Mon Oct 29

Exam 2

Ave 13.6 / 20

Med. 14

Approximate grade ranges

16 – 20 ≈ A

12 – 15 ≈ B

8 – 11 ≈ C

Next topic: "Induction"

(A.K.A. the "Well-Ordering Principle".)

Something Pythagoras knew:

$\forall n \in \mathbb{N} = \{1, 2, 3, \ldots\}$ we have

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Proof: Given $n \geq 1$,

let $X := \sum_{i=1}^{n} i = 1 + 2 + \cdots + n$

Then

$$2X = (1 + 2 + 3 + \cdots + n) + (n + n-1 + n-2 + \cdots + 1)$$

$$= \underbrace{(n+1) + (n+1) + (n+1) + \cdots + (n+1)}_{n \text{ times}}$$

$$= n(n+1).$$

$$\Longrightarrow \quad X = n(n+1) / 2.$$

Carl Friedrich Gauss (1777 – 1855)

- greatest mathematician of his time
- anecdote (109 versions):

To keep the students busy, Gauss' teacher assigned them to compute

$$1 + 2 + 3 + \cdots + 100$$

Young Gauss returned the answer within seconds. $\frac{100 \cdot 101}{2} = 5050$.

Something Archimedes Knew:

$\forall\, n \in \mathbb{N}$ we have

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof? Start small.

$n=1$ $\quad 1^2 = \frac{1 \cdot 2 \cdot 3}{6} = 1$ ✓

$n=2$ $\quad 1^2 + 2^2 = \frac{2 \cdot 3 \cdot 5}{6} = 5$ ✓

$n=3$ $\quad 1^2 + 2^2 + 3^2 = \frac{3 \cdot 4 \cdot 7}{6} = 14$ ✓

We're tired. Use a computer.
Computer verifies the result up to $n = 10^{100}$. Computer breaks down ☹

Now What?

Finite $\rightsquigarrow$ Infinite

How to bridge this gap?
(We <u>can't</u>. We need an axiom.)

Axiom: Well-Ordering Principle.

Every nonempty subset $S \subseteq \mathbb{N}$ has a smallest element.

Let S be the set of $n \in \mathbb{N}$ such that

"$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$"

is FALSE. Show that $S = \emptyset$ (i.e. it's true $\forall n \in \mathbb{N}$).

Suppose for contradiction that $S \neq \emptyset$ then by Well-Ordering $\exists$ smallest element. Call it $m \in S$. (our "minimal criminal").

Know: $m > 10^{100}$ (or wherever we stopped)

Know: $1^2 + 2^2 + \cdots + (m-1)^2 = \frac{(m-1)(m)(2(m-1)+1)}{6}$

since $m-1 \notin S$.

$\lightning$

But then

$$1^2 + 2^2 + \cdots + m^2$$

$$= \underbrace{1^2 + 2^2 + \cdots + (m-1)^2}_{} + m^2$$

$$= \left[\frac{(m-1)(m)(2(m-1)+1)}{6} \right] + m^2 \qquad \text{since } m-1 \notin S$$

$$= \frac{m}{6}\left[(m-1)(2m-1) + 6m \right]$$

$$= \frac{m}{6}\left[2m^2 + 3m + 1 \right]$$

$$= \frac{m}{6}(m+1)(2m+1) \qquad \text{OOPS!}$$

We just proved that $m \notin S$.
Contradiction.

Hence $S = \emptyset$ as desired. $\blacksquare$

We assumed

$$\exists n \in \mathbb{N}, \ 1^2 + 2^2 + \cdots + n^2 \neq \frac{n(n+1)(2n+1)}{6}$$

and got a contradiction. Hence

$$\forall n \in \mathbb{N}, \ 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

[Discussion: Let U be a set. For each $x \in U$, let $P(x)$ be a logical statement about x.

Q: What is the opposite of the statement

$\forall x \in U, \ P(x)$?

"for all $x \in U$, $P(x)$ is true"

A: NOT $(\forall x, \ P(x))$

$= \exists x \in U, \ \text{NOT } P(x)$

"there exists some $x \in U$ such that $P(x)$ is false."

Similarly, NOT ($\exists x \in U$, $P(x)$)

$= \forall x \in U$, NOT $P(x)$.

Logical Principle:

NOT exchanges $\forall$ and $\exists$

universal quantifier — existential quantifier

Let $P(n) =$ "$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$"

We proved that

"$\exists n \in \mathbb{N}$, $P(n) = F$" $= F$.

Take NOT on both sides to get

"$\forall n \in \mathbb{N}$, $P(n) = T$" $= T$

(To prove a $\forall$ statement, enough to disprove an $\exists$ statement)

Wed Oct 31

HW 4:
Ave 16.5 / 20
Med 18

Recall: Something Archimedes Knew

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad \forall n \in \mathbb{N}$$

Proof: $\forall n \in \mathbb{N}$ let

$$P(n) = \underbrace{\text{“}1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}\text{”}}_{\text{logical statement depending on } n.}$$

Let $S = \{ n \in \mathbb{N} : P(n) = F \}$.

Claim: $S = \emptyset$.
If not, then Well-Ordering $\Rightarrow$ S has a smallest element $m \in S$.

Since $P(1) = T$ we know that $m > 1$.
Hence

$$P(m) = F \text{ and } P(m-1) = T$$

i.e. we have

$$1^2 + 2^2 + \cdots + (m-1)^2 = \frac{(m-1)(m)(2(m-1)+1)}{6}$$

(That was logic. Now the math.)
But then

$$1^2 + 2^2 + \cdots + m^2$$
$$= (1^2 + 2^2 + \cdots (m-1)^2) + m^2$$
$$= \frac{(m-1)(m)(2(m-1)+1)}{6} + m^2$$

algebra

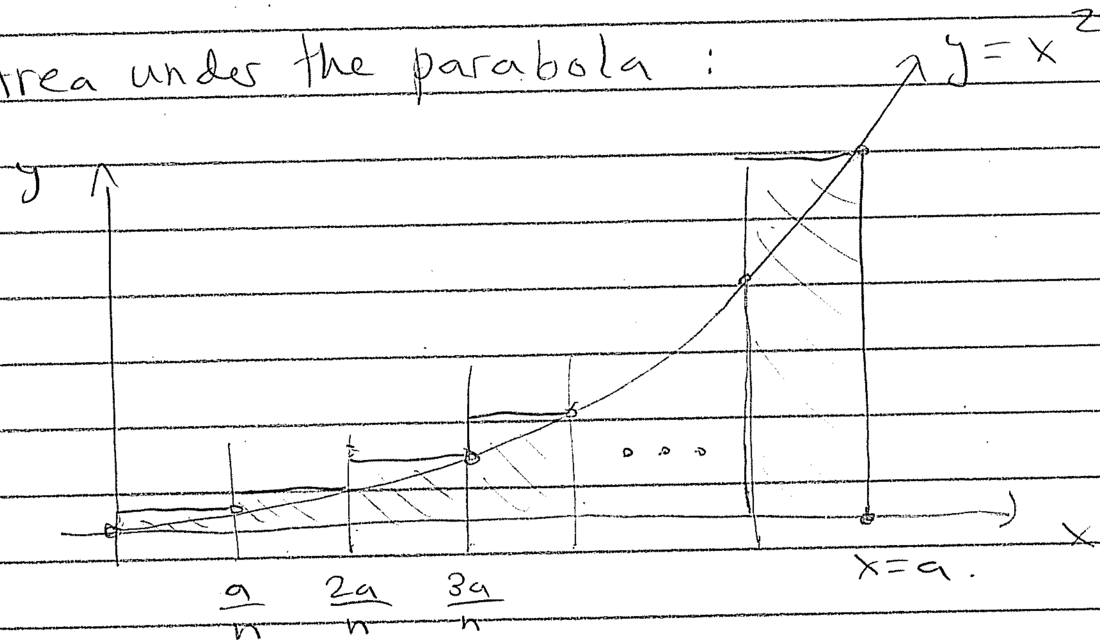
$$= \frac{m(m+1)(2m+1)}{6}.$$

Hence $P(m) = T$. Contradiction.

We conclude that $S = \emptyset$ as desired $\blacksquare$

Why did Archimedes care?

Area under the parabola:



area $\int_0^a x^2\,dx \approx$ sum of rectangles.

$$\frac{a}{n}\left(\frac{a}{n}\right)^2 + \frac{a}{n}\left(\frac{2a}{n}\right)^2 + \cdots + \frac{a}{n}\left(\frac{na}{n}\right)^2$$

$$= \frac{a^3}{n^3}\left[1^2 + 2^2 + \cdots + n^2\right]$$

$$= \frac{a^3}{n^3}\left[\frac{n(n+1)(2n+1)}{6}\right]$$

$$= \frac{a^3}{n^3}\left[\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n\right]$$

$$= a^3 \left(\frac{1}{3} + \underbrace{\frac{1}{2n} + \frac{1}{6n^2}}_{\text{small for large } n} \right) \longrightarrow \frac{a^3}{3}$$

Answer: $\displaystyle\int_0^a x^2\,dx = \frac{a^3}{3}$.

Fermat investigated the sum

$1^p + 2^p + \cdots + n^p = ?$ (HW 5)

To prove that $\displaystyle\int_0^a x^p\,dx = \frac{a^{p+1}}{p+1}$

The key to our proof was that

$\forall\, m > 1$ we have

$$\boxed{P(m-1) = T \implies P(m) = T}$$

This implied that

$$S = \{ n \in \mathbb{N} : P(n) = F \} = \emptyset$$

as desired.

We can rephrase this as a principle.

★. The Principal of Induction (PI)

For each $n \in \mathbb{N}$, let $P(n)$ be a logical statement about n. If

① $P(1) = T$
② $\forall k \geq 1$, $P(k) \implies P(k+1)$.

Then $P(n) = T \ \forall n \in \mathbb{N}$

an <u>infinite</u> statement.

Q: Is PI "true"?

A: All we know is that

$$\underbrace{WO \iff PI}_{\text{logically equivalent}}$$

One is an axiom
One is a theorem } you choose which

Fri Nov 2

Class canceled on Wed Nov 7

Now: Chapter 4 (Induction)

Principle of Induction (PI) 4.13:

Let P be a function $P: \mathbb{N} \to \{T, F\}$
i.e. for each $n \in \mathbb{N}$, $P(n)$ is a logical statement about n. If

(1) $P(1) = T$
(2) $\forall k \geq 1$, $P(k) = T \Rightarrow P(k+1) = T$

then $P(n) = T \quad \forall n \geq 1$. ///

Application: Assume PI holds.

Let $P(n) =$ " $1 + 3 + 5 + \cdots + (2n-1) = n^2$ "

Prove that $P(n) = T \quad \forall n \geq 1$.

Proof (by induction):

First note that $P(1) = T$ since $1 = 1^2$.

Next, (assume for induction that $P(k) = T$ for some $k \geq 1$, i.e. $1 + 3 + 5 + \cdots + (2k-1) = k^2$. In this case we also have

$$1 + 3 + 5 + \cdots + (2(k+1) - 1)$$

$$= \underbrace{\left[1 + 3 + \cdots + (2k-1)\right]} + (2(k+1) - 1)$$

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

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

$$= (k+1)^2.$$

proof within a proof

Hence $P(k+1) = T$.)

By PI we conclude that $P(n) = T \ \forall n \geq 1$

Induction has 2 steps.

(1) Find some truth.
(2) Build a machine for moving truth
(an arrow $\Rightarrow$)

¡Neither is enough by itself!

Example (1 is not enough)

Let $P(n) =$ "$n^2 < 2n$"

Claim: $P(n) = T \quad \forall n \in \mathbb{N}$.

Proof: $P(1) = T$ since $1^2 < 2$.
Therefore $P(n) = T \quad \forall n \geq 1$. $\boxtimes$

Example (2 is not enough)

Let $P(n) =$ "$n+1 < n$"

Claim: $P(n) = T \quad \forall n \geq 1$.

Proof: Assume for induction that $P(k) = T$ for some $k \geq 1$ i.e $k+1 < k$.
Add 1 to both sides to get

$$k+1 < k$$
$$\Rightarrow k+2 < k+1$$
$$\text{i.e. } (k+1)+1 < (k+1).$$

Hence $P(k+1) = T$. $\blacksquare$

We showed if $P(k) = T$ then $P(k+1) = T$.
But this is useless if $\nexists$ k such that $P(k) = T$

"Dominoes"

$$P(1) \quad P(2) \quad P(3) \quad P(4) \quad P(5) \quad \cdots$$
$$T \quad T \quad T \quad T \quad T \quad \cdots$$

(1) Your Finger
(2) Gravity.

Q: What is a "number"?
A: The modern definition was given by Giuseppe Peano (1889).

Peano Arithmetic (Definition of $\mathbb{N}$):

Let $\mathbb{N}$ be a set with an equivalence relation "$=$" and a function $S: \mathbb{N} \to \mathbb{N}$ satisfying 4 axioms:

P1 $\quad 0 \in \mathbb{N}$

P2 $\quad \forall n \in \mathbb{N}, \quad S(n) \neq 1$.

P3 $\quad S$ is injective

i.e. $\forall m, n \in \mathbb{N}, \quad S(m) = S(n) \Rightarrow m = n$.

P4 If a subset $K \subseteq \mathbb{N}$ satisfies

- $0 \in K$
- $\forall n \in \mathbb{N}, \quad n \in K \Rightarrow S(n) \in K$

Then $K = \mathbb{N}$.

That's All.

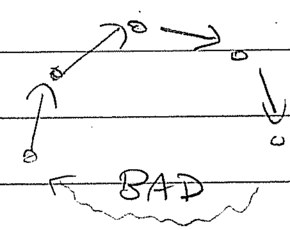
We should think $S(n) =$ "$n+1$"
even though $+$ isn't defined yet.

S stands for "successor".

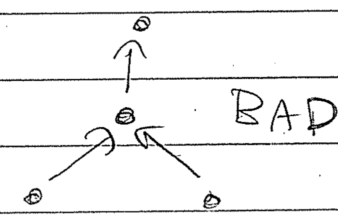
Meaning:

(P1) $\exists$ a number and every number has a successor.

(P2) numbers don't loop



(P3) numbers don't branch



(P4) PI is true
(allows us to make statements about "all" numbers)

That's pretty efficient, but it doesn't look much like $\mathbb{Z}$.
With some work (!) we can construct $\mathbb{Z}, +, \times, 0, \leq$ and prove the desired properties.

Idea: Define $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ recursively by

- $a + 0 = a \quad \forall a \in \mathbb{N}$.
- $a + S(b) = S(a+b) \quad \forall a, b \in \mathbb{N}$.

Define an integer as an ordered pair $(a,b) \in \mathbb{N}^2$ and say

$$(a,b) \approx (c,d) \iff a + d = b + c.$$

Think: $(a,b) =$ "$a - b$"

Then we say

$$\mathbb{Z} := \mathbb{N}^2 / \approx$$

The "integer" "2" is really an infinite set

etc. $\{(2,0), (3,1), (4,2), (5,3), \ldots\}$

natural numbers

Do you like this?

Mon Nov 5

HW5 due Fri Nov 16.

Class canceled Wed Nov 7.

There are many ways to say "Induction".

WO Well-Ordering Principle:

Every nonempty subset of $\mathbb{N}$ has a least element.

Peano's Axiom (4.11):

If $S \subseteq \mathbb{Z}$ is a set satisfying

(i) $b \in S$

(ii) $\forall k \geq b$, $k \in S \Rightarrow k+1 \in S$

then $S = \{b, b+1, b+2, \ldots\}$

PI Principle of Induction (4.13):

For all $n \geq b$ let $P(n)$ be a statement about n. If

(i) $P(b) = T$, and

(ii) $\forall k \geq b$, $P(k) = T \Rightarrow P(k+1) = T$

then $P(n) = T \quad \forall n \geq b$.

$\Big\Downarrow$

PSI

Principle of Strong Induction (4.18):

For all $n \geq b$ let $P(n)$ be a statement about n. If

(i) $P(b) = T$, and

(ii) $\forall k \geq b$ we have

$$[P(b) = P(b+1) = \cdots = P(k) = T] \Rightarrow [P(k+1) = T]$$

then $P(n) = T \quad \forall n \geq b$.

Example of PSI.

Theorem: Every integer $n \geq 2$ has a prime factor.

Proof: Let $P(n) =$ "n has a prime factor".

(i) Note that $P(2) = T$.

(ii) Now fix $k \geq 2$ and assume that
$P(2) = P(3) = \cdots = P(k) = T$.
In this case, we want to show that $P(k+1) = T$.

Well if $k+1$ is prime then $P(k+1) = T$, so suppose $k+1$ is composite; i.e., $\exists\ 1 < a, b < k+1$ such that $k+1 = ab$

Since $a \leq k$ we have $P(a) = T$ so $\exists\, p, k \in \mathbb{Z}$ with p prime such that $a = pk$.
But then

$$k+1 = ab = (pk)b = p(kb)$$

$$\Longrightarrow P(k+1) = T.$$

By PSI we conclude that $P(n) = T \ \forall n \geq 2$. ∎

Claim: In the presence of the other axioms of $\mathbb{N}$ (or $\mathbb{Z}$) we have

$$\begin{tikzcd}
 & \text{PI} \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \\
\text{WO} \arrow[rr, Leftrightarrow] & & \text{PSI}
\end{tikzcd}$$

"logically equivalent".

Prepare yourself. We are going to prove that WO $\Rightarrow$ PI.

<u>Proof</u>: [<u>Assume</u> that WO holds. Want to show that PI holds. [So <u>suppose</u> that $P: \mathbb{N} \to \{T, F\}$ satisfies (1) $P(b) = T$ and (2) $\forall k \geq b$, $P(k) \Rightarrow P(k+1)$. Want to show that $P(n) = T$ $\forall n \geq b$.

[So <u>suppose</u> not; i.e., <u>suppose</u> $\exists n \geq b$ with $P(n) = F$. Let

$$S = \{n \geq b : P(n) = F\}.$$

Since by assumption $S \neq \emptyset$, WO $\Rightarrow$ $\exists$ <u>smallest</u> $m \in S$. Since $P(b) = T$ by (1), we have

$$P(m-1) = T \quad \& \quad P(m) = F$$

But this contradicts assumption (2).]

Hence $P(n) = T$ $\forall n \geq b$]

Hence PI holds.]

Hence WO $\Rightarrow$ PI. ▨

Fri Nov 9

HW 5 due Fri Nov 16.

Recall: There are several equivalent ways to say "Induction":

$$\begin{tikzcd}
 & PI \arrow[dl, Leftrightarrow] \arrow[dr, Leftrightarrow] & \\
WO \arrow[rr, Leftrightarrow] & & PSI
\end{tikzcd}$$

We proved $WO \Rightarrow PI$ in class with lots of parentheses.
You'll prove $PSI \Rightarrow WO$ on HW 5.4.

Today: Fibonacci (c. 1170 – 1250).
("son of Bonacci")

- also called Leonardo of Pisa
- book "Liber Abaci" (1202)
- introduced Hindu numerals to Europe

i.e. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

first appearance (c. 628) in "correctly established doctrine of Brahma".

And yet: We remember Fibonacci for a silly reason.

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, etc.

Define:

$$\begin{cases} f(0) := 0 \\ f(1) := 1 \\ f(n) := f(n-1) + f(n-2) \quad \forall\, n \geq 2 \end{cases}$$

This is a "recursive" definition.

Q: Is there a "formula" for $f(n)$?
A: Yes.

Theorem: For all $n \geq 0$ we have

$$f(n) = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right] \qquad (!)$$

- maybe not anyone could guess this
- but, once guessed, anyone can prove it.

Proof: Base cases (we need two!):

$$f(0) = \frac{1}{\sqrt{5}}\left[1-1\right] = 0 \checkmark$$

$$f(1) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{2\sqrt{5}}{2}\right] = \underline{1} \checkmark$$

Induction Step:
First define $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$ and observe that

$$\alpha^2 = \alpha + 1 \quad \text{and} \quad \beta^2 = \beta + 1.$$

(Proof: α, β are the roots of $x^2 - x - 1 = 0$ ///)

Now fix $k \geq 2$ and assume that

$$f(n) = \frac{1}{\sqrt{5}}\left[\alpha^n - \beta^n\right] \quad \text{for all } 0 \leq n \leq k.$$

"strong induction"

In this case we want to show that

$$f(k+1) = \frac{1}{\sqrt{5}}\left[\alpha^{k+1} - \beta^{k+1}\right].$$

Indeed, we have

$$\frac{1}{\sqrt{5}}\left[\alpha^{k+1}-\beta^{k+1}\right]$$

$$=\frac{1}{\sqrt{5}}\left[\alpha^{k-1}\alpha^{2}-\beta^{k-1}\beta^{2}\right]$$

$$=\frac{1}{\sqrt{5}}\left[\alpha^{k-1}(\alpha+1)-\beta^{k-1}(\beta+1)\right]$$

$$=\frac{1}{\sqrt{5}}\left[\alpha^{k}+\alpha^{k-1}-\left(\beta^{k}+\beta^{k-1}\right)\right]$$

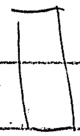
$$=\frac{1}{\sqrt{5}}\left[\alpha^{k}-\beta^{k}\right]+\frac{1}{\sqrt{5}}\left[\alpha^{k-1}-\beta^{k-1}\right]$$

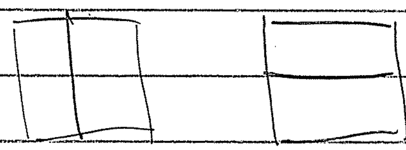
$= f(k) + f(k-1)$ by induction

$= f(k+1)$ by definition]

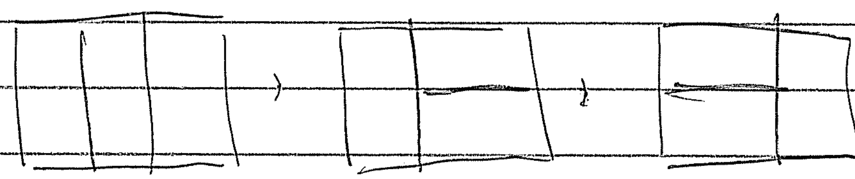
By PSI we are done ∎

Next, let $g(n)$ = # tilings of $2 \times n$ rectangle by 2×1 "dominoes".

$n=1$  $g(1) = 1$.

$n=2$  $g(2) = 2$

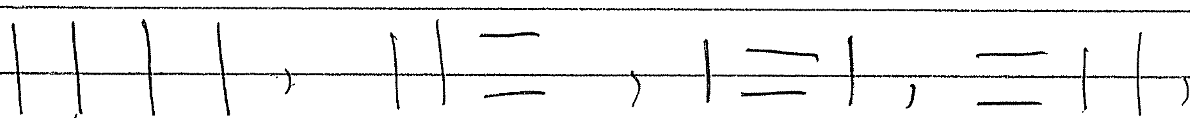
$n=3$

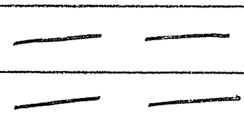


$g(3) = 3$.

Guess: $g(n) = n$? No.

$n=4$



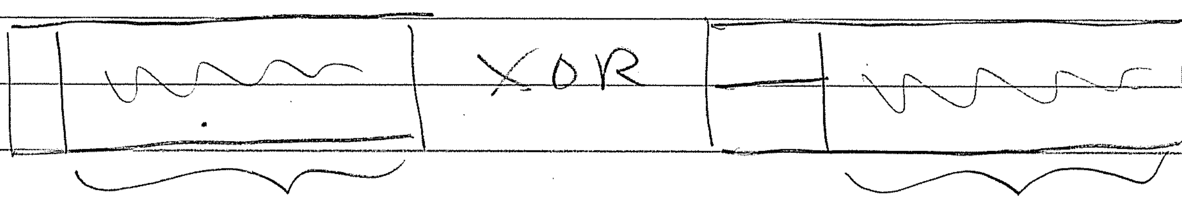
 $g(4) = 5$ (!)

claim: $g(n) = f(n+1)$ (Fibonacci)

Proof: Base cases: $g(1) = f(2) = 1$ ✓
$g(2) = f(3) = 1$ ✓

Induction Step:

First, I claim that $g(n) = g(n-1) + g(n-2)$ $\forall n \geq 3$.
Proof: When tiling a $2 \times n$ rectangle, the left end looks like



$g(n-1)$ ways to finish

$g(n-2)$ ways to finish ///

Finally, [assume that $g(n) = f(n+1)$ for all $1 \leq n \leq k$. Want to show $g(k+1) = f(k+2)$.
Indeed,

$$
\begin{aligned}
g(k+1) &= g(k) + g(k-1) && \text{from above} \\
&= f(k+1) + f(k) && \text{by assumption} \\
&= f(k+2) && \text{by definition}
\end{aligned}
$$
]

By PSI we're done