Lecture 14: Induction

Look at bottom (right) of course web page:

Handouts

Solving Modular Equations
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!

```java
for(int i=0; i < n; n++) { ... }
```
  • Show P(i) holds after i times through the loop

```java
public int f(int x) {
    if (x == 0) { return 0; }
    else { return f(x - 1); }
}
```
  • f(x) = x for all values of x ≥ 0 naturally shown by induction.
Prove $\forall a, b, m > 0 \forall k \in \mathbb{N} \ (a \equiv b \, (\text{mod} \, m) \rightarrow a^k \equiv b^k \, (\text{mod} \, m))$

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

Suppose that $a \equiv b \, (\text{mod} \, m)$.

We know $(a \equiv b \, (\text{mod} \, m) \land a \equiv b \, (\text{mod} \, m)) \rightarrow a^2 \equiv b^2 \, (\text{mod} \, m)$ by multiplying congruences. So, applying this repeatedly, we have:

$$(a \equiv b \, (\text{mod} \, m) \land a \equiv b \, (\text{mod} \, m)) \rightarrow a^2 \equiv b^2 \, (\text{mod} \, m)$$

$$(a^2 \equiv b^2 \, (\text{mod} \, m) \land a \equiv b \, (\text{mod} \, m)) \rightarrow a^3 \equiv b^3 \, (\text{mod} \, m)$$

... 

$$(a^{i-1} \equiv b^{i-1} \, (\text{mod} \, m) \land a \equiv b \, (\text{mod} \, m)) \rightarrow a^k \equiv b^k \, (\text{mod} \, m)$$

The “...”s is a problem! We don’t have a proof rule that allows us to say “do this over and over”.
But there such a property of 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(5)?

\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ P(0) \]
\[ P(0) \rightarrow P(1) \quad \text{element} \]
\[ P(1) \quad \text{mp} \]
\[ P(1) \rightarrow P(2) \quad \text{element} \quad \text{mp} \]
\[ P(2) \quad \text{mp} \]

\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]
\[ P(0) \]
\[ P(0) \rightarrow P(1) \quad \text{element} \]
\[ P(1) \quad \text{mp} \]
\[ P(1) \rightarrow P(2) \quad \text{element} \quad \text{mp} \]
\[ P(2) \quad \text{mp} \]
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 \( P(5) \)?

1. First, we have \( P(0) \).
2. 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.
3. Since \( P(n) \rightarrow P(n+1) \) for all \( n \), we have \( P(1) \rightarrow P(2) \).
   - 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

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

1. $P(0)$

\[\forall n \ (P(n) \rightarrow P(n+1))\]

5. $\forall n \ P(n)$ \hspace{1cm} \text{Induction from 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. Prove \( P(0) \)
2. Let \( k \) be an arbitrary integer \( \geq 0 \)

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

\( \text{Induction: } 1, 4 \)
Using The Induction Rule In A Formal Proof

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

1. Prove \( P(0) \)
2. Let \( k \) be an arbitrary integer \( \geq 0 \)
   
   \[\begin{array}{c}
   \exists! \ P(k) \ \\
   \text{Assumption}
   \end{array}\]

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

\[ P(0) \]

\[ \forall k \ (P(k) \rightarrow P(k + 1)) \]

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

1. 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. \( P(k) \rightarrow P(k+1) \) \hspace{1cm} Direct Proof Rule
4. \( \forall k \ (P(k) \rightarrow P(k+1)) \) \hspace{1cm} Intro \( \forall \): 2, 3
5. \( \forall n \ P(n) \) \hspace{1cm} 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 \( P(0) \) (Base Case)
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. \( P(k) \rightarrow P(k+1) \) (Direct Proof Rule)
4. \( \forall k \ (P(k) \rightarrow P(k+1)) \) (Intro \( \forall \): 2, 3)
5. \( \forall n \ P(n) \) (Induction: 1, 4)

Domain: Integers \( \geq 0 \)
Translating To An English Proof

Induction 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 some \( k \in \mathbb{N} \).

Induction Step:
We want to prove that \( P(k + 1) \) is true.

[...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:
   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: 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 \[ 1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1 \]

1. Let \( P(n) \) be "\[1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1\]". We prove by induction that \( P(n) \) is true for all \( n \geq 0 \).
1. Let $P(n)$ be “$1 + 2 + \ldots + 2^n = 2^{n+1} – 1$”. We will show $P(n)$ is true for all natural numbers by induction.

2. Base case: $n = 0$. $P(0)$ implies $1 = 2^1 – 1$
Prove \( 1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1 \)

1. Let \( P(n) \) be “\( 1 + 2 + \ldots + 2^n = 2^{n+1} - 1 \)”. 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.

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 \( 1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1 \) by IH
   - Adding \( 2^{k+1} \) to both sides, we get:
     \[
     1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1
     \]
   - Note that \( 2^{k+1} + 2^{k+1} = 2(2^{k+1}) = 2^{k+2} \).
   - So, we have \( 1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1 \), which is exactly \( P(k+1) \).

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

1. Let \( P(n) \) be “\( 1 + 2 + \ldots + 2^n = 2^{n+1} - 1 \).” 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.
3. Induction Hypothesis: Suppose that \( P(k) \) is true for some arbitrary integer \( k \geq 0 \).
4. Inductive Step: Goal: Show \( P(k+1) \), i.e.,
   \[ 1 + 2 + 4 + \ldots + 2^{k+1} = 2^{k+2} - 1 \]
Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. Let $P(n)$ be "$1 + 2 + \ldots + 2^n = 2^{n+1} - 1$". 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.
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 $1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1$

   By I.H. \[ 1 + 2 + 4 + \ldots + 2^k = 2^{k+1} - 1 \]

   Add $2^{k+1}$ to both sides.

   \[ 1 + 2 + 4 + \ldots + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1 \]

   \[ \sim 1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1 \] by I.H.
Prove $1 + 2 + 4 + ... + 2^n = 2^{n+1} - 1$

1. Let $P(n)$ be “$1 + 2 + ... + 2^n = 2^{n+1} - 1$”. 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 $k \geq 0$.

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

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

   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 $P(k+1)$. 
1. Let $P(n)$ be “$1 + 2 + \ldots + 2^n = 2^{n+1} - 1$”. 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.

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 $1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1$

   $1 + 2 + \ldots + 2^k = 2^{k+1} - 1$ **by IH**

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

   $1 + 2 + \ldots + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1$

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

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

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

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

4. Induction Step:
   
   **Goal:** Show $P(k+1)$, i.e. show $1 + 2 + ... + n + (n+1) = (n+1)(n+2)/2$
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 
   \[
   1 + 2 + \ldots + n + (n+1) = (n+1)(n+2)/2
   \]
   
   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 \( P(n) \) is true for all \( n \in \mathbb{N} \), by induction.
Another example of a pattern

- $2^0 - 1 = 1 - 1 = 0 = 3 \cdot 0$
- $2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1$
- $2^4 - 1 = 16 - 1 = 15 = 3 \cdot 5$
- $2^6 - 1 = 64 - 1 = 63 = 3 \cdot 21$
- $2^8 - 1 = 256 - 1 = 255 = 3 \cdot 85$
- ...
Prove: \(3 \mid (2^{2n} - 1)\) for all \(n \geq 0\)
Prove: $3 \mid 2^{2n} - 1$ for all $n \geq 0$

1. Let $P(n)$ be “$3 \mid 2^{2n} - 1$”. We will show $P(n)$ is true for all natural numbers by induction.

2. Base Case ($n=0$):
Prove: \( 3 \mid 2^{2n} - 1 \) for all \( n \geq 0 \)

1. Let \( P(n) \) be “\( 3 \mid 2^{2n} - 1 \)”. We will show \( P(n) \) is true for all natural numbers by induction.

2. Base Case \((n=0)\): \( 2^{2\cdot0} - 1 = 1 - 1 = 0 = 3 \cdot 0 \) Therefore \( P(0) \) is true.

3. Induction Hypothesis: Suppose that \( P(k) \) is true for some arbitrary integer \( k \geq 0 \).

4. Induction Step:

   \[ \text{Goal: Show } P(k+1), \text{ i.e. show } 3 \mid \left(2^{2(k+1)} - 1\right) \]
Prove: \(3 \mid 2^{2n} - 1\) for all \(n \geq 0\)

1. Let \(P(n)\) be “\(3 \mid 2^{2n} - 1\)”. We will show \(P(n)\) is true for all natural numbers by induction.

2. Base Case (\(n=0\)): \(2^{2\cdot0}-1=1-1=0=3\cdot0\) 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 \(3 \mid 2^{2(k+1)} - 1\)

   By IH, \(3 \mid 2^{2k} - 1\) so \(2^{2k} - 1 = 3j\) for some integer \(j\)
   
   So \(2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j+1) - 1 = 12j+3 = 3(4j+1)\)

   Therefore \(3 \mid 2^{2(k+1)} - 1\) which is exactly \(P(k+1)\).

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