LaTeX Condensed Concepts Notes

saffron_

Contents

Number Sets

- set: collection of objects
- $x \in X$ means x is an element of X (extends to $\notin$)
- $\mathbb{N}$: natural numbers ($\{0, 1, 2, 3, \dots\}$)
  - domain $[0, \infty)$
  - $+/\times$ of two $\mathbb{N}$ is still $\mathbb{N}$
  - has commutativity, associativity, distributivity of $+/\times$
- $\mathbb{Z}$: integers ($\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$)
  - domain $(-\infty, \infty)$
  - $+/-/\times$ of two $\mathbb{Z}$ is still $\mathbb{Z}$
  - $\mathbb{Z}^+$: positive integers ($\{1, 2, 3, 4, \dots\}$)
  - **Defn:** For $a, b \in \mathbb{Z}$, we say *a divides b* ($a \mid b$), iff $\exists c \in \mathbb{Z}$ s.t. $b = ac$
  - **Thrm 2.1.1** (Divisibility is Transitive). *Let $a, b, c \in \mathbb{Z}$. If $c|b$ and $b|a$, then $c|a$*
  - **Defn:** Let $n \in \mathbb{Z}$. Then n is even iff $2 \mid n$ and odd iff $2 \nmid n$
  - **Thrm 2.1.2** (The Division Theorem). *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There are unique integers q, r s.t. $a = bq + r$ with $0 \leq r < |b|$*
    ie $\forall a, b \in \mathbb{Z}, (b \neq 0 \Rightarrow \exists! q, r \in \mathbb{Z}, (a = bq + r \wedge 0 \leq r < |b|))$
- $\mathbb{Q}$: rational numbers (all numbers $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$)
  - domain $(-\infty, \infty)$
  - $+/-/\times/\div$ (except 0) of two $\mathbb{Q}$ is still $\mathbb{Q}$
- $\mathbb{R}$: real numbers (the entire number line)
  - domain $(-\infty, \infty)$
  - $+/-/\times/\div$ (except 0) of two $\mathbb{R}$ is still $\mathbb{R}$
  - $\times$ two nonzero $\mathbb{R}$ is nonzero (applies to the rest)
  - real $r \in \mathbb{R}$ is *irrational* iff $r \in \mathbb{Q}$

Sets

Polynomials over Number Sets

- *single variable polynomial* over S with respect to x:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \text{ where } n \in \mathbb{N} \text{ and each } a_i \in S \text{ for } 0 \leq i \leq n$$

  - $a_0, a_1, \ldots, a_n$ are called *coefficients*
  - *degree* of a polynomial: largest $i \in \mathbb{N}$ s.t. $a_i \neq 0$
  - *zero polynomial* defined as degree $-\infty$
  - denoted $p(x)$ where x is the indeterminate

- $S[x]$, read "S adjoin x": set of all polynomials with coefficients from S
  - **eg:** $\mathbb{Z}[x]$ is set of poly.s with integer coeff.s — $5x^2+2x \in \mathbb{Z}[x], \in \mathbb{Q}[x]$, and $\in \mathbb{R}[x]$

Set Notation

- **Roster notation** (informal): $A = \{1, 2\}$, $B = \{2, 4, 6, \ldots\}$
- **Set-Builder notation:** $\{x \in S \mid p(x)\}, A = \{x \in \mathbb{N} \mid x \leq 5\}$ (use | or :)
- Alternate Set-Builder (informal): $\{expression(x) \mid x \in S\}, E = \{2n \mid n \in \mathbb{Z}\}$

Other Special Sets

- $\varnothing$ = empty set = $\{\}$
- for $n \in \mathbb{N}, [n]$ = first n positive $\mathbb{Z}$ ($[3] = \{1, 2, 3\}$)

Set Equality and Subsets

- set A is a *subset* of set B ($A \subseteq B$) iff every element in A is also an element of B
- $A = B$ iff $A \subseteq B$ and $B \subseteq A$
- $A \nsubseteq B$: A not a subset of B
- $A \subsetneq B$: A is a *proper subset* of B (ie $A \subseteq B, A \neq B$)

Logic

Symbolic Notation

- For $x \in \mathbb{R}$,
  - *floor* of x: greatest $n \in \mathbb{Z}, n \leq x$.
  - *ceiling* of x: least $n \in \mathbb{Z}, x \leq n$.
- *propositional variable:* a symbol representing the proposition (eg p, q, etc)
- *propositional formula:* either a prop. variable or expression built from them and connectives (logical operators)
  - **Conjunction** ($p \wedge q$): "and"
  - **Disjunction** ($p \vee q$): "or"
  - **Negation** ($\neg p$): "not"
  - **Logical Implication** ($p \Rightarrow q$): "if p then q"
    * p is called the *hypothesis*, *supposition*, or *antecedent*
    * q is called the *consequent* or *conclusion*
    * $q \Rightarrow p$ is the *converse* of $p \Rightarrow q$
    *

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

  - **Biconditional Operator** ($p \Leftrightarrow q$): "p iff q"
    * if $p \Leftrightarrow q$ is a tautology, p and q are *logically equivalent* ($\equiv$)
    *

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$p \Rightarrow q \wedge q \Rightarrow p$ aka $p \Leftrightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

- *tautology:* propositional formula that is always **true** no matter how T/F is assigned
- *contradiction:* proposition that is known or assumed to be **false**

Equivalences

- **Thrm 3.2.1** (DeMorgan's Laws for Connectives).
  (i) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
  (ii) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- Other important equivalences
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ (distributivity)
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (distributivity part 2)
  - (commutativity, associativity, double negation)
  - $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ (biconditional equivalence)
  - $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ (contraposition)
  - $p \Rightarrow q \equiv \neg p \vee q$ (disjunctive form of implication)

Quantifiers

- a variable x is *free* iff you can sub in elements for x. Otherwise, it is *bound*.
- *predicate:* statement involving free variables, denoted $p(x_1, x_2, \ldots, x_n)$
- *quantifiers:* $\forall$: "for all," $\exists$: "there exists," $\exists!$: "there exists only one"

Maximally Negating Propositions

- **Thrm 5.1.1** (DeMorgan's Laws for Quantifiers).
  (i) $\neg(\forall x \in S, p(x)) \equiv \exists x \in S, \neg p(x)$
  (ii) $\neg(\exists x \in S, p(x)) \equiv \forall x \in S, \neg p(x)$
- a proposition is *maximally negated* iff only $\neg$ s appear immediately before a predicate or propositional variable

Proof Writing

- Proving Universal Statements ($\forall x \in S, p(x)$)
  - Direct: let $x \in S$ be arbitrary and fixed, prove p(x) true
  - Indirect: AFSOC $\exists x \in S, \neg p(x)$ and find a contradiction
- Proving Existential Statements ($\exists x \in S, p(x)$)
  - Direct: give an element $x \in S$, show $p(x)$ is true
  - Indirect: AFSOC $\forall x \in S, \neg p(x)$ and find a contradiction
- Proving Conditional Statements ($p \Rightarrow q$)
  - Direct: assume p is true. show q is true
  - Indirect:
    * by contraposition: recall $\neg q \Rightarrow \neg p$. assume $\neg q$. show $\neg p$.
    * by contradiction: assume $p \wedge \neg q$ and find a contradiction
- Proving Biconditional Statements ($p \Leftrightarrow q$)
  - prove $p \Rightarrow q$ and $q \Rightarrow p$
- Proving Disjunctions ($\vee, \wedge$)
  - proving $(p \vee q) \Rightarrow r$ directly (with 2 cases)
    * **Case 1:** assume p holds, show r holds
    * **Case 2:** assume q holds, show r holds
    * no distinction between cases 1 and 2? use WLOG
  - proving $p \Rightarrow (q \vee r)$ directly
    * assume p is true
    * if q holds then we're done, so...
    * assume $\neg q$ holds and prove r holds
- Proving Existence and Uniqueness ($\exists! x \in S, p(x)$)
  - Existence: prove $\exists x \in S, p(x)$
  - Uniqueness: Let $a, b \in S$ s.t. both $p(a)$ and $p(b)$ hold. show that $a = b$

Sets (Part 2)

- *power set of* A ($\mathcal{P}(A)$): set of all subsets of A
  - for any set A, $\varnothing \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$

Set Proofs

- *Containment* (prove $A \subseteq B$): Fix an arbitrary $a \in A$, show $a \in B$, conclude $a \subseteq B$
- *Double Con.* (prove $A = B$): prove $A \subseteq B$, prove $B \subseteq A$, conclude $A = B$
- chain of $\Leftrightarrow$'s (prove $A = B$): fix arb $x \in U$, show $x \in A \Leftrightarrow x \in B$ with iff's

Set Operations

- **Set Intersection**: $A \cap B = \{x \in U \mid x \in A \wedge x \in B\}$ (A and B are *disjoint* iff $A \cap B = \varnothing$)
- **Set Union**: $A \cup B = \{x \in U \mid x \in A \vee x \in B\}$
- **Set Difference**: $A \setminus B = \{x \in U \mid x \in A \wedge x \notin B\}$
- **Family of Sets** indexed by I: sets A_i for each $i \in I$, denoted $\{A_i \mid i \in I\}$ or $\{A_i\}_{i \in I}$
- **Indexed Intersection**: $\displaystyle\bigcap_{i \in I} A_i = \{x \in U \mid \forall i \in I, x \in A_i\}$
- **Indexed Union**: $\displaystyle\bigcup_{i \in I} A_i = \{x \in U \mid \exists i \in I, x \in A_i\}$
- **Cartesian Product** of A and B: $A \times B = \{(a, b) \mid a \in A, b \in B\}$
  - notation: $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
  - $A \times \varnothing = \varnothing \times A = \varnothing$
  - $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$ $= \displaystyle\prod_{i=1}^{n} A_i$ $(a_1, a_2, \ldots, a_n)$: ordered n-tuple (eg $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$)

Set Properties

- **Thrm 9.1.1** (Properties of Unions and Intersections). *letting* A, B *be sets,*
  - $A \cap B = B \cap A$
  - $A \cup B = B \cup A$
  - $A \cap B \subseteq A$
  - $A \subseteq A \cup B$
  - $A \subseteq B \Leftrightarrow A \cap B = A$
- **Thrm 9.1.2** (DeMorgan's Laws for Sets). *For any sets* A, X, *and* Y, *and if* $\{X_i \mid i \in I\}$ *is an indexed family of sets,*
  - $A \setminus (X \cup Y) = (A \setminus X) \cap (A \setminus Y)$
  - $A \setminus (X \cap Y) = (A \setminus X) \cup (A \setminus Y)$
  - $A \setminus \bigcup_{i \in I} X_i = \bigcap_{i \in I} (A \setminus X_i)$
  - $A \setminus \bigcap_{i \in I} X_i = \bigcup_{i \in I} (A \setminus X_i)$

good luck on exam 1 <3

Functions

- a *function* from a domain set X to a codomain set Y is a specification of elements $f(x) \in Y$ for each $x \in X$ s.t. $\forall x \in X, \exists! y \in Y, y = f(x)$
- given a mapping $f : A \to B$, f is a function iff...
  - $\forall a \in A, f(a)$ is defined **i.e.** domain $= A$
  - $\forall a \in A, f(a) \in B$ **i.e.** codomain $= B$
  - $\forall a, a' \in A, (a = a' \Rightarrow f(a) = f(a'))$ **i.e.** uniqueness, vertical line test
- To define the following, let $f : A \to B$ be a function.
- $f = g$ iff $\forall a \in A, f(a) = g(a)$ **i.e.** for all inputs you get the same outputs
- the *graph* of f, $Gr(f) = \{(a, b) \in A \times B \mid b = f(a)\} \subseteq A \times B$
- for $X \subseteq A$, *image of X under f*: $\text{Im}_f(X) = f[X] = \{b \in B \mid \exists x \in X, f(x) = b\}$
  - *image of f* (of the entire domain): $\text{Im}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$
- for $Y \subseteq B$, *preimage of Y under f*: $\text{PreIm}_f(Y) = f^{-1}[y] = \{a \in A \mid f(a) \in Y\}$
- f is *injective/1-to-1* iff $\forall x, y \in A, (f(x) = f(y) \Rightarrow x = y)$ (ie f passes HLT)
- f is *surjective/onto* iff $\forall b \in B, \exists a \in A, f(a) = b$ (ie $\text{Im}(f) = B$)
- f is a *bijection* iff f is both a injection and a surjection
- h is a *composition* of g with f, denoted $h = g \circ f$ iff $h(a) = g(f(a))$
  - when A, B, C are sets and $f : A \to B, g : B \to C$ are functions. creates $h : A \to C$
  - as long as $\text{Im}(f) \subseteq \textit{domain}(g)$, this operation works
  - **Thrm 14.1.1** (Associativity of Comp.). Let $f : A \to B, g : B \to C, h : C \to D$.
    - $h \circ (g \circ f) = (h \circ g) \circ f$
- bruh where was the identity function
- **Thrm 14.1.2**. Let $f : A \to B, g : B \to C$.
  - If f and g are in/sur/bijections, then $g \circ f$ is an in/sur/bijection.
- Let $f : A \to B, g : B \to C$.
  - g is a *left inverse* for f iff $g \circ f = id_A$ (f is injective)
  - g is a *right inverse* for f iff $f \circ g = id_B$ (f is surjective)
  - g is a *(2-sided) inverse* for f iff g is a left and right inverse
  - f is *invertible* iff f has a (2-sided) inverse
  - **Thrm 14.1.3** (Uniqueness of Inverses). If f is invertible than its inverse f^{-1} is unique.
  - **Thrm 14.1.4**. f is invertible iff f is a bijection. (ie can prove $f : A \to B$ is a bijection by making a well defined $g : B \to A$ and proving g is an inverse of f)

wtf the natural numbers 2 electric boogaloo???

TODO

- informal definition
- formal definition w/ peano's axioms for $\mathbb{N}$
  - $0 \notin \mathrm{Im}_S(\mathbb{N})$
  - s is injective
  - For all sets X, if $0 \in X$ and $\forall n \in N, (n \in X \to s(n) \in X)$ then $\mathbb{N} \subseteq X$.
- **Thrm 15.2.1** (Recursion Theorem).
- math with $\mathbb{N}$ 2, electric boogaloo
- recursive function definitions

$$\sum_{k=1}^{n} a_k = \begin{cases} \sum\limits_{k=1}^{0} a_k = 0 \\ \\ \sum\limits_{k=1}^{m+1} a_k = (\sum\limits_{k=1}^{m} a_k) + a_{m+1} \text{ if } n = m+1 \end{cases}$$

$$\prod_{k=1}^{n} a_k = \begin{cases} \prod\limits_{k=1}^{0} a_k = 1 \\ \\ \prod\limits_{k=1}^{m+1} a_k = (\prod\limits_{k=1}^{m} a_k) \cdot a_{m+1} \text{ if } n = m+1 \end{cases}$$

$$n! = \sum_{k=1}^{n} k$$

The Principle of Mathmatical Induction (PMI)

- **Thrm 16.2.1** (PMI).
  - WTS $p(n)$ is true for all natural numbers $n \geq n_0$.
  - Let $p(n)$ be a predicate defined on $\mathbb{N}, n_0 \in \mathbb{N}$, and $S = \{n \in \mathbb{N} \mid n \geq n_0\}$.
  - To prove $\forall n \in S, p(n) \ldots$
    * (Base Case) Verify that $p(n_0)$ holds.
    * (Inductive Step) Fix $n \in S$ and assume $p(n)$ holds.
      - **or for strong pmi:** Fix that $n \in S$ s.t. $\forall i \in S$, with $n_0 \leq i \leq n, p(i)$ holds. n_0 should be the last base case if there are multiple.
    * Prove that $p(n+1)$ must also be true.
    * By PMI, we conclude $\forall n \in S, p(n)$. $\square$

Well-Ordering Principle

- *well-ordered:* a set of which every nonempty subset has a least element
- **Thrm 19.1.1** (Well-Ordering-Principle). $\mathbb{N}$ is a well-ordered set.
- Proof by Infinite Descent ($\forall n \in \mathbb{N}, p(n)$)
  - AFSOC $\exists n \in \mathbb{N}$ st $\neg p(n)$ holds.
    * ie $S = \{n \in \mathbb{N} \mid \neg p(n)\} \neq \varnothing$
  - Let $n \in S$ be the least such element, by the WOP.
  - Show $\exists k \in S$ with $k < n \rightarrow\leftarrow$ contradicts the minimality of n.
  - Conclude that $\forall n \in \mathbb{N}, p(n)$.

Binary Relations

- A binary relation links or compares two elements.
- A *binary relation* from S to T is a predicate $R(s,t)$ defined on $S \times T$.
  - S is the *domain* of R
  - T is the *codomain* of R
  - If $S = T$ then R is a *homogenous relation* and we say "R is a relation on S"
  - can also be written as the *graph* of R, $\mathrm{Gr}(R) = \{(s,t) \in S \times T \mid R(s,t)\}$
  - **Thrm 19.2.1**. Let S and T be sets. Every subset of $S \times T$ is the graph of a unique relation from S to T.
- the *discrete relation* from S to T
  - $\mathrm{Gr}(R) = S \times T$
  - ie $\forall s \in S, \forall t \in T, R(s,t)$
  - everything is related to everything
- the *empty relation* from S to T
  - $\mathrm{Gr}(R) = \varnothing$
  - ie $\forall s \in S, \forall \in T, \neg R(s,t)$
  - nothing is related to anything
- **Defn:** (Congruence Modulo m). Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. a is congruent to b modulo m, denoted $a \equiv b \pmod{m}$ or $a \equiv_m b$, iff $m \mid a - b$.
  - **Thrm 20.1.1**. Congruence modulo m is an equivalence relation.
  - For $m \in \mathbb{Z}^+$, the set of equivalence classes for $\equiv_m$, called *congruence classes*, is denoted $\mathbb{Z}/m\mathbb{Z}$.
    - eg, $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$
- **Defn:** Let R be an equivalence relation on a set S.
  - For $x \in S$ we define the *equivalence class of x under R*, $[x]_R = \{y \in S \mid R(x,y)\}$ = the set of elements in S which are equivalent to x.
  - the set of all equivalence classes is called *S modulo R*, $S/R = \{[x]_R \mid x \in S\}$

Properties of Homogenous Relations

Let R be a relation on S. Then R is called

- *reflexive* iff $\forall x \in S, R(x,x)$
- *irreflexive* iff $\forall x \in S, \neg R(x,x)$
- *symmetric* iff $\forall x, y \in S, (R(x,y) \to R(y,x))$
- *antisymmetric* iff $\forall x, y \in S, (R(x,y) \wedge R(y,x) \to x = y)$ (or equivly, its contrapos.)
- *transitive* iff $\forall x, y, z \in S, ((R(x,y) \wedge R(y,z)) \to R(x,z))$
- *total* iff $\forall x, y \in S, (x \neq y \to (R(x,y) \vee R(y,x)))$
- *an equivalence relation* iff R is reflexive, symmetric, and transitive

Partitions

- **Defn:** Let S be a set, I an index set, and $A_i \in \mathcal{P}(S)$ for each $i \in I$. The indexed family of sets $\{A_i \mid i \in I\}$ is a *partition* of S iff
  1. $\forall i \in I, A_i \neq \varnothing$
  2. $\forall i, j \in I, (A_i = A_j \vee A_i \cap A_j = \varnothing)$
  3. $\bigcup_{i \in I} A_i = S$
- **Thrm** (Fundamental Thrm of Equivalence Relations): Let S be a nonempty set.
  1. If R is an equivalence relation on S, then S/R is a partition of S.
  2. If $\mathcal{F}$ is a partition of S then there exists an equivalence relation R on S s.t. $S/R = \mathcal{F}$

Order Relations

Let R be a binary relation on a set S.

- R is a *partial order of* S iff R is reflexive, antisymmetric, and transitive.
- If R is a partial order on S, then we call (S,R) a *poset* (eg $(\mathcal{P}(x), \subseteq)$ and $(\mathbb{R}, \leq)$)
- R is a *strict partial order* of S iff R is irreflexive, antisymmetric, and transitive. (eg $(\mathcal{P}(x), \subsetneq)$ and $(\mathbb{R}, <)$)
- R is a *total order* or *linear order* iff R is a partial order and also total

good luck on exam 2 <3

Cardinality

- **Defn:** Two sets A and B have the same *cardinality* (aka are *equinumerous*), iff there exists a bijection $f : A \to B$.
- A set X is *finite* iff $\exists n \in \mathbb{N}$ and a bijection $f : [n] \to X$. We denote this $|X| = n$.
- A set X is *infinite* iff X is not finite.
- **Thrm:** If X is a finite set then $\exists! n \in \mathbb{N}, |X| = n$. This has some corollaries.
  - For any $n \in \mathbb{N}$, all subsets of $[n]$ are finite.
  - If $f : A \to B$ is an injection and B is finite, then $|A| \leq |B|$. In particular, if $A \subseteq B$ then $|A| \leq |B|$.
  - If $g : B \to A$ is a surjection and B is finite then $|A| \leq |B|$.
  - If A is finite and B is any set then $|A \cap B| \leq |A|$ and $|A \setminus B| \leq |A|$
- **Thrm:** If A and B are finite sets, then
  - $|A \times B| = |A| * |B|$
  - $|A \cup B| = |A| + |B| - |A \cap B|$
- **Lemma:** If $A \subseteq \mathbb{N}$ is finite and nonempty, then A has a maximum element.
- **Thrm:** $\mathbb{N}$ is infinite.
- **Defn:** A set A is
  - *countably infinite* iff $|A| = |\mathbb{N}|$
  - *countable* (or *listable* or *denumerable*) iff A is finite or countably infinite
  - *uncountable* iff A is not countable
  - (Note: every set is either finite, countably infinite, or uncountable)
- **Thrm:**
  - For all $n \in \mathbb{Z}^+, |\mathbb{N}^n| = |\mathbb{N}|$
  - If $n \in \mathbb{Z}^+$ and $X_1, X_2, \ldots, X_n$ are nonempty countable sets, then
    * $\prod_{i=1}^{n} X_1$ is countable
    * If at least one X_i is infinite, then $\prod_{i=1}^{n} X_i$ is countably infinite.
- Let X be a nonempty set. Then the following are equivalent.
  - X is countable
  - There exists an injection $f : X \to \mathbb{N}$
  - There exists a surjection $g : \mathbb{N} \to X$
- **Thrm:** $|\mathbb{Q}| = |\mathbb{N}|$

- **Thrm** (Countable Union of Countable Sets is Countable): If $\{A_n \mid n \in \mathbb{N}\}$ is a family of countable sets, then $\bigcup_{n\in\mathbb{N}} A_n$ is countable.
- $\mathbb{R}$ is uncountable
- For any set S, $|S| \neq |\mathcal{P}(\mathcal{S})|$ (Cantor's theorem)
- $|A| \leq |B|$ iff there exists an injection $f : A \to B$ ($\geq$ vice versa)
  - this is transitive
- **Thrm** (Schröder-Bernstein Thrm): If there exist injections $f : A \to B$ and $g : B \to A$, then there exists an injection $h : A \to B$.

Number Theory

- a *unit* is the natural number $n = 1$
- a natural > 1 is *prime* iff its only positive divisors are 1 and itself
- a natural > 1 is *composite* iff n is not prime (ie $\exists a, b \in \mathbb{Z}, (1 < a \leq b < n \to n = ab)$)
- *coprime* iff the gcd of two integers is 1
- every integer $n \geq 2$ is either prime or the product of primes (induction)
- Let m, n be nonzero integers. If $m|n$ then $|m| \leq |n|$
  - **Corollary:** If $m|n \wedge n|m$ then $m = n \vee m = -n$
  - if $n \in \mathbb{Z}$ and $n \neq 0$, then n only has a finite number of divisors, since $m|n \to |m| \leq |n|$
- if $n \in \mathbb{N}$ is composite, then n has a prime factor $\leq \sqrt{n}$
- for $a, b \in \mathbb{Z}$, not both 0, define the *greatest common divisor* of a and b, denoted $\gcd(a, b)$, as the largest $d \in \mathbb{Z}$ s.t. $d|a \wedge d|b$.
  - ie $d = \gcd(a, b) \Leftrightarrow d|a \wedge d|b \wedge \forall c \in \mathbb{Z}, ((c|a \wedge c|b) \to c \leq d)$
  - $\gcd(a, b) = \gcd(|a|, |b|)$
  - note that $\gcd(0, b) = |b|$
- Let $a, b \in \mathbb{Z}$, not both 0, and $d = \gcd(a, b)$. Then $\frac{a}{d}$ and $\frac{b}{d}$ are coprime
- The Euclidean Algorithm
  - EA Lemma: Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $\gcd(a, b) = \gcd(b, a - bk)$ for any integer k.

- Let $a, b \in \mathbb{Z}$ with $a > b > 0$. To find $\gcd(a, b)$: (transcribe formal)

$$\begin{aligned} &\text{Consider 148 and 40} \\ 148 &= 40 * 3 + 28 \\ 40 &= 28 * 1 + 12 \\ 28 &= 12 * 2 + 4 \\ 12 &= 4 * 3 + 0 \end{aligned}$$

  Last nonzero remainder (4) is the gcd

- Bezout's Lemma. Let $a, b \in \mathbb{Z}$, not both 0. Then
  - $\exists x, y \in \mathbb{Z}, (ax + by = \gcd(a, b))$
  - If $x, y \in \mathbb{Z}$ s.t. $ax + by > 0$ then $ax + by \geq \gcd(a, b)$
  - ie $\gcd(a, b)$ is the smallest positive integer of the form $ax + by$
  - Corollaries (Let $a, b \in \mathbb{Z}$, not both 0):
    - If $d = \gcd(a, b)$ and $t \in \mathbb{Z}$ then $(t|a \wedge t|b) \Leftrightarrow t|d$
      - (any common divisor of a and b divides $\gcd(a, b)$ and vice versa)
    - $\forall c \in \mathbb{Z}, (\exists x, y \in \mathbb{Z}, (ax + by = c) \Leftrightarrow \gcd(a, b)|c)$
    - a and b are coprime iff $\exists x, y \in \mathbb{Z}, (ax + by = 1)$
    - $\forall m \in \mathbb{Z}^+, (\gcd(ma, mb) = m * \gcd(a, b))$

- Linear Diophantine Equations
  - Diophantine equations are polynomial equations, typically in several variables, in which integer solutions are desired.
  - For $a, b, c \in \mathbb{Z}$, a Diophantine equation of the form $ax + by = c$ is called a linear Diophantine equation in 2 variables
  - We know that $\exists x, y \in \mathbb{Z}, (ax + by = c)$ iff $\gcd(a, b) \mid c$. We can find such x, y with reverse Euclidean alg. *(transcribe)*
  - how do we find all such solutions?
    - **Thrm:** If $d = \gcd(a, b)$ and $d \mid c$ then there are infinitely many integer solutions to $ax + by = c$. Moreover, if (x_0, y_0) is one such solution, then the set of all solutions is

$$\{(x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d}) \mid k \in \mathbb{Z}\}$$

- The Least Common Multiple
  - For $a, b \in \mathbb{Z}$, not both 0, we definte the *least common multiple of a and b*, denoted $\text{lcm}[a, b]$, as the smallest $c \in \mathbb{Z}^+$ s.t. $a \mid c \wedge b \mid c$
  - Let $a, b \in \mathbb{Z}$, both nonzero. Then $\forall n \in \mathbb{Z}, (\text{lcm}[a, b] \mid n \Leftrightarrow a \mid n \wedge b \mid n)$
    - ie Any common multiple is divisible by the least common multiple

- Corollaries: Let $a, b \in \mathbb{Z}$, not both 0. Then,
  - $a \mid b \Leftrightarrow \text{lcm}[a, b] = |b|$
  - $\forall m \in \mathbb{Z}^+, \text{lcm}[ma, mb] = m * \text{lcm}[a, b]$
- (GCD-LCM Theorem). $\forall a, b \in \mathbb{Z}^+, \gcd(a, b) * \text{lcm}[a, b] = ab$

- Prime Factorizations
  - Euclid's Lemma. Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. If $a \mid bc$ then $a \mid c$.
    - Corollary (also Euclid's Lemma). Let $p, a, b \in \mathbb{Z}$ with p prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.
  - Fundamental Theorem of Arithmetic. Every natural number $n > 1$ can be written uniquely as a product of prime numbers. (Unique up to reordering of the factors).
    - ie If $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ for primes p_i, q_j s.t. $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$ then $r = s$ and $p_i = q_i$ for all i.
    - Corollary: exist infinitely many primes.

- Divisors
  - Let $\mathbb{P}$ be the set of prime numbers. For each $p \in \mathbb{P}$ and $n \in \mathbb{Z}^+$, define $v_p(n) = \max\{a \in \mathbb{Z} : p^a \mid n\}$
  - note: If $a \mid n$ then $\forall p \in \mathbb{P}, v_p(a) \leq v_p(n)$
  - Suppose n has prime factorization ah fuck it