LECTURE #6

Mathematical Induction

What is the sum of the first n positive odd integers?

$n=1$ $\quad 1 = 1 = 1^2$

$n=2$ $\quad 1+3 = 4 = 2^2$

$n=3$ $\quad 1+3+5 = 9 = 3^2$

$n=4$ $\quad 1+3+5+7 = 16 = 4^2$

$\left.\right\} n^2$?

So far the pattern is true, but this is not sufficient to claim that this is true for every n. How can we prove this?

Think of row of dominos standing on end, imagine such a row that went on forever. Say the first domino is domino 1, the second 2, and so on. What happens when a domino falls over – it knocks over the next domino, so if domino k falls over, domino $k+1$ also falls over. Since domino $k+1$ falls over domino $k+2$ also falls over, and so on.

We can express what happens using rules of inference:

Let $P(k)$: "domino k falls over"

We argue:

$$\begin{array}{l} P(1) \\ \forall k\,(P(k) \to P(k+1)) \\ \hline \therefore \forall n\, P(n) \end{array}$$

– all dominos fall over is our conclusion.

Intuitively this makes sense and is valid:

① $P(1)$
② $\forall K\,(P(K) \rightarrow P(K+1))$ $\quad\therefore \forall n\, P(n)$

③ $P(1) \rightarrow P(2)$ UI ②
④ $P(2)$ MP ①③
⑤ $P(2) \rightarrow P(3)$ UI ②.
⑥ $P(3)$ MP ④⑤.
⑦ $P(3) \rightarrow P(4)$ UI ② . . .

⋮

(?) $\underbrace{P(1) \wedge P(2) \wedge P(3) \wedge P(4)}_{\forall n\, P(n)}$ Conj.

$\forall n\, P(n)$ – definition of $\forall$

This gives us a proof technique when we want to prove $\forall x\, P(x)$ and the univese of discourse is the natural numbers (works if we start at zero too). To summarize:

$$\left[P(1) \wedge \forall K(P(K) \rightarrow P(K+1))\right] \longrightarrow \forall n\, P(n)$$

Universal Generalization.

Why do we need this?

- before we know how to prove $\forall x(A(x) \rightarrow B(x))$, since we could pick an arbitrary x and attempt a direct proof; but that doesn't always work <u>easily</u>.
- now we converted a proof of $\forall n P(n)$ into an implication, so we can use a direct proof. By making an assumption we get more leverage.

To show $\forall n P(n)$, we just assume the hypothesis of the implication is true, we prove the implication holds (is true) and thus the conclusion is true. We must also prove that $P(1)$ holds!

Proving $P(1)$ is the <u>BASIS STEP</u>.

Proving $P(k) \rightarrow P(k+1)$ is the <u>INDUCTIVE STEP</u>.

↳ we are doing this for some <u>arbitrary</u> k (as in Universal Generalization). Typically we can use a direct proof, so we call $P(k)$ the INDUCTION HYPOTHESIS, and assume it to be true in order to prove $P(k+1)$.

→ we are not assuming $P(k)$ is true for <u>all</u> positive integers (this is circular reasoning) we are only assuming that $P(k)$ is true for an arbitrary k, in the same way we do for a regular direct proof of an implication.

Now, lets try to prove our guess that the sum of the first 'n' positive odd integers is n^2.

Let $P(n)$ = "the sum of the first n positive odd integers is n^2"

We want $\forall n P(n)$ where domain is $\mathbb{Z}^+$.

<u>BASIS STEP</u>: Show that $P(1)$. $P(1)$ says that the sum of the first 1 positive odd integers is $1^2 = 1$. This is true.

<u>INDUCTIVE HYPOTHESIS</u>: Assume $P(k)$ for an arbitrary k: the sum of the first k positive odd integers is k^2

$$1 + 3 + 5 + 7 + \dots (2k-1) = k^2$$

recall the k^{th} odd number is $2k-1$.

<u>INDUCTIVE STEP</u>: We must show $P(k+1)$ is true using the inductive hypothesis.

$P(k+1)$ is true if the sum of the first $k+1$ positive odd integers is $(k+1)^2$, so lets look at the first $k+1$ positive odd integers.

$$1 + 3 + 5 + 7 + \cdots\cdots + \underset{k}{\underset{\uparrow}{2k-1}} + \underset{k+1}{\underset{\uparrow}{2k+1}} \quad (*)$$

By our inductive hypothesis. $1 + 3 + 5 + \cdots + 2k - 1 = k^2$
so the above equation is equal to:

$$k^2 + 2k + 1$$

By factoring this we get $(k+1)^2$, so the sum of the first $k+1$ positive odd integers is $(k+1)^2$. So $P(k+1)$ is true under the assumption $P(k)$. So $P(k) \rightarrow P(k+1)$.
Since k was arbitrary, $\forall k\,(P(k) \rightarrow P(k+1))$ is true.

An alternate way to look at this. If our implication is true $P(k+1) = (k+1)^2$
We assume $P(k) = k^2$.
Given $P(k)$ we know $P(k+1) = P(k) + \underbrace{2(k+1) - 1}_{\text{the } (k+1)^{th} \text{ odd integer}}$
$= k^2 + 2k + 2 - 1$
$\equiv k^2 + 2k + 2 - 1$
$= k^2 + 2k + 1$
$= (k+1)^2$

By the basis step we already have $P(1)$. By the inductive step we have $\forall k(P(k) \rightarrow P(k+1))$, so $P(1) \wedge \forall k(P(k) \rightarrow P(k+1))$ is true. Thus the principle of mathematical induction tells us $\forall n P(n)$ as we had hoped.

Notes

Remember the structure: Basis Step, Inductive Hypothesis, Inductive Step, label them - it will help keep things straight.
It is not necessary to define a function using quantifiers and predicates, but you can, however don't use them unless you explicitly state their meanings.

Induction works on inequalities too.

Ex: Prove $n < 2^n$ for all positive integers n.

BASIS STEP: $n = 1$, so $1 < 2^1 = 2$ which is true.

INDUCTIVE HYP: Assume $k < 2^k$ for some positive integer k.

INDUCTIVE STEP: We must show $k+1 < 2^{k+1}$.

$$
\begin{aligned}
k + 1 &< 2^k + 1 \quad (\text{since } 1 = 1 \text{ and } k < 2^k) \\
&< 2^k + 2^k \quad (\text{since } 2^k > 1 \text{ for } k > 0) \\
&= 2 \cdot 2^k \\
&= 2^1 \cdot 2^k = 2^{k+1}
\end{aligned}
$$

More Notes:

1. write out what it is you must do in the inductive and basis steps.
2. In the inductive step you must prove $P(k+1)$: thus you cannot assume it anywhere. Notice that in the last proof we started with one side of the inequality and derived the other – we didn't take $P(k+1)$ and simplify to change it to $P(k)$ this is the wrong direction.

How do you know when to use mathematical induction? Look for statements like "for all positive integers" and other signs of universal quantification where you don't get anywhere by just proving it by picking an arbitrary n and showing $P(n)$ and then applying universal generalization

We can show things other than quantifiers/inequalities too: a[illegible] the.

Ex: Show $n^3 - n$ is divisible by 3 for all positive integers n.

Basis Step: $(n=1)$ $1^3 - 1 = 0 = 3 \cdot 0$. so it is divisible by 3.

Inductive Hyp: Assume $k^3 - k$ is divisible by 3, for some positive integer k.

Inductive Step: We must show $=(k+1)^3 - (k+1)$ is divisible by 3.

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

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

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

$$= \underbrace{(k^3 - k)}_{\text{divisible by 3 due to inductive hypothesis}} + 3(\underset{\uparrow \text{ divisible by 3.}}{k^2 + k})$$

There is nothing special about starting at 1, we can start at __any__ integer b and by using b in our basis step we will show $\forall n P(n)$ where domain is all integers $\geq b$ ... $\{b, b+1, b+2, \ldots\}$.

Ex: Show $1 + 2 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 1$ for all $\mathbb{Z}^+$.

BASIS STEP: 0 is smallest non-negative integer. $2^0 = 0$ and $2^{0+1} - 1 = 2^1 - 1 = 2 - 1 = 1$ so basis step is proven.

INDUCTIVE HYP: Assume $1^0 + 2^1 + 2^2 + 2^3 + \dots 2^k = 2^{k+1} - 1$

INDUCTIVE STEP: we must show that

$$\underbrace{1^0 + 2^1 + 2^2 + \dots 2^k + 2^{k+1}}_{2^{k+1} - 1 + 2^{k+1}} = 2^{(k+1)+1} - 1 = 2^{k+2} - 1$$

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

Recall that the sum of a geometric sequence:

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \dots + a^n$$

Show that $\displaystyle\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}$ for $r \neq 1$ and $\mathbb{Z}^+$.

BASIS STEP $(n = 0)$

$$\sum_{j=0}^{0} ar^0 = 0 \qquad \frac{ar^1 - a}{r-1} = \frac{ar - a}{r-1} = \frac{a(r-1)}{r-1} = a$$

So $P(0)$ is true...

INDUCTIVE HYPOTHESIS:

not, this is from the formula, this is not $k+1$

Assume $\displaystyle\sum_{j=0}^{k} ar^j = \frac{ar^{k+1} - a}{r-1}$ for some non-negative k.

INDUCTIVE STEP

We want to show $\displaystyle\sum_{j=0}^{k+1} ar^j = \frac{ar^{(k+1)+1} - a}{r-1} = \frac{ar^{k+2} - a}{r-1}$

$$\sum_{j=0}^{k+1} ar^j = \sum_{j=0}^{k} ar^j + ar^{k+1}$$

$$= \frac{ar^{k+1} - a}{r-1} + ar^{k+1}$$

$$= \frac{ar^{k+1} - a}{r-1} + \frac{ar^{k+1}(r-1)}{r-1}$$

$$= \frac{\cancel{ar^{k+1}} - a + ar^{k+2} - \cancel{ar^{k+1}}}{r-1}$$

$$= \frac{ar^{k+2} - a}{r-1} \quad \text{hooray!}$$

$$\boxed{\text{BREAK TIME.}}$$

Ex:

The j^{th} Harmonic number H_j $(j \geq 1)$ is

$$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{j}$$

Show $H_{2^n} \geq 1 + \frac{n}{2}$ for non-negative integers $\mathbb{Z}^+$.

BASIS STEP: $(n=0)$ $H_{2^0} = H_1 = 1 \geq 1 + \frac{0}{2} = 1$

INDUCTIVE HYP: $H_{2^k} \geq 1 + \frac{k}{2}$ for some non-negative integer k.

INDUCTIVE STEP:

Show $H_{2^{k+1}} \geq 1 + \frac{k+1}{2}$

$$H_{2^{k+1}} = \underbrace{1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{2^k}} + \frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots \frac{1}{2^{k+1}}$$

$$= H_{2^k} + \frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots \frac{1}{2^{k+1}}$$

$$\geq \left(1 + \frac{k}{2}\right) + \underbrace{\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots \frac{1}{2^{k+1}}}_{2^k \text{ terms} - 2\cdot 2^k}$$

$$\geq \left(1 + \frac{k}{2}\right) + 2^k\left(\frac{1}{2^{k+1}}\right)$$

{recall, I can replace any term with something bigger since I want to show the RHS is less than $H_{2^{k+1}}$.

$$\geq 1 + \frac{k}{2} + \frac{2^k}{2^{k+1}}$$

$$\equiv 1 + \frac{k}{2} + \frac{1}{2} = 1 + \frac{k+1}{2}$$

$\boxed{\text{Trivia: this shows that this sum diverges as } n \to \infty}$

SETS

Ex: Recall that the size of a powerset of a set of size n is 2^n (Power set $P\{S\}$ - set of all subsets of S). How do we prove this.

Basis Step: $n=0$. If $n=0$ then the set is empty and thus the only subset is the empty set $\emptyset$. Thus there is $2^0 = 1$ subset.

Inductive Hyp: The powerset of a set of size k is 2^k for some non-negative integer k.

Induction Step: Let T be a set of $k+1$ elements, where we write $T = S \cup \{a\}$ where $a \in T$ and $S = T \setminus \{a\}$

Assume that $|S| = 2^k$

Now, consider the 2^k subsets of S, when we create the set T by adding $\{a\}$, then for each subset of S, denote X ($X \subseteq S$). there will be two subsets in T, X and $X \cup \{a\}$.

Since each X is distinct, each $X \cup \{a\}$ is distinct. since $\{a\} \notin S$.

Now recall $|T| = k+1$, $|S| = k$. So there are 2^k subsets in S, and each results in 2 new subsets in T, so $2 \cdot 2^k = 2^{k+1}$ is the number of subsets of T.

Summuction

Ex: Recall the sum of the first n positive integers is $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Prove!

BASIS: $(n=1)$, $\sum_{i=1}^{1} 1 = 1$, $\frac{1(1+1)}{2} = \frac{2}{2} = 1$

INDUCTIVE HYPOTHESIS: Assume $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, for some $k \in \mathbb{Z}^+$

INDUCTIVE STEP: $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + k+1$ and $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2}$

$$= \frac{k(k+1)}{2} + k+1 = \frac{k^2+k+2k+2}{2}$$

$$= \frac{k^2+3k+2}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

done!

Ex: Show that $2^n < n!$ for $\mathbb{Z}^+, n \geq 4$

Basis: $2^4 = 16 \qquad 4 \times 3 \times 2 \times 1 = 24. \qquad 16 < 24.$

Ind Hyp: Assume $2^k < k!$ for some $k \geq 4$.

Ind Step: Show $2^{k+1} < (k+1)!$

$$\begin{aligned} 2^{k+1} = 2 \cdot 2^k &\underset{\text{by Ind. Hyp.}}{<} 2 \cdot k! \\ &< (k+1) \cdot k! \quad (\text{Since } k+1 > 2 \\ &= (k+1)! \end{aligned}$$

Back to sets, show that

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$$ where $A_1, \ldots A_n$ are sets and $n \geq 2$.

recall this is the negation of the intersection of the sets.

this is the union of negation of the individual sets.

Basis Step: $(n=2)$ $\overline{\bigcap_{j=1}^{2} A_j} = \overline{A_1 \cap A_2} \equiv \overline{A_1} \cup \overline{A_2}$ - De Morgans

$$\equiv \bigcup \overline{A_1}$$

Inductive Hyp: Assume $\overline{\bigcap_{j=1}^{k} A_j} = \bigcup_{j=1}^{k} \overline{A_j}$ for some $k \geq 2$.

Inductive Step: $\overline{\bigcap_{j=1}^{k+1} A_j} = \overline{\bigcap_{j=1}^{k} A_j \cap A_{k+1}}$ By Defn.

$= \overline{\bigcap_{j=1}^{k} A_j} \cup \overline{A_{k+1}}$ De Morgans

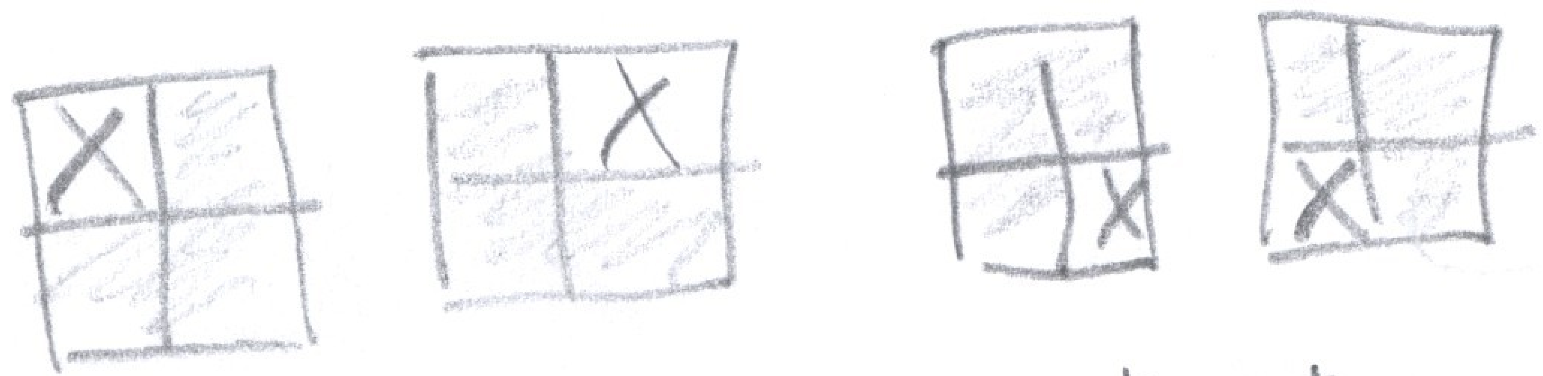
$$= \bigcup_{j=1}^{k} \overline{A_j} \cup \overline{A_{k+1}}$$ – By Inductive Hypothesis

$$= \bigcup_{j=1}^{k+1} A_j$$ By Defn.

Mathematical induction can also be used in many other creative ways.

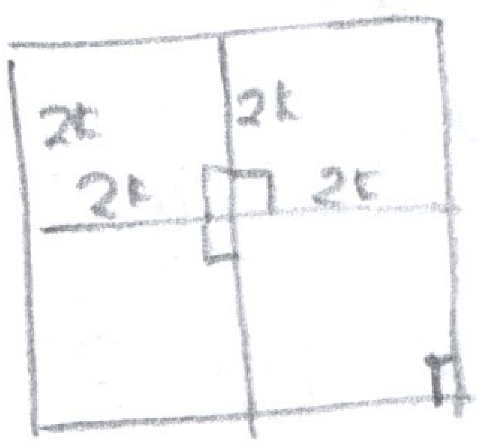
Let n be a positive integer. Show that any $2^n \times 2^n$ checkerboard with one square removed can be tiled with L shaped peices covering 3 squares. (Right triominos)

<u>Basis Step</u>: $n = 1$



<u>Ind Hyp</u>: Assume that any $2^k \times 2^k$ checkerboard w̄ one square removed can be tiled with triominos (L-shaped).

<u>Inductive Step</u>: Consider a $2^{k+1} \times 2^{k+1}$ board it is composed of 4, $2^k \times 2^k$ boards.



Say the missing square falls in the lower right $2^k \times 2^k$ board (and we put it in the lower right corner

By the inductive hyp. the lower right can be tiled.

Now we arrange the 3 remaining boards so that thier missing cells meet at the centre. We can place a single triomino to cover these three squares. We now have a $2^{k+1} \times 2^{k+1}$ with a single missing square.

Ex: Prove that given $n \geq 2$ lines in the plane (no two of which are parallel), the total # of intersections is at most $\frac{n(n+1)}{2}$.

(Recall any two non-parallel lines intersect in exactly one point)

Basis step: $n=2$ By the above they intersect at 1 point and

$$\frac{2(2+1)}{2} = 3 > 1.$$

Inductive Hyp: Total # of intersections of k lines is $\leq \frac{k(k+1)}{2}$.

Inductive Step: Consider the collection of k lines, by the IH there are $\frac{k(k+1)}{2}$ intersections. Now insert a new line, it is not parallel to any other line so it intersects the other k lines, for k new intersections.

$$\frac{k(k+1)}{2} + k = \frac{k(k+1)}{2} + \frac{2k}{2}$$

$$= \frac{k^2+3k}{2}$$

$$\leq \frac{k^2+3k+2}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

Recall.

$$\boxed{\frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2}.}$$

Strong Induction

Recall that our argument for Mathematical Induction was

① $P(1)$

② $\forall k\,(P(k) \rightarrow P(k+1)) \quad \therefore \forall n\, P(n)$

---

③ $P(1) \rightarrow P(2)$ UI ②

④ $P(2)$ MP ① ③.

⑤ $P(2) \rightarrow P(3)$ UI ②

⑥ $P(3)$ MP ④ ⑤

⋮

and so on.

Notice that when proving $P(k+1)$ we actually know $P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ is true, so we can use $P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ as our induction hypothesis to prove that $P(k+1)$ is true. This can be easier, though they are equivalent in theory.

Ex: If $n > 1$, the n can be written as the product of primes.

Basis Step: $n = 2$, $2 \cdot 1 = 2$ so 2 can be written as the product of two primes.

Ind Hyp: Assume $n = 1 < j \leq k$ can be written as the product of primes for some k.

Inductive Step: Must show $k+1$ can be written as product of primes.

Case 1: $k+1$ is prime, done $\quad 1 \cdot (k+1)$

Case 2: $k+1$ is not prime. Then $k+1 = a \cdot b$ where $2 \leq a \leq b < k+1$, by the inductive hypothesis both a and b are products of primes.

$$a = p_1 p_2 \ldots p_i \quad b = q_1 q_2 \ldots q_z$$

$$k+1 = p_1 p_2 \cdots p_i \cdot q_1 \cdot \ldots \cdot q_z$$ & is a product of primes.

EX: Consider a game: two players & two piles of matches. Starting w/ player 1 a player can remove <u>any</u> number of matches from one pile OR the other. The player removing the last match wins. Piles start with an equal number of matches with $n \geq 1$. Show that the player 2 can always win.

BASIS: ($n=1$ - 1 in each pile) Player 1 has one choice remove one match from one pile, leaving player 2 to pick up the other match and win.

INDUCTIVE HYP: If there are $1 \leq j \leq k$ matches in each pile, player 2 always has a winning strategy.

INDUCTIVE STEP: Suppose we have 2 equal piles of $k+1$ matches. Player 1 removes $r \geq 1$ matches from one of the piles, leaving $j = k+1-r \leq k$ matches in the pile. Player 2 removes r matches from the other pile, so it too has j matches. So now we have a game with j matches, but player 2 has a winning strategy for any game with $1 \leq j \leq k$ matches (by I.H.).

Some problems can be solved with either technique.

Ex: Prove that every amount of postage $\geq 12¢$ can be formed using $4¢$ and $5¢$ stamps.

	INDUCTION	STRONG INDUCTION
BASIS STEP:	$12¢$ formed by $3 \times 4¢$	$12¢ = 3 \times 4¢$ $P(12)$ $13¢ = 2 \times 4¢, 1 \times 5¢$ $P(13)$ $14¢ = 2 \times 5¢, 1 \times 4¢$ $P(14)$ $15¢ = 3 \times 5¢$ $P(15)$

	MATH INDUCTION	STRONG INDUCTION
IND HYP:	Assume that postage of k¢ can be formed using 4¢ and 5¢ stamps for $k \geq 12$.	Assume we can form postage of j cents for $12 \leq j \leq k$ for $k \geq 15$.
IND. STEP:	Now, $k+1$ cents. ① if a 4¢ stamp was used then we can replace it w/ a 5¢ stamp and we are done. ② if no 4¢ stamp was used, then there must be at least 3×5¢ stamps for any $k \geq 10$, so replace 3×5¢ with 4×4¢ to get $k+1$	Use stamps for $j = k-3$ cents and add a 4¢ stamp.

Note that the Strong Induction proof is a bit 'easier' to understand.

Recursive Definitions

Recursively defined functions are similar to induction, you first specify the function at a few small values and then define the function at one value in terms of the function at smaller values.

EX: Let f be defined by:

$$f(0) = 2$$
$$f(n+1) = 2 \cdot f(n) + 4$$

$$f(1) = 2 \cdot f(0) + 4 = 8$$
$$f(2) = 2 \cdot f(1) + 4 = 20$$
$$f(3) = 2 \cdot f(2) + 4 = 44$$
$$f(4) = 2 \cdot f(3) + 4 = 92$$

The Factorial function can be defined by

$f(0) = 1$ $\quad\quad 0! = 1$

$f(n+1) = n+1 \cdot f(n)$ $\quad\quad (n+1)! = (n+1) \cdot n!$

Sometimes a value is a combination of two (or more) smaller values (or functions of smaller values)

Ex: The Fibonacci numbers $f(0) = 0$ $f(1) = 1$

$f(n+1) = f(n) + f(n-1)$ where $n \geq 1$.

or more often we see

Use this

$f_n = f_{n-1} + f_{n-2}$ where $n \geq 2$.

$f_2 = f_1 + f_0 = 1 + 0 = 1$

$f_3 = f_2 + f_1 = 1 + 1 = 2$

$f_4 = f_3 + f_2 = 2 + 1 = 3$

$f_5 = f_4 + f_3 = 3 + 2 = 5$

$f_6 = f_5 + f_4 = 5 + 3 = 8$

We can also define sets recursively!

Give one (or more) base elements in the set, and recursively define additional elements in terms of elements already in the sets:

$S = \{3\}$

RECURSIVE STEP: If $x \in S$ and $y \in S$ then $(x+y) \in S$.

So $3 + 3 = 6$ is in the set

$3 + 6 = 9$, $6 + 6 = 12$ are in the set. (as is $6+3=9$)

and so on - ends up as the set of all #s divisible by 3.

[It would be a good strong induction question to prove this holds ...]

We can even use recursion to define what a compound propositional formula should look like.

T, F, p are well formed formulas (p is a propositional variable).

IF Z and W are well formed formula then

$$(\neg Z),\ (Z \vee W),\ (Z \wedge W),\ (Z \rightarrow W),\ (Z \leftrightarrow W)$$

are also well formed...

i.e. you can never end up with

$p \neg \vee q$ using these rules.

$\boxed{\text{END LECTURE \#6}}$