Today.

Finish up counting.

Countabiity.

Some Practice.

How many orderings of letters of CAT?

3 ways to choose first letter, 2 ways for second, 1 for last.

$\implies 3 \times 2 \times 1 = 3!$ orderings

How many orderings of the letters in ANAGRAM?

Ordered, except for A!

total orderings of 7 letters. 7!
total "extra counts" or orderings of three A's? 3!

Total orderings? $\frac{7!}{3!}$

How many orderings of MISSISSIPPI?

4 S's, 4 I's, 2 P's.
11 letters total.
$11!$ ordered objects.
$4! \times 4! \times 2!$ ordered objects per "unordered object"

$\implies \frac{11!}{4!4!2!}$.

Summary.

First rule: $n_1 \times n_2 \cdots \times n_3$.

k Samples with replacement from n items: n^k.
Sample without replacement: $\frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1)$

Second rule:
When order doesn't matter (sometimes) can divide...

Sample without replacement and order doesn't matter:
$\binom{n}{k} = \frac{n!}{(n-k)!k!}$. "$n$ choose k"

One-to-one rule: equal in number if one-to-one correspondence.
Bijection!

Sample k times n with replacement and order doesn't matter:
$\binom{k+n-1}{n-1}$.

Sampling...

Sample k items out of n

Without replacement:
Order matters: $n \times n-1 \times n-2 \ldots \times n-k+1 = \frac{n!}{(n-k)!}$
Order does not matter:
Second Rule: divide by number of orders – "k!"
$\implies \frac{n!}{(n-k)!k!}$.
"n choose k"

With Replacement.
Order matters: $n \times n \times \ldots n = n^k$
Order does not matter: Second rule ???

Problem: depends on how many of each item we chose!
Different number of unordered elts map to each unordered elt.

Unordered elt: 1,2,3 $\quad$ 3! ordered elts map to it.
Unordered elt: 1,2,2 $\quad \frac{3!}{2!}$ ordered elts map to it.

How do we deal with this mess??

Splitting 5 dollars..

How many ways can Alice, Bob, and Eve split 5 dollars.

Alice gets 3, Bob gets 1, Eve gets 1: (A, A, A, B, E).

Separate Alice's dollars from Bob's and then Bob's from Eve's.

Five dollars are five stars: $\star\star\star\star\star$.

Alice: 2, Bob: 1, Eve: 2.
Stars and Bars: $\star\star|\star|\star\star$.

Alice: 0, Bob: 1, Eve: 4.
Stars and Bars: $|\star|\star\star\star\star$.

Each split "is" a sequence of stars and bars.
Each sequence of stars and bars "is" a split.

Counting Rule: if there is a one-to-one mapping between two sets they have the same size!

Stars and Bars.

How many different 5 star and 2 bar diagrams?

$| \star | \star \star \star \star$.

7 positions in which to place the 2 bars.

$-\ -\ -\ -\ -\ -\ -$

Alice: 0; Bob 1; Eve: 4
$| \star | \star \star \star \star$.
Bars in first and third position.

Alice: 1; Bob 4; Eve: 0
$\star | \star \star \star \star |$.
Bars in second and seventh position.

$\binom{7}{2}$ ways to do so and
$\binom{7}{2}$ ways to split 5 dollars among 3 people.

Stars and Bars.

Ways to add up n numbers to sum to k? or

" k from n with replacement where order doesn't matter."

In general, k stars $n-1$ bars.

$$\star\star|\star|\cdots|\star\star.$$

$n+k-1$ positions from which to choose $n-1$ bar positions.

$$\binom{n+k-1}{n-1}$$

Or: k unordered choices from set of n possibilities with replacement.
Sample with replacement where order doesn't matter.

Counting basics.

First rule: $n_1 \times n_2 \cdots \times n_3$.

k Samples with replacement from n items: n^k.
Sample without replacement: $\frac{n!}{(n-k)!}$

Second rule: when order doesn't matter divide..when possible.

Sample without replacement and order doesn't matter: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.
"n choose k"

One-to-one rule: equal in number if one-to-one correspondence.

Sample with replacement and order doesn't matter: $\binom{k+n-1}{n-1}$.

Bijection: sums to 'k' $\rightarrow$ stars and bars.

$S = \{(n_1, n_2, n_3) : n_1 + n_2 + n_3 = 5\}$

$T = \{s \in \{'|', '\star'\} : |s| = 7, \text{number of bars in s} = 2\}$

$f((n_1, n_2, n_3)) = \star^{n_1} \quad '|' \quad \star^{n_2} \quad '|' \quad \star^{n_3}$

Bijection:
argument: unique (n_1, n_2, n_3) from any s.

$|S| = |T| = \binom{7}{2}$.

Stars and Bars Poll

Mark whats correct.
(A) ways to split n dollars among k: $\binom{n+k-1}{k-1}$
(B) ways to split k dollars among n: $\binom{k+n-1}{n-1}$
(C) ways to split 5 dollars among 3: $\binom{7}{5}$
(D) ways to split 5 dollars among 3: $\binom{5+3-1}{3-1}$

All correct.

Sum Rule

Two indistinguishable jokers in 54 card deck.
How many 5 card poker hands?
Sum rule: Can sum over disjoint sets.
No jokers "exclusive" or One Joker "exclusive" or Two Jokers

$$\binom{52}{5} + \binom{52}{4} + \binom{52}{3}.$$

Two distinguishable jokers in 54 card deck.
How many 5 card poker hands? Choose 4 cards plus one of 2 jokers!

$$\binom{52}{5} + 2 * \binom{52}{4} + \binom{52}{3}$$

Wait a minute! Same as choosing 5 cards from 54 or

$$\binom{54}{5}$$

Theorem: $\binom{54}{5} = \binom{52}{5} + 2 * \binom{52}{4} + \binom{52}{3}$.

Algebraic Proof: Why? Just why? Especially on Thursday!
Already have a **combinatorial proof.** □

Combinatorial Proofs.

Theorem: $\binom{n}{k} = \binom{n}{n-k}$

Proof: How many subsets of size k? $\binom{n}{k}$

How many subsets of size k?
Choose a subset of size $n-k$
and what's left out is a subset of size k.
Choosing a subset of size k is same
as choosing $n-k$ elements to not take.
$\Longrightarrow \binom{n}{n-k}$ subsets of size k.

□

Pascal's Triangle

0
1 1
1 2 1
1 3 3 1
1 4 6 4 1

Row n: coefficients of $(a+b)^n = (a+b)(a+b)\cdots(a+b)$.

Foil (4 terms) on steroids:
$(a+b)^2 = a^2 + ab + ba + b^2$
$aaa + aab + aba + abb + baa + bab + bba + bbb$.
2^n terms: choose 1 or x from each term $(1+x)$.

Simplify: collect all terms corresponding to x^k.
Coefficient of $a^k b^{n-k}$ $\binom{n}{k}$: choose k terms for a and $n-k$ for b.

$\binom{0}{0}$
$\binom{1}{0}$ $\binom{1}{1}$
$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$
$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$

Pascal's rule $\implies \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.
Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

Sum Rule: size of union of disjoint sets of objects.
Without and with first element $\rightarrow$ disjoint.

So, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. $\square$

Combinatorial Proof.

Theorem: $\binom{n}{k} = \binom{n-1}{k-1} + \cdots + \binom{k-1}{k-1}$.
Proof: Consider size k subset where i is the first element chosen.

$$\{1,\ldots,i,\underline{\ldots,n}\}$$

Must choose $k-1$ elements from $n-i$ remaining elements.
$\implies \binom{n-i}{k-1}$ such subsets.

Add them up to get the total number of subsets of size k which is also $\binom{n+1}{k}$. $\square$

Binomial Theorem: $x = 1$

Theorem: $2^n = \binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{0}$

Proof: How many subsets of $\{1,\ldots,n\}$?
Construct a subset with sequence of n choices:
element i **is in** or **is not** in the subset: 2 poss.
First rule of counting: $2 \times 2 \cdots \times 2 = 2^n$ subsets.

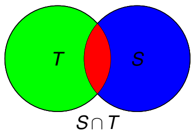
How many subsets of $\{1,\ldots,n\}$?
$\binom{n}{i}$ ways to choose i elts of $\{1,\ldots,n\}$.
Sum over i to get total number of subsets..which is also 2^n. $\square$

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$
Used to reason about all subsets
by adding number of subsets of size 1, 2, 3,...

Also reasoned about subsets that contained
or didn't contain an element. (E.g., first element, first i elements.)

Inclusion/Exclusion Rule:
For any S and T, $|S \cup T| = |S| + |T| - |S \cap T|$.



In T. $\implies |T|$
In S. $\implies + \ |S|$
Elements in $S \cap T$ are counted twice.
Subtract. $\implies -|S \cap T|$

$$|S \cup T| = |S| + |T| - |S \cap T|$$

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$
Used to reason about all subsets
by adding number of subsets of size 1, 2, 3,...

Also reasoned about subsets that contained
or didn't contain an element. (E.g., first element, first i elements.)

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.$|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

$S \cap T$ = phone numbers with 7 as first and second digit. $|S \cap T| = 10^8$.

Answer: $|S| + |T| - |S \cap T| = 10^9 + 10^9 - 10^8$.

Inclusion/Exclusion

$|A_1 \cup \cdots \cup A_n| =$
$\sum_i |A_i| - \sum_{i,j} |A_i \cap A_j| + \sum_{i,j,k} |A_i \cap A_j \cap A_k| \cdots (-1)^n |A_1 \cap \cdots A_n|.$

Idea: For $n = 3$ how many times is an element counted?

Consider $x \in A_i \cap A_j$.
x counted once for $|A_i|$ and once for $|A_j|$.
x subtracted from count once for $|A_i \cap A_j|$.
Total: 2 -1 = 1.

Consider $x \in A_1 \cap A_2 \cap A_3$
x counted once in each term: $|A_1|, |A_2|, |A_3|$.
x subtracted once in terms: $|A_1 \cap A_3|$, $|A_1 \cap A_2|$, $|A_2 \cap A_3|$.
x added once in $|A_1 \cap A_2 \cap A_3|$.
Total: 3 - 3 + 1 = 1.

Formulaically: x is in intersection of three sets.
$\binom{3}{1}$ for terms of form $|A_i|$, $\binom{3}{2}$ for terms of form $|A_i \cap A_j|$.
$\binom{3}{3}$ for terms of form $|A_i \cap A_j \cap A_k|$.
Total: $\binom{3}{1} - \binom{3}{2} + \binom{3}{3} = 1$.

Inclusion/Exclusion

$|A_1 \cup \cdots \cup A_n| =$
$\sum_i |A_i| - \sum_{i,j} |A_i \cap A_j| + \sum_{i,j,k} |A_i \cap A_j \cap A_k| \cdots (-1)^n |A_1 \cap \cdots A_n|.$

Idea: how many times is each element counted?
Element x in m sets: $x \in A_{i_1} \cap A_{i_2} \cdots \cap A_{i_m}$.
Counted $\binom{m}{i}$ times in ith summation.
Total: $\binom{m}{1} - \binom{m}{2} + \binom{m}{3} \cdots + (-1)^{m-1} \binom{m}{m}$.

Binomial Theorem:
$(x+y)^m = \binom{m}{0} x^m + \binom{m}{1} x^{m-1} y + \binom{m}{2} x^{m-2} y^2 + \cdots \binom{m}{m} y^m.$
Proof: m factors in product: $(x+y)(x+y)\cdots(x+y)$.
Get a term $x^{m-i} y^i$ by choosing i factors to use for y.
are $\binom{m}{i}$ ways to choose factors where y is provided. □

For $x = 1, y = -1$,
$0 = (1-1)^m = \binom{m}{0} - \binom{m}{1} + \binom{m}{2} \cdots + (-1)^m \binom{m}{m}$
$\implies \quad 1 = \binom{m}{0} = \binom{m}{1} - \binom{m}{2} \cdots + (-1)^{m-1} \binom{m}{m}$.

Each element counted once!

Summary.

First Rule of counting: Objects from a sequence of choices:
n_i possibilitities for ith choice : $n_1 \times n_2 \times \cdots \times n_k$ objects.

Second Rule of counting: If order does not matter.
Count with order: Divide number of orderings. Typically: $\binom{n}{k}$.

Stars and Bars: Sample k objects with replacement from n.
Order doesn't matter: Typically: $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$.

Inclusion/Exclusion: two sets of objects.
Add number of each subtract intersection of sets.
Sum Rule: If disjoint just add.

Combinatorial Proofs: Identity from counting same in two ways.
Pascal's Triangle Example: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.
RHS: Number of subsets of $n+1$ items size k.
LHS: $\binom{n}{k-1}$ counts subsets of $n+1$ items with first item.
$\binom{n}{k}$ counts subsets of $n+1$ items without first item.
Disjoint – so add!

Summary: lecture 1.

Propositions are statements that are true or false.

Propositional forms use $\wedge, \vee, \neg$.

Propositional forms correspond to truth tables.

Logical equivalence of forms means same truth tables.

Implication: $P \implies Q \iff \neg P \vee Q$.

Contrapositive: $\neg Q \implies \neg P$
Converse: $Q \implies P$

Predicates: Statements with "free" variables.

Quantifiers: $\forall x\ P(x)$, $\exists y\ Q(y)$

Now can state theorems! And disprove false ones!

DeMorgans Laws: "Flip and Distribute negation"
$\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$
$\neg \forall x\ P(x) \iff \exists x\ \neg P(x)$.

Propositions.

Poll.

(A) $P \vee Q \equiv (\neg P \implies Q)$ True

A version of $R \implies S \equiv \neg R \vee S$.

(B) $\exists n \in N, \neg P(n) \equiv \neg \forall n, P(n)$. True

If its not always true, it must be false at some point.

(C) $\forall n \in N, Q(n) \vee P(n) \equiv \forall n \in N, Q(n) \vee \forall n \in N, P(n)$ False

$Q(n)$ could be true on evens and $P(n)$ could be true on false.
The left hand side is true, and the right is false.

Lecture 2

Poll.

(A) Direct proof: $P \implies Q$ $a|b$ and $a|c$, $\implies a|(b-c)$
(B) Contraposition: $P \implies Q \equiv \neg Q \implies \neg Q$
n^2 is even $\implies$ n is even. $\equiv$ n is odd implies n^2 is odd.
(C) Contradiction: $\not P \implies R \wedge \not R$

Lecture 3. Summary: principle of induction.

Today: More induction.

$(P(0) \wedge ((\forall k \in N)(P(k) \implies P(k+1)))) \implies (\forall n \in N)(P(n))$

Statement to prove: $P(n)$ for n starting from n_0
Base Case: Prove $P(n_0)$.
Ind. Step: Prove. For all values, $n \geq n_0$, $P(n) \implies P(n+1)$.
Statement is proven!

Strong Induction:
$(P(0) \wedge ((\forall n \in N)(P(n) \implies P(n+1)))) \implies (\forall n \in N)(P(n))$

Also Today: strengthened induction hypothesis.

Strengthen theorem statement.
Sum of first n odds is n^2. pause
Hole anywhere on tiles.
Not same as strong induction. E.g., used in product of primes proof.

Induction $\equiv$ Recursion.

Poll:lecture 3.

What's after 0, 1, 2, 3, ...

What's before 100, 99, 98, ...

What is recursion?

Program works on smaller inputs.
ARGUMENT.
So it works on this one.

```
WriteAsPrimes(x):
  if prime(x): write x
  else: x = ab.
       write(a), write(b).
```

Lecture 4: Takeaways.

Analysis of cool algorithm with interesting goal: stability.

"Economic": different utilities.

Definition of optimality: best utility in stable world.

Action gives better results for individuals but gives instability.

Induction over steps of algorithm.

Proofs carefully use definition:
Stability:
Improvement Lemma plus every day the job gets to choose.
Optimality proof:
Job Optimality:
contradiction of the existence of a better *stable* pairing.
that is, no rogue couple by improvement, job choice,
and well ordering principle.
Candidate Pessimality:
contradiction plus cuz job optimality implies better pairing.

Life Lesson:ask, you will do better even if rejection is hard.

Exercise.

Why does it get better for candidates?

They get to choose.

Lecture 5 Summary.

Graphs.
Basics.
Degree, Incidence, Sum of degrees is $2|E|$. Connectivity.
Connected Component.
maximal set of vertices that are connected.
Algorithm for Eulerian Tour.
Take a walk until stuck to form tour.
Remove tour.
Recurse on connected components.

Trees: degree 1 lemma $\implies$ equivalence of several definitions.
G: n vertices and $n-1$ edges and connected.
remove degree 1 vertex.
$n-1$ vertices, $n-2$ edges and connected $\implies$ acyclic.
(Ind. Hyp.)
degree 1 vertex is not in a cycle.
G is acyclic.

Exercise

Removing a degree 1 vertex does change connectivity of graph.

Why?

No path goes through it.

Lecture 6 Summary.

Euler: $v+f=e+2$.
Tree. Plus adding edge adds face.
Planar graphs: $e \leq 3v=6$.
Count face-edge incidences to get $2e \leq 3f$.
Replace f in Euler.
Coloring:
degree d vertex can be colored if $d+1$ colors.
Small degree vertex in planar graph: 6 color theorem.
Recolor separate and planarity: 5 color theorem.
Graphs:
Trees: sparsest connected.
Complete:densest
Hypercube:
very connected, beautiful structure, bits,bits,bits.

Exercise

Why $v+f=e+2$?

Tree had $e=v-1$ and $f=1$.
Adding edge makes new face.

Lecture 7: Modular Arithmetic Lecture in a minute.

Modular Arithmetic: $x \equiv y \pmod{N}$ if $x=y+kN$ for some integer k.

For $a \equiv b \pmod{N}$, and $c \equiv d \pmod{N}$,
$ac=bd \pmod{N}$ and $a+b=c+d \pmod{N}$.

Division? Multiply by multiplicative inverse.
$a \pmod{N}$ has multiplicative inverse, $a^{-1} \pmod{N}$.
If and only if $gcd(a,N)=1$.

Why? If: $f(x)=ax \pmod{N}$ is a bijection on $\{1,\ldots,N-1\}$.
$ax-ay=0 \pmod{N} \implies a(x-y)$ is a multiple of N.
If $gcd(a,N)=1$,
then $(x-y)$ must contain all primes in prime factorization of N,
and is therefore be bigger than N.
Only if: For $a=xd$ and $N=yd$,
any $ma+kN=d(mx-ky)$ or is a multiple of d,
and is not 1.

Euclid's Alg: $gcd(x,y)=gcd(y \mod x, x)$
Fast cuz value drops by a factor of two every two recursive calls.

Know if there is an inverse, but efficiently find it? On Thursday!

Exercise

$d|x$ and $d|y \implies d|(x-y)$.

Is this used in Euclid?

With induction.

Fundamental Theorem of Algebra.

Any number can be written as a unique prime factorization.

$gcd(n,m)=1$. $n|x$ and $m|x$, implies $mn|x$.

Lecture 8 in a minute.

Extended Euclid: Find a,b where $ax+by=gcd(x,y)$.
Idea: compute a,b recursively (euclid), or iteratively.
Inverse: $ax+by=ax=gcd(x,y) \pmod{y}$.
If $gcd(x,y)=1$, we have $ax=1 \pmod{y}$
$\rightarrow a=x^{-1} \pmod{y}$.

Fundamental Theorem of Algebra:
Unique prime factorization of any natural number.
Claim: if $p|n$ and $n=xy$, $p|x$ of $p|x$.
From Extended Euclid.
Induction.

Chinese Remainder Theorem:
If $gcd(n,m)=1$, $x=a \pmod{n}, x=b \pmod{m}$ unique sol.

Proof: Find $u=1 \pmod{n}$, $u=0 \pmod{m}$,
and $v=0 \pmod{n}$, $v=1 \pmod{m}$.
Then: $x=au+bv=a \pmod{n}$...
$u=m(m^{-1} \pmod{n}) \pmod{n}$ works!

Fermat: Prime p, $a^{p-1}=1 \pmod{p}$.
Proof Idea: $f(x)=a(x) \pmod{p}$: bijection on $S=\{1,\ldots,p-1\}$.
Product of elts == for range/domain: a^{p-1} factor in range.

Exercise

Unique? $x = a \pmod{m}, x = b \pmod{n}$.

Assume two, $x, y \in \{0, \ldots, mn-1\}$

$n|(x-y)$ and $m|(x-y)$

$mn|(x-y)$.

Summary: Lecture 9

Public-Key Encryption.

RSA Scheme:
$N = pq$ and $d = e^{-1} \pmod{(p-1)(q-1)}$.
$E(x) = x^e \pmod{N}$.
$D(y) = y^d \pmod{N}$.

Repeated Squaring $\implies$ efficiency.

Fermat's Theorem $\implies$ correctness.

Good for Encryption and Signature Schemes.

Exercise

$x^{p-1} = 1 \pmod{p}$

$x^p = x \pmod{p}$.

$p|x^p - x$

Lecture 10 Summary

Two points make a line.

Compute solution: m, b.
Unique:
Assume two solutions, show they are the same.

Today: $d+1$ points make a unique degree d polynomial.

Cuz:
Can solve linear system.
Solution exists: lagrange interpolation.
Unique:
Roots fact: Factoring sez $(x-r)$ is root.
Induction, says only d roots.
Apply: $P(x)$, $Q(x)$ degree d.
$P(x) - Q(x)$ is degree $d \implies d$ roots.
$P(x) = Q(x)$ on $d+1$ points $\implies P(x) = Q(x)$.

Secret Sharing:
k points on degree $k-1$ polynomial is great!
Can hand out n points on polynomial as shares.

Exercise

Unique polynomial $P(x)$ that goes through $d+1$ points? Why?

$P(x) - Q(x)$ can only have d roots.

Lecture 11 Summary. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$
How to encode? With polynomial, $P(x)$.
Of degree? $n-1$
Recover? Reconstruct $P(x)$ with any n points!

Communicate n packets, with k errors.

How many packets? $n+2k$
Why?
k changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?
Reconstruct error polynomial, $E(X)$, and $P(x)$!
Nonlinear equations.
Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.
Polynomial division! $P(x) = Q(x)/E(x)$!

Reed-Solomon codes. Welsh-Berlekamp Decoding. Perfection!

Lecture 12/13.

First Rule of counting: Objects from a sequence of choices:
n_i possibilitities for ith choice : $n_1 \times n_2 \times \cdots \times n_k$ objects.

Second Rule of counting: If order does not matter.
Count with order: Divide number of orderings. Typically: $\binom{n}{k}$.

Stars and Bars: Sample k objects with replacement from n.
Order doesn't matter: Typically: $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$.

Inclusion/Exclusion: two sets of objects.
Add number of each subtract intersection of sets.
Sum Rule: If disjoint just add.

Not on exam. Combinatorial Proofs: Identity from counting same in two ways.
Pascal's Triangle Example: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.
RHS: Number of subsets of $n+1$ items size k.
LHS: $\binom{n}{k-1}$ counts subsets of $n+1$ items with first item.
$\binom{n}{k}$ counts subsets of $n+1$ items without first item.
Disjoint – so add!