PUTNAM SEMINAR WEEK 2

INVARIANTS, SEMI-INVARIANTS, ALGEBRAIC IDENTITIES

AN INVARIANT OF A SYSTEM IS A PRESERVED QUANTITY.

- E.G. ENERGY, MOMENTUM IN CLASSICAL MECHANICS.

A SEMI-INVARIANT CHANGES IN ONLY 1 WAY (INCR/DECR) EX: ENTROPY.

EXAMPLE:

SUPPOSE GIVEN n MARKERS IN A LINE, 1-SIDE W, 1-SIDE BLACK

INITIALLY ALL WHITE-SIDE UP.

A MOVE CONSISTS OF TAKING AWAY A WHITE CHIP, NOT AN ENDPT, AND FLIPPING THE 2 NEIGHBORS.

Q: CAN YOU END WITH 2 CHIPS LEFT?

1ST INVARIANT:

NOTICE THE NUMBER OF BLACK CHIPS ALWAYS CHANGES BY A MULT. OF 2, AND HENCE IS ALWAYS EVEN.

THIS MEANS, IF WE END WITH ONLY 2 CHIPS, BOTH WHITE OR BOTH BLACK

2ND INVARIANT: GIVEN A WHITE CHIP, LET t BE THE NUMBER OF BLACK CHIPS THAT PRECEEDS IT

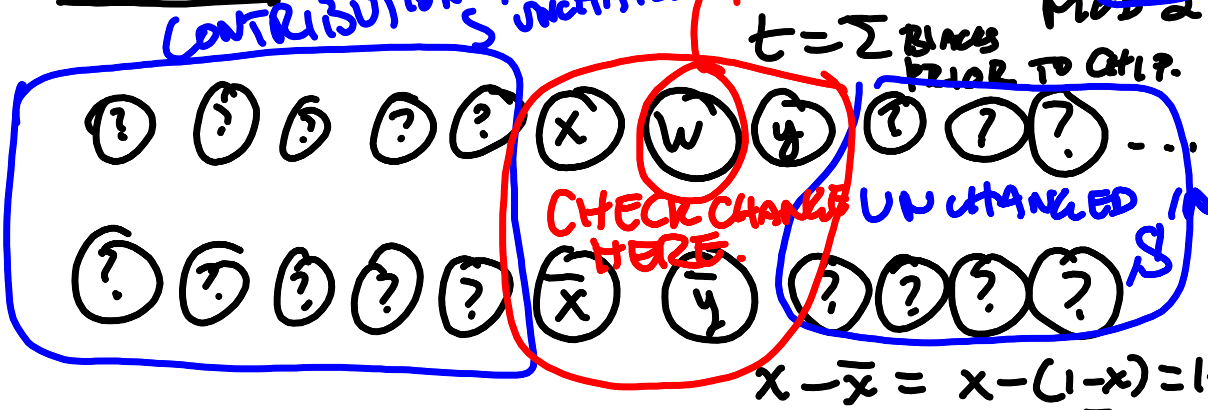
$$S = \sum_{\text{WHITE CHIPS } C} (-1)^{t(C)}$$

CLAIM: S MODULO 3 IS AN INVARIANT.

PROOF: $\bar{x} = 1-x$ $W=0$
$\bar{y} = 1-y$ $B=1$

$x-\bar{x} \equiv y-\bar{y}$ MOD 2
$x+y \equiv \bar{x}+\bar{y}$ MOD 2 ✓

$t = \Sigma$ BLACKS PRIOR TO CHIP.



$x-\bar{x} = x-(1-x) = 1-2x$
$\equiv 1$ MOD 2
$\equiv y-\bar{y}$

4 POSSIBILITIES: ΔS

$x=W$ $y=W$: $-(-1)^t - (-1)^t - (-1)^t$

$B=\bar{x}$ $x=W$ $y=B$ ($\bar{y}=W$): $-(-1)^t - (-1)^t + (-1)^{t+1}$

$x=B$ $y=W$: $-(-1)^t + (-1)^{t+1} - (-1)^t$

$x=B$ $y=B$: $-(-1)^t + (-1)^{t+1} + (-1)^{t+1}$

$-(-1)^t$ COMES FROM LOSING W.

EACH OF THESE TERMS IS
$= -(-1)^t \cdot 3 \equiv 0$ MOD 3.

WE'VE SHOWN:

S MOD 3 IS AN INVARIANT.

W W $\quad S = (-1)^0 + (-1)^0 = 2$

B B $\quad S = 0.$

TO END IN EITHER CONFIG,

$S \equiv 0$ OR 2 MOD 3.

GIVEN n WHITE CHIPS

$\underbrace{\text{W W} \cdots \text{W}}_{n}$ $\quad (-1)^t = 1$ EACH CHIP.

$S = n.$

THUS, A CONDITION TO REACH THE FINAL OUTCOME IS

$n \equiv 0$ OR 2 MOD 3.

EXAMPLES:

n=3: W W W $\longmapsto$ B B

n=5; W W W W W

B B W W

B W B

W W.

BOTH SOLVABLE

IN GENERAL: n CIRCS

W W W W W [W - - - -]

B B W W (W - -)

B W B (W - - -)

W W [W - - -]

GIVEN n WHITES, CAN PASS TO n-3 WHITES.

THIS SHOWS THAT

$n \equiv 0,2 \bmod 3$ IS A SUFFICIENT CONDITION.

EXAMPLE: GIVEN 3 NUMBERS (a, b, c), PERFORM AN OP, PICK TWO, E.G. a, b, REPLACE THEM WITH $\frac{a+b}{\sqrt{2}}, \frac{a-b}{\sqrt{2}}$.

Qn: CAN WE MOVE FROM $(1, \sqrt{2}, 1+\sqrt{2})$ TO $(2, \sqrt{2}, \frac{1}{\sqrt{2}})$?

Ans: INVARIANT: $a^2+b^2+c^2$.

PF: BEFORE $a^2+b^2+c^2$

AFTER $\left(\frac{a+b}{\sqrt{2}}\right)^2+\left(\frac{a-b}{\sqrt{2}}\right)^2+c^2$

$$= \frac{a^2+2ab+b^2}{2} + \frac{a^2-2ab+b^2}{2} + c^2$$

$$= a^2+b^2+c^2$$

$I(1, \sqrt{2}, 1+\sqrt{2}) = 1+2+1+2 \cancel{\ } +2\sqrt{2}$

$I(2, \sqrt{2}, \frac{1}{\sqrt{2}}) = 4+2+\frac{1}{2}$

ALGEBRAIC IDENTITIES:

HINT FOR PROBLEMS:

ITS SOMETIMES POSSIBLE TO FACTOR A POLYNOMIAL BY WRITING IT AS A DIFF OF TWO SQUARES.

$$x^2+6x+5 = (x+3)^2 - 2^2$$
$$= (x+5)(x+1).$$

$$a^2+b^2 = (a+ib)(a-ib).$$

IF $n = a^2+b^2$, $m = c^2+d^2$.

$$(a+ib)(c+id) = (ac-bd) + i(bc+ad)$$

$$\Longrightarrow mn = (ac-bd)^2 + (bc+ad)^2.$$

<u>SUMS OF 4 SQUARES:</u>

QUATERNIONS $\mathbb{H}$: q: $a+ib+jc+kd$
$a,b,c,d \in \mathbb{Z}$.

<u>NON-COMMUTATIVE RING</u>

$i \cdot j = k$, $j \cdot i = -k$.

$j \cdot k = i$, $k \cdot j = -i$. $\quad i^2 = j^2 = k^2 = -1$

$k \cdot i = j$, $i \cdot k = -j$.

EXAMPLE: IF x, y, z ARE DISTINCT,

$$(x-y)^{1/3} + (y-z)^{1/3} + (z-x)^{1/3} \neq 0.$$

SUGGESTION: TRY PROVING THIS WITH CONVEXITY / ANALYSIS.

ALGEBRAIC PROOF:

LET $a = (x-y)^{1/3}$, $b = (y-z)^{1/3}$, $c = (z-x)^{1/3}$.

SO $a^3 + b^3 + c^3 = 0$.

SUPPOSE FOR CONTRADICTION $a+b+c=0$.

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-ac-bc)$$

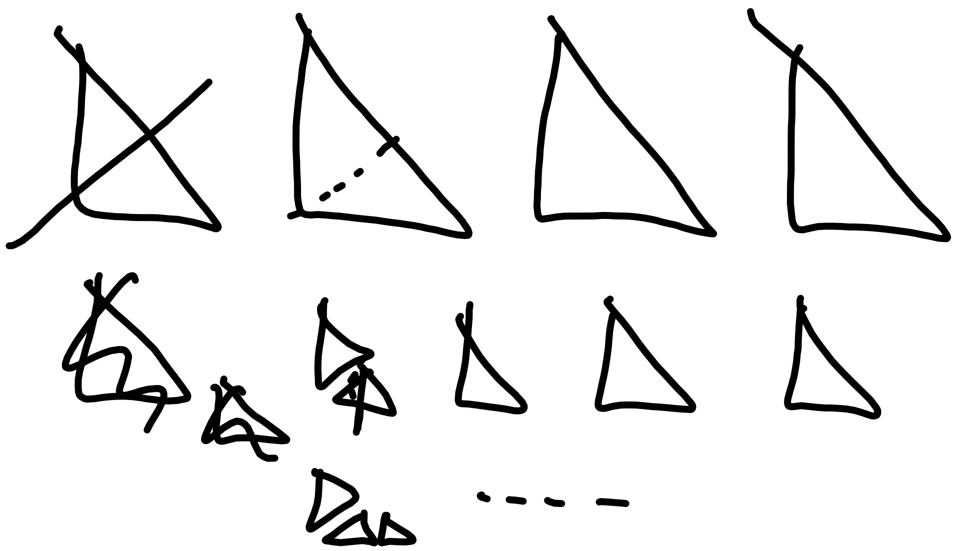
THIS MEANS: IF $(a+b+c)=0$

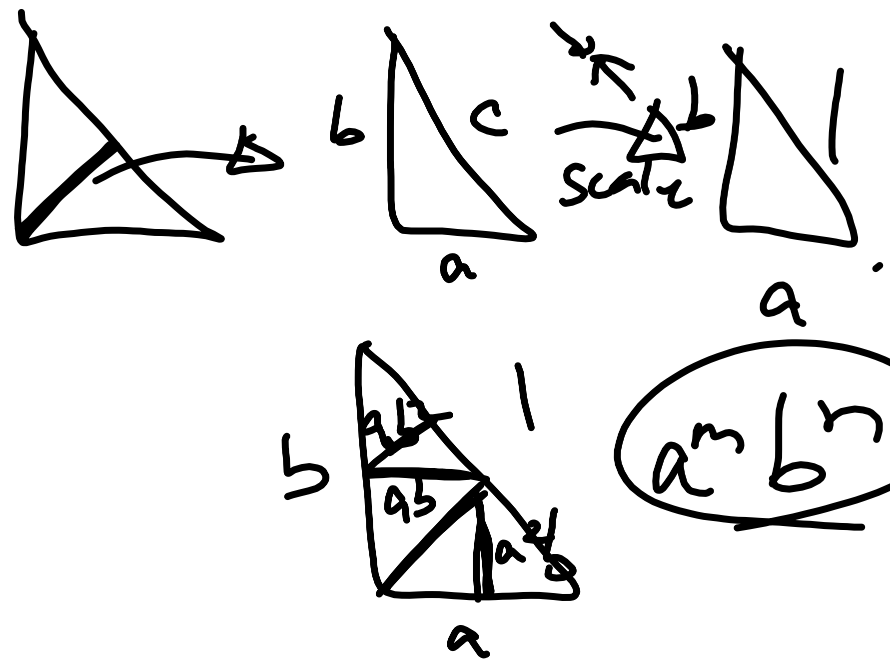
$\Longrightarrow abc=0$, SO ONE OF $a, b, c = 0 \Rightarrow x=y$ OR $x=z$ OR $y=z$.

PROBLEMS TO PRESENT;

~~2~~ ~~7~~ ~~1~~ ~~4~~ ~~13~~ 16

17 19 5



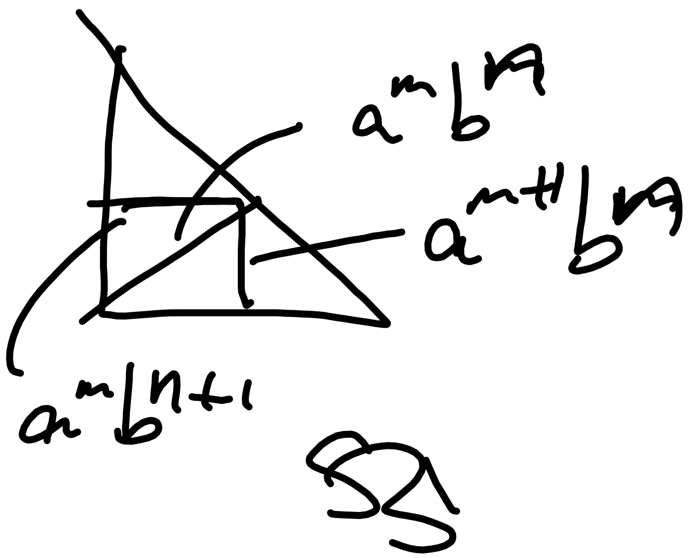


$a^m b^n$

$a^m b^n \sim (m, n)$

$m, n \geq 1$

$S = \{(1,1), (2,1)$
$(2,1), \sim\}$


a^m b^n
a^{m+1} b^n
a^m b^{n+1}

$$(a_1 + b_1 i + c_1 j + d_1 k)$$
$$(a_2 + b_2 i + c_2 j + d_2 k)$$

FOIL:

$$a_1 a_2 + a_1 b_2 i + a_1 c_2 j + a_1 d_2 k$$
$$+ b_1 a_2 i + b_1 b_2 \underbrace{i^2}_{-1} + b_1 c_2 \underbrace{ij}_{k} + b_1 d_2 \underbrace{ik}_{-j}$$
$$+ c_1 a_2 j + c_1 b_2 \underbrace{j \cdot i}_{-k} + c_1 c_2 \underbrace{j^2}_{-1} + c_1 d_2 \underbrace{jk}_{i}$$
$$+ d_1 a_2 k + d_1 b_2 \underbrace{ki}_{j} + d_1 c_2 \underbrace{kj}_{-i} + d_1 d_2 \underbrace{k^2}_{-1}$$

$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2)$$
$$+ (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i$$
$$+ (a_1 c_2 + c_1 a_2 - b_1 d_2 + d_1 b_2) j$$
$$+ (a_1 d_2 + a_2 d_1 + b_1 c_2 - b_2 c_1) k.$$

$$N(a + ib + jc + kd) = a^2 + b^2 + c^2 + d^2$$

ONE CAN SHOW $N(q_1 q_2) = N(q_1) N(q_2)$

SO IF m, n ARE SUMS OF 4 SQUARES, SO IS mn.

THIS IS FREQUENTLY USED TO PROVE LAGRANGE'S THM: ALL IN ARE A SUM OF 4 SQUARES

$$S \mapsto S \setminus \{(m,n)\} \cup \{(m,n+1),(m+1,n)\}$$

$$w : \mathbb{Z}^2 \longrightarrow \mathbb{R}$$

$$w(h,k) = \frac{1}{2^{h+k}}.$$

$$w(m,n) = \frac{1}{2^{m+n}},$$

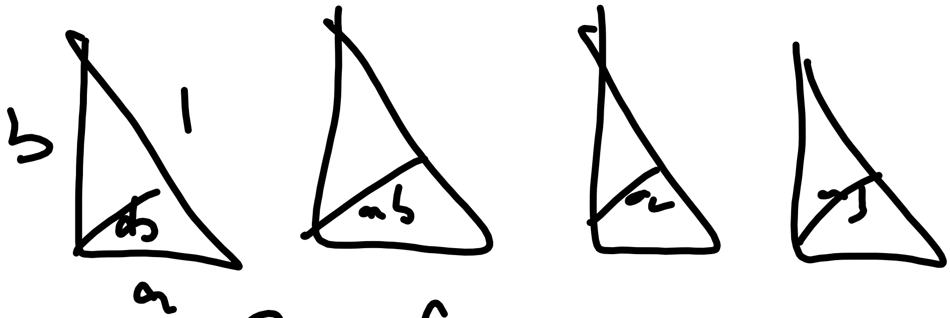
$$W(m,n+1)+W(m+1,n)$$

$$=\frac{1}{2^{m+n+1}}+\frac{1}{2^{m+1+n}}$$

$$=\frac{1}{2}\cdot\left(\frac{1}{2^{m+n}}+\frac{1}{2^{m+n}}\right)=\frac{1}{2^{m+n}}$$

$$\sum_{(h,k)\in S} W(h,k) = \sum S$$

$\sum$ initial.



$S = \{(1,1), (1,1), (1,1), (1,1)\}$

$\sum S = \sum \frac{1}{2^n} = 1$

$S \leftarrow_{(m,n)}$

$$\sum S = \sum_{(h,k)\in S} W(h,k)$$

$$= \sum_{(h,k)\in S} \frac{1}{2^{h+k}}$$

$$< \sum_{h,k=1}^{\infty} \frac{1}{2^{h+k}}$$

$$= \sum_{h=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{2^{h+k}}$$

$$\sum_{n=1}^{\infty} \frac{1}{2^n} \sum_{k=1}^{\infty} \frac{1}{2^k}$$

!

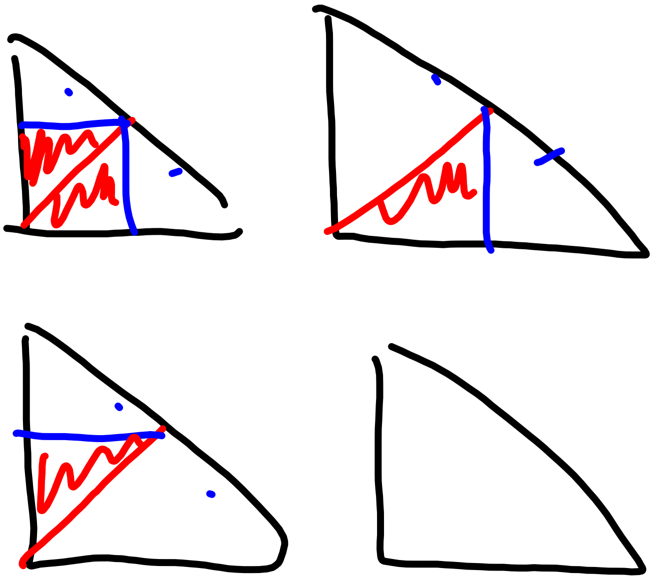
$$= \sum = 1.$$

$$\sum S \neq 1$$

① (m, n, m, n)

$$\dot{v}(x, y, u, v) = xv + yu$$

$$\dot{v}(x, y-x, u, v+u) = xv + \cancel{xu} + yu - \cancel{xu}$$



REPEAT
IN THE
4 SMALLER
TRIANGLES.
$\Rightarrow$ CONCLUSION
BY DESCENT.

7 SHOW ∞-MANY $a > 0$ SO THAT $n^4 + a$ IS NEVER PRIME.

WRITE $n^4 + a =$

$$n^4 + 4n^2 + 4 = (n^2+2)^2$$

$$\rightarrow \quad n^4 + 4 = (n^2+2)^2 - 4n^2$$
$$= (n^2+2n+2)(n^2-2n+2)$$

$$\qquad\qquad\qquad\qquad\qquad = (n-1)^2+1$$

DIFFICULTY AT $n=1$, $n>1$ NOT PRIME.

CONSIDER:

$$(n^2+2k^2)^2 = n^4+4k^2n^2+4k^4$$

$$\Rightarrow n^4+4k^4 = (n^2+2k^2)^2 - 4k^2n^2$$

$$\Rightarrow n^4+4k^4 = (n^2-2kn+2k^2)(n^2+2kn+2k^2).$$

LET $k \geq 1$. WE REQUIRE

FOR ALL n, $n^2-2kn+2k^2 \neq 1$

$(n-k)^2+k^2$ SO OK IF $k>1$ $\square$

$$n^4 + 2\sqrt{a}\,n^2 + a - 2\sqrt{a}\,n^2$$

$$= (n^2 - \sqrt{a})^2 - 2\sqrt{a}\,n^2$$

$$= (n^2 - \sqrt{a} - \sqrt{2\sqrt{a}}\,n)(n^2 - \sqrt{a} + \sqrt{2\sqrt{a}}\,n)$$

1 (x, y, u, v)

(m, n, m, n)

$\gcd(m,n)\,\mathrm{lcm}(m,n) = mn$

$$v(x-y, y, u+v, v)$$

$$= xv - \cancel{yv} + yu + \cancel{yv}$$

$$= xv + yu$$

$$(m,n,m,n) \sim (\gcd(m,n), \gcd(m,n), u, v)$$

$2mn = \gcd(m,n)\,(u+v)$

$u+v = 2\,\mathrm{lcm}(m,n)$

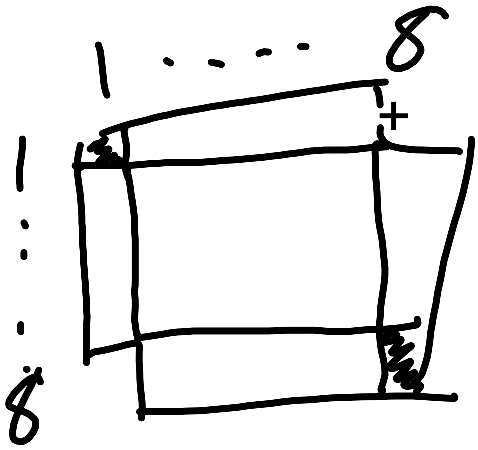
$\frac{u+v}{2} =$

4 $(n+3)(n^2+3n+3)$

$= n^3+6n^2+12n+9$

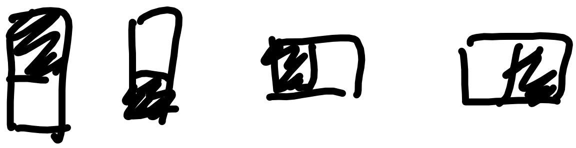
$= n^3+6n^2+12n+8+1$

$= (n+2)^3+1$



$B=32$
$W=32$

$B=32$ $\quad$ $B=2$
$W=30 \rightarrow W=0$



RECALL: THE FUNDAMENTAL THM OF ALGEBRA SAYS THAT, OVER $\mathbb{C}$ A POLYNOMIAL $P(x)$ FACTORS AS

$$P(x) = A(x-x_1)(x-x_2)\cdots(x-x_n).$$

OVER $\mathbb{R}$ ANY COMPLEX ROOTS COME IN COMPLEX CONJ. PAIRS

$P(x) = \overline{P(x)}$ IF x REAL $x_i \notin \mathbb{R}$ $\overline{x_i}$ IS ALSO A ROOT.

$x_i = a + bi$

$$(x-x_i)(x-\overline{x_i}) = (x-a)^2 + b^2$$

SUM OF TWO SQUARES.

IF $p(x)$ TAKES ONLY NON-NEG VALUES THEN IT FACTORS

AS LINEAR FACTORS

$(x-x_j)^2$ AND QUAD IRRED. FACTORS

x_j REAL

$(x-a+bi)(x-a-bi)$
$= ((x-a)^2+b^2)$

IF ODD ORDER REAL ROOT, THERE WOULD BE A SIGN CHANGE IN THE NBD OF THE ROOT.

$$P(x) = \cancel{A}(x-x_1)^2 \cdots (x-x_m)^2$$

REAL ROOTS.

$$\times\ Q_1(x) \cdots Q_j(x)$$

QUAD IRREDUCIBLES.

$Q_1, \ldots, Q_j$ ARE ALL THE SUM OF TWO SQUARES

SO THEIR PRODUCT IS ALSO BY USING $(a^2+b^2)\cdot(c^2+d^2) = N\big((a+ib)(c+id)\big)$

YOU CAN INCLUDE THE SQUARE OF THE REAL-ROOT FACTOR AS A FACTOR IN BOTH POLYNOMIALS. $\square$

16: $x_i \in \mathbb{Z}$.

$S_1 = x_1$

$S_2 = x_1 + x_2$

$S_3 = x_1 + x_2 + x_3$

$\vdots$

$S_n = x_1 + x_2 + \dots + x_n = 1$

LET $S_j = \min(S_1, \dots, S_n)$

FOR $m \geq j$ $\quad S_m - S_j \geq 0$.

CYCLE TO HAVE THE ORDER

$x_j, x_{j+1}, \dots, x_n, x_1, x_2, \dots, x_m, \dots, x_{j-1}$.

THE PARTIAL SUMS EITHER HAVE FORM $S_m - S_j \geq 0 \quad m \geq j$.

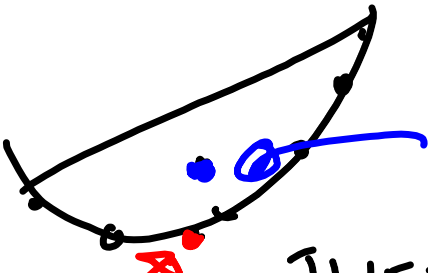
OR $S_m + S_n - S_j \quad m < j$

$= S_m + 1 - S_j > 0$

SINCE $S_m \geq S_j$. $\square$

17 JENSEN'S INEQUALITY:

LET $f(x)$ BE CONVEX



$f''(x) \geq 0$.

SECANTS ABOVE GRAPH.

THEN

$$\frac{1}{n}\left(f(x_1)+\dots+f(x_n)\right) \geq f\left(\frac{x_1+\dots+x_n}{n}\right).$$

WE WISH TO SHOW
THAT FOR $a_1, \dots, a_n \geq 0$,
$$(1+a_1)^{\frac{1}{n}}(1+a_2)^{\frac{1}{n}} \cdots (1+a_n)^{\frac{1}{n}} \geq (1+(a_1 \cdots a_n)^{1/n})$$

$a_i = e^{x_i}$ POSSIBLE SINCE $a_i \geq 0$

IF SOME $a_i = 0$, TRIVIAL, ASSUME $a_i > 0$.

WISH TO SHOW, AFTER TAKING logs.
$$\frac{1}{n}\left(\log(1+e^{x_1}) + \dots + \log(1+e^{x_n})\right) \geq \log\left(1+e^{\frac{x_1+\dots+x_n}{n}}\right)$$

$\overline{f(x)}$ $\qquad$ $f(\bar{x})$

$$f(x) = \log(1+e^x).$$

$$f(\bar{x}) = f\left(\frac{x_1+\dots+x_n}{n}\right)$$

$$\overline{f(x)} = \frac{f(x_1)+\dots+f(x_n)}{n}.$$

BY JENSEN, SUFFICES
TO CHECK CONVEXITY.

$$f(x) = \log(1+e^x)$$

$$f'(x) = \frac{e^x}{1+e^x} = 1 - \frac{1}{1+e^x}$$

$$f''(x) = \frac{e^x}{(1+e^x)^2} > 0. \qquad \square$$