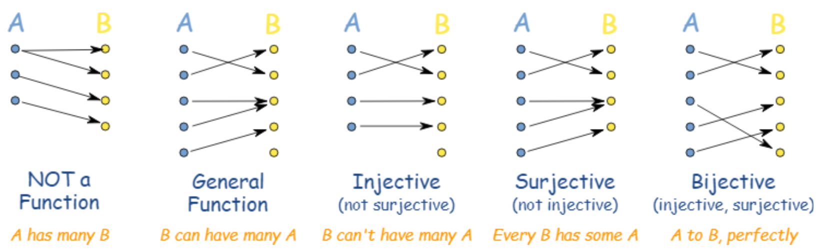
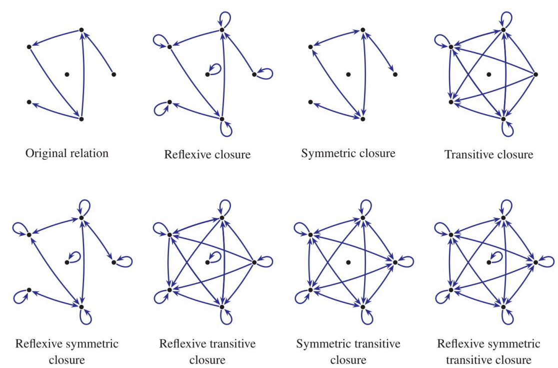
- Tree method
    - Negate conclusion, rewrite hypotheses, start at top of hypothesis and make branches - if not all branches are killed, counter-example exists
- Equivalence relation = reflexive, transitive, symmetric connecting classes (a ~ b) ; equivalence class = pairwise disjoint groups that make relations
- relations are subsets of cartesian products
- The composition of injective functions is injective and the composition of surjective functions is surjective, thus the composition of bijective functions is bijective.
    - injective = 1 to 1 ; surjective = b is mapped by at least one a ; bijective = both inj and surj
    - A function f has an inverse if and only if f is a bijection. (inverse is x and y switched)
- Proofs
    - Contrapositive: p → c becomes not c → not p
    - Contradiction (indirect): Assume p ∧ ¬q. Follow a series of logical steps to conclude r ∧ ¬r for some proposition r.
    - Proof by cases: universal statement such as ∀x P(x) breaks the domain for the variable x into different classes and gives a different proof for each class





- A symmetric and transitive closure is also reflective!

RSA Process: choose 2 prime numbers (p,q), calculate n = pq, calculate m = (p-1)(q-1), choose nums e and d such that ed has a remainder of 1 when divided by m, public key = (n, e)

Other person finds public key (n, e), finds remainder C = M^e (M is provided value) mod n, sends ciphertext C

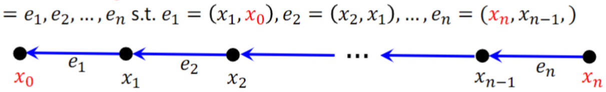
Private key = (n, d), find R = C^d mod n, R should == M :)

- Walk - A sequence of alternating vertices and edges that starts and ends in vertices in which the vertices before and after each edge are the two endpoints of that edge; length = # of edges traced; a walk from x0 to x1 is a sequence!
- Trail - walk in which no edge is repeated ; Circuit - CLOSED walk in which no edge is repeated
    - Path - trail where no vertex is repeated
        - WALK with no repeated nodes
    - Cycle - circuit in length >= 1 with same start and end vertices + no repeated vertex
        - WALK that begins and ends at a node and has no repeated nodes
- Eulerian - trail/circuit that traverses each edge exactly once
- Directed graph G = (V, E) ; V = set of vertices, E ⊆ V x V = a set of directed edges, each edge is an ordered pair (u, v) wih u, v ∈ V
- Outdegree: # of outgoing edges aka # of edges with v as initial node (denoted as deg+(v))
- Indegree: # of incoming edges aka # of edges with v as end node (denoted as deg-(v))
- For a given directed graph G = (V, E) - each edge has one initial node, # of edges = # of initial nodes
- Strongly connected graph: directed graph where there is a directed path from every node to every other node

---

Prove: If G = (V, E) is a DAG, then G has a node with indegree 0.

Proof:
- Given G is a DAG, ~~we assume G has no n~~ode with indegree 0, i.e., every node in G has indegree ≥ 1. Let $|V| = n$.
  Proof by Contradiction
- Then for **each node**, we can **move backwards** through an **incoming edge**.
- Pick any node x_0, if we walk backwards **n** times, it forms a backward walk $P = e_1, e_2, \ldots, e_n$ s.t. $e_1 = (x_1, x_0), e_2 = (x_2, x_1), \ldots, e_n = (x_n, x_{n-1},)$



- P passes through $n + 1$ nodes and there are only n distinct nodes,
- By the pigeonhole principle: P must have passed through some node **twice**.
- Thus, there is a cycle, which contradict the fact that G is a DAG.

Prove: If G = (V, E) is a DAG, then G has a topological ordering.

Proof by Induction on # of nodes $|V|$

- Base Case: If G is a DAG with 1 node, $G = (\{v\}, \emptyset)$, the topological ordering is v
- Inductive Hypothesis: Assume if G is a DAG with n nodes, G has a topological ordering.
- Inductive Step: When G' is a DAG with $n + 1$ nodes,
    - Pick a node $v \in G'$ with no indegree 0.
    - $G'' = G' - \{v\}$ is a DAG since deleting nodes/edges does not create cycles.
    - By IH, the DAG G'' with n nodes has a topological ordering.
    - v, followed by the topological ordering of G'' is a topological ordering of G'

G' has a topological ordering.

- Topological order: a linear ordering of nodes so for every directed edge (u, v) ∈ G, node u comes before v in order
- Every connected subgraph of a tree T is also a tree, If the subgraph is a cycle, T must also be a cycle
- There is a unique path between every pair of vertices
- Adding an edge between any two nonadjacent vertices in a tree creates a cycle
  - The new edge and the unique path connecting the vertices in the tree creates a cycle
- Removing any tree edge disconnects some pair of vertices - disconnects end points
- Every tree with at least 2 vertices contains at least 2 leaves, every tree with n vertices has n-1 edges
- A graph is planar if it can be drawn on the plane without crossing edges
- Outerplanar: at least two vertices of degree not exceeding 2 and at least three vertices of degree not exceeding 3, sandeep proof that at there is at least one vertex of degree at most 2
- Handshake lemma: number of vertices touching an off num of edges must be even, sum of degrees of all vertices must be even / double the number of edges
- 3 inverse mod 13 is 9 because 3 * 9 is 27 and 27 mod 13 is 1, 2 inv. mod 13 is 7 because 2 * 7 is 14, 14 % 13 = 1
- CRT formula: (a1y1m1 + a2y2m2 + a3y3m3) mod m gives final answer!! (a1 is x in x mod y form first step thing)

proof two vertices of equal degree in undirected graph

Since the graph is not directed and does not contain self-loops and each vertex can have either 0 or 1 edges, then every vertex can have a degree from the range of $[1 \dots N-1]$ (or $[0 \dots N-2]$) but there is a total of N vertices meaning that since the sum of all degrees for each vertex must equal $N-1$, then by the pigeonhole principle, there must be at least 2 vertices of equal degree.

At most one person loves Layla.

$\exists x: Loves(x, Layla) \rightarrow \forall y: (y \neq x \rightarrow \neg Loves(y, Layla))$

Exactly one person loves Layla.

$\exists x: Loves(x, Layla) \wedge \forall y: (y \neq x \rightarrow \neg Loves(y, Layla))$

Exactly two people love Layla.

$\exists\, x, y: (x \neq y) \wedge Loves(x, Layla) \wedge Loves(y, Layla)$

$\wedge \forall z: ((z \neq x \wedge z \neq y) \rightarrow \neg Loves(z, Layla))$

b) Prove that every full binary tree with N leaves has exactly $N-1$ internal vertices.

Proof by induction. Basis is $N = 1$. For the inductive step, let the subtrees of the root have n_1, n_2 leaves and, buy the IH contain $n_1 - 1, n_2 - 1$ internal nodes each. The total number of internal nodes, including the root, is therefore $1 + n_1 - 1 + n_2 - 1 = n_1 + n_2 - 1 = N - 1$.

A different argument by induction uses the result of part (a) in the inductive step. Remove the two sibling leaves – this results in a full binary tree with $N - 2 + 1 = N - 1$ leaves (the parent becomes a leaf). By the IH, this has $N - 2$ internal nodes; counting the parent, which was an internal node in the original tree, there were $N - 2 + 1 = N - 1$ internal nodes in the original tree.

c) Prove that every full binary tree of height h has at most $2^{h+1} - 1$ vertices.

Proof by induction on h. Basis: $h = 1$. Use a strong inductive hypothesis: every full binary tree of height at most k contains at most $2^{k+1} - 1$ vertices. In the inductive step, the subtrees of the root of the tree of height $k + 1$ are each of height k or less. Therefore, the tree of height $k + 1$ contains at most $1 + 2(2^{k+1} - 1) = 2^{k+2} - 1$ vertices.

e). $\gcd(a, b) = \gcd(b, rem(a, b))$, where rem(a,b) is the remainder when a is divided by

$rem(a, b) = a - qb = r$

$g = \gcd(a, b)$

$g|a$ and $g|b$

$\Rightarrow g|qb$, therefore $g|a - qb \Rightarrow g|r$

Since $g|b$ and $g|r$, then $g|\gcd(b, r)$

$x = \gcd(b, r)$

$x|b$ and $x|r$

$x|qb$, therefore $x|qb + r \Rightarrow x|a$

d). (Since $x|a$ and $x|b$, then $x|\gcd(a, b)$

1. $a|bc \rightarrow bc = ax$
2. $\gcd(a, b) = 1 \Rightarrow sa + tb = 1$
3. $csa + ctb = c$
4. $csa + bct = c$
5. $csa + axt = c$
6. $a(cs + xt) = c$
7. $a|c$

Phrase	Logical translation
P, but Q	$P \wedge Q$
Either P or Q	$P \vee Q$
P or Q, but not both	$(P \vee Q) \wedge \neg(P \wedge Q)$
P if Q	$Q \rightarrow P$
P is necessary for Q	$Q \rightarrow P$
P is sufficient for Q	$P \rightarrow Q$
P only if Q	$P \rightarrow Q$
P is equivalent to Q	$P \leftrightarrow Q$
P whenever Q	$Q \rightarrow P$

Prove that for $N \geq 3$, an N sided polygon can be partioned into $N-2$ triangular regions using interior diagonals

Basis: $N = 3$, $3 - 2 = 1$ triangular regions

I.H: $\forall i, \forall k$, $3 \leq i \leq k$ $P(i)$: $i-2$ triangular regions when its k sides

I.S: Add an additional side for $k+1$ sides, and splits into h_1 and h_2 sides respectivelly, the +1 edge is shared with h_1 & h_2 so $h_1, h_2 \leq k$, since we are not accounting for the side we have, then $k+1 = (h_1 - 1) + (h_2 - 1)$ $= (h_1 + h_2) - 2 \underset{I.H}{\Rightarrow} (h_1 - 2) + (h_2 - 2) - 2 = k + 1 - 2 = k - 1$ ✓

Model each room and the outside of the mansion by a vertex and each door by an edge that connects two rooms. The degree of the outside is 1 (only one entrance). By the handshake lemma, the number of vertices of odd degree in a graph must be even … ergo, there's at least one room with an odd number of doors. Safe!

$A \rightarrow (B \rightarrow C)$

$\neg C \rightarrow (\neg B \wedge D)$

$D \rightarrow A \vee \neg C$

$\therefore \neg A \rightarrow (D \rightarrow B)$

✓ $A \rightarrow (B \rightarrow C)$

✓ $\neg C \rightarrow (\neg B \wedge D)$

✓ $D \rightarrow A \vee \neg C$

✓ $\neg(\neg A \rightarrow (D \rightarrow B))$

✓ $\neg(A \vee (D \rightarrow B))$

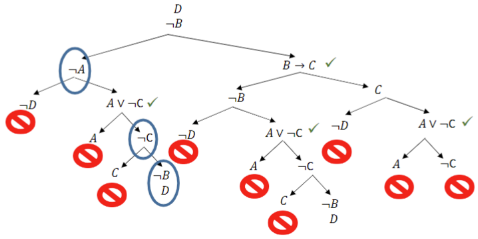
$\neg A$

✓ $\neg(D \rightarrow B)$

✓ $\neg(\neg D \vee B)$

D

$\neg B$



Counterexample!

A: False
B: False
C: False
D: True

Divisibility Lemma. The following statements are true:

a. $a|b \implies \forall c: a|bc$

b. $a|b \;\wedge\; b|c \implies a|c$

c. $a|b \;\wedge\; a|c \implies \forall s, t \in \mathbb{Z}: \; a|(sb + tc)$

d. $\forall c \neq 0: \; a|b \iff ca|cb$

a. $\forall c \in \mathbb{Z}: \; (c|a \;\wedge\; c|b) \implies c|\gcd(a, b)$

b. $\forall k > 0: \gcd(ka, kb) = k \cdot \gcd(a, b)$

c. $(\gcd(a, b) = 1 \;\wedge\; \gcd(a, c) = 1) \implies \gcd(a, bc) = 1$

d. $(a|bc \;\wedge\; \gcd(a, b) = 1) \implies a|c$

e. $\gcd(a, b) = \gcd(b, rem(a, b))$

where $rem(a, b)$ is the remainder on dividing a by b.

Lemma:

1) If p is prime, then $\phi(p)$

2) If p, q are primes then ϕ

In general, if $p_1, p_2, \dots, p_k$ are

1. $a \equiv b \; (mod\ m) \implies a + c \equiv b + c \; (mod\ m)$ Add common term to both sides.
2. $a \equiv b \; (mod\ m) \implies a \cdot c \equiv b \cdot c \; (mod\ m)$ Multiply by common term on both sides.
3. $a \equiv b \; (mod\ m) \;\wedge\; c \equiv d \; (mod\ m) \implies a + c \equiv b + d \; (mod\ m)$ Add equal numbers.
4. $a \equiv b \; (mod\ m) \;\wedge\; c \equiv d \; (mod\ m) \implies a \cdot c \equiv b \cdot d \; (mod\ m)$ Multiply equal numbers.