# CS1231(S) Cheatsheet

for Mid-term of AY 19/20 Semester 1, by Howard Liu

Appendix A of Epp is not covered. Theorems, corollaries, lemmas, etc. not mentioned in the lecture notes are marked with an asterisk (*).

## Proofs

### Basic Notation

- $\mathbb{R}$: the set of all real numbers
- $\mathbb{Z}$: the set of integers
- $\mathbb{N}$: the set of natural numbers (include 0, i.e. $\mathbb{Z}_{\geq 0}$)
- $\mathbb{Q}$: the set of rationals
- $\exists$: there exists...
- $\exists!$: there exists a unique...
- $\forall$: for all...
- $\in$: member of...
- $\ni$: such that...
- $\sim$: not ...

### Proof Types

- **By Construction**: finding or giving a set of directions to reach the statement to be proven true.
- **By Contraposition**: proving a statement through its logical equivalent contrapositive.
- **By Contradiction**: proving that the negation of the statement leads to a logical contradiction.
- **By Exhaustion**: considering each case.
- **By Mathematical Induction**: proving for a base case, then an induction step.
  1. $P(a)$
  2. $\forall k \in \mathbb{Z}, k \geq a\ (P(k) \to P(k+1))$
  3. $\therefore \forall n \in \mathbb{Z}, n \geq a\ (P(n))$
- **By Strong Induction**: mathematical induction assuming $P(k), P(k-1), \cdots, P(a)$ are all true.
- **By Structural Induction**: MI assuming $P(x)$ is true, prove $P(f(x))$ is true ($f(x)$ is the recursion set rule, i.e. if $x \in S, f(x) \in S$)

### Order of Operations

In the ascending order (1 executes first, 3 is the latest, can be overwritten by parenthesis)

1. **Negation**: $\sim$ (also represented as $\neg$)
2. **Logic AND & OR**: $\wedge$ and $\vee$
3. **Implication**: $\to$

### Universal & Existential Generalisation

*'All boys wear glasses'* is written as

$$\forall x(\text{Boy}(x) \to \text{Glasses}(x))$$

If conjunction was used, this statement would be falsified by the existence of a 'non-boy' in the domain of $x$.

*'There is a boy who wears glasses'* is written as

$$\exists x(\text{Boy}(x) \wedge \text{Glasses}(x))$$

If implication was used, this statement would true even if the domain of $x$ is empty.

### Valid Arguments as Tautologies

All valid arguments can be *restated* as tautologies.

### Rules of Inference

Modus ponens

$$p \to q$$
$$p$$
$$\therefore q$$

Modus tollens

$$p \to q$$
$$\sim q$$
$$\therefore \sim p$$

Generalization

$$p$$
$$\therefore p \vee q$$

Specialization

$$p \wedge q$$
$$\therefore p$$

Elimination

$$p \vee q$$
$$\sim q$$
$$\therefore p$$

Transitivity

$$p \to q$$
$$q \to r$$
$$\therefore p \to r$$

Proof by Division into Cases

$$p \vee q$$
$$p \to r$$
$$q \to r$$
$$\therefore r$$

Contradiction Rule

$$\sim p \to \textbf{c(ontradiction)}$$
$$\therefore p$$

### Universal Rules of Inference

Only modus ponens, modus tollens, and transitivity have universal versions in the lecture notes.

### Implicit Quantification

The notation $P(x) \implies Q(x)$ means that every element in the truth set of $P(x)$ is in the truth set of $Q(x)$, or equivalently, $\forall x, P(x) \to Q(x)$.

The notation $P(x) \iff Q(x)$ means that $P(x)$ and $Q(x)$ have identical truth sets, or equivalently, $\forall x, P(x) \leftrightarrow Q(x)$.

### Implication Law

$$p \to q \equiv \sim p \vee q$$

### Universal Instantiation

If some property is true of everything in a set, then it is true of any particular thing in the set.

### Universal Generalization

If $P(c)$ must be true, and we have assumed nothing about $c$, then $\forall x, P(x)$ is true.

### Regular Induction

$$P(0)$$
$$\forall k \in \mathbb{N}, P(k) \to P(k+1)$$
$$\therefore \forall$$

### Epp T2.1.1 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

$$p \wedge \textbf{true} \equiv p$$
$$p \vee \textbf{false} \equiv p$$

Negation Laws

$$p \vee \sim p \equiv \textbf{true}$$
$$p \wedge \sim p \equiv \textbf{false}$$

Double Negative Law

$$\sim (\sim p) \equiv p$$

Idempotent Laws

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

Universal Bound Laws

$$p \vee \textbf{true} \equiv \textbf{true}$$
$$p \wedge \textbf{false} \equiv \textbf{false}$$

De Morgan's Laws

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

Absorption Laws

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

Negations of **true** and **false**

$$\sim \textbf{true} \equiv \textbf{false}$$
$$\sim \textbf{false} \equiv \textbf{true}$$

**Definition 2.2.1 (Conditional)**
If $p$ and $q$ are statement variables, the conditional of $q$ by $p$ is "if $p$ then $q$" or "$p$ implies $q$", denoted $p \to q$. It is false when $p$ is true and $q$ is false; otherwise it is true. We call $p$ the *hypothesis* (or *antecedent*), and $q$ the *conclusion* (or *consequent*).

A conditional statement that is true because its hypothesis is false is called *vacuously true* or *true by default*.

**Definition 2.2.2 (Contrapositive)**
The contrapositive of $p \to q$ is $\sim q \to \sim p$. Note: one will always be equivalent to the other.

**Definition 2.2.3 (Converse)**
The converse of $p \to q$ is $q \to p$.

**Definition 2.2.4 (Inverse)**
The inverse of $p \to q$ is $\sim p \to \sim q$.

**Definition 2.2.6 (Biconditional)**
The biconditional of $p$ and $q$ is denoted $p \leftrightarrow q$ and is true if both $p$ and $q$ have the same truth values, and is false if $p$ and $q$ have opposite truth values.

**Definition 2.2.7 (Necessary & Sufficient)**
"$r$ is sufficient for $s$" means $r \to s$, "$r$ is necessary for $s$" means $\sim r \to \sim s$ or equivalently $s \to r$.

**Definition 2.3.2 (Sound & Unsound Arguments)**
An argument is called *sound*, iff it is valid and all its premises are true.

**Definition 3.1.2 (Universal Statement)**
A *universal statement* is of the form

$$\forall x \in D, Q(x)$$

It is defined to be true iff $Q(x)$ is true for every $x$ in $D$. It is defined to be false iff $Q(x)$ is false for at least one $x$ in D.

**Definition 3.1.3 (Existential Statement)**
A *existential statement* is of the form

$$\exists x \in D \text{ s.t. } Q(x)$$

It is defined to be true iff $Q(x)$ is true for at least one $x$ in $D$. It is defined to be false iff $Q(x)$ is false for all $x$ in $D$.

**Theorem 3.1.6 (Equivalent Forms of Universal and Existential State.)**
By narrowing $\mathcal{U}$ to be the domain $D$ consisting of all values of the variable $x$ that makes $P(x)$ **true**,

$$\forall_{x \in \mathcal{U}}, P(x) \implies Q(x) \equiv \forall_{x \in D}, Q(x)$$

Similarly,

$$\exists x \text{ s.t. } P(x) \wedge Q(x) \equiv \exists x \in D \text{ s.t. } Q(x)$$

**Theorem 3.2.1 (Negation of Universal State.)**
The negation of a statement of the form

$$\forall x \in D, P(x)$$

is logically equivalent to a statement of the form

$$\exists x \in D \text{ s.t. } \sim P(x)$$

**Theorem 3.2.2 (Negation of Existential State.)**
The negation of a statement of the form

$$\exists x \in D \text{ s.t. } P(x)$$

is logically equivalent to a statement of the form

$$\forall x \in D, \sim P(x)$$

Note: for negation of $\exists!$, consider

$$\exists! x \text{ s.t. } P(x) \equiv \exists x \text{ s.t. } (P(x) \wedge (\forall_{y \in \mathcal{U}} P(y) \to (y = x))$$

**Theorem 3.2.4 (Vacuous Truth of Universal State.)**
In general, a statement of the form

$$\forall_{x \in D}, P(x) \to Q(x)$$

is called **vacuously true/true by default** iff $P(x)$ is **false** for every $x$ in $D$

## Sets

**Definition 6.1.1 (Subsets & Supersets)**
$S$ is a subset of $T$ if all the elements of $S$ are elements of $T$, denoted $S \subseteq T$. Formally,

$$S \subseteq T \longleftrightarrow \forall x \in S(x \in T)$$

**Definition 6.2.1 (Empty Set)**
An empty set has no element, and is denoted $\varnothing$ or $\{\}$. Formally, where $\mathcal{U}$ is the universal set:

$$\forall Y \in \mathcal{U}(Y \notin \varnothing)$$

**Epp T6.24**
An empty set is a subset of all sets.

$$\forall S,\ S \text{ is a set}, \varnothing \subseteq S$$

**Definition 6.2.2 (Set Equality)**
Two sets are equal iff they have the same elements.

**Proposition 6.2.3**
For any two sets $X, Y$, $X$ and $Y$ are subsets of each other iff $X = Y$. Formally,

$$\forall X, Y((X \subseteq Y \wedge Y \subseteq X) \longleftrightarrow X = Y)$$

**Epp C6.2.5 (Empty Set is Unique)**
It's what it says.

**Definition 6.2.4 (Power Set)**
The power set of a set $S$ denoted $\mathcal{P}(S)$, or $2^S$; is the set whose elements are all possible subsets of $S$. Formally,

$$\mathcal{P}(S) = \{X \mid X \subseteq S\}$$

**Theorem 6.3.1**
If a set $X$ has $n$ elements, $n \geq 0$, then $\mathcal{P}(X)$ has $2^n$ elements.

**Definition 6.3.1 (Union)**
Let $S$ be a set of sets. $T$ is the union of sets in $S$, iff each element of $T$ belongs to some set in $S$. Formally,

$$T = \bigcup S = \bigcup_{X \in S} X = \{y \in \mathcal{U} \mid \exists X \in S(y \in X)\}$$

**Definition 6.3.3 (Intersection)**
Let $S$ be a non-empty set of sets. $T$ is the intersection of sets in $S$, iff each element of $T$ also belongs to all the sets in $S$. Formally,

$$T = \bigcap S = \bigcap_{X \in S} X$$
$$= \{y \in \mathcal{U} \mid \forall X((X \in S) \to (y \in X))\}$$

**Definition 6.3.5 (Disjoint)**
Let $S, T$ be sets. $S$ and $T$ are disjoint iff $S \cap T = \varnothing$.

**Definition 6.3.6 (Mutually Disjoint)**
Let $V$ be a set of sets. The sets $T \in V$ are mutually disjoint iff every two distinct sets are disjoint. Formally,

$$\forall X, Y \in V(X \neq Y \to X \cap Y = \varnothing)$$

**Definition 6.3.7 (Partition)**
Let $S$ be a set, and $V$ a set of non-empty subsets of $S$. Then $V$ is a partition of $S$ iff

1. The sets in $V$ are mutually disjoint
2. The union of sets in $V$ equals $S$

**Definition 6.3.8 (Non-symmetric Difference)**
Let $S, T$ be two sets. The (non-symmetric) difference of $S$ and $T$ denoted $S - T$ or $S \setminus T$ is the set whose elements belong to $S$ and do not belong to $T$. Formally,

$$S - T = \{y \in \mathcal{U} \mid y \in S \wedge y \notin T\}$$

This is analogous to subtraction for numbers.

**Definition 6.3.10 (Set Complement)**
Let $A \subseteq \mathcal{U}$. Then, the complement of A denoted $\overline{A}$ is $\mathcal{U} - A$.

**Set Properties**
Let $A, B, C$ be sets, some properties are:

- $\bigcup \varnothing = \bigcup_{A \in \varnothing} A = \varnothing$
- $\bigcup \{A\} = A$
- **Commutative Laws**: $A \cup B = B \cup A$, $A \cap B = B \cap A$
- **Associative Laws**: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$
- **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**: $A \cup \varnothing = A$, $A \cap \mathcal{U} = A$
- **Complement Laws**: $A \cup \overline{A} = \mathcal{U}$, $A \cap \overline{A} = \varnothing$
- **Double Complement Law**: $\overline{(\overline{A})} = A$
- **Idempotent Laws**: $A \cup A = A$, $A \cap A = A$
- **Universal Bound Laws**: $A \cup \mathcal{U} = \mathcal{U}$, $A \cap \varnothing = \varnothing$
- **De Morgan's Laws**: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- **Adsorption Laws**: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$
- **Set Difference Law**: $A - B = A \cap \overline{B}$
- $\overline{\mathcal{U}} = \varnothing$, $\overline{\varnothing} = \mathcal{U}$
- $A \subseteq B \leftrightarrow A \cup B = B \leftrightarrow A \cap B = A$

## Functions

**Definition 7.1.1 (Function)**
Let $f$ be a relation such that $f \subseteq S \times T$. Then $f$ is a function from $S$ to $T$ denoted $f : S \to T$ iff

$$\forall x \in S, \exists! y \in T(x\ f\ y)$$

(Intuitively, this means that every element in $S$ must have exactly one 'outgoing arrow', **AND** the 'arrow' must land in $T$.)

**Definitions 7.1.[2-5]**
Let $f : S \to T$ be a function, $x \in S$ and $y \in T$ such that $f(x) = y$; $U \subseteq S$, and $V \subseteq T$.

$x$ is a pre-image (7.1.2) of $y$.

The inverse image of the element (7.1.3) $y$ is the set of all its pre-images, i.e. $\{x \in S \mid f(x) = y\}$.

The inverse image of the set (7.1.4) $V$ is the set that contains all the pre-images of all the elements of $V$, i.e. $\{x \in S \mid \exists y \in V(f(x) = y)\}$.

The restriction (7.1.5) of $f$ to $U$ is the set $\{(x, y) \in U \times T \mid f(x) = y\}$.

**Definition 7.2.1 (Injective, or One-to-one)**
Let $f : S \to T$ be a function. $f$ is injective (or one-to-one) iff

$$\forall y \in T, \forall x_1, x_2 \in S((f(x_1) = y \wedge f(x_2) = y) \to x_1 = x_2)$$

(Intuitively, this means that every element in $T$ has **at most** one 'incoming arrow'.)

**Definition 7.2.2 (Surjective, or Onto)**
Let $f : S \to T$ be a function. $f$ is surjective (or onto) iff

$$\forall y \in T, \exists x \in S(f(x) = y)$$

(Intuitively, this means that every element in $T$ has **at least** one 'incoming arrow'.)

**Definition 7.2.3 (Bijective)**
A function is bijective (or is a bijection) iff it is injective and subjective.
(Intuitively, this means that every element in $T$ has exactly one incoming arrow.)

**Definition 7.2.4 (Inverse)**
Let $f : S \to T$ be a function and let $f^{-1}$ be the inverse relation of $f$ from $T$ to $S$. Then $f$ is bijective iff $f^{-1}$ is a function.
(Note: $f^{-1}$ is defined but not necessary a function. When $A \subseteq T$, $f^{-1}(A)$ means finding all the preimages of each image in $A$, and this is not a function if the $f$ is not bijective.)

**Definition 7.3.1 (Composition)**
Let $f : S \to T$, $g : T \to U$ be functions. The composition of $f$ and $g$ denoted $g \circ f$ is a function from $S$ to $U$.

**Definition 7.3.2 (Identity)**
The identity function on a set $A$, $\mathcal{I}_A$ is defined by,

$$\forall x \in A(\mathcal{I}_A(x) = x)$$

**Proposition 7.3.3**
Let $f : A \to A$ be an injective function of A. Then $f^{-1} \circ f = \mathcal{I}_A$.

**Inclusive Map**
Let $B$ be a subset of A. Then function $\iota_B^A : B \to A; b \mapsto b$ is called the **inclusive map** of $B$ in $A$
**Equality of Functions** Two functions $f$ and $g$ are **equal**, denoted $f = g$, iff:

- the domains of $f$ and $g$ are equal;
- the codomains of $f$ and $g$ are equal;
- $f(x) = g(x)$ for all $x$ in their domains

**Properties of Composite Functions**
Let $f : A \to B, g : B \to C$ and $h : C \to D$ to be functions. Then

- $h \circ (g \circ f) = (h \circ g) \circ f$
- If $f$ and $g$ are injective, $g \circ f$ is injective.
- If $f$ and $g$ are surjective, $g \circ f$ is surjective.
- If $g \circ f$ is injective, then $f$ is injective.
- If $g \circ f$ is surjective, then $g$ is surjective.

**Cantor-Bernstein Theorem**
Let $f : A \to B, g : B \to A$ be injective functions. Then there exists a bijective function $h : A \to B$

## Recursion

**First-order Recurrence Relation**
Let $k, d \in \mathbb{R} with k \neq 0$. Suppose that the sequence $a_1, a_2, \ldots$ of integers satisfies

$$a_{n+1} = ka_n + d$$

for all $n \in \mathbb{Z}^+$. Then

$$a_n = \begin{cases} k^{n-1}a_1 + \frac{k^{n-1}-1}{k-1}d, & \text{if } k \neq 1; \\ a_1 + (n-1)d, & \text{if } k = 1 \end{cases}$$

for all $n \in \mathbb{Z}^+$
**Second-order Recurrence Relation**
Let $s, p \in \mathbb{R}$ with $p \neq 0$ and $s^2 \geq -4p$. Suppose that the sequence $a_1, a_2, \ldots$ of integers satisfies

$$a_{n+2} = sa_{n+1} + pa_n$$

for all $n \in \mathbb{Z}^+$. Let $\alpha$ and $\beta$ be the (real) roots of the quadratic equation $x^2 - sx - p = 0$. Then

$$a_n = \begin{cases} A\alpha^n + B\beta^n, & \text{if } \alpha \neq \beta; \\ (Cn + D)\alpha^n, & \text{if } \alpha = \beta \end{cases}$$

for all $n \in \mathbb{Z}^+$, where $A, B, C, D \in \mathbb{R}$ satisfy

$$\begin{cases} A\alpha + B\beta = a_1 \\ A\alpha^2 + B\beta^2 = a_2 \end{cases} \text{ and } \begin{cases} (C + D)\alpha = a_1 \\ (2C + D)\alpha^2 = a_2 \end{cases}$$

**Recursively Defined Sets**
A recursively defined set consists of following components:

1. **Base:** A statement that certain object is in the set. (e.g. $3 \in S$)
2. **Recursion:** A collection of rules saying how to form new objects that is in the set from those already known to be in the set. (e.g. $\forall x, y \in S, x + y \in S$)
3. **Restriction:** A statement that no object belong to the set other those from base and recursion.

## Number Theory

**Properties (of Numbers)**
Closure, i.e.

$$\forall x, y \in \mathbb{Z},\ x + y \in \mathbb{Z}, \text{ and } xy \in \mathbb{Z}$$

Commutativity, i.e.

$$a + b = b + a \text{ and } ab = ba$$

Distributivity, i.e.

$$a(b + c) = ab + ac \text{ and } (b + c)a = ba + ca$$

Trichotomy, i.e.

$$(a < b) \oplus (b < a) \oplus (a = b)$$

(Can be used without proof)

**Definition 1.3.1 (Divisibility)**
If $n$ and $d$ are integers and $d \neq 0$,

$$d|n \iff \exists k \in \mathbb{Z} \text{ s.t. } n = dk$$

We must take note that $k$ can be 0.

**Example/Lemma on Divisibility**
$\forall a, b, c \in \mathbb{Z}$,

- $(1|a) \wedge (a|a) \wedge (a|0)$
- $(a|1) \to a = \pm 1$
- $(0|a) \to a = 0$
- $(a|b) \leftrightarrow (-a|b) \leftrightarrow (a| - b)$
- $(a|b) \wedge (b|a) \to (a = b \vee a = -b)$
- $(a|b) \wedge (b|c) \to (a|c)$
- $(a|b) \to (ac|bc)$
- $(ac|bc) \wedge (c \neq 0) \to (a|b)$
- $(a|b) \wedge (b \neq 0) \to (|a| \leq |b|)$

**Proposition 1.3.2 (Linear Combination)**

$$\forall a, b, c \in \mathbb{Z},\ a|b \wedge a|c \rightarrow \forall x, y \in \mathbb{Z},\ a|(bx + cy)$$

If $a$ divides $b$ and $c$, then it also divides their linear combination $(bx + cy)$.

**$b$-adic Expansion**
Let $b, n \in \mathbb{Z}^+$ with $b \geq 2$. We say that $n$ has a $b$-adic expansion/decomposition if there exist $k \in \mathbb{Z}^+, a_0, a_1, \ldots, a_k \in \mathbb{Z}$ with $1 \leq a_k < b$ and $0 \leq a_0, a_1, \ldots, a_{k-1} < b$ such that

$$n = a_0 b^0 + a_1 b^1 + \cdots + a_k b^k$$

in which case, $a_0 b^0 + a_1 b^1 + \cdots + a_k b^k$ is the $b$-adic expansion of $n$. This expansion is **unique**

**Representation of Integers (Algorithm for $b$-adic Expansion)**
Given any positive integer $n$ and base $b$, repeatedly apply the Quotient-Remainder Theorem to get,

$$\begin{aligned} n &= bq_0 + r_0 \\ q_0 &= bq_1 + r_1 \\ q_1 &= bq_2 + r_2 \\ &\cdots \\ q_{m-1} &= bq_m + r_m \end{aligned}$$

The process stops when $q_m = 0$. Eliminating the quotients $q_i$ we get,

$$n = r_m b^m + r_{m-1} b^{m-1} + \cdots r_1 b + r_0$$

Which may be represented compactly in base $b$ as a sequence of the digits $r_i$,

$$n = (r_m r_{m-1} \cdots r_1 r_0)_b$$

**Theorem 4.4.1 (Quotient-Remainder Theorem)**
Given any integer $a$ and any positive integer $b$, there exist unique integers $q$ and $r$ such that

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

**Definition 4.5.1 (Greatest Common Divisor)**
Let $a$ and $b$ be integers, not both zero. The *greatest common divisor* of $a$ and $b$, denoted $\gcd(a, b)$, is the integer $d$ satisfying

1. $d \mid a$ and $d \mid b$
2. $\forall c \in \mathbb{Z}\ ((c \mid a)\ \wedge (c \mid b) \rightarrow c \leq d)$

**Greatest Common Divisor Example**
$\forall a, b \in \mathbb{Z} \wedge (a \neq 0)$,

- $\gcd(a, 0) = |a| = \gcd(a, a)$
- $(a|b) \rightarrow \gcd(a, b) = a$
- $\gcd(a, b) = \gcd(|a|, |b|)$

**Proposition 4.5.2 (Existence of gcd)**
For any integers $a$, $b$, not both zero, their gcd exists and is unique.

**Theorem 4.5.3 (Bézout's Identity)**
Let $a$, $b$ be integers, not both zero, and let $d = \gcd(a, b)$. Then there exists integers $x$, $y$ such that

$$ax + by = d$$

Or, the gcd of two integers is some linear combination of the said numbers, where $x$, $y$ above have multiple solution pairs once a solution pair $(x, y)$ is found. Also solutions, for any integer $k$,

$$(x + \frac{kb}{d}, y - \frac{ka}{d})$$

***Epp T8.4.8 (Euclid's Lemma)**
For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

***Epp Lemma 4.8.2 (modified)**
If $a, b \in \mathbb{Z}^+$, and $q, r \in \mathbb{Z}$ s.t. $r = a - bq$, then

$$\gcd(a, b) = \gcd(b, r)$$

In particular, we have:

$$\gcd(a, b) = \gcd(b, a \textbf{ mod } b)$$

**Euclidean Algorithm**
By applying **Epp L4.8.2** we can find gcd of $a, b \in \mathbb{Z}$ (not both 0) using the following algorithm:

1. while not $(a \textbf{ mod } b = 0)$ do
   1.1 $r := a \textbf{ mod } b$
   1.2 $a := b$
   1.3 $b := r$
2. enddo
3. return $|b|$;

**Corollary on GCD**
Let $a, b \in \mathbb{Z}$ (not both 0). We have:

1. Every common divisor of $a$ and $b$ divides $\gcd(a, b)$
2. $\gcd(a, b) = \min\{n \in \mathbb{Z}^+ | \exists x, y \in \mathbb{Z}(n = ax + by)\}$. That is, $\gcd(a, b)$ is the smallest positive integer linear combination of $a$ and $b$.

**Proposition 4.5.5**
For any integers $a$, $b$, not both zero, if $c$ is a common divisor of $a$ and $b$, then $c \mid \gcd(a, b)$.

**Definition 4.2.1 (Prime number)**

$$\begin{aligned} n \text{ is prime} &\iff \forall r, s \in \mathbb{Z}^+ \\ &\quad n = rs \rightarrow \\ &\quad (r = 1 \wedge s = n) \vee (r = n \wedge s = 1) \\ n \text{ is composite} &\iff \exists r, s \in \mathbb{Z}^+ \text{ s.t.} \\ &\quad n = rs \wedge \\ &\quad (1 < r < n) \wedge (1 < s < n) \end{aligned}$$

**Proposition 4.2.2**
For any two primes $p$ and $p'$,

$$p \mid p' \rightarrow p = p'$$

**Theorem 4.2.3**
If $p$ is a prime and $x_1, x_2, \cdots, x_n$ are any integers s.t. $p \mid x_1 x_2 \cdots x_n$, then $p \mid x_i$ for some $x_i, i \in \{1, 2, \cdots, n\}$.

**Fundamental Theorem of Arithmetic**
Given any integer $n > 1$

$$\begin{aligned} &\exists k \in \mathbb{Z}^+, \\ &\exists p_1, p_2, \cdots, p_k \in \text{ primes}, \\ &\exists e_1, e_2, \cdots, e_k \in \mathbb{Z}^+, \end{aligned}$$

such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and any other expression for $n$ as a product of prime numbers is identical, except perhaps for the order in which the factors are written.

**Epp Proposition 4.7.3**
For any $a \in \mathbb{Z}$ and any prime $p$,

$$p \mid a \rightarrow p \nmid (a + 1)$$

**Epp T4.7.4 (Infinitude of Primes)**
The set of primes is infinite.

**Definition 4.5.4 (Relatively Prime/Coprime)**
Integers $a$ and $b$ are *relatively prime* (or *coprime*) iff $\gcd(a, b) = 1$.

**Definition 4.3.1 (Lower Bound)**
An integer $b$ is said to be a *lower bound* for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.

Does not require $b$ to be in $X$.

**Theorem 4.3.2 (Well Ordering Principle)**
If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then $S$ has a least element.

Note three conditions: $|S| > 0$, $S \subseteq \mathbb{Z}$, and $S$ has lower bound.

Likewise, if ... upper bound ... has a greatest element.

**Proposition 4.3.3 (Uniqueness of least element)**
If a set $S$ has a least element, then the least element is unique.

**Proposition 4.3.4 (Uniqueness of greatest e.)**
If a set $S$ has a greatest element, then the greatest element is unique.

**Definitoin 4.7.1 (Congruence modulo)**
Let $m, z \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. We say that $m$ is *congruent* to $n$ *modulo* $d$ and write

$$m \equiv n \pmod{d}$$

iff

$$d \mid (m - n)$$

More concisely,

$$m \equiv n \pmod{d} \iff d \mid (m - n)$$

**Epp T8.4.1 (Modular Equivalences)**
Let $a, b, n \in \mathbb{Z}$ and $n > 1$. The following statements are all equivalent,

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some $k \in \mathbb{Z}$
4. $a$ and $b$ have the same non-negative remainder when divided by $n$
5. $a \bmod n = b \bmod n$

**Epp T8.4.3 (Modulo Arithmetic)**
Let $a, b, c, d, n \in \mathbb{Z}$, $n > 1$, and suppose

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$, for all $m \in \mathbb{Z}^+$

**Lemmas on Modulo Congruences**
Let $a, b, c, n \in \mathbb{Z}$, $n > 0$. Suppose that $ac \equiv bc \pmod{n}$. Then

$$a \equiv b \pmod{\frac{n}{\gcd(c, n)}}$$

Also, $\exists x \in \mathbb{Z}$ s.t. $ax \equiv b \pmod{n}$ iff. $\gcd(a, n) | b$.
This means, when we assume $\gcd(a, n) | b$, $\forall x \in \mathbb{Z}$, we have

$$ax \equiv b \pmod{n} \Leftrightarrow \frac{a}{\gcd(a, n)} x \equiv \frac{b}{\gcd(a, n)} \pmod{\frac{n}{\gcd(a, n)}}$$

**Epp Corollary 8.4.4**
Let $a, b, c, d, n \in \mathbb{Z}$, $n > 1$, then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n}$$

or equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n$$

In particular, if $m$ is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}$$

**Definition 4.7.2 (Multiplicative inv. modulo $n$)**
For any integers $a, n$ with $n > 1$, if an integer $s$ is such that $as \equiv 1 \pmod{n}$, then $s$ is the *multiplicative inverse of $a$ modulo $n$*. We may write $s$ as $a^{-1}$.

Because the commutative law still applies in modulo arithmetic, we also have

$$a^{-1} a \equiv 1 \pmod{n}$$

Multiplicative inverses are not unique. If $s$ is an inverse, then so is $(s + kn)$ for any integer $k$.

**Corollary on m. inverse**
Let $a, n \in \mathbb{Z}$ with $n > 0$. Suppose that $a$ and $n$ are coprime and let $a'$ be a multiplicative inverse of $a$ modulo $n$. Then

$$\forall x \in \mathbb{Z}(ax \equiv b \pmod{n} \Leftrightarrow x \equiv a'b \pmod{n})$$

**Theorem 4.6.3 (Existence of multiplicative inverse)**
For any integer $a$, its multiplicative inverse modulo $n$ where $n > 1$, $a^{-1}$, exists iff $a$ and $n$ are coprime.

**Finding the Multiplicative Inverse/Extended Euclidean Algorithm**
For example, to find the multiplicative inverse of 5 mod 18,

$$\begin{aligned} 18 &= 3 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 1 &= 1 \times 1 + 0 \end{aligned}$$

So

$$\begin{aligned} 1 &= 1 \times 1 + 0 = 1 \\ &= 1(3 - 1 \times 2) = 3 - 2 \\ &= 3 - (5 - 3) = 2 \times 3 - 5 \\ &= 2(18 - 3 \times 5) - 5 = 2 \times 18 - 7 \times 5 \\ 1 - 2 \times 18 &= -7 \times 5 \\ 1 - 2 \times 18 &\equiv -7 \times 5 \pmod{18} \\ 1 &\equiv -7 \times 5 \pmod{18} \end{aligned}$$

Therefore, we have $5^{-1} \bmod 18 = -7$, or equivalently under modulo 11.

**Corollary 4.7.4 (Special case: $n$ is prime)**
If $n = p$ is a prime number, then all integers $a$ in the range $0 < a < p$ have multiplicative inverses modulo $p$.

**Epp T8.4.9 (Cancellation Law for mod. arith.)**
For all $a, b, c, n \in \mathbb{Z}$, $n > 1$, and $a$ and $n$ are coprime,

$$ab \equiv ac \pmod{n} \rightarrow b \equiv c \pmod{n}$$

## Relations

**Definition**
A **relation** $R$ from $A$ to $B$ is a subset of $A \times B$. Function can be thought as special cases of relations.

**Domain** of $R$ is the set $a \in A | \exists b \in B aRb$ **Range** of $R$ is the set $b \in B | \exists a \in A aRb$

**Inverse** of $R$, denoted $R^{-1}$, is the relation from $B$ to $A$ defined by

$$R^{-1} = \{(b, a) \in B \times A | aRb\}$$

We say that a binary relation $R$ on $A$ is:

- **reflexive** iff. $\forall x \in A, xRx$
- **symmetric** iff. $\forall x, y \in A, (xRy \rightarrow yRx)$
- **transitive** iff. $\forall x, y, z \in A, (xRy \wedge yRz \rightarrow xRz)$
- **an equivalence relation** iff. it satisfies all 3 above

**Equivalence Classes**
Let $R$ be an equivalence relation on $A$ (assumed non-empty). For each $a \in A$, the equivalence class of $a$ with respect to $R$, denoted $[a]$, is the set

$$[a] = \{x \in A | aRx\}$$

The set of all equivalence classes of $R$ is denoted as $A/R$.

Any two distinct equivalence classes of an equivalence relation are disjoint. Also, $A/R$ is a partition of $A$.

Every partition is a set of equivalence classes. That is, let $P \subseteq \mathcal{P}(A)$ be a partition of $A$, there exist a equivalence relation $R$ s.t. $A/R = P$.

**Partial Order**
Keywords: partial order, $\preceq$, Hasse diagram
Refer to Lecture Notes 9 (IX), part II.

## Counting and Probability

**Application to Decimal Expansions of Fractions**
By using pigeonhole principle, we can prove that the decimal expansion of any rational number either terminates or repeats.

**Generalized Pigeonhole Principle**
For any function $f$ from a finite set $X$ with $n$ elements to a finite set $Y$ with $m$ elements and for any positive integer $k$, if for each $y \in Y$, $f^{-1}(\{y\})$ has at most $k$ elements, then $X$ has at most $km$ elements. In other words, $n \leq km$.
**Repetition Allowed - Combination** If order does not matter (C) and repetition is allowed, we use:

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

**Pascal's Formula**
Suppose $n$ and $r$ are positive integers with $r \leq n$. Then

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

**Binomial Theorem**
Given $a, b \in \mathbb{R}$ and $n \in \mathbb{Z}_{\geq 0}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Consider $a = b = 1$, we have:

$$\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

**Linearity of Expectation**
For random variable $X$ and $Y$ **(which can be dependent)**,

$$E[X + Y] = E[X] + E[Y]$$

**Conditional Probability**

$$P(A \cap B) = P(B|A) \cdot P(A)$$

**Bayer's Theorem**
Suppose that a sample space $S$ is a union of mutually disjoint events $B_1, B_2, B_3, \ldots, B_n$.
Suppose $A$ is an event in $S$, and suppose $A$ and all $B_i$ have non-zero probabilities.
If $k$ is an integer with $1 \leq k \leq n$, then

$$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + \cdots + P(A|B_n) \cdot P(B_n)}$$

**Independent Events**
Two events $A$ and $B$ are independent iff. $P(A \cap B) = P(A) \cdot P(B)$.
We can observe that $P(A|B) = P(A)$.

We must take note that pairwise independent is different from mutually independent. $A$, $B$ and $C$ are 3 events, they are pairwise independent if they satisfy condition 1-3 below. They are mutually independent if they satisfy all 4.

1. $P(A \cap B) = P(A) \cdot P(B)$
2. $P(A \cap C) = P(A) \cdot P(C)$
3. $P(B \cap C) = P(B) \cdot P(C)$
4. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

**Important:** Knowing 1-3 cannot deduct 4 above, and the converse (knowing 4 cannot deduct 1-3)is also applicable.

## Graphs and Tree

**Definitions**

- **graph, edges, endpoints, connect, vertices, adjacent** XII-9
- **directed graph** XII-12
- **simple graph** XII-19
- **complete (bipartite) graph** XII-20/21
- **walk, trail, path, closed walk, circuit/cycle, simple circuit** XII-34
- **connectedness** XII-37
- **Euler Circuit** XII-44 (Existence condition: XII-48: Every vertex has positive even degree)
- **Euler Trail** XII-49 (Existence condition: XII-49)
- **Hamiltonian Circuit** XII-56 (properties: XII-61)
- **matrices of graph (calculating walks)** XII-66
- **tree, trivial tree** XIII-3
- **rooted tree, height, level** XIII-23
- **child, sibling, parent, ancestor, descendent** XIII-24
- **(full) binary tree** XIII-27
- **spanning tree** XIII-52

**Handshake Theorem**
Total degree of $G = 2 \times$ (the number of edges of $G$)

**Theorem 10.5.4(XIII-19)**
If $G$ is a connected graph with $n$ vertices and $n - 1$ edges, then $G$ is a tree.

**Full Binary Tree Theorem**
If $T$ is a full binary tree with $n$ internal vertices, then $T$ has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices.

**Theorem 10.6.2(XIII-36)**
A binary tree with height $h$ has at most $2^h$ terminal vertices.

**Minimum spanning tree**
Kruskal's Algo (XIII-57): Add edges in order of low weight to high weight

Prim's Algo (XIII-62): Choose a starting point, then add edges of the least weight connecting the part of the tree and the part not in the tree