MACM 101

Dr. C. Kay Wiese

1 Counting

1.1 The Rules of Sums and Products

Be careful of initial conditions (duplicates and assumptions)
Rules of Sums

If task A can be performed in m ways, while task B can be performed in n ways and A and B cannot be done simultaneously, then performing either task can be done in any one of $m + n$ ways
Rules of Products

A procedure P can be broken down into A and B stage. If A has m outcomes and B has n outcomes, P can be carried out in $m * n$ ways.

1.2 Permutations

- Distinct Objects
- Linear arrangement objects, i.e. the *order* of objects is important

Definition 1.1. *Factorials*

For integer $n \geq 0$,

$$n! = \begin{cases} 1 & n = 0 \\ n * (n-1)! & n \geq 1 \end{cases}$$

Definition 1.2.

If there are n distinct objects and $1 \leq r \leq n$, then, by rule of product, the number of permutations of size r for the n objects is

$$P(n, r) = \frac{n!}{(n-r)!}$$

1.3 Combinations

Definition 1.3.

If there are n distinct objects and $1 \leq r \leq n$, then the number of combinations of size r for the n objects is

$$\binom{n}{k} = C(n,r) = \frac{n!}{(n-r)!r!}$$

You can use a combinatorial argument in proofs.

Proposition 1.3.1. *For positive integers n and k with $n = 2k$, $\frac{n!}{2!^k}$ is an integer.*

Proof. Consider the n symbols: $x_1, x_1, x_2, x_2, \cdots, x_k, x_k$. The number of arrangements of all these $n = 2k$ symbols is an integer that equals

$$\frac{n!}{\underbrace{2!2!\cdots 2!}_{\text{k factors of 2!}}} = \frac{n!}{2!^k}$$

Definition 1.4. *Sigma notation*

$$a_m + a_{m+1} + a_{m+2} + \cdots + a_{m+n} = \sum_{i=m}^{m+n} a_i$$

Definition 1.5. *Weight*

Weight of a string $X = x_1 x_2 \ldots x_n$ is defiined as $\text{wt}(X) = \sum_{i=1}^{n} x_i$

Theorem 1.1. *Binomial Theorem*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Corollary 1.1.1.

Set $x = y = 1$, then it follows that

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Corollary 1.1.2.

Similary, set $x = -1$ and $y = 1$, then it follows that

$$\sum_{i=0}^{n} -1^i \binom{n}{i} = 0$$

Theorem 1.2. *Multinomial Theorem*

With integers $n, t > 0$, the coefficient of $x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$ in the expansion of $(x_1 + x_2 + \cdots + x_t)^n$ is

$$\frac{n!}{n_1! n_2! \cdots n_t!} = \binom{n}{n_1, n_2, \cdots n_t}$$

where each n_i is an integer with $0 \leq n_i \leq n$, for all $1 \leq i \leq t$, and $n_1 + n_2 + \cdots + n_t = n$.

Proof. Choose x_1 from n_1 out of n factors, then choose x_2 from n_2 out of $n - n_1$ factors, and so on. This gives

$$\begin{aligned}
& \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{t-1}}{n_t} \\
= \; & \frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdots\frac{(n-n_1-n_2-\cdots-n_{t-1})!}{n_t!(n-n_1-n_2-\cdots-n_{t-1}-n_t)!} \\
= \; & \frac{n!}{n_1! n_2! \cdots n_t!}
\end{aligned}$$

1.4 Combinations with Repetition

The number of ways to select r of n distinct objects with repetitions is

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

It is equivalent to the number of ways to separate r identical stones with $n - 1$ identical sticks where there are n slots to represent how many times the nth object was chosen with the number of stones.

Same logic can be used for counting how many ways r objects can be distributed to n containers, or how many ways n nonnegative integers can add up to r (order matters).

You can also count the number of execution of such codes:

```
counter := 0;
for i = 1 to n do
    for j = 1 to i do
        for k = 1 to j do
            counter := counter + 1;
```

It is equivalent to counting how many triples of (i, j, k) satisfy $1 \leq k \leq j \leq i \leq n$, which is choosing 3 numbers from n numbers with repetitions. *counter* would be $\binom{n+3-1}{3}$.

2 Fundamentals of Logic

2.1 Basic Connectives and Truth Tables

Definition 2.1. Declarative sentences that are either true or false are called *statements*(or *propositions*), and we use lowercase letters of the alphabet to represent such statements.

Primitive statements cannot be broken down into anything simpler, and new statements can be obtained from existing ones in two ways.

1. Transform a given statement p to $\neg p$ (Not p).

2. Combine two or more statements into a *compound* statement, using one of the *logical connectives*.

   (a) Conjunction: $p \wedge q$ (p and q)

   (b) Disjunction:

      i. $p \vee q$ (p or q)

      ii. $p \veebar q$

   (c) Implication: $p \rightarrow q$ (p implies q)

   (d) Biconditional: $p \leftrightarrow q$ (p if and only if q)

Here is the truth table.[1]

p	q	$p \wedge q$	$p \vee q$	$p \veebar q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

Definition 2.2. A compound statement is called a *tautology* if it is always true. If it is always false, it is called a *contradiction.*

We use the symbol T_0 to denote any tautology and the symbol F_0 to denote any contradiction.

[1]Sometimes, 0 and 1 are used for F and T instead, similar to bit-logic.

2.2 Logical Equivalence: The Laws of Logic

Definition 2.3. Two statements s_1, s_2 are said to be *logically equivalent* when $s_1 \leftrightarrow s_2$, and we write $s_1 \Leftrightarrow s_2$.

If 2 statements are not logically equivalent, we write $s_1 \not\Leftrightarrow s_2 \quad (\neg(s_1 \Leftrightarrow s_2))$.

The Laws of Logic

1)	$\neg\neg p \Leftrightarrow p$	Law of Double Negation
2)	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	DeMorgan's Laws
	$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	
3)	$p \wedge q \Leftrightarrow q \wedge p$	Commutative Laws
	$p \vee q \Leftrightarrow q \vee p$	
4)	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Associative Laws
	$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	
5)	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributive Laws
	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	
6)	$p \vee p \Leftrightarrow p$	Idempotent Laws
	$p \wedge p \Leftrightarrow p$	
7)	$p \vee F_0 \Leftrightarrow p$	Identity Laws
	$p \wedge T_0 \Leftrightarrow p$	
8)	$p \vee \neg p \Leftrightarrow T_0$	Inverse Laws
	$p \wedge \neg p \Leftrightarrow F_0$	
9)	$p \wedge F_0 \Leftrightarrow F_0$	Domination Laws
	$p \vee T_0 \Leftrightarrow T_0$	
10)	$p \vee (p \wedge q) \Leftrightarrow p$	Absorption Laws
	$p \wedge (p \vee q) \Leftrightarrow p$	

Following statements are also equivalent.

1. $p \to q \Leftrightarrow \neg p \vee q$
2. $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p) \Leftrightarrow (\neg p \vee q) \wedge (\neg q \vee p)$
3. $p \veebar q \Leftrightarrow (p \vee q) \wedge \neg(p \wedge q)$

Using the above logival equivalences, we can eliminate those three connectives($\to$, $\leftrightarrow, \veebar$) from any logical compound statements.

Definition 2.4. Let s be a statement containing only $\wedge$ and $\vee$ as logical connectives. The dual of s, denoted s^d, is derived from s by replacing each $\wedge$ with $\vee$, $\vee$ with $\wedge$, T_0 with F_0, and F_0 with T_0.

If p is a primitive statement, then p_d is the same as p.

$$p = p^d$$

Theorem 2.1. *The Principle of Duality.* Let s and t be statements containing no logical connectives other than $\wedge$ and $\vee$. If $s \Leftrightarrow t$, then $s^d \Leftrightarrow t^d$.

2.2.1 The Subtitution Rules

1. Suppose, compound statement P is a tautology. If p is a primitive statement that appears in P and we replace all occurrences of p by an arbitrary statement q, then the resulting compound statement P_1 is also a tautology.

2. P is a compound statement, p is an arbitrary statement that appears in P, let q be a statement such that $p \Leftrightarrow q$. Now replace 1 or more occurrences of p by q, this yields P_1. Now, $P_1 \Leftrightarrow P$.

2.2.2 Relatives of the Implication $p \to q$

Inverse:	$\neg p \to \neg q$
Converse:	$q \to p$
Contrapositive:	$\neg q \to \neg p$

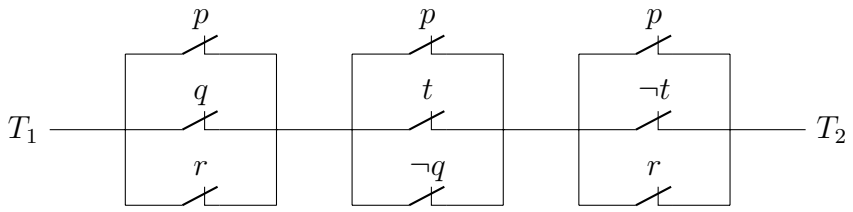
1)	$p \to q \Leftrightarrow \neg q \to \neg p$	Implication $\Leftrightarrow$ Contrapositive
2)	$q \to p \Leftrightarrow \neg p \to \neg q$	Converse $\Leftrightarrow$ Inverse
3)	$p \to q \not\Leftrightarrow q \to p$	Implication $\not\Leftrightarrow$ Converse
4)	$\neg p \to \neg q \not\Leftrightarrow \neg q \to \neg p$	Contrapositive $\not\Leftrightarrow$ Inverse

An implication is logically equivalent to its contrapositive, but not to its inverse or converse. At the same time, its inverse and converse are logically equivalent.

(*Note:* The negation of an it-then statement (in words) does not begin with the word if. i.e. it is not another implication.)

2.2.3 Applications: Simplifying Switching Networks

A switching network is made up of wires and switches connecting two Terminals T_1 and T_2. In such a network, each switch is either open (0) so current doesn't flow, or closed (1) so current does flow through it. Switches in *parallel* are represented by $\vee$, and switches in *series* are represented by $\wedge$.



Such network can be represented by the statement $(p \vee q \vee r) \wedge (p \vee t \vee \neg q) \wedge (p \vee \neg t \vee r)$. This can be simplified using the laws of logic.

		Reasons
	$(p \vee q \vee r) \wedge (p \vee t \vee \neg q) \wedge (p \vee \neg t \vee r)$	
$\Leftrightarrow$	$p \vee [(q \vee r) \wedge (t \vee \neg q) \wedge (\neg t \vee r)]$	Distributive Law of $\wedge$ over $\vee$
$\Leftrightarrow$	$p \vee [(q \vee r) \wedge (\neg t \vee r) \wedge (t \vee \neg q)]$	Commutative Law of $\wedge$
$\Leftrightarrow$	$p \vee [((q \wedge \neg t) \vee r) \wedge (t \vee \neg q)]$	Distributive Law of $\wedge$ over $\vee$
$\Leftrightarrow$	$p \vee [((q \wedge \neg t) \vee r) \wedge (\neg\neg t \vee \neg q)]$	Law of Double Negation
$\Leftrightarrow$	$p \vee [((q \wedge \neg t) \vee r) \wedge \neg(\neg t \wedge q)]$	DeMorgan's Law
$\Leftrightarrow$	$p \vee [\neg(\neg t \wedge q) \wedge ((\neg t \wedge q) \vee r)]$	Commutative Law of $\wedge$
$\Leftrightarrow$	$p \vee [(\neg(\neg t \wedge q) \wedge (\neg t \wedge q)) \vee (\neg(\neg t \wedge q) \wedge r)]$	Distributive Law of $\wedge$ over $\vee$
$\Leftrightarrow$	$p \vee [F_0 \vee (\neg(\neg t \wedge q) \wedge r)]$	$s \wedge \neg s \Leftrightarrow F_0$ for any statement s
$\Leftrightarrow$	$p \vee [\neg(\neg t \wedge q) \wedge r]$	F_0 is the Identity for $\vee$
$\Leftrightarrow$	$p \vee [r \wedge \neg(\neg t \wedge q)]$	Commutative Law of $\wedge$
$\Leftrightarrow$	$p \vee [r \wedge (t \vee \neg q)]$	DeMorgan's Law and the Law of Double Negation

2.3 Logical Implication: Rules of Inference

We show an argument with premises $(p_1, p_2, \cdots, p_n)$ and conclusion q is valid by showing the following implication is a tautology:

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

To show the following implication is a tautology, we need to show that q is true if all the premises are true.

You can incorporate this into an automatic "inference engine", the basic component of an AI expert system. These systems combine basic facts to develop more facts.

Definition 2.5. If p, q are arbitrary statements such that $p \to q$ is a tautology, then we say that p *logically implies* q and we write $p \Rightarrow q$ to denote this situation.

The notation $p \not\Rightarrow q$ is used to indicate that $p \to q$ is *not* a tautology — so the given implication $(p \to q)$ is not a logical implication. If $p \Leftrightarrow q$, then $p \leftrightarrow q$ is a tautology. This means $p \to q$ and $q \to p$ are tautologies, too, thus $p \Rightarrow q$ and $q \Rightarrow p$. The converse is also true.

When establishing the validity of an argument, the rules of inferences will enable us to consider only the cases wherein all the premises are true. They are fundamental in the development of a step-by-step validation of how the conclusion q logically follows from the premises $p_1, p_2, \cdots, p_n$ in an implication of the form

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q.$$

This development will establish the validity of the given arguement, for it will show how the truth of the conclusion can be deduced from the truth of the premises.

	Rule of Inference	Related Logical Implication	Name of Rule
1)	p $p \to q$ $\therefore \quad q$	$[p \wedge (p \to q)] \to q$	Rule of Detachment / Modus Ponens
2)	$p \to q$ $q \to r$ $\therefore \quad p \to r$	$[(p \to q) \vee (q \to r)] \to (p \to r)$	Law of the Syllogism
3)	$p \to q$ $\neg q$ $\therefore \quad \neg p$	$[(p \to q) \wedge \neg q)] \to \neg p$	Modus Tollens
4)	p q $\therefore \quad p \wedge q$		Rule of Conjunction
5)	$p \vee q$ $\neg p$ $\therefore \quad q$	$[(p \vee q) \wedge \neg p] \Rightarrow q$	Rule of Disjunctive Syllogism
6)	$\neg p \to F_0$ $\therefore \quad p$	$(\neg p \to F_0) \to p$	Rule of Contradiction
7)	$p \wedge q$ $\therefore \quad p$	$(p \wedge q) \to p$	Rule of Conjunctive Simplification
8)	p $\therefore \quad p \vee q$	$p \to p \vee q$	Rule of Disjunctive Amplification
9)	$p \wedge q$ $p \to (q \to r)$ $\therefore \quad r$	$[(p \wedge q) \wedge [p \to (q \to r)]] \to r$	Rule of Conditional Proof
10)	$p \to r$ $q \to r$ $\therefore \quad (p \vee q) \to r$	$[(p \to r) \wedge (q \to r)] \to [(p \vee q) \to r]$	Rule for Proof Cases
11)	$p \to q$ $r \to s$ $p \vee r$ $\therefore \quad q \vee s$	$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to (q \vee s)$	Rule of the Constructive Dilemma
12)	$p \to q$ $r \to s$ $\neg q \vee \neg s$ $\therefore \quad \neg p \vee \neg r$	$[(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s)] \to (\neg p \vee \neg r)$	Rule of Destructive Dilemma

The Rule of Contradiction is the basis of a method of *Proof by Contradiction*, or *Reductio ad Absurdum*. In a Proof of Contradiction, we establish the validity of the argument

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

by establishing the validity of the logically equivalent argument

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge q) \rightarrow F_0.$$

We first assume that what we are trying to prove is actually false, then produce a contradiction of the form $s \wedge \neg s$, for some statement s. This contradiction concludes that the statement that was assumed to be false is in fact true, and this validates the argument (or completes the proof).

2.4 Predicate Logic and Quantifiers

Definition 2.6. A declarative sentence is an *open statement* if

1. It contains one or more variables, and
2. It is not a statement, but
3. It becomes a statement when the variables in it are replaced by certain allowable choices.

All of these are open statements:

The number $x - 5$ is an even integer.
$x - 5 = 7$
$3x + y > 7$

The allowable choices of variable constitute what is called the *universe*[2] or *universe of discourse* for the open statement. Open statements are denoted by $p(x), q(x, y)$, etc. (also called predicates).

We can *quantify* an open statement with two types of quantifiers:

1. existential quantifier: $\exists$
   $\exists x$: For some x
   For at least one x
   There exists an x such that ...

[2]This is an example of a *set*

2. universal quantifier: $\forall$

   $\forall x$: For all x
   For any x
   For every x

Variable x is called a *free* variable in an open statement and a *bound* variable in a quantified open statement.

Let $p(x)$ denote any open statement with a prescribed *nonempty* universe. Then,

$$\forall x\ p(x) \Rightarrow \exists x\ p(x).$$

Definition 2.7. Let $p(x), q(x)$ be open statements defined for a given universe.

When the biconditional $p(a) \leftrightarrow q(a)$ is true for each replacement a from the universe (that is, $p(a) \Leftrightarrow q(a)$ for each a in universe), we write $\forall x\ [p(x) \Leftrightarrow q(x)]$.

If the implication $p \rightarrow q$ is true for each a in the universe (that is, $p(a) \Rightarrow q(a)$ for each a in universe), then we write $\forall x\ [p(x) \Rightarrow q(x)]$.

Definition 2.8. For open statements $p(x), q(x)$ — defined for a prescribed universe — and the universally quantified statement $\forall x\ [p(x) \rightarrow q(x)]$, we define:

1)	Contrapositive of	$\forall x\ [p(x) \rightarrow q(x)]$	to be	$\forall x\ [\neg q(x) \rightarrow \neg p(x)]$
2)	Converse of	$\forall x\ [p(x) \rightarrow q(x)]$	to be	$\forall x\ [q(x) \rightarrow p(x)]$
3)	Inverse of	$\forall x\ [p(x) \rightarrow q(x)]$	to be	$\forall x\ [\neg p(x) \rightarrow \neg q(x)]$

For a prescribed universe and any open statements $p(x), q(x)$ in the variable x:

$$\exists x\ [p(x) \wedge q(x)] \Rightarrow [\exists x\ p(x) \wedge \exists x\ q(x)]$$

$$\exists x\ [p(x) \vee q(x)] \Leftrightarrow [\exists x\ p(x) \vee \exists x\ q(x)]$$

$$\forall x\ [p(x) \wedge q(x)] \Leftrightarrow [\forall x\ p(x) \wedge \forall x\ q(x)]$$

$$[\forall x\ p(x) \vee \forall x\ q(x)] \Rightarrow \forall x\ [p(x) \vee q(x)]$$

Negation of quantifications:

$$\neg[\forall x\ p(x)] \Leftrightarrow \exists x\ \neg p(x)$$

$$\neg[\exists x\ p(x)] \Leftrightarrow \forall x\ \neg p(x)$$

3 Sets

3.1 Introduction to Sets

Definition 3.1. A set is a collection of objects. The objects in a set are also called its *members,* or *elements.* A set is said to contain its elements.

- Elements of sets can be related, or completely unrelated.
- Uppercase letters A, B, C, ..., S, T, ... are used to denote sets.
- Order of elements does not matter.
- $x \in A$ indicates that x is an element of A.
- $x \notin A$ indicates that x is not an element of A.

3.1.1 Infinite Sets

- $\mathbb{N}$ = Set of natural numbers
- $\mathbb{Z}$ = Set of integers
- $\mathbb{Q}$ = Set of rational numbers
- $\mathbb{R}$ = Set of real numbers

3.1.2 Set Builder Notation

$$A = \{x|condition\}$$

The vertical line | is read *such that*, and the symbols $\{x|\dots\}$ are read *the set of all x such that ....*

Definition 3.2. Two sets are equal if and only if they have exactly the same elements.[3]

3.1.3 Cardinality

Definition 3.3. Let S be a set. If there are exactly n distinct elements in S, we say S is a finite set and that n is the cardinality of n denoted by $|S|$.

Definition 3.4. A set is infinite if it is not finite.

[3] $A = \{1, 2, 3\}$ and $B = \{1, 1, 2, 3, 2, 3, 3\}$ are considered to be the same set.

3.1.4 Cartesian Product

Definition 3.5. Let A and B be sets. The cartesian product of A and B, denoted by $A \times B$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}$$

3.2 Subsets

Definition 3.6. Set A is said to be a subset of B if and only if every element of A is also an element of B. We use $A \subseteq B$ to indicate that A is a subset of B. In predicate logic,

$$A \subseteq B \leftrightarrow \forall x \, [x \in A \rightarrow x \in B].$$

- $A \subset B$ means A is a proper subset of B when $(A \subseteq B) \wedge (A \neq B)$
- To show that $A = B$, we show that $(A \subseteq B) \wedge (B \subseteq A)$.

Definition 3.7. The *null set,* or *empty set,* is the set containing no elements. It is denoted by $\emptyset$ or $\{\ \}$.

3.2.1 The Power Set

Definition 3.8. Given a set S, the *power set* of S is the set of all subsets of S. We denote this by $P(S)$[4].

For any finite set A with $|A| = n \geq 0$, A has 2^n subsets and $|P(A)| = 2^n$.

3.3 Set Operations

Definition 3.9. For $A, B \subseteq U$, we define the following:

- $A \cup B = \{x | x \in A \vee x \in B\}$
- $A \cap B = \{x | x \in A \wedge x \in B\}$
- $A \triangle B = \{x | x \in A \cup B \wedge x \notin A \cap B\}$

[4]In some computer science books 2^A is used for $P(A)$.

Definition 3.10. Let $S, T \subseteq U$. The sets S and T are called *disjoint,* or *mutually disjoint,* when $S \cap T = \emptyset$.

Definition 3.11. For a set $A \subseteq U$, the *complement* of A, denoted $U - A$, or $\overline{A}$, is given by $\{x | x \in U \wedge x \notin A\}$

The Laws of Set Theory

1)	$\overline{\overline{A}} = A$	Law of Double Complement
2)	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	DeMorgan's Laws
	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	
3)	$A \cup B = B \cup A$	Commutative Laws
	$A \cap B = B \cap A$	
4)	$A \cup (B \cup C) = (A \cup B) \cup C$	Associative Laws
	$A \cap (B \cap C) = (A \cap B) \cap C$	
5)	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C))$	
6)	$A \cup A = A$	Idempotent Laws
	$A \cap A = A$	
7)	$A \cup \emptyset = A$	Identity Laws
	$A \cap U = A$	
8)	$A \cup \overline{A} = U$	Inverse Laws
	$A \cap \overline{A} = \emptyset$	
9)	$A \cup U = U$	Domination Laws
	$A \cap \emptyset = \emptyset$	
10)	$A \cup (A \cap B) = A$	Absorption Laws
	$A \cap (A \cup B) = A$	

Definition 3.12. Let s be a statement dealing with the equality of two set expressions. The *dual* of s, denoted s^d, is obtained from replacing (1) each occurrence of $\emptyset$ and U by U and $\emptyset$, respectively; and (2) each occurrence of $\cap$ and $\cup$ by $\cup$ and $\cap$, respectively.

Theorem 3.1. *The Principle of Duality.* Let s be a theorem dealing with the equality of two set expressions. Then s^d, the dual of s, is also a theorem.

4 Properties of the Integers: Mathematical Induction

4.1 The Well-Ordering Principle

Definition 4.1. *The Well-Ordering Principle.* Every *nonempty* subset of $\mathbb{Z}^+$ contains a smallest element. ($\mathbb{Z}^+$ is *well ordered.)*

$$\forall X \subseteq \mathbb{Z}^+ \wedge X \neq \emptyset \; \exists \, a \in X \mid \forall x \in X : a \leq x$$

We can express the set $\mathbb{Z}^+$ using the inequality symbol $\geq$:

$$\mathbb{Z}^+ = \{x \in \mathbb{Z} | x > 0\} = \{x \in \mathbb{Z} | x \geq 1\}.$$

You cannot with $\mathbb{Q}^+$ and $\mathbb{R}^+$ because they are not well ordered. If q is a positive rational number, then since $0 < q/2 < q$, we would have a smaller positive rational number $q/2$.

Theorem 4.1. *The Principle of Mathematical Induction.* Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n, which represents a positive integer.

(a) If $S(1)$ is true; and

(b) If whenever $S(k)$ is true (for some particular, but arbitrarily chosen, $k \in \mathbb{Z}^+$), then $S(k+1)$ is true;

then $S(n)$ is true for all $n \in \mathbb{Z}^+$.
Proof. Let $S(n)$ be such an open statement satisfying conditions (a) and (b), and let $F = \{t \in \mathbb{Z}^+ | S(t) \text{ is false}\}$. We wish to prove that $F = \emptyset$, so to obtain a contradiction we assume that $F \neq \emptyset$. Then by the Well-Ordering Principle, F has a least element m. Since $S(1)$ is true, it follows that $m \neq 1$, so $m > 1$, and consequently $m - 1 \notin F$, we have $S(m-1)$ true. So by condition (b) it follows that $S((m-1)+1) = S(m)$ is true, contradicting $m \in F$. This contradiction arose from the assumption that $F \neq \emptyset$. Consequently, $F = \emptyset$.

Theorem 4.2. *The Principle of Mathematical Induction — Alternate Form.* Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n, which represents a positive integer. Also let. $n_0, n_1 \in \mathbb{Z}^+$ with $n_0 \leq n_1$.

(a) If $S(n_0), S(n_0+1), \ldots, S(n_1-1)$, and $S(n_1)$ are true; and

(b) If whenever $S(n_0), S(n_0+1), \ldots, S(k-1)$, and $S(k)$ are true for some (particular, but arbitrarily chosen), $k \in \mathbb{Z}^+$), where $k \geq n_1$, then the statement $S(k+1)$ is also true;

then $S(n)$ is true for all $n \geq n_0$.

4.2 The Division Algorithm: Prime Numbers

Definition 4.2. If $a, b \in \mathbb{Z}$ and $b \neq 0$, we say that b divides a, and we write $b|a$, if there is an integer n such that $a = bn$. When this occurs we say that b is a *divisor* of a, or a is a *multiple* of b.

- When $ab = 0$ for $a, b \in \mathbb{Z}$, then $a = 0$ or $b = 0$. We say that $\mathbb{Z}$ has no proper divisors of 0.
- This allows us to *cancel* as in $2x = 2y \Rightarrow x = y$, for $x, y \in \mathbb{Z}$, because $2x = 2y \Rightarrow 2(x-y) = 0 \Rightarrow 2 = 0$ or $x = y \Rightarrow x = y$ (Note that we did not multiply both sides by $\frac{1}{2}$ which is outside the system $\mathbb{Z}$).
- Whenever we divide by an integer a, we assume $a \neq 0$.

Theorem 4.3. For all $a, b, c \in \mathbb{Z}$

a) $1|a$ and $a|0$.

b) $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$.

c) $[(a|b) \wedge (b|c)] \Rightarrow a|c$.

d) $a|b \Rightarrow a|bx$ for all $x \in \mathbb{Z}$.

e) If $x = y + z$, for some $x, y, z \in \mathbb{Z}$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.

f) $[(a|b) \wedge (a|c)] \Rightarrow a|(bx+cy)$[5] for all $x, y \in \mathbb{Z}$.

g) For $1 \leq i \leq n$, let $c_i \in \mathbb{Z}$. If a divides each c_i, then $a|(c_1x_1 + c_2x_2 + \cdots + c_nx_n)$, where $x_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.

[5]This is called a *linear combination of* b, c.

Using this binary operation of integer division we find ourselves in the area of mathematics called *number theory*, which examines the properties of integers and other sets of numbers.

All $n \in \mathbb{Z}^+$ where $n > 1$ have at least 2 divisors, namely, 1 and n. Some integers, such as 2, 3, 5, 7, and 11 have exactly two divisors. These integers are called *primes*. All other integers (greater than 1 and not prime) are called *composite*.

Lemma 4.1. If $n \in \mathbb{Z}^+$ and n is composite, then there is a prime p such that $p|n$.
Proof. If not, let S be the set of all composite integers that have no prime divisor. If $S \neq \emptyset$, then by the Well-Ordering Principle, S has a least element m. But if m is composite, then $m = m_1 m_2$, where $m_1, m_2 \in \mathbb{Z}^+$ with $1 < m_1 < m$ and $1 < m_2 < m$. Since $m = m_1 m_2$, if now follows that $p|m$, and so $S = \emptyset$.

Theorem 4.4. (Euclid) There are infinitely many primes.
Proof. If not, let $p_1, p_2, \ldots, p_k$ be the finite list of all primes, and let $B = p_1 p_2 \cdots p_k + 1$. Since $B > p_i$ for all $1 \leq i \leq k$, B cannot be prime. Hence B is composite. So by Lemma 4.1 there is a prime p_j where $1 \leq j \leq k$ and $p_j|B$. Since $p_j|p_1 p_2 \cdots p_k + 1$ and $p_j|p_1 p_2 \cdots p_k$, it follows that $p_j|1$. (Contradiction) This contradiction arises from the assumption that there are only finitely many primes; hence there are infinitely many primes.

Theorem 4.5. *The Division Algorithm.* If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique $q, r \in \mathbb{Z}$ with $a = qb + r, 0 \leq r < b$.

4.2.1 Representation of Integers in Different Bases

Given an integer n written in base 10, to write it in base b, we can use the division algorithm. Keep applying the algorithm until the quotient is 0:

$$\begin{aligned} n &= q_0 b + r_0 \\ q_0 &= q_1 b + r_1 \\ &\cdots \\ q_{n-1} &= 0 \cdot b + r_n \end{aligned}$$

Then, $n = (r_n r_{n_1} \ldots r_1 r_0)_b$.

One commonly used base is 16, and it is called the *hexadecimal notation*. Because we only have 10 symbols in the standard base-10 system, we use the following 6 additional symbols:

10:	A (Alfa)	11:	B (Bravo)	12:	C (Charlie)
13:	D (Delta)	14:	E (Echo)	15:	F (Foxtrot)

One benefit of using the hexadecimal notation is that it is easy to switch with binary. Breaking a base-2 number into blocks of four bits, then converting each block of four bits to its base-16 representation will result in the hexadecimal notation of the same number. This is because $16 = 2^4$, and four bits can represent a single digit in hexadecimal. We replace each hexadecimal digit into four bits to go from base-16 to base-2.

4.3 The Greatest Common Divisor: The Euclidean Algorithm

Definition 4.3. For $a, b \in \mathbb{Z}$, a positive integer c is said to be a *common divisor of a and b* if $c|a$ and $c|b$.

Definition 4.4. Let $a, b \in \mathbb{Z}$, where either $a \neq 0$ or $b \neq 0$. Then $c \in \mathbb{Z}^+$ is called a *greatest common divisor* of a, b if

1. $c|a$ and $c|b$
2. for any common divisor d of a and b, we have $d|c$.

Theorem 4.6. For $a, b \in \mathbb{Z}^+$, there exists a unique $c \in \mathbb{Z}^+$ that is *the* greatest common divisor of a, b.

Proof. Given $a, b \in \mathbb{Z}^+$, let $S = \{as + bt | s, t \in \mathbb{Z}, as + bt > 0\}$. Since $S \neq \emptyset$, by the Well-Ordering Principle S has a least element c. We claim that c is a greatest common divisor of a, b.

Since $c \in S$, $c = ax + by$, for some $x, y \in \mathbb{Z}$. Consequently, if $d \in \mathbb{Z}$ and $d|a$ and $d|b$, $d|(ax + by)$, so $d|c$.

Now we show that $c|a$ and $c|b$. If $c \nmid a$, we can use the division algorithm to write $a = qc + r$, with $q, r \in \mathbb{Z}^+$ and $0 < r < c$. Then $r = a - qc = a - q(ax + by) = (1 - qx)a + (-qy)b$, so $r \in S$, contradicting the choice of c as the least element of S. Consequently, $c|a$ and by a similar argument, $c|b$.

Hence, all $a, b \in \mathbb{Z}^+$, the greatest common divisor of a, b exists, and it is unique.

Theorem 4.7. *Euclidean Algorithm.* Let $a, b \in \mathbb{Z}^+$. Set $r_0 = a$ and $r_1 = b$ and apply the division algorithm n times as follows:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\cdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n \end{aligned}$$

Then, r_n, the last nonzero remainder, equals $\gcd(a, b)$.

Proof. To verify that $r_n = \gcd(a, b)$, we establish the two conditions of Definition 4.4.

If $d|a$ and $d|b$ (where $a = r_0$ and $b = r_1$), then since $r_0 = q_1 r_1 + r_2$, it follows that $d|r_2$. Similarly, $[(d|r_i) \wedge (d|r_{i+1})] \Rightarrow d|r_{i+2}$, so we conclude that $d|r_n$ continuing down the division process. This verifies the second condition.

To verify the first condition, we go in reverse order. From the last equation, $r_n|r_{n-1}$, so $r_n|r_{n-2}$ since $r_{n-2} = q_{n-1} r_{n-1} + r_n$. Similarly, $[(r_n|r_{i+2}) \wedge (r_n|r_{i+1})] \Rightarrow r_n|r_i$, so continuing up through the equations, we get to $r_n|r_1$ and $r_n|r_0$.

Hence, $r_n = \gcd(a, b)$.

Theorem 4.8. If $a, b, c \in \mathbb{Z}^+$, the Diophantine equation $ax + by = c$ has an integer solution $x = x_0$, $y = y_0$ if and only if $\gcd(a, b)$ divides c.