Fermat's Little Theorem: For any prime p and any a $\in$ {1,2,...,p-1}, $a^{p-1} \equiv 1$ mod p. factorial!
Pigeonhole Principle: n elements --> n-1 holes, there must be at least two elements in a hole
Encryption/Decryption Theorem: $(x^e)^d$ = x mod N = x mod (pq)
Polynomials **$P(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0$. degree d, roots P(x) = 0**
Property 1: A non-zero polynomial of degree d has at most d roots.
Property 2: Given d+1 pairs $(x_1,y_1),...,(x_{d+1},y_{d+1})$ (all x_i distinct), there is only one unique polynomial p(x) of degree at most d such that $P(x_i) = y_i$ for $1 \leq i \leq d+1$
POLYNOMIAL INTERPOLATION Lagrange, $\Delta_n(x)$ equations (0 at every point otherwise noted, 1 at point x=n) $P(x) = \text{sum}(y_n\Delta_n(x))$, don't forget to verify
Finite Fields = set + extra axioms - properties hold (MODULAR P is prime)
Property1/2 - holds when x spans complex numbers/real numbers/rational numbers
-DO NOT HOLD when values are natural numbers/integers
Secret Sharing - we want k people to pool knowledge/get secret, k-1 people have no knowledge
Work over GF(q)...q > n,s...n is number of officials. s is secret. P(0) = s. P(1) = 1st official, etc.
e.g. n=5, s=1, GF(7). 3 people should figure it out, so degree = 2. e.g. $P(x) = 3x^2 + 5x + 1$.
Erasure Errors - n packet message, $\leq$k packets lost. Send packets P(1)...P(n+k).
General Errors - noisy modem, k corrupted packets. **redundant, n+2k (labeled) packets sent
Error-locator $E(x) = (x-e_1)...(x-e_k)$. P(i)E(i) = R(i)E(i) for all i packets sent. (at errors, E(i) = 0).
Q(x) = P(x)E(x) = degree n+k-1 = $a_{n+k-1}x^{n+k-1}+...+a_1x + a_0$ $E(x) = (x^k) + b_{k-1}x^{k-1}+...+b_1x+b_0$
Graph ***when induction start big and break graphs down***
Edge set of a directed graph = subset: E $\subseteq$ V x V
simple path - no repeated vertices **Connected** - $\exists$ path between any two distinct vertices
cycle - begins/ends on same vertex **Complete** - every vertex adjacent to all other vertexes
If undirected graph, then *degree* of vertex v $\in$ V is number of edges incident to v (isolated: d=0)
in-degree: number of edges from other vertices $\rightarrow$ v. *out-degree*: # of edges, v $\rightarrow$ other vertices
tree = connected, acyclic, E = V-1 (any two imply third) (any tree edge removal creates exactly two connected components)
Eulerian Path - 7 bridges problem. *Multigraph*: >1 edges okay between vertices
Eulerian path= travel on all edges, can skip/repeat vertices.
Eulerian tour/cycle=eulerian path+cycle iff(directed graph): connected, in-degree=out-degree
Eulerian Theorem - Undirected Graph (V,E) has Eulerian tour iff graph is connected (except possibly isolated vertices) AND every vertex has even degree
Proof - if Tour, then every vertex must lie on tour, = connected.
if Tour, use all edges by entering vertex once and exiting once, so vertexes: even degree
if G = (V,E) is connected and all vertices have even degree:
If we walk from "u" and never repeat edges until stuck, we only get stuck at u
If we are stuck, then we pick an untraversed edge and closed-walk, splice it in
(# of edges traversed must be even at all vertices)
In any walk u to v, only vertices with odd degree (of edges used) are u and v
DeBrujin Graph - 2^n bit circular sequence, from de brujin graph G = (V,E). Bit-shifting.
Eulerian tour of vertexes = graph. in-degree = out-degree = 2.
Hypercubes - vertex set is $\{0,1\}^n$ (2^n vertices). Edges iff vertices differ by one bit.
Hamiltonian path - undirected. Path that goes through every vertex exactly once. Also $\exists$ cycle.
Gray code: ordering: n-bit binary strings, next string differs by 1 bit. applications: error correction
COUNTING. - inference: uncertainty $\rightarrow$ certainty
n bins, k indistinguishable balls: n-1 separations, k balls = (n+k-1) choose (k) = ${}_{n+k-1}C_k$ outcomes
m Balls and n Bins - P[bin 1 is empty] = $(1 - 1/n)^m$
1st rule of counting: 5 ice cream flavors, 3 cones, = 5*3 possibilities (* independent choices)
balls, bins, *with/without replacement - w*ith replacement = n^k; without replacement = n! / (n-k)!
2nd rule of counting: unordered objects (n!) / ((n-k)!(k!)) (k! indistinguishable) [n choose k]
Combinatorial Proofs - (n k) = (n n-k); (n k) = (n-1 k-1) + (n-1 k);
(n k+1) = (n-1 k) + (n-2 k) + ... + (k k) (n 0) + (n 1) + ... + (n n) = 2^n
definition of conditional probability $P[A|B] = P[A\cap B] / P[B]$ - false positives?#medical
Bayesian Inference - $P[A|B] = P[A\cap B] / P[B] = (P[B|A]P[A]) / P[B]$