Plan

We will:

- Finish **Section 5.1 (Rosen)** *Mathematical Induction*
  Section 11.4 (ZyBooks) – one more example

- Cover **Section 5.2** *Strong induction and well-ordering*
  Section 11.5 (ZyBooks)

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ "

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k +1 - k - 1 =$

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

$=$

keep
(we will use it later)

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

$= k^3 - k + 3(k^2 + k)$

divisible by IH

divisible by 3 because 3 is a factor

Section 5.1 Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

$= k^3 - k + 3(k^2 + k)$

divisible by IH

divisible by 3 because 3 is a factor

hence their sum is divisible by 3

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

$= k^3 - k + 3(k^2 + k)$

divisible by IH

divisible by 3 because 3 is a factor

we showed that P(k+1) also holds under the IH

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let $n = 1$, then

P(1): " 1^3-1 is divisible by 3, $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

$= k^3 - k + 3(k^2 + k)$

divisible by IH

divisible by 3 because 3 is a factor

we showed that P(k+1) also holds under the IH

This completes the inductive step

Mathematical Induction (continues)

Example: prove that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

Proof: Let P(n): " n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$ "

Base step: let n = 1, then

P(1): " 1^3-1 is divisible by 3 if $1 \in \mathbf{Z}^+$ " True!

0 is divisible by 3

By mathematical induction we proved that n^3-n is divisible by 3 if $n \in \mathbf{Z}^+$

qed

Inductive step: assume P(k) is true for any arbitrary fixed k, i.e. " k^3-k is divisible by 3 if $k \in \mathbf{Z}^+$ " IH

Let's show that in this case P(k+1) is also true:

$(k+1)^3 - (k+1) = k^3+3k^2 + 3k + \cancel{1} - k - \cancel{1} = k^3+3k^2 + 3k - k =$

$= k^3 - k + 3(k^2 + k)$

divisible by IH

divisible by 3 because 3 is a factor

thus we showed that P(k+1) also holds under the IH

This completes the inductive step

Mathematical Induction (continues)

Recommended:

- see the proof of the *cardinality of the powerset of a finite set S with n elements* (powerset P(S) has 2^n cardinality)

Video on YouTube: https://youtu.be/LNFcdH-QAAc (*Rosen book: Example 10 on page 323*).

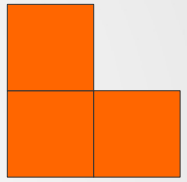
- see proofs of closed forms for the sum of terms in an arithmetic sequence and for the sum of terms in a geometric sequence in zyBooks, section 11.5
- do the participation Activity 11.5.6 (*in Rosen book: Example 11 on page 323*), which proves the generalization of one of De Morgan's laws about sets:

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$$

Mathematical Induction (continues)

Example:

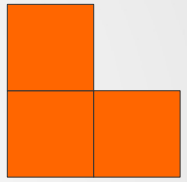
Let n be a positive integer. Show that every $2^n \times 2^n$, $n > 0$, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



Mathematical Induction (continues)

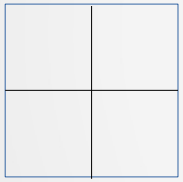
Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, $n > 0$, checkerboard with one square removed can be tiled using *right trominoes*, pieces shaped like the letter "L."



2^1

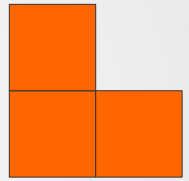
2^1



Mathematical Induction (continues)

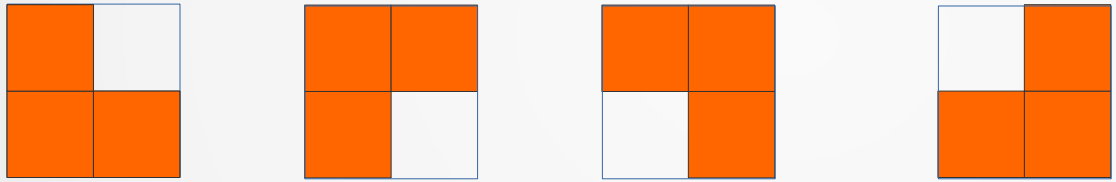
Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



2^1

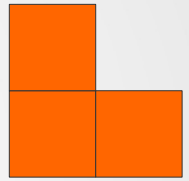
2^1



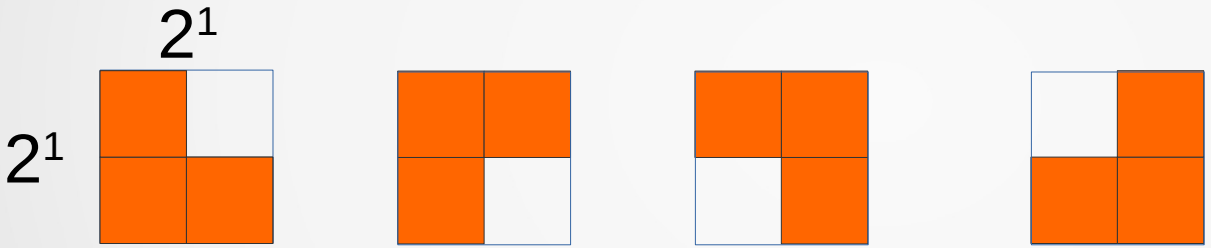
Mathematical Induction (continues)

Example:

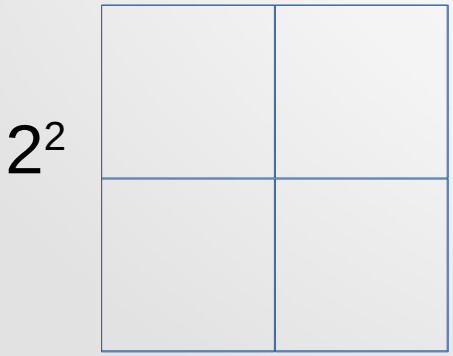
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



2^1



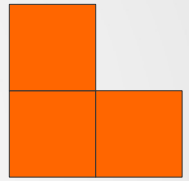
2^2



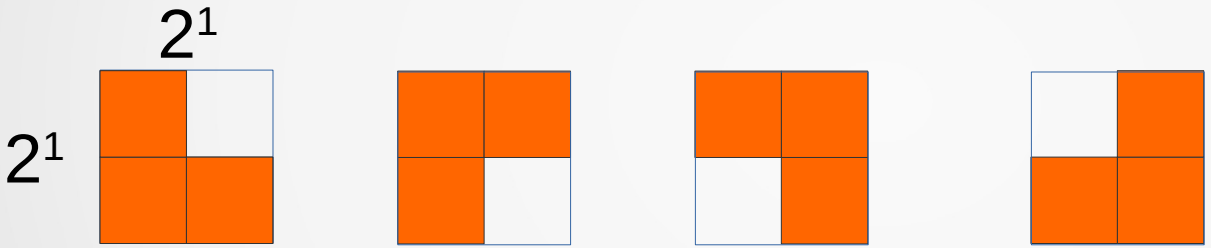
Mathematical Induction (continues)

Example:

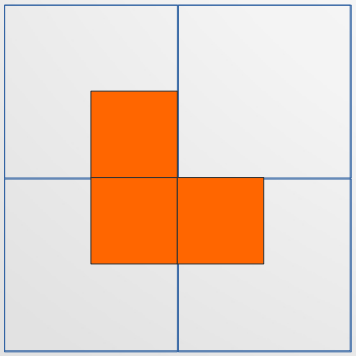
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right trominoes*, pieces shaped like the letter "L."



2^1



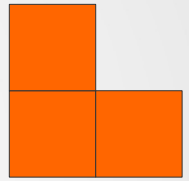
2^2



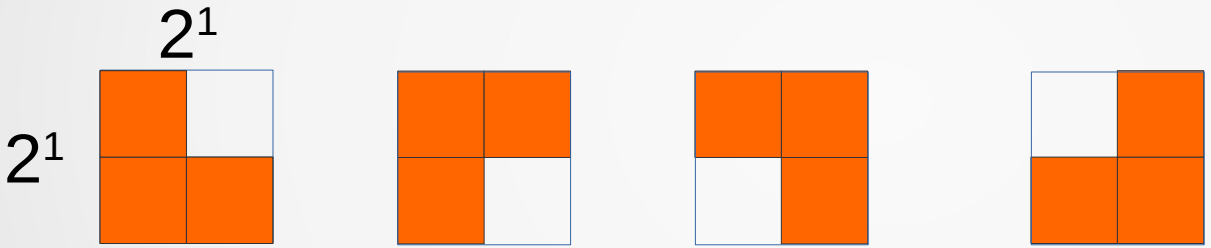
Mathematical Induction (continues)

Example:

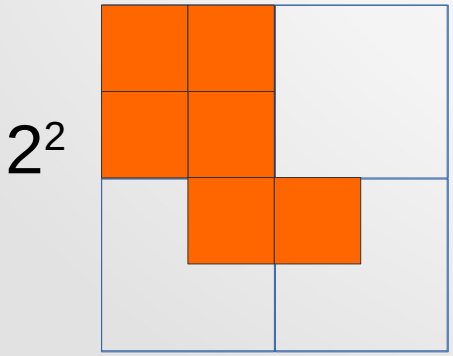
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



2^1



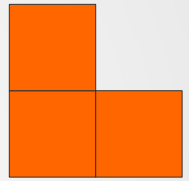
2^2



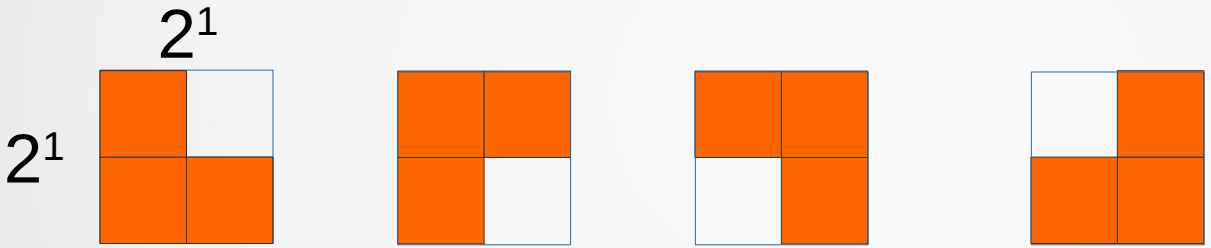
Mathematical Induction (continues)

Example:

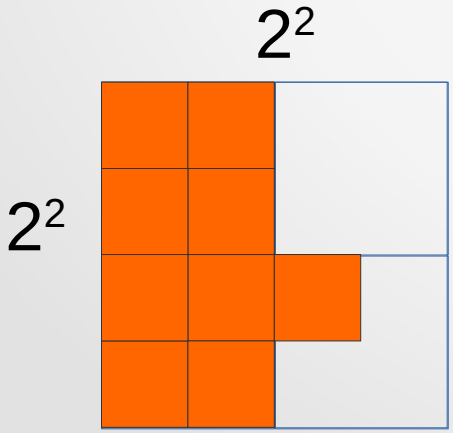
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



2^1



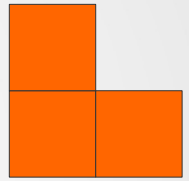
2^2



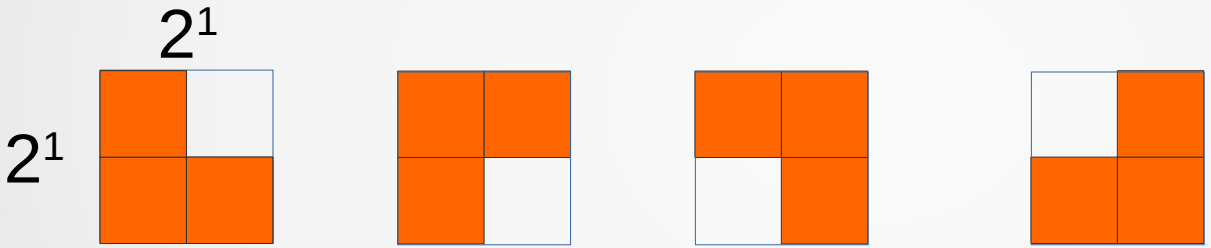
Mathematical Induction (continues)

Example:

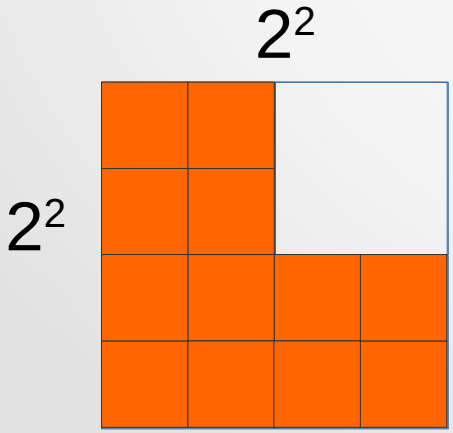
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



2^1



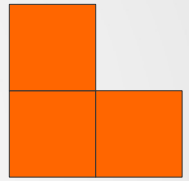
2^2



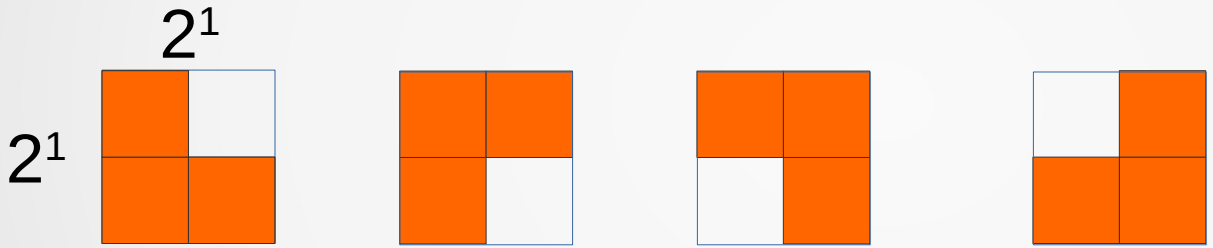
Mathematical Induction (continues)

Example:

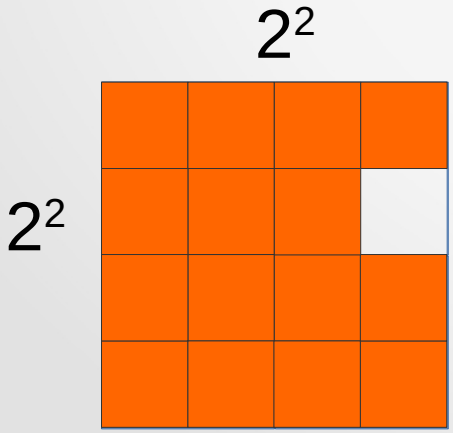
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter “L.”



2^1



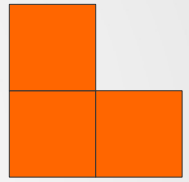
2^2

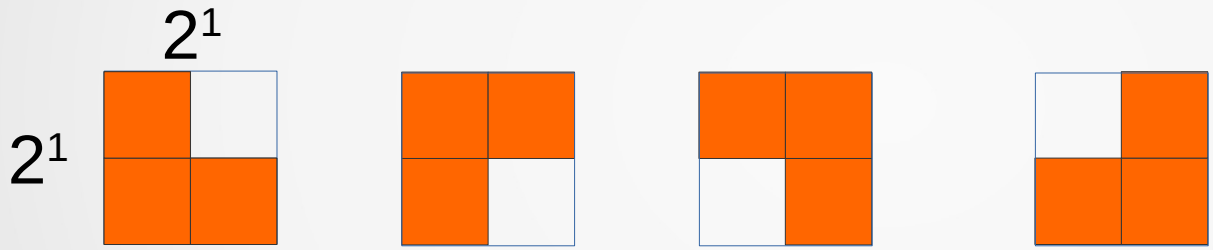


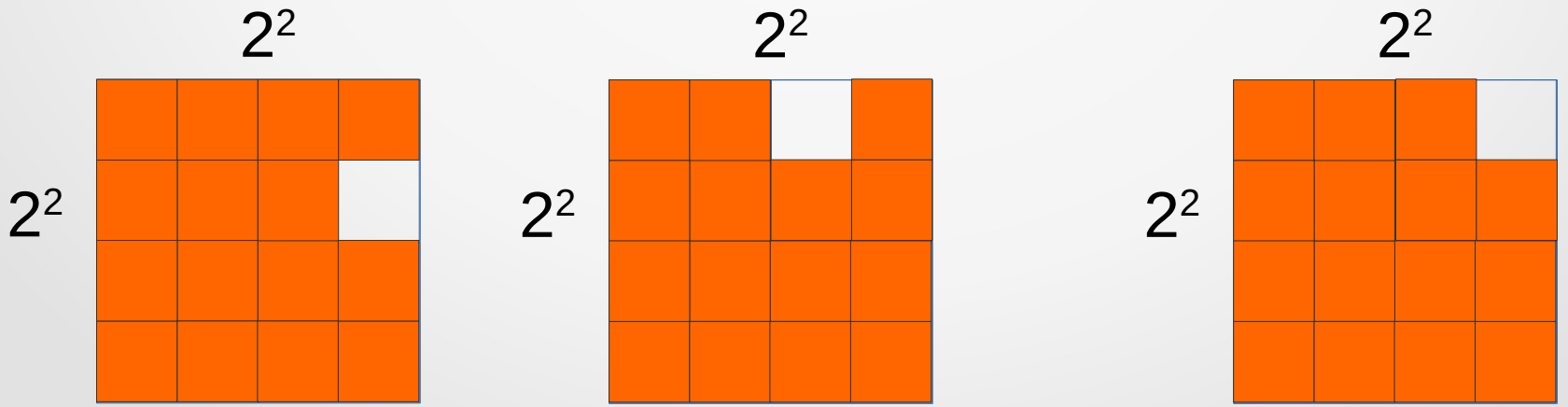
Mathematical Induction (continues)

Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."







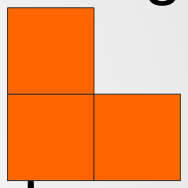
Note that any square can be removed from the checkerboard, we still can tile it!

Mathematical Induction (continues)

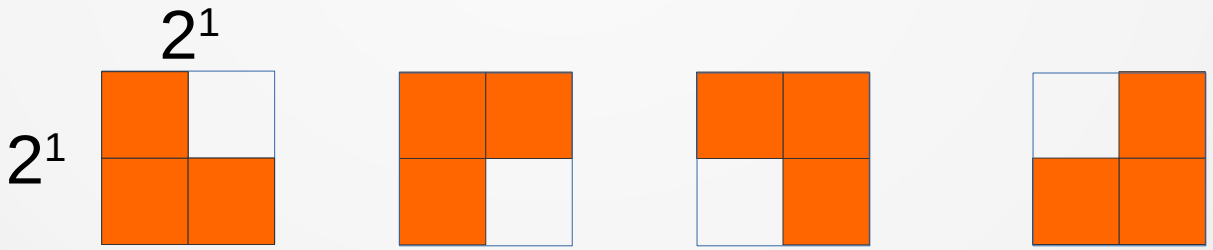
P(n)

Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."



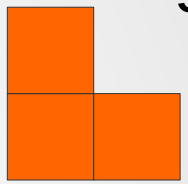
Basis step: n = 1, hence we have 2×2 checkerboard



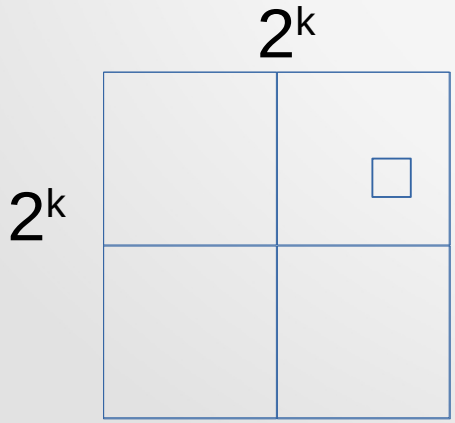
Mathematical Induction (continues)

Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."



Inductive step: assume that for any arbitrary fixed k, every $2^k \times 2^k$ checkerboard with one square removed can be tiled using right triominoes. (IH)

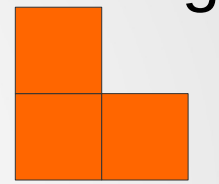


We need to show that in this case a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed can be tiled using right triominoes as well.

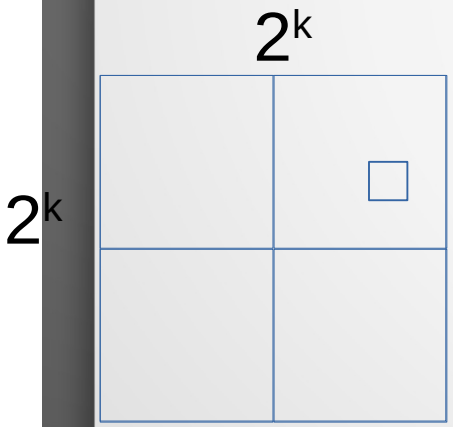
Mathematical Induction (continues)

Example:

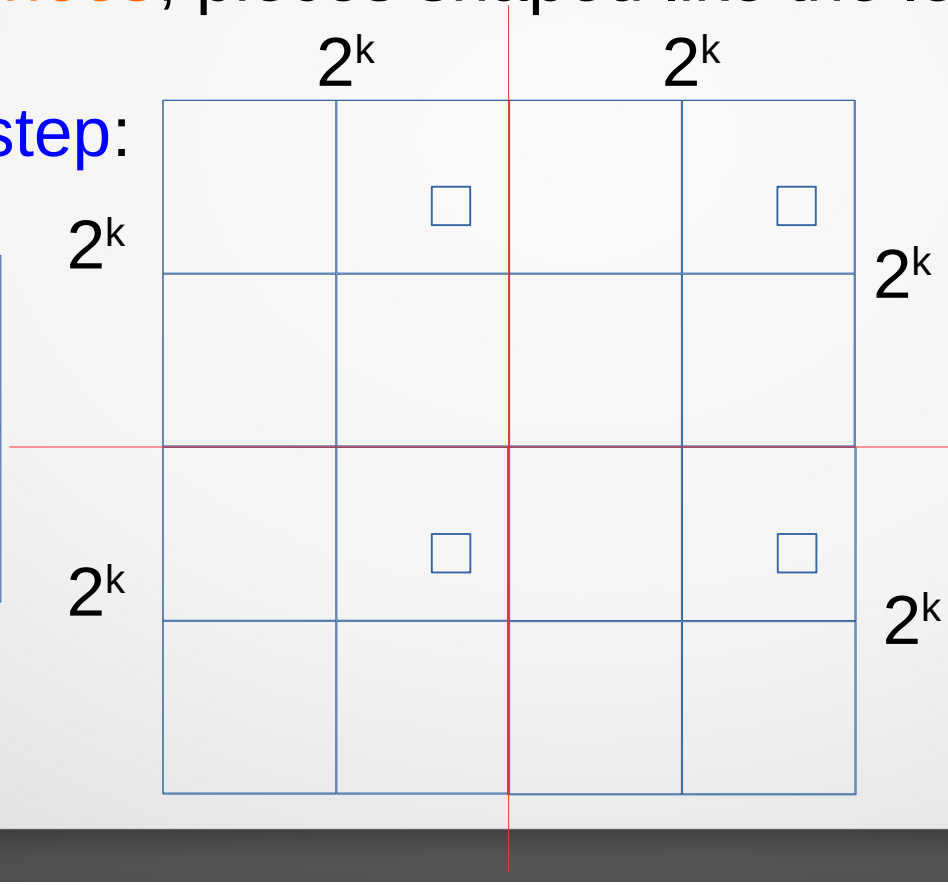
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right trominoes*, pieces shaped like the letter "L."



Inductive step:



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

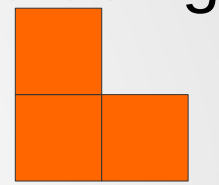


Cut the $2^{k+1} \times 2^{k+1}$ checkerboard into four $2^k \times 2^k$ checkerboards. For each of them IH works.

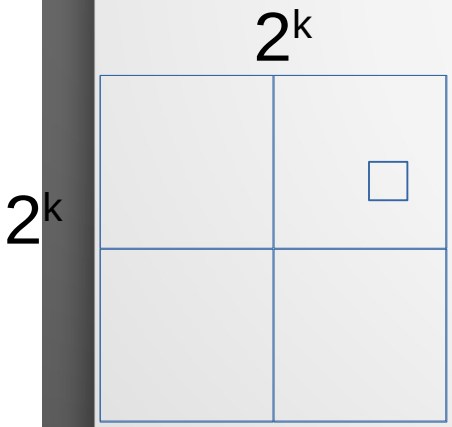
Mathematical Induction (continues)

Example:

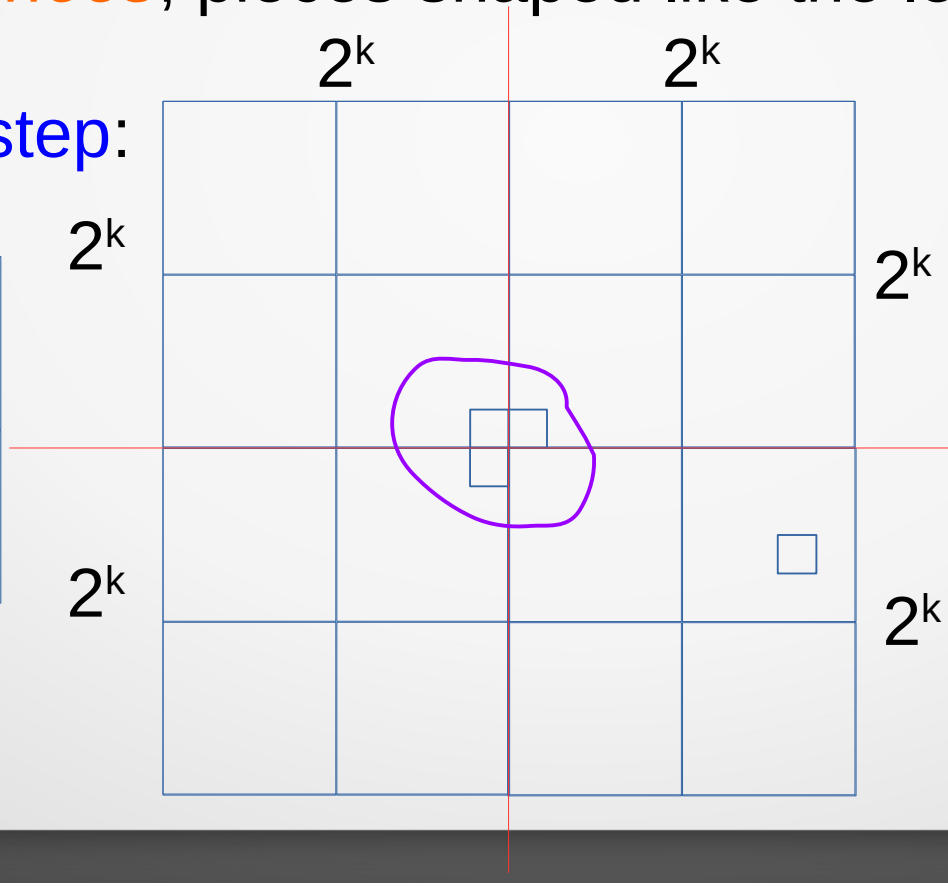
Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."



Inductive step:



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

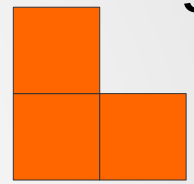


Let's remove the "center" square of each of any three $2^k \times 2^k$ checkerboards – it will be tiled/ covered by the right triominoe.

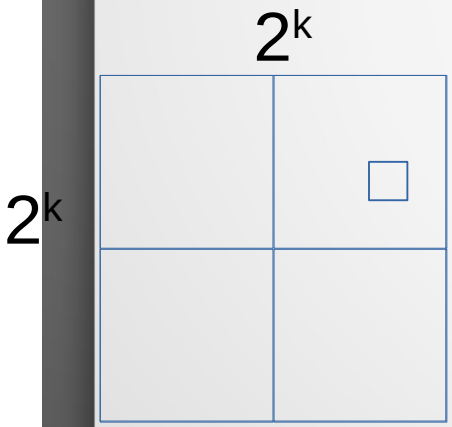
Mathematical Induction (continues)

Example:

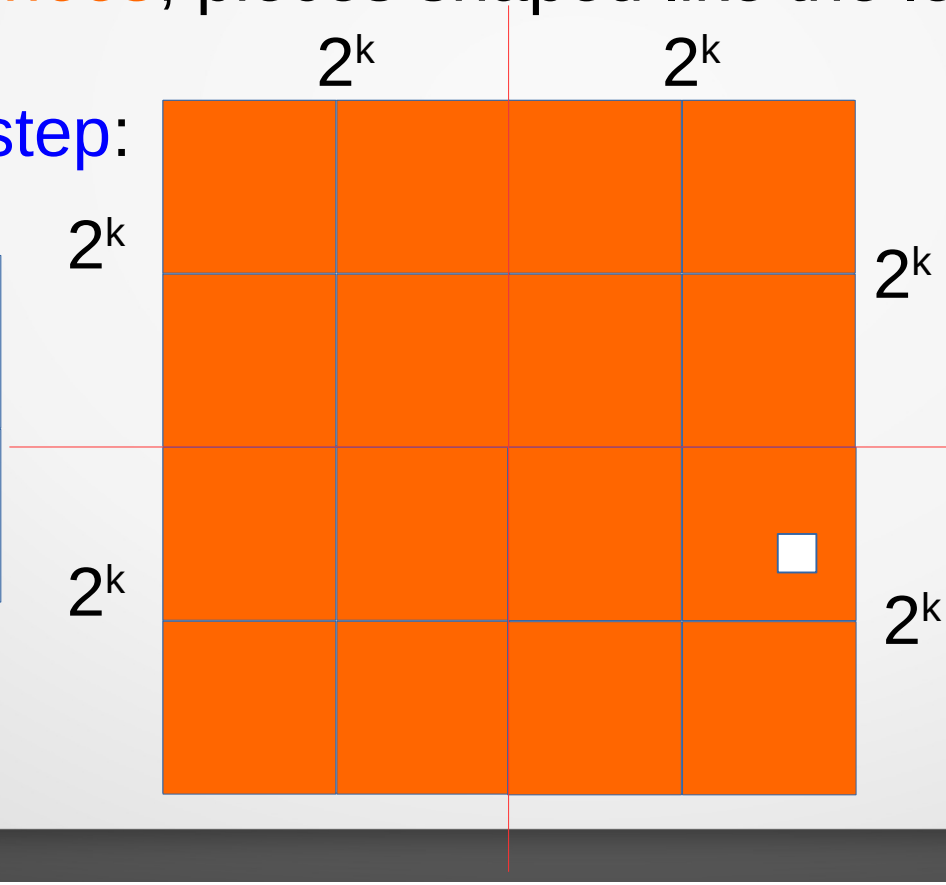
Let n be a positive integer. Show that every $2^n \times 2^n$, $n > 0$, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."



Inductive step:



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

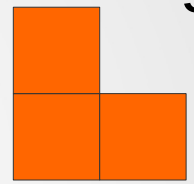


Let's remove the "center" square of each of any three $2^k \times 2^k$ checkerboards – it will be tiled/ covered by the right triominoe.

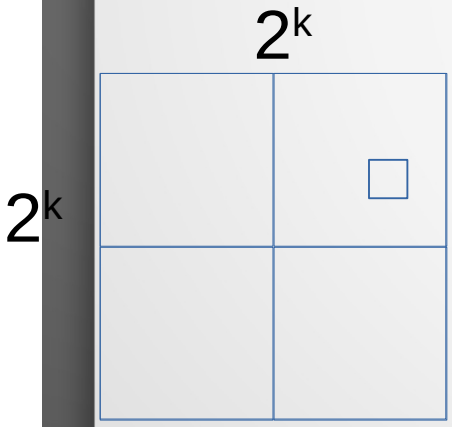
Mathematical Induction (continues)

Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."



Inductive step:



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

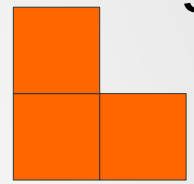
Let's remove the "center" square of each of any three $2^k \times 2^k$ checkerboards – it will be tiled/ covered by the right triominoe.

This completes the inductive step.

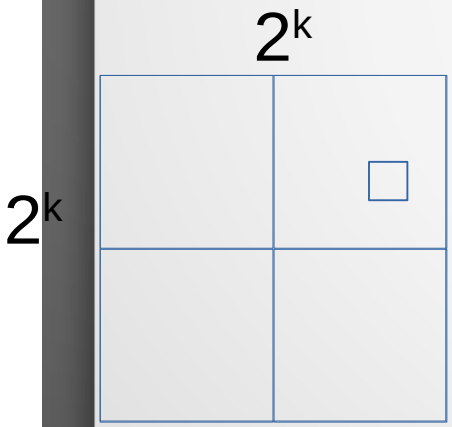
Mathematical Induction (continues)

Example:

Let n be a positive integer. Show that every $2^n \times 2^n$, n > 0, checkerboard with one square removed can be tiled using *right triominoes*, pieces shaped like the letter "L."



Inductive step:



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

Let's remove the "center" square of each of any three $2^k \times 2^k$ checkerboards – it will be tiled/ covered by the right triominoe.

This completes the inductive step.

By mathematical induction we proved P(n) for any positive n.

Mathematical Induction (continues)

Mistakes in math. induction proofs:

- can be hidden in the basis step
- can be in the inductive step

Mathematical Induction (continues)

Example:
What is wrong in the proof of the *"Theorem":* for every $n \in \mathbf{Z}^+$, $\sum_{i=1}^{n} i = \frac{\left(n+\frac{1}{2}\right)^2}{2}$?

Basis step: the formula is true for n = 1

Ind. step: assume for any arb. fixed $k \in \mathbf{Z}^+$, $\sum_{i=1}^{k} i = \frac{\left(k+\frac{1}{2}\right)^2}{2}$

Then $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{\left(k+\frac{1}{2}\right)^2}{2} + (k+1) = \frac{k^2+k+\frac{1}{4}}{2} + (k+1) = \ldots$

by IH

$$\ldots = \frac{k^2+k+\frac{1}{4}}{2} + \frac{2(k+1)}{2} = \frac{k^2+k+\frac{1}{4}+2k+2}{2} = \frac{k^2+3k+\frac{9}{4}}{2} = \ldots$$

$$\ldots = \frac{\left(k+\frac{3}{2}\right)^2}{2} = \frac{\left((k+1)+\frac{1}{2}\right)^2}{2}$$

As we can see, P(k+1) is also true. This completes the inductive step, and the proof. qed

Mathematical Induction (continues)

Example:
What is wrong in the proof of the *"Theorem":* for every n ∈ **Z**⁺, $\sum_{i=1}^{n} i = \frac{\left(n+\frac{1}{2}\right)^2}{2}$

Basis step: the formula is true for n = 1

false

$1! = \frac{\left(1+\frac{1}{2}\right)^2}{2} = \frac{9}{8}$

Ind. step: assume for any arb. fixed k ∈ **Z**⁺,

Then $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{\left(k+\frac{1}{2}\right)^2}{2} + (k+1) = \frac{k^2+k+\frac{1}{4}}{2} + (k+1) = \ldots$

by IH

$$\ldots = \frac{k^2+k+\frac{1}{4}}{2} + \frac{2(k+1)}{2} = \frac{k^2+k+\frac{1}{4}+2k+2}{2} = \frac{k^2+3k+\frac{9}{4}}{2} = \ldots$$

$$\ldots = \frac{\left(k+\frac{3}{2}\right)^2}{2} = \frac{\left((k+1)+\frac{1}{2}\right)^2}{2}$$

As we can see, P(k+1) is also true. This completes the inductive step, and the proof. qed

Mathematical Induction (continues)

Example:
What is wrong in the proof of the *"Theorem":* for every $n \in \mathbf{Z}^+$, $\sum_{i=1}^{n} i = \frac{\left(n+\frac{1}{2}\right)^2}{2}$

Basis step: the formula is true for n = 1

false

$$1! = \frac{\left(1+\frac{1}{2}\right)^2}{2} = \frac{9}{8}$$

Ind. step: assume for any arb. fixed $k \in \mathbf{Z}^+$, $\sum_{i=1}^{k} i = \frac{\left(k+\frac{1}{2}\right)^2}{2}$

Then $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{\left(k+\frac{1}{2}\right)^2}{2} + (k+1) = \frac{k^2+k+\frac{1}{4}}{2} + (k+1) = \ldots$

by IH

$$\ldots = \frac{k^2+k+\frac{1}{4}}{2} + \frac{2(k+1)}{2} = \frac{k^2+k+\frac{1}{4}+2k+2}{2} = \frac{k^2+3k+\frac{9}{4}}{2} = \ldots$$

$$\ldots = \frac{\left(k+\frac{3}{2}\right)^2}{2} = \frac{\left((k+1)+\frac{1}{2}\right)^2}{2}$$

As we can see, P(k+1) is also true. This completes the inductive step, and the proof. qed

Strong Induction and well-ordering

Strong Induction and well-ordering

Strong Induction and well-ordering

Why do we need strong induction?

The Fibonacci sequence is defined by initial values $f_0 = 0$, $f_1 = 1$ and the recurrence relation for $n \geq 2$:

$$f_n = f_{n-1} + f_{n-2}$$

There is an upper bound on the Fibonacci numbers:
$f_n \leq 2^n$, for all $n \geq 0$.

Strong Induction and well-ordering

Why do we need strong induction?

The Fibonacci sequence is defined by initial values $f_0 = 0$, $f_1 = 1$ and the recurrence relation for $n \geq 2$:

$$f_n = f_{n-1} + f_{n-2}$$

There is an upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Let's try to prove it using math. Induction:

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Strong Induction and well-ordering

Why do we need strong induction?

The Fibonacci sequence is defined by initial values $f_0 = 0$, $f_1 = 1$ and the recurrence relation for $n \geq 2$:

$$f_n = f_{n-1} + f_{n-2}$$

There is an upper bound on the Fibonacci numbers:

$f_n \leq 2^n$, for all $n \geq 0$.

Inductive step:

assume for any arbitrary fixed $k \geq 0$, P(k) is true. IH

P(k+1): $f_{k+1} = f_k + f_{k-1}$

Strong Induction and well-ordering

Why do we need strong induction?

The Fibonacci sequence is defined by initial values $f_0 = 0$, $f_1 = 1$ and the recurrence relation for $n \geq 2$:

$$f_n = f_{n-1} + f_{n-2}$$

There is an upper bound on the Fibonacci numbers:

$f_n \leq 2^n$, for all $n \geq 0$.

Inductive step:

assume for any arbitrary fixed $k \geq 0$, P(k) is true. IH

P(k+1): $f_{k+1} = f_k + f_{k-1} \leq 2^k + f_{k-1}$, now what to do with f_{k-1}?

(by IH)

Strong Induction and well-ordering

Why do we need strong induction?

The Fibonacci sequence is defined by initial values $f_0 = 0$, $f_1 = 1$ and the recurrence relation for $n \geq 2$:

$$f_n = f_{n-1} + f_{n-2}$$

There is an upper bound on the Fibonacci numbers:
$f_n \leq 2^n$, for all $n \geq 0$.

Inductive step:
assume for any arbitrary fixed $k \geq 0$, P(k) is true. IH
P(k+1): $f_{k+1} = f_k + f_{k-1} \leq 2^k + f_{k-1}$, now what to do with f_{k-1}?
(by IH)
The inductive hypothesis for standard induction only provides the bound on f_k.

Strong Induction and well-ordering

Why do we need strong induction?

The Fibonacci sequence is defined by initial values $f_0 = 0$, $f_1 = 1$ and the recurrence relation for $n \geq 2$:

$$f_n = f_{n-1} + f_{n-2}$$

There is an upper bound on the Fibonacci numbers:
$f_n \leq 2^n$, for all $n \geq 0$.

Inductive step:
assume for any arbitrary fixed $k \geq 0$, P(k) is true. IH
P(k+1): $f_{k+1} = f_k + f_{k-1} \leq 2^k + f_{k-1}$, now what to do with f_{k-1}?
(by IH)
The inductive hypothesis for standard induction only provides the bound on f_k. We cannot finish the proof!

Strong Induction and well-ordering

The principle of strong induction assumes that the fact to be proven holds for *all values less than or equal to* k and proves that the fact holds for k+1.

The standard form of induction only assumes that the fact *holds for* k *in proving that it holds for* k+1.

For the Fibonacci numbers example we can do:

Base case: P(0) and P(1) are true.

Inductive step: we need to show that for every $k \geq 1$,

$(P(0) \wedge P(1) \wedge .... \wedge P(k)) \rightarrow P(k + 1)$.

Strong Induction and well-ordering

Strong induction:

To prove $P(n)$ is true for all integers $n \geq b$, where $P(n)$ is a propositional function, we complete two steps:

Basis step(s): verify $P(b)$ is true ($P(b),\ldots, P(b+m)$ is true)

Inductive step: show that for every $k \geq b$,

$(P(b) \wedge P(b+1) \wedge .... \wedge P(k)) \rightarrow P(k+1)$ is true

i.e. we assume that for every $k \geq b$,
$P(b) \wedge P(b+1) \wedge .... \wedge P(k)$ is true and show that in this case $P(k+1)$ is also true.

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH
$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

$f_{k+1} = f_k + f_{k-1}$

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

$f_{k+1} = f_k + f_{k-1} \leq 2^k + 2^{k-1} =$

by IH twice

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

$f_{k+1} = f_k + f_{k-1} \leq 2^k + 2^{k-1} = 2^{k-1}(2+1) = 3 \cdot 2^{k-1}$

by IH twice

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

$f_{k+1} = f_k + f_{k-1} \leq 2^k + 2^{k-1} = 2^{k-1}(2+1) = 3 \cdot 2^{k-1} \leq 4 \cdot 2^{k-1} = 2^{k+1}$

by IH twice

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

$f_{k+1} = f_k + f_{k-1} \leq 2^k + 2^{k-1} = 2^{k-1}(2+1) = 3 \cdot 2^{k-1} \leq 4 \cdot 2^{k-1} = 2^{k+1}$

by IH twice

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, i.e.

$$\forall j (j \in Z \wedge 0 \leq j \leq k) P(j)$$

Let's show that is this case, P(k+1) is also true:

$f_{k+1} = f_k + f_{k-1} \leq 2^k + 2^{k-1} = 2^{k-1}(2+1) = 3 \cdot 2^{k-1} \leq 4 \cdot 2^{k-1} = 2^{k+1}$

by IH twice

We showed that P(k+1) is also true

This completes the inductive step.

Strong Induction and well-ordering

Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$, for $n \geq 2$

Example: Let's prove the upper bound on the Fibonacci numbers: $f_n \leq 2^n$, for all $n \geq 0$.

Basis step: n = 0, $f_0 = 0 \leq 2^0 = 1$

n = 1 $f_1 = 1 \leq 2^1 = 2$

Inductive step: assume for any arbitrary $k \geq 0$, IH

$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true.

We showed that P(k+1) is also true

By strong induction we proved that $f_n \leq 2^n$, for all $n \geq 0$.

q.e.d.

Strong Induction and well-ordering

Multiple base cases:

As you noticed, we had two base cases in the basis step.

Basis step is not limited to one base case.

To some extent, determining how many base cases are required in a strong induction proof requires some trial and error, but some common sense reasoning can be applied

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):

Cans of juice come in packs of 3 or 4. For any $n \geq 6$ it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):

Cans of juice come in packs of 3 or 4. For any n ≥ 6 it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Basis step:

P(6) is true

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):

Cans of juice come in packs of 3 or 4. For any n ≥ 6 it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Basis step:

P(6) is true

P(7) is true

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):

Cans of juice come in packs of 3 or 4. For any n ≥ 6 it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Basis step:

P(6) is true

P(7) is true

P(8) is true

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):

Cans of juice come in packs of 3 or 4. For any n ≥ 6 it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Basis step:

P(6) is true

P(7) is true

P(8) is true

We checked all variations of two packs of juice packs

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):
Cans of juice come in packs of 3 or 4. For any $n \geq 6$ it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Inductive step: assume that for any $k \geq 8$,

$P(6) \wedge \ldots \wedge P(k)$ is true.

Let's show that in this case $P(k+1)$ is true:

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):
Cans of juice come in packs of 3 or 4. For any $n \geq 6$ it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Inductive step: assume that for any $k \geq 8$,

$P(6) \wedge \ldots \wedge P(k)$ is true.

Let's show that in this case $P(k+1)$ is true:
Since $P(k-2)$ is true, i.e. $k-2$ cans can be presented as a combination of 3-packs and 4-packs, then by adding one 3-pack it will be getting exactly $k+1$ cans in total.
$(k-2) + 3 = k+1$

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):
Cans of juice come in packs of 3 or 4. For any $n \geq 6$ it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Inductive step: assume that for any $k \geq 8$,

$P(6) \wedge \ldots \wedge P(k)$ is true.

Let's show that in this case P(k+1) is true:
Since P(k-2) is true, i.e. k-2 cans can be presented as a combination of 3-packs and 4-packs, then by adding one 3-pack it will be getting exactly k+1 cans in total.
(k-2) + 3 = k+1
Hence P(k+1) is also true.
This completes the inductive step.

Strong Induction and well-ordering

Example (multiple base cases) (from ZyBooks):
Cans of juice come in packs of 3 or 4. For any $n \geq 6$ it is possible to buy *n* cans of juice by purchasing a combination of *3-packs* or *4-packs* only.

Inductive step: assume that for any $k \geq 8$,

$P(6) \wedge \ldots \wedge P(k)$ is true.

Let's show that in this case $P(k+1)$ is true:
Since $P(k-2)$ is true, i.e. $k-2$ cans can be presented as a combination of 3-packs and 4-packs, then by adding one 3-pack it will be getting exactly $k+1$ cans in total.
$(k-2) + 3 = k+1$
Hence $P(k+1)$ is also true.
This completes the inductive step.
By strong induction the statement above is true.

q.e.d.

Strong Induction and well-ordering

Well-ordering:

The **well-ordering principle** says that any non-empty subset of the non-negative integers has a smallest element.

We used it before to show that mathematical induction is valid.

It is possible to use this principle directly in proofs.

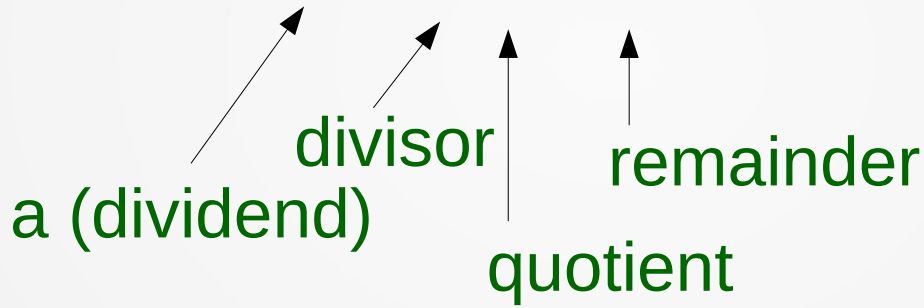
Furthermore, the well-ordering principle, the mathematical induction and strong induction are all equivalent.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

$$17 = 5*3 + 2$$



Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Let S be the set of non-negative integers of the form $a – dq$, where $q \in Z$.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Let S be the set of non-negative integers of the form $a - dq$, where $q \in Z$.

$|S| \neq 0$ because $-dq$ can be made as large as desired (with q as negative integer and large absolute value)

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq + r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Let S be the set of non-negative integers of the form $a - dq$, where $q \in Z$.

$|S| \neq 0$ because $-dq$ can be made as large as desired (with q as negative integer and large absolute value)

By the well-ordering principle, S has a smallest element $r = a - dq_0$.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Let S be the set of non-negative integers of the form $a - dq$, where $q \in Z$.

$|S| \neq 0$ because $-dq$ can be made as large as desired (with q as negative integer and large absolute value)

By the well-ordering principle, S has a smallest element $r = a - dq_0$.

$r \geq 0$ (by the way the set S is built, of non-negative integers)

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Let S be the set of non-negative integers of the form $a - dq$, where $q \in Z$.

$|S| \neq 0$ because $-dq$ can be made as large as desired (with q as negative integer and large absolute value)

By the well-ordering principle, S has a smallest element $r = a - dq_0$.

$r \geq 0$ (by the way the set S is built, of non-negative integers)

$r < d$ (otherwise there would be a smaller non-negative element in S, namely, $a - d(q_0+1)$; but r is a smallest!).

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

Let S be the set of non-negative integers of the form $a - dq$, where $q \in Z$.

$|S| \neq 0$ because $-dq$ can be made as large as desired (with q as negative integer and large absolute value)

By the well-ordering principle, S has a smallest element $r = a - dq_0$.

$r \geq 0$ (by the way the set S is built, of non-negative integers)

$r < d$ (otherwise there would be a smaller non-negative element in S, namely, $a - d(q_0+1)$; but r is a smallest!).

Therefore, $0 \leq r < d$

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq + r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r - r_1 =$

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r - r_1 = (a - dq_0) - (a - dq_1)$

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r-r_1 = (a-dq_0) - (a-dq_1) = d(q_1 - q_0)$ i.e. d divides $r-r_1$.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r-r_1 = (a-dq_0) - (a-dq_1) = d(q_1 - q_0)$ i.e. d divides $r-r_1$.

In addition, $-d < r-r_1 < d$.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r-r_1 = (a-dq_0) - (a-dq_1) = d(q_1 - q_0)$ i.e. d divides $r-r_1$.

In addition, $-d < r-r_1 < d$.

Therefore, $r = r_1$,

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r-r_1 = (a-dq_0) - (a-dq_1) = d(q_1 - q_0)$ i.e. d divides $r-r_1$.

In addition, $-d < r-r_1 < d$.

Therefore, $r = r_1$, and hence $r-r_1 = d(q_1 - q_0)$, q_0 must be equal to q_1.

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, r is the smallest element of S, and $r = a - dq_0$, $0 \leq r < d$

Now we need to proof that q_0 and r are unique!

Assume that $\exists\ q_1 \in Z\ (q_1 \neq q_0)$ and $\exists!\ r_1 \in Z\ (0 \leq r_1 < d)$ such that $r_1 = a - dq_1$

Then $r-r_1 = (a-dq_0) - (a-dq_1) = d(q_1 - q_0)$ i.e. d divides $r-r_1$.

In addition, $-d < r-r_1 < d$.

Therefore, $r = r_1$, and hence $r-r_1 = d(q_1 - q_0)$, q_0 must be equal to q_1. We got a contradiction!

Strong Induction and well-ordering

Example: use the well-ordering principle to prove the division algorithm.

If $a \in Z$, and $d \in Z^+$, then $\exists!\ q \in Z$ and $\exists!\ r \in Z\ (0 \leq r < d)$ such that $a = dq+r$.

Proof: Assume $a \in Z$, and $d \in Z^+$.

… *skipped*

So, we showed that r is the smallest element of S,

$r = a - dq_0$, $0 \leq r < d$

We proved that q_0 and r are unique!

This completes the proof of the division algorithm.

q.e.d.