

# Mathematical Induction II

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	



1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

# This Lecture

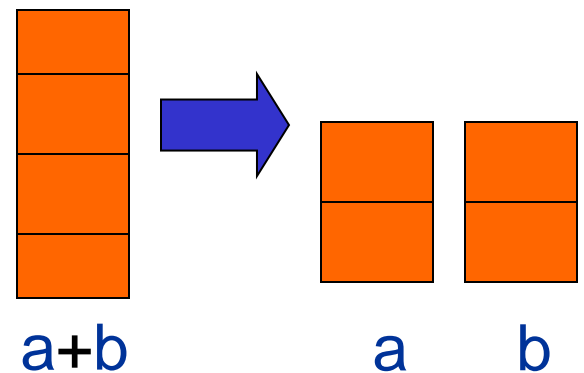
We will continue our discussions on mathematical induction.

The new elements in this lecture are some variations of induction:

- Strong Induction
- Well Ordering Principle
- Invariant Method

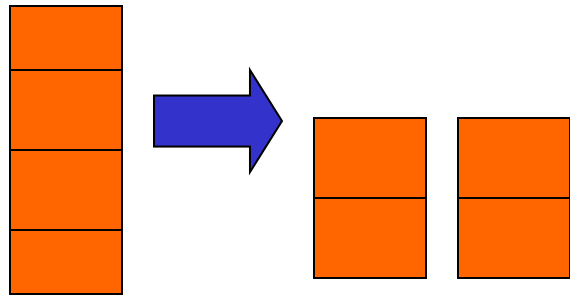
# Unstacking Game

- Start: a stack of boxes
- Move: split any stack into two stacks of sizes  $a, b > 0$
- Scoring:  $ab$  points
- Keep moving: until stuck
- Overall score: sum of move scores

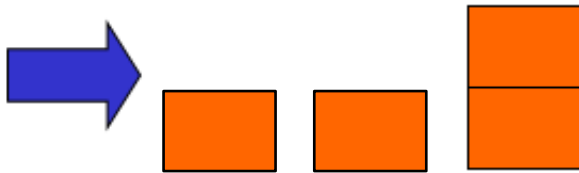


# Unstacking Game

**Example:** Suppose there are 4 boxes.



Gain score:  $2 \times 2 = 4$



Gain score:  $1 \times 1 = 1$

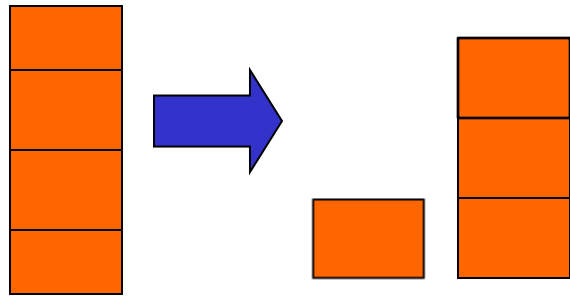


Gain score:  $1 \times 1 = 1$

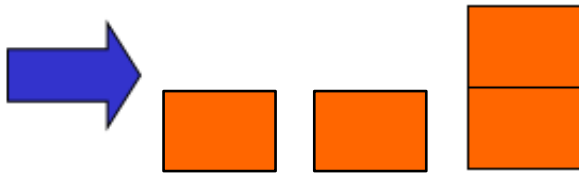
So total score =  $4 + 1 + 1 = 6$ .

# Unstacking Game

**Example:** Suppose there are 4 boxes.



Gain score:  $1 \times 3 = 3$



Gain score:  $1 \times 2 = 2$



Gain score:  $1 \times 1 = 1$

So total score =  $3 + 2 + 1 = 6$ .

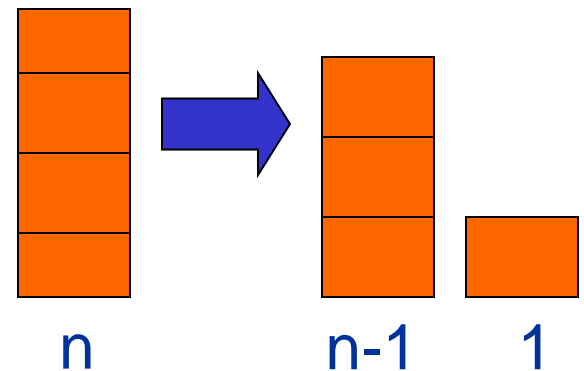
# Unstacking Game

What is the best way to play this game?

Suppose there are  $n$  boxes.

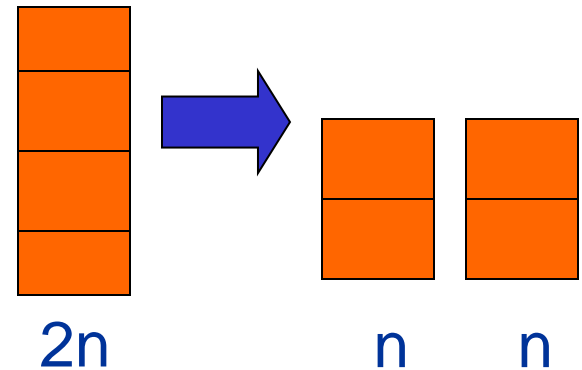
What will be the total score if we just move one box at a time?

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$$



# Unstacking Game

What is the best way to play this game?



Suppose there are  $n$  boxes.

What is the score if we cut the stack into half each time?

Say  $n=8$ , then the score is  $1 \times 4 \times 4 + 2 \times 2 \times 2 + 4 \times 1 = 28$

first round      second      third

Say  $n=16$ , then the score is  $8 \times 8 + 2 \times 28 = 120$

Not better  
than the first  
strategy!

$$\frac{n(n-1)}{2}$$

# Unstacking Game

*Claim:* Every way of unstacking gives the same score.

*Claim:* Starting with size  $n$  stack, the **highest** score will be  $\frac{n(n-1)}{2}$

*Proof:* by Induction with  $Claim(n)$  as hypothesis

**Base case**  $n = 0$ :

$$\text{score} = 0 = \frac{0(0-1)}{2}$$

$Claim(0)$  is okay.



# Unstacking Game

**Inductive step.** assume for  $n$ -stack,  
and then prove  $C(n+1)$ :

$$(n+1)\text{-stack score} = \frac{(n+1)n}{2}$$

**Case**  $n+1 = 1$ . verify for 1-stack:

$$\text{score} = 0 = \frac{1(1-1)}{2}$$

$C(1)$  is okay.

# Unstacking Game

**Case**  $n+1 > 1$ . So split into an  $a$ -stack and a  $b$ -stack,  
where  $a + b = n+1$ .

$$(a + b)\text{-stack score} = ab + a\text{-stack score} + b\text{-stack score}$$

by induction:

$$a\text{-stack score} = \frac{a(a-1)}{2}$$

$$b\text{-stack score} = \frac{b(b-1)}{2}$$

# Unstacking Game

$$(a + b)\text{-stack score} = ab + a\text{-stack score} + b\text{-stack score}$$

$$ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} =$$

$$\frac{2ab + a^2 - a + b^2 - b}{2} = \frac{(a+b)^2 - (a+b)}{2} =$$

$$\frac{(a+b)((a+b)-1)}{2} = \frac{(n+1)n}{2}$$

so  $C(n+1)$  is okay.      We're done!

# Induction Hypothesis

**Wait:** we assumed  $C(a)$  and  $C(b)$  where  $1 \leq a, b \leq n$ .

**But** by induction can only assume  $C(n)$

**the fix:** rephrase the induction hypothesis to

$$Q(n) ::= \\ \forall m \leq n. C(m)$$

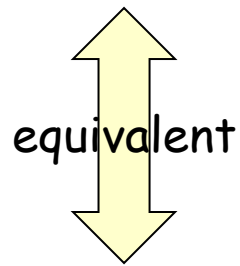
In words, it says that we  
assume the claim is true  
for all numbers up to  $n$ .

Proof goes through fine using  $Q(n)$  instead of  $C(n)$ .

So it's OK to assume  $C(m)$  for all  $m \leq n$  to prove  $C(n+1)$ .

# Strong Induction

Strong induction



Prove  $P(0)$ .

Then prove  $P(n+1)$  assuming *all* of  
 $P(0), P(1), \dots, P(n)$  (instead of just  $P(n)$ ).

Conclude  $\forall n. P(n)$

Ordinary induction

$0 \rightarrow 1, 1 \rightarrow 2, 2 \rightarrow 3, \dots, n-1 \rightarrow n$ .

So by the time we get to  $n+1$ , already know *all* of  
 $P(0), P(1), \dots, P(n)$

The point is: assuming  $P(0), P(1)$ , up to  $P(n)$ , it is often easier to prove  $P(n+1)$ .

# Divisibility by a Prime

**Theorem.** Any integer  $n > 1$  is divisible by a prime number.

Remember this slide?

Now we can prove it by strong induction very easily. In fact we can prove an even stronger theorem very easily.

- Let  $n$  be an integer.
- If  $n$  is a prime number, then we are done.
- Otherwise,  $n = ab$ , both are smaller than  $n$ .
- If  $a$  or  $b$  is a prime number, then we are done.
- Otherwise,  $a = cd$ , both are smaller than  $a$ .
- If  $c$  or  $d$  is a prime number, then we are done.
- Otherwise, repeat this argument, since the numbers are getting smaller and smaller, this will eventually stop and we will find a prime factor of  $n$ .

Idea of induction

# Prime Products

**Theorem.** Any integer  $n > 1$  is divisible by a prime number.

**Theorem:** Every integer  $> 1$  is a product of primes.

*Proof:* (by strong induction)

- Base case is easy.
- Suppose the claim is true for all  $2 \leq i < n$ .
- Consider an integer  $n$ .
- If  $n$  is prime, then we are done.
- Otherwise  $n = k \cdot m$  for integers  $k, m$  where  $2 \leq k, m < n$ .
- By the induction hypothesis, both  $k$  and  $m$  are product of primes

$$k = p_1 \cdot p_2 \cdot \cdots p_{94}$$

$$m = q_1 \cdot q_2 \cdot \cdots q_{214}$$

# Prime Products

*Theorem:* Every integer  $> 1$  is a product of primes.

...So

$$n = k \cdot m = p_1 \cdot p_2 \cdot \cdots \cdot p_{94} \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_{214}$$

is a prime product.

$\therefore$  This completes the proof of the induction step.



# Postage by Strong Induction

Available stamps:



5¢



3¢

What amount can you form?

*Theorem:* Can form any amount  $\geq 8¢$

Prove by strong induction on  $n$ .

$P(n) ::=$  can form  $n¢$ .

# Postage by Strong Induction

Base case ( $n = 8$ ):

8¢:



Inductive Step: assume  $m$ ¢ for  $8 \leq m < n$ ,  
then prove  $n$ ¢

cases:

$n=9$ :



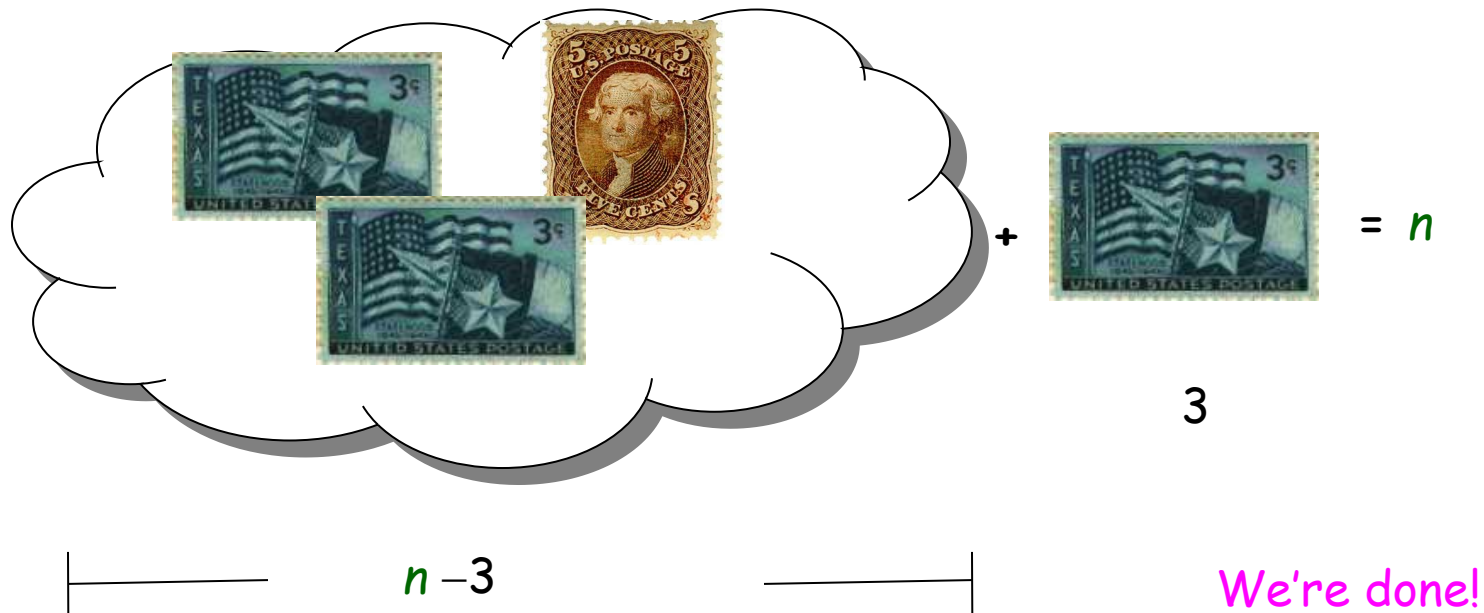
$n=10$ :



# Postage by Strong Induction

case  $n \geq 11$ : let  $m = n - 3$ .

Then  $n > m \geq 8$ , so by induction hypothesis have:



# Postage by Strong Induction

Given an unlimited supply of 5-cent and 7-cent stamps,  
what postages are possible?

**Theorem:** For all  $n \geq 24$ ,

it is possible to produce  $n$  cents of postage from 5¢ and 7¢ stamps.

# This Lecture

- Strong Induction
- Well Ordering Principle
- Invariant Method

# Well Ordering Principle

**Fact**

Every nonempty set of *natural numbers*  
has a *least element*  
*(least here has its usual meaning: smallest)*

This fact is a consequence of axiom of induction.

Note that some similarly-looking statements are not true:

Every nonempty set of *nonnegative real numbers*  
has a *least element*.

NO!

Every nonempty set of ~~*nonnegative*~~ *integers*  
has a *least element*.

NO!

# Well Ordering Principle

**Fact**

Every nonempty set of *natural numbers*  
has a *least element*.

The following variations (as consequences of this axiom) are also called *Well Ordering Principle*.

- A union of *finitely many negative integers and the natural numbers* has a *least element*.
- A nonempty subset of  $\mathbb{Z}^+$  has a *least element*.

# Well Ordering Principle

Thm:  $\sqrt{2}$  is irrational

Proof: suppose  $\sqrt{2} = \frac{m}{n}$

Remember  
this proof?



...can **always** find such  $m, n$  **without common factors**...

why **always**?

By **WOP**,  $\exists$  **minimum**  $|m|$  s.t.  $\sqrt{2} = \frac{m}{n}$ .

so  $\sqrt{2} = \frac{m_0}{n_0}$  where  $|m_0|$  is **minimum**





# Well Ordering Principle

but if  $m_0, n_0$  had a common factor  $c > 1$ , then

$$\sqrt{2} = \frac{m_0 / c}{n_0 / c}$$

and  $|m_0 / c| < |m_0|$  **contradicting** minimality of  $|m_0|$ .

In this example, the well ordering principle is used as follows.

- We first construct a set  $S$  (*which we want it to be well ordered*).
- Assume the hypothesis not true, so that  $S$  is well ordered.
- Take a "**smallest**" element from  $S$ , show that there is an even "**smaller**" one in  $S$ .
- Reach a contradiction, so the hypothesis holds.

# Non-Fermat Theorem

It is difficult to prove there is no positive integer solutions for

$$a^3 + b^3 = c^3$$

Fermat's theorem

But it is easy to prove there is no positive integer solutions for

$$4a^3 + 2b^3 = c^3$$

Non-Fermat's theorem

**Hint:** Prove by contradiction using well ordering principle...

# Non-Fermat Theorem

**Theorem.** There is no positive integer solutions for

$$4a^3 + 2b^3 = c^3$$

- Using the previous strategy, we construct the set

$$S ::= \{a \in \mathbb{Z}^+ \mid \exists b, c \in \mathbb{Z}^+, 4a^3 + 2b^3 = c^3\}$$

- Suppose the theorem not true. Then  $S$  is not empty.
- So  $S$  is a well-ordered set, and there exists

$$(a, b, c) \in S \quad \text{where } a \text{ is the smallest among all "a"s}$$

If we can find  $(a', b', c') \in S$  where  $a' < a$ , then we can reach a contradiction.

## Non-Fermat Theorem

**Theorem.** There is no positive integer solutions for

$$4a^3 + 2b^3 = c^3$$

We shall show that  $a, b, c$  must be even, and hence  $(a/2, b/2, c/2) \in S$ .

This contradicts to the "smallness" of  $a$ , so the theorem is proved.

First, since  $c^3$  is even,  $c$  must be even. (because odd power is odd).

Let  $c = 2c'$ , then  $4a^3 + 2b^3 = (2c')^3$

$$4a^3 + 2b^3 = 8c'^3$$

$$b^3 = 4c'^3 - 2a^3$$

## Non-Fermat Theorem

$$b^3 = 4c'^3 - 2a^3$$

Since  $b^3$  is even,  $b$  must be even. (because odd power is odd).

Let  $b = 2b'$ , then  $(2b')^3 = 4c'^3 - 2a^3$

$$8b'^3 = 4c'^3 - 2a^3$$

$$a^3 = 2c'^3 - 4b'^3$$

Since  $a^3$  is even,  $a$  must be even. (because odd power is odd).

Therefore,  $a, b, c$  are all even, so we are done.

# Well Ordering Principle in Proofs

To prove “ $\forall n \in \mathbb{N} P(n)$ ” using WOP:

1. Construct the set

$$S ::= \{n \in \mathbb{N} \mid \neg P(n)\}$$


2. Assume  $\neg P(n)$  exists, so that  $S$  is a well-ordered set.
3. By WOP, have a “least” element  $n_0 \in S$ . (*we may have different meanings of “least” in some circumstances.*)
4. Reach a contradiction (*use whatever methods you want including mathematical induction*)
  - usually by finding an element of  $S$  that is  $< n_0$ .
5. Conclude that  $P(n)$  is true. QED

**Note:** this is the general strategy, but it may vary in practice.

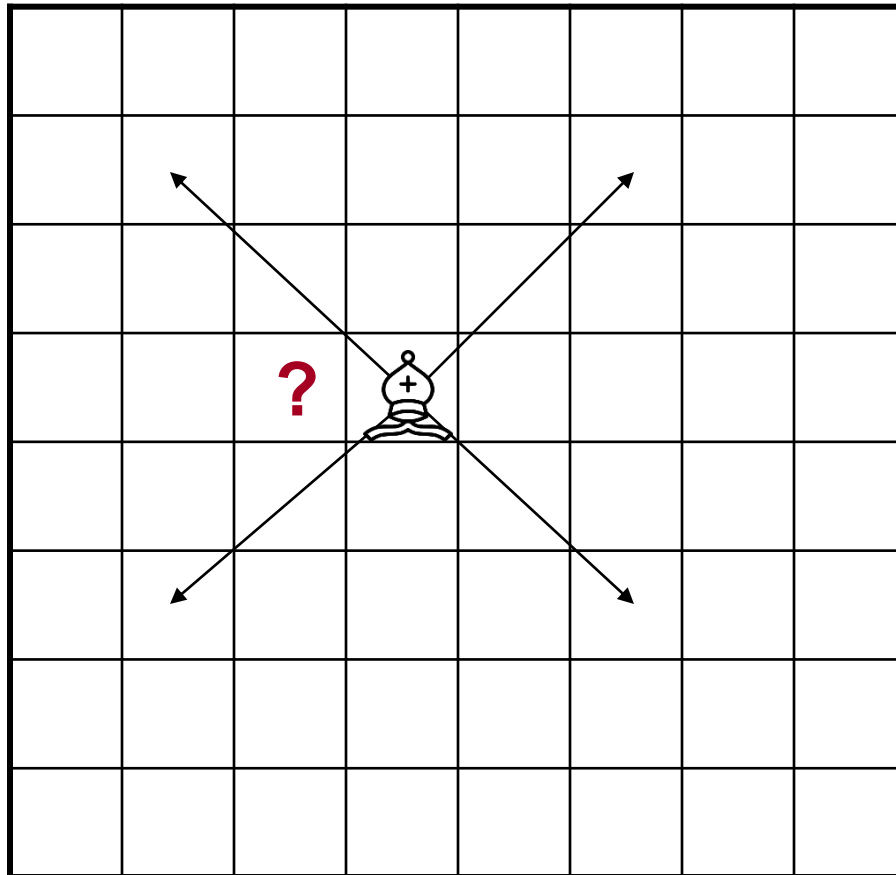
# This Lecture

- Strong Induction
- Well Ordering Principle
- Invariant Method

# A Chessboard Problem

A bishop  can only move along a diagonal

Can a bishop move from its current position to the question mark?





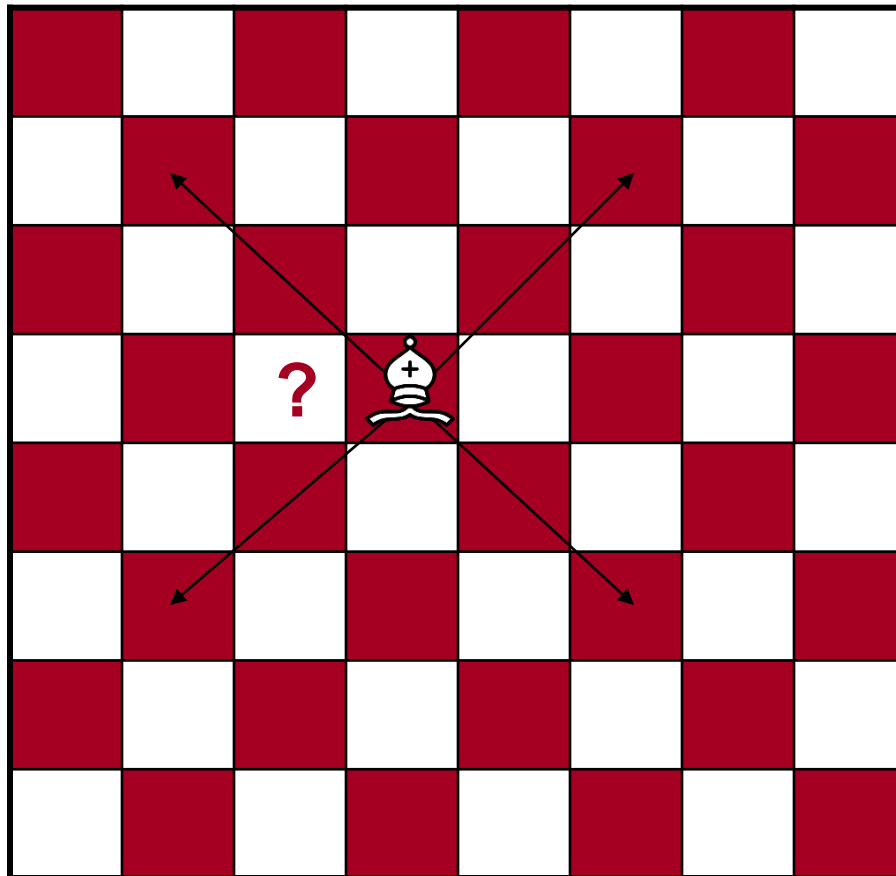
# A Chessboard Problem

A bishop  can only move along a diagonal

Can a bishop move from its current position to the question mark?

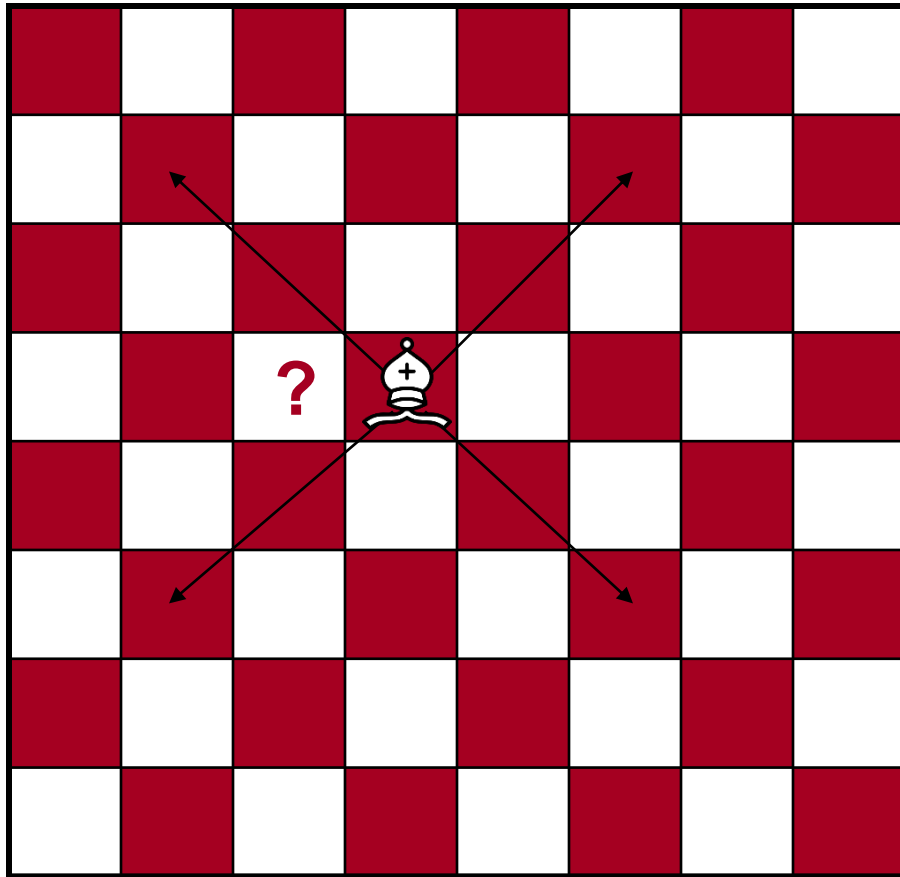
Impossible!

Why?



# A Chessboard Problem

**Invariant!**



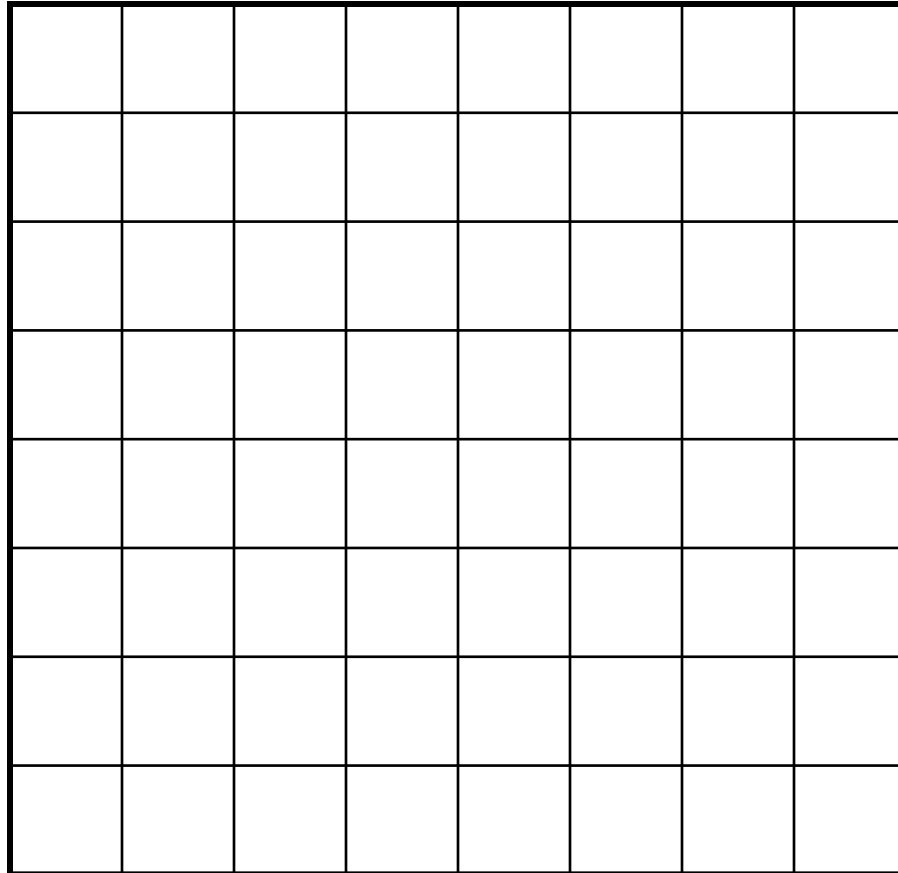
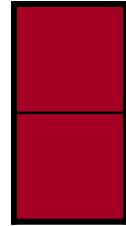
1. The bishop is in a **red** position.
2. A **red** position can only move to a **red** position by diagonal moves.
3. The question mark is in a **white** position.
4. So it is impossible for the bishop to go there.

This is a simple example of the invariant method.

# Domino Puzzle

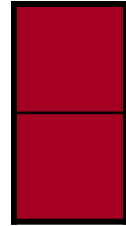
An 8x8 chessboard, 32 pieces of dominos

Can we fill the chessboard?

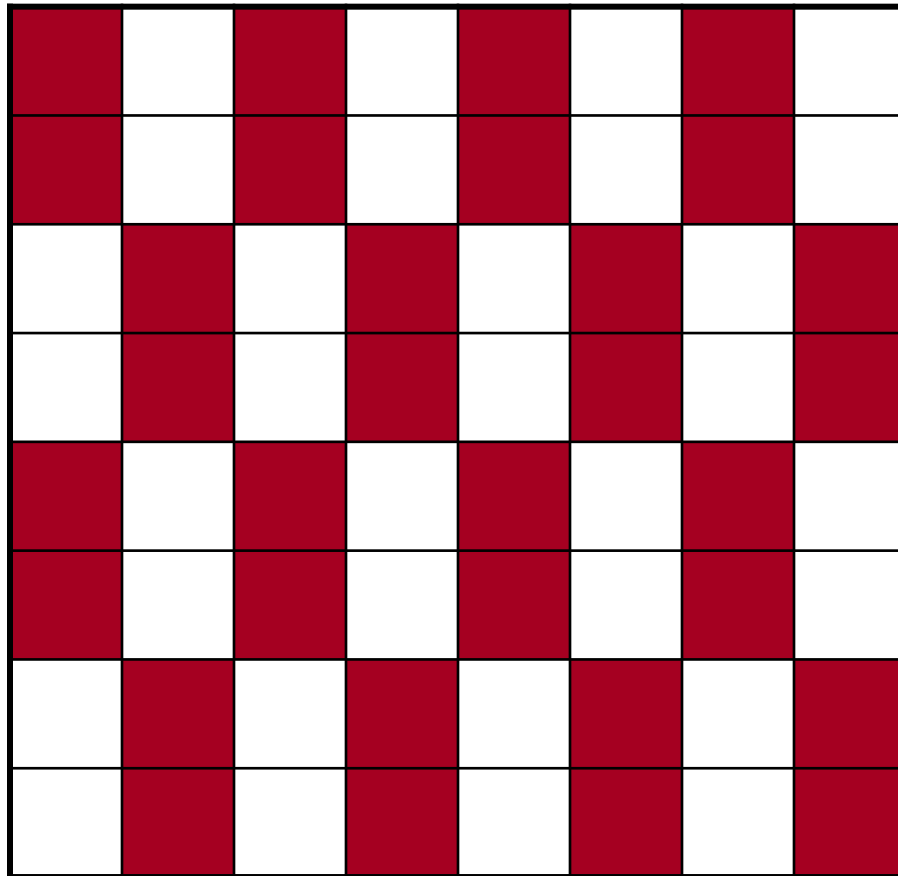


# Domino Puzzle

An 8x8 chessboard, 32 pieces of dominos



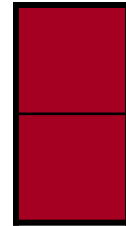
Easy!



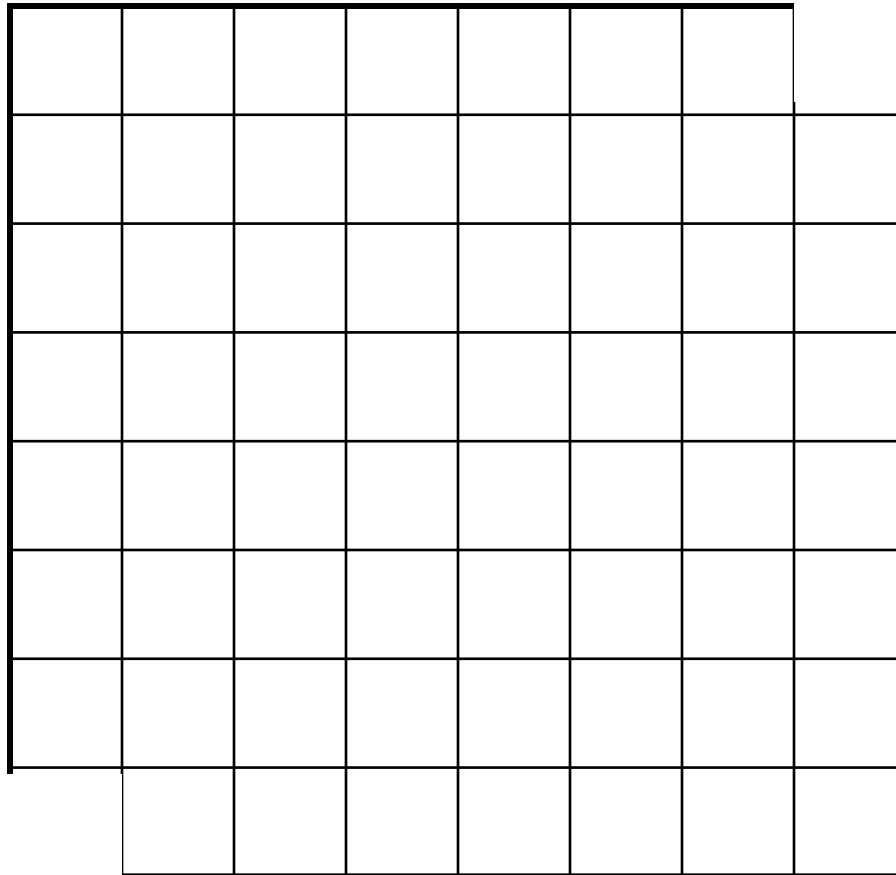
# Domino Puzzle

An 8x8 chessboard with **two holes**, **31** pieces of dominos

Can we fill the chessboard?



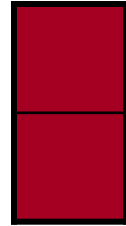
Easy??



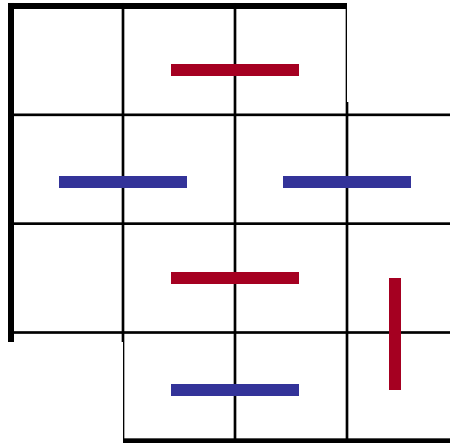
# Domino Puzzle

An 4x4 chessboard with **two holes**, **7** pieces of dominos

Can we fill the chessboard?



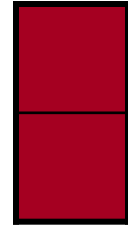
Impossible!



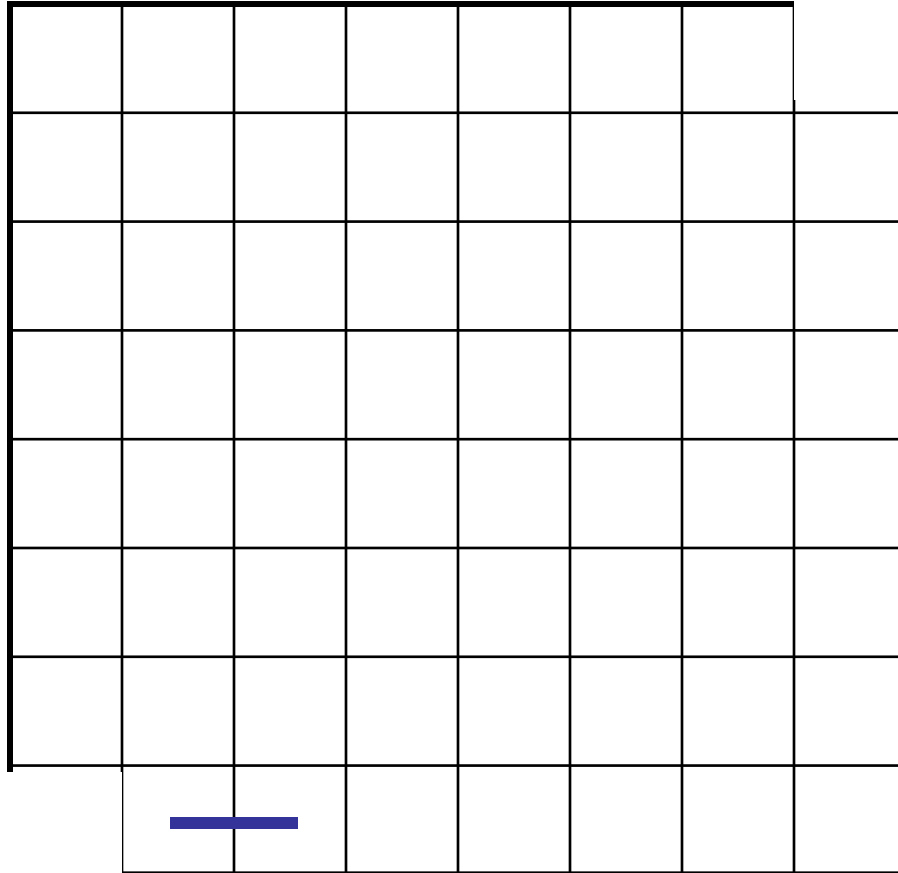
# Domino Puzzle

An 8x8 chessboard with **two holes**, **31** pieces of dominos

Can we fill the chessboard?



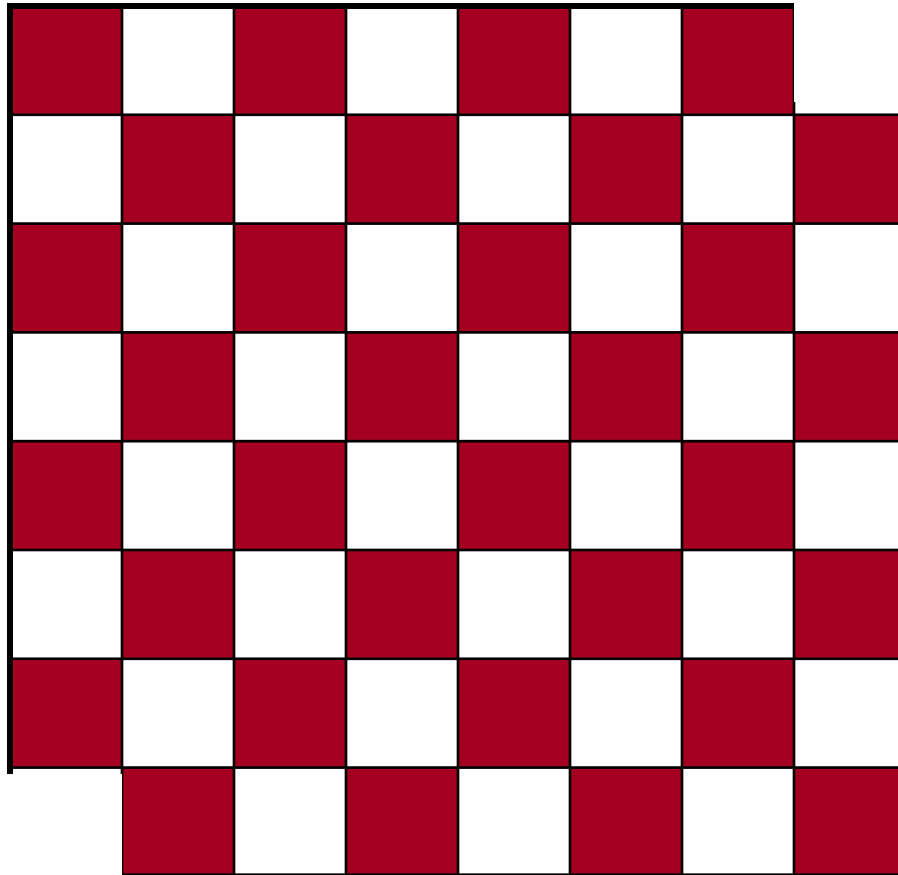
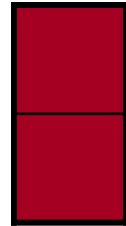
Then what??



# Domino Puzzle

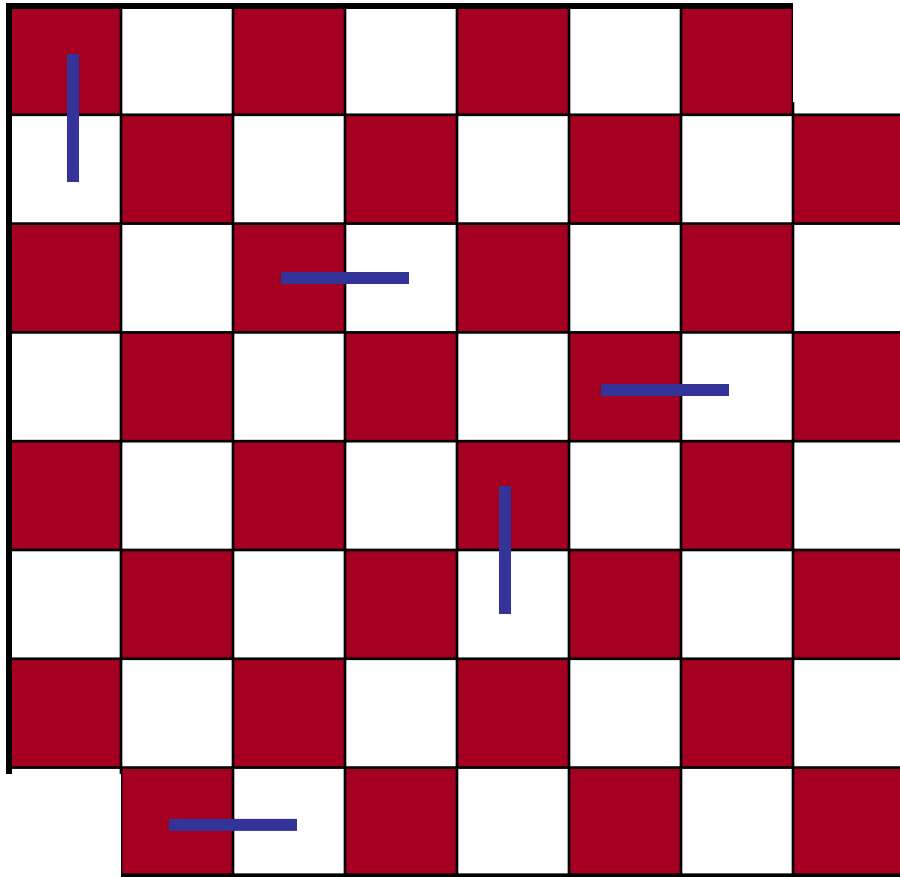
An 8x8 chessboard with **two holes**, **31** pieces of dominos

Can we fill the chessboard?





# Domino Puzzle



**Invariant!**



1. Each domino will occupy one white square and one red square.
2. There are 32 red squares but only 30 white squares.
3. So it is impossible to fill 31 dominos with 30 white squares!

This is another example of the invariant method.

# Invariant Method

1. Observe properties (**the invariants**) that are satisfied throughout the whole process (**by induction**).
2. Show that the target do not satisfy the properties.
3. Conclude that the target is not achievable.

In the bishop example, the invariant is the colour of the positions of the bishop.

In the domino example, the invariant is that any placement of dominos will occupy the same number of red positions and white positions.

Very useful in analysis of algorithms.

## Challenge

Can we move from the left state to the right state?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	



1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Usually, the invariant methods are not easy.

We will come back to this problem later.



**EXCUSE ME ?**

## Quick Summary

Induction is perhaps the most important proof technique in computer science.

For example it is very important in proving the correctness of an algorithm (by invariant method) and also analyzing the running time of an algorithm.

There is no particular example that you should remember.

The point here is to understand the principle of mathematical induction (the way that you “reduce” a large problem to smaller problems), and apply it to the new problems that you will encounter in future.

Possibly the only way to learn this is by doing more exercises.