prove).
 • n + 1 is prime. Done (nothing to prove).
 - n + 1 is not prime, $n + 1 = k\ell$, where $2 \le k, \ell \le n$. $P(k) \to k$ is a product of primes. $P(\ell) \to \ell$ is a product of primes.
P(n): n is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

- 2: [Induction step] Show Q(n) → Q(n + 1) for n ≥ 2 (direct proof). Assume Q(n) is T: each of 2, 3, ..., n are a product of primes. Show Q(n + 1) is T: each of 2, 3, ..., n, n + 1 is a product of primes. Since we assumed Q(n), we already have that 2, 3, ..., n are products of primes. To prove Q(n + 1), we only need to prove n + 1 is a product of primes.
 • n + 1 is prime. Done (nothing to prove).
 - n + 1 is not prime, $n + 1 = k\ell$, where $2 \le k, \ell \le n$. $P(k) \to k$ is a product of primes. $P(\ell) \to \ell$ is a product of primes. $n + 1 = k\ell$ is a product of primes and Q(n + 1) is T.

P(n): n is a product of primes.

$$Q(n) = P(2) \land P(3) \land P(4) \land \dots \land P(n).$$

Proof. (By Induction that Q(n) is T for $n \ge 2$.) 1: [Base case] Q(1) claims that 2 is a product of primes, which is clearly T.

- 2: [Induction step] Show Q(n) → Q(n + 1) for n ≥ 2 (direct proof). Assume Q(n) is T: each of 2, 3, ..., n are a product of primes. Show Q(n + 1) is T: each of 2, 3, ..., n, n + 1 is a product of primes. Since we assumed Q(n), we already have that 2, 3, ..., n are products of primes. To prove Q(n + 1), we only need to prove n + 1 is a product of primes.
 • n + 1 is prime. Done (nothing to prove).
 - n + 1 is not prime, $n + 1 = k\ell$, where $2 \le k, \ell \le n$. $P(k) \to k$ is a product of primes. $P(\ell) \to \ell$ is a product of primes. $n + 1 = k\ell$ is a product of primes and Q(n + 1) is T.

3: By induction, Q(n) is $T \forall n \ge 2$.

Q(n) : each of P(1), P(2), ..., P(n) are T.

Ordinary Induction

Base Case

Prove P(1)

	Ordinary Induction
Base Case	Prove $P(1)$
Induction Step	Assume: $P(n)$ Prove: $P(n+1)$

	Ordinary Induction	Strong Induction
Base Case	Prove $P(1)$	Prove $Q(1) = P(1)$
Induction Step	Assume: $P(n)$	
	Prove: $P(n+1)$	

	Ordinary Induction	Strong Induction
Base Case	Prove $P(1)$	Prove $Q(1) = P(1)$
Induction Step	Assume: $P(n)$	Assume: $Q(n) = P(1) \wedge P(2) \wedge \cdots \wedge P(n)$
	Prove: $P(n+1)$	

	Ordinary Induction	Strong Induction
Base Case	Prove $P(1)$	Prove $Q(1) = P(1)$
Induction Step	Assume: $P(n)$	Assume: $Q(n) = P(1) \land P(2) \land \dots \land P(n)$
	Prove: $P(n+1)$	Prove: $P(n+1)$

Q(n) : each of P(1), P(2), ..., P(n) are T.

	Ordinary Induction	Strong Induction
Base Case	Prove $P(1)$	Prove $Q(1) = P(1)$
Induction Step	Assume: $P(n)$	Assume: $Q(n) = P(1) \wedge P(2) \wedge \cdots \wedge P(n)$
	Prove: $P(n+1)$	Prove: $P(n+1)$

Strong induction is always easier.

$$22 = 2^1 + 2^2 + 2^4. \qquad (22_{\text{binary}} = \overset{2^4}{1} \overset{2^3}{0} \overset{2^2}{1} \overset{2^1}{1} \overset{2^0}{0}.)$$

Every $n \ge 1$ Has a Binary Expansion

P(n): Every $n \ge 1$ is a sum of distinct powers of two (its binary expansion).

$$22 = 2^1 + 2^2 + 2^4. \qquad (22_{\text{binary}} = \overset{2^4}{1} \overset{2^3}{0} \overset{2^2}{1} \overset{2^1}{1} \overset{2^0}{0}.)$$

Base Case: P(1) is T: $1 = 2^{0}$

$$22 = 2^1 + 2^2 + 2^4. \qquad (22_{\text{binary}} = \overset{2^4}{1} \overset{2^3}{0} \overset{2^2}{1} \overset{2^1}{1} \overset{2^0}{0}.)$$

Base Case: P(1) is T: $1 = 2^{0}$

Strong Induction: Assume $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ and prove P(n+1).

$$22 = 2^1 + 2^2 + 2^4. \qquad (22_{\text{binary}} = \overset{2^4}{1} \overset{2^3}{0} \overset{2^2}{1} \overset{2^1}{1} \overset{2^0}{0}.)$$

Base Case: P(1) is T: $1 = 2^{0}$

Strong Induction: Assume $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ and prove P(n+1).

If n is even, then $n + 1 = 2^0$ + binary expansion of n, e.g. $23 = 2^0 + \underbrace{2^1 + 2^2 + 2^4}_{22}$

$$22 = 2^1 + 2^2 + 2^4. \qquad (22_{\text{binary}} = \overset{2^4}{1} \overset{2^3}{0} \overset{2^2}{1} \overset{2^1}{1} \overset{2^0}{0}.)$$

Base Case: P(1) is T: $1 = 2^{0}$

Strong Induction: Assume $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ and prove P(n+1).

If n is even, then $n + 1 = 2^0$ + binary expansion of n, e.g. $23 = 2^0 + \underbrace{2^1 + 2^2 + 2^4}_{22}$

If n is odd, then multiply each term in the expansion of $\frac{1}{2}(n+1)$ by 2 to get n+1. e.g. $24 = 2 \times (\underbrace{2^2 + 2^3}_{12}) = 2^3 + 2^4$

Exercise. Give the formal proof by strong induction.

Tournament rankings, greedy or recursive algorithms, games of strategy,

Equal Pile Nim (old English/German: to steal or pilfer)

00000

Tournament rankings, greedy or recursive algorithms, games of strategy,

Equal Pile Nim (old English/German: to steal or pilfer)











Tournament rankings, greedy or recursive algorithms, games of strategy,



P(n): Player 2 can win the game that starts with n pennies in each row.

Tournament rankings, greedy or recursive algorithms, games of strategy,



P(n): Player 2 can win the game that starts with n pennies in each row.

Equalization strategy:



Tournament rankings, greedy or recursive algorithms, games of strategy,



P(n): Player 2 can win the game that starts with n pennies in each row.

Equalization strategy:

$$\begin{array}{c|c} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \end{array} \begin{array}{c} \hline \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array} \begin{array}{c} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \end{array}$$

Tournament rankings, greedy or recursive algorithms, games of strategy,



P(n): Player 2 can win the game that starts with n pennies in each row.

Equalization strategy:

$$\begin{array}{c|c} \mathbf{0} \mathbf{0} \mathbf{0} \mathbf{0} \mathbf{0} \\ \mathbf{0} \mathbf{0} \mathbf{0} \mathbf{0} \end{array} \xrightarrow{\text{player 1}} \begin{array}{c} \mathbf{0} \mathbf{0} \mathbf{0} \mathbf{0} \mathbf{0} \\ \mathbf{0} \mathbf{0} \end{array} \xrightarrow{\text{player 2}} \begin{array}{c} \mathbf{0} \mathbf{0} \\ \mathbf{0} \mathbf{0} \end{array}$$

Player 2 can always return the game to *smaller* equal piles.

Tournament rankings, greedy or recursive algorithms, **games of strategy**,



Equalization strategy:

 $\begin{array}{c|c} \mathbf{OOOOO} & \underline{\text{player 1}} & \mathbf{OOOOO} & \underline{\text{player 2}} & \mathbf{OO} \\ \mathbf{OO} & \mathbf{OO} & \mathbf{OO} & \mathbf{OO} & \mathbf{OO} \end{array}$

Player 2 can always return the game to *smaller* equal piles. If Player 2 wins the smaller game, Player 2 wins the larger game. That's strong induction!

Exercise. Give the full formal proof by strong induction.

Challenge. What about more than 2 piles. What about unequal piles. (Problem 6.20).

Uniqueness of binary representation as a sum of distinct powers of 2:

Problem 6.27

General Nim:

Problem 6.39



Please, Please! Become Good at Induction!

	Checklist When Approaching an Induction Problem.
٢	Are you trying to prove a "For all " claim?
٢	Identify the claim $P(n)$, especially the parameter n . Here is an example.

	Checklist When Approaching an Induction Problem.
٢	Are you trying to prove a "For all " claim?
٢	Identify the claim $P(n)$, especially the parameter n . Here is an example. Prove: geometric mean \leq arithmetic mean.

	Checklist When Approaching an Induction Problem.
٢	Are you trying to prove a "For all" claim?
٢	Identify the claim $P(n)$, especially the parameter n . Here is an example. Prove: geometric mean \leq arithmetic mean. What is $P(n)$?
















