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.

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

What if someone gets zero? '$***|**$' versus '$***||**$'

Sure can count number of '$***|**$' + number of '$**|*|**$'.
Second pattern is complicated: bars at least one apart.

For four number which is three bars:
'$***|**|$' - two bars on top of each other. Which two?

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.

Balls in bins.

"k Balls in n bins" $\equiv$ "k samples from n possibilities."

"indistinguishable balls" $\equiv$ "order doesn't matter"

"only one ball in each bin" $\equiv$ "without replacement"

5 balls into 10 bins
5 samples from 10 possibilities with replacement
Example: 5 digit numbers.

5 indistinguishable balls into 52 bins only one ball in each bin
5 samples from 52 possibilities without replacement
Example: Poker hands.

5 indistinguishable balls into 3 bins
5 samples from 3 possibilities with replacement and no order
Dividing 5 dollars among Alice, Bob and Eve.

Poll

Mark whats correct.

k Balls in n bins.

dis == distinguishiable unique = one ball in each bin.

(A) dis $=> n^k$
(B) dis,unique $=> n!/(n-k)!$
(C) indis, unique $=> \binom{n}{k}$
(D) dis, $=> n!/(n-k)!$
(E) indis, $=> \binom{n+k-1}{k-1}$
(F) dis,unique $=> \binom{n}{k}$

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 Tuesday!
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.
$\implies \binom{n}{n-k}$ 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 $(1+x)^n = (1+x)(1+x)\cdots(1+x)$.

Foil (4 terms) on steroids:
2^n terms: choose 1 or x from each term $(1+x)$.

Simplify: collect all terms corresponding to x^k.
Coefficient of x^k $\binom{n}{k}$: choose k terms with x in product.

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

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

□

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

□

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.

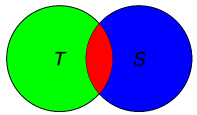
□

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



$S \cap T$

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.
3 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!

Midterm Review

Now...

First there was logic...

A statement is true or false.
Statements?
$3 = 4 - 1$? Statement!
$3 = 5$? Statement!
3 ? Not a statement!
$n = 3$? Not a statement...but a predicate.
Predicate: Statement with free variable(s).
Example: $x = 3$
Given a value for x, becomes a statement.
Predicate?
$n > 3$? Predicate: $P(n)$!
$x = y$? Predicate: $P(x, y)$!
$x + y$? No. An expression, not a statement.
Quantifiers:
$(\forall x)\ P(x)$. For every x, $P(x)$ is true.
$(\exists x)\ P(x)$. There exists an x, where $P(x)$ is true.

$(\forall n \in N), n^2 \geq n$.
$(\forall x \in R)(\exists y \in R) y > x$.

Connecting Statements

$A \wedge B$, $A \vee B$, $\neg A$.

You got this!

Propositional Expressions and Logical Equivalence

$(A \implies B) \equiv (\neg A \vee B)$
$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$

Proofs: truth table or manipulation of known formulas.

$(\forall x)(P(x) \wedge Q(x)) \equiv (\forall x)P(x) \wedge (\forall x)Q(x)$

..and then proofs...

Direct: $P \implies Q$
Example: a is even $\implies a^2$ is even.
Approach: What is even? $a = 2k$
$a^2 = 4k^2$.
What is even?
$a^2 = 2(2k^2)$
Integers closed under multiplication!
a^2 is even.

Contrapositive: $P \implies Q$ or $\neg Q \implies \neg P$.
Example: a^2 is odd $\implies a$ is odd.
Contrapositive: a is even $\implies a^2$ is even.

Contradiction: P
$\neg P \implies$ **false**
$\neg P \implies R \wedge \neg R$
Useful for prove something does not exist:
Example: rational representation of $\sqrt{2}$ does not exist.
Example: finite set of primes does not exist.
Example: rogue couple does not exist.

...jumping forward..

Contradiction in induction:
contradict place where induction step doesn't hold.

Well Ordering Principle.
Stable Marriage:
first day where canditate gets worse job on string.
first day where any job is rejected by optimal candidate.
Do not exist.

...and then induction...

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

Thm: For all $n \geq 1$, $8|3^{2n} - 1$.

Induction on n.

Base: $8|3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.
$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2} - 1 &= 9(3^{2n}) - 1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1) - 1 \\ &= 72d + 8 \\ &= 8(9d+1) \end{aligned}$$

Divisible by 8.

□

Stable Matching: a study in definitions and WOP.

n-jobs, n-candidate.

Each entity has completely ordered preference list
contains every entity of opposite type.

Pairing.
Set of pairs (m_i, w_j) containing all entities *exactly* once.
How many pairs? n.
Entities in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.
Pairing with no rogue couples.

Does stable pairing exist?

No, for roommates problem.

TMA.

Job Propose or reject Matching Algorithm:

Each Day:
All jobs propose to favorite non-rejecting candidate.
Every candidate rejects all but best job who proposes.

Useful Algorithmic Definitions:
Job **crosses off** candidate who rejected him.
Candidate's current proposer is **"on string."**

"Propose and Reject." : Either jobs propose or candidate. But not both.
Traditional propose and reject where jobs propose.

Key Property: Improvement Lemma:
Every day, if job on string for candidate,
$\implies$ any future job on string is better.

Stability: No rogue couple.
rogue couple (M,W)
$\implies$ M proposed to W
$\implies$ W ended up with someone she liked better than M.
Not rogue couple!

Optimality/Pessimal

Optimal partner if best partner in any stable pairing.
  Not necessarily first in list.
  Possibly no stable pairing with that partner.

Job-optimal pairing is pairing where every job gets optimal partner.

Thm: TMA produces male optimal pairing, S.
  First job M to lose optimal partner.
  Better partner W for M.
  Different stable pairing T.
  TMA: M asked W first!
  There is M' who bumps M in TMA.
  W prefers M'.
  M' likes W at least as much as optimal partner.
    Since M' was not the first to be bumped.
  M' and W is rogue couple in T.

Thm: candidate pessimal.

  Job optimal $\implies$ Candidate pessimal.
  Candidate optimal $\implies$ Job pessimal.

...Graphs...

$G = (V, E)$
  V - set of vertices.
  $E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
  In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
  Edge is incident to 2 vertices.
  Degree of vertices is total incidences.

Pair of Vertices are Connected:
  If there is a path between them.

Connected Component: maximal set of connected vertices.

Connected Graph: one connected component.

Graph Algorithm: Eulerian Tour

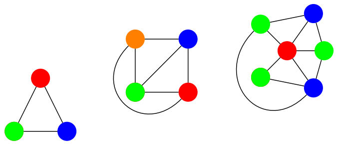
Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:
  Take a walk using each edge at most once.
   Property: return to starting point.
    Proof Idea: Even degree.

  Recurse on connected components.
  Put together.
   Property: walk visits every component.
    Proof Idea: Original graph connected.

Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

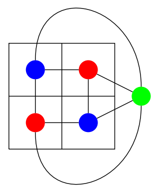


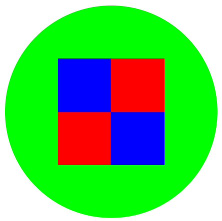
Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Interesting things to do. Algorithm!

Planar graphs and maps.

Planar graph coloring $\equiv$ map coloring.





Four color theorem is about planar graphs!

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
  From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

  Remove vertex v of degree at most 5.
   Inductively color remaining graph.
  Color is available for v since only five neighbors...
     and only five colors are used.

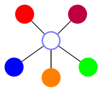
$\square$

Five color theorem: summary.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

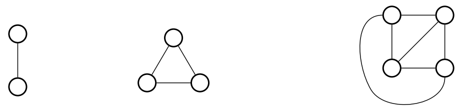
Theorem: Every planar graph can be colored with five colors.

Proof: Again with the degree 5 vertex. Again recurse.



Either switch green.
Or try switching orange.
One will work.

Graph Types: Complete Graph.

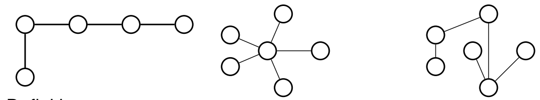


K_n, $|V| = n$

every edge present.
degree of vertex? $|V| - 1$.

Very connected.
Lots of edges: $n(n-1)/2$.

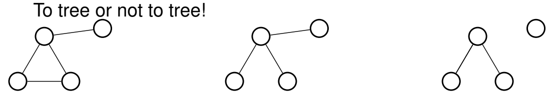
Trees.



Definitions:

A connected graph without a cycle.
A connected graph with $|V| - 1$ edges.
A connected graph where any edge removal disconnects it.
An acyclic graph where any edge addition creates a cycle.

To tree or not to tree!



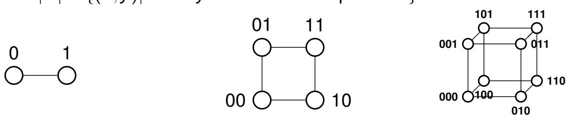
Minimally connected, minimum number of edges to connect.

Property:
Can remove a single node and break into components of size at most $|V|/2$.

Hypercube

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

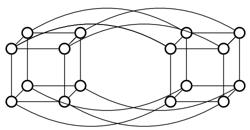
$G = (V, E)$
$|V| = \{0,1\}^n$,
$|E| = \{(x,y) | x$ and y differ in one bit position.$\}$



Recursive Definition.

A 0-dimensional hypercube is a node labelled with the empty string of bits.

An n-dimensional hypercube consists of a 0-subcube (1-subcube) which is a $n-1$-dimensional hypercube with nodes labelled $0x$ ($1x$) with the additional edges $(0x, 1x)$.



Hypercube:properties

Rudrata Cycle: cycle that visits every node.
Eulerian? If n is even.

Large Cuts: Cutting off k nodes needs $\geq k$ edges.
Best cut? Cut apart subcubes: cuts off 2^n nodes with 2^{n-1} edges.

FYI: Also cuts represent boolean functions.

Nice Paths between nodes.
Get from 000100 to 101000.
000100 $\rightarrow$ 100100 $\rightarrow$ 101100 $\rightarrow$ 101000
Correct bits in string, moves along path in hypercube!

Good communication network!

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0,\dots,m-1\}$
and integer $i \equiv a \pmod{m}$
if $i = a + km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58+32=90=6 \pmod{7}$
$58+32=2+4=6 \pmod{7}$
$58+32=2+-3=-1=6 \pmod{7}$

Negative numbers work the way you are used to.
$-3=0-3=7-3=4 \pmod{7}$

Additive inverses are intuitively negative numbers.

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod{7}$? 5
$5^{-1} \pmod{7}$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod{n}$
$ax = bx = 1 \pmod{n}$
$axb = bxb = b \pmod{n}$
$a = b \pmod{n}$.

$3^{-1} \pmod{6}$? No, no, no....

$\{3(1),3(2),3(3),3(4),3(5)\}$
$\{3,6,3,6,3\}$

See,... no inverse!

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m)=1$.

Group structures more generally.

Proof Idea:
$\{0x,\dots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m)=1$.

Finding gcd.
$gcd(x,y) = gcd(y,x-y) = gcd(y, x \pmod{y})$.

Give recursive Algorithm! Base Case? $gcd(x,0)=x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax+by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax+bm = ax \pmod{m}$.

Idea: egcd.
gcd produces 1
by adding and subtracting multiples of x and y

Hand calculation: egcd.

Extended GCD: egcd$(7,60)=1$.
egcd(7,60).

$$\begin{aligned} 7(0)+60(1) &= 60 \\ 7(1)+60(0) &= 7 \\ 7(-8)+60(1) &= 4 \\ 7(9)+60(-1) &= 3 \\ 7(-17)+60(2) &= 1 \end{aligned}$$

Confirm: $-119+120=1$

$d = e^{-1} = -17 = 43 = \pmod{60}$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$a^{p-1} \equiv 1 \pmod{p}$.

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \dots, a\cdot(p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1,\dots,p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \not\in T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$(a\cdot 1)\cdot(a\cdot 2)\cdots(a\cdot(p-1)) \equiv 1\cdot 2\cdots(p-1) \mod p$,

Since multiplication is commutative.

$a^{(p-1)}(1\cdots(p-1)) \equiv (1\cdots(p-1)) \mod p$.

Each of $2,\dots(p-1)$ has an inverse modulo p,
mulitply by inverses to get...

$a^{(p-1)} \equiv 1 \mod p$. □

RSA

RSA:
$N = p,q$
e with gcd$(e,(p-1)(q-1))=1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed}-x$ is divisible by p and q $\implies$ theorem!

$x^{ed}-x = x^{k(p-1)(q-1)+1}-x = x((x^{k(q-1)})^{p-1}-1)$

If x is divisible by p, the product is.
Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.
$\implies (x^{k(q-1)})^{p-1}-1$ divisible by p.

Similarly for q. □

RSA, Public Key, and Signatures.

RSA:
$N = p, q$
e with $\gcd(e,(p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

$E(D(C,k),K) = (C^d)^e = C \pmod{N}$

Modular Arithmetic in a minute.

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

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

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.

Modular Arithmetic Fact: Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d+1$ points.

Only d roots.

Lemma 1: $P(x)$ has root a iff $P(x)/(x-a)$ has remainder 0: $P(x) = (x-a)Q(x)$.

Proof: $P(x) = (x-a)Q(x) + r$.
Plugin a: $P(a) = r$.
It is a root if and only if $r = 0$. □

Lemma 2: $P(x)$ has d roots; $r_1, \ldots, r_d$ then
$P(x) = c(x)(x-r_1)(x-r_2)\cdots(x-r_d)$.
Proof Sketch: By induction.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1. $Q(x)$ has smaller degree so use the induction hypothesis. □

Implication: $d+1$ roots $\rightarrow \geq d+1$ terms $\implies$ degree is $\geq d+1$.

Roots fact: Any degree $\leq d$ polynomial has at most d roots.

Secret Sharing

Modular Arithmetic Fact: Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d+1$ points.

Shamir's k out of n Scheme:
Secret $s \in \{0, \ldots, p-1\}$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0$ with $a_0 = s$.
3. Share i is point $(i, P(i) \mod p)$.

Roubustness: Any k knows secret.
Knowing k pts, only one $P(x)$, evaluate $P(0)$.
Secrecy: Any $k-1$ knows nothing.
Knowing $\leq k-1$ pts, any $P(0)$ is possible.
Efficiency: ???

Efficiency.

Need $p > n$ to hand out n shares: $P(1) \ldots P(n)$.

For b-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between n and $2n$.
Chebyshev said it,
And I say it again,
There is always a prime
Between n and 2n.

Working over numbers within 1 bit of secret size.
Minimal!

With k shares, reconstruct polynomial, $P(x)$.

With $k-1$ shares, any of p values possible for $P(0)$!

(Within 1 bit of) any b-bit string possible!

(Within 1 bit of) b-bits are missing: one $P(i)$.

Within 1 of optimal number of bits.

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!

Midterm format

Time: 120 minutes.

Some short answers.
Get at ideas that you learned.

Know material well:	fast, correct.
Know material medium:	slower, less correct.
Know material not so well:	Uh oh.

Some longer questions.
Proofs, algorithms, properties.
Not so much calculation.

Wrapup.

Other issues....
sp21@eecs70.org
Private message on piazza.

Good Studying!!!!!!!!!!!!!!!!