

# 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

**Statement:** 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:  $p \rightarrow q$

$$\begin{array}{c} \Gamma \quad p \longrightarrow q \quad \Gamma \\ | \quad (\text{hypothesis}) \quad (\text{conclusion}) | \\ \vdash \quad \text{antecedent} \quad \text{consequent} \end{array}$$

Proof:

- Assume  $p$  [assume hypothesis]
- 
- 
- 
- Thus  $q$  ■ [reach conclusions]

    |  
    >[direct logical steps]  
    |

## If-and-only-if Proof

Claim:  $p \leftrightarrow q$  [equivalent to  $p \rightarrow q$  and  $q \rightarrow p$ ]

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  $n, n+1, n+2, \dots, n+(k-1)$ , where  $n \in \mathbb{Z}$ .

Theorem:

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

Claim

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

Proof.

- $(\Rightarrow)$  Assume  $x$  is odd
- Then  $x = 2c+1$  where  $c \in \mathbb{Z}$ .
- So  $x = c + (c+1)$  where  $c \in \mathbb{Z}$ .
- $x$  is the sum of two consec. int.

TRY  
THIS  
FIRST

- $(\Leftarrow)$  Assume  $x$  is the sum of two consec. int.
- So  $x = n + (n+1)$ .
- Thus  $x = 2n+1$  where  $n \in \mathbb{Z}$ .
- Thus  $x$  is odd.

# Section 6: Counterexample

**Prove or Disprove?**

Claim: If  $a|bc$  then  $a|b$  or  $a|c$ . FALSE.

How do you decide?  
Try to prove → play with numbers/concrete numbers

Proof.

- ▶ Assume  $a|bc$
- ▶ Then by defn  $ax = bc$  for some  $x \in \mathbb{Z}$ .
- ▶ So  $a(\frac{x}{c}) = b$  BUT is  $\frac{x}{c} \in \mathbb{Z} ??$
- ▶ Or  $a(\frac{x}{b}) = c$  BUT is  $\frac{x}{b} \in \mathbb{Z} ??$

Ex.  $4|83$  and  $4|8$  but  $4 \nmid 3$   
 $4 \cdot 6 = 83$

CounterEx!  $4|6 \cdot 2$  BUT  $4 \nmid 6$  and  $4 \nmid 2$   
 $\rightarrow a=4, b=6, c=2$ . Note ↗

□

# 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 they are equal for all possible values of their inputs

<b>Implies/Converse/Inverse/Contrapositive</b> <p>Suppose: <math>p \rightarrow q</math></p> <ul style="list-style-type: none"> <li>▶ If I am making pancakes, the kitchen smells good.</li> </ul> <p>Can I also conclude the following?</p> <ul style="list-style-type: none"> <li>▶ CONVERSE: If the kitchen smells good, then I am making pancakes. <math>q \rightarrow p</math></li> <li>▶ INVERSE: Does not follow; Could be making brownies.</li> <li>▶ CONTRAPOSITIVE: If I'm not making pancakes, the kitchen doesn't smell good. <math>\neg p \rightarrow \neg q</math></li> <li>▶ If the kitchen doesn't smell good, I am not making pancakes. <math>\neg q \rightarrow \neg p</math></li> </ul> <p><b>DID</b> DOES follow</p>	<b>Example proof</b> <p>Claim: <math>p \rightarrow q</math> and <math>\neg q \rightarrow \neg p</math> are logically equivalent.</p> <p>Proof.</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse; text-align: center;"> <thead> <tr> <th><math>p</math></th> <th><math>q</math></th> <th><math>\neg p</math></th> <th><math>\neg q</math></th> <th><math>p \rightarrow q</math></th> <th><math>\neg q \rightarrow \neg p</math></th> </tr> </thead> <tbody> <tr> <td>T</td> <td>T</td> <td>F</td> <td>F</td> <td>T</td> <td>T</td> </tr> <tr> <td>T</td> <td>F</td> <td>F</td> <td>T</td> <td>F</td> <td>T</td> </tr> <tr> <td>F</td> <td>T</td> <td>T</td> <td>F</td> <td>T</td> <td>F</td> </tr> <tr> <td>F</td> <td>F</td> <td>T</td> <td>T</td> <td>F</td> <td>T</td> </tr> </tbody> </table> <p>BONUS: These are also logically equivalent. Note they are contrapositives of each other. ↗</p> <p>Note these are the same. Thus they are logically equivalent. ↗</p> <p style="text-align: right;">□</p>	$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$	T	T	F	F	T	T	T	F	F	T	F	T	F	T	T	F	T	F	F	F	T	T	F	T
$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$																										
T	T	F	F	T	T																										
T	F	F	T	F	T																										
F	T	T	F	T	F																										
F	F	T	T	F	T																										

**Boolean Properties:**

$$\begin{aligned} \text{Commutative Laws: } & p \wedge q = q \wedge p \\ & p \vee q = q \vee p \end{aligned}$$

$$\begin{aligned} \text{Associative Laws: } & (p \wedge q) \wedge r = p \wedge (q \wedge r) \\ & (p \vee q) \vee r = p \vee (q \vee r) \end{aligned}$$

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

B = it is a baby	M = it can manage a crocodile
L = it is logical	D = it is despised

Now rewrite each statement using these variables:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Lastly, string these together.

$$B \rightarrow \neg L \rightarrow D \rightarrow \neg M$$

$$\begin{array}{c} B \rightarrow \neg L \\ M \rightarrow \neg D \\ \neg L \rightarrow D \\ \hline \text{Contrapositive:} \\ D \rightarrow \neg M \end{array}$$

What is the overall conclusion, in both math and English?

$B \rightarrow \neg M$ , i.e. babies cannot manage crocodiles.

## 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 Repetition:

List of length k, each element has n possibilities:

$$n^k \text{ possible lists} = \underbrace{[ \quad ]}_{\text{k times}}^{n * n * n * \dots * n}$$

4. How many lists can you make of length 5 using the numbers 1, 2, 3, ..., 10 which contain at least one odd number? (repetition OK)

$$\begin{aligned} & \text{5} \cdot 10 \cdot 10 \cdot 10 \cdot 10 \quad \text{How about } (2, 6, 3, 8, 2)? \\ & \text{Counts every time} \\ & \text{Don't get everything} \quad \text{makes this odd} \\ & \underline{5 \cdot 10 \cdot 10 \cdot 10 \cdot 10 + 10 \cdot 5 \cdot 10 \cdot 10 \cdot 10 + 10 \cdot 10 \cdot 5 \cdot 10 \cdot 10 + 10 \cdot 10 \cdot 10 \cdot 5 \cdot 10 + 10 \cdot 10 \cdot 10 \cdot 10 \cdot 5} \\ & \text{Will be counted too many times.} \\ & \text{All such lists — lists with all evens.} \\ & \text{SUBTRACT } 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 - 5 \cdot 5 \cdot 5 \cdot 5 \\ & \text{COMPLEMENT } [10^5 - 5^5] \end{aligned}$$

### Without Repetition:

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

$$(n - (k - 1)) = \frac{n * (n - 1) * (n - 2) * \dots * (n - k + 1)}{\text{length } k}$$

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

$$\begin{array}{rcl} \text{All lists} & - & \text{all evens.} \\ 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 & - & 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \end{array}$$

## Section 9: Factorial

Definitions:

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

**" $n$  factorial" ( $n!$ ):** for  $n \in \{1, 2, 3, \dots\}$ , define  $n! = n(n-1)(n-2)\dots(3)(2)(1)$

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

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

## Section 10: Sets

Definitions:

**Set:** a set is a repetition-free, unordered collection of objects, called elements. If  $x$  is an element of a set  $A$ , we write  $x \in A$

**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.

**Subset:** for sets  $A, B$ , we say  $A$  is a subset of  $B$  (written  $A \subseteq B$ ) if  $x \in A \rightarrow x \in B$   
i.e., every element of  $A$  is an element of  $B$

### Proving Sets are Equal:

Let  $A, B$  be two sets, To show  $A = B$  ( $x \in A \leftrightarrow x \in B$ ) we show

$A \subseteq B$  ( $x \in A \rightarrow x \in B$ ) and  $B \subseteq A$  ( $x \in B \rightarrow x \in A$ )

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

**Claim:**  $A = B$

**Proof:** (1) 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 consecutive integers.  
Then  $x \in B$ .

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

(2) Suppose  $x \in B$ . Then  $x$  is the sum of 3 consecutive integers.  
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 unusual-looking  $2^S$

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

↑ cardinality of S  
↑ ↑  
the cardinality  
of the power set

## Section 11: Quantifiers

Definitions:

**Qualifiers:** are defined with respect to a universe  $U$ . They either describe something that is true about all elements of  $U$ , or at least one element of  $U$ .

$\forall$  = “for all” (universal quantifier).  
 $\exists$  = “there exists” (existential quantifier).

Proofs:

### Single Qualifiers

Claim:  $\forall x \in U, p(x)$

Proof:

- Let  $x \in U$ . ( $x$  could be anything in  $U$ )  
...  
- (show  $p(x)$  is true) ■

Claim:  $\exists x \in U, p(x)$

Proof:

- Let  $x =$  (some specific element of  $U$ )  
...  
- (show  $p(\text{that elt})$  is true) ■

### Double Qualifiers

Claim:  $\forall x \in U, \exists y \in U, p(x, y)$

Proof:

- Let  $x \in U$ . Let  $y =$  (specific elt of  $U$ , can depend on  $x$ )  
...  
- (show  $p(x, y)$  is true) ■

Claim:  $\exists y \in U, \forall x \in U, p(x, y)$

Proof:

- Let  $y =$  (some specific elt of  $U$ )  
- Let  $x \in U$  (could be anything)  
...  
- (show  $p(x, y)$  is true) ■

## Disproving Quantifiers

Claim:  $\forall x p(x)$

Negation:  $\neg(\forall x p(x))$

$$= \exists x \neg p(x) \text{ ↳ } \text{counterexample}$$

Claim:  $\exists x p(x)$

Negation:  $\neg(\exists x p(x))$

$$= \forall x \neg p(x) \text{ ↳ } \text{show } p(x) \text{ ALWAYS fails}$$

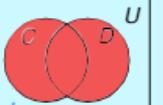
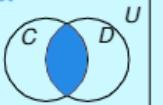
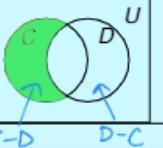
# Section 12: Sets

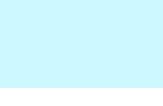
Union, Intersection, Difference, Symmetric difference, complement, and Cartesian product

Let  $U = \{\text{students in this class}\}$

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

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

Operation	Name	Definition	Venn diagram
$C \cup D$	Union	$\{x : x \in C \text{ or } x \in D\}$	
$C \cap D$	Intersection	$\{x : x \in C \text{ and } x \in D\}$	
$C - D$ (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 $\bar{C}$ )	Complement	$\{x : x \notin C\}$ . Also $\{x : \neg(x \in C)\}$	
$C \times D$	Cartesian product	$\{(x, y) : x \in C \text{ and } y \in D\}$ <i>Ex: <math>\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}</math></i>	

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

The Following Are Equivalent

## 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.  $A \cap \emptyset = \emptyset = \emptyset \cap A$ . 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.  $A \cup \emptyset = A = \emptyset \cup A$ . 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:

OK to assume

- ▶  $A \subseteq (A \cup B)$ . In other words,  $x \in A \rightarrow x \in A \cup B$ .
- ▶  $A \cap B \subseteq A$ . In other words,  $x \in A \cap B \rightarrow x \in A$ .
- ▶  $(x \in A \cup B \text{ and } x \notin A) \rightarrow x \in B$ .

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

Techniques to prove or disprove claims about sets:

**Subset both ways:** Show  $S = T$  by showing  $S \subseteq T$  and  $T \subseteq S$

**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:

Claim:  $LHS = RHS$

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 0s and 1s.

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

**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)

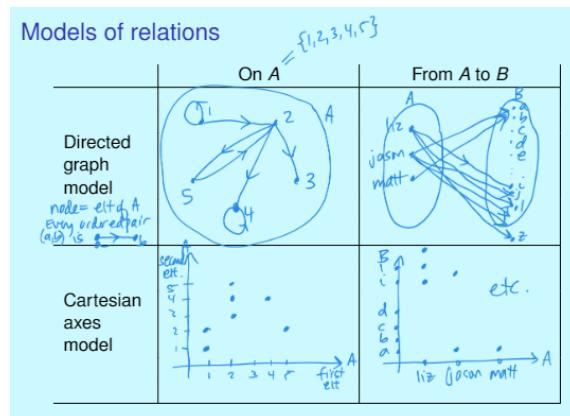
## Section 14: Relations

Definitions:

**Relations:** a relation is a set of ordered pairs

If  $R \subseteq A \times A$  then R is a relation on A

If  $R \subseteq A \times B$  then R is a relation on A to B



Properties:

**Reflexive:** if for all  $x \in A$ ,  $xRx$ . [everything is related to itself]

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

**Symmetric:** if  $xRy \Rightarrow yRx$  [for any ordered pair, its "opposite" (inverse) is also in the relation]

**Antisymmetric:**

**Transitive:** if  $(xRy \wedge yRz) \Rightarrow xRz$

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  $a$ .

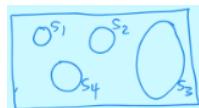
# Section 16: Partitions

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  $S_1, S_2, \dots, S_n$  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 (or 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.



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

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



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  $T$ .

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

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	CD A	DCA	DC A
ACE	AEC	CAE	C EA	EAC	ECA
ACF	AFC	CAF	C FA	FAC	FCA
ADE	AED	DAE	D EA	EAD	EDA
ADF	AFD	DAF	D FA	FAD	FDA
AEF	AFE	EAF	E FA	FAE	FEA
BCE	ECB	CBE	C EB	EBC	E CB
BCF	FCB	CBF	C FB	FBC	F CB
BDE	BED	DBE	D BE	EBD	E DB
BDF	BFD	DBF	D BF	FBD	F DB
BEF	BFE	EBF	E FB	FBE	F EB
CDE	DEC	CED	C ED	ECD	E DC
CFD	DFC	DCF	D FC	FCD	F DC
CEF	CFE	EFC	E FC	FCE	F EC
DEF	DEF	EDF	E FD	FDE	F ED

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

## Relation:

Now define the following relation  $R$  on  $T$ :

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

For example,

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

Observations:

1.  $R$  is an equivalence relation (why?) Refl Symm Trans
2. It would be SUPER ANNOYING to write everything in  $R$  BUT...  $\{(ABC, ACB), (CBF, FBC), \dots\}$
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	CD A	DCA	DC A
ACE	AEC	CAE	C EA	EAC	ECA
ACF	AFC	CAF	C FA	FAC	FCA
ADE	AED	DAE	D EA	EAD	EDA
ADF	AFD	DAF	D FA	FAD	FDA
AEF	AFE	EAF	E FA	FAE	FEA
BCE	ECB	CBE	C EB	EBC	E CB
BCF	FCB	CBF	C FB	FBC	F CB
BDE	BED	DBE	D BE	EBD	E DB
BDF	BFD	DBF	D BF	FBD	F DB
BEF	BFE	EFB	E FB	FBE	F EB
CDE	DEC	CED	C ED	ECD	E DC
CFD	DFC	DCF	D FC	FCD	F DC
CEF	CFE	EFC	E FC	FCE	F EC
DEF	DEF	EDF	E FD	FDE	F ED

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?  $120 = \frac{120}{6} = 20 = \# \text{bowls}$

$\begin{matrix} \# \text{cones} \\ (\# \text{lists per set}) \end{matrix}$

$\begin{matrix} \# \text{bowls} \\ (\# \text{sets per bowl}) \end{matrix}$

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.

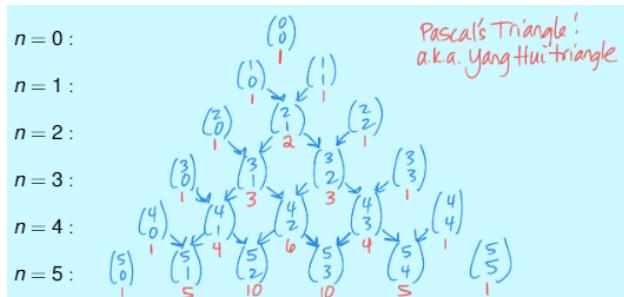
## Section 17: Binomial Coefficients (a.k.a “Choose”)

Definitions:

$$\begin{aligned} \binom{n}{k} &= \text{number of ways to choose } k \text{ elements from } n \text{ elements} \\ &= \frac{\# k - \text{element lists from } n \text{ elements (no repetition)}}{\# k - \text{element lists from } k \text{ elements (no repetition)}} \\ &= \# k - \text{element sets from } n \text{ elements} \\ &= \frac{n(n-1)(n-2) \dots (n-k+1)}{k(k-1)(k-2) \dots (1)} = \frac{n!}{k!(n-k)!} \\ &= \binom{n-1}{k} + \binom{n-1}{k-1} \end{aligned}$$

“ $n$  choose  $k$ ” = number of  $k$ -element subsets of an  $n$ -element set

Pascals Triangle:



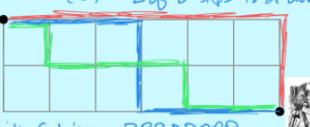
Lattice Paths:

Alice is in the lily garden but wants to find Tweedledum and Tweedledee. She can travel along the edges of the grid shown. Assume (even though this is very un-Alice-like) she always heads in a correct direction, i.e., either down or to the right.

How many different paths are possible?



Notice: 8 steps total, 6 to the right, 2 are down.  
Answer:  $\binom{8}{2} = \text{number of ways to choose } 2 \text{ d} \text{ o } 8 \text{ steps to be down.} = \binom{8}{6} = \# \text{ ways to choose steps to right.}$



Can also think of strings:  
How many ways to pick 2 of 8 characters to be D?  
 $\text{RRR D D R R P}$   
 $\text{R D R R D D R P}$   
 $\text{R R R R R R D D}$

# Section 20: Contradiction and Contrapositive

Proof Templates:

**Proof by Contradiction Template #1 Generic:**

Claim:  $p$

Proof:

Suppose\* FSOC  $\neg p$

...

Contradiction.  $\rightarrow\leftarrow$

Thus we conclude  $p$ .

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

Claim:  $q \rightarrow r$

Proof:

Suppose\* FSOC  $\neg(q \rightarrow r)$

In other words  $q \wedge \neg r$

...

Contradiction.  $\rightarrow\leftarrow$

Thus  $q \rightarrow r$

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

Claim:  $q \rightarrow r$

Proof:

Assume  $q$

Suppose\* FSOC  $\neg r$

...

Contradiction.  $\rightarrow\leftarrow$

Thus  $r$

Proof by Contrapositive Template:

Claim:  $p \rightarrow q$  [contrapositive  $\neg q \rightarrow \neg p$  is equivalent]

Proof:

Assume  $\neg q$

...

Then  $\neg p$

By the contrapositive,  $p \rightarrow q$

Definitions:

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

$\mathbb{R}$ : real numbers

Lemmas:

**Lemma 1 (proved by contradiction):** No integer is both even and 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  $\{\text{evens}\}, \{\text{odd}\}$ . 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 our 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 Modus 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  $n \geq n_0$

Definitions:

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

$$F_0 = 1$$

$$F_1 = 1$$

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

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

# Section 22.5: Strong Induction

**Proof Template:**

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

Base Case: Show  $p(0)$  is true

Strong Inductive Step:

Assume  $p(0), p(1), \dots, p(k)$  are all true for some  $k \geq 0$

...

Then  $p(k+1)$  is true

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

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  $p(n_0), p(n_0+1), \dots, p(k)$  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 diagonals between the vertices so that the vertices of the resulting triangles belong to the original polygon

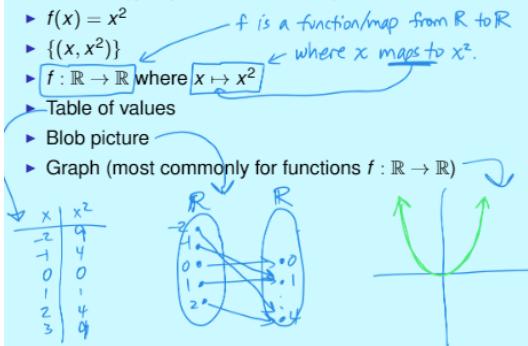
**Exterior Triangles:** an exterior triangle is a triangle where two (or three) of the sides belong to the original polygon

# Section 24: Functions

Definitions:

**Function:** a function  $f$  is a relation where  $(a, b) \in f$  and  $(a, c) \in f$  implies  $b = c$

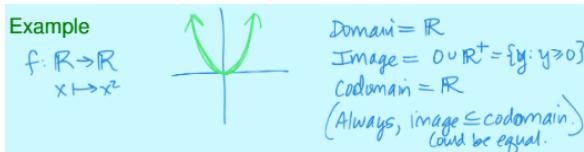
Ex: All of the following notations and pictures can be used to describe  $f = \{(x, y) : x, y \in \mathbb{R}, y = x^2\}$ :

- ▶  $f(x) = x^2$
  - ▶  $\{(x, x^2)\}$
  - ▶  $f : \mathbb{R} \rightarrow \mathbb{R}$  where  $x \mapsto x^2$
  - ▶ Table of values
  - ▶ Blob picture
  - ▶ Graph (most commonly for functions  $f : \mathbb{R} \rightarrow \mathbb{R}$ )
- 

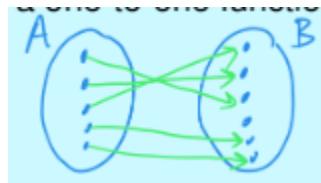
**Domain:** the domain of a function is  $\text{Dom}(f) = \{a : \exists b, (a, b) \in f\}$ , namely, the set of all inputs of  $f$

**Image:** the image of a function is  $\text{Im}(f) = \{b : \exists a, (a, b) \in f\}$ , namely, the set of all outputs of  $f$

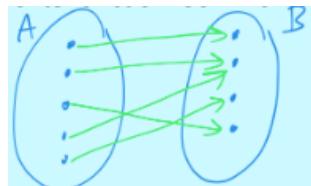
**Codomain:** when a function is written  $f : A \rightarrow B$ , A is the domain and B is called the codomain. The codomain is a set that contains the image, but is not necessarily equal to the image



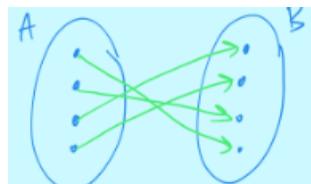
**One-to-one:** a function is called one-to-one (or 1:1 or injective) if  $(a, b) \in f$  and  $(c, b) \in f$  implies  $a = c$



**Onto:** a function  $f : A \rightarrow B$  is called onto (or subjective) if for every  $b \in B$  there is an  $a \in A$  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

Definitions:

**The Pigeonhole Principle:** if  $f : A \rightarrow B$  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  $|\text{objects}| > |\text{buckets}|$ , there's at least one bucket with at least 2 objects

**Generalized Pigeonhole Principle:** if  $f : A \rightarrow B$  where  $|A| = n$  and  $|B| = m$ , then  $\exists b \in B$  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.

Key idea: there's at least one bucket with at least the avg # of objects in it.  
If avg is not an integer, then at least one bucket has the ceiling of avg i.e.  $\lceil \frac{\# \text{objects}}{\# \text{buckets}} \rceil$  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  $\lceil \frac{\# \text{objects}}{\# \text{buckets}} \rceil$
4. Thus...?

## Section 25.5: Cantor's Theorem

Definitions:

**Finite:** size relation on finite sets A, B:

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

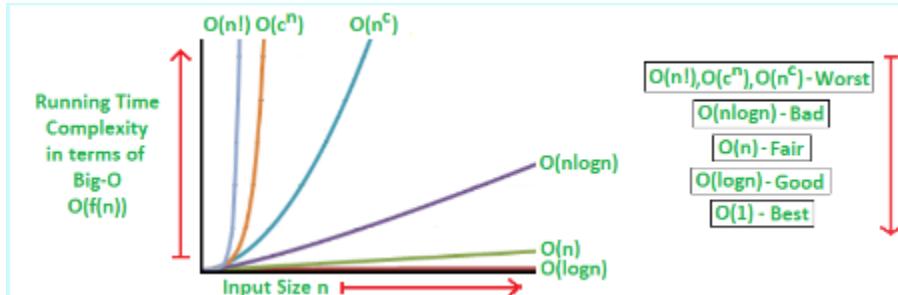
**Infinite:** size relation on infinite sets A, B:

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

**Cantor's Theorem:** any function  $f : A \rightarrow 2^A$  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:

$f(n) < \dots < \dots < c g(n)$ . (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  $f(n) \leq c g(n)$

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

For Algorithms 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

Definitions:

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

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

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

**Equivalence Relation:** the statement  $a \equiv b \pmod{n}$  is either TRUE or FALSE

Recall: this means  
 $n \mid a - b$

**Binary Operation:** the operation  $a \bmod b$  is a NUMBER

Note: If  
 $a \equiv b \pmod{n}$   
then  
 $a \bmod n = b \bmod n \quad (\mathbb{Z})$

# Section 36: Euclid's Algorithm

Definitions:

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

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

**Relatively Prime:** Let  $a, b \in \mathbb{Z}$ . 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  $\{ax + by : x, y \in \mathbb{Z}\}$  is  $\gcd(a, b)$

Proof:

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

Part 2:  $\gcd(a, b)$  is indeed an element of  $\{ax + by : x, y \in \mathbb{Z}\}$ . In other words, there exists  $x, y \in \mathbb{Z}$  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 remainder
4. Plug in from the bottom up

# Section 37: Modular Arithmetic

Definitions:

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

$$x \equiv y \pmod{n} \text{ if } n \mid x - y$$

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

**Inverses:** if  $ab=1 \pmod{n}$  then  $a$  and  $b$  are multiplicative inverses. We write:

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

( $b$  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

$\begin{matrix} -1 \\ 11 \end{matrix}$

**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 Theorem

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.

- 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:  
 $n \nmid ab - 1$   
 $\Rightarrow nk = ab - 1$

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  $\gcd(a, n) = d$   
 $\text{Since } d \mid a, d \mid n, \text{ then } d \mid ax$   
 $\text{But } d \mid n, \text{ so } d \mid 1$

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

## 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 egns 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  $ab = 0 \pmod{n}$**

↓

$$b = 0 \pmod{n}$$

Proof: Suppose  $a$  is relatively prime to  $n$ , and

$$ab = 0 \pmod{n}$$

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

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

$$\text{Thus } bb = 0 \pmod{n}$$

**Lemma #2: if  $a$  is relatively prime to  $n$ , then  $ab - ac \pmod{n}$**

↓

$$b = c \pmod{n}$$

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

If  $ab = ac \pmod{n}$ , multiply by  $a^{-1}$ :

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

$$b = c \pmod{n}$$

**Lemma #3: If  $a$  is relatively prime to  $n$ , then multiplication by  $a$  permutes the elements  $1, 2, 3, \dots, n - 1$ .**

Proof: By lemma #1,

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

By lemma #2,

multiplying  $a$  by different elements  $\{1, 2, \dots, n-1\}$  gives  
DIFFERENT elements of  $\{1, 2, \dots, n-1\}$

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

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

**Proof:** Since  $p$  is prime and  $a \neq 0$ , then  $a$  is relatively prime to  $p$ .  
 By Lemma #3,  $\{a \cdot 1, a \cdot 2, a \cdot 3, \dots, a \cdot (p-1)\} = \{1, 2, 3, \dots, p-1\} \pmod{p}$ .  
 Taking the product,  $(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdots (a \cdot (p-1)) = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$   
 Factoring out the  $a$ 's,  $a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$   
 Want to cancel!!  
 Can do that because  $1, 2, 3, \dots, p-1$  are all relatively prime to  $p$  so they have inverses!  
 $a^{p-1} = 1 \pmod{p}$

Example:  $\mathbb{Z}_7$

Mod 7:  
 $\Rightarrow$  prime  
 $\Rightarrow 1=6$   
 $\Rightarrow p-1=6$

$a$	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

$\downarrow a \neq 0$

By Fermat's Little Theorem  
 Note: on next row we get a again

Definitions:

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

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

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 DIFFERENT

elements of  $\mathbb{Z}_n^*$

So multiplying  $a$  by  $\mathbb{Z}_n^*$  must 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  $a^{\phi(n)} \equiv 1 \pmod{n}$

**Proof:** Since  $a$  is rel prime to  $n$ , by Lemma #5 multiplying  $a$  by elts of  $\mathbb{Z}_n^*$  gives exactly  $\mathbb{Z}_n^*$ .  
 let  $\mathbb{Z}_n^* = \{x_1, x_2, x_3, \dots, x_{\phi(n)}\}$  (set of rel prime elts to  $n$ ).  
 So by lemma #5,  $\{a \cdot x_1, a \cdot x_2, a \cdot x_3, \dots, a \cdot x_{\phi(n)}\} = \{x_1, x_2, x_3, \dots, x_{\phi(n)}\} \pmod{n}$   
 Taking the product,  $(a \cdot x_1) \cdot (a \cdot x_2) \cdot (a \cdot x_3) \cdots (a \cdot x_{\phi(n)}) \equiv x_1 \cdot x_2 \cdot x_3 \cdots x_{\phi(n)} \pmod{n}$   
 Factoring out the  $a$ 's,  $a^{\phi(n)} \cdot x_1 \cdot x_2 \cdot x_3 \cdots x_{\phi(n)} \equiv x_1 \cdot x_2 \cdot x_3 \cdots x_{\phi(n)} \pmod{n}$   
 want to cancel which we can  
 b/c those are all rel prime so they have inverses!!  
 so  $a^{\phi(n)} \equiv 1 \pmod{n}$  !!

Example:  $\mathbb{Z}_9$

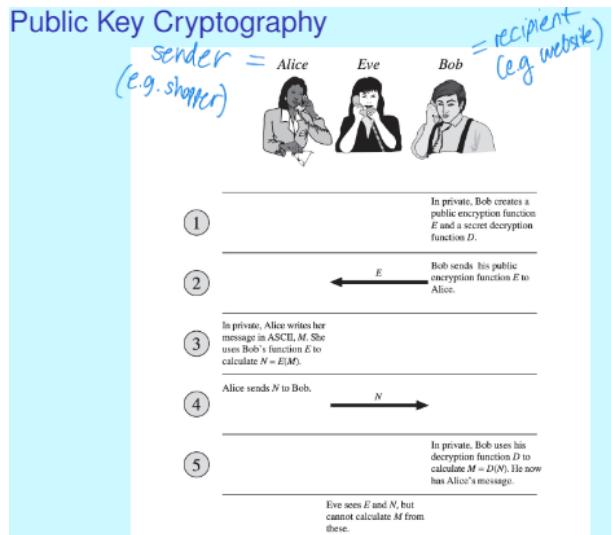
Mod 9:  
 $n=9$   
 $\phi(n)=6$

#'s rel prime to 9

$a$	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

by Euler's Theorem  
 notice we get a back again RSA ??

## Section 44: Public Key Cryptography



# Section 46: RSA Cryptography

## The Steps of RSA

- ▶  $p$  = Choose a prime number (in actual applications, an extremely large one)
  - ▶  $q$  = Choose another prime number (ditto)
  - ▶  $n = p \cdot q$
  - ▶  $\varphi(n) = (p - 1)(q - 1)$  (Why?)
  - ▶  $e$  = Choose a number which is relatively prime to  $\varphi(n)$
  - ▶  $d = e^{-1} \pmod{\varphi(n)}$ . Can be computed using Euclid's algorithm method.
  - ▶  $M$  = message. Chosen by sender. Must be a number mod  $n$ .
  - ▶  $N = E(M) = M^e \pmod{n}$ . This is the encrypted message that can be publicly sent.
  - ▶  $M = D(M) = N^d = (M^e)^d = M^{ed} = M \pmod{n}$  (Why?)
- Public Key:  $(n, e)$       Decryption  
Private Key:  $(n, d)$

We will use two different mods:  
 $\text{Mod } n$  (public)       $\text{Mod } \varphi(n)$  (private)

# 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-elements subsets of  $V$

$V$ : vertex set of  $G = V(G)$

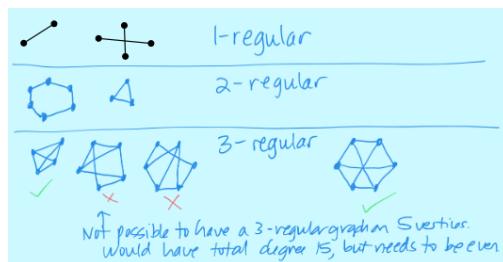
$E$ : edge set of  $G = E(G)$

**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 if you can relabel their 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  $k$ -regular 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  $K_n$

Example



Q: Is there a formula for the total # of edges in a complete graph with  $n$  vertices?

$$\# \text{edges} = (n-1) + (n-2) + (n-3) + \dots + 3+2+1+0$$

from first vertex      from second vertex

Q: other ways to think about it?

$$\# \text{edges} = \frac{\text{total degree}}{2} = \frac{n(n-1)}{2}$$

# of vertices      degree of each vertex

$$\# \text{edges} = \frac{\# \text{of pairs i.e. size-2 subsets of } n \text{ vertices}}{2} = \binom{n}{2}$$

## Section 48: Subgraphs

Definitions:

same set  
 $\downarrow$

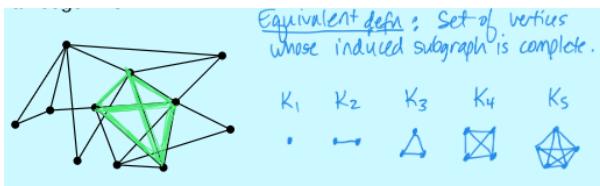
$$\begin{cases} V(G) = V(H) \\ E(G) \subseteq E(H) \end{cases}$$

(Only choices we make are to delete edges.)

**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)

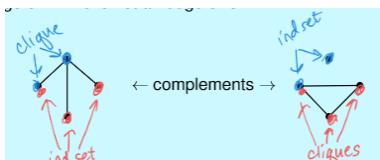
**Cliques:** Given  $G$ , a subset  $S$  of  $V(G)$  is a clique if every  $s_i, s_j \in S$  share an edge in  $G$ .



**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  $G$

Equivalent defn: Subgraph induced by that set of vertices is edgeless.

**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

Definitions:

**Walk:** a walk is a sequence of vertices  $(v_i, v_{i+1}, v_{i+2}, \dots, v_k)$  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

Definitions:

**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 acyclic 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 tour. If, in addition, the trail begins and ends at the same vertex, it is called an Eulerian trail.

Question: Which of the following graphs have an Eulerian tour? Which ones have an Eulerian trail?  $\rightarrow \square$

The page contains several hand-drawn graphs for analysis:

- A graph with two vertices connected by three edges forming a triangle; it is labeled "NO".
- A complete graph  $K_4$  with four vertices and all possible edges; it is labeled "NO".
- A graph with four vertices in a square arrangement, where each vertex is connected to its neighbors and one additional vertex outside the square; it is labeled "TRAIL".
- A graph with five vertices in a pentagonal arrangement, where each vertex is connected to all other vertices; it is labeled "TOUR".
- A 3x3 grid graph; the bottom-left vertex is labeled "NO", while the top-right vertex is labeled "SE".
- A 3x3 grid graph with a path from the bottom-left to the top-right vertex; it is labeled "TOUR TRAIL".
- A graph with six vertices in a hexagonal arrangement; the top vertex is labeled "SE", and the bottom-right vertex is labeled "TOUR".
- A graph with four vertices in a square arrangement, where each vertex is connected to all other vertices; it is labeled "NO".

Annotations on the right side of the page include:

- "every thing needs to be an even degree" with arrows pointing to the  $K_4$  and the 6-vertex hexagonal graphs.
- "two can be odd and the rest must be even" with an arrow pointing to the 3x3 grid graphs.
- "COOL FACT: These conditions are not only necessary, but also sufficient!" with an arrow pointing to the 6-vertex hexagonal graph.

# 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  $f : V(G) \rightarrow \{1, 2, \dots, k\}$  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?

The page shows several hand-drawn graphs for coloring analysis:

- A graph with three vertices in a triangle, each colored with a different color; it is labeled "3".
- A complete graph  $K_4$  with four vertices, each colored with a different color; it is labeled "4".
- A graph with four vertices in a square arrangement, each colored with a different color; it is labeled "4".
- A complete graph  $K_5$  with five vertices, each colored with a different color; it is labeled "5".
- A 3x3 grid graph with each cell vertex colored with a different color; it is labeled "2".
- A 3x3 grid graph with a specific coloring pattern; it is labeled "3".
- A 3x3 grid graph with a different coloring pattern; it is labeled "3".
- A graph with four vertices in a square arrangement, each colored with a different color; it is labeled "2".

Annotations on the right side of the page include:

- "Cool Fact: Partitioning a graph is an NP-complete problem" with an arrow pointing to the  $K_4$  graph.
- "In a complete graph every vertex has to be a different color." with an arrow pointing to the  $K_5$  graph.
- "will always be planar graphs thus by 4-color theorem  $\chi \leq 4$ " with an arrow pointing to the 3x3 grid graphs.
- "thus where the chromatic number  $\geq 6$  take it can't be planar" with an arrow pointing to the  $K_5$  graph.

At the bottom left, the text "WHAT CAN YOU SAY ABOUT..." is followed by definitions of graph colorability:

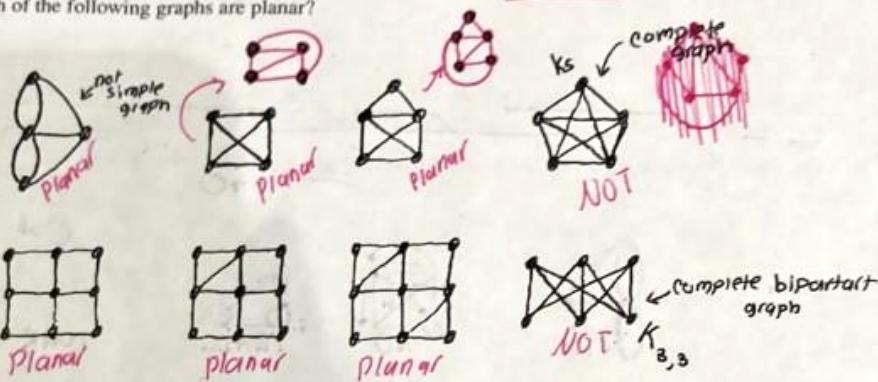
- 1-colorable graph: no edges
- 2-colorable graph:  $V = A \cup B$  where  $A \cap B = \emptyset$  i.e. partition of  $V$  into two sets no edges within a set (all edges within a set)
- 3-colorable graph: similar to above for 3 sets  $A, B, C$

# Section 53: Planarity

## Section 53 - Planar graphs

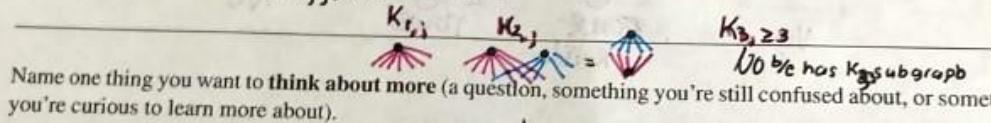
Defn: A planar graph  $G$  is a graph that can be drawn in the plane without crossing edges.

Question: Which of the following graphs are planar?



Which complete graphs ( $K_i$ ) are planar?  $K_1$ ,  $K_2$ ,  $K_3$ ,  $K_4$   $\rightarrow$  NO  $K_5 \rightarrow$  NO  $\rightarrow$  They have  $K_3$ 's in them

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



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).

Cool, all non-  
FACT: planar graphs  
contain a subdivision  
of  $K_3$  or  
 $K_{3,3}$