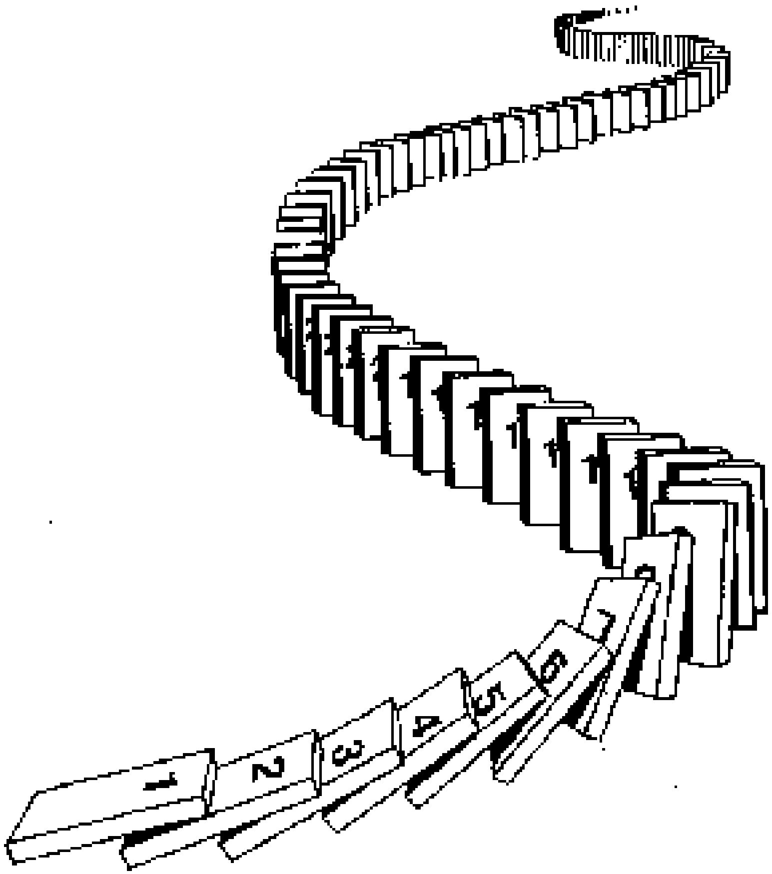
CSE 311: Foundations of Computing

Lecture 14: Induction



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

```
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 $\forall a, b, m > 0\ \forall k \in \mathbb{N}\ (a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m})$

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

Suppose that $a \equiv b \pmod{m}$**.**

We know $\big(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^2 \equiv b^2 \pmod{m}$ **by multiplying congruences. So, applying this repeatedly, we have:**

$$\big(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^2 \equiv b^2 \pmod{m}$$
$$\big(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^3 \equiv b^3 \pmod{m}$$

$a^3 \equiv b^3 \bmod m$

$a^4 \equiv b^4 \bmod m$

$$\dots$$
$$\big(a^{i-1} \equiv b^{i-1} \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^k \equiv b^k \pmod{m}$$

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

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

Induction Is A Rule of Inference

Domain: Natural Numbers

$$P(0)$$

$$\forall k \ (P(k) \longrightarrow P(k+1))$$

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

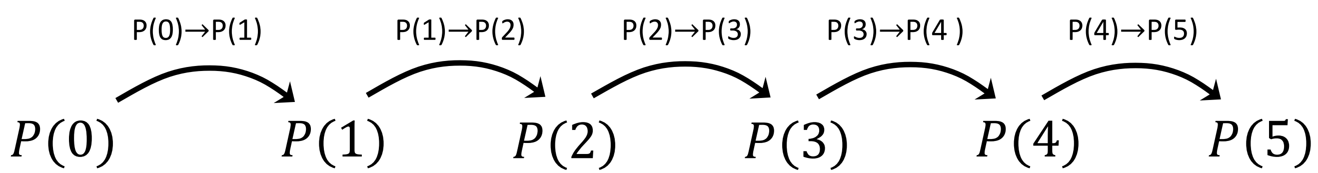
How do the givens prove P(5)?

Induction Is A Rule of Inference

Domain: Natural Numbers

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

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.

Using The Induction Rule In A Formal Proof

$$P(0)$$

$$\forall k\ (P(k) \longrightarrow P(k+1))$$

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

Using The Induction Rule In A Formal Proof

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

1. Prove P(0)

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

Using The Induction Rule In A Formal Proof

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

1. Prove P(0)
2. Let k be an arbitrary integer ≥ 0

   3.1 Assume P(k)

   ⋮

   3.20 P(k+1)

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

Using The Induction Rule In A Formal Proof

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

1. Prove P(0)
2. Let k be an arbitrary integer ≥ 0
    - 3.1. Assume that P(k) is true
    - 3.2. ...
    - 3.3. Prove P(k+1) is true
3. P(k) → P(k+1) — Direct Proof Rule
4. ∀k (P(k) → P(k+1)) — Intro ∀: 2, 3
5. ∀n P(n) — Induction: 1, 4

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. Assume 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

Translating To An English Proof

1. Prove P(0) — **Base Case**
2. Let k be an arbitrary integer ≥ 0 — **Inductive Hypothesis**
    3.1. Assume that P(k) is true
    3.2. ... — **Inductive Step**
    3.3. Prove P(k+1) is true
3. $P(k) \to P(k+1)$ — Direct Proof Rule
4. $\forall k\,(P(k) \to P(k+1))$ — Intro $\forall$: 2, 3
5. $\forall n\, P(n)$ — Induction: 1, 4

Conclusion

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 "$1 + 2 + \ldots + 2^n = 2^{n+1} - 1$".

2. $1 = 2^0 = 2^{0+1} - 1 = 1$ ✓ P(0) holds true

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

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.**

$a^{x+y} = a^x \cdot a^y$

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. IH: Assume P(k) for some arbitrary integer $k \geq 0$.
4. Goal: P(k+1) holds true.

we want to prove $1 + 2 + \cdots + 2^{k+1} = 2^{k+1+1} - 1$.

By IH: $1 + 2 + \cdots + 2^k = 2^{k+1} - 1$?

$+ 2^{k+1}$ $\quad$ $+ 2^{k+1}$

$1 + 2 + \cdots + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1 = 2 \cdot 2^{k+1} - 1 = 2^{k+1+1} - 1$

P(k+1) holds.

5. P(n) holds for all n.

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** $k \geq 0$**.**

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

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

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

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

$$1 + 2 + \ldots + 2^k + 2^{k+1} = (1+2+ \ldots + 2^k) + 2^{k+1}$$

$$= 2^{k+1} - 1 + 2^{k+1} \quad \textbf{by the IH}$$

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

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).

Alternative way of writing the inductive step

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

   $$1 + 2 + \ldots + 2^k + 2^{k+1} = (1+2+ \ldots + 2^k) + 2^{k+1}$$
   $$= 2^{k+1} - 1 + 2^{k+1} \text{ by the IH}$$

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

1. Let P(n) be "$1 + 2 + \ldots + n = n(n+1)/2$".
2. Base Case: P(0) "$0 = 0(0+1)/2$" is true

0+

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.**

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.**

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.
4. **Induction Step:**

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

P(k) is $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$

$$1 + 2 + \ldots + k + k+1 = \frac{k(k+1)}{2} + k+1 \quad \text{by IH}$$

$$= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

P(k+1) holds.

5. P(n) holds for all n ≥ 0 by ind

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.
4. **Induction Step:**

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

   1 + 2 + … + k + (k+1) = (1 + 2 + … + k) + (k+1)

   = k(k+1)/2 + (k+1) **by IH**

   Now k(k+1)/2 + (k+1) = (k+1)(k/2 + 1) = (k+1)(k+2)/2.

   So, we have 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.**

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 $n \geq 0$

1. Let $P(n)$ be "$3 \mid (2^{2n}-1)$". We prove $P(n)$ for all $n \geq 0$.

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

1. **Let** P(n) **be** "3 | (2^{2n} – 1)". **We will show** P(n) i**s true for all natural numbers by induction.**
2. **Base Case** (n=0): $3 \mid 2^{2\cdot 0} - 1 = 0$ ✓

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

$a^{x+y} = a^x \cdot a^y$

1. **Let** P(n) **be "**3 | (2^{2n} – 1)**". We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}$-1=1-1=0=3·0 **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0**.**

   $3 \mid (2^{2k}-1)$

4. **Induction Step:**

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

$2^{2k}-1 = q \cdot 3$ for some q.

So $2^{2k} = 1 + q \cdot 3$

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

$2^{2(k+1)}-1 = (1+q\cdot 3)\cdot 4 - 1 = q \cdot 12 + 3 = 3(4\cdot q+1)$

So $3 \mid 2^{2(k+1)}-1$ implies $P(k+1)$.

5 $P(n)$ holds for all n.

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): $2^{2\cdot 0}$-1=1-1=0=3·0 **Therefore** $P(0)$ **is true.**
3. **Induction Hypothesis: Suppose that** $P(k)$ **is true for some arbitrary integer** $k \geq 0$**.**
4. **Induction Step:**

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

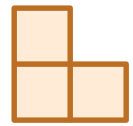
   By IH, $3 \mid (2^{2k} - 1)$ **so** $2^{2k} - 1 = 3j$ **for some integer** j

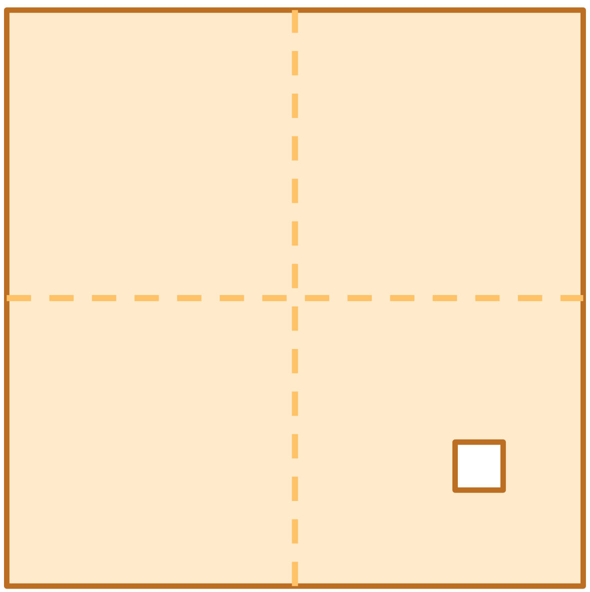
   So $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j+1) - 1$

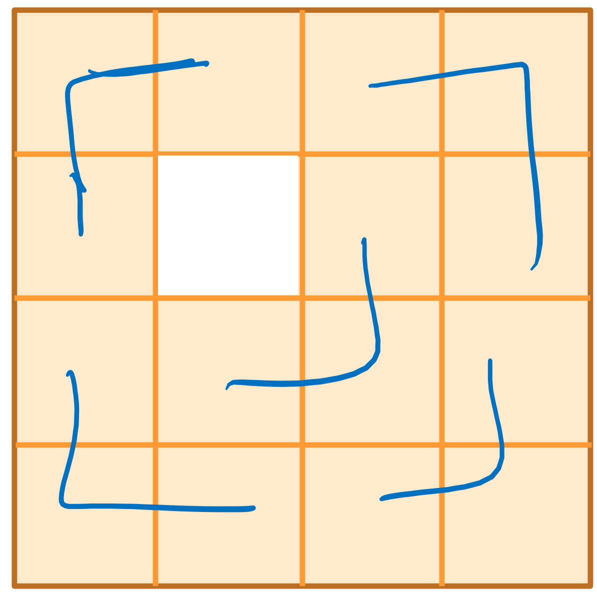
   $= 12j+3 = 3(4j+1)$

   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.**

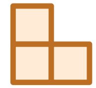
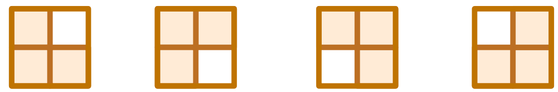
Checkerboard Tiling

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

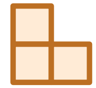
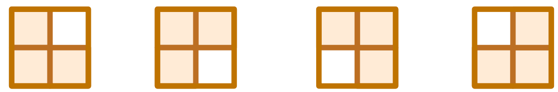


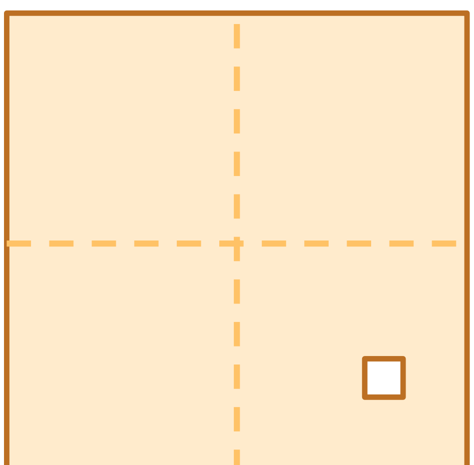


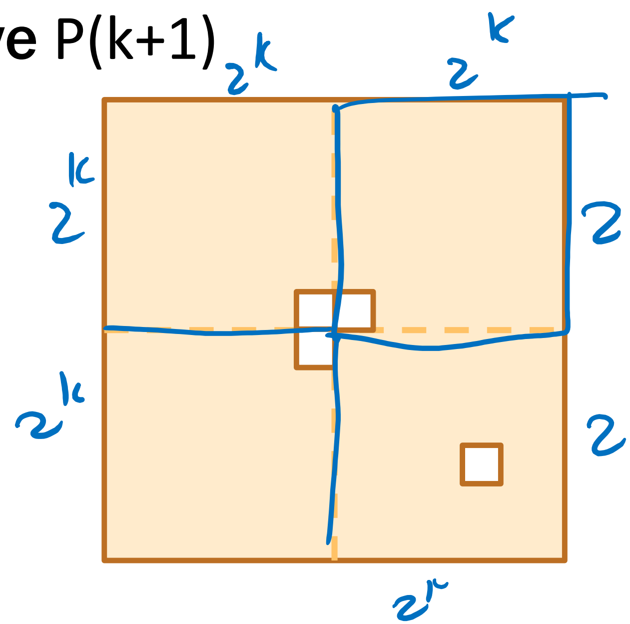
Checkerboard Tiling

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 $k \geq 1$
4. Inductive Step: Prove $P(k+1)$





Apply IH to each quadrant then fill with extra tile.