,

CS1231S

AY20/21 Sem 1

01. PROOFS

sets of numbers

$\mathbb{N}$: natural numbers ($\mathbb{Z}_{\geq 0}$)
$\mathbb{Z}$: integers
$\mathbb{Q}$: rational numbers
$\mathbb{R}$: real numbers
$\mathbb{C}$: complex numbers

basic properties of integers

closure (under addition and multiplication)
$x + y \in \mathbb{Z} \wedge xy \in \mathbb{Z}$
commutativity
$a + b = b + a \wedge ab = ba$
associativity
$a + b + c = a + (b + c) = (a + b) + c$
$abc = a(bc) = (ab)c$
distributivity
$a(b + c) = ab + ac$
trichotomy
$(a < b) \vee (a > b) \vee (a = b)$
transitive law
$(a < b) \wedge (b < c) \implies (a < c)$

definitions

even/odd
n is even $\leftrightarrow \exists k \in \mathbb{Z} \mid n = 2k$
n is odd $\leftrightarrow \exists k \in \mathbb{Z} \mid n = 2k + 1$
prime/composite
n is prime $\leftrightarrow n > 1$ and $\forall r, s \in \mathbb{Z}^+, n = rs \rightarrow (r = n) \vee (r = s)$
n is composite $\leftrightarrow n > 1$ and $\exists r, s \in \mathbb{Z}^+ s.t. n = rs$ and $1 < r < n$ and $1 < s < n$
divisibility (d divides n)
$d \mid n \leftrightarrow \exists k \in \mathbb{Z} \mid n = kd$
rationality
r is rational $\leftrightarrow \exists a, b \in \mathbb{Z} \mid r = \frac{a}{b}$ and $b \neq 0$
floor/ceiling
$\lfloor x \rfloor$: largest integer y such that $y \leq x$
$\lceil x \rceil$: smallest integer y such that $y \geq x$

rules of inference

generalisation	elimination
$p, \therefore p \vee q$	$p \vee q; \ \sim q, \therefore p$
specialisation	transitivity
$p \wedge q, \therefore p$	$p \rightarrow q; \ q \rightarrow r; \ \therefore p \rightarrow r$

04. METHODS OF PROOF

Proof by Exhaustion/Cases

1. list out possible cases
   1.1. Case 1: n is odd OR If $n = 9$, ...
   1.2. Case 2: n is even OR If $n = 16$, ...
2. therefore ...

Proof by Contradiction

1. Suppose that ...
   1.1. <proof>
   1.2. ...but this contradicts ...
2. Therefore the assumption that ...is false. Hence ....

Proof by Contraposition

1. Contrapositive statement: $\sim q \rightarrow \sim p$
2. let $\sim q$
   2.1. <proof>
   2.2. hence $\sim p$
3. $\therefore p \rightarrow q$

Proof by Construction

1. Let $x = 3, y = 4, z = 5$.
2. Then $x, y, z \in \mathbb{Z}_{\geq 1}$ and $x^2 + y^2 = 3^2 + 4^2 = 9 + 16 = 25 = 5^2$.
3. Thus $\exists x, y, z \in \mathbb{Z}_{\geq 1}$ such that $x^2 + y^2 = z^2$.

Proof by Induction

1. For each $n \in \mathbb{Z}_{\geq 1}$, let $P(n)$ be the proposition "$\ldots$"
2. (base step) $P(1)$ is true because <manual method>
3. (induction step)
   3.1. let $k \in \mathbb{Z}_{\geq 1}$ s.t. $P(k)$ is true
   3.2. Then ...
   3.3. proof that $P(k + 1)$ is true - e.g. $P(k + 1) = P(k) + term_{k+1}$
   3.4. So $P(k + 1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geq 1} P(n)$ is true by MI.

Proofs for Sets

Equality of Sets (A=B)

1. $(\Rightarrow)$
   1.1. Take any $z \in A$.
   1.2. $\ldots$
   1.3. $\therefore z \in B$.
2. $(\Leftarrow)$
   2.1. Take any $z \in B$.
   2.2. $\ldots$
   2.3. $\therefore z \in A$.

Element Method

1. $A \cap (B \backslash C) = \{x : x \in A \wedge x \in (B \backslash C)\}$ (by def. of $\cap$)
2. $= \{x : x \in A \wedge (x \in B \wedge x \notin C)\}$ (by def. of $\backslash$)
3. $\ldots$
4. $= (A \cap B) \backslash C$ (by def. of $\backslash$)

Other Proofs

iff ($A \leftrightarrow B$)

1. $(\Rightarrow)$ Suppose A.
   1.1. $\ldots$ <proof> $\ldots$
   1.2. Hence $A \rightarrow B$
2. $(\Leftarrow)$ Suppose B.
   2.1. $\ldots$ <proof> $\ldots$
   2.2. Hence $B \rightarrow A$

02. COMPOUND STATEMENTS

operations

1 $\sim$: negation (not)
2 $\wedge$: conjunction (and)
2 $\vee$: disjunction (or) - coequal to $\wedge$
3 $\rightarrow$: if-then

logical equivalence

- identical truth values in truth table
- definitions
- to show non-equivalence:
  - truth table method (only needs 1 row)
  - counter-example method

conditional statements

hypothesis $\rightarrow$ conclusion
$antecedent \rightarrow consequent$

- **vacuously true** : hypothesis is false
- **implication law** : $p \rightarrow q \equiv \sim p \vee q$
- common if/then statements:
  - if p then q: $p \rightarrow q$
  - p if q: $q \rightarrow p$
  - p only if q: $p \rightarrow q$
  - p iff q: $p \leftrightarrow q$

- **contrapositive** : $\sim q \rightarrow \sim p$
- **inverse** : $\sim p \rightarrow \sim q$
- **converse** : $q \rightarrow p$

converse $\equiv$ inverse
statement $\equiv$ contra-positive

- r is a **necessary** condition for s: $\sim r \rightarrow \sim s$ and $s \rightarrow r$
- r is a **sufficient** condition for s: $r \rightarrow s$
- **necessary** & **sufficient** : $\leftrightarrow$

valid arguments

- determining validity: construct truth table
  - valid $\leftrightarrow$ conclusion is true when premises are true
- **syllogism** : (argument form) 2 premises, 1 conclusion
- **modus ponens** : $p \rightarrow q; \ p; \ \therefore q$
- **modus tollens** : $p \rightarrow q; \ \sim q; \ \therefore \sim p$
- **sound argument** : is valid & all premises are true

fallacies

converse error	inverse error
$p \rightarrow q$	$p \rightarrow q$
q	$\sim p$
$\therefore p$	$\therefore \sim q$

03. QUANTIFIED STATEMENTS

- **truth set** of $P(x) = \{x \in D \mid P(x)\}$
- $P(x) \Rightarrow Q(x) : \forall x (P(x) \rightarrow Q(x))$
- $P(x) \Leftrightarrow Q(x) : \forall x (P(x) \leftrightarrow Q(x))$

relation between $\forall, \exists, \wedge, \vee$

- $\forall x \in D, Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge \cdots \wedge Q(x_n)$
- $\exists x \in D \mid Q(x) \equiv Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n)$

05. SETS

notation

- set roster notation [1]: $\{x_1, x_2, \ldots, x_n\}$
- set roster notation [2]: $\{x_1, x_2, x_3, \ldots\}$
- set-builder notation: $\{x \in \mathbb{U} : P(x)\}$

definitions

- **equal sets** : $A = B \leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$
  - $A = B \leftrightarrow (A \subseteq B) \wedge (A \supseteq B)$
- **empty set**, $\emptyset$: $\emptyset \subseteq$ all sets
- **subset** : $A \subseteq B \leftrightarrow \forall x (x \in A \rightarrow x \in B)$
- **proper subset** : $A \subsetneq B \leftrightarrow (A \subseteq B) \wedge (A \neq B)$
- **power set** of A : $\mathcal{P}(A) = \{X \mid X \subseteq A\}$
  - $|\mathcal{P}(A)| = 2^{|A|}$, given that A is a finite set
- **cardinality** of a set, $\mid A \mid$: number of distinct elements
- **singleton** : sets of size 1
- **disjoint** : $A \cap B = \emptyset$

methods of proof for sets

- direct proof
- element method
- truth table

boolean operations

- **union:** $A \cup B = \{x : x \in A \vee x \in B\}$
- **intersection:** $A \cap B = \{x : x \in A \wedge x \in B\}$
- **complement** (of B in A): $A \backslash B = \{x : x \in A \wedge x \notin B\}$
- **complement** (of B): $\bar{B}$ or $B^c = U \backslash B$
  - set difference law: $A \backslash B = A \cap \bar{B}$

ordered pairs and cartesian products

- **ordered pair** : (x, y)
  - $(x, y) = (x', y') \leftrightarrow x = x'$ and $y = y'$
- **Cartesian product** : $A \times B = \{(x, y) : x \in A$ and $y \in B\}$
  - $|A \times B| = |A| \times |B|$
- **ordered tuples** : expression of the form $(x_1, x_2, \ldots, x_n)$

06. FUNCTIONS

definitions

- **function/map** from A to B : assignment of each element of A to exactly one element of B.
  - $f : A \rightarrow B$: "f is a function from A to B"
  - $f : x \rightarrow y$: "f maps x to y"
  - **domain** of f = A
  - **codomain** of f = B
  - **range/image** of f = $\{f(x) : x \in A\}$ $= \{y \in B \mid y = f(x)$ for some $x \in A\}$
- **identity function** on A, $\text{id}_A : A \rightarrow A$
  - $\text{id}_A : x \rightarrow x$
  - range = domain = codomain = A
- **well-defined function** : every element in the domain is assigned to exactly one element in the codomain

equality of functions

- same codomain and domain
- for all $x \in$ codomain, same output

function composition

- $(g \circ f)(x) = g(f(x))$
- for $(g \circ f)$ to be well defined, codomain of f must be equal to the domain of g
- $\times$ commutative
- $\checkmark$ associative

image & pre-image

for $f : A \to B$

- if $X \subseteq A$, **image** of X, $f(X) = \{y \in B : y = f(x)$ for some $x \in X\}$
- if $Y \subseteq B$, **pre-image** of Y, $f^{-1}(Y) = \{x \in A : y = f(x)$ for some $y \in Y\}$

injection & surjection

- **surjective** (onto) : codomain = range
  - $\forall y \in B, \exists x \in A\ (y = f(x))$
  - surjective test: $\forall Y \subseteq B, Y \subseteq f(f^{-1}(Y))$
- **injective** : one-to-one
  - $\forall x, x' \in A (f(x) = f(x') \Rightarrow x = x')$
  - injective test: $\forall X \subseteq A, X \subseteq f^{-1}(f(X))$
- **bijective** : both surjective & injective
  - has an inverse

inverse

- $\forall x \in A, \forall y \in B (f(x) = y \Leftrightarrow g(y) = x)$

07. INDUCTION

mathematical induction

to prove that $\forall n \in \mathbb{Z}_{\geq m}(P(n))$ is true,

- base step: show that $P(m)$ is true
- induction step: show that $\forall k \in \mathbb{Z}_{\geq m}(P(k) \Rightarrow P(k+1))$ is true.
  - induction hypothesis: assumption that $P(k)$ is true

strong MI

to prove that $\forall n \in \mathbb{Z}_{\geq 0}(P(n))$ is true,

- base step: show that $P(0), P(1)$ are true
- induction step: show that $\forall k \in \mathbb{Z}_{\geq 0}(P(0) \cdots \wedge P(k+1) \Rightarrow P(k+2))$ is true.

justification:

- $P(0) \wedge P(1)$ by base case
- $P(0) \wedge P(1) \to P(2)$ by induction with $k = 0$
- $P(0) \wedge P(1) \wedge P(2) \to P(3)$ by induction with $k = 1$
- $\dots$
- we deduce that $P(0), P(1), \dots$ are all true by a series of **modus ponens**

well-ordering principle

- every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.
- application: recursion has a base case

RECURSION

a sequence is **recursively defined** if the definition of a_n involves $a_0, a_1, \dots, a_{n-1}$ for all but finitely many $n \in \mathbb{Z}_{\geq 0}$.

recursive definitions

e.g. recursive definition for $\mathbb{Z}$

1. (**base clause**) $0 \in \mathbb{Z}_{\geq 0}$
2. (**recursion clause**) If $x \in \mathbb{Z}_{\geq 0}$, then $x + 1 \in \mathbb{Z}_{\geq 0}$
3. (**minimality clause**) Membership for $\mathbb{Z}_{\geq 0}$ can be demonstrated by (finitely many) successive applications of the clauses above

recursion vs induction

- **recursion** - to define the set
- **induction** - to show things about the set

well-formed formulas (WFF)

in propositional logic

define the set of WFF(Σ) as follows

1. (base clause) every element ρ of Σ is in WFF(Σ)
2. (recursion clause) if x, y are in WFF(Σ), then $\sim x$ and $(x \wedge y)$ and $(x \vee y)$ are in WFF(Σ)
3. (minimality clause) Membership for WFF(Σ) can be demonstrated by (finitely many) successive applications of the clauses above

08. NUMBER THEORY

divisibility

- $n \mod d$ is always non-negative.

transitivity of divisibility

If $a \mid b$ and $b \mid c$, then $a \mid c$.

closure lemma (non-standard name)

Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

division theorem

$\forall n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, $\exists! q, r \in \mathbb{Z}$ s.t.

$n = dq + r$ and $0 \leq r < d$

$q = n\ div\ d = \lfloor n/d \rfloor$

$r = n\ mod\ d = n - dq$

base-b representation

of positive integer n is $(a_\ell a_{\ell-1} \dots a_0)_b$

where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \dots, a_\ell \in \{0, 1, \dots, b-1\}$

s.t. $n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \dots + a_0 b^0$ and $a_\ell \neq 0$

greatest common divisor

- $m\ mod\ n$
- if $m \neq 0$ and $n \neq 0$, then gcd(m, n) exists and is positive.
- **Euclidean Algorithm** for finding gcd

Bezout's Lemma:

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $gcd(m, n) = ms + nt$.

Euclid's Lemma:

Let $m, n \in Z^+$. If p is prime and $p \mid mn$, then $p \mid m$ or $p \mid n$.

prime factorization

- **Fundamental Theorem of Arithmetic**: Every integer $n \geq 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.
  - aka Prime Factorisation Theorem

modular arithmetic

Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

congruence

$a \equiv b \pmod n \Leftrightarrow a \bmod n = b \bmod n$

Then $\exists k \in \mathbb{Z} \mid a = nk + b$ and $n \mid (a - b)$

reflexivity

$a \equiv a \pmod n$

symmetry

$a \equiv b \pmod n \to b \equiv a \pmod n$

transitivity

$a \equiv b \pmod n \wedge b \equiv c \pmod n \to a \equiv c \pmod n$

additive inverse

b is an *additive inverse* of $a \bmod n \Leftrightarrow a + b \equiv 0 \pmod n$.

b is an *additive inverse* of $a \bmod n \Leftrightarrow b \equiv -a \pmod n$.

multiplicative inverse

b is a multiplicative inverse of $a \bmod n \Leftrightarrow ab \equiv 1 \pmod n$.

- If b, b' are multiplicative inverses of a, then $b \equiv b' \pmod n$.
- exists $\Leftrightarrow \gcd(a, n) = 1$.
  - a, n are coprime
- to find multiplicative inverse: **Euclidean Algorithm**

09. EQUIVALENCE RELATIONS

relations

Let R be a relation from A to B and $(x, y) \in A \times B$. Then:

xRy for $(x, y) \in R$ and $x \not R y$ for $(x, y) \notin R$

- A relation from A to B is a subset of $A \times B$.
- A **(binary) relation** on set A is a relation from A to A.
  - subset of A^2

reflexivity, symmetry, transitivity

Let A be a set and R be a relation on A.

reflexive

$\forall x \in A\ (xRx)$

symmetric

$\forall x, y \in A\ (xRy \Rightarrow yRx)$

transitive

$\forall x, y, z \in A\ (xRy \wedge yRz \Rightarrow xRz)$

- **equivalence relation**: a relation that is reflexive, symmetric and transitive
- **equivalence class**: the set of all things equivalent to x

equivalence classes

Let A be a set and R be an equivalence relation on A.

- $[x]_R$: **equivalence class** of x with respect to R
  - $\forall x \in A, [x]_R = \{y \in A : xRy\}$
- A/R : The set of all equivalent classes
  - $A/R = \{[x]_R : x \in A\}$

$xRy \Rightarrow [x] = [y] \Rightarrow [x] \cap [y] \neq \emptyset$

partitions

- a **partition** of a set A is a set $\mathscr{C}$ of *non-empty subsets* of A such that
  $(\geq 1)\ \forall x \in A,\ \exists S \in \mathscr{C}(x \in S)$
  $(\leq 1)\ \forall x \in A,\ \forall S, S \in \mathscr{C}(x \in S \wedge x \in S' \Rightarrow S = S')$
- **components** : elements of a partition
- every partition comes from an equivalence relation

partial orders

Let A be a set and R be a relation on A.

- R is **antisymmetric** if $\forall x, y \in A\ (xRy \wedge yRx \to x = y)$
  - includes vacuously true cases (e.g. $xRy \Leftrightarrow x < y$)
- x and y are **comparable** if $\forall x, y \in A\ (xRy \vee yRx)$
- R is a **(non-strict) partial order** if R is reflexive, antisymmetric and transitive.
  - $\preccurlyeq$ - partial order
  - $x \prec y \Leftrightarrow x \preccurlyeq y \wedge x \neq y$ (NOT a partial order)
  - Hasse diagram
- R is a **(non-strict) total order** if R is a partial order and x and y are comparable

min and max

Let $\preccurlyeq$ be a partial order on a set A, and $c \in A$.

- c is a **minimal element** if $\forall x \in A\ (x \preccurlyeq c \Rightarrow c = x)$
  - nothing is strictly below it
- c is a **maximal element** if $\forall x \in A\ (c \preccurlyeq x \Rightarrow c = x)$
  - nothing is strictly above it
- c is the **smallest element** or **minimum element** if $\forall x \in a\ (c \preccurlyeq x)$.
- c is the **largest element** or **maximum element** if $\forall x \in a\ (x \preccurlyeq c)$.

linearization

Let A be a set and $\preccurlyeq$ be a partial order on A.

Then there exists a total order $\preccurlyeq^*$ on A such that

$\forall x, y \in A\ (x \preccurlyeq y \Rightarrow x \preccurlyeq^* y)$

LOGICAL EQUIVALENCES

commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
identity laws	$p \wedge true \equiv p$	$p \vee false \equiv p$
idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
universal bound laws	$p \vee true \equiv true$	$p \wedge false \equiv false$
negation laws	$p \vee \sim p \equiv true$	$p \wedge \sim p \equiv false$
double negation law	$\sim(\sim p) \equiv p$	—
absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
De Morgan's Laws	$\sim(p \vee q) \equiv \sim p \wedge \sim q$	$\sim(p \wedge q) \equiv \sim p \vee \sim q$

SET IDENTITIES

commutative laws	$A \cap B = B \cap A$	$A \cup B = B \cup A$
associative laws	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
distributive laws	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
identity laws	$A \cap U = A$	$A \cup \emptyset = A$
idempotent laws	$A \cap A = A$	$A \cup A = A$
universal bound laws	$A \cap \emptyset = \emptyset$	$A \cup U = U$
complement laws	$A \cap \overline{A} = \emptyset$	$A \cup \overline{A} = U$
double **complement** law	$\overline{(\overline{A})} = A$	—
absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$

proven:

- L1E1 - the product of 2 consecutive odd numbers is always odd.
- L1E5 - the difference between 2 consecutive squares is always odd
- L4E4 - the sum of any 2 even integers is even
- L4T4.6.1 - there is no greatest integer
- L4T4.3.1 - for all positive integers a and b, if $a|b$, then $a \leq b$.
- L1P4.6.4 - for all integers n, if n^2 is even then n is even
- L4T4.2.1 - all integers are rational numbers
- L4T4.2.2 - the sum of any 2 rational numbers is rational
- L1E7 - there exist irrational numbers p and q such that p^q is rational
- L4T4.7.1 - $\sqrt{2}$ is irrational.
- L4T4.3.2 - the only divisors of 1 are 1 and -1.
- L4T4.3.3 - **transitivity of divisibility**
  - if $a|b$ and $b|c$, then $a|c$.
- L3T3.2.1 - **negation of a universal statement**:
  - $\sim(\forall x \in D, P(x)) \equiv \exists x \in D \mid \sim P(x)$
- L3T3.2.2 - **negation of an existential statement**:
  - $\sim(\exists x \in D \mid P(x)) \equiv \forall x \in D, \sim P(x)$
- L5T5.1.14 - there exists a unique set with no element. It is denoted by $\emptyset$.
- L5E5.3.7 - for all A, B: $(A \cap B) \cup (A \backslash B) = A$
- L5T5.3.11(1) - let A, B be disjoint finite sets. Then $|A \cup B| = |A| + |B|$
- L5T5.3.11(2) - let $A_1, A_2, \ldots, A_n$ be pairwise disjoint finite sets. Then $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$
- L5T5.3.12 - **Inclusion-Exclusion Principle**:
  - for all finite sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$
- L6T6.1.26 - **associativity of function composition**:
  - $f \circ (g \circ h) = (f \circ g) \circ h$
- L6P2.6.16 - **uniqueness of inverses**:
  - If g, g' are inverses of $f : A \to B$, then $g = g'$.
- E6.1.24 - $f \circ \text{id}_A = f$ and $\text{id}_A \circ f = f$
- T6.2.18 - bijective $\Leftrightarrow$ has an inverse
- L7.3.19 - If $x \in \text{WFF}^+(\Sigma)$, then assigning false to all elements of Σ makes x evaluate to false.
- T7.3.20 - $\sim(\forall x \in \text{WFF}(\Sigma), \exists y \in \text{WFF}^+(\Sigma) \;\; y \equiv x) \equiv \exists x \in \text{WFF}(\Sigma) \;\; \forall y \in \text{WFF}^+(\Sigma) \;\; y \not\equiv x$ aka $\sim$ (not) must be included in the definition of WFF.
- L8.1.5 - Let $d, n \in \mathbb{Z}$ with $d \neq 0$. Then $d \mid n \Leftrightarrow n/d \in \mathbb{Z}$
- L8.1.9 - Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $-d \mid n$ and $d \mid -n$ and $-d \mid -n$
- L8.1.10 - Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $d \neq 0$, then $|d| \leq |n|$
- L8.2.5 - **Prime Divisor Lemma** (non-standard name):
  - Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime divisor.
- P8.2.6 - **sizes of prime divisors**:
  - Let n be a composite positive integer. Then n has a prime divisor $p \leq \sqrt{n}$.
- T8.2.8 - there are infinitely many prime numbers
- T8.3.13 - $\forall n \in \mathbb{Z}^+, \exists! \ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$ such that <the definition of base-b representation> holds.
- L8.4.11 - If $x, y, r \in \mathbb{Z}$ such that $x \; mod \; y = r$, then $gcd(x, y) = gcd(y, r)$.
- Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ s.t. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.
  - P8.6.6 - **addition:** Then $a + c \equiv b + d \pmod{n}$
  - P8.6.13 - **multiplication:** Then $ac \equiv bd \pmod{n}$
- T9.3.4 - Let R be an equivalence relation on a set A. Then A/R is a partition of A.
- T9.3.5 - If $\mathscr{C}$ is a partition of A, then there is an equivalence relation of R on A such that $A/R = \mathscr{C}$.
- L9.5.5 - Consider a partial order $\preccurlyeq$ on set A.
  - A smallest element is minimal.
  - There is at most one smallest element.

abbreviations

- L - lemma
- E - example
- P - proposition
- T - theorem