TABLE OF CONTENTS

Section 3: Definition

Definitions:

Even: an integer is called even provided it is divisible by 2

Divisible: Let a and b be integers. We say a is divisible by b if there exists an integer c such that bc=a. Equivalently, “b divides a”, or b|a

Proof:

Claim: If x is odd and y is even then x + y is odd

- Assume x is odd and y is even
- Since x is odd, x=2c+1 for some c $\in \mathbb{Z}$
- Since y is even, 2|y, so y=2b for some b $\in \mathbb{Z}$
- Adding these equations, we get x+y=2c+1+2b
- Then x+y=2(c+b)+1 where c+b $\in \mathbb{Z}$
- Then x+y is odd, by definition ■

Definitions:

Prime: p > 1 is prime if the only positive divisors are 1 and p

Composite: a positive integer a is composite if there is an integer b s.t. 1<b<a and b|a

Section 4: Theorem

Definitions:

Theorem: a theorem is a statement which has been proven to be true

Conjecture: a conjecture is a statement which has not yet been proven true or false

Statment: a statement (also **Boolean expression** or **predicate**) is a sentence (in English or math!) whose value is true or false.

Boolean Operations:

		AND	OR	NOT		IMPLIES or “IF-THEN”	
p	**q**	**$p \wedge q$**	**$p \vee q$**	**$\neg p$**	**$\neg q$**	**$p \rightarrow q$**	**$q \rightarrow p$**
T	T	T	T	F	F	T	T
T	F	F	T	F	T	F	T
F	T	F	T	T	F	T	F
F	F	F	F	T	T	T	T

Section 5: Proof

TEMPLATE

Direct Proof (of if-then)

Claim: $p \to q$ ⌜ p ——————→ q ⌝
| (hypothesis) (conclusion) |
⌞ antecedent consequent ⌟

Proof:

- Assume p [assume hypothesis]
  ·
  · 〉[direct logical steps]
  ·
- Thus q ■ [reach conclusions]

If-and-only-if Proof

Claim: $p \leftrightarrow q$ [equivlent to $p \to q$ and $q \to p$]

Proof:

- ($\Rightarrow$) Assume p
  ·
  ·
- Thus q

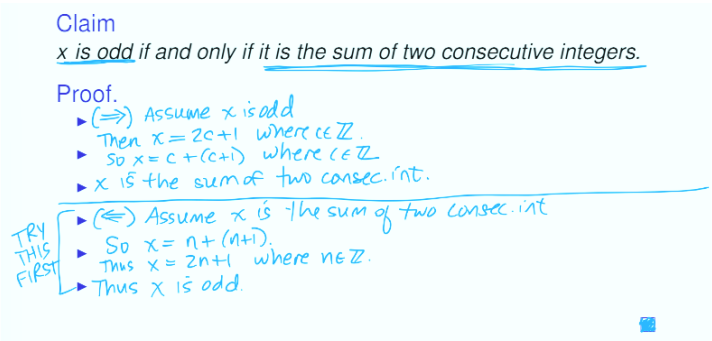
- ($\Leftarrow$) Assume q
  ·
  ·
- Thus p ■

Definitions:

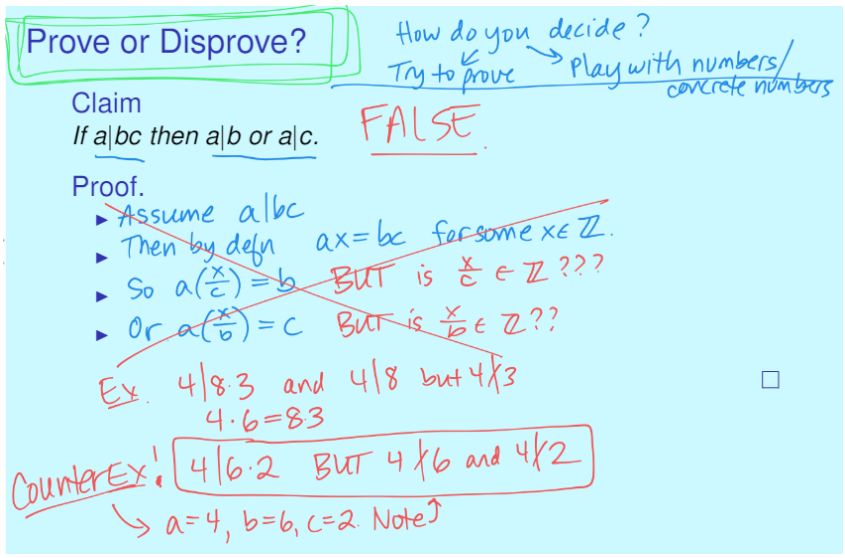
Consecutive Integers: Two consecutive integers are integers of the form n, n+1 (where $n \in \mathbb{Z}$). In general, k consecutive integers are integers of the form n, n+1, n+2, … n+(k-1), where $n \in \mathbb{Z}$.

Theorem:

x is odd if and only if it is the sum of two consecutive integers



Section 6: Counterexample

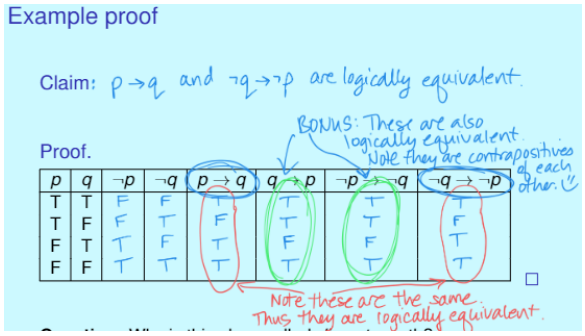


Section 7: Boolean Algebra

Definitions:

Boolean algebra: based on the values TRUE and FALSE (or statements or variables that represent the values true or false), and operations that send {TRUE, FALSE} to {TRUE, FALSE}.

Logically Equivalent: two boolean expressions are logically equivalent if there are equal for all possible values of their inputs



Boolean Properties:

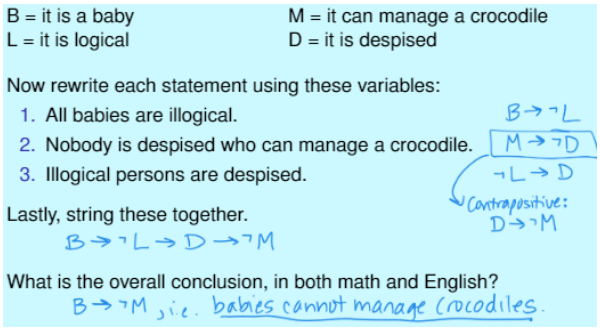
Commutative Laws: $p \wedge q = q \wedge p$
$p \vee q = q \vee p$

Associative Laws: $(p \wedge q) \wedge r = p \wedge (q \wedge r)$
$(p \vee q) \vee r = p \vee (q \vee r)$

Identity Laws:	$p \wedge T = p$ $p \vee F = p$	
Negation Laws:	$p \wedge \neg p = F$ $p \vee \neg p = T$	[CONTRADICTION because always false] [TAUTOLOGY because always true]
DeMorgan's Laws:	$\neg(p \wedge q) = \neg p \vee \neg q$ $\neg(p \vee q) = \neg p \wedge \neg q$	
Distributive Laws:	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$	

Syllogisms:

Solving a syllogism



Section 8: Lists

Definitions:

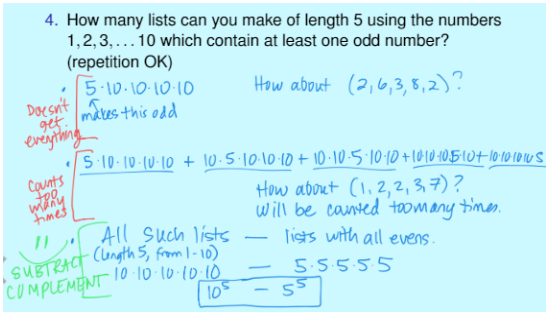
List: a list is an ordered sequence of objects, called elements

Multiplication Principle: In a list of length two, if there are n choices for the first element and m choices for the second element, there are nm lists altogether.

With Repetion:

List of length k, each element has n possibilities:

n^k possible lists = $\underbrace{n * n * n * n * \ldots * n}_{k \text{ times}}$



Without Repetion:

There are n possibilities for the first element, n-1 remaining possibilities for the second element and so on:

(n - (k - 1)) = $\underbrace{n*(n-1)*(n-2)*\ldots*(n-k+1)}_{lenght\ k}$

5. How many lists can you make of length 5 using the numbers $1, 2, 3, \ldots 10$ which contain at least one odd number and don't repeat any numbers?

All lists — all evens.

$10 \cdot 9 \cdot 8 \cdot 7 \cdot 6$ — $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

Section 9: Factorial

Definitions:

Natural Numbers($\mathbb{N}$): $\mathbb{N}$ = { 0, 1, 2, 3, …}

"n fatorial" (n!): for n ϵ {1, 2, 3, …}, define n! = n(n - 1)(n - 2)...(3)(2)(1)

#lists of length k from n elements without repetition = $\frac{n!}{(n-k)!}$

$\underbrace{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}_{\text{length } k} = \frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)\cdots(1)}{(n-k)\cdots(1)} = \frac{n!}{(n-k)!}$

Section 10: Sets

Definitions:

Set: a ser is a repetition-free, unordered collection of objects, called elements. IF x is an element of a set A, we write xϵA

Cardinality: The cardinality or size of a set is the number of elements in a set, denoted |A|. Elements of a set can themselves be sets.

Sudset: for sets A, B, we say A is a subset of B (written A$\subseteq$B) if xϵA$\rightarrow$xϵB

i.e, every element of A is an element of B

Proving Sets are Equal:

Let A, B be two sets, To show A = B (x ϵA$\leftrightarrow$xϵB) we show A$\subseteq$B (xϵA$\rightarrow$xϵB) and B$\subseteq$A (xϵB$\rightarrow$xϵA)

Example: Let $A = \{x \in \mathbb{Z} : 3|x\}$, and $B = \{x \in \mathbb{Z} : x$ can be written as the sum of 3 consecutive integers$\}$.

Claim: $A = B$

Proof: ($\subseteq$) Suppose $x \in A$. Then $3|x$
Then $3c = x$ for $c \in \mathbb{Z}$
Then we can write $x = (c-1)+c+(c+1)$
So x is the sum of 3 consec. int.
Then $x \in B$

OPTION:
e.g. let
$c-1 = n$
or $c = n+1$

($\supseteq$) Suppose $x \in B$. Then x is the sum of 3 consec. int.
So $x = n + (n+1) + (n+2)$
$x = 3n+3 = 3(n+1)$ where $n+1 \in \mathbb{Z}$

So $3|x$
Then $x \in A$

Definitions:

Power Set of S: The set of all subsets of S is called the power set of S, denoted P(S), also denoted by the slightly unusal-looking 2^S

Cute Formula: $|2^S| = 2^{|S|}$

$|\_\_\_\_\_|$ the cardinality of the power set; $\ulcorner\bar{\ }\urcorner$ $cardinality\ of\ S$

Section 11: Quantifiers

Defintions:

Qualifiers: are defined with respect to a universe U $\nearrow^{\{times\}\{people\}\{integers\}}$. They either describe something that is true about all elements of U, or at least one element of U.

∀ **= "for all" (universal quantifier).**

∃ **= "there exists" (existential qualifier).**

Proofs:

Single Qualifiers

Claim: ∀xϵU, p(x)

Proof:

- Let xϵU. (x could be anything in U)

  …
- (show p(x) is true) ■

Claim: ∃xϵU, p(x)

Proof:

- Let x = (some specific element of U)

  …
- (show p(thaat elt) is true ■

Double Qualifiers

Claim: ∀xϵU, ∃yϵU, p(x, y)

Proof:

- Let xϵU. Let y = (specific elt of U, can depend on x)

  …
- (show p(x, y) is true) ■

Claim: ∃yϵU, ∀xϵU, p(x, y)

Proof:

- Let y = (some specific elt of U)
- Let x ϵ U (could be anything)

  …
- (show p(x,y) is true) ■

Disproving Quantifiers

Claim: ∀x p(x)

Negation: ¬(∀x p(x))

= ∃x ¬p(x)$\hookrightarrow^{countrexample}$

Claim: ∃x p(x)

Negation: ¬(∃x p(x))

= ∀x ¬p(x)$\hookrightarrow^{show\ p(x)\ ALWAYS\ fails}$

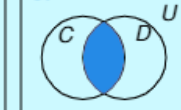
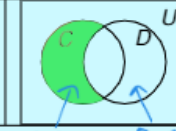
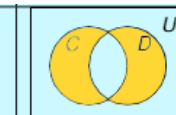
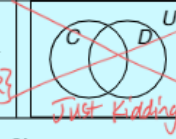
Section 12: Sets

Union, Intersection, Difference, Symmetric difference, complement, and Cartesian product

Let U = {students in this class}

Let C = {students in this class who have had a cat at home}

Let D = {students in this class who have had a dog at home}

Operation	Name	Definition	Venn diagram
$C \cup D$	Union	$\{x : x \in C \text{ or } x \in D\}$	
$C \cap D$	Inter-section	$\{x : x \in C \text{ and } x \in D\}$	
$C - D$ (or $C \setminus D$)	Set difference	$\{x : x \in C \text{ and } x \notin D\}$	
$C \Delta D$	Symmetric difference	$(C - D) \cup (D - C)$	
C^c (or $\overline{C}$)	Comple-ment	$\{x : x \notin C\}$. Also $\{x : \neg(x \in C)\}$	
$C \times D$	Cartesian product	$\{(x, y) : x \in C \text{ and } y \in D\}$	

Note that TFAE: $x \in \overline{C} \Leftrightarrow x \notin C \Leftrightarrow \neg(x \in C)$

Set Properties

Set Properties. In this class 1–6 can be used without proof.
Let A, B and C be any sets. Then:

1. $(A \cap (B \cap C)) = ((A \cap B) \cap C)$. *Intersection is associative.*
2. $A \cap B = B \cap A$. *Intersection is commutative.*
3. $A \cap \varnothing = \varnothing = \varnothing \cap A$. *The empty set is the zero for intersection.*
4. $(A \cup (B \cup C)) = ((A \cup B) \cup C)$. *Union is associative.*
5. $A \cup B = B \cup A$. *Union is commutative.*
6. $A \cup \varnothing = A = \varnothing \cup A$. *The empty set is the identity for union.*
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. *Intersection distributes over union.*
8. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *Union distributes over intersection.*
9. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$. *De Morgan's law part one.*
10. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. *De Morgan's law part two.*

OK to assume

Need to prove e.g. truth tables

There are other simple assumptions you may use during proofs, such as:

- $A \subseteq (A \cup B)$. In other words, $x \in A \to x \in A \cup B$.
- $A \cap B \subseteq A$. In other words, $x \in A \cap B \to x \in A$.
- $(x \in A \cup B$ and $x \notin A) \to x \in B$.

OK to assume

Note these are based directly on the definitions of these operations, plus simple Boolean rules like $((p \wedge q)$ and $\neg p)$ implies q.

Techniques to prove or disprove claims about sets:

Subset both ways: Show S = T by showing S⊆T and T⊆S
Proof by case: (e.g., if a set in question is a union of other sets)
Equivalent Logical Expressions: describe elements of equivalence logical expressions
Counterexample: if claim is false

Section 13: Combinatorial Proofs

Definition:

Combinatorial Proof: a combinatorial proof (counting something 2 ways) proves an equation is true by showing that both sides of the equation are answers to a common question (by counting).

Proof Template:

Clam: LHS = RHS
Proof:

- Question: How many..?
- (LHS) Count it one way to get LHS
- (RHS) Count it a different way to get RHS
- Conclusion: Since they count the same thing, the two sides are equal

Definitions:

n-bit string: An n-bit binary string of length n composed of)s and 1s.

How many n-bit binary strings are there for a fixed n? $\mathbf{2^n}$

Binary Number: a binary number is a natural number expressed in binary, which has a unique description as a binary string that starts with a 1 (unless it's the number 0)

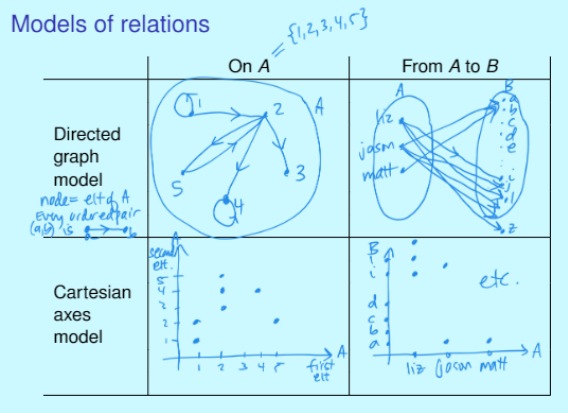
Section 14: Relations

Definitions:

Relations: a relation is a set of ordered pairs

If R⊆A×A then R is a relation on A

If R⊆A×B then R is a relation on A to B



Properties:

Reflexive: if for all x∈A, xRx. [everything is related to itself]

Irreflexive: if for all x∈A, x $\not R$ x [Everything is not related to itself]

Symmetric: if xRy ⇒yRx [for any ordered pair, it's "opposite" (inverse) is also in the relation]

Antismmetric: if (xRy ∧ yRx) ⇒ x = y

Transitive: if (xRy ∧ yRz) ⇒ xRz

Definitions:

Inverse: Given a relation R, the inverse of R, denoted R^{-1}, is the relation formed by reversing the order of all the ordered pairs in R

If R is a relation from A to B, then R^{-1} is a relation from B to A.

Section 15: Equivalence Relations

Definitions:

Equivalence Relation: An equivalence relation is a relation which is reflexive, symmetric, and transitive.

Mod: mod n relation on $\mathbb{Z}$ is given by $R = \{(x,y) : n|(x - y)\}$

xRy is written $x = y \pmod n$ or sometimes $x \equiv y \pmod n$, and we say "x equals y mod n"

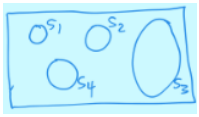
Equivalence Class: If R is an equivalence relation on A and $a \in A$, then the equivalence class of a is all elements related to a.

Section 16: Partitions

Definitions:

Disjoint: Two sets S and T are called disjoint if they do not intersect, that is, if $S \cap T = \emptyset$.

Pairwise disjoint: a collection of sets $S_1, S_2, \ldots, S_n$ is called pairwise disjoint if any two are disjoint, that is, if $S_i \cap S_j = \emptyset$ whenever $i \neq j$.



Partition of: a set of sets with these three properties:

1. They are nonempty
2. They are pairwise disjoint
3. Their union is A

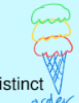
Is called a partition of A.

Parts: the elements of the partition (which are themselves sets) are called the parts (of block) of the partitions

Counting Questions:

Question: How many triple *cones* are there with three distinct flavors chosen from 6?
Question: How many triple *bowls* are there with three distinct flavors chosen from 6?

First we define the set T of cones.
These can be thought of as **lists** of three flavors.



$T = \{$Triple ice cream cones (order matters) with three distinct flavors chosen from Apricot, Banana, Chocolate, Dark chocolate, Eclair and French vanilla$\}$

In order to find the set of bowls, we will group cones together if they have the same flavor, using a relation R.

$R = \{(t_1, t_2) : t_1, t_2 \in T$ and t_1 has the same flavors as $t_2\}$.

The equivalence classes of R will correspond to our bowls.
These can be thought of as **sets** of three flavors.

Underlying Set:

First we will look at T.

$T = \{$Triple ice cream cones (order matters) with three distinct flavors chosen from Apricot, Banana, Chocolate, Dark chocolate, Eclair and French vanilla$\}$ =

ABC,	ACB,	BAC,	BCA,	CAB,	CBA,
ABD,	ADB,	BAD,	BDA,	DAB,	DBA,
ABE,	AEB,	BAE,	BEA,	EAB,	EBA,
ABF,	AFB,	BAF,	BFA,	FAB,	FBA,
ACD,	ADC,	CAD,	CDA,	DAC,	DCA,
ACE,	AEC,	CAE,	CEA,	EAC,	ECA,
ACF,	AFC,	CAF,	CFA,	FAC,	FCA,
ADE,	AED,	DAE,	DEA,	EAD,	EDA,
ADF,	AFD,	DAF,	DFA,	FAD,	FDA,
AEF,	AFE,	EAF,	EFA,	FAE,	FEA,
BCD,	BDC,	CBD,	CDB,	DBC,	DCB,
BCE,	BEC,	CBE,	CEB,	EBC,	ECB,
BCF,	BFC,	CBF,	CFB,	FBC,	FCB,
BDE,	BED,	DBE,	DEB,	EBD,	EDB,
BDF,	BFD,	DBF,	DFB,	FBD,	FDB,
BEF,	BFE,	EBF,	EFB,	FBE,	FEB,
CDE,	CED,	DCE,	DEC,	ECD,	EDC,
CDF,	CFD,	DCF,	DFC,	FCD,	FDC,
CEF,	CFE,	ECF,	EFC,	FCE,	FEC,
DEF,	DFE,	EDF,	EFD,	FDE,	FED,

$|T| = 120$
$= 6 \cdot 5 \cdot 4$

Relation:

Now define the following relation R on T:

$R = \{(t_1, t_2) : t_1, t_2 \in T$ and t_1 has the same flavors as $t_2\}$.

For example,

- $_{ABC}R_{ACB}$, i.e., $(_{ABC},{}_{ACB}) \in R$
- $_{CBF}R_{FBC}$, i.e., $(_{CBF},{}_{FBC}) \in R$

Observations:

1. R is an equivalence relation (why?) Refl Symm Trans
2. R It would be SUPER ANNOYING to write everything in R BUT... $\{(ABC, ACB), (CBF, FBC), \ldots\}$ 3
3. It's easy to show the partition associated to R. ☺

Partition:

Draw the partition given by R here:

ABC	ACB	BAC	BCA	CAB	CBA
ABD	ADB	BAD	BDA	DAB	DBA
ABE	AEB	BAE	BEA	EAB	EBA
ABF	AFB	BAF	BFA	FAB	FBA
ACD	ADC	CAD	CDA	DAC	DCA
ACE	AEC	CAE	CEA	EAC	ECA
ACF	AFC	CAF	CFA	FAC	FCA
ADE	AED	DAE	DEA	EAD	EDA
ADF	AFD	DAF	DFA	FAD	FDA
AEF	AFE	EAF	EFA	FAE	FEA
BCD	BDC	CBD	CDB	DBC	DCB
BCE	BEC	CBE	CEB	EBC	ECB
BCF	BFC	CBF	CFB	FBC	FCB
BDE	BED	DBE	DEB	EBD	EDB
BDF	BFD	DBF	DFB	FBD	FDB
BEF	BFE	EBF	EFB	FBE	FEB
CDE	CED	DCE	DEC	ECD	EDC
CDF	CFD	DCF	DFC	FCD	FDC
CEF	CFE	ECF	EFC	FCE	FEC
DEF	DFE	EDF	EFD	FDE	FED

Counting questions:

1. How many elements are in T? $120 = 6 \cdot 5 \cdot 4$
2. How many elements are in *each equivalence class* of R? $6 = 3 \cdot 2 \cdot 1$
3. Thus, how many equivalence classes are there? $\frac{120}{6} = 20 =$ # bowls

(#lists) / # cones per bowl (#lists per set) = (#sets)

Counting Equivalence Classes:

Theorem: If R is an equivalence relation on a finite set A and all equivalence classes have the same size m then there are $\frac{|A|}{m}$ classes.

Section 17: Binomial Coefficiemts (a.k.a "Choose")

Definitions:

$\binom{n}{k}$ = number of ways to choose k elements from n elements

= $\frac{\#k-elemnt\ lists\ from\ n\ elements\ (no\ repetition)}{\#\ k-elemnt\ lists\ from\ k\ elements\ (no\ repetion)}$

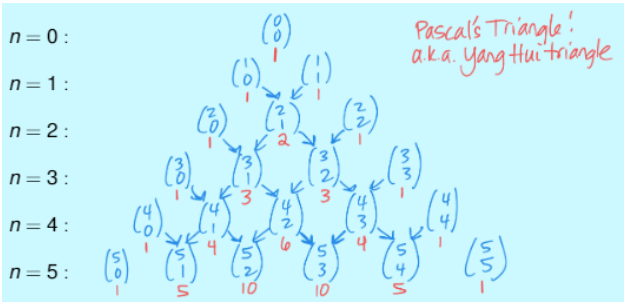
= # k-elements sets from n elements

= $\frac{n(n-1)(n-2)\dots(n-k+1)}{k(k-1)(k-2)\dots(1)} = \frac{n!}{k!\,(n-k)!}$

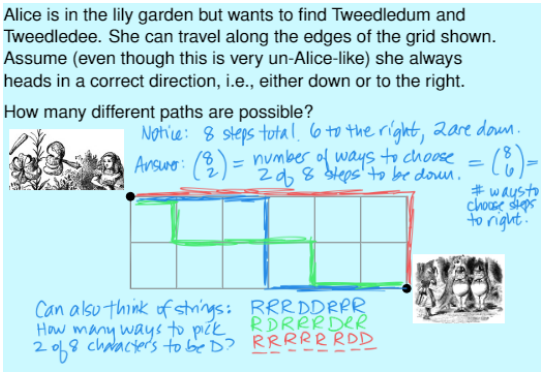
= $\binom{n-1}{k} + \binom{n-1}{k-1}$

"n choose k" = number of k-element subsets of an n-element set

Pascals Triangle:



Lattice Paths:



Section 20: Contradiction and Contrapositive

Proof Templates:

Proof by Contradiction Template #1 Generic:

Claim: p
Proof:
Suppose* FSOC ¬p
…
Contradiction. →←
Thus we conclude p.

Proof by Contradiction Template #2 If-then statements, negating original claim:

Claim: q→r
Proof:
Suppose* FSOC ¬(q→r)
In other words q∧ ¬r
…
Contradiction. →←
Thus q→r

Proof by Contradiction Template #3 If-then statements, contradiction within proof:

Claim: q→r
Proof:
Assume q
Suppose* FSOC ¬r
…
Contradiction. →←
Thus r

Proof by Contrapositive Template:

Claim: p→q [contrapositve ¬q → ¬p is equivlent]
Proof:
Assume ¬q
…
Then ¬p
By the contrapositive, p→q

Defintions:

$\mathbb{Q}$: rational numbers - is a real number that can be written as $\frac{a}{b}$ where a,b ϵ $\mathbb{Z}$

$\mathbb{R}$: real numbers

Lemmas:

Lemma 1 (proved by contradiction): No integer is bith even adn odd

Lemma 2 (proved by smallest counterexample): Every natural number is even or odd

Together, Lemmas 1 and 2 tell us that the integers are in fact exactly partitioned into {{evens}, {odd}}. That is, every integer is even or odd but not both. This allowed us to easily prove that final lemma:

Lemma 3 (proved by contrapositive): For all $x \in \mathbb{Z}$, if x^2 is even then x is even

Section 22: Induction

Theory:

In out proofs we often use a tool of logic called Modus Ponens:

If we assume:	Then we can conclude:
p and $q \rightarrow p$	q

Induction is the repeated application of Modsu Ponens.

Proof Template:

Proof by Induction Template:

Claim: $\forall n \geq n_0$

Base Case: Show $p(n_0)$ is true

Inductive Step:

Assume p(k) is true for some $k \geq n_0$

…

Then p(k+1) is true

Conclusion: Thus p(n) is true for all $n \geq n_0$

Defintions:

Fibonacci Numbers: the Fibonacci Numbers are defined as follows for any positive integer n:

$F_0 = 1$

$F_1 = 1$

$F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7
1	1	2	3	5	8	13	21

Section 22.5: Strong Induction

Proof Template:

Claim: $\forall n \epsilon \mathbb{N}$, p(n)

Base Case: Show p(0) is ture

Strong Inductive Step:

Assume p(0), p(1), …, p(k) are all true for some k≥0

…

Then p(k+1) is true

Conclusion: Thus p(n) is true for all $\mathbb{N}$

Note #1: **Different base case**. If the statement is instead true for all $n \geq n_0$ for some n_0, the base case is $p(n_0)$ and the inductive hypothesis is $p(n_0), p(n_0+1), \ldots p(k)$ for some $k \geq n_0$.

Note #2: **Multiple base cases**. For example, some inductive steps need the previous *two* cases to be true, i.e., in order to prove $p(k+1)$ we must know both $p(k)$ and $p(k-1)$. Then you must prove *two* base cases, otherwise the inductive step cannot "get started."

Definitions:

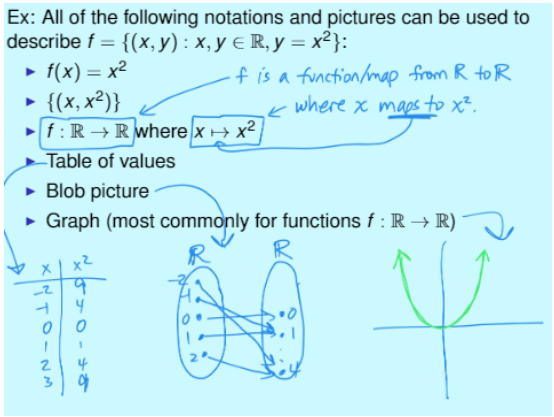
Triangulated Polygon: a triangulated polygon is a polygon that has been divided up into triangles. Specifically, draw diagnals between the vertices so that the vertices of the resulting triangles belong to the original polygon

Exterior Triangles: an exterior triangle is a triangle where two (or three) of the sides belong to the original polygon

Section 24: Functions

Defintions:

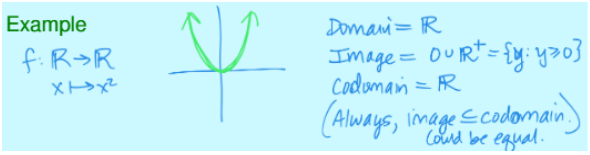
Function: a function f is a relation where (a, b)ϵf and (a,c)ϵf implies b=c



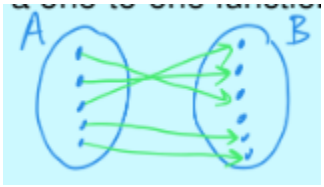
Domain: the domain of a function is Dom(f) ={a: ∃b, (a,b) ϵ f }, namely, the set of all inputs of f

Image: the image of a function is Im(f) = {b : ∃a, (a,b) ϵ f }, namely, the set of all outputs of f

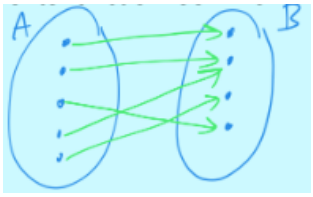
Codomain: when a function is written f : A→B, A is the domain and B is called the codomain, The codomain is a set that contains the image, but is not necessarily equal to the image



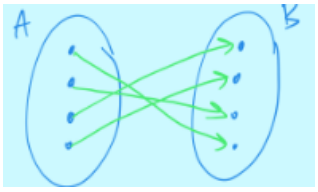
One-to-one: a function is called one-to-oen (or 1:1 or injective) if (a, b) ϵ f and (c, b) ϵ f implies a = c



Onto: a function f : A→B is called onto (or subjective) if for every b ϵ B there is an a ϵ A such that f(a) = b



Bijective: a function is called bijective (or a one-to-one correspondence) if it is injective (one-to-one) and surjective (onto)



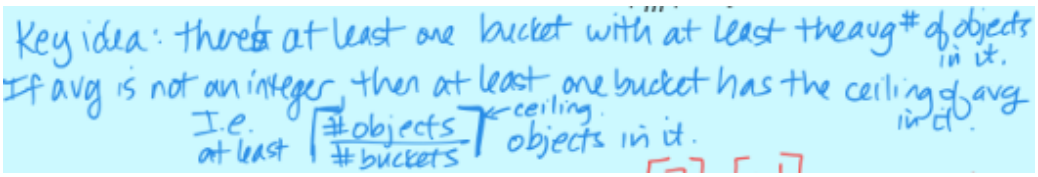
Section 25: Pigeonhole Principle

Defintions:

The Pigeonhole Principle: if f : A→B where A and B are finite and |A|>|B|, then f is not one-to-one. (Thus two distinct inputs must map to the same output)

If |objects|>|buckets|, there's at least one bucket with at least 2 objects

Generalized Pigeonhole Principle: if f : A→B where |A|=n and |B|=m, then ∃bϵB with at least $\lceil \frac{n}{m} \rceil$ elements of A that map to it. In other words, if we are putting n objects into m buckets, there is at least one bucket with $\lceil \frac{n}{m} \rceil$ objects in it.



Proof Template:

For Pigeonhole Principle:

1. Identify buckets (how many?)
2. Identify objects (how many?)
3. Conclude at least one bucket has $\lceil \frac{\#objects}{\#buckets} \rceil$
4. Thus…?

Section 25.5: Cantor's Theorem

Defintions:

Finite: size relation on finite sets A, B:

R = "same-size-as" = {(A, B) : |A| = |B|}

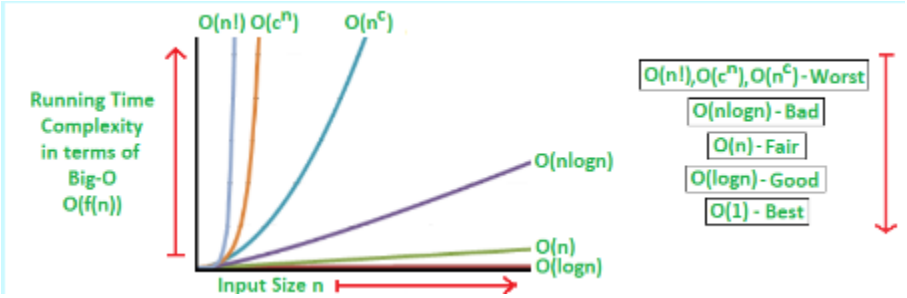
Infinite: size relation on infinite sets A, B:

R = "same-size-as" = {(A, B) : There is bijection from A to B}

Cantor's Theorem: any function $f : A \to 2^A$ cannot be onto.

(thus A is not the same size as 2^A)

Section 29: Big-O



Proof of big-O:

Claim: f(n) = O(g(n))

Proof:

f(n)<...<...<cg(n). (where some of these inequalities might only be true for $n>n_0$)

Thus for this c and all $n \geq n_0$ we have $f(n) \leq cg(n)$

Hence f(n)=O(g(n))

For Algoritms in Computer Science:

- Linear search, Find-Max, Find-Min, $O(n)$
- Binary search, $O(\log n)$
- Selection, $O(n)$
- Insertion sort, $O(n^2)$
- Mergesort, $O(n \log n)$
- Quicksort, $O(n^2)$ (but expected time $O(n \log n)$)
- Euclidean algorithm for gcd(a, b), $O(\log(\min(a, b)))$
- Build-Max-Heap, $O(n \log n)$ or $O(n)$

Section 35: Mod as a Binary Operation

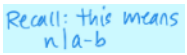
Defintions:

Division Theorem: Let a, b ϵ $\mathbb{Z}$ with b>0, There exist integers q and r such that

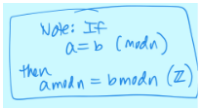
$$a = qb+r \text{ and } 0 \leq r < b$$

Morover, there is only one such pair of integers (q, r) that satisfies these conditions

Equivalnece Relation: the statement a = b (mod n) is either TRUE or FALSE



Binary Operation: the operation a mod b is a NUMBER



Section 36: Euclid's Algorithm

Defintions:

Euclid's Algorithm: Assume a, b ϵ $\mathbb{Z}^+$

```
GCD (a, b)
Let c = a mod b
      if c = 0
            return b
      else
            GCD (b, c)
```

Relatively Prime: Let a, b ϵ $\mathbb{Z}$. We say a and b are relatively prime if gcd(a, b) = 1 (i.e., they have no prime factors in common)

Extended Euclid's Algorithm Proof:

Claim: Given integers a, b $\neq$ 0, the smallest positive element of $\{ax + by : x, y \epsilon \mathbb{Z}\}$ is gcd(a, b)

Proof:

Part 1: you cannot have a positive element of $\{ax + by : x, y \epsilon \mathbb{Z}\}$ which is less than gcd(a, b)

Part 2: gcd(a, b) is indeed an element of $\{ax + by : x, y \epsilon \mathbb{Z}\}$. In other words, there exists x, y ϵ $\mathbb{Z}$ s..t. Ax + by = gcd(a, b). Proof by construction using **Extended Euclid's Algorithm,** as follows:

1. Apply Euclid's algorithm to find gcd(a, b)
2. Rewrite each equation used to compute c (except the last one)
3. Solve for the remainer
4. Plug in from the bottom up

Section 37: Modular Aithmetic

Defintions:

mod n equivalence relation: x and y differ by a multiple of n

$x = y \pmod{n}$ if $n \mid x - y$

Arithmetic in mod n: we define addition and multiplication in mod n by simply adding and multiplying any integers that represent the equivalence clases, then taking the equivalence class of the result. Thus **[a] + [b] = [a + b]** and **[a] * [b] = [ab]**

Inverses: if ab=1 mod n then a and b are multiplicative inverseses. We write:

$b = a^{-1} \bmod n$, and $a = b^{-1} \bmod n$

(b is the inverse of a and a is the inverse of b)

Mod 12:

a	0	1	2	3	4	5	6	7	8	9	10	11
a^{-1}	DNE	1	DNE	DNE	DNE	5	DNE	7	DNE	DNE	DNE	11

Theorem: Let a $\in \mathbb{Z}$. a has an inverse mod n iff a and n are relatively prime.

relatively prime.

How does this relate to the chart for mod 12?

Mod 12:

a	0	1	2	3	4	5	6	7	8	9	10	11
a^{-1}		1				5		7				11

Section 43: Fermat's Little Theorem and Euler's Thorem

Summary of Important Connections:

Let n be a positive integer, and a an element of $\mathbb{Z}_n$.

1. a has an inverse mod n. (here, "inverse" refers to the multiplicative inverse.)
2. a^{-1} exists mod n.
3. There is a b such that $ab = 1 \pmod{n}$.
4. There exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$.
5. $\gcd(a, n) = 1$
6. a and n are relatively prime.

Summary: Inverse Exists iff Relatively Prime

Let n be a positive integer, and a an element of $\mathbb{Z}_n$.

Items that have been grouped by color are the same by definition.

1. a has an inverse mod n. (here, "inverse" refers to the multiplicative inverse.)
2. a^{-1} exists mod n.
3. There is a b such that $ab = 1 \pmod{n}$.

Def of mod n: $n \mid ab-1$, $nk = ab-1$

In mod n, $ny = 0$ so we get $ax = 1 \pmod{n}$

4. There exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. ($in \mathbb{Z}$)

Let $\gcd(a,n) = d$. Since $d \mid a$, $d \mid n$, then $d \mid ax+ny$. But then $d \mid 1$, so $d = 1$.

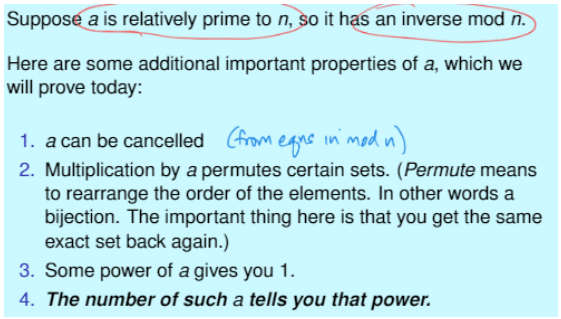
extended Euclid's

5. $\gcd(a, n) = 1$
6. a and n are relatively prime.

BY DEFN

BY DEFN

Additional Properties of a:



Suppose *a* is relatively prime to *n*, so it has an inverse mod *n*.

Here are some additional important properties of *a*, which we will prove today:

1. *a* can be cancelled (from eqns in mod n)
2. Multiplication by *a* permutes certain sets. (*Permute* means to rearrange the order of the elements. In other words a bijection. The important thing here is that you get the same exact set back again.)
3. Some power of *a* gives you 1.
4. ***The number of such a tells you that power.***

Lemmas:

Lemma #1: If a is relatively prime to n, then ab = 0 (mod n)

↓

b = 0 (mod n)

Proof: Suppose a is relatively prime to n, and

ab = 0 (mod n)

Since a is relatively prime, it has an inverse. Multiply by a^{-1} :

$a^{-1} * ab = a^{-1} * 0 \pmod{n}$

Thus bb = 0 (mod n)

Lemma #2: if a is relatively prime to n, then ab - ac (mod n)

↓

b = c (mod n)

Proof: Since a is relatively prime to n, it has an inverse

If ab = ac (mod n), multiply by a^{-1} :

$a^{-1} * ab = a^{-1} * ac$

b = c (mod n)

Lemma #3: If a is relitvely prime to n, then multiplication by a permutes the elements 1, 2, 3, … n - 1.

Proof: By lemma #1,

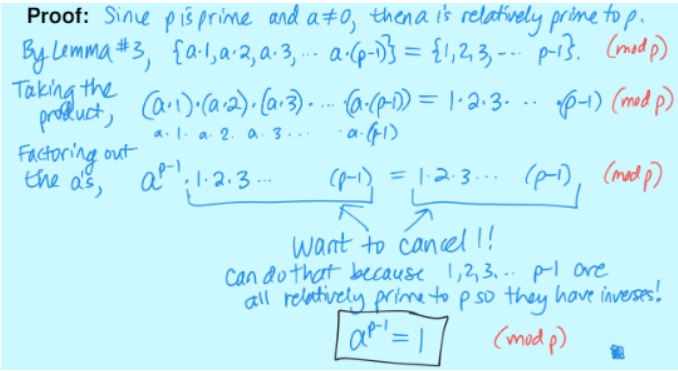
multiplying a by elements in b {1, 2, …, n-1}, never gives 0,
i.e. always gives an element of {1, 2, …, n - 1}

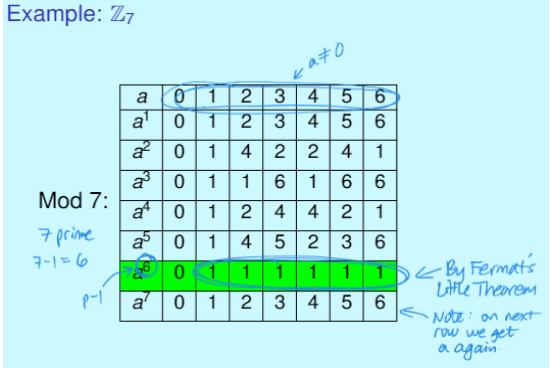
By lemma #2,

multiplying a by different elements {1, 2, …, n-1} gives
DIFFRENT elements of {1, 2, …, n-1}

Since multiplying a by {1, 2, …, n - 1} are all different, we must get the set {1, 2, …, n-1} back again exactly, i.e. a permutation

Fermat's Little Theorem: if p is prime and $a \neq 0 \pmod p$, then $a^{p-1} = 1 \pmod p$





a	0	1	2	3	4	5	6
a^1	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1
a^3	0	1	1	6	1	6	6
a^4	0	1	2	4	4	2	1
a^5	0	1	4	5	2	3	6
a^6	0	1	1	1	1	1	1
a^7	0	1	2	3	4	5	6

Definitions:

$\mathbb{Z}_n^*$ = { a : 1 ≤ a ≤ n, gcd(a, n) = 1} = elements of $\mathbb{Z}_n$ which are relatively prime to n

$\varphi(n) = \left|\mathbb{Z}_n^*\right|$ = phi(n) (Euler's Totient) = #of elements of $\mathbb{Z}_n$ which are relatively prime to n

Lemmas:

Lemma #4: if a, b $\in \mathbb{Z}_n^*$, then ab $\in \mathbb{Z}_n^*$

Proof: Suppose a, b $\in \mathbb{Z}_n^*$. Since they are relatively prime to n, they have inverses a^{-1}, b^{-1}.

Note that $a^{-1}b^{-1} * ab = a^{-1}a * b^{-1}b = 1 * 1 = 1$

So $a^{-1}b^{-1}$ is the inverse of ab.

So ab is relatively prime to n, hence ab$\in \mathbb{Z}_n^*$

Lemma #5: if a is relatively prime to n, then multiplication by a permutes the elements of $\mathbb{Z}_n^*$.

Proof: (similar to proof for lemma #3)

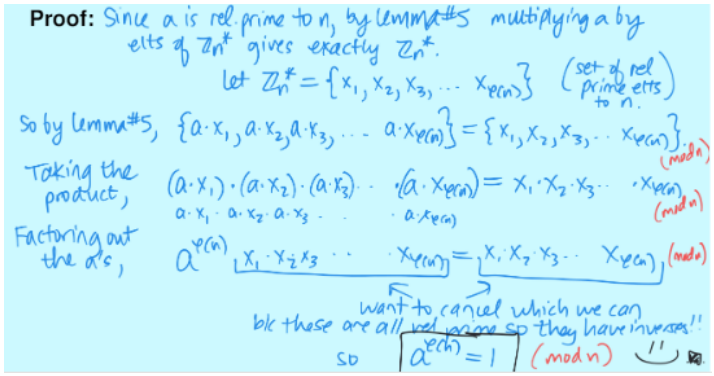
By lemma #4, multiplying a by elements of $\mathbb{Z}_n^*$ gives elements of $\mathbb{Z}_n^*$

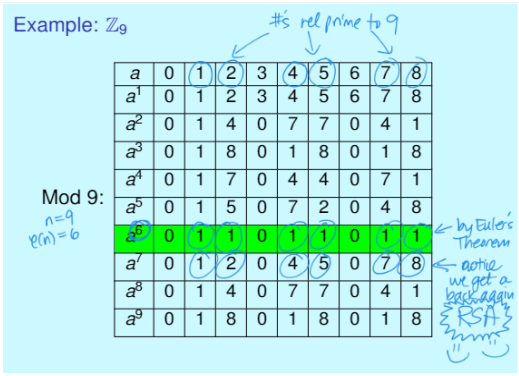
By lemma #2 multiplying a by elements of $\mathbb{Z}_n^*$ gives DIFFRENT elements of $\mathbb{Z}_n^*$

So multtiplying a by $\mathbb{Z}_n^*$ musch give exactly $\mathbb{Z}_n^*$

i.e. it permutes the elements of $\mathbb{Z}_n^*$

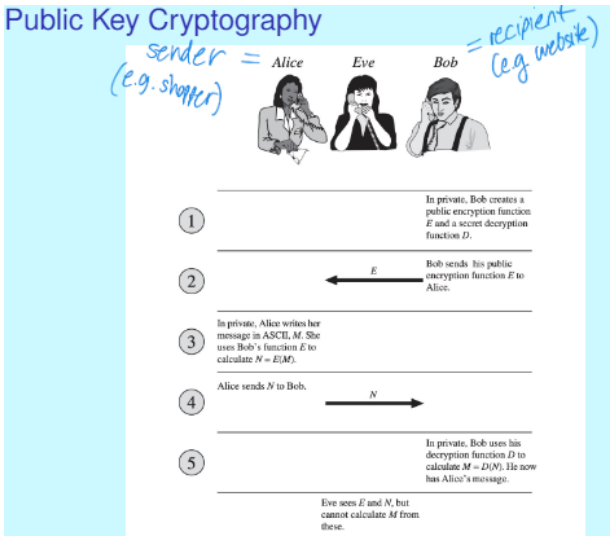
Euler's Theorem: if a is relatively prime to n, then $a^{\varphi(n)} = 1 \pmod{n}$



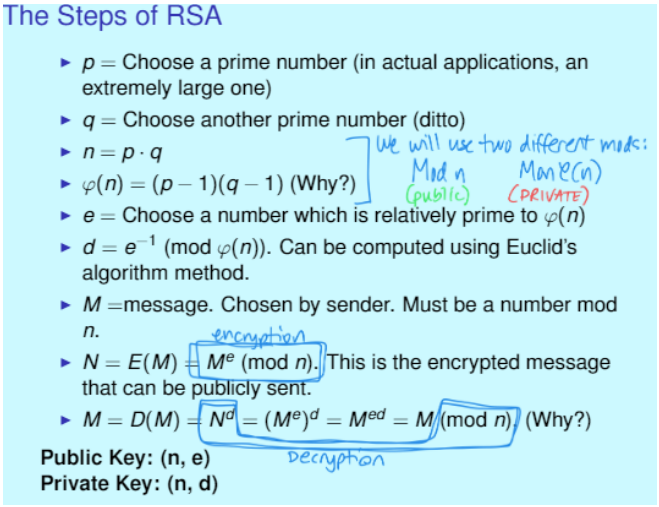


a	0	1	2	3	4	5	6	7	8
a^1	0	1	2	3	4	5	6	7	8
a^2	0	1	4	0	7	7	0	4	1
a^3	0	1	8	0	1	8	0	1	8
a^4	0	1	7	0	4	4	0	7	1
a^5	0	1	5	0	7	2	0	4	8
a^6	0	1	1	0	1	1	0	1	1
a^7	0	1	2	0	4	5	0	7	8
a^8	0	1	4	0	7	7	0	4	1
a^9	0	1	8	0	1	8	0	1	8

Section 44: Public Key Cryptography



Section 46: RSA Cyrptography



Section 47: Graph Theory

Definitions:

Graph: a graph is a (nonempty) set of vertices and a (possible empty) set of edges, each of which connect two vertices.

Mathematically, we define a graph as G = (V, E), where:

V = any nonempty set

E = a set of 2-elemnts subsets of V

V: vertex set of G = V(G)

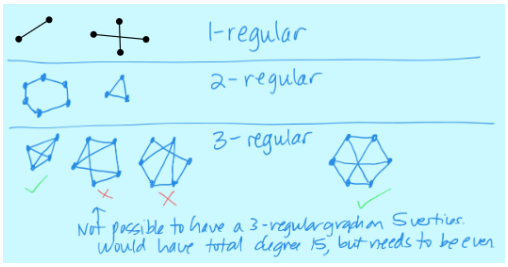
E: edge set of G = E(G)

Incident and Adjacent: If e ={u, v} we say e is **incident** to u and v, and we say u and v are **adjacent**. We also use the shorthand e=uv

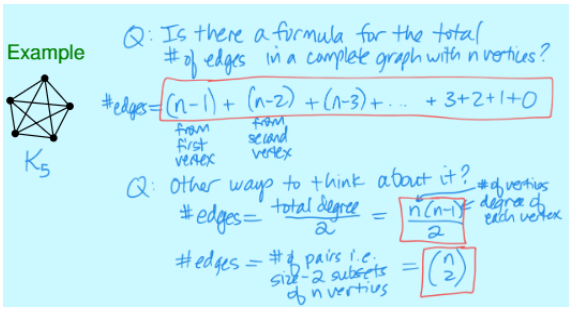
Isomorphism: two graphs are isomorphic is you can relabel they vertices of one graph to obtain the other graph.

Degree: the degree of a vertex d(v) is the number of edges incident to the vertex

Regular graphs: a graph is k-regularr if every vertex has degree k

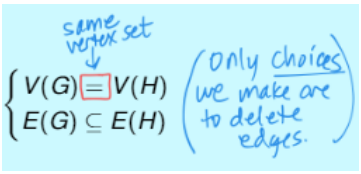


Complete graph: a complete graph contains all possible edges between vertices i.e. a complete graph on n vertices is (n - 1)-regular. The complete graph on n vertices is called K_n



Section 48: Subgraphs

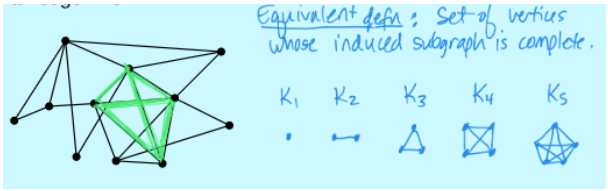
Defintions:



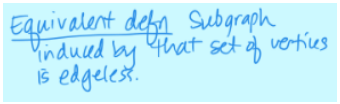
Spanning Subgraph: G is a spanning subgraph of H if

Induced Subgraph: If you only remove edges as a result of removing vertices, then G is an induced subgraph (only choices we make are to remove vertices)

Cliques: Given G, a subset S of V(G) is a clique if every s_i, $s_j \in S$ share an edge in G.



Independent Set: Given G, a subset S of V(G) is an independent set if no s_i, $s_j \in S$ share an edge in G



Complement: the complement of a graph G is a graph H which has the same vertex set but the complementary edge set; that is, e is an edge of H iff e is not an edge of G

Section 49: Connection

Defintions:

Walk: a walk is a sequence of vertices (v_i, v_{i+1}, v_{i+2}, …, v_k) such that every v_j, v_{j+1} is an edge ($i \leq j < k$)
Path: a path is a walk with no repeated vertices
Connected to: a vertex x is connected to a vertex y if there is a path from x to y
Connected: a graph is connected if every pair of vertices is connected
Component: if vertex x is connected to vertex y, then they are in the same component
Cut vertex: if G – v has more components than G, then v is a cut vertex
Cut edge: if G – e has more components than G, then e is a cut edge
Cycle: like a path, but has one repeated vertex: start vertex = end vertex

Section 50: Trees

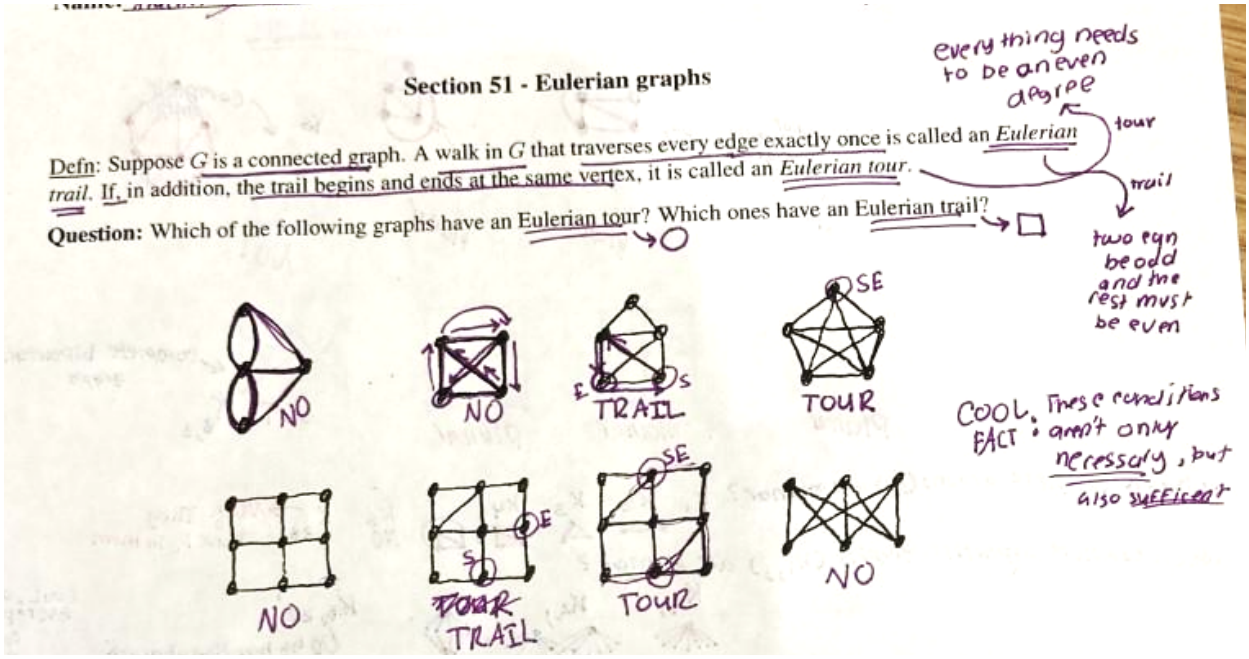
Defintions:

Cycle: a cycle is a walk of at least three vertices with all vertices distinct except the first equals the last
Acyclic: an acyclic graph is a graph with no cycles
Tree: a tree is a connected acrylic graph
Forest: a forest an acyclic graph
Leaf: a leaf is a vertex of degree 1

Based on the results of various proofs, we conclude the following are equivalent:

- *G* is a tree
- *G* is acyclic and connected
- *G* has a unique path between any pair of vertices
- *G* is connected and every edge is a cut edge
- *G* is connected and has $n - 1$ edges

Section 51: Eulerian Walks



Section 51 - Eulerian graphs

Defn: Suppose G is a connected graph. A walk in G that traverses every edge exactly once is called an *Eulerian trail*. If, in addition, the trail begins and ends at the same vertex, it is called an *Eulerian tour*.

Question: Which of the following graphs have an Eulerian tour? Which ones have an Eulerian trail?

everything needs to be an even degree → tour

trail → two can be odd and the rest must be even

NO

NO

TRAIL

TOUR

COOL FACT: These conditions aren't only necessary, but also sufficient

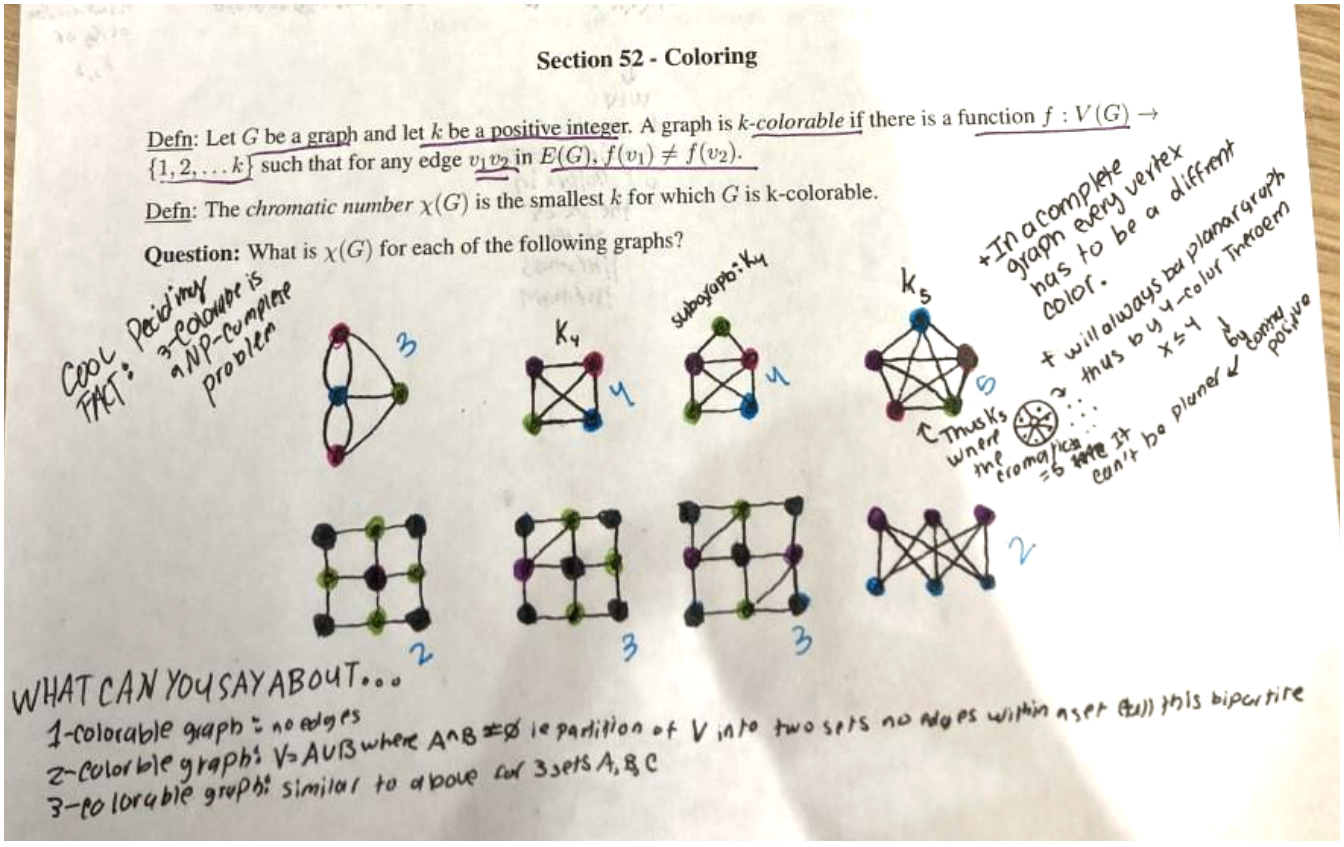
NO

TRAIL

TOUR

NO

Section 52: Graph Coloring



Section 52 - Coloring

Defn: Let G be a graph and let k be a positive integer. A graph is *k-colorable* if there is a function $f : V(G) \to \{1, 2, \ldots k\}$ such that for any edge v_1v_2 in $E(G)$, $f(v_1) \neq f(v_2)$.

Defn: The *chromatic number* $\chi(G)$ is the smallest k for which G is k-colorable.

Question: What is $\chi(G)$ for each of the following graphs?

COOL FACT: Deciding 3-colorable is a NP-complete problem

3

K_4

4

subgraph: K_4

4

K_5

5

Thus χ where the chromatic number is 5 since it can't be planar

+ In a complete graph every vertex has to be a different color.

+ will always be planar graph thus by 4-color Theorem $\chi \leq 4$ by comm. positive

2

3

3

2

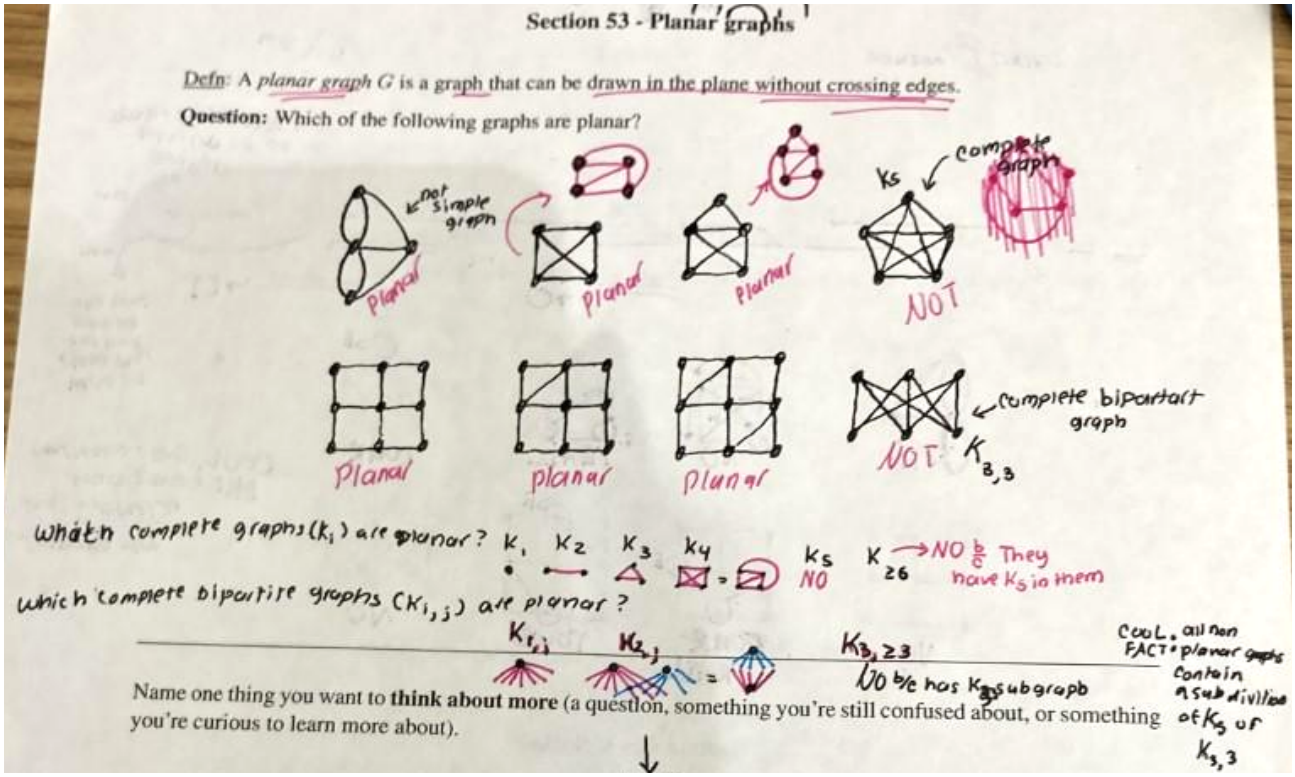
WHAT CAN YOU SAY ABOUT...

1-colorable graph: no edges

2-colorable graph: $V = A \cup B$ where $A \cap B \neq \emptyset$ ie partition of V into two sets no edges within a set (all this bipartite

3-colorable graph: similar to above for 3 sets A, B & C

Section 53: Planarity



Section 53 - Planar graphs

Defn: A *planar graph* G is a graph that can be drawn in the plane without crossing edges.

Question: Which of the following graphs are planar?

not simple graph

Planar

Planar

Planar

K_5

complete graph

NOT

Planar

planar

Planar

NOT

$K_{3,3}$

complete bipartart graph

Whatn complete graphs (K_i) are planar? K_1 K_2 K_3 K_4 K_5 NO $K_{\geq 6}$ → NO b/c They have K_5 in them

Which complete bipartite graphs ($K_{i,j}$) are planar?

$K_{1,j}$ $K_{2,j}$ $K_{3,\geq 3}$ NO b/c has $K_{3,3}$ subgraph

Cool. all non FACT: planar graphs contain a subdivision of K_5 or $K_{3,3}$

Name one thing you want to **think about more** (a question, something you're still confused about, or something you're curious to learn more about).