Matthew Tran
CS70

Cardinality - size of set
Subset - $A \subseteq B$, all A in B
Proper subset - $A \subsetneq B$
Intersection - $A \cap B$
Disjoint - $A \cap B = \emptyset$
Union - $A \cup B$
Complement/set difference = $A \setminus B$
Significant Sets -
N - natural #'s $\{0, 1, 2, \ldots\}$
Z - integers
Q - rationals $\{\frac{a}{b} \mid a, b \in Z, b \neq 0\}$
R - real #'s
C - complex
Cartesian/cross product - $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- all possible pairs

Power set - all subsets
$\sum_{i=0}^{k} f(i)$ - sum $\prod_{i=0}^{k} f(i)$ - product

Universal Quantifier $\forall$ } order matters!
Existential Quantifier $\exists$

Predicate - has free variables
Proposition - statement true or false, no gray
- can be joined to make more complex statements

Propositional Form
- Conjunction ("and") - $P \land Q$
- Disjunction ("or") - $P \lor Q$
- Negation ("not") - $\neg P$
- Tautology - always true
- Contradiction - always false
- Implication - $P \Rightarrow Q$
  - $\neg P \lor Q$
  - false if P true, Q false
  - Contrapositive - $\neg Q \Rightarrow \neg P$
  - Converse - $Q \Rightarrow P$

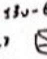
Demorgan's Law - u know dis
Logical equivalence - $\equiv$
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$
- $\neg \exists x P(x) \equiv \forall x \neg P(x)$
- $a \mid b$, divides $b = aq$, $q \in Z$

☆ Proofs (don't assume what u proving)
- Direct Proof - $P \Rightarrow Q$, assume P, show Q
- Contraposition - $\neg Q \Rightarrow \neg P$, assume $\neg Q$, show $\neg P$
- Contradiction - P, assume $\neg P$, show $\neg R \land R$
- Cases - all cases, "non-constructive" proof

Lemma - "subroutine", mini proof used in larger proof

Induction !
- Format
  Proof: we will prove by induction on n
  Base Case(s):
  Inductive Hypothesis: k
  Inductive Step: k+1
- Strengthening - make statement more precise
- Strong Induction ☆
  - assume $0 \leq k \leq n$ true, reduce n+1 to $0 \leq k \leq n$
  - having multiple base case can help.
- Well-ordering Principle $(\forall n \in N, \neg P(n+1) \Rightarrow \neg P(n))$ $\Rightarrow (\neg P(0) \lor \forall n \in N, P(n))$
  - any subset of N has smallest
  - opposite of induction
  - start big, work to smallest
- Principle of Excluded Middle - either P or $\neg P$ true
- Pigeonhole Principle - n items in m containers, $n > m$
  $\Rightarrow$ one m has > 1 items

Stable Marriage Algorithm
- algorithm (TMA?)
  1) Each man proposes to woman most preferred and not rejected yet
  2) Each woman rejects all but best choice, "string"
  3) Each man cross off woman who rejects him
- defined properties for algorithm
  - steps
  - "good pairing"
- Lemma: SMA always halts
  - on each day, no halt, someone crossed off, have to stop in at most n^2 days
- Stability
  - no rogue couples - x & y prefer each other to current partners
  - Improvement Lemma ☆: If $x \xrightarrow{\text{proposes}} y$ on k^{th} day, on every subsequent day y gets something $\geq x$
    - Proof by Induction, basically every day $j \geq k$
      - bc of algorithm x comes back, either x' better or x
- Lemma: SMA always end in pairing
  - Proof by Contradiction: ends when n^2 proposes n Y, need all X.
- Thm: always stable
  - no rogue couple, M prop to W before if they liked each other more. M would've been on string.
- Optimality - best pick in any stable pairing
  - Theorem: male optimal
    - basically contradiction, rogue couple exists
  - Theorem: female ~~optimal~~ pessimal
- Note: In any stable pairing S & T, one person prefers S and one prefers T

Graphs Theory
- $G = (V, E)$; V-vertices, E-edges
  - undirected, directed
  - for us
    - no self-loops
    - no multi-edges
- Path - sequence of edges between vertices
  - simple - unique/distinct vertices
  - neighbors - u & v directly connected by edge
  - cycle - aka circuit, start/stop v, simple
  - walk - path w/ repeated edges
  - tour - walk that start/stops same vertex
- Degree - # of incident edges
  - edge is incident to what it connects
- Connected - path between any vertices
- Eulerian walk - visit each edge once
  - tour - if start/stop same vertex
  - has tour iff even degree, connected
- Planar Graph
  - draw in 2D, no edge crossings
  - Euler's Formula ☆ - $v + f = e + 2$
    - edge divide faces
    - Proof: induction on e
      2 cases:
      1) Tree ✓
      2) find cycle, remove, e and f dec by one, by induction it's good
  - sides of a face $\sum s_i = 2e$
    $3f \leq 2e$ // each face ≥ 3 sides
    $e \leq 3v - 6$
  - $K_{3,3}$ 
- Cool Graph Classes
  - Complete Graph K_n
    - each vertex connect to each vertex
    - $(n-1)n/2$ edges
  - bipartite - v based dis
    - Trees are bipartite
    - each face - 4 edges
  - Tree
    - remove edge disconnects
    - connected, no cycles
    - connected, n-1 edges
    - no cycles, add edge makes cycle
  - Hypercube
    - n-bit strings, connect 1 bit off
    - recursive definition
    - $n2^{n-1} = |E|$
      - $n \cdot 2^n / 2$ edges
      vertices, bit flips, 2 count
- Hamiltonian Path - every vertex once
  exactly

Modular Arithmetic
- $x \equiv y \pmod m \Leftrightarrow m \mid (x - y)$
  - $x \bmod m = y \bmod m$
  - $x - y = km$, $k \in Z$
- multiplication, addition, subtraction works
  - use def of $x \equiv y \pmod m$, $x - y = km$ to prove
- exponentiation - ~~mod~~
- inverses - multiplicative inverse is the cool part
  - $xy \equiv 1 \pmod m$
  - only exists if $\gcd(x, m) = 1$ → Proof: Consider $0_x, 2x, \ldots, (m-1)x$, all distinct mod m, m distinct vals mod m, so 1 for one a and m. Contradiction $ax \equiv bx \pmod m$, $(a-b)x = km$, since $\gcd(x,m)=1$, m must divide a-b
- Euclid's Algorithm
  - $\gcd(x, y) = \gcd(y, x \bmod y)$
  - $\gcd(x, 0) = x$
  If $\gcd(x, y) = d$ $\Rightarrow d \mid x$, $d \mid y$
- Extended Euclid's Algorithm
  - $\gcd(x, y) = ax + by$
  - $ax + by = 1$, b is inverse of y mod x
- Bijection - one-to-one and onto
  - injective - $f(x) = f(y) \Rightarrow x = y$
  - surjective - all $y \in$ range, exists $x \in$ domain, $f(x) = y$

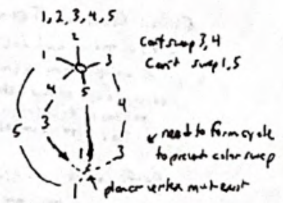
Chinese Remainder Theorem
- $x \equiv a \pmod m$ and $x \equiv b \pmod n$ where $\gcd(m, n) = 1$
  $\Rightarrow$ unique soln. $x \pmod{mn}$
- ex. can use eqn or this method
  $x \equiv 5 \bmod 7$, $x \equiv 7 \bmod 9$. By CRT unique soln $x \pmod{63}$
  $x = \underline{a} \cdot 9 + \underline{b} \cdot 7 = 61$ (divisible by mod 9, mod 7) $a = 6, b = 1$
  $9a \equiv 5 \pmod 7$, $7b \equiv 7 \bmod 9$
  Solve for a & b, using egcd or something
- Proof: Consider $u = n(n^{-1} \pmod m)$, $v = m(m^{-1} \pmod n)$
  $u \equiv 1 \pmod m$, $u \equiv 0 \pmod n$ (be multiple of n), $v \equiv 0 \pmod m$, $v \equiv 1 \pmod n$
  let $x = au + bv \equiv a \bmod m$ ✓
  $x = au + bv \equiv b \bmod n$ ✓
  Now show it's only soln. Proof by contradiction. Assume 2 soln. x, y
  $(x - y) \equiv 0 \pmod m$ $(x - y) \equiv 0 \pmod n$
  $\Rightarrow$ $(x - y)$ is multiple of m and n bc $\gcd(m, n) = 1$
  $\Rightarrow x - y \geq mn \Rightarrow x, y \notin \{0, \ldots, mn-1\}$ contradiction bc they have to be

Fermat's Little Theorem
- For prime p, $a \not\equiv 0 \pmod p$, $a^{p-1} \equiv 1 \pmod p$
  - actually $\gcd(a, p) = 1$ is only requirement i.e. inverse
- ex. $2^{101} \bmod 7$
  $\gcd(2, 7) = 1$, FLT → $2^6 \equiv 1 \bmod 7$; $2^{101} = 2^{6 \cdot 16 + 5} = 2^5 = 32 \equiv 4 \bmod 7$ (basically equal to $1^{16} \cdot 1$) woah!
- Proof: Consider $S = \{a \cdot 1, \ldots, a \cdot (p-1)\}$
  All diff mod p bc a has inverse mod p ← easy proof $ax_1 \equiv ax_2 \bmod p$, $x_1 \equiv x_2 \bmod p$, $x_1 < p$ and $x_2 < p$, so $x_1 = x_2$ ✓
  S contains representative of $\{1, \ldots, p-1\}$ mod p
  $(a \cdot 1) \cdot (a \cdot 2) \cdots (a(p-1)) \equiv 1 \cdot 2 \cdots (p-1) \bmod p$
  $a^{p-1}(1 \cdot 2 \cdots (p-1)) \equiv (1 \cdot 2 \cdots (p-1)) \bmod p$
  Each of $2, \ldots, (p-1)$ has inverse mod p
  $a^{p-1} \equiv 1 \pmod p$ ✓

RSA
- algorithm:
  Pick 2 large primes p, q; $N = pq$
  Pick e relatively prime to $(p-1)(q-1)$
  Compute $d = e^{-1} \bmod (p-1)(q-1)$
  Public key N, e : $K = (N, e)$
  Encoding $E(m, K) = m^e \bmod N$
  Decoding $D(m, K) = m^d \bmod N$
  $D(E(m)) = m^{ed}$ ~~mod~~ $\equiv m \pmod N$? Yes!
- ex. $p = 7, q = 11$, $N = 77$
  $(p-1)(q-1) = 60$, $e = 7$
  $d = -17 = 43$
  E $m = 2$, $2^7 = 128 \equiv -17 = 51$
  D $51^{43} = 51^{32+8+2+1}$
  ↑ use repeated squaring
- Proof:
  $d = e^{-1} \bmod (p-1)(q-1) \Leftrightarrow ed = k(p-1)(q-1) + 1$
  By CRT, isomorphism between $(a \bmod p, b \bmod q)$ and $x \bmod pq$
  $e = d^{-1} \bmod pq$
  $x^{ed} \equiv x^{1 + k(p-1)(q-1)} \pmod{pq}$
  Now $x \equiv a \bmod p$, $x \equiv b \bmod q$
  $a^{1 + k(p-1)(q-1)} \equiv a(a^{p-1})^{k(q-1)} \equiv a \pmod p$
  By Fermat: $a^{p-1} \equiv 1 \pmod p$
  $b^{1 + k(p-1)(q-1)} \equiv b(b^{q-1})^{k(p-1)} \equiv b \pmod q$
  By Fermat: $b^{q-1} \equiv 1 \pmod q$
  $x^{ed} \equiv a \pmod p$ and $x^{ed} \equiv b \pmod q$
  CRT $\Rightarrow x^{ed} \equiv x \pmod{pq}$
- Prime Number Theorem
  $\pi(N)$: number primes less than ~~or~~ N
  For $N \geq 17$ $\pi(N) \geq N / \ln(N)$, $1/\ln N$ chance of being prime

Graph Coloring

- colors to vertices so edge diff color
- Lemma: max degree d, $d+1$ colors
  - Base: 1 vertex ✓
  - Ind: Remove v, color w/ $d+1$ by hyp, neighbors use at most d colors, one color available for v
- 6 color theorem
  - $e \leq 3v - 6$
  - Total degree: $2e$
  - Avg. degree $= \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$
  - There exists a vertex v w/ degree ≤ 5
    Remove v and inductively color w/ 6 colors, but only 5 used by 5 neighbors, so one left for v
- 5 color theorem (red, orange, green, blue, white)
  - observation: connected components of vertices w/ 2 colors in a legal coloring
  - Proof: again w/ degree 5 vertex, again recurse
    - Assume neighbors all diff color
      - Otherwise 1 color left ⇒ Done!
    - Switch green, blue in green's component
      - Done unless path to blue
    - Switch orange and red in orange's component
      - Done unless path to red
    - Planar ⇒ paths intersect at vertex
    - What color is it?
      - Must be blue or green to be on that path
      - Must be red or orange to be on that path
      - contradiction, can recolor a neighbor, give a color for vertex



Exam Tips

- T/F: Think of a contradiction first, then the proof if you want

- Secret Sharing
  - secrecy - k-1 know nothing
  - robust - k know secret
  - efficient - minimize storage
  - Polynomial
    - mod p, $x \in \{0 \dots p-1\}$
    - 1 deg $\leq d$ poly has d+1 pts.
    - $P(x) = a_k x^k + \dots + a_0$
    - Shamir's k out of n Scheme
      - $a_0 = s$, make poly
    - Interpolation
      - 1 for pt., 0 rest, ? otherwise
  - Field - + and × operations
  - Delta Polynomial

    $$\Delta_i(x) = \frac{\prod_{i \neq j}(x - x_j)}{\prod_{i \neq j}(x_i - x_j)}$$
  - Roots Fact - any nontrivial degree d poly at most d roots
  - Uniqueness Fact - at most 1 deg d poly d+1 pts
    - proof by contradiction
  - Minimality
    - $p > n$ to hand out n info
    - $p > 2^b$ for b-bit secret
    - always prime between n & 2n
      - work w/ p w/in 1 bit, pretty optimal
    - runtime $O(\log p)$
- Erasure Codes
  - n packet message, lose k; msg: $m_1 \dots m_n$
  - total packet loss ⇒ send n+k
  - Corruption?
    - Reed-Solomon Codes
      - $P(x)$ deg n-1, $P(i) = m_i$
        - // also could $a_i = m_i$, use coeff instead
      - Send $P(1) \dots P(n+2k)$
      - Receive $R(1) \dots R(n+2k)$
      - Props
        - $P(i) = R(i)$ for at least n+k
        - $P(x)$ is unique deg n-1, w/ ≥ n+k pts
    - Berlekamp-Welch
      - error poly. $E(x)$, 0 if error, deg k (x^k is 1) k coeff unknown
      - $P(x)$ deg n-1; $Q(x) = E(x)P(x)$, deg n+k-1
        - $Q(x)$, n+k unknown coefficients
      - n+2k total unknown coefficients (n+2k points!)
      - Solve $Q(i) \equiv R(i)E(i) \pmod p$
        - Then $P(x) = \frac{Q(x)}{E(x)}$
      - Uniqueness
        - Assume $Q'(x)$ and $E'(x) \ni \frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x)$

          ⇒ $Q'(x)E(x) = Q(x)E'(x)$ for n+2k vals but deg n+2k-1, so same poly
        - $E(x)$ and $E'(x)$ at most k zeros, divide at n pts

          ⇒ $\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)}$ at n points, both ≤ n degree
    - $\alpha = \frac{k}{n}$, $\alpha \geq 1/2$ impossible
  - Lagrange Interpolation - sum up the delta polynomials

- Infinity
  - Isomorphism principle - if $f: D \to R$ bijection, $|D| = |R|$
  - Countable (like $\mathbb{N}$ be counting numbers) (0,1,2,...)
    - S countable if bijection S and $\mathbb{N}$, or subset
      - countably infinite ⇒ subset infinite
    - Can prove either way for bijection
    - Method 1: make bijection
    - Method 2: Listings / Enumeration
      - interleaving helps
      - any subset of countable S is countable
      - ex. binary strings n bits, appear before 2^{n+1}
      - $\mathbb{N} \times \mathbb{N}$ ☆
        - pair (a+b), in $(a+b+1)(a+b)/2$ elements
        - $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, same cardinality
  - Diagonalization (uncountable)
    - diff from every element, make new
  - Continuum Hypothesis
    - no set w/ cardinality between $\mathbb{N}$ and $\mathbb{R}$
- Undecidability
  - Program is a text string
    - Text string can be input
    - Program can be input to a program
  - To prove undecidable:
    - reduce to some form of HALT
    - assume exists, then write program with it, basically show TOF
  - ex. HALT
    - Turing(P)
      1. IF HALT(P, P), loop forever
      2. halt
    - Turing(Turing) halt?
      - yes → loops } contradiction
      - no → halts
    - Diagonalization View
      - each program string, can enumerate

        $$\begin{array}{c|cc} & P_1 & P_2 \\ \hline P_1 & \vdots & \cdots \\ P_2 & \vdots & \ddots \end{array}$$

        HALT - diagonal
        Turing - not HALT
        diff every P_i, not on list, not a program, can be made from Halt, doesn't exist!
        (b/c it flips the answer - for all input)
  - ex. 2 next one
    - Does P print "Hello World!"?
      - P': if (stop HALT(P, I))
        remove all print
        find exit and add print("Hello World!")
        PrintsHelloWorld(P', I)
        // P halts only if P' prints HelloWorld

- Counting
  - Rules
    - 1) Product Rule: $n_1 \cdot n_2 \cdot \ldots \cdot n_k$
    - 2) If order doesn't matter, count ordered, then divide # of orders
    - Sum Rule - can sum non-disjoint sets
  - ex. $\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$
    - ex. ANAGRAMS, if repeat divide by $n_i!$, n_i = #
  - General Inclusion/Exclusion
    - sets $A_1 \dots A_n$

      $$\left|\bigcup_i A_i\right| = \sum |A_i| - \sum_{i_1, i_2} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$
    - Derangement - no item in same proper place
  - Stars and Bars
    - sum n # numbers to k
    - n-1 bars to split k stars ⇒ n+k-1 positions
    - $\binom{n+k-1}{n-1}$ // order doesn't matter for bars
  - Remember the vacation problem
  - Combinatorial Proofs
    - show both sides equal w/ diff approach to define something
    - ex. $2^n = \binom{n}{n} + \binom{n}{n-1} + \dots + \binom{n}{0}$ // subsets of n objects
- Probability
  - Sample Space Ω, $P(\omega)$, use <u>trees</u>
  - Axioms
    - 1) nonnegativity $P(A) \geq 0$
    - 2) $P(\Omega) = 1$ normalization
    - 3) $A_1 \cap A_2 = \phi \Rightarrow P(A_1 \cup A_2) = P(A_1) + P(A_2)$
      mutually exclusive
  - $P(A) = \frac{|A|}{|\Omega|}$, $A \cup A^c = \Omega$, $P(A) = 1 - P(A^c)$
  - Law of Total Probability - $P(B) = P(B \cap A_1) + \dots + P(B \cap A_n)$

    $P(B) = P(B \cap A) + P(B \cap A^c)$
  - Conditional Probability
    - $P(A|B) = \frac{P(A \cap B)}{P(B)}$ // probability of A given B happened
    - Bayes' Rule ☆
      - $P(A|B) = \frac{P(B|A)P(A)}{P(B)}$
      - Useful for test validity and given random bins (coin test here)
  - Partition: A partitioned into $A_1, \dots, A_n$ if $A = A_1 \cup \dots \cup A_n$

    $A_i \cap A_j = \phi$ all $i \neq j$
  - Independence: A and B if $P(A \cap B) = P(A) \cdot P(B)$
    - Mutually independent - all subsets independent
  - Product Rule - $P\left(\bigcap_{i=1}^n A_i\right) = P(A_1) \cdot P(A_2|A_1) \cdot P(A_3|A_1 \cap A_2) \cdot \ldots \cdot P\left(A_n \middle| \bigcap_{i=1}^{n-1} A_i\right)$
  - Principle of Inclusion Exclusion
    - $P\left(\bigcup_{i=1}^n A_i\right) = \sum P(A_i) - \sum_{i,j} P(A_i \cap A_j) + \dots + (-1)^{n-1} P(A_1 \cap \dots \cap A_n)$
  - Boole's Inequality / Union Bound
    - $P\left(\bigcup_{i=1}^n A_i\right) \leq \sum_{i=1}^n P(A_i)$
  - Hashing - $m \leq \sqrt{n}$ for $P(\text{collision}) \leq 1/2$, similar to birthday problem

    $$m \leq \sqrt{2\ln\left(\tfrac{1}{1-\epsilon}\right)} \cdot \sqrt{n}$$
  - Load Balancing - want to pick random processor to load, $\ln k! \approx k \ln k - k$ for large k

- Random Variable (RV)
  - maps points in sample space to $\mathbb{R}$, $X: \underset{\text{event}}{\Omega} \to \mathbb{R}$
  - Probability mass function (PMF) - $P(\overset{\text{RV}}{X} = x) = P_X(x)$
  - Expected value - $E(X) = \sum_x x P_X(x)$
  - Uniform RV
    - $P_R(r) = \begin{cases} \frac{1}{n+1} & r = 0,1,2,\dots \\ 0 & e/w \end{cases}$
    - $E(R) = \sum_{r=0}^{n} r \cdot \frac{1}{n+1} = \frac{1}{n+1}\left(\frac{n(n+1)}{2}\right) = \frac{n}{2}$
  - Bernoulli RV
    $K \begin{cases} 1 & p \\ 0 & 1-p \end{cases}$ $E(K) = p$ $\sigma_K^2 = p(1-p)$
  - Geometric RV
    - like flip coin until first head - memoryless
    - $P_L(\ell) = \begin{cases} (1-p)^{\ell-1} p & \ell = 1,2,3,\dots \\ 0 & e/w \end{cases}$
    - $E(L) = \sum_{\ell=1}^{\infty} \ell (1-p)^{\ell-1} p = \frac{1}{p}$ see below
  - Binomial RV
    - n coin flips, M = # heads
    - modeled n Bernoulli RV
    - $P_M(m) = \begin{cases} \binom{n}{m}(1-p)^{n-m} p^m & m = 0,1,2,\dots,n \\ 0 & e/w \end{cases}$
    - $E(M) = np$, $var(M) = np(1-p)$
  - Indicator RV
    $I_A(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \omega \notin A \end{cases}$
  - RV in terms of another RV
    - $Y = g(X)$ $E(Y) = \sum_y y P_Y(y) = E(g(X))$
      $= \sum_x g(x) P_X(x)$
    - Note: $E(g(X)) \neq g(E(X))$ unless $g(x)$ is linear
  - Law of Total Expectation
    - $E(X) = \sum_i P(A_i) E(X \mid A_i)$ basically can split up
  - Lightbulb Problem - p prob of dying every hour
    - look at like coin flips
    - $E(L) = \underset{1}{E(L \mid H_1)}\, \underset{p}{P(H_1)} + \underset{1+E(L)}{E(L \mid T_1)}\, \underset{1-p}{P(T_1)}$
    - $E(L) = \frac{1}{p}$ Geometric RV
  - Variance of RVs
    - Law of Expectation Invariance $E(g(X)) = \sum_x g(x) P_X(x)$
    - $\sigma_X^2 = var(X) \stackrel{\Delta}{=} E((X - E(X))^2) = \underset{\text{2nd moment}}{E(X^2)} - E^2(X)$
    - $E(X^2) = \sum_x x^2 P_X(x)$
  - Poisson RV
    - n items, k events at prob p each, $n \gg 1$, $p \ll 1$, $k \ll n$
    - $P_L(\ell) = \begin{cases} e^{-\lambda} \frac{\lambda^\ell}{\ell!} & \ell = 0,1,2,\dots \\ 0 & e/w \end{cases}$
    - $E(L) = \lambda$ $\sigma_L^2 = \lambda$
    - $Z = \underset{\lambda}{X} + \underset{\mu}{Y} \sim Poisson(\lambda + \mu)$
- Joint PMFs
  - $P_{X,Y}(x,y) = P(X = x \cap Y = y)$
  - $P_{X|Y}(x|y) = P(X = x \mid Y = y) = \frac{P_{X,Y}(x,y)}{P_Y(y)}$
  - $P_{X,Y}(x,y) = P_X(x) P_Y(y)$ if independent
    - think of it like 2D graph rectangle points
  - $Z = X + Y$ $\sigma_Z^2 = \sigma_X^2 + \sigma_Y^2 + 2(\underbrace{E(XY) - E(X)E(Y)}_{cov(X,Y) \text{ covariance; } 0 \text{ if independent}})$

- Continuous RVs
  - probability density function (PDF) - $f_X(x)$
    - area = 1, nonnegative
  - Cumulative Distribution Function (CDF)
    - $F_X(x) = P(X \leq x)$
    - $f_X(x) = \frac{dF_X(x)}{dx}$
    - $F_X(x) = \int_{-\infty}^{x} f_X(\lambda)\, d\lambda$
  - Exponential Distribution RV
    - $f_X(x) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & e/w \end{cases}$
    - $E(X) = \frac{1}{\lambda}$
  - Expected Value/Mean
    - $E(X) \stackrel{\Delta}{=} \int_{-\infty}^{\infty} x f_X(x)\, dx$
  - Standard Normal/Gaussian RV
    - $f_Z(z) = \frac{1}{\sqrt{2\pi}} e^{-z^2/2}$ $E(Z) = 0$
    - $F_Z(z) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-z^2/2}\, dz$
  - Distribution of Transformed RVs
    - $Y = aZ + b$
    - $E(Y) = E(aZ + b) = aE(Z) + b$
    - $\sigma_Y^2 = E((Y - E(Y))^2) = E((aZ + b - aE(Z) - b)^2)$
      $= E(a^2(Z - E(Z))^2) = a^2 E((Z - E(Z))^2)$
    - $\sigma_Y^2 = a^2 \sigma_Z^2$
    - $F_Y(y) = P(Y \leq y) = P(aZ + b \leq y)$
      $= P(Z \leq \frac{y-b}{a})$
    - $F_Y(y) = F_Z(\frac{y-b}{a})$
    - $f_Y(y) = \frac{d}{dy} F_Y(y) = \frac{1}{a} f_Z(\frac{y-b}{a})$
    - ex $Z \sim N(0,1)$ Gaussian RV
      $Y \sim N(\underset{\text{mean}}{b}, \underset{\text{variance}}{a^2})$
      - $f_Y(y) = \frac{1}{a\sqrt{2\pi}} e^{-\frac{(y-b)^2}{2a^2}}$
  - Joint PDFs
    - $f_{X,Y}(x,y) = \frac{P(x \leq X \leq x + dx \cap y \leq Y \leq y + dy)}{dx\,dy}$
    - ex. Buffon's needle
      - polar approach useful, split up into components that are randomly chosen
  - Tail Probability Formula
    - Proof involves splitting up a summation
    - $E(X) = \int_0^\infty F_X^c(x)\, dx = \int_0^\infty P(X > x)\, dx$
      - $X \geq 0$ though
  - Markov's Inequality
    - $P(X \geq a) \leq \frac{E(X)}{a}$ $\left(P(|Y| \geq c) \leq \frac{E(|Y|^r)}{c^r}\right)$ generalized
  - Chebyshev's Inequality
    - $P((X - E(X))^2 \geq a) \leq \frac{\sigma_X^2}{a}$
    - $P(|X - E(X)| \geq \epsilon) \leq \frac{\sigma_X^2}{\epsilon^2}$
  - Weak Law of Large Numbers
    - $X_1 \dots X_n$, $M_n = \frac{X_1 + \dots + X_n}{n}$, $E(M_n) = E(X)$, $var(M_n) = \frac{\sigma_X^2}{n}$
    - $P(|M_n - E(X)| \geq \epsilon) \leq \frac{\sigma_X^2}{n\epsilon^2}$
    - $\lim_{n \to \infty} P(|M_n - E(X)| \geq \epsilon) = 0$
  - Central Limit Theorem (CLT)
    - $X_1 \dots X_n$ IID (independent, identically distributed)
    - $E(X_i) = \mu$, $var(X_i) = \sigma_x^2$, $M_n = \frac{X_1 + \dots + X_n}{n}$
    - $E(M_n) = \mu$, $var(M_n) = \frac{\sigma_x^2}{n}$
    - $Z_n = \frac{M_n - \mu}{\sqrt{var(M_n)}}$
    - CLT: $\lim_{n \to \infty} F_{Z_n}(z) = \underbrace{\Phi(z)}_{\text{Standard Gaussian CDF}} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-x^2/2}\, dx$

- Pollster Problem
  - How many polls to have 95% confidence within 0.03?
  - $\begin{cases} X_i = 1 & \mu \\ X_i = 0 & 1-\mu \end{cases}$ $M_n = \frac{X_1 + \dots + X_n}{n} \approx \mu$ (estimate)
    $\sigma_{M_n}^2 = \frac{\sigma_X^2}{n}$, $\underset{\max 1/4}{\mu(1-\mu)}$
    $\sigma_{M_n} = \frac{\sigma_X}{\sqrt{n}} = \frac{1}{2\sqrt{n}}$ worst case
  - $P(|M_n - \mu| \leq 0.03) \geq 0.95$
  - $P(|M_n - \mu| > 0.03) \leq 0.05$
  - $P(|\frac{M_n - \mu}{\sigma_{M_n}}| > 0.06\sqrt{n}) \leq 0.05$
  - $P(|Z_n| > 0.06\sqrt{n}) \leq 0.05$ area ≤ 0.05
    CLT this is like normal distr
    $\Phi(\alpha) \geq 0.9750 \Rightarrow \alpha = 1.9$ $n = 1068$

- Markov Chains (Finite)
  - state - position
  - state space - set of possible state values
  - state transition diagram - pics
  - transition probability - $P(X_{n+1} = a \mid X_n = b)$
    - amnesic - only depends on current state
    - can also make a matrix, vector of current state $\vec{\mu}^{(n)}$
    - $P_{ij} = P(X_{n+1} = j \mid X_n = i)$ ← same for matrix $P_{row, column}$
    - Thm: $\vec{\mu}^{(n)} = \underset{\text{horizontal}}{\vec{\mu}^{(0)}} P^n$
  - Hitting Time
    - $\tau(i)$ - avg. time to reach target from i
      - $\tau(\text{target}) = 0$
      - $\tau(i) = \underset{\text{counts 1 step before moving on}}{1} +$ probability of other state $\cdot\, \tau(\text{other state}) + \dots$
        - $\tau(i) = 1 + \sum P_{ij} \tau(j)$
    - use a start state
  - Probability of hitting A before B
    - A and B are disjoint states of space P
    - $\alpha(i) = 1$ $i \in A$ } make sense
    - $\alpha(i) = 0$ $i \in B$
    - $\alpha(i) = \sum_{j \in P} P_{ij} \alpha(j)$ $i \notin A \cup B$
  - Stationary/Invariant Distribution
    - if $\vec{\pi} = \vec{\pi} P$, $\vec{\pi}$ is invariant
    - balance equation - basically plug in one step of P
    - usually need sum limit on $\vec{\pi}$ to limit soln. to 1
  - Long Run Behavior of Markov Chains
    - $n \to \infty$, how much time spent in $i \in P$
    - irreducible - can go from any state to any other
      - basically can't get stuck anywhere
    - Thm: finite space P, matrix P is irreducible, for any $\vec{\mu}^{(0)}$, all $i \in P$ $\lim_{n \to \infty} \frac{1}{n} \sum_{m=0}^{n-1} \underset{\text{indicator for } i}{I\{X_m = i\}} \to \pi_i$
    - periodic - always oscillates
    - Thm: irreducible, matrix P, $i \in P$
      - $d(i) := g.c.d\{n > 0 \mid [P^n]_{ii} = P(X_n = i \mid X_0 = i) > 0\}$
        1) $d(i)$ same value for all i, if = 1, aperiodic
           - otherwise periodic w/ period d
        2) If aperiodic $P(X_n = i) = \pi_i$ $n \to \infty$
      - $d(i)$ is greatest common divisors of all integers $n > 0$ so that Markov chain can go from i to i in n steps
    - periodic if gcd of all cycles is 1
    - if self loop, then aperiodic by cycle of length 1
    - if aperiodic has limiting state probabilities ($\sum \pi = 1$)

- Cool Questions
  - polynomial bijection?
    - RSA $a^{1+k(p-1)(q-1)} \equiv a \pmod{pq}$

      so $a^{k(p-1)(q-1)} \equiv$ [redacted] $\pmod{pq}$
    - $f(x) = x^p$ if just a prime, then $p-1$ needed
      - if p is relatively prime to $(p-1)(q-1)$, bijection
      - if not, then not bc can find counter
  - Euler's Totient Theorem (like FLT)
    - $a^{\phi(n)} \equiv 1 \pmod{n}$ $\phi(n)$ is # of + integers less than or equal to n which are coprime to n include 1.

      & factor multiply -1
  - Fixed Points - undecidability
    - see if exists x, $F(x) = x$, problem FixedPoint(P)
    - def TestHalt(F, x):

      ```
      def TestHalt(F, x):
          def F_prime(y):
              F(x)
              return y
          return FixedPoint(F_prime)
      ```

      if F(x) halts, then FixedPoint returns true bc every input is one. if F(x) doesn't halt, then no fixed points. Thus TestHalt works
  - Get Standard Gaussian from 2 uniform

    $\sqrt{-2\ln(U_1)}\cos(2\pi U_2)$
  - $E(aX + bY) = aE(X) + bE(Y)$ even if dependent
    - expectation doesn't care about dependent
  - False $E(XY) = E(X)E(Y)$ iff. independent

    & def true if independent tho
  - Coupon collectors Problem
    - n coupons, 1 in each box, L: # boxes to get all
    - L_i: 1) each coupon distinct coupon

      $L_1 = 1$ L_2: $\frac{n-1}{n} \to 1$, $\frac{1}{n} \to 0$ … L_j: $\frac{n-(j-1)}{n} \to 1$, $1 - \frac{n-(j-1)}{n} \to 0$

      $E(L_1) = 1$ $E(L_2) = \frac{n}{n-1}$ $E(L_3) = \frac{n}{n-2}$
    - L_i follows geometric distribution, go until get one, so $E(L_j) = \frac{1}{P(L_j)}$
    - $E(L) = n\underbrace{\left(1 + \frac{1}{2} + \dots + \frac{1}{n}\right)}_{\approx \ln n + \gamma + \frac{1}{2n}}$

      $\gamma \approx 0.577216$
  - Polynomials over $GF^{(q)}$ with k roots
    - $\binom{q}{k}$ possible ways to choose k distinct roots
    - q^{k+1} total polynomials
    - remember with this the $P(x) = a\,Q(x)$, a constant factor
      - $q-1$ ways to choose a (not 0)
  - Halting - use P in some way, show that we solve halting if do it
  - $\binom{n}{3}$ triangles in K_n, bc pick any 3 vertices
  - $Cov(A,B) = E(AB) - E(A)E(B)$
  - $P(X<Y) = \frac{\lambda}{\lambda + \mu}$ given $X, Y \sim Exp(\lambda), Exp(\mu)$
  - $Normal(\mu, \sigma^2)$
  - Linear comb of Normal is also Normal
    - ~~use~~ $\frac{Z - \mu}{\sigma}$ to normalize
  - $Var(X^2) = E(X^4) - E^2(X^2)$
  - Graph coloring, remember color flipping
  - $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$
  - complete graph K_n needs n colors to color
  - $f(x) = ax \bmod N$ is bijection iff $\gcd(a, N) = 1$
    - Bij proof - find an inverse
  - $\sum \deg(v) = 2|E|$
  - # of programs is countable
  - $a^{(p-1)(q-1)} = 1 \bmod pq$ ← primes
  - intersection - subtract, find roots
    - always some constant at beginning $a_0(x - r_1)\dots(x - r_d)$
- For $[0, \dots, p^k - 1)$, p^{k-1} number div by p
- RV X, $X=3$ and $X=4$ are mutually exclusive, not independent

  $P(X=3 \cap X=4) = 0 \neq P(X=3) \cdot P(X=4)$
- $MMSE(X|Y) = E(X|Y)$
- joint density independent - see if single PDF depend on val of other
- uniform $[0,1]$ $E(X) = 1/2$, $var(X) = 1/12$
  - For width ℓ, $\ell^2/12$
- Use Markov, just add to make nonnegative
- Bayes's rule w/ continuous $f_X(x\,dx)\,dx = P(X = x)$

  $P(x \le X \le x + dx)$
- Law of Iterated Expectation
  - $E(X) = E(E(X|Y))$
- joint distr independent $P(X|Y) = P(X)$
- $E(XY) = \sum_x \sum_y xy\,P(X=x, Y=y)$
- $LLSE\{Y|X\} = \frac{cov(X,Y)}{var(X)}(X - E(X)) + E(Y)$
- To find CDF of function, just plug in more stuff around
- $\phi(pq) = (p-1)(q-1)$, p, q are primes