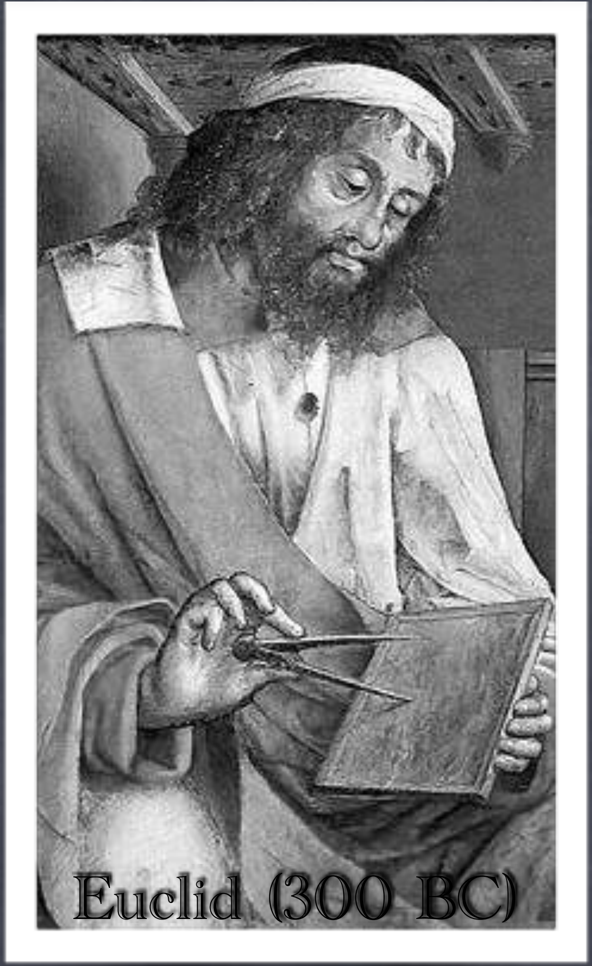


Mathematical Induction

Proof by Programming

The Fable of the Proof Deity!

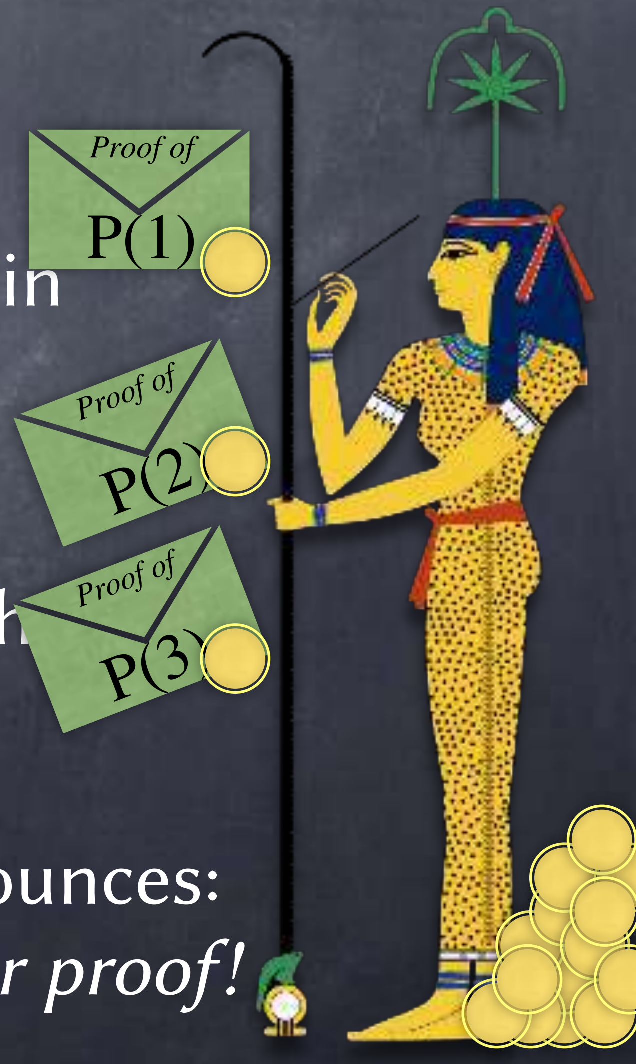
(OK, I made it up :))

- You have been imprisoned in a dungeon. The guard gives you a predicate P and tells you that the next day you will be asked to produce the proof for P(n) for some $n \in \mathbb{Z}^+$. If you can, you'll be let free!
- You pray to Seshat, the deity of wisdom.
- You tell her what P is. She thinks for a bit and says, indeed, $\forall n \in \mathbb{Z}^+\ P(n)$. But she wouldn't give you a proof.
- You plead with her. She relents a bit and tells you: *If you give me the proof for* P(k) *for a* k, *and give me a gold coin, I will give you the proof for* P(k+1).
- You are hopeful, because you have worked out the proof for P(1) (and you're very rich) ...

The Fable of the Proof Deity!

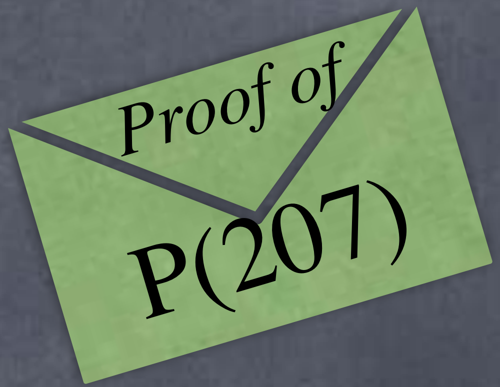
(OK, I made it up :))

- The next morning, the guard asks you for a proof of P(207)
- You invoke Seshat, and submit to her an envelope with your proof for P(1) and a gold coin
  - She returns an envelope with the proof for P(2)
  - You give that envelope back to her, with another gold coin
  - She gives you an envelope with the proof for P(3)
  - ... and after spending 206 coins, you get an envelope with the proof of P(207), which you submit to the guard
- After a while the guard returns with the envelope and announces: *Congratulations! The court mathematicians have verified your proof! You are free to leave! (Yay!)*



The Fable of the Proof Deity!

(OK, I made it up :))



- After getting out of the dungeon, you have the envelope with the proof of P(207) with you. You open it.
  - The first page is the proof of P(1) you gave.
  - The second page has a beautiful proof for a Lemma: $\forall k \in \mathbb{Z}^+ \ \ P(k) \longrightarrow P(k+1)$.
  - The third page has:

> Since P(1) and, by Lemma, $P(1) \longrightarrow P(2)$, we have P(2).
> Since P(2) and, by Lemma, $P(2) \longrightarrow P(3)$, we have P(3).
> ⋮
> Since P(206) and, by Lemma, $P(206) \longrightarrow P(207)$, we have P(207).
> QED

- You feel a bit silly for having paid 206 gold coins. But at least, you learned something...

Proof by Induction

"Proof by programming": This is a program that takes n as input and produces a proof for P(n)

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:

An axiom in our system for $\mathbb{Z}^+$

- First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$

Weak

The Principle of Mathematical Induction

For any n, we can run this procedure to generate a proof for P(n), and hence for any n, P(n) holds.

$P(1)$	$P(1) \rightarrow P(2)$
$P(2)$	$P(2) \rightarrow P(3)$
$P(3)$	$P(3) \rightarrow P(4)$
$P(4)$	$P(4) \rightarrow P(5)$
$P(5)$	$P(5) \rightarrow P(6)$
$\vdots$	$\vdots$

$\forall n \in \mathbb{Z}^+ \; P(n)$

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $\boxed{P(1)}$ and $\boxed{\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)}$
  - Then by (weak) <u>mathematical induction</u>, $\boxed{\forall n \in \mathbb{Z}^+ \; P(n)}$

Base case

Induction step

Induction hypothesis

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \;\; P(n)$:
  - First, we prove $\boxed{P(1)}$ and $\boxed{\forall k \in \mathbb{Z}^+ \;\; P(k) \rightarrow P(k+1)}$
  - Then by (weak) mathematical induction, $\boxed{\forall n \in \mathbb{Z}^+ \;\; P(n)}$

Base case

Induction step

Induction hypothesis

- Conventional phrasing while proving a claim written using a variable n
  - We prove the claim by induction on n.
  - Base case: First we prove that the claim holds for n = 1. ... P(1)
  - We shall prove that for any k≥1, if the claim holds for n=k then it holds for n=k+1. P(k+1) P(k)
  - Fix a k≥1. Suppose the claim holds for n=k. ...

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$
  - Then by (weak) mathematical induction, $\forall n \in \mathbb{Z}^+ \; P(n)$

Base case

Induction step

Induction hypothesis

- Base case may cover several values of the induction variable
  - e.g., Base cases: $P(1)$, $P(2)$, $P(3)$, and induction step: For all $k \geq 3$, $P(k) \rightarrow P(k+1)$
- Claim may use a different range for n
  - e.g., to prove $\forall n \geq 0 \; P(n)$ we may use Base case: $P(0)$, and induction step: For all $k \geq 0$, we prove that $P(k) \rightarrow P(k+1)$

$p|q$: p divides q
i.e., $\exists r$ s.t. $q=pr$

Example

- $\forall n \in \mathbb{N}$, $3 \mid n^3 - n$
  - Base case: $n=0$. $3|0$.
  - Induction step: For all integers $k \geq 0$
    Induction hypothesis: Suppose true for $n=k$. i.e., $k^3-k = 3m$
    To prove: Then, true for $n=k+1$. i.e., $3 \mid (k+1)^3-(k+1)$
    - $(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1$
      $= (k^3 - k) + 3k^2 + 3k$
      $= 3m + 3k^2 + 3k$ ✔
- The non-inductive proof: $n^3-n = n(n^2-1) = (n-1)n(n+1)$.
  $3 \mid (n-1)n(n+1)$ since one of 3 consecutive integers is a multiple of 3

Proof by Induction

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - First, we prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; P(k) \rightarrow P(k+1)$
  - Then by (weak) mathematical induction, $\forall n \in \mathbb{Z}^+ \; P(n)$

In disguise

Well Ordering Principle

Every non-empty subset of $\mathbb{Z}^+$ has a minimum element.

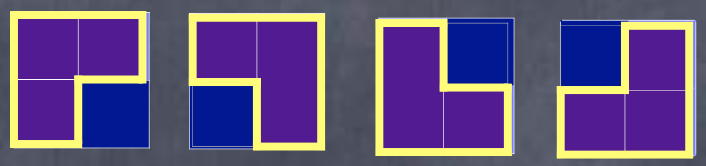
(Can be used instead of Principle of Mathematical Induction)

- To prove $\forall n \in \mathbb{Z}^+ \; P(n)$:
  - Prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \; \neg P(k+1) \rightarrow \neg P(k)$
  - For the sake of contradiction, suppose $\neg (\forall n \in \mathbb{Z}^+ \; P(n))$.
  - Let k' be the smallest $n \in \mathbb{Z}^+$ s.t. $\neg P(n)$. $k' \neq 1$ (since $P(1)$).
  - Let $k = k'-1$. Then, $k \in \mathbb{Z}^+$ and $\neg P(k+1)$. Then, $\neg P(k)$.
  - Contradicts the fact that k' is the smallest $n \in \mathbb{Z}^+$ s.t. $\neg P(n)$.

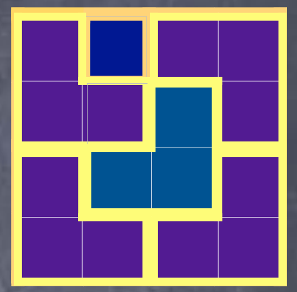
Tromino Tiling

- L-trominoes can be used to tile a "punctured" $2^n \times 2^n$ grid (punctured = one cell removed), for all positive integers n

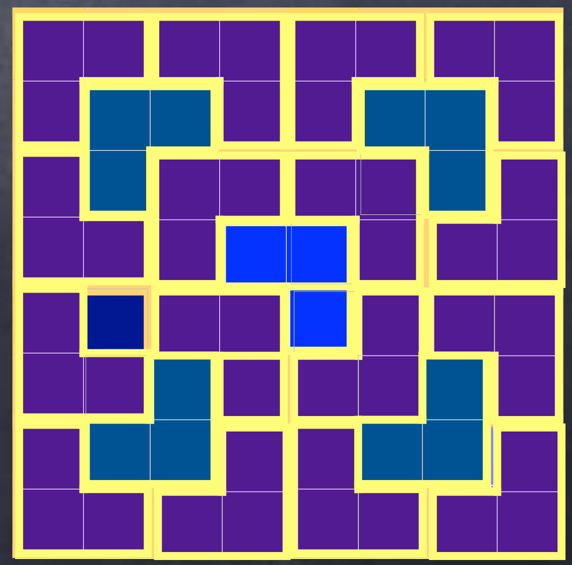
- Base case: n=1



- Inductive step: For all integers $k \geq 1$:
  - Hypothesis: suppose, true for n=k
  - To prove: then, true for n=k+1



  - Idea: can partition the $2^{k+1} \times 2^{k+1}$ punctured grid into four $2^k \times 2^k$ punctured grids, plus a tromino. Each of these can be tiled using trominoes (by inductive hypothesis).



- Actually gives a (recursive) algorithm for tiling

Structured Problems

- P(n) may refer to an object or structure of "size" n (e.g., a punctured grid of size $2^n \times 2^n$)
- To prove $P(k) \rightarrow P(k+1)$
  - Take the object of size k+1
  - Derive (one or more) objects of size k
  - Appeal to the induction hypothesis P(k), to draw conclusions about the smaller objects
  - Put them back together into the original object, and draw a conclusion about the original object, namely, P(k+1)

Common mistake:
Going in the opposite direction!
Not enough to reason about (k+1)-sized objects derived from k-sized objects

Strong Induction

Induction hypothesis: $\forall n {\leq} k\ P(n)$

- To prove $\forall n \in \mathbb{Z}^+\ P(n)$: we prove $\boxed{P(1)}$ (as before) and that

$$\boxed{\forall k \in \mathbb{Z}^+\ \ (P(1) \wedge P(2) \wedge \ldots \wedge P(k)) \rightarrow P(k+1)}$$

$P(1)$	$P(1) \rightarrow P(2)$
$P(2)$	$P(1) \wedge P(2) \rightarrow P(3)$
$P(3)$	$P(1) \wedge .. \wedge P(3) \rightarrow P(4)$
$P(4)$	$P(1) \wedge .. \wedge P(4) \rightarrow P(5)$
$P(5)$	$P(1) \wedge .. \wedge P(5) \rightarrow P(6)$
:	:

$$\boxed{\forall n \in \mathbb{Z}^+\ \ P(n)}$$

<u>Mathematical Induction</u>

The fact that for any n, we can run this procedure to generate a proof for P(n), and hence for any n, P(n) holds.

Same as weak induction for $\forall n\ Q(n)$, where $Q(n) \triangleq \forall m \in [1,n]\ \ P(m)$