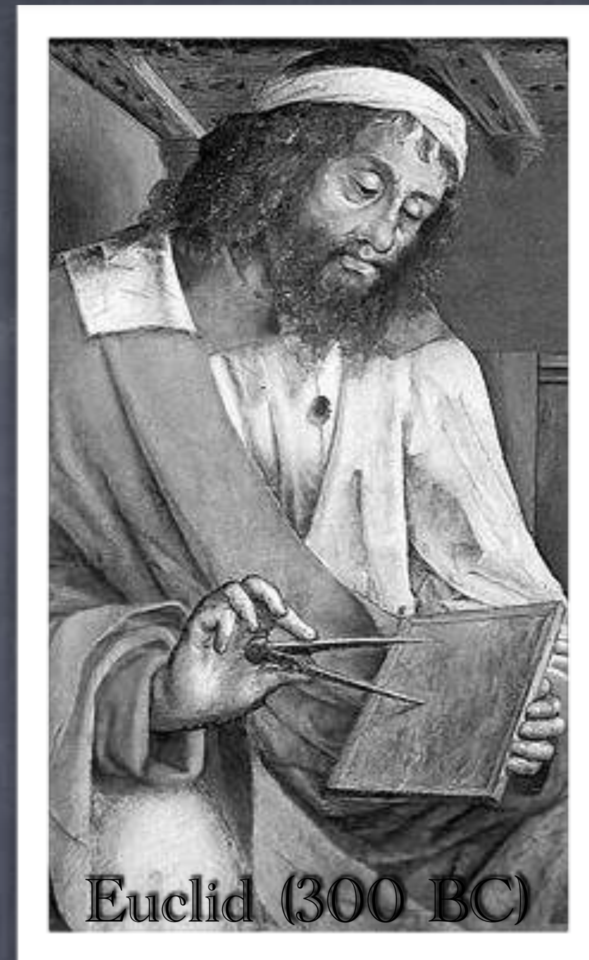


Proofs: Logic in Action

Using Logic

- Logic is used to deduce results in any (mathematically defined) system
  - Typically a human endeavour (but can be automated if the system is relatively simple)
- Proof is a means to convince others (and oneself) that a deduced result is correct
  - Verifying a proof is meant to be easy (automatable)
  - Coming up with a proof is typically a lot harder (not easy to fully automate, but sometimes computers can help)

What are we proving?

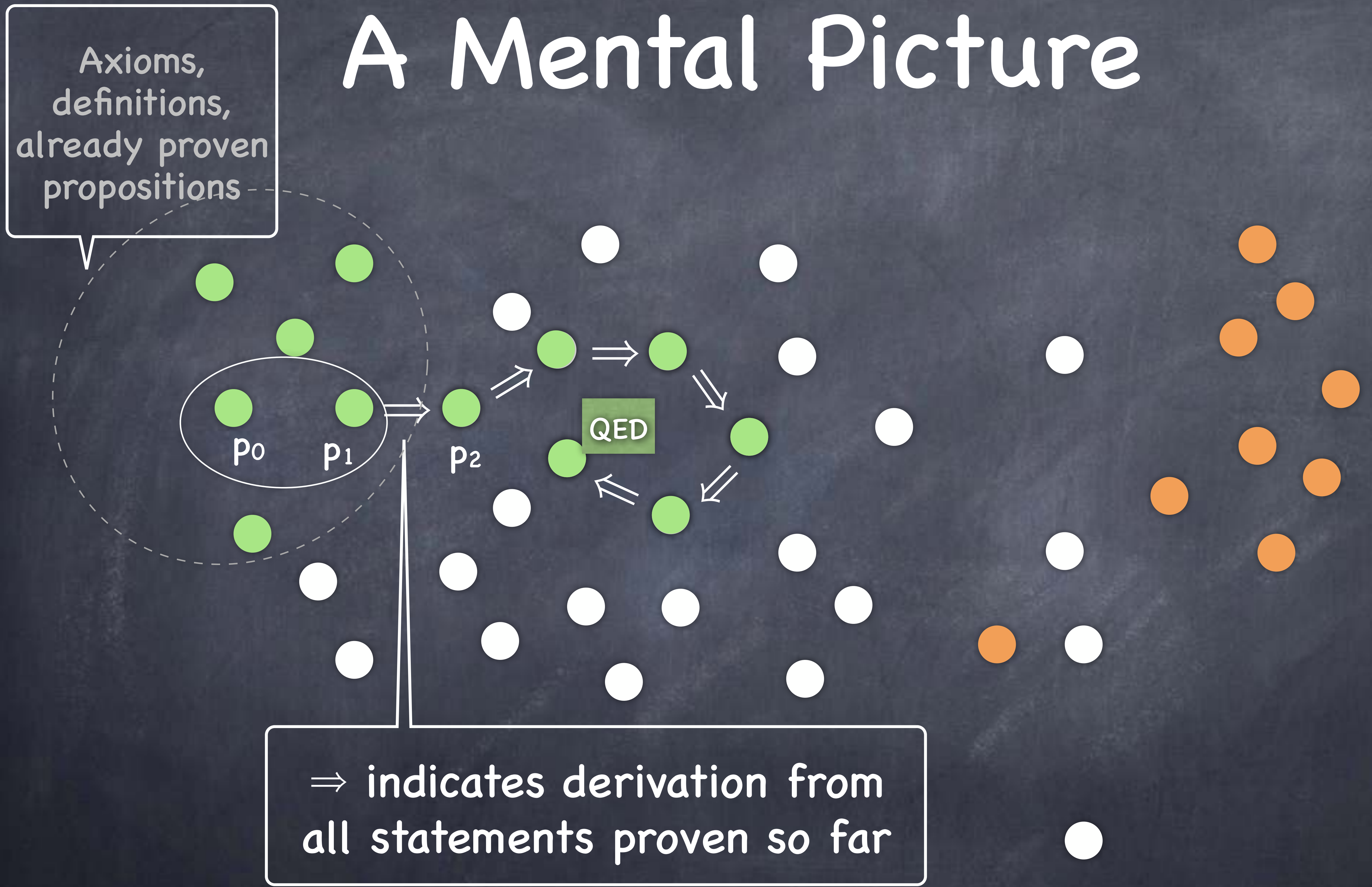
- We are proving propositions
  - Often called Theorems, Lemmas, Claims, …
- Propositions may employ various predicates already specified as Definitions
  - e.g. All positive even numbers are larger than 1
    - $\forall x \in \mathbb{Z}$ (Positive(x) $\wedge$ Even(x)) $\rightarrow$ Greater(x,1)
- These predicates are specific to the system (here arithmetic). The system will have its own "axioms" too (e.g., $\forall x\ x+0=x$)
  - For us, numbers (integers, rationals, reals) and other systems like sets, graphs, functions, …

Anatomy of a Proof

- Clearly state the proposition p to prove (esp'ly, if rephrased)
- Derive propositions $p_0, \ldots, p_n$ where for each k, either p_k is an axiom or an already proven proposition in the system, or $(p_0 \wedge p_1 \wedge \ldots \wedge p_{k-1}) \rightarrow p_k$ holds (i.e., is True)
  - Usually one or two propositions so far would imply the next

    [verify!] if $(p_i \wedge p_j) \rightarrow p_k$, then $(\ldots \wedge p_i \wedge \ldots \wedge p_j \ldots) \rightarrow p_k$
  - An explanation should make it easy to verify the implication (e.g., "By p_j and p_{k-1}, we obtain p_k")
- p_n should be the proposition to be proven
- May use "sub-routines" (lemmas)
  - e.g., Derive $p_0, \ldots, p_{k-1}$. Let p_k be a lemma proven separately. Say, $p_k \equiv p_{k-1} \rightarrow p$. Now, let p_{k+1} be p, as $(p_{k-1} \wedge p_k) \rightarrow p$ holds.

A Mental Picture



Example

- Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like +, -, *, /, exponentiation…)
  - We will not attempt to formally define this system!
- Definition: An integer x is said to be odd if there is an integer y s.t. x=2y+1

  "if" used by convention; actually means "iff"

  - $\forall x \in \mathbb{Z}\ Odd(x) \leftrightarrow \exists y \in \mathbb{Z}\ (x=2y+1)$
- Proposition: If x is an odd integer, so is x^2
  - $\forall x \in \mathbb{Z}\ \ Odd(x) \rightarrow Odd(x^2)$

Example

- Def: $\forall x \in \mathbb{Z}$ Odd(x) $\leftrightarrow$ $\exists y \in \mathbb{Z}$ $(x = 2y+1)$
- Proposition: $\forall x \in \mathbb{Z}$ Odd(x) $\rightarrow$ Odd(x^2)
- Proof: (should be written in more readable English)
  - Let x be an arbitrary element of $\mathbb{Z}$. Variable x introduced.
  - Suppose Odd(x). Then, we need to show Odd(x^2).
  - By def., $\exists y \in \mathbb{Z}$ $x=2y+1$. So let $x=2a+1$ where $a \in \mathbb{Z}$. Variable a.
  - Then, $x^2 = (2a+1)^2 = 4a^2 + 4a + 1$

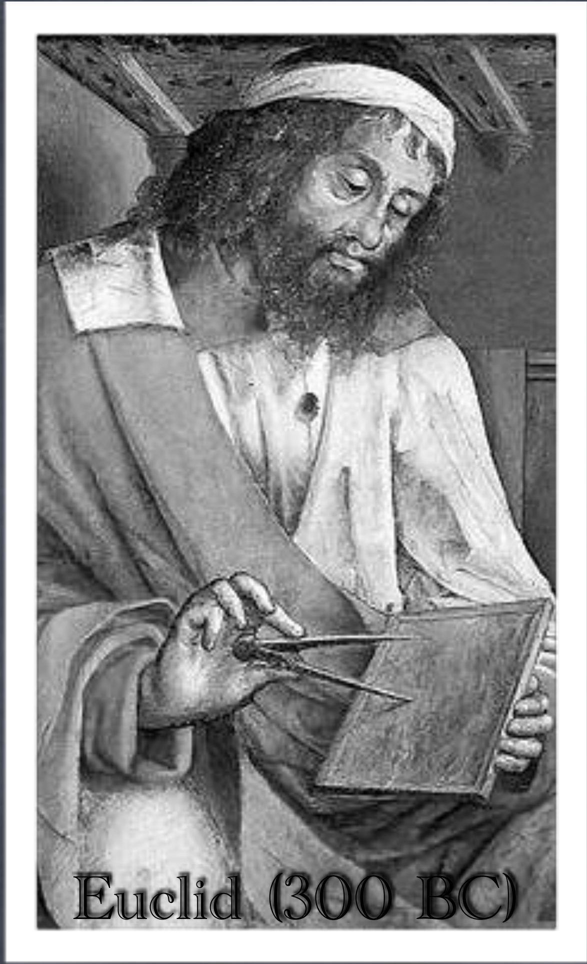
    $= 2(2a^2+2a) + 1.$ From arithmetic.
  - $\exists w \in \mathbb{Z}$ $(2a^2+2a)=w$. From arithmetic.
  - So let $2a^2+2a=b$, where $b \in \mathbb{Z}$ Variable b.
  - Hence, $x^2 = 2b+1$
  - Then, by definition, Odd(x^2).
  - Hence for every x, Odd(x) $\rightarrow$ Odd(x^2). QED.

Proving vs. Verifying

- Proofs should be easy to verify. All the cleverness goes into finding/writing the proof, not reading/verifying it!

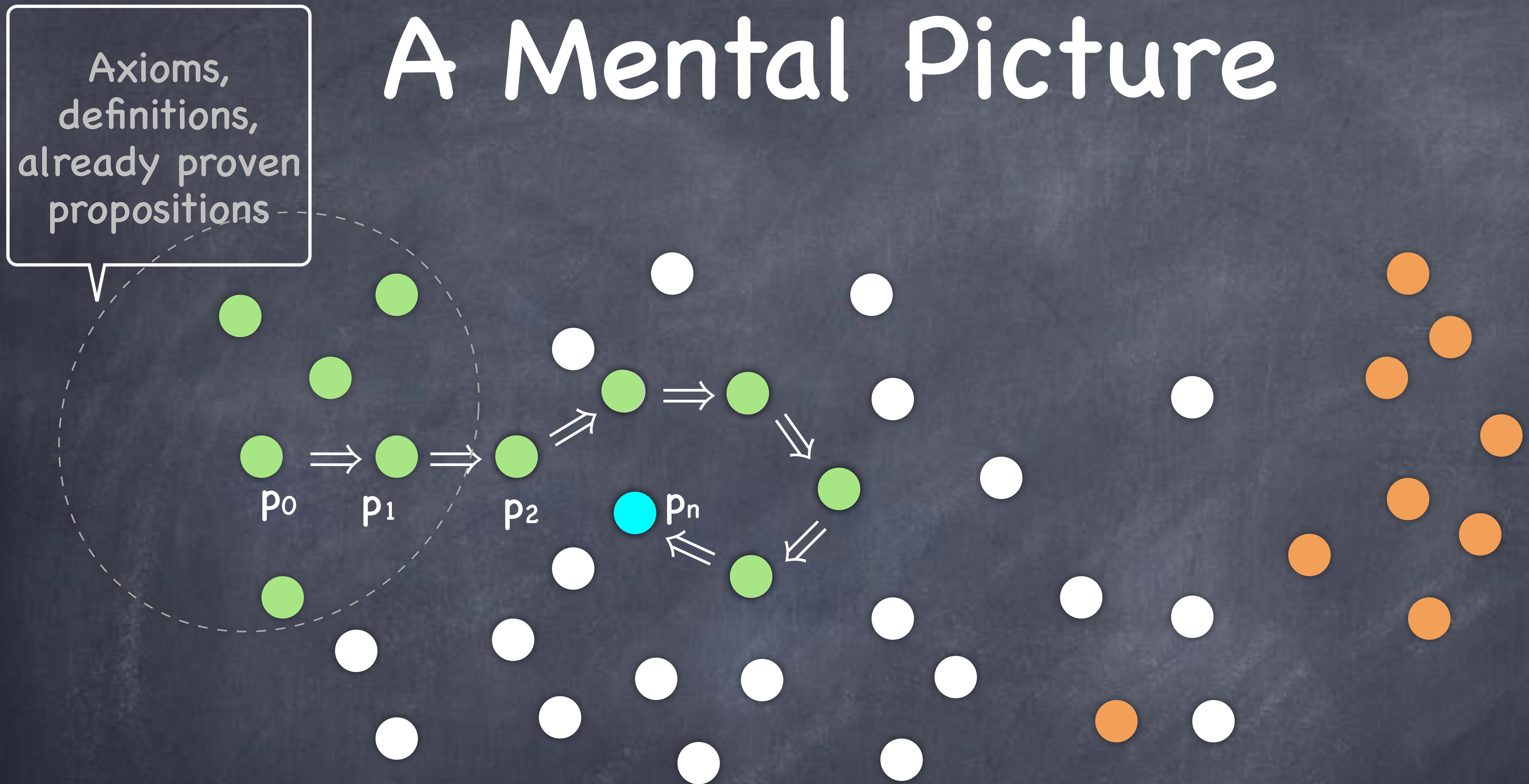
"**P** *vs.* **NP**" *(informally) :*
P = *class of problems for which finding a proof is computationally easy.*
NP = *class of problems for which verifying a proof is computationally easy.*
We believe that many problems in **NP** *are not in* **P**
(but we haven't been able to prove it yet!)

- Multiple approaches:
  - Direct deduction; Rewriting the proposition, e.g., as contrapositive; Proof by contradiction; Proof by giving a (counter)example, when applicable; Mathematical Induction.



Some Proof Templates

A Mental Picture



Template for $p \rightarrow q$

- To prove $p \rightarrow q$:
  - May set p_0 as p (even though we don't know if p is True), and proceed to prove q
    - Proof starts with "Suppose p."
  - Why is this a proof of $p \rightarrow q$?
    - If p is True, the above is a valid proof that q holds. And if q holds, $p \rightarrow q$ holds.
    - If p is False, the above proof is not valid. But we already have that $p \rightarrow q$ is vacuously true.
    - In either case $p \rightarrow q$ holds
  - Or, could rewrite the proof as $(p \rightarrow p_1) \Rightarrow (p \rightarrow p_2) \Rightarrow \ldots \Rightarrow (p \rightarrow q)$

Rephrasing

- Often it is helpful to first rewrite the proposition into an **equivalent proposition** and prove that.

  $p_{orig} \leftrightarrow p_{equiv}$

  $p_0 \Rightarrow p_1 \Rightarrow \dots \Rightarrow p_{equiv} \Rightarrow p_{orig}$

- Should clearly state this if you are doing this.
- An important example: **contrapositive**
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
    - Both equivalent to $\neg p \vee q$

Contrapositive

- $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- An example:

  Positive integers

  - Proposition: $\forall x,y \in \mathbb{Z}^+ \;\; x \cdot y > 25 \rightarrow (x \geq 6) \vee (y \geq 6)$
  - Enough to prove that: $\forall x,y \in \mathbb{Z}^+ \;\; (x < 6) \wedge (y < 6) \rightarrow x \cdot y \leq 25$
- Another example:
  - If function f is "hard" then crypto scheme S is "secure" $\equiv$ If crypto scheme S is not "secure," then function f is not "hard"
  - To prove the former, we can instead show how to transform any attack on S into an efficient algorithm for f

Rephrasing

- Often it is helpful to first rewrite the proposition into an equivalent proposition and prove that.

  $p_{orig} \leftrightarrow p_{equiv}$

  $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_{equiv} \Rightarrow p_{orig}$

- Should clearly state this if you are doing this.
- An important example: contrapositive
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Another instance: proof by contradiction
  - $p \equiv \neg p \rightarrow \text{False}$
  - So, to prove p, enough to show that $\neg p \rightarrow \text{False}$.

Contradiction

- To prove p, enough to show that $\neg p \to$ False.
- Recall: To prove $\neg p \to$ False, we can start by assuming $\neg p$
  - Can start the proof directly by saying "Suppose for the sake of contradiction, $\neg p$" (instead of saying we shall prove $\neg p \to$ False)
  - p_n is simply "False"
    - E.g., we may have $\neg p \Rightarrow \ldots \Rightarrow q \ldots \Rightarrow \neg q \Rightarrow$ False
      - "But that is a contradiction! Hence p holds."

Example

- Claim: There's a village barber who gives haircuts to exactly those in the village who don't cut their own hair
- Proposition: The claim is false
- Proposition, formally: $\neg(\exists B \forall x \ \ \neg\text{cut-hair}(x,x) \longleftrightarrow \text{cut-hair}(B,x))$
  - Suppose for the sake of contradiction, $\exists B \ \forall x \ \ \neg\text{cut-hair}(x,x) \longleftrightarrow \text{cut-hair}(B,x)$
  - $(\exists B \ \forall x \ \ \neg\text{cut-hair}(x,x) \longleftrightarrow \text{cut-hair}(B,x)\ )$

    $\Rightarrow (\exists B \ \neg\text{cut-hair}(B,B) \longleftrightarrow \text{cut-hair}(B,B)\ )$

    $\Rightarrow \exists B$ False

    $\Rightarrow$ False, which is a contradiction!

Example

- For every pair of distinct primes p,q, $\log_p(q)$ is irrational
- (Will use basic facts about log and primes from arithmetic.)
- Suppose for the sake of contradiction that there exists a pair of distinct primes (p,q), s.t. $\log_p(q)$ is rational.
- $\Rightarrow \log_p(q) = a/b$ for positive integers a,b.

  (Note, since $q>1$, $\log_p(q) > 0$.)
- $\Rightarrow p^{a/b} = q \Rightarrow p^a = q^b$.
- But p, q are distinct primes. Thus p^a and q^b are two distinct prime factorisations of the same integer!
- Contradicts the Fundamental Theorem of Arithmetic!

Will prove later

Reduction

- Often it is helpful to break up the proof into two parts
- To prove p, show $r \rightarrow p$ and separately show r
  - The proof $r \rightarrow p$ is said to "reduce" the task of proving p to the task of proving r
  - Many sophisticated proofs are carried out over several works, each one reducing it to a simpler problem

$$p_0 \Rightarrow \ldots \Rightarrow r' \Rightarrow \ldots \Rightarrow r \Rightarrow \ldots \Rightarrow p$$

  - Proving $r \rightarrow p$ leaves open the possibility that $\neg p$ will be proven later, which will yield a proof for $\neg r$ instead

Template for $\exists x\ P(x)$

- To prove $\exists x\ P(x)$
  - Demonstrate a particular value of x s.t. $P(x)$ holds
- e.g. to prove $\exists x\ P(x) \rightarrow Q(x)$
  - find an x s.t. $P(x) \rightarrow Q(x)$ holds
    - if you can find an x s.t. $P(x)$ is false, done!
    - or, you can find an x s.t. $Q(x)$ is true, done!
    - (May not be easy to show either, but still may be able to find an x and argue $\neg P(x) \vee Q(x)$)
  - (May not be able to find one, but still show one exists!)

Template for $\neg(\forall x\ P(x))$

- To prove $\neg(\forall x\ P(x))$
  - $\equiv \exists x\ \neg P(x)$
  - Demonstrate a particular value of x s.t. P(x) doesn't hold
  - Proof by counterexample
- e.g. to disprove the claim that all odd numbers > 1 are prime
  - i.e., to prove $\neg(\forall x \in S, \text{Prime}(x))$ where S is the set of all odd numbers > 1
  - Enough to show that $\exists x \in S\ \neg\text{Prime}(x)$
    - take $x = 9 = 3 \times 3$ (or, say, $x = 207 = 9 \times 23$)

Template for $\forall x\ P(x)$

- To prove $\forall x\ P(x)$
  - Let x be an arbitrary element (in the domain of the predicate P)
  - Now prove P(x) holds
  - x is arbitrary: the proof applies to every x. Hence $\forall x\ P(x)$
- e.g., To prove $\forall x\ \underline{Q(x) \rightarrow R(x)}$
  - To prove $Q(x) \rightarrow R(x)$ for an arbitrary x
    - Assume Q(x) holds, i.e., set p_0 to be Q(x). Then prove R(x) using a sequence, $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_n$, where p_n is R(x)
  - Caution: You are not proving $(\forall x\ Q(x)) \rightarrow (\forall x\ R(x))$. So to prove R(x), may only assume Q(x), and not Q(x′) for $x' \neq x$.

Cases

- Often it is helpful to break a proposition into various "cases" and prove them one by one
- e.g., To prove q, prove the following
  - $c_1 \vee c_2 \vee c_3$
  - $c_1 \rightarrow q$
  - $c_2 \rightarrow q$
  - $c_3 \rightarrow q$
  - $\Rightarrow (c_1 \vee c_2 \vee c_3) \rightarrow q$
  - $\Rightarrow q$

$$(c_1 \rightarrow q) \wedge (c_2 \rightarrow q) \wedge (c_3 \rightarrow q)$$

$$\equiv$$

$$(c_1 \vee c_2 \vee c_3) \rightarrow q$$

$$c \wedge (c \rightarrow q) \Rightarrow q$$

Cases

- Often it is helpful to break a proposition into various "cases" and prove them one by one
- e.g., To prove $p \rightarrow q$, prove the following
  - $p \rightarrow c_1 \vee c_2 \vee c_3$
  - $c_1 \rightarrow q$
  - $c_2 \rightarrow q$
  - $c_3 \rightarrow q$
  - $\Rightarrow (c_1 \vee c_2 \vee c_3) \rightarrow q$
  - $\Rightarrow p \rightarrow q$

$$(c_1 \rightarrow q) \wedge (c_2 \rightarrow q) \wedge (c_3 \rightarrow q)$$
$$\equiv$$
$$(c_1 \vee c_2 \vee c_3) \rightarrow q$$

$$((p \rightarrow c) \wedge (c \rightarrow q)) \Rightarrow (p \rightarrow q)$$

Cases: Example

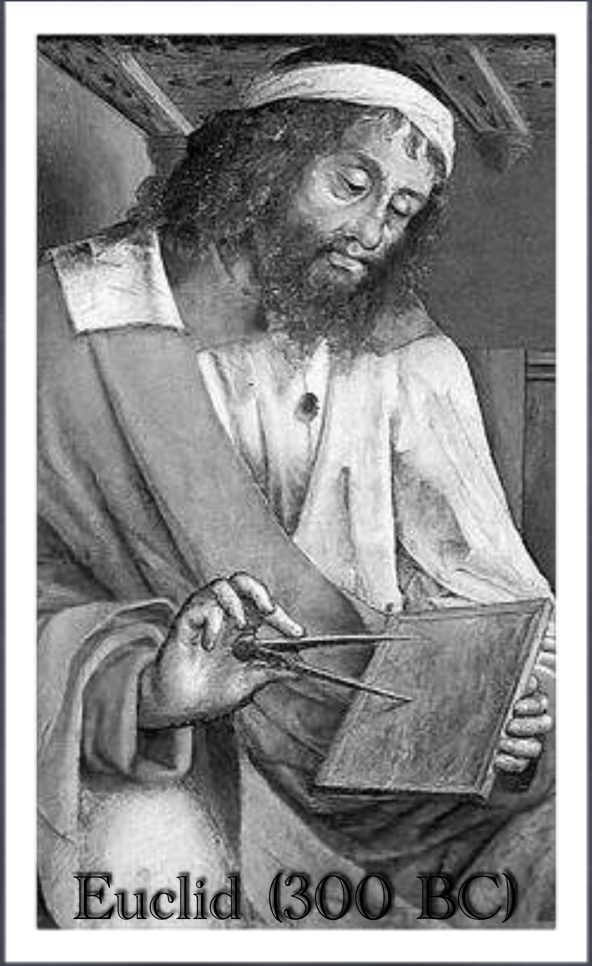
- Proving equivalences of logical formulas
- To prove: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  - $\forall p,q,r \in \{T,F\} \quad (p \vee (q \wedge r)) \longleftrightarrow ((p \vee q) \wedge (p \vee r))$
- Two cases: $p \vee \neg p$
- Case p: $p \vee (q \wedge r) \equiv T$

  $(p \vee q) \wedge (p \vee r) \equiv T$
- Case ¬p: $p \vee (q \wedge r) \equiv (q \wedge r)$

  $(p \vee q) \wedge (p \vee r) \equiv (q \wedge r)$

Cases: Example

- $\forall a,b,c,d \in \mathbb{Z}^+$ If $a^2+b^2+c^2 = d^2$, then d is even iff a,b,c are all even.
- Suppose $a,b,c,d \in \mathbb{Z}^+$ s.t. $a^2+b^2+c^2 = d^2$. Will show d is even iff a,b,c are all even.
- 4 cases based on number of a,b,c which are even.
- Case 1: a,b,c all even $\Rightarrow d^2 = a^2+b^2+c^2$ even $\Rightarrow$ d even.
- Case 2: Of a,b,c, 2 even, 1 odd. Without loss of generality, let a be odd and b, c even. i.e., $a=2x+1$, $b=2y$, $c=2z$ for some x,y,z. Then, $d^2 = a^2+b^2+c^2 = 2(2x^2+2x+2y^2+2z^2) + 1 \Rightarrow d^2$ odd $\Rightarrow$ d odd.
- Case 3: Of a,b,c, 1 even, 2 odd. W.l.o.g, $a=2x+1, b=2y+1, c=2z$. Then, $d^2=a^2+b^2+c^2 = 4(x^2+x+y^2+y+4z^2) + 2$. Contradiction! (why?)
- Case 4: a,b,c all odd $\Rightarrow d^2 = a^2+b^2+c^2 = 4w+3 \Rightarrow$ d odd.



Mathematical Induction

Proof by Programming

The Fable of the Proof Deity!

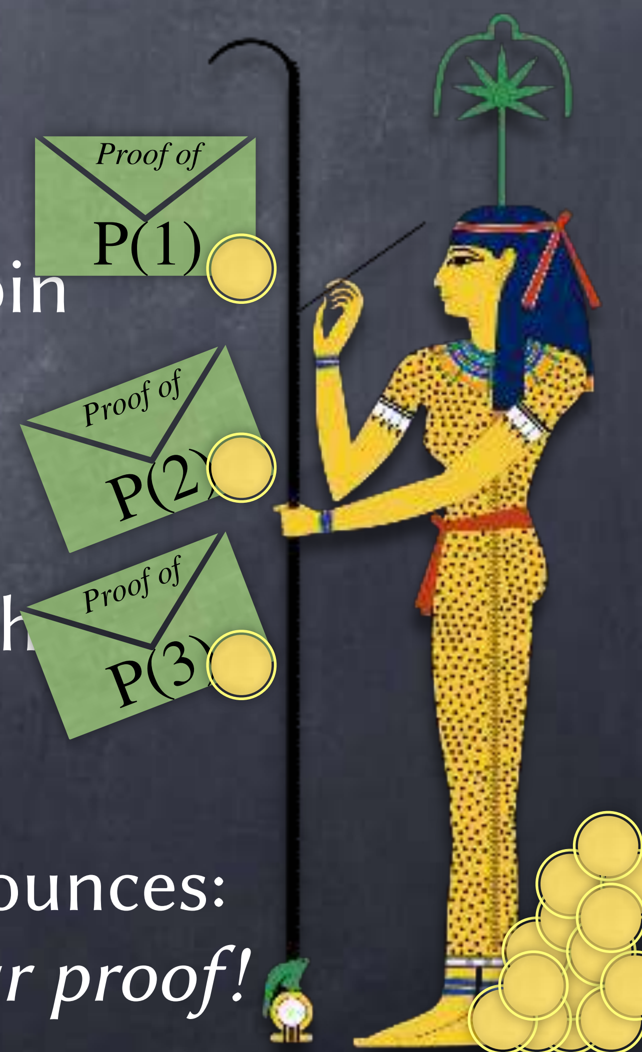
(OK, I made it up :))

- 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!

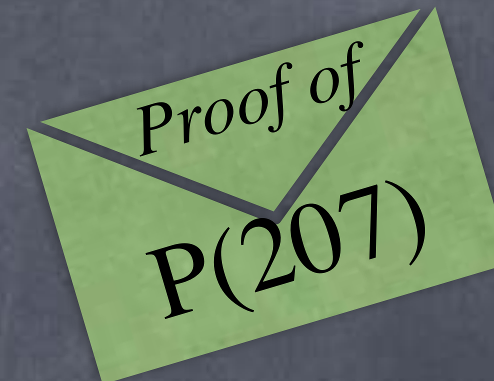
(OK, I made it up :))

- 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) ⟶ P(2), we have P(2).
> Since P(2) and, by Lemma, P(2) ⟶ P(3), we have P(3).
> ⋮
> Since P(206) and, by Lemma, P(206) ⟶ 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 $\boxed{P(1)}$ and $\boxed{\forall k \in \mathbb{Z}^+ \ \ P(k) \rightarrow P(k+1)}$

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.

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

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

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

Base case

Induction step

Induction hypothesis

Proof by Induction

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

- 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 <u>the claim holds for n = 1</u>. … P(1)
  - We shall prove that for any k≥1, if <u>the claim holds for n=k</u> (P(k)) then <u>it holds for n=k+1</u>. P(k+1)
  - 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 $P(k) \rightarrow P(k+1)$

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

Well Ordering Principle

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

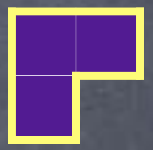
(Can be used instead of Principle of Mathematical Induction)

In disguise

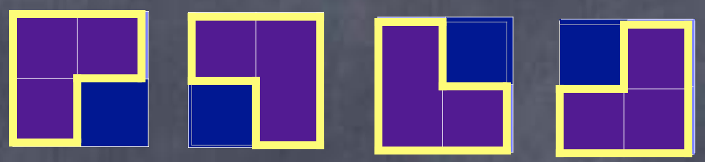
- To prove $\forall n \in \mathbb{Z}^+ \ P(n)$:
  - Prove $P(1)$ and $\forall k \in \mathbb{Z}^+ \ \neg P(k+1) \rightarrow \neg P(k)$
  - For the sake of contradiction, suppose $\neg \, (\forall n \in \mathbb{Z}^+ \ P(n))$.
  - Let k' be the smallest $n \in \mathbb{Z}^+$ s.t. $\neg P(n)$. $k' \neq 1$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



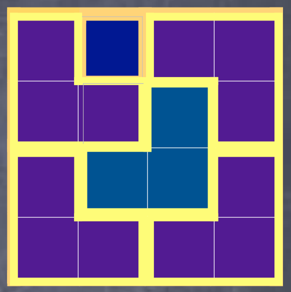
- Base case: n=1



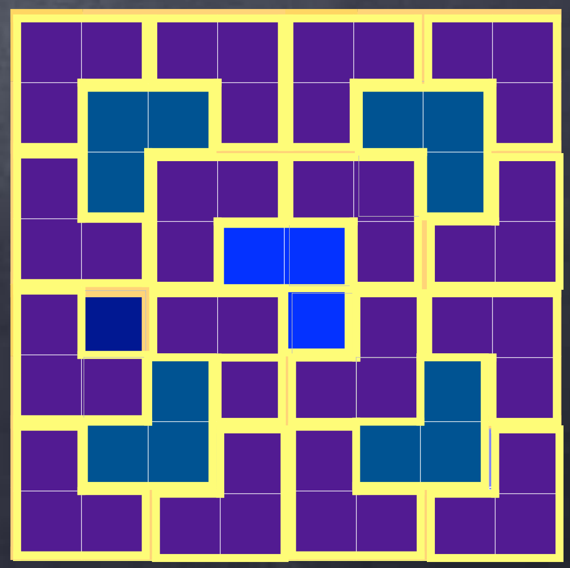
- Inductive step: For all integers $k \geq 1$:

  <u>Hypothesis</u>: suppose, true for n=k

  <u>To prove</u>: 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 $P(1)$ (as before) and that

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

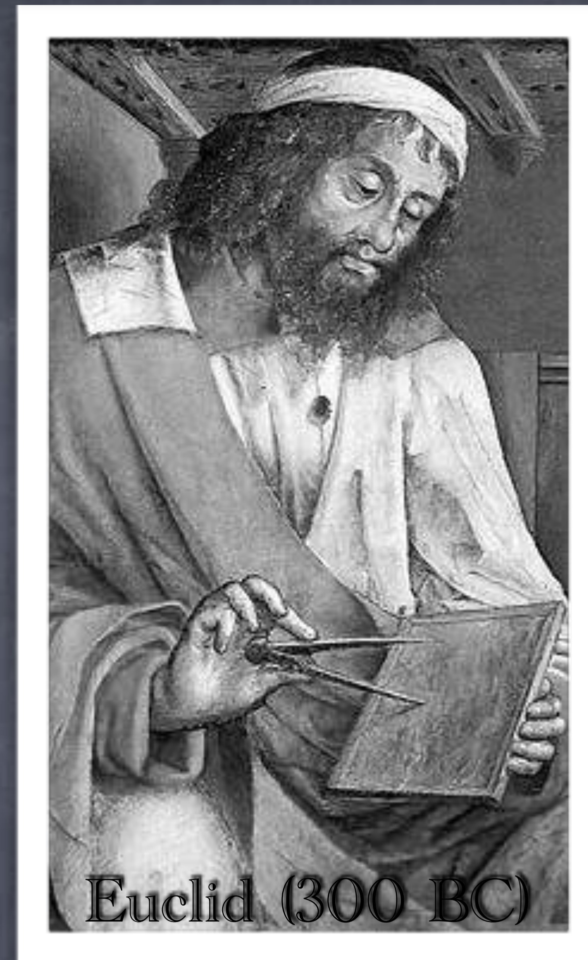
Mathematical Induction

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.

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

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

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



Mathematical Induction

Examples

Strong Induction

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

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

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

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

Mathematical Induction

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.

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

Postage Stamps

- Claim: Every amount of postage that is at least ₹12 can be made from ₹4 and ₹5 stamps
  - i.e., $\forall n \in \mathbb{Z}^+ \;\; n \geq 12 \rightarrow \exists a,b \in \mathbb{N} \;\; n=4a+5b$
- Base cases: n=1,..,11 (vacuously true) and $n = 12 = 4\cdot 3 + 5\cdot 0$, $n = 13 = 4\cdot 2 + 5\cdot 1$, $n = 14 = 4\cdot 1 + 5\cdot 2$, $n = 15 = 4\cdot 0 + 5\cdot 3$.
- Induction step: For all integers $k \geq 16$:

  Strong induction hypothesis: Claim holds for all n s.t. $1 \leq n < k$

  To prove: Holds for $n=k$
  - $k \geq 16 \rightarrow k-4 \geq 12$.
  - So by induction hypothesis, $k-4=4a+5b$ for some $a,b \in \mathbb{N}$.
  - So $k = 4(a+1) + 5b$.

Prime Factorization

Need some more work to show unique factorization.

p prime $\wedge$ p|ab $\rightarrow$ p|a $\vee$ p|b

- Every positive integer $n \geq 2$ has a prime factorization i.e, $n = p_1 \cdot \ldots \cdot p_t$ (for some $t \geq 1$) where all p_i are prime

- Base case: $n=2$. ($t=1$, $p_1=2$).
- Induction step:

  (Strong) induction hypothesis: for all $n \leq k$, $\exists p_1,\ldots,p_t$, s.t. $n= p_1 \cdot \ldots \cdot p_t$

  To prove: $\exists q_1,\ldots,q_u$ (also primes) s.t. $k+1= q_1 \cdot \ldots \cdot q_u$

  - Case $k+1$ is prime: then $k+1=q_1$ for prime q_1
  - Case $k+1$ is not prime: $\exists a \in \mathbb{Z}^+$ s.t. $2 \leq a \leq k$ and $a|k+1$ (def. prime).
  - i.e., $\exists a,b \in \mathbb{Z}^+$ s.t. $2 \leq a,b \leq k$ and $k+1=a.b$ (def. divides; $a \geq 2 \rightarrow a.b > b$)
  - Now, by (strong) induction hypothesis, both a & b have prime factorizations: $a=p_1\ldots p_s$, $b=r_1\ldots r_t$.
  - Then $k+1=q_1\ldots q_u$, where $u=s+t$, $q_i = p_i$ for $i=1$ to s and $q_i = r_{i-s}$, for $i=s+1$ to $s+t$.

Be careful about ranges!

- Claim: Every non-empty set of integers has either all elements even or all elements odd. (Of course, false!)
- "Proof" (bogus): By induction on the size of the set.
- Base case: $|S|=1$. The only element in S is either even or odd ✓
- Induction step: For all $k > 1$,

  Bug: Induction hypothesis cannot be bootstrapped from the base case

  Induction hypothesis: suppose all non-empty S with $|S| = k$, has either all elements even or all elements odd.

  To prove: then, it holds for all S with $|S|=k+1$.

  - Let $S = \{a,b\} \cup S'$, where $|S'|=k-1$. (Note: S' is not empty)
  - By IH, $S' \cup \{a\}$ has all even or all odd. Say, all even. Then S' is all even. Now, $S' \cup \{b\}$ is also all even or all odd. Since S' not empty, it is all even. Thus $S = S' \cup \{a,b\}$ is all even. QED.

Be careful about ranges!

- Claim: Every non-empty set of integers has either all elements even or all elements odd. (Of course, false!)
- “Proof” (bogus): By induction on the size of the set.
  - We proved $P(1)$ and $\forall k>1 \quad P(k) \rightarrow P(k+1)$

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

Nim

- Alice and Bob take turns removing matchsticks from two piles
- Initially both piles have equal number of matchsticks
- At every turn, a player must choose one pile and remove one or more matchsticks from that pile
- Goal: be the person to remove the last matchstick
- Claim: In Nim, the second player has a winning strategy
  - (Aside: in every finitely-terminating two player game without draws, one of the players has a winning strategy)
- Claim: The following is a winning strategy for the second player: keep the piles matched at the end of your turn

Nim

- Claim: The following is a winning strategy for the second player: keep the piles matched at the end of your turn
- Induction variable: n = number of matchsticks on each pile at the beginning of the game.
- Base case: n=1. Alice must remove one. Next, Bob wins. ✔
- Induction step: for all integers $k \geq 1$

  Induction hypothesis: when starting with $n \leq k$, Bob always wins

  strong

  To prove: when starting with $n = k+1$, Bob always wins

  - Case 1: Alice removes all k+1 from one pile. Next, Bob wins.
  - Case 2: Alice removes j, $1 \leq j \leq k$ from one pile. After Bob's move $k+1-j$ left in each pile. By induction hypothesis, Bob will win from here.