# CSE 311 Lecture 16: Induction

Emina Torlak and Kevin Zatloukal

# Topics

**Mathematical induction**

A method for proving statements about all natural numbers.

**Using induction**

Using induction in formal and English proofs.

**Example proofs by induction**

Example proofs about sums and divisibility.

**Induction starting at any integer**

Proving theorems about all integers $n \geq b$ for some $b \in \mathbb{Z}$.

**Strong induction**

Induction with a stronger hypothesis.

**Using strong induction**

An example proof and when to use strong induction.

# Mathematical induction

A method for proving statements about all natural numbers.

# How would you prove this theorem?

**Mods and exponents**

For all integers $a, b, m > 0$ and $k \geq 0$,
$a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$.

# How would you prove this theorem?

**Mods and exponents**

For all integers $a, b, m > 0$ and $k \geq 0$,
$a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$.

**Proof**

Let $a, b, m > 0 \in \mathbb{Z}$ and $k \geq 0 \in \mathbb{Z}$ be arbitrary. Suppose that $a \equiv b \pmod{m}$.
By the multiplication property, we know that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. So, taking $c$ to be $a$ and $d$ to be $b$, we have $a^2 \equiv b^2 \pmod{m}$.
Applying this reasoning repeatedly, we have

$$(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$
$$(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$
$$\dots$$
$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

# How would you prove this theorem?

## Mods and exponents

For all integers $a, b, m > 0$ and $k \geq 0$,
$a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$.

**Proof (almost):**

Let $a, b, m > 0 \in \mathbb{Z}$ and $k \geq 0 \in \mathbb{Z}$ be arbitrary. Suppose that $a \equiv b \pmod{m}$.
By the multiplication property, we know that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. So, taking $c$ to be $a$ and $d$ to be $b$, we have $a^2 \equiv b^2 \pmod{m}$.
Applying this reasoning repeatedly, we have

$$(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$
$$(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$
$$\dots$$
$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

This, uhm, completes the proof? □

# How would you prove this theorem?

**Mods and exponents**

For all integers $a, b, m > 0$ and $k \geq 0$,
$a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$.

**Proof (almost):**

Let $a, b, m > 0 \in \mathbb{Z}$ and $k \geq 0 \in \mathbb{Z}$ be arbitrary. Suppose that $a \equiv b \pmod{m}$.
By the multiplication property, we know that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. So, taking $c$ to be $a$ and $d$ to be $b$, we have $a^2 \equiv b^2 \pmod{m}$.
Applying this reasoning repeatedly, we have

$$(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$
$$(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$
$$\dots$$
$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

This, uhm, completes the proof? □

We don't have a proof rule to say "perform this step repeatedly."

# Perform a step repeatedly with induction!

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

# Perform a step repeatedly with induction!

**Induction** $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

**Induction is a logical rule of inference that applies (only) over $\mathbb{N}$.**

If we know that a property $P$ holds for 0, and
we know that $\forall k.\, P(k) \rightarrow P(k+1)$, then
we can conclude that $P$ holds for all natural numbers.

# Perform a step repeatedly with induction!

**Induction** $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

**Induction is a logical rule of inference that applies (only) over $\mathbb{N}$.**

If we know that a property $P$ holds for 0, and
we know that $\forall k.\, P(k) \rightarrow P(k+1)$, then
we can conclude that $P$ holds for all natural numbers.

```
// f(x) = x for all x >= 0.
public int f(int x) {
  if (x == 0) { return 0; }
  else        { return f(x - 1) + 1; }
}
```

Induction is essential for reasoning about programs with loops and recursion.

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

1. First, we have $P(0)$. **P(0)**

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$.

**P(0)**

$\Downarrow$ **P(0)→P(1)**

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

1. First, we have $P(0)$. **P(0)**
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$. $\Downarrow$ **P(0)→P(1)**
3. Applying Modus Ponens to 1 and 2, we get $P(1)$. **P(1)**

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$.
3. Applying Modus Ponens to 1 and 2, we get $P(1)$.
4. Since $P(k) \to P(k+1)$ for all $k$, we have $P(1) \to P(2)$.

$\mathbf{P(0)}$

$\Downarrow_{\mathbf{P(0) \to P(1)}}$

$\mathbf{P(1)}$

$\Downarrow_{\mathbf{P(1) \to P(2)}}$

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

1. First, we have $P(0)$. **P(0)**
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$. ⇓ **P(0)→P(1)**
3. Applying Modus Ponens to 1 and 2, we get $P(1)$. **P(1)**
4. Since $P(k) \to P(k+1)$ for all $k$, we have $P(1) \to P(2)$. ⇓ **P(1)→P(2)**
5. Applying Modus Ponens to 3 and 4, we get $P(2)$. **P(2)**

# Induction: how does it work?

**Induction** $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: natural numbers ($\mathbb{N}$).

Suppose that we are given $P(0)$ and $\forall k.\, P(k) \to P(k+1)$.

How does that give us $P(k)$ for a concrete $k$ such as $5$?

1. First, we have $P(0)$. — **P(0)**
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$. — ⇓ **P(0)→P(1)**
3. Applying Modus Ponens to 1 and 2, we get $P(1)$. — **P(1)**
4. Since $P(k) \to P(k+1)$ for all $k$, we have $P(1) \to P(2)$. — ⇓ **P(1)→P(2)**
5. Applying Modus Ponens to 3 and 4, we get $P(2)$. — **P(2)**

⋮ — ⇓ **P(k)→P(k+1)**

11. Applying Modus Ponens to 9 and 10, we get $P(5)$. — **P(5)**

# Using induction

Using induction in formal and English proofs.

# Using the induction rule in a formal proof

**Induction** $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

1. Prove $P(0)$

5. $\forall k.\, P(k) \rightarrow P(k+1)$
6. $\forall n.\, P(n)$ **Induction: 1, 5**

# Using the induction rule in a formal proof

**Induction** $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

4. $P(k) \rightarrow P(k+1)$
5. $\forall k.\, P(k) \rightarrow P(k+1)$ — Intro ∀: 2, 4
6. $\forall n.\, P(n)$ — Induction: 1, 5

# Using the induction rule in a formal proof

$$\textbf{Induction}\ \frac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$$

1. Prove $P(0)$
2. Let $k \geq 0$ be an arbitrary integer
   - 3.1. Assume that $P(k)$ is true
   - 3.2. …
   - 3.3. Prove $P(k+1)$ is true
4. $P(k) \rightarrow P(k+1)$ — Direct Proof Rule
5. $\forall k.\, P(k) \rightarrow P(k+1)$ — Intro ∀: 2, 4
6. $\forall n.\, P(n)$ — Induction: 1, 5

# Using the induction rule in a formal proof: key parts

$$\textbf{Induction}\ \frac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$$

| | | |
|---|---|---|
| 1. Prove $P(0)$ | | Base case |
| 2. Let $k \geq 0$ be an arbitrary integer | | Inductive hypothesis |
| 3.1. Assume that $P(k)$ is true | | |
| 3.2. … | | Inductive step |
| 3.3. Prove $P(k+1)$ is true | | |
| 4. $P(k) \rightarrow P(k+1)$ | Direct Proof Rule | Conclusion |
| 5. $\forall k.\, P(k) \rightarrow P(k+1)$ | Intro ∀: 2, 4 | |
| 6. $\forall n.\, P(n)$ | Induction: 1, 5 | |

# Translating to an English proof: the template

**① Let $\mathbf{P(n)}$ be *[ definition of $P(n)$ ]*.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

**② Base case ($\mathbf{n = 0}$):**

*[ Proof of $P(0)$. ]*

**③ Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

**④ Inductive step:**

We want to prove that $P(k+1)$ is true.

*[ Proof of $P(k+1)$. This proof **must** invoke the inductive hypothesis somewhere. ]*

**⑤ The result follows for all $\mathbf{n \geq 0}$ by induction.**

| | | |
|---|---|---|
| 1. Prove $P(0)$ | | Base case |
| 2. Let $k \geq 0$ be an arbitrary integer | | Inductive hypothesis |
| 3.1. Assume that $P(k)$ is true | | |
| 3.2. … | | Inductive step |
| 3.3. Prove $P(k+1)$ is true | | |
| 4. $P(k) \to P(k+1)$ | Direct Proof Rule | Conclusion |
| 5. $\forall k.\, P(k) \to P(k+1)$ | Intro ∀: 2, 4 | |
| 6. $\forall n.\, P(n)$ | Induction: 1, 5 | |

# Translating to an English proof: the template

**① Let $\mathbf{P(n)}$ be *[ definition of $P(n)$ ]*.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

**② Base case ($\mathbf{n = 0}$):**

*[ Proof of $P(0)$. ]*

**③ Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

**④ Inductive step:**

We want to prove that $P(k+1)$ is true.

*[ Proof of $P(k+1)$. This proof **must** invoke the inductive hypothesis somewhere. ]*

**⑤ The result follows for all $\mathbf{n \geq 0}$ by induction.**

| | | |
|---|---|---|
| 1. Prove $P(0)$ | | Base case |
| 2. Let $k \geq 0$ be an arbitrary integer | | Inductive hypothesis |
| 3.1. Assume that $P(k)$ is true | | |
| 3.2. … | | Inductive step |
| 3.3. Prove $P(k+1)$ is true | | |
| 4. $P(k) \to P(k+1)$ | Direct Proof Rule | Conclusion |
| 5. $\forall k.\, P(k) \to P(k+1)$ | Intro ∀: 2, 4 | |
| 6. $\forall n.\, P(n)$ | Induction: 1, 5 | |

Induction **do**s and **don't**s:

- **Do** write out all 5 steps.
- **Do** point out where you are using the inductive hypothesis in step ④.
- **Don't** assume $P(k+1)$!

# Example proofs by induction

Example proofs about sums and divisibility.

# What is $\sum_{i=0}^{n} 2^i$ for an arbitrary $n \in \mathbb{N}$?

Recall that $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n$.

# What is $\sum_{\mathbf{i=0}}^{\mathbf{n}} \mathbf{2^i}$ for an arbitrary $\mathbf{n} \in \mathbb{N}$?

Recall that $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n$.

**Let's look at a few examples:**

$$\sum_{i=0}^{0} 2^i = 1$$
$$\sum_{i=0}^{1} 2^i = 1 + 2 = 3$$
$$\sum_{i=0}^{2} 2^i = 1 + 2 + 4 = 7$$
$$\sum_{i=0}^{3} 2^i = 1 + 2 + 4 + 8 = 15$$
$$\sum_{i=0}^{4} 2^i = 1 + 2 + 4 + 8 + 16 = 31$$

# What is $\sum_{i=0}^{n} 2^i$ for an arbitrary $n \in \mathbb{N}$?

Recall that $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n$.

**Let's look at a few examples:**

$\sum_{i=0}^{0} 2^i = 1$

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

$\sum_{i=0}^{2} 2^i = 1 + 2 + 4 = 7$

$\sum_{i=0}^{3} 2^i = 1 + 2 + 4 + 8 = 15$

$\sum_{i=0}^{4} 2^i = 1 + 2 + 4 + 8 + 16 = 31$

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

Let's use induction to prove it!

Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

# Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

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

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

# Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

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

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):

$\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$ so $P(0)$ is true.

# Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

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

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**

$\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$ so $P(0)$ is true.

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

# Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$.**
We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

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

③ **Inductive hypothesis:**
Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ **Inductive step:** **Assume $P(k)$ to prove $P(k+1)$, not vice versa!**
We want to prove that $P(k+1)$ is true, i.e., $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$. Note that $\sum_{i=0}^{k+1} 2^i = (\sum_{i=0}^{k} 2^i) + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1}$ by the inductive hypothesis.
From this, we have that $(2^{k+1} - 1) + 2^{k+1} = 2 * 2^{k+1} - 1 = 2^{k+1+1} - 1 = 2^{k+2} - 1$, which is exactly $P(k+1)$.

# Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$.**
We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

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

③ **Inductive hypothesis:**
Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ **Inductive step:** **Assume $P(k)$ to prove $P(k+1)$, not vice versa!**
We want to prove that $P(k+1)$ is true, i.e., $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$. Note that $\sum_{i=0}^{k+1} 2^i = (\sum_{i=0}^{k} 2^i) + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1}$ by the inductive hypothesis.
From this, we have that $(2^{k+1} - 1) + 2^{k+1} = 2 * 2^{k+1} - 1 = 2^{k+1+1} - 1 = 2^{k+2} - 1$, which is exactly $P(k+1)$.

⑤ **The result follows for all $n \geq 0$ by induction.**

Prove $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$

# Prove $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$

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

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

# Prove $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$

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

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):

$\sum_{i=0}^{n} i = 0 = 0(0+1)/2$ so $P(0)$ is true.

# Prove $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n+1)/2$.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**

$\sum_{i=0}^{n} i = 0 = 0(0+1)/2$ so $P(0)$ is true.

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

# Prove $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n+1)/2$.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**

$\sum_{i=0}^{n} i = 0 = 0(0+1)/2$ so $P(0)$ is true.

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$. Note that $\sum_{i=0}^{k+1} i = (\sum_{i=0}^{k} i) + (k+1) = (k(k+1)/2) + (k+1)$ by the inductive hypothesis. From this, we have that $(k(k+1)/2) + (k+1) = (k+1)(k/2+1) = (k+1)(k+2)/2$, which is exactly $P(k+1)$.

# Prove $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n+1)/2$.**
We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**
$\sum_{i=0}^{n} i = 0 = 0(0+1)/2$ so $P(0)$ is true.

③ **Inductive hypothesis:**
Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ **Inductive step:**
We want to prove that $P(k+1)$ is true, i.e., $\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$. Note that $\sum_{i=0}^{k+1} i = (\sum_{i=0}^{k} i) + (k+1) = (k(k+1)/2) + (k+1)$ by the inductive hypothesis. From this, we have that $(k(k+1)/2) + (k+1) = (k+1)(k/2+1) = (k+1)(k+2)/2$, which is exactly $P(k+1)$.

⑤ **The result follows for all $n \geq 0$ by induction.**

# What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?

# What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?

**Let's look at a few examples:**

$$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$$
$$2^{2*1} - 1 = 4 - 1 = 3 = 3 * 1$$
$$2^{2*2} - 1 = 16 - 1 = 15 = 3 * 5$$
$$2^{2*3} - 1 = 64 - 1 = 63 = 3 * 21$$
$$2^{2*4} - 1 = 256 - 1 = 255 = 3 * 85$$

# What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?

**Let's look at a few examples:**

$$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$$
$$2^{2*1} - 1 = 4 - 1 = 3 = 3 * 1$$
$$2^{2*2} - 1 = 16 - 1 = 15 = 3 * 5$$
$$2^{2*3} - 1 = 64 - 1 = 63 = 3 * 21$$
$$2^{2*4} - 1 = 256 - 1 = 255 = 3 * 85$$

**It looks like $3|(2^{2n} - 1)$.**

Let's use induction to prove it!

# Prove $3|(2^{2n}-1)$ for all $n \in \mathbb{N}$

# Prove $3|(2^{2n}-1)$ for all $n \in \mathbb{N}$

① Let $P(n)$ be $3|(2^{2n}-1)$.

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

# Prove $3|(2^{2n}-1)$ for all $n \in \mathbb{N}$

① Let $P(n)$ be $3|(2^{2n}-1)$.

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ so $P(0)$ is true.

# Prove $3|(2^{2n}-1)$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $3|(2^{2n}-1)$.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ so $P(0)$ is true.

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

# Prove $3|(2^{2n}-1)$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $3|(2^{2n}-1)$.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ so $P(0)$ is true.

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $3|(2^{2(k+1)} - 1)$. By inductive hypothesis, $3|(2^{2k} - 1)$ so $2^{2k} - 1 = 3j$ for some integer $j$. We therefore have that $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j+1) - 1 = 12j + 3 = 3(4j+1)$. So $3|(2^{2(k+1)} - 1)$, which is exactly $P(k+1)$.

# Prove $3|(2^{2n}-1)$ for all $n \in \mathbb{N}$

① **Let $P(n)$ be $3|(2^{2n}-1)$.**

We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② **Base case ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ so $P(0)$ is true.

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $3|(2^{2(k+1)} - 1)$. By inductive hypothesis, $3|(2^{2k} - 1)$ so $2^{2k} - 1 = 3j$ for some integer $j$. We therefore have that $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j+1) - 1 = 12j + 3 = 3(4j+1)$. So $3|(2^{2(k+1)} - 1)$, which is exactly $P(k+1)$.

⑤ **The result follows for all $n \geq 0$ by induction.**

# Induction starting at any integer

Proving theorems about all integers $n \geq b$ for some $b \in \mathbb{Z}$.

# Changing the start line

How can we prove $P(n)$ for all integers $n \geq b$ for some integer $b$?

# Changing the start line

How can we prove $P(n)$ for all integers $n \geq b$ for some integer $b$?

**Define a predicate $\mathbf{Q(n) = P(n + b)}$ for all $\mathbf{n \geq 0}$.**

Then $(\forall n.\, Q(n)) \equiv (\forall n \geq b.\, P(n))$

# Changing the start line

How can we prove $P(n)$ for all integers $n \geq b$ for some integer $b$?

**Define a predicate $\mathbf{Q(n) = P(n + b)}$ for all $\mathbf{n \geq 0}$.**

Then $(\forall n.\, Q(n)) \equiv (\forall n \geq b.\, P(n))$

**Use ordinary induction to prove $\mathbf{Q}$:**

Prove $Q(0) \equiv P(b)$.

Prove $(\forall k.\, Q(k) \to Q(k+1)) \equiv (\forall k \geq b.\, P(k) \to P(k+1))$.

# Changing the start line

How can we prove $P(n)$ for all integers $n \geq b$ for some integer $b$?

**Define a predicate $\mathbf{Q(n) = P(n + b)}$ for all $\mathbf{n \geq 0}$.**

Then $(\forall n.\, Q(n)) \equiv (\forall n \geq b.\, P(n))$

**Use ordinary induction to prove $\mathbf{Q}$:**

Prove $Q(0) \equiv P(b)$.

Prove $(\forall k.\, Q(k) \to Q(k+1)) \equiv (\forall k \geq b.\, P(k) \to P(k+1))$.

By convention, we don't define $Q$ explicitly. Instead, we modify our proof template to account for the non-zero base case $b$.

# Inductive proofs for any base case $\mathbf{b} \in \mathbb{Z}$

① **Let $\mathbf{P(n)}$ be** *[ definition of $P(n)$ ]*.

We will show that $P(n)$ is true for every integer $n \geq b$ by induction.

② **Base case ($\mathbf{n = b}$):**

*[ Proof of $P(b)$. ]*

③ **Inductive hypothesis:**

Suppose that $P(k)$ is true for an arbitrary integer $k \geq b$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true.

*[ Proof of $P(k+1)$. This proof **must** invoke the inductive hypothesis. ]*

⑤ **The result follows for all $\mathbf{n \geq b}$ by induction.**

# Example: prove $3^n \geq n^2 + 3$ for all $n \geq 2$

# Example: 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 that $P(n)$ is true for every integer $n \geq 2$ by induction.

# Example: 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 that $P(n)$ is true for every integer $n \geq 2$ by induction.

② **Base case ($n = 2$):**

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

# Example: 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 that $P(n)$ is true for every integer $n \geq 2$ 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 an arbitrary integer $k \geq 2$.

# Example: 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 that $P(n)$ is true for every integer $n \geq 2$ 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 an arbitrary integer $k \geq 2$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $3^{(k+1)} \geq (k+1)^2 + 3 = k^2 + 2k + 4$. Note that $3^{(k+1)} = 3(3^k) \geq 3(k^2 + 3)$ by the inductive hypothesis. From this we have $3(k^2 + 3) = 2k^2 + k^2 + 9 \geq k^2 + 2k + 4 = (k+1)^2 + 3$ since $k \geq 2$. Therefore $P(k+1)$ is true.

# Example: 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 that $P(n)$ is true for every integer $n \geq 2$ 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 an arbitrary integer $k \geq 2$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $3^{(k+1)} \geq (k+1)^2 + 3 = k^2 + 2k + 4$. Note that $3^{(k+1)} = 3(3^k) \geq 3(k^2 + 3)$ by the inductive hypothesis. From this we have $3(k^2 + 3) = 2k^2 + k^2 + 9 \geq k^2 + 2k + 4 = (k+1)^2 + 3$ since $k \geq 2$. Therefore $P(k+1)$ is true.

⑤ **The result follows for all $n \geq 2$ by induction.**

# Strong induction

Induction with a stronger hypothesis.

# Recall how induction works

**Induction** $\dfrac{P(0);\ \forall k.\ P(k) \to P(k+1)}{\therefore\ \forall n.\ P(n)}$

Domain: natural numbers ($\mathbb{N}$).

How do we get $P(5)$ from $P(0)$ and $\forall k.\ P(k) \to P(k+1)$?

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$.
3. Applying Modus Ponens to 1 and 2, we get $P(1)$.
4. Since $P(k) \to P(k+1)$ for all $k$, we have $P(1) \to P(2)$.
5. Applying Modus Ponens to 3 and 4, we get $P(2)$.

⋮

11. Applying Modus Ponens to 9 and 10, we get $P(5)$.

**P(0)**
⇓ **P(0)→P(1)**
**P(1)**
⇓ **P(1)→P(2)**
**P(2)**
⇓ **P(k)→P(k+1)**
**P(5)**

# Recall how induction works

**Induction** $\dfrac{P(0);\ \forall k.\ P(k) \to P(k+1)}{\therefore\ \forall n.\ P(n)}$

Domain: natural numbers ($\mathbb{N}$).

How do we get $P(5)$ from $P(0)$ and $\forall k.\ P(k) \to P(k+1)$?

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all $k$, we have $P(0) \to P(1)$.
3. Applying Modus Ponens to 1 and 2, we get $P(1)$.
4. Since $P(k) \to P(k+1)$ for all $k$, we have $P(1) \to P(2)$.
5. Applying Modus Ponens to 3 and 4, we get $P(2)$.

$\vdots$

11. Applying Modus Ponens to 9 and 10, we get $P(5)$.

**P(0)**
⇓ P(0)→P(1)
**P(1)**
⇓ P(1)→P(2)
**P(2)**
⇓ P(k)→P(k+1)
**P(5)**

Note that we have $P(0), \ldots, P(k)$ when proving $k+1$.
So we can safely assume all of them, rather than just $P(k)$.

# The strong induction rule of inference

**Strong Induction** $\dfrac{P(0); \forall k.\, (P(0) \wedge P(1) \wedge \ldots \wedge P(k)) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

Domain: $\mathbb{N}$.

**Strong induction for $\mathbf{P}$ follows from ordinary induction for $\mathbf{Q}$ where**

$$Q(k) = P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$$

**To see why, note the following:**

$$Q(0) \equiv P(0)$$
$$Q(k+1) \equiv Q(k) \wedge P(k+1)$$
$$(\forall n.\, Q(n)) \equiv (\forall n.\, P(n))$$

# Strong inductive proofs for any base case $\mathbf{b} \in \mathbb{Z}$

① **Let $\mathbf{P(n)}$ be** *[ definition of $P(n)$ ]*.

We will show that $P(n)$ is true for every integer $n \geq b$ by strong induction.

② **Base case ($\mathbf{n = b}$):**

*[ Proof of $P(b)$. ]*

③ **Inductive hypothesis:**

Suppose that for some arbitrary integer $k \geq b$, $P(j)$ is true for every integer $b \leq j \leq k$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true.

*[ Proof of $P(k+1)$. The proof **must** invoke the strong inductive hypothesis. ]*

⑤ **The result follows for all $\mathbf{n \geq b}$ by strong induction.**

# Using strong induction

An example proof and when to use strong induction.

# Example: the fundamental theorem of arithmetic

**Fundamental theorem of arithmetic**

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

**Examples**

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$

$591 = 3 \cdot 197$

$45,523 = 45,523$

$321,950 = 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137$

$1,234,567,890 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3,607 \cdot 3,803$

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

# Prove that every integer $\geq 2$ is a product of primes

# Prove that every integer $\geq 2$ is a product of primes

**① Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

# Prove that every integer $\geq 2$ is a product of primes

**① Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

**② Base case ($\mathbf{n = 2}$):**

2 is prime, so it is a product of primes. Therefore $P(2)$ is true.

# Prove that every integer $\geq 2$ is a product of primes

**① Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

**② Base case ($\mathbf{n = 2}$):**

2 is prime, so it is a product of primes. Therefore $P(2)$ is true.

**③ Inductive hypothesis:**

Suppose that for some arbitrary integer $k \geq 2$, $P(j)$ is true for every integer $2 \leq j \leq k$.

# Prove that every integer $\geq 2$ is a product of primes

**① Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

**② Base case ($\mathbf{n = 2}$):**

2 is prime, so it is a product of primes. Therefore $P(2)$ is true.

**③ Inductive hypothesis:**

Suppose that for some arbitrary integer $k \geq 2$, $P(j)$ is true for every integer $2 \leq j \leq k$.

**④ Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $k+1$ is a product of primes.

# Prove that every integer $\geq 2$ is a product of primes

① **Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

② **Base case ($\mathbf{n = 2}$):**

2 is prime, so it is a product of primes. Therefore $P(2)$ is true.

③ **Inductive hypothesis:**

Suppose that for some arbitrary integer $k \geq 2$, $P(j)$ is true for every integer $2 \leq j \leq k$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $k+1$ is a product of primes.

**Case: $\mathbf{k+1}$ is prime**. Then by definition, $k+1$ is a product of primes.

# Prove that every integer $\geq 2$ is a product of primes

① **Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

② **Base case ($\mathbf{n = 2}$):**

2 is prime, so it is a product of primes. Therefore $P(2)$ is true.

③ **Inductive hypothesis:**

Suppose that for some arbitrary integer $k \geq 2$, $P(j)$ is true for every integer $2 \leq j \leq k$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $k+1$ is a product of primes.

**Case: $\mathbf{k+1}$ is prime**. Then by definition, $k+1$ is a product of primes.

**Case: $\mathbf{k+1}$ is composite**. Then by $k+1 = ab$ for some integers $ab$ where $2 \leq a, b \leq k$.

By inductive hypothesis, we have $P(a) = p_1 p_2 \ldots p_r$ and $P(b) = q_1 q_2 \ldots q_s$, where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are prime. Thus, $k+1 = ab = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$, which is a product of primes.

# Prove that every integer $\geq 2$ is a product of primes

① **Let $\mathbf{P(n)}$ be "$\mathbf{n}$ is a product of primes".**

We will show that $P(n)$ is true for every integer $n \geq 2$ by strong induction.

② **Base case ($\mathbf{n = 2}$):**

2 is prime, so it is a product of primes. Therefore $P(2)$ is true.

③ **Inductive hypothesis:**

Suppose that for some arbitrary integer $k \geq 2$, $P(j)$ is true for every integer $2 \leq j \leq k$.

④ **Inductive step:**

We want to prove that $P(k+1)$ is true, i.e., $k+1$ is a product of primes.

**Case: $\mathbf{k+1}$ is prime**. Then by definition, $k+1$ is a product of primes.

**Case: $\mathbf{k+1}$ is composite**. Then by $k+1 = ab$ for some integers $ab$ where $2 \leq a, b \leq k$.

By inductive hypothesis, we have $P(a) = p_1 p_2 \ldots p_r$ and $P(b) = q_1 q_2 \ldots q_s$, where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are prime. Thus, $k+1 = ab = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$, which is a product of primes.

⑤ **The result follows for all $\mathbf{n \geq 2}$ by strong induction.**

# Strong induction is particularly useful when …

We need to reason about procedures that given an input $k$ invoke themselves recursively on an input different from $k - 1$.

**Example:**

Euclidean algorithm for computing $\mathrm{GCD}(a, b)$.

```
// Assumes a >= b >= 0.
public static int gcd(int a, int b) {
  if (b == 0)
    return a;              // GCD(a, 0) = a
  else
    return gcd(b, a % b); // GCD(a, b) = GCD(b, a mod b)
}
```

We use strong induction to reason about this algorithm and other functions with recursive definitions.

# Summary

**Induction lets us prove statements about all natural numbers.**

A proof by induction must show that $P(0)$ is true (*base case*).

And it must use the *inductive hypothesis* $P(k)$ to show that $P(k+1)$ is true (*inductive step*).

**Induction also lets us prove theorems about integers $\mathbf{n \geq b}$ for $\mathbf{b \in \mathbb{Z}}$.**

Adjust all parts of the proof to use $n \geq b$ instead of $n \geq 0$.

**Strong induction lets us assume a stronger inductive hypothesis.**

This makes some proofs easier.

But every proof by strong induction can be transformed into a proof by ordinary induction and vice versa.