CSCI 2200
FOUNDATIONS OF COMPUTER SCIENCE

David Goldschmidt
goldsd3@rpi.edu
Fall 2022

NUMBER THEORY – DIVISIBILITY AND GCD

Quotient-Remainder Theorem

For $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, $n = qd + r$. The quotient $q \in \mathbb{Z}$ and remainder $0 \le r < d$ are *unique*.

Definition. Greatest Common Divisor, GCD

Let m, n be two integers not both zero. $\gcd(m, n)$ is the largest integer that divides both m and n: $\gcd(m,n)|m$, $\gcd(m,n)|n$ and … $d\,|\,m \wedge d\,|\,n \rightarrow d \le \gcd(m, n)$.

Theorem.

$\gcd(m, n) = \gcd(\text{rem}(n, m), m)$.

Euclid's Algorithm

NUMBER THEORY – GCD AND BEZOUT'S IDENTITY

(i) $\gcd(m, n) = \gcd(m, \text{rem}(n, m))$.
(ii) Every common divisor of m, n divides $\gcd(m, n)$.
(iii) For $k \in \mathbb{N}$, $\gcd(km, kn) = k \cdot \gcd(m, n)$.
(iv) IF $\gcd(l, m) = 1$ AND $\gcd(l, n) = 1$, THEN $\gcd(l, mn) = 1$.
(v) IF $d|mn$ AND $\gcd(d, m) = 1$, THEN $d|n$.

Theorem. Bezout's Identity

$\gcd(m, n)$ is the *smallest positive integer linear combination* of m and n:

$$\gcd(m, n) = mx + ny \qquad \text{for } x, y \in \mathbb{Z}.$$

Relatively Prime

If $\gcd(m, n) = 1$, then m, n are relatively prime.

NUMBER THEORY — USING BEZOUT'S IDENTITY

(v) IF $d|mn$ AND $\gcd(d,m)=1$, THEN $d|n$.

Proof. We prove claim (v) — if $d \mid mn$ and $\gcd(d, m) = 1$, then $d \mid n$

Since d and m are *relatively prime*, i.e., $\gcd(d, m) = 1$, integers x and y exist such that

$$dx + my = 1 \qquad \text{[from Bezout's Identity]}$$

Multiplying both sides by n, we obtain

$$n\,(\,dx + my\,) = dnx + mny = n$$

Also see Exercise 10.7…

Both dnx and mny are divisible by d — here, $d \mid mn$ implies that mny is divisible by d.

If the LHS is divisible by d, then the RHS must also be divisible by d, thus $d \mid n$. ■

NUMBER THEORY — EUCLID'S LEMMA

(v) IF $d|mn$ AND $\gcd(d,m)=1$, THEN $d|n$.

Euclid's Lemma claims: if p is prime and $p \mid mn$, then $p \mid m$ or $p \mid n$ (but not both!)

Proof. We prove Euclid's Lemma using a direct proof. Assume $m > 1$ and $n > 1$. Given p is prime and $p \mid mn$, we have two cases.

Case 1. $p \mid m$ — since p is prime and $n > 1$, by definition, p cannot divide n.

Case 2. $\gcd(p, m) = 1$ — here, we conclude from (v) that $p \mid n$. ■

…and if p, m, and n are primes, then either $p = m$ or $p = n$

Generalizing Euclid's Lemma, if $p, q_1, q_2, \ldots, q_n$ are primes and $p \mid q_1 q_2 \ldots q_n$, then p must be equal to exactly one of $q_1, q_2, \ldots, q_n$

See Exercise 10.8…

NUMBER THEORY — PRIME NUMBERS

We can define the set of *prime* numbers P using divisibility…

note that 1 is not prime

$$P = \{\, p \mid p \geq 2 \text{ with positive divisors 1 and } p\text{, i.e., } x \mid p \text{ iff } x = 1 \text{ or } x = p \,\}$$

The *Fundamental Theorem of Arithmetic* states that for all natural numbers $n \geq 2$, we can write n as the product of one or more prime numbers

We proved this theorem using strong induction… (go back and do this again…)

…but we did not prove the *uniqueness* of these products (aside from reordering)

e.g., $43 \times 47 = 2021$ is unique; $7 \times 17 \times 17 = 2023$ is unique; etc.

No other group of prime numbers will produce 2021 or 2023 when multiplied together!

FUNDAMENTAL THEOREM OF ARITHMETIC — PART II

Theorem. Uniqueness of Prime Factorization
Every $n \geq 2$ is *uniquely* (up to reordering) a product of primes.

Proof. We prove the claim using contradiction and the Well-Ordering Principle.

Let n_* be the smallest possible number (with $n_* > 2$) that we can write as a product of primes in at least two different ways, i.e.,

$$n_* = p_1 p_2 \ldots p_n \quad \text{and} \quad n_* = q_1 q_2 \ldots q_k$$

Here, $p_1 \mid n_*$ — therefore, $p_1 \mid q_1 q_2 \ldots q_k$ and so p_1 must equal one of q_i (Euclid's Lemma).

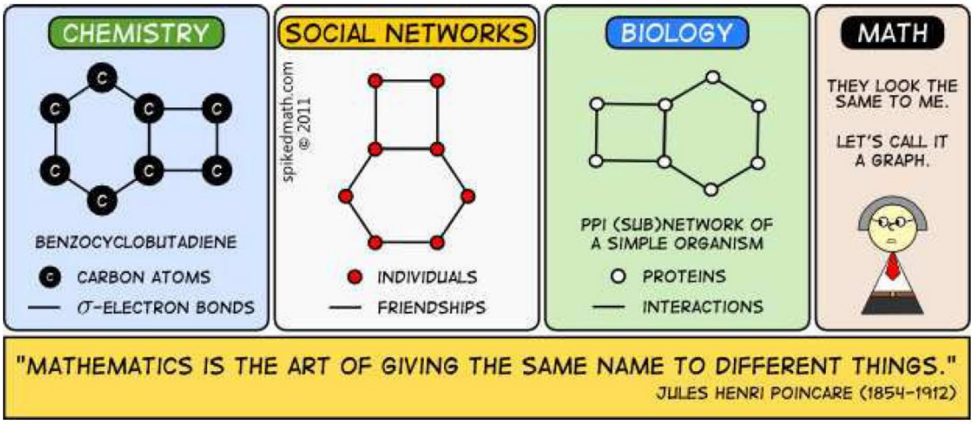
Without loss of generality, let $q_i = q_1$ — therefore, $q_1 = p_1$ and we have

$$n_* = p_1 p_2 \ldots p_n \quad \text{and} \quad n_* = p_1 q_2 \ldots q_k$$

Divide both sides by p_1 to get n_*/p_1 as a product of primes in two different ways.

Since $p_1 \geq 2$, we have $n_*/p_1 < n_*$ as a smaller counterexample — a contradiction! ■

GRAPHS

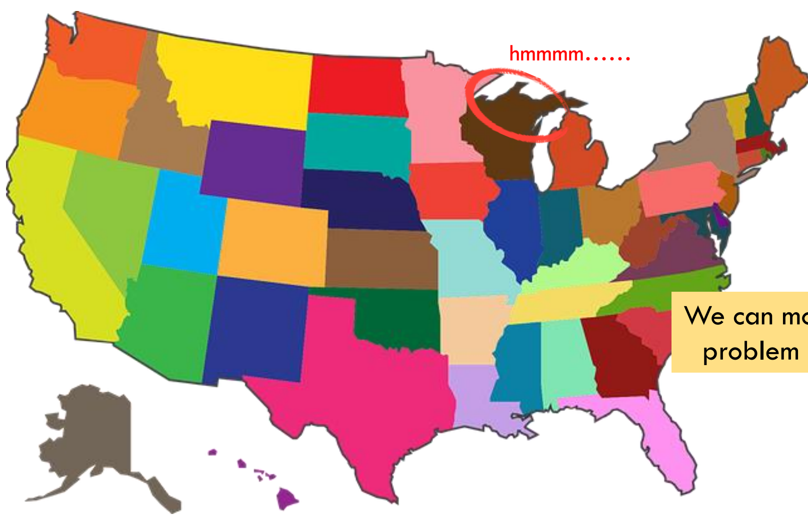

CHEMISTRY
BENZOCYCLOBUTADIENE
CARBON ATOMS
σ-ELECTRON BONDS
SOCIAL NETWORKS
spikedmath.com © 2011
INDIVIDUALS
FRIENDSHIPS
BIOLOGY
PPI (SUB)NETWORK OF A SIMPLE ORGANISM
PROTEINS
INTERACTIONS
MATH
THEY LOOK THE SAME TO ME.
LET'S CALL IT A GRAPH.
"MATHEMATICS IS THE ART OF GIVING THE SAME NAME TO DIFFERENT THINGS."
JULES HENRI POINCARE (1854-1912)

What is the minimum number of colors needed to color in this map without any adjacent states using the same color?

GRAPH COLORING PROBLEM

What is the minimum number of colors needed to color in this map without any adjacent states using the same color?

GRAPH COLORING PROBLEM – SOLVED?



We can model and solve this problem using a graph…

UNDIRECTED GRAPHS

We disallow *self-loops*, e.g., edges (A,A) and (B,B), and *multi-graphs* with multiple edges between two vertices

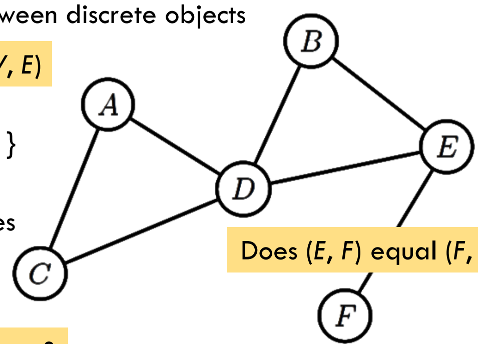
A *graph* models and helps visualize relationships between discrete objects

We define a graph using two sets V and E $G = (V, E)$

Set V contains the vertices, e.g., $V = \{ A, B, C, D, E, F \}$

Set E contains the edges, in this case undirected edges

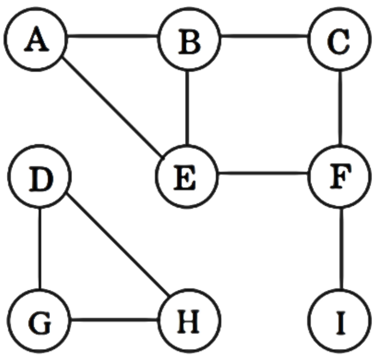
$E = \{ (A,C), (A,D), (C,D), (B,D), (B,E), (D,E), (E,F) \}$



Does (E, F) equal (F, E)?

What does $|V|$ and $|E|$ represent? Can either be zero?

UNDIRECTED GRAPHS



For given graph Q = (V, E), what are V and E?

Set $V = \{ A, B, C, D, E, F, G, H, I \}$

Set E contains all undirected edges…

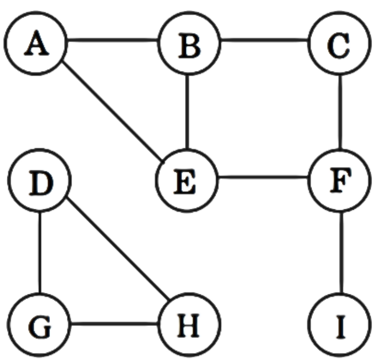
$E = \{$ (A,B), (A,E), (B,C), (B,E), (C,F), (D,G), (D,H) (E,F), (F,I), (G,H) $\}$

Therefore, $|V| = 9$ and $|E| = 10$

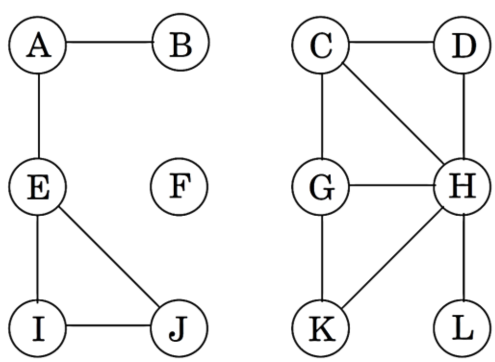
Define *degree* ∂_q as the number of edges that are *incident on* (or *adjacent to*) some vertex q…

What is ∂_F, i.e., the degree of vertex F?

UNDIRECTED GRAPHS



For this graph, what is ∂_i (i.e., the degree of each vertex i)?



$\partial = [\,5, 3, 3, 3, 2, 2, 2, 2, 2, 1, 1, 0\,]$

DEGREE SEQUENCE

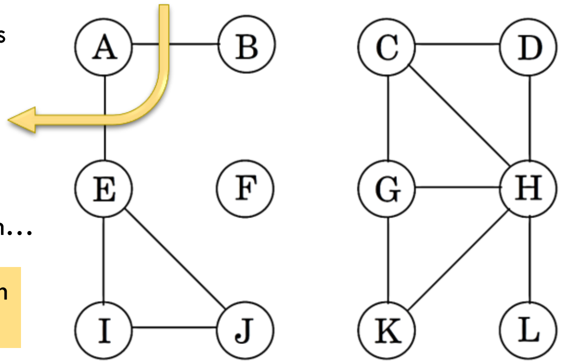
Degree sequence ∂ lists all vertex degrees of the graph from highest to lowest...

∂ = [5, 3, 3, 3, 2, 2, 2, 2, 2, 1, 1, 0]

On its own, a degree sequence ∂ is not guaranteed to uniquely describe a graph...

Can you draw two different graphs with ∂ = [2, 2, 2, 2, 2, 2]?

the degree of the graph itself is therefore 5...



Can you draw two different graphs with ∂ = [3, 3, 2, 1, 1]?

How about ∂ = [3, 3, 3, 2, 1, 1]?

```
degree sequence is [2,2,2,2,2,2]

 O-----O    O               O---O
 |    /    /|              /     \
 |   /    / |     and     O       O
 |  /    /  |              \     /
 |/     /   |               O---O
 O    O-----O
                      (these two are isomorphic)
                        O----O----O
                        |         |
                        O----O----O
```

```
degree sequence is [3,3,2,1,1]

           O
          / \
         /   \
        O-------O          (no other possible graph!)
       /         \
      /           \
     O             O
```

DEGREE SEQUENCE – HANDSHAKING THEOREM

Can you draw two different graphs with ∂ = [3, 3, 3, 2, 1, 1]?

We cannot construct such a graph because when we add an edge, it has two endpoint vertices and therefore increases the sum of degrees by two…

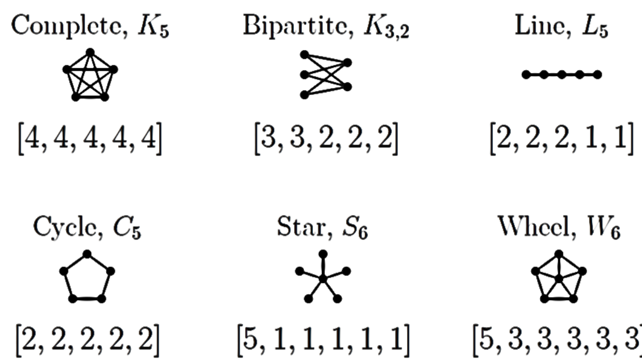
Prove this theorem using induction…

Theorem. Handshaking Theorem

For any graph the sum of vertex-degrees equals twice the number of edges, $\sum_{i=1}^{n} \delta_i = 2|E|$.

DEGREE SEQUENCE — GRAPH PATTERNS

- K_n Complete graph or n-clique
- $K_{n,\ell}$ Complete bipartite graph with n left and ℓ right vertices
- L_n Line or path with n vertices
- C_n Cycle with n vertices
- S_{n+1} Star with a central vertex connected to n peripheral vertices, i.e., $K_{1,n}$
- W_{n+1} Wheel — a cycle of n vertices with a central vertex



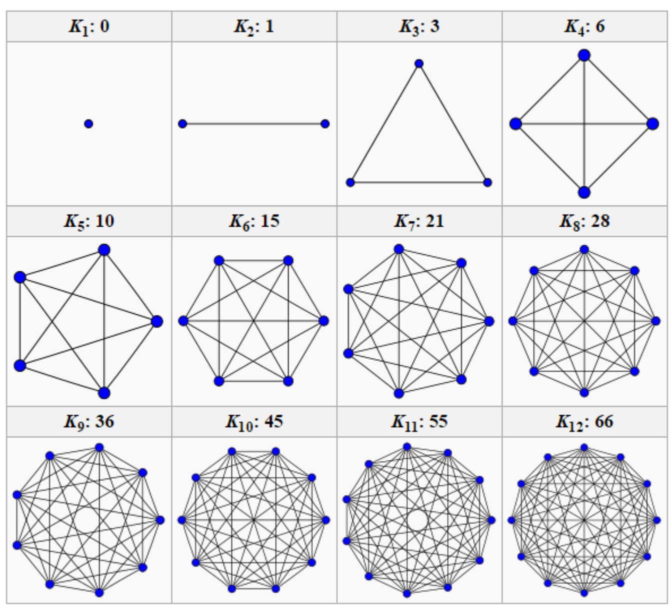
COMPLETE GRAPHS

The *Traveling Salesman Problem* (*TSP*) requires a complete graph…

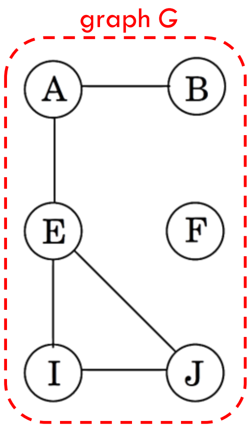
For weighted graph K_n, we must find a cycle that visits all n vertices and has the lowest total weight or cost

Is TSP $\in \Theta(n!)$?

If I claim cycle C is a solution, how do you know if C is correct…?



(SUB)GRAPH ISOMORPHISM



Let $G = (V, E)$ and $H = (V', E')$ be two distinct graphs

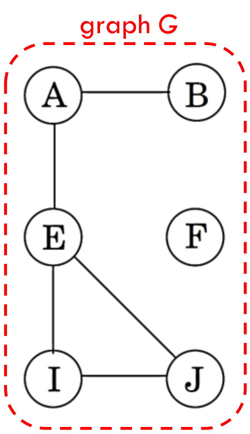
Graphs G and H are *isomorphic* iff there is a way to map each vertex in V to a vertex in V' such that all edges in E also map to E'

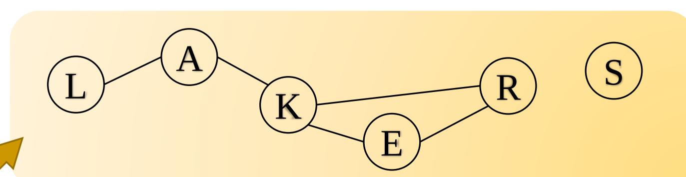
In other words, we *relabel* at least one vertex, all the while maintaining the structure of the graph…

Note that we can apply this concept to subgraphs, too!

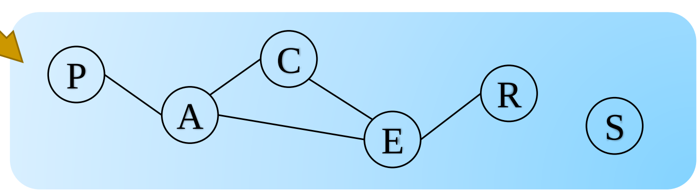
Graphs G and H are *isomorphic* iff there is a way to map each vertex in V to a vertex in V' such that all edges in E also map to E'

(SUB)GRAPH ISOMORPHISM



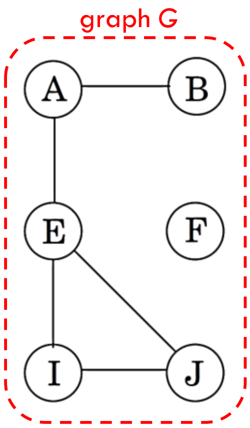


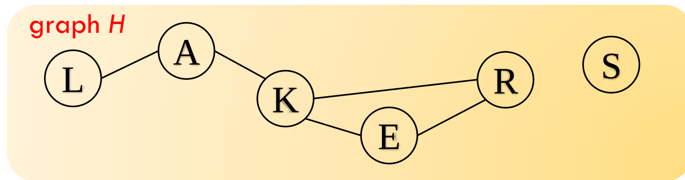
which of these two graphs is isomorphic to graph G…?



Graphs G and H are *isomorphic* iff there is a way to map each vertex in V to a vertex in V' such that all edges in E also map to E'

(SUB)GRAPH ISOMORPHISM



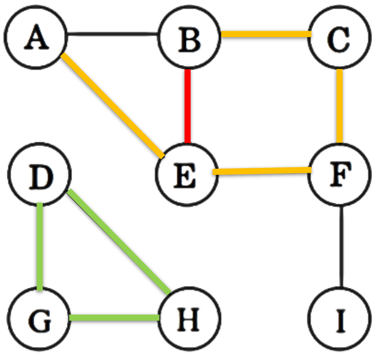


These two subgraphs are isomorphic because we can map vertices of G to vertices of H...

$A \rightarrow A$	$F \rightarrow S$
$B \rightarrow L$	$I \rightarrow E$
$E \rightarrow K$	$J \rightarrow R$

Vertices *u* and *v* are *connected* if there is a path from *u* to *v*…

PATHS, SIMPLE PATHS, AND CYCLES



A *path* is a sequence of vertices with a designated start and end vertex for which we have an edge between each pair of consecutive vertices…

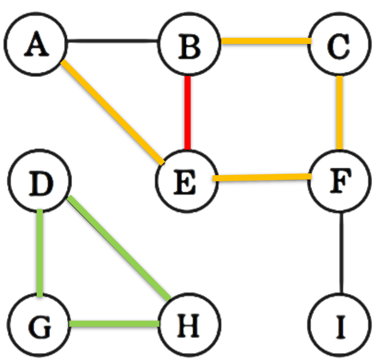
A *simple path* does not repeat vertices

e.g., *AEFCB* is a simple path of length 4 since we traverse 4 edges

e.g., *AEFCBE* is a path of length 5

e.g., *DHGD* is a *cycle* since we start and end on the same vertex — and we do not traverse any edge more than once

CONNECTIVITY AND ISOMORPHISM



Vertices *u* and *v* are *connected* iff there is a path from vertex *u* to vertex *v*

A graph is *connected* iff every pair of vertices is connected

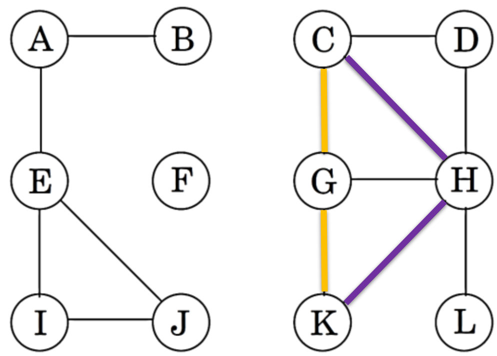
Two graphs are isomorphic iff both graphs have the same paths…

Can you prove this?

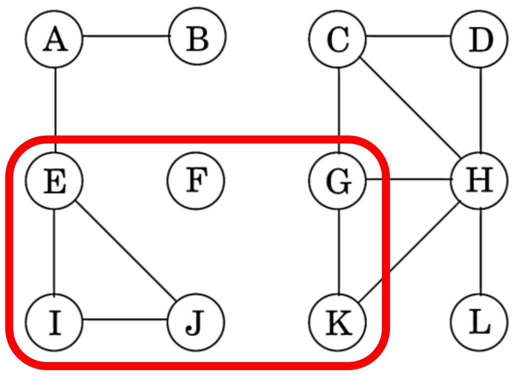
EDGE-DISJOINT PATHS

Edge-disjoint paths start and end on the same vertex but have no edges in common

Given a graph and a specific pair of start and end vertices, can we reliably determine how many edge-disjoint paths there are…?



(INDUCED) SUBGRAPHS



Define *subgraph* $H = (V', E')$ of graph $G = (V, E)$…

…with $V' \subseteq V$ and $E' \subseteq E$ such that all edges of E' are guaranteed to have endpoints in V'

Define *induced subgraph* H' such that all edges of set E that connect vertices of V' are in set E'

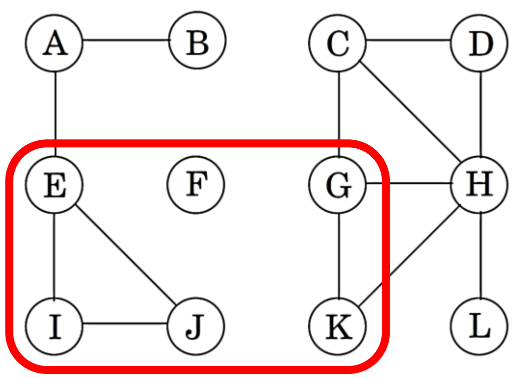
What is the induced subgraph shown in red…?

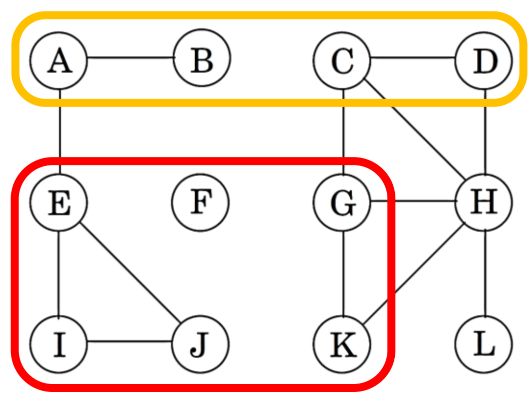
$V' = \{ E, F, G, I, J, K \}$ and

$E' = \{ (E,I), (E,J), (G,K), (I,J) \}$

What is a subgraph of G that is *disjoint* from H…?

(INDUCED) SUBGRAPHS & DISJOINT SUBGRAPHS



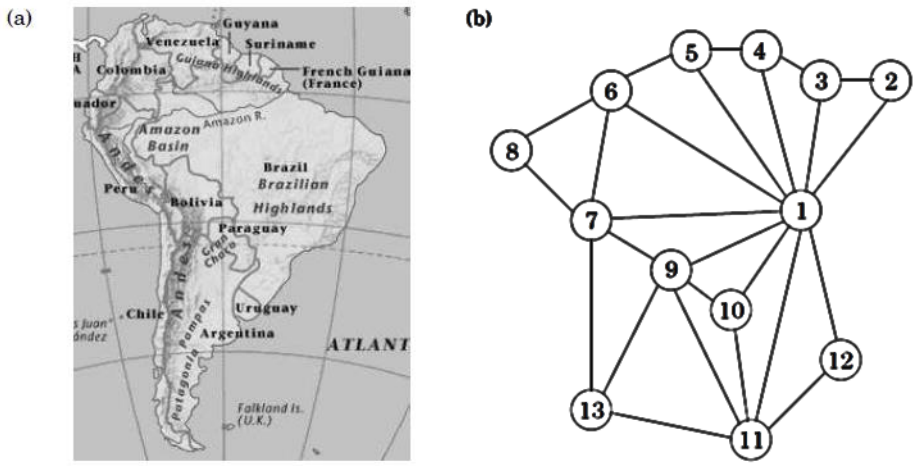


Two graphs are *disjoint* from one another if they do not share any common vertices (or edges)

GRAPH COLORING PROBLEM

…from Dasgupta's *Algorithms* book

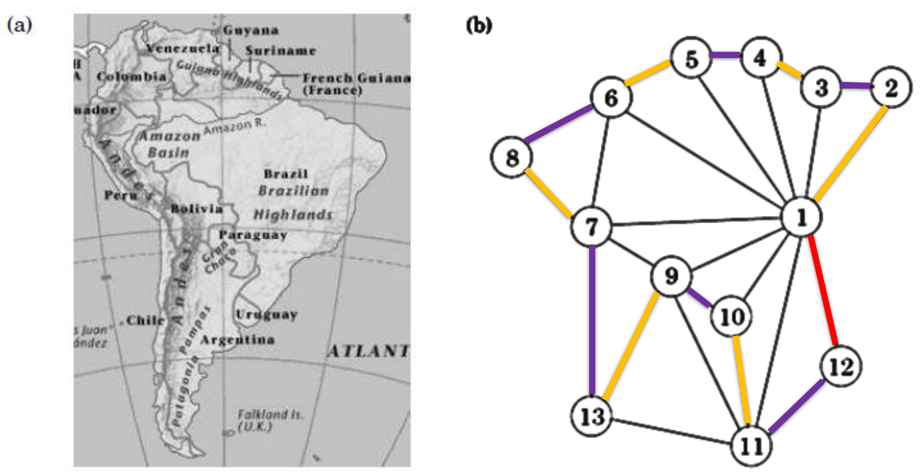
Figure 3.1 (a) A map and (b) its graph.



GRAPH COLORING PROBLEM

…from Dasgupta's *Algorithms* book

Figure 3.1 (a) A map and (b) its graph.



WHAT NEXT...?

Homework 4 has been posted and is due by 11:59PM on Thursday, November 3

Practice! Tinker! Practice!

Practice! Tinker! Practice!