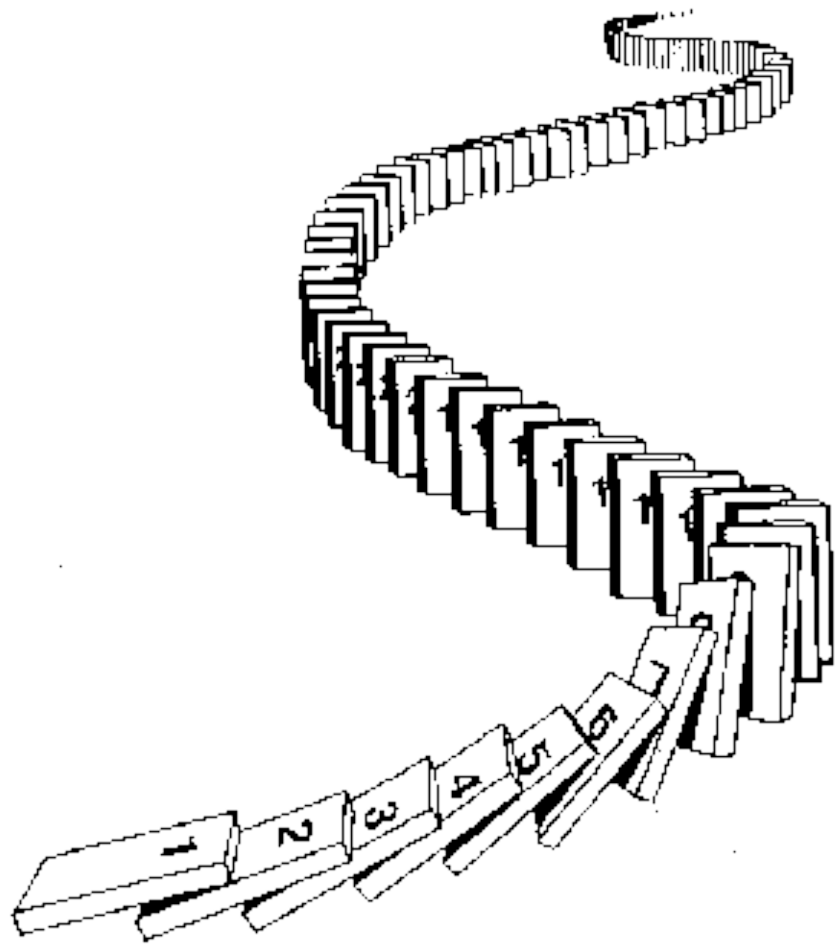
CSE 311: Foundations of Computing

Lecture 15: Induction & Strong Induction



But there such a property of the natural numbers!

Domain: Natural Numbers

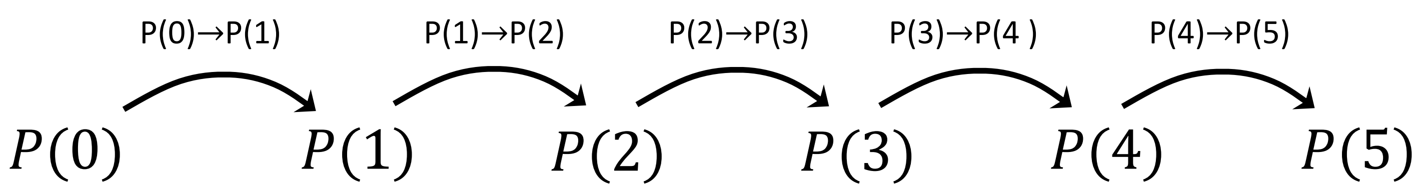
$$\frac{P(0) \qquad \forall k\,(P(k) \longrightarrow P(k+1))}{\therefore \forall n\ P(n)}$$

Induction Is A Rule of Inference

Domain: Natural Numbers

$$\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \\ \hline \therefore \forall n\ \ P(n) \end{array}$$

How do the givens prove P(5)?



First, we have P(0).
Since P(n) ⟶ P(n+1) for all n, we have P(0) ⟶ P(1).
Since P(0) is true and P(0) ⟶ P(1), by Modus Ponens, P(1) is true.
Since P(n) ⟶ P(n+1) for all n, we have P(1) ⟶ P(2).
Since P(1) is true and P(1) ⟶ P(2), by Modus Ponens, P(2) is true.

Translating to an English Proof

$$P(0)$$
$$\forall k\ (P(k) \longrightarrow P(k+1))$$
$$\therefore \forall n\ \ P(n)$$

1. Prove P(0) — **Base Case**

2. Let k be an arbitrary integer ≥ 0
   3.1. Suppose that P(k) is true — **Inductive Hypothesis**
   3.2. ...
   3.3. Prove P(k+1) is true — **Inductive Step**

3.	$P(k) \rightarrow P(k+1)$	Direct Proof Rule
4.	$\forall k\ (P(k) \rightarrow P(k+1))$	Intro $\forall$: 2, 3
5.	$\forall n\ P(n)$	Induction: 1, 4

Conclusion

Inductive Proofs In 5 Easy Steps

1. "Let $P(n)$ be… . We will show that $P(n)$ is true for all integers $n \geq 0$ by induction."
2. "Base Case:" Prove $P(0)$
3. "Inductive Hypothesis:

   Assume $P(k)$ is true for some arbitrary integer $k \geq 0$"
4. "Inductive Step:" Prove that $P(k+1)$ is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume $P(k+1)$!!)
5. "Conclusion: $P(n)$ is true for all integers $n \geq 0$"

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**

Summation Notation

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + 3 + \ldots + n$$

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**

Summation Notation

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + 3 + \ldots + n$$

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0**. I.e., suppose** 1 + 2 + …+ k = k(k+1)/2

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0. **I.e., suppose** 1 + 2 + …+ k = k(k+1)/2
4. **Induction Step:**

   Goal: Show P(k+1), **i.e. show** 1 + 2 + …+ k+ (k+1) = (k+1)(k+2)/2

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$**. I.e., suppose** 1 + 2 + …+ k = k(k+1)/2
4. **Induction Step:**

$$
\begin{aligned}
1 + 2 + \ldots + k + (k+1) &= (1 + 2 + \ldots + k) + (k+1) \\
&= k(k+1)/2 + (k+1) \quad \textbf{by IH} \\
&= (k+1)(k/2 + 1) \\
&= (k+1)(k+2)/2
\end{aligned}
$$

   So, we have shown 1 + 2 + … + k + (k+1) = (k+1)(k+2)/2,

   which is exactly P(k+1).

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

Induction: Changing the start line

- **What if we want to prove that $P(n)$ is true for all integers $n \geq b$ for some integer b?**

- **Define predicate $Q(k) = P(k+b)$ for all k.**
  - **Then** $\forall n\, Q(n) \equiv \forall n \geq b\ \ P(n)$

- **Ordinary induction for Q:**
  - **Prove** $Q(0) \equiv P(b)$
  - **Prove**
    $\forall k\, \big(Q(k) \longrightarrow Q(k+1)\big) \equiv \forall k \geq b\big(P(k) \longrightarrow P(k+1)\big)$

Inductive Proofs In 5 Easy Steps

1. "Let $P(n)$ be... . We will show that $P(n)$ is true for all integers $n \geq \boldsymbol{b}$ by induction."
2. "Base Case:" Prove $P(\boldsymbol{b})$
3. "Inductive Hypothesis:

   Assume $P(k)$ is true for an arbitrary integer $k \geq \boldsymbol{b}$"
4. "Inductive Step:" Prove that $P(k+1)$ is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume $P(k+1)$!!)
5. "Conclusion: $P(n)$ is true for all integers $n \geq \boldsymbol{b}$"

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. Let P(n) be "$3^n \geq n^2+3$". We will show P(n) is true for all integers $n \geq 2$ by induction.

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. **Let** P(n) **be** "$3^n \geq n^2+3$". **We will show** P(n) **is true for all integers** $n \geq 2$ **by induction.**
2. **Base Case** (n=2): $3^2 = 9 \geq 7 = 4+3 = 2^2+3$ **so** P(2) **is true.**

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. **Let** P(n) **be** "$3^n \geq n^2+3$". **We will show** P(n) **is true for all integers** $n \geq 2$ **by induction.**
2. **Base Case** (n=2): $3^2 = 9 \geq 7 = 4+3 = 2^2+3$ **so** P(2) **is true.**
3. **Inductive Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 2$. **I.e., suppose** $3^k \geq k^2+3$.

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. **Let** P(n) **be** "$3^n \geq n^2+3$". **We will show** P(n) **is true for all integers** $n \geq 2$ **by induction.**
2. **Base Case** (n=2): $3^2 = 9 \geq 7 = 4+3 = 2^2+3$ **so** P(2) **is true.**
3. **Inductive Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 2$. **I.e., suppose** $3^k \geq k^2+3$.
4. **Inductive Step:**

Goal: Show P(k+1), **i.e. show** $3^{k+1} \geq (k+1)^2+3$

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. **Let** P(n) **be** "$3^n \geq n^2+3$". **We will show** P(n) **is true for all integers** $n \geq 2$ **by induction.**
2. **Base Case** (n=2): $3^2 = 9 \geq 7 = 4+3 = 2^2+3$ **so** P(2) **is true.**
3. **Inductive Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 2$. **I.e., suppose** $3^k \geq k^2+3$.
4. **Inductive Step:**

Goal: Show P(k+1), **i.e. show** $3^{k+1} \geq (k+1)^2+3=k^2+2k+4$

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. **Let** P(n) **be** "$3^n \geq n^2+3$". **We will show** P(n) **is true for all integers** $n \geq 2$ **by induction.**
2. **Base Case** (n=2): $3^2 = 9 \geq 7 = 4+3 = 2^2+3$ **so** P(2) **is true.**
3. **Inductive Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 2$**. I.e., suppose** $3^k \geq k^2+3$**.**
4. **Inductive Step:**

Goal: Show P(k+1)**, i.e. show** $3^{k+1} \geq (k+1)^2+3=k^2+2k+4$

$3^{k+1} = 3(3^k)$

$\geq 3(k^2+3)$ **by the IH**

$= 3k^2+9$

$= k^2+2k^2+9$

$\geq k^2+2k+4 = (k+1)^2+3$ **since** $k \geq 1$.

Therefore P(k+1) **is true.**

Prove $3^n \geq n^2 + 3$ for all $n \geq 2$

1. **Let** P(n) **be** "$3^n \geq n^2+3$". **We will show** P(n) **is true for all integers** $n \geq 2$ **by induction.**
2. **Base Case** (n=2): $3^2 = 9 \geq 7 = 4+3 = 2^2+3$ **so** P(2) **is true.**
3. **Inductive Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 2$. **I.e., suppose** $3^k \geq k^2+3$.
4. **Inductive Step:**

   Goal: Show P(k+1), **i.e. show** $3^{k+1} \geq (k+1)^2+3=k^2+2k+4$

   $3^{k+1} = 3(3^k)$

   $\geq 3(k^2+3)$ **by the IH**

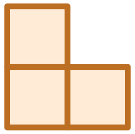
   $= k^2+2k^2+9$

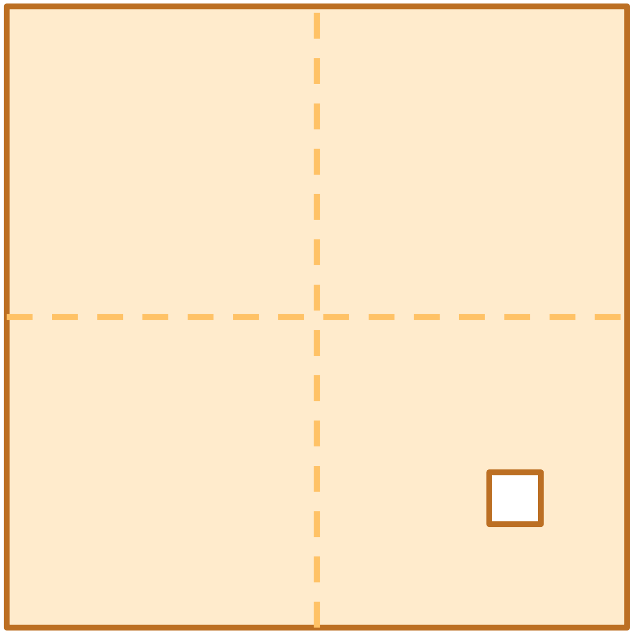
   $\geq k^2+2k+4 = (k+1)^2+3$ **since** $k \geq 1$.

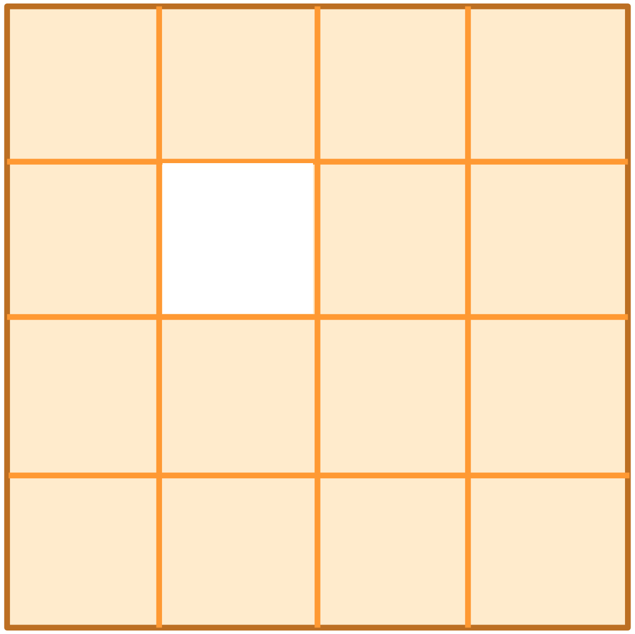
   Therefore P(k+1) **is true.**

5. **Thus** P(n) **is true for all integers** $n \geq 2$, **by induction.**

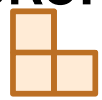
Checkerboard Tiling

- Prove that a $2^n \times 2^n$ checkerboard with one square removed can be tiled with: 

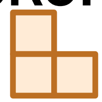
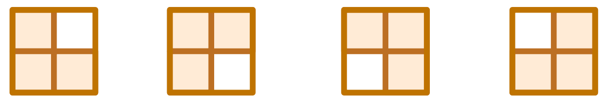




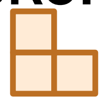
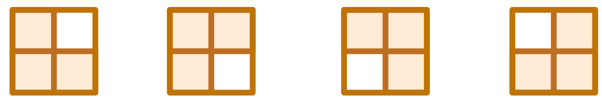
Checkerboard Tiling

1. **Let** $P(n)$ **be any** $2^n \times 2^n$ **checkerboard with one square removed can be tiled with**  **.**
   We prove $P(n)$ **for all** $n \geq 1$ **by induction on** n.

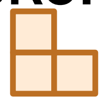
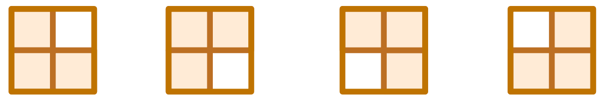
Checkerboard Tiling

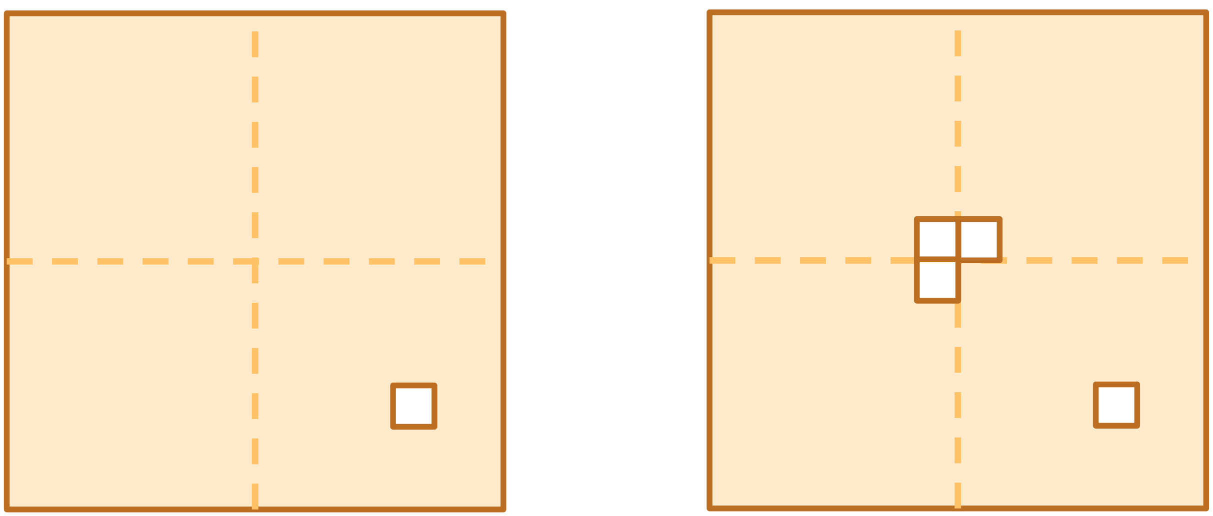
1. **Let** $P(n)$ **be any** $2^n \times 2^n$ **checkerboard with one square removed can be tiled with**  **.**
   We prove $P(n)$ **for all** $n \geq 1$ **by induction on** n.
2. **Base Case:** $n=1$ 

Checkerboard Tiling

1. Let $P(n)$ be any $2^n \times 2^n$ checkerboard with one square removed can be tiled with  .
   We prove $P(n)$ for all $n \geq 1$ by induction on n.
2. Base Case: $n=1$ 
3. Inductive Hypothesis: Assume $P(k)$ for some arbitrary integer $k \geq 1$

Checkerboard Tiling

1. **Let** $P(n)$ **be any** $2^n \times 2^n$ **checkerboard with one square removed can be tiled with**  **.**
   We prove $P(n)$ **for all** $n \geq 1$ **by induction on** n.
2. **Base Case:** $n=1$ 
3. **Inductive Hypothesis: Assume** $P(k)$ **for some arbitrary integer** $k \geq 1$
4. **Inductive Step: Prove** $P(k+1)$



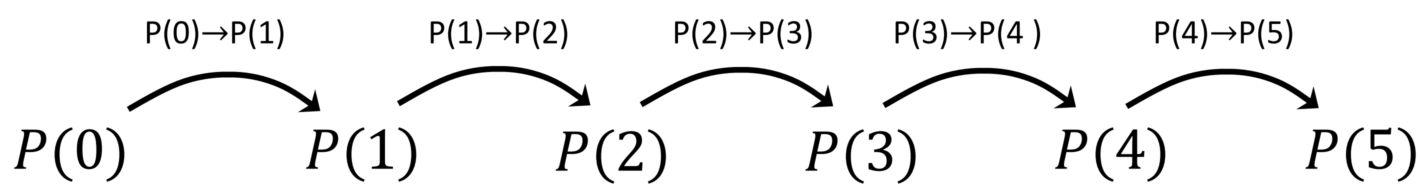
Apply IH to each quadrant then fill with extra tile.

Recall: Induction Rule of Inference

Domain: Natural Numbers

$$\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \\ \hline \therefore \forall n\ \ P(n) \end{array}$$

How do the givens prove P(5)?



Recall: Induction Rule of Inference

Domain: Natural Numbers

$$\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \\ \hline \therefore \forall n\ \ P(n) \end{array}$$

How do the givens prove P(5)?

$$P(0) \xrightarrow{P(0)\to P(1)} P(1) \xrightarrow{P(1)\to P(2)} P(2) \xrightarrow{P(2)\to P(3)} P(3) \xrightarrow{P(3)\to P(4)} P(4) \xrightarrow{P(4)\to P(5)} P(5)$$

We made it harder than we needed to …

- **When we proved** $P(2)$ **we knew BOTH** $P(0)$ **and** $P(1)$
- **When we proved** $P(3)$ **we knew** $P(0)$ **and** $P(1)$ **and** $P(2)$
- **When we proved** $P(4)$ **we knew** $P(0)$, $P(1)$, $P(2)$, $P(3)$
- **etc.**

That's the essence of the idea of Strong Induction.

Strong Induction

$$P(0)$$

$$\forall k \; \Big(\big(P(0) \land P(1) \land P(2) \land \cdots \land P(k) \big) \rightarrow P(k+1) \Big)$$

$$\therefore \; \forall n \; P(n)$$

Strong Induction

$$P(0)$$

$$\forall k \left(\left(P(0) \land P(1) \land P(2) \land \cdots \land P(k) \right) \rightarrow P(k+1) \right)$$

$$\therefore \forall n\, P(n)$$

Strong induction for P **follows from ordinary induction for** Q **where**

$$Q(k) = P(0) \land P(1) \land P(2) \land \cdots \land P(k)$$

Note that $Q(0) \equiv P(0)$ **and** $Q(k+1) \equiv Q(k) \land P(k+1)$ **and** $\forall n\, Q(n) \equiv \forall n\, P(n)$

Inductive Proofs In 5 Easy Steps

1. "Let $P(n)$ be... . We will show that $P(n)$ is true for all integers $n \geq b$ by induction."
2. "Base Case:" Prove $P(b)$
3. "Inductive Hypothesis:

   Assume that for some arbitrary integer $k \geq b$,

   $P(k)$ is true"
4. "Inductive Step:" Prove that $P(k+1)$ is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume $P(k+1)$!!)

5. "Conclusion: $P(n)$ is true for all integers $n \geq b$"

Strong Inductive Proofs In 5 Easy Steps

1. "Let $P(n)$ be... . We will show that $P(n)$ is true for all integers $n \geq b$ by *strong* induction."
2. "Base Case:" Prove $P(b)$
3. "Inductive Hypothesis:

   Assume that for some arbitrary integer $k \geq b$,

   $P(j)$ is true for every integer j from b to k"
4. "Inductive Step:" Prove that $P(k+1)$ is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. (that $P(b), \ldots, P(k)$ are true) and point out where you are using it.
   (Don't assume $P(k+1)$!!)
5. "Conclusion: $P(n)$ is true for all integers $n \geq b$"

Recall: Fundamental Theorem of Arithmetic

Every integer > 1 has a unique prime factorization

48 = 2 • 2 • 2 • 2 • 3
591 = 3 • 197
45,523 = 45,523
321,950 = 2 • 5 • 5 • 47 • 137
1,234,567,890 = 2 • 3 • 3 • 5 • 3,607 • 3,803

We use strong induction to prove that a factorization into primes exists, but not that it is unique.

Every integer ≥ 2 is a product of (one or more) primes.

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** n $\geq$ 2 **by strong induction.**

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** n $\geq$ 2 **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime.**
   Therefore P(2) **is true.**

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** n $\geq$ 2 **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime. Therefore** P(2) **is true.**
3. **Inductive Hyp: Suppose that for some arbitrary integer** k ≥ 2, P(j) **is true for every integer** j **between** 2 **and** k

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** $n \geq 2$ **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime. Therefore** P(2) **is true.**
3. **Inductive Hyp: Suppose that for some arbitrary integer** $k \geq 2$, P(j) **is true for every integer** j **between** 2 **and** k
4. **Inductive Step:**

Goal: Show P(k+1); **i.e.** k+1 **is a product of primes**

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** $n \geq 2$ **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime. Therefore** P(2) **is true.**
3. **Inductive Hyp: Suppose that for some arbitrary integer** $k \geq 2$, P(j) **is true for every integer** j **between** 2 **and** k
4. **Inductive Step:**

Goal: Show P(k+1); **i.e.** k+1 **is a product of primes**

<u>Case: k+1 is prime</u>: **Then by definition** k+1 **is a product of primes**

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** $n \geq 2$ **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime. Therefore** P(2) **is true.**
3. **Inductive Hyp: Suppose that for some arbitrary integer** $k \geq 2$, P(j) **is true for every integer** j **between** 2 **and** k
4. **Inductive Step:**

   Goal: Show P(k+1); **i.e.** k+1 **is a product of primes**

   <u>**Case:** k+1 **is prime**</u>**: Then by definition** k+1 **is a product of primes**
   <u>**Case:** k+1 **is composite:**</u> **Then** k+1=ab **for some integers** a **and** b **where** $2 \leq a, b \leq k$.

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** $n \geq 2$ **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime. Therefore** P(2) **is true.**
3. **Inductive Hyp: Suppose that for some arbitrary integer** $k \geq 2$, P(j) **is true for every integer** j **between** 2 **and** k
4. **Inductive Step:**

Goal: Show P(k+1); **i.e.** k+1 **is a product of primes**

<u>**Case:** k+1 **is prime**</u>: **Then by definition** k+1 **is a product of primes**

<u>**Case:** k+1 **is composite:**</u> **Then** k+1=ab **for some integers** a **and** b **where** $2 \leq a, b \leq k$. **By our IH,** P(a) **and** P(b) **are true so we have**

$a = p_1 p_2 \cdots p_r$ **and** $b = q_1 q_2 \cdots q_s$

for some primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$.

Thus, $k+1 = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ **which is a product of primes.**

Since $k \geq 1$, **one of these cases must happen and so** P(k+1) **is true.**

Every integer ≥ 2 is a product of (one or more) primes.

1. **Let** P(n) **be** "n is a product of primes". **We will show that** P(n) **is true for all integers** $n \geq 2$ **by strong induction.**
2. **Base Case** (n=2): 2 **is prime, so it is a product of (one) prime.**
   Therefore P(2) **is true.**
3. **Inductive Hyp: Suppose that for some arbitrary integer** $k \geq 2$, P(j) **is true for every integer** j **between** 2 **and** k
4. **Inductive Step:**

   Goal: Show P(k+1); **i.e.** k+1 **is a product of primes**

   Case: k+1 **is prime: Then by definition** k+1 **is a product of primes**

   Case: k+1 **is composite: Then** k+1=ab **for some integers** a **and** b **where** $2 \leq a, b \leq k$. **By our IH,** P(a) **and** P(b) **are true so we have**

   $a = p_1 p_2 \cdots p_r$ **and** $b = q_1 q_2 \cdots q_s$

   for some primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$.

   Thus, $k+1 = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ **which is a product of primes.**

   Since $k \geq 2$, **one of these cases must happen and so** P(k+1) **is true.**
5. **Thus** P(n) **is true for all integers** $n \geq 2$, **by strong induction.**

Strong Induction is particularly useful when…

…we need to analyze methods that on input k make a recursive call for an input different from $k-1$.

e.g.: Recursive Modular Exponentiation:

– For exponent $k > 0$ it made a recursive call with exponent $\mathrm{j} = k/2$ when k was even or $\mathrm{j} = k-1$ when k was odd.

Fast Exponentiation

```
public static int FastModExp(int a, int k, int modulus) {

        if (k == 0) {
            return 1;

        } else if ((k % 2) == 0) {
            long temp = FastModExp(a,k/2,modulus);
            return (temp * temp) % modulus;

        } else {
            long temp = FastModExp(a,k-1,modulus);
            return (a * temp) % modulus;
        }
}
```

$$a^{2j} \bmod m = \left(a^j \bmod m\right)^2 \bmod m$$

$$a^{2j+1} \bmod m = \left((a \bmod m) \cdot (a^{2j} \bmod m)\right) \bmod m$$

Strong Induction is particularly useful when…

…we need to analyze methods that on input k make a recursive call for an input different from $k-1$.

e.g.: Recursive Modular Exponentiation:

- For exponent $k > 0$ it made a recursive call with exponent $\mathrm{j} = k/2$ when k was even or $\mathrm{j} = k-1$ when k was odd.

We won't analyze this particular method by strong induction, but we could.

However, we will use strong induction to analyze other functions with recursive definitions.