CSE 311: Foundations of Computing

Topic 7: Induction

IF WE HIT THAT BULLSEYE, THE REST OF THE DOMINOES SHOULD FALL LIKE A HOUSE OF CARDS.

CHECKMATE.
Mathematical Induction

Method for proving statements about all natural numbers

– A new logical inference rule!
  • It only applies over the natural numbers
  • The idea is to use the special structure of the naturals to prove things more easily

– Particularly useful for reasoning about programs!

  for (int i=0; i < n; n++) { … }
  • Show P(i) holds after i times through the loop
Prove \( \forall a, b, m > 0 \ \forall k \in \mathbb{N} \ ((a \equiv_m b) \rightarrow (a^k \equiv_m b^k)) \)

Let \( a, b, m > 0 \) be arbitrary. Let \( k \in \mathbb{N} \) be arbitrary.

Suppose that \( a \equiv_m b \).

We know \(((a \equiv_m b) \land (a \equiv_m b)) \rightarrow (a^2 \equiv_m b^2)\) by multiplying congruences. So, applying this repeatedly, we have:

\[
\begin{align*}
((a \equiv_m b) \land (a \equiv_m b)) & \rightarrow (a^2 \equiv_m b^2) \\
((a^2 \equiv_m b^2) \land (a \equiv_m b)) & \rightarrow (a^3 \equiv_m b^3) \\
& \quad \text{...} \\
((a^{k-1} \equiv_m b^{k-1}) \land (a \equiv_m b)) & \rightarrow (a^k \equiv_m b^k)
\end{align*}
\]

The “…”s is a problem! We don’t have a proof rule that allows us to say “do this over and over”.

But there is such a rule for the natural numbers!

Domain: Natural Numbers

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]
Induction Is A Rule of Inference

Domain: Natural Numbers

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]

How do the givens prove \( P(3) \)?
Induction Is A Rule of Inference

Domain: Natural Numbers

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]

How do the givens prove P(5)?

First, we have \( P(0) \).
Since \( P(n) \rightarrow P(n+1) \) for all \( n \), we have \( P(0) \rightarrow P(1) \).
Since \( P(0) \) is true and \( P(0) \rightarrow P(1) \), by Modus Ponens, \( P(1) \) is true.
Since \( P(1) \) is true and \( P(1) \rightarrow P(2) \), by Modus Ponens, \( P(2) \) is true.
Using The Induction Rule In A Formal Proof

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]
Using The Induction Rule In A Formal Proof

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]

1. \( P(0) \)

4. \( \forall k \ (P(k) \rightarrow P(k+1)) \)

5. \( \forall n \ P(n) \) \quad \text{Induction: 1, 4}
Using The Induction Rule In A Formal Proof

\[
P(0) \\
\forall k \ (P(k) \rightarrow P(k + 1)) \\
\therefore \ \forall n \ P(n)
\]

1. P(0)
2. Let k be an arbitrary integer \( \geq 0 \)

3. \( P(k) \rightarrow P(k+1) \)
4. \( \forall k \ (P(k) \rightarrow P(k+1)) \) \hspace{1cm} \text{Intro } \forall: 2, 3
5. \( \forall n \ P(n) \) \hspace{1cm} \text{Induction: 1, 4}
Using The Induction Rule In A Formal Proof

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]

1. \( P(0) \)
2. Let \( k \) be an arbitrary integer \( \geq 0 \)
   
   3.1. \( P(k) \) \hspace{1cm} \text{Assumption}
   
   3.2. ... 
   
   3.3. \( P(k+1) \)
3. \( P(k) \rightarrow P(k+1) \) \hspace{1cm} \text{Direct Proof Rule}
4. \( \forall k \ (P(k) \rightarrow P(k+1)) \) \hspace{1cm} \text{Intro} \ \forall: 2, 3
5. \( \forall n \ P(n) \) \hspace{1cm} \text{Induction: 1, 4}
Translating to an English Proof

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]

1. Prove \( P(0) \)

2. Let \( k \) be an arbitrary integer \( \geq 0 \)
   3.1. Suppose that \( P(k) \) is true
   3.2. ...
   3.3. Prove \( P(k+1) \) is true

3. \( P(k) \rightarrow P(k+1) \)

4. \( \forall k \ (P(k) \rightarrow P(k+1)) \)

5. \( \forall n \ P(n) \)

Base Case

Inductive Hypothesis

Inductive Step

Direct Proof Rule

Intro \( \forall \): 2, 3

Induction: 1, 4

Conclusion
Translating to an English Proof

1. Prove $P(0)$
2. Let $k$ be an arbitrary integer $\geq 0$
   3.1. Assume that $P(k)$ is true
   3.2. ...
   3.3. Prove $P(k+1)$ is true

3. $P(k) \rightarrow P(k+1)$
4. $\forall k\ (P(k) \rightarrow P(k+1))$
5. $\forall n\ P(n)$

Inductive Hypothesis
Inductive Step
Conclusion

Induction English Proof Template

 [...]Define P(n)...]
We will show that $P(n)$ is true for every $n \in \mathbb{N}$ by Induction.
Base Case: [...]proof of $P(0)$ here...
Induction Hypothesis:
Suppose that $P(k)$ is true for an arbitrary $k \in \mathbb{N}$.
Induction Step:
 [...]proof of $P(k + 1)$ here...]
The proof of $P(k + 1)$ must invoke the IH somewhere.
So, the claim is true by induction.
**Inductive Proofs In 5 Easy Steps**

**Proof:**

1. “Let \( P(n) \) be... . We will show that \( P(n) \) is true for every \( n \geq 0 \) by Induction.”

2. “Base Case:” Prove \( P(0) \)

3. “Inductive Hypothesis:
   
   Suppose \( P(k) \) is true for an 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: Result follows by induction”
What is $1 + 2 + 4 + \ldots + 2^n$?

- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 4 = 7$
- $1 + 2 + 4 + 8 = 15$
- $1 + 2 + 4 + 8 + 16 = 31$

It sure looks like this sum is $2^{n+1} - 1$

How can we prove it?

We could prove it for $n = 1, n = 2, n = 3, \ldots$ but that would literally take forever.

Good that we have induction!
Prove $1 + 2 + 4 + ... + 2^n = 2^{n+1} - 1$
1. Let $P(n)$ be “$2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$”. We will show $P(n)$ is true for all natural numbers by induction.
Prove \( 1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1 \)

1. Let \( P(n) \) be “\( 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1 \)”. We will show \( P(n) \) is true for all natural numbers by induction.

2. Base Case (\( n=0 \)): \( 2^0 = 1 = 2 - 1 = 2^{0+1} - 1 \) so \( P(0) \) is true.
1. Let $P(n)$ be “$2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$”. We will show $P(n)$ is true for all natural numbers by induction.

2. Base Case ($n=0$): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. Induction Hypothesis: Suppose that $P(k)$ is true for some arbitrary integer $k \geq 0$, i.e., that $2^0 + 2^1 + ... + 2^k = 2^{k+1} - 1$.

\[ \text{Goal: Show } P(k+1) \text{, i.e., show } 2^0 + 2^1 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1. \]

Adding $2^{k+1}$ to both sides, we get:

\[ 1 + 2 + ... + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1 \]

Note that $2^{k+1} + 2^{k+1} = 2(2^{k+1}) = 2^{k+2}$.

So, we have $1 + 2 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1$, which is exactly $P(k+1)$.

5. Thus $P(k)$ is true for all $k \in \mathbb{N}$, by induction.
Prove $1 + 2 + 4 + ... + 2^n = 2^{n+1} - 1$

1. Let $P(n)$ be “$2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$”. We will show $P(n)$ is true for all natural numbers by induction.

2. Base Case ($n=0$): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. Induction Hypothesis: Suppose that $P(k)$ is true for some arbitrary integer $k \geq 0$, i.e., that $2^0 + 2^1 + ... + 2^k = 2^{k+1} - 1$.

4. Induction Step:
   
   Goal: Show $P(k+1)$, i.e. show $2^0 + 2^1 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1$

   Adding $2^{k+1}$ to both sides, we get:
   
   $1 + 2 + ... + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1$

   Note that $2^{k+1} + 2^{k+1} = 2(2^{k+1}) = 2^{k+2}$.

   So, we have $1 + 2 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1$, which is exactly $P(k+1)$.

5. Thus $P(k)$ is true for all $k \in \mathbb{N}$, by induction.
Let $P(n)$ be $2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$. We will show $P(n)$ is true for all natural numbers by induction.

2. **Base Case** ($n=0$): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. **Induction Hypothesis:** Suppose that $P(k)$ is true for some arbitrary integer $k \geq 0$, i.e., that $2^0 + 2^1 + ... + 2^k = 2^{k+1} - 1$.

4. **Induction Step:**

   
   $2^0 + 2^1 + ... + 2^k = 2^{k+1} - 1$ \text{ by IH}

   Adding $2^{k+1}$ to both sides, we get:

   $2^0 + 2^1 + ... + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1$

   Note that $2^{k+1} + 2^{k+1} = 2(2^{k+1}) = 2^{k+2}$.

   So, we have $2^0 + 2^1 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1$, which is exactly $P(k+1)$.

Thus $P(k)$ is true for all $k \in \mathbb{N}$, by induction.
1. Let $P(n)$ be “$2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$”. We will show $P(n)$ is true for all natural numbers by induction.

2. Base Case ($n=0$): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. Induction Hypothesis: Suppose that $P(k)$ is true for some arbitrary integer $k \geq 0$, i.e., that $2^0 + 2^1 + ... + 2^k = 2^{k+1} - 1$.

4. Induction Step:
   We can calculate
   \[2^0 + 2^1 + ... + 2^k + 2^{k+1} = (2^0+2^1+...+2^k) + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1}\]
   by the IH
   \[= 2(2^{k+1}) - 1\]
   \[= 2^{k+2} - 1,\]
   which is exactly $P(k+1)$.

Alternative way of writing the inductive step
1. Let $P(n)$ be “$2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$”. We will show $P(n)$ is true for all natural numbers by induction.

2. **Base Case** $(n=0)$: $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. **Induction Hypothesis:** Suppose that $P(k)$ is true for some arbitrary integer $k \geq 0$, i.e., that $2^0 + 2^1 + ... + 2^k = 2^{k+1} - 1$.

4. **Induction Step:**
   We can calculate 
   
   $2^0 + 2^1 + ... + 2^k + 2^{k+1} = (2^0+2^1+...+2^k) + 2^{k+1}$
   
   $= (2^{k+1} - 1) + 2^{k+1}$ by the IH
   
   $= 2(2^{k+1}) - 1$
   
   $= 2^{k+2} - 1$,
   
   which is exactly $P(k+1)$.

5. **Thus $P(n)$ is true for all $n \in \mathbb{N}$, by induction.**
Prove $1 + 2 + 3 + ... + n = n(n + 1)/2$
Prove $1 + 2 + 3 + \ldots + n = n(n + 1)/2$

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 “$0 + 1 + 2 + \ldots + n = n(n+1)/2$”. 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 $k \geq 0$.

4. **Induction Step:**
   - **Goal:** Show $P(k+1)$, i.e. show $1 + 2 + \ldots + n + (n+1) = (n+1)(n+2)/2$
   - $1 + 2 + \ldots + n = n(n+1)/2$ by IH
   - Adding $n+1$ to both sides, we get:
     $$1 + 2 + \ldots + n + (n+1) = n(n+1)/2 + (n+1)$$
   - Now $n(n+1)/2 + (n+1) = (n+1)(n/2 + 1) = (n+1)(n+2)/2$.
   - So, we have $1 + 2 + \ldots + n + (n+1) = (n+1)(n+2)/2$, which is exactly $P(k+1)$.

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

**Summation Notation**

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + 3 + \ldots + n$$
1. Let $P(n)$ be \(0 + 1 + 2 + \ldots + n = n(n+1)/2\). 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.
Let $P(n)$ be $0 + 1 + 2 + \ldots + n = n(n+1)/2$. We will show $P(n)$ is true for all natural numbers by induction.

Base Case ($n=0$): $0 = 0(0+1)/2$. Therefore $P(0)$ is true.

Induction Hypothesis: Suppose that $P(k)$ is true for some arbitrary integer $k \geq 0$. I.e., suppose $1 + 2 + \ldots + k = k(k+1)/2$.

Adding $n+1$ to both sides, we get:

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

Now $n(n+1)/2 + (n+1) = (n+1)(n/2 + 1) = (n+1)(n+2)/2$.

So, we have $1 + 2 + \ldots + n + (n+1) = (n+1)(n+2)/2$, which is exactly $P(k+1)$.

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

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

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

Prove $1 + 2 + 3 + ... + n = n(n + 1)/2$
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:
   \[
   1 + 2 + ... + k + (k+1) = (1 + 2 + ... + k) + (k+1) \\
   = k(k+1)/2 + (k+1) \quad \text{by IH} \\
   = (k+1)(k/2 + 1) \\
   = (k+1)(k+2)/2
   \]
   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 $\forall k \ (Q(k) \rightarrow Q(k + 1)) \equiv \forall k \geq b \ (P(k) \rightarrow P(k + 1))$
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 $P(k)$ is true for an arbitrary integer $k \geq b$”

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 $n \geq b$”

Template for induction from a different base case
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.

2. Base Case ($n=2$): $3^2 = 9 \geq 7 = 4+3 = 2^2 + 3$ so $P(2)$ is true.

3. Hypothesis: Suppose that $P(k)$ is true for some arbitrary integer $k \geq 2$.

4. Induction 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

   $= k^2 + 2k + 9 \geq k^2 + 2k + 1 = (k+1)^2$ since $k \geq 1$.

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

5. Thus $P(n)$ is true for all $n \in \mathbb{N}$, 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 $3^k \geq k^2+3$.

4. Therefore $P(k+1)$ is true.

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

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 $3^{k+1} \geq (k+1)^2+3 = k^2+2k+4$

   
   \[
   3^{k+1} = 3(3^k) \geq 3(k^2+3) \text{ by the IH} \\
   = 3k^2+9 \\
   = k^2+2k^2+9 \\
   \geq k^2+2k+4 = (k+1)^2+3 \text{ since } k \geq 1.
   \]

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

5. Thus $P(n)$ 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.

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 $3^{k+1} \geq (k+1)^2+3 = k^2+2k+4$

   \[
   3^{k+1} = 3(3^k)
   \geq 3(k^2+3) \text{ by the IH}
   = k^2+2k^2+9
   \geq k^2+2k+4 = (k+1)^2+3 \text{ since } k \geq 1.
   \]

   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:
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 $\square$. We prove $P(n)$ for all $n \geq 1$ by induction on $n$.

2. Base Case: $n=1$
1. Let $P(n)$ be any $2^n \times 2^n$ checkerboard with one square removed can be tiled with \[
\begin{array}{c}
\text{\textbullet} \\
\text{\textbullet} \\
\text{\textbullet} \\
\end{array}
\].
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 $k \geq 1$
1. Let $P(n)$ be any $2^n \times 2^n$ checkerboard with one square removed can be tiled with $\square \quad \square$. 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

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ \therefore \forall n \ P(n) \]

How do the givens prove \( P(5) \)?
Recall: Induction Rule of Inference

Domain: Natural Numbers

\[ P(0) \]
\[ \forall k \ (P(k) \rightarrow P(k+1)) \]
\[ \therefore \forall n \ P(n) \]

How do the givens prove \( P(5) \)?

\( P(0) \rightarrow P(1) \) \quad P(1) \quad P(2) \quad P(3) \quad P(4) \rightarrow 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

\[ P(0) \quad \forall k \left( \forall j \ (0 \leq j \leq k \rightarrow P(j)) \rightarrow P(k + 1) \right) \]

\[ \therefore \forall n \ P(n) \]
Strong Induction

\[ P(0) \quad \forall k \left( \forall j \ (0 \leq j \leq k \rightarrow P(j)) \rightarrow P(k + 1) \right) \]

: \ \forall n \ P(n)

Strong induction for \( P \) follows from ordinary induction for \( Q \) where

\[ Q(k) := \forall j \ (0 \leq j \leq k \rightarrow P(j)) \]

Note that \( Q(0) = P(0) \) 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 $P(b)$, ..., $P(k)$ 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

\[
\begin{align*}
48 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \\
591 &= 3 \cdot 197 \\
45,523 &= 45,523 \\
321,950 &= 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137 \\
1,234,567,890 &= 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3,607 \cdot 3,803
\end{align*}
\]

We use strong induction to prove that a factorization into primes exists, but not that it is unique.
Every integer $\geq 2$ is a product of (one or more) primes.
Every integer $\geq 2$ is a product of (one or more) primes.

1. Let $P(n)$ be “$n$ is a product of some list of primes”. We will show that $P(n)$ is true for all integers $n \geq 2$ by strong induction.
1. Let $P(n)$ be “$n$ is a product of some list 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 $\geq 2$ is a product of (one or more) primes.
Every integer $\geq 2$ is a product of (one or more) primes.

1. Let $P(n)$ be “$n$ is a product of some list 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 $a = p_1 p_2 \ldots p_m$ and $b = q_1 q_2 \ldots q_n$ for some primes $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_n$.
   
   Thus, $k+1 = ab = p_1 p_2 \ldots p_m q_1 q_2 \ldots q_n$ which is a product of primes.

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

Thus $P(n)$ is true for all integers $n \geq 2$, by induction.
Every integer \( \geq 2 \) is a product of (one or more) primes.

1. Let \( P(n) \) be “\( n \) is a product of some list 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.

Since \( k \geq 1 \), 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 induction.
1. Let $P(n)$ be “$n$ is a product of some list 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 $a = p_1 p_2 \cdots p_m$ and $b = q_1 q_2 \cdots q_n$ for some primes $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_n$. Thus, $k+1 = ab = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$ which is a product of primes.

5. Thus $P(n)$ is true for all integers $n \geq 2$, by induction.
Every integer $\geq 2$ is a product of (one or more) primes.

1. Let $P(n)$ be “$n$ is a product of some list 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 $2 \leq a, b \leq k$.

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

Every integer $\geq 2$ is a product of (one or more) primes.
Every integer $\geq 2$ is a product of (one or more) primes.

1. Let $P(n)$ be “$n$ is a product of some list 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 $a = p_1p_2\cdots p_r$ and $b = q_1q_2\cdots q_s$ for some primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$.

   Thus, $k+1 = ab = p_1p_2\cdots p_rq_1q_2\cdots q_s$ 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 induction.
Every integer $\geq 2$ is a product of (one or more) primes.

1. Let $P(n)$ be “$n$ is a product of some list 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 $a = p_1p_2 \cdots p_r$ and $b = q_1q_2 \cdots q_s$ for some primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$. Thus, $k+1 = ab = p_1p_2 \cdots p_rq_1q_2 \cdots q_s$ 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 $j = k/2$ when $k$ was even or $j = k - 1$ when $k$ was odd.
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;
    }
}

\[a^{2j} \mod m = (a^j \mod m)^2 \mod m\]
\[a^{2j+1} \mod m = (a \mod m) \cdot (a^{2j} \mod m) \mod m\]