Theorems and Definitions

1 Definitions

1.1 Sets and Logic

1. Logical Operator: A logical operator is a symbol that acts on a logical statement. The operators act as follows

		Negation	Disjunction	Conjunction	Implication
P	Q	$\neg$ P	P $\wedge$ Q	P $\vee$ Q	P $\implies$ Q
1	1	0	1	1	1
1	0	0	0	1	0
0	1	1	0	1	1
0	0	1	0	0	1

   A statement that is always true (i.e. P $\vee$ $\neg$P) is called a Tautology. A statement that is always false (i.e. P $\wedge$ $\neg$P) is called a contradiction.
   An implication P $\implies$ Q is made of two parts: the hypothesis (P) and the conclusion (Q).
   Additionally, statements can be quantified using the two quantifiers, the universal quantifier, for all ($\forall$) and the existential quantifier, there exists ($\exists$).

2. Set: A set is a collection of objects. The objects in a set are called elements.

3. Empty Set: The empty set, symbolized by $\emptyset$ is the set with no elements.

4. Subset: A set $\mathcal{A}$ is a subset of a set $\mathcal{B}$ (noted $\mathcal{A} \subset \mathcal{B}$) if for all $x \in \mathcal{A}$, $x \in \mathcal{B}$.

5. Power Set: The power set of a set $\mathcal{A}$ (noted $\mathcal{P}(\mathcal{A})$) is the set of all subsets of $\mathcal{A}$.

6. The Universal Set: The universal set, $\mathcal{U}$ is the set of which all sets are subsets.

7. Intersection: For sets $\mathcal{A}$ and $\mathcal{B}$, the intersection ($\mathcal{A} \cap \mathcal{B}$) is the set of elements in both $\mathcal{A}$ and $\mathcal{B}$.

$$\mathcal{A} \cap \mathcal{B} = \{x | x \in \mathcal{A} \wedge x \in \mathcal{B}\}.$$

   To say that $\mathcal{A}$ and $\mathcal{B}$ have a trivial intersection means that $\mathcal{A} \cap \mathcal{B} = \emptyset$. This is equivalent to saying $\mathcal{A}$ and $\mathcal{B}$ are disjoint.

8. Union: For sets $\mathcal{A}$ and $\mathcal{B}$, the union ($\mathcal{A} \cup \mathcal{B}$) is the set of elements in either $\mathcal{A}$ or $\mathcal{B}$.

$$\mathcal{A} \cup \mathcal{B} = \{x | x \in \mathcal{A} \vee x \in \mathcal{B}\}.$$

9. Set Difference: The set difference of a set $\mathcal{A}$ and a set $\mathcal{B}$ ($\mathcal{A} - \mathcal{B}$) is the set of all elements in $\mathcal{A}$ that are not in $\mathcal{B}$.

$$\mathcal{A} - \mathcal{B} = \{x | x \in \mathcal{A} \wedge x \notin \mathcal{B}\}.$$

   The complement of a set $\mathcal{A}$ in regards to $\mathcal{U}$ is $\mathcal{U} - \mathcal{A}$.

10. Cartesian Product: For sets $\mathcal{A}$ and $\mathcal{B}$, the cartesian product ($\mathcal{A} \times \mathcal{B}$) is defined to be the set of ordered pairs (a, b) such that $a \in \mathcal{A}$ and $b \in \mathcal{B}$.

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

11. Axiom: An axiom is a statement whose truth value is accepted without proof.
12. Theorem: A theorem is a mathematical statement whose truth value can be verified through proof.
13. Lemma: A Lemma is a mathematical result that is used to prove other results.
14. Corollary: A corollary is a mathematical result that follows from another result.

1.2 Number Theory

1. Division: To say that a divides b ($a \mid b$) implies that $\exists x \in \mathbb{Z}$ such that $b = ax$.
2. Relation: A relation $\mathcal{R}$ from $\mathcal{A}$ to $\mathcal{B}$ is a subset of $\mathcal{A} \times \mathcal{B}$. $\mathcal{A}$ is related to $\mathcal{B}$ ($a\mathcal{R}b$) if $(a, b) \in \mathcal{R}$ for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$. The domain of $\mathcal{R}$ is the set $\{x \mid (x, y) \in \mathcal{R}\}$. The range of $\mathcal{R}$ is the set $\{y \mid (x, y) \in \mathcal{R}\}$. If $\mathcal{R}$ has an inverse $\mathcal{R}^{-1}$, then it is $\{(y, x) \mid (x, y) \in \mathcal{R}\}$. A relation between two elements $a \in \mathcal{A}$ and $b \in \mathcal{B}$ is denoted by $a \sim b$.
3. Reflexive: A relation $\mathcal{R}$ is reflexive if $x\mathcal{R}x$ for all $x \in \mathcal{A}$.
4. Symmetric: A relation $\mathcal{R}$ is symmetric if $x\mathcal{R}y$ and $y\mathcal{R}x$ for all $x \in \mathcal{A}$ and $y \in \mathcal{B}$.
5. Transitive: A relation $\mathcal{R}$ is transitive if $x\mathcal{R}y$ and $y\mathcal{R}z$ implies $x\mathcal{R}z$ for all $x \in \mathcal{A}$, $y \in \mathcal{B}$, and $z \in \mathcal{C}$.
6. Equivalence Relation: An equivalence relation is a relation that is reflexive, symmetric, and transitive.
7. Equivalence Class: For a non-empty set $\mathcal{A}$ containing elements a and b, the equivalence class of a, noted $[a]$ is the set $\{b \mid b \sim a\}$.
8. Partition: A partition of a non-empty set $\mathcal{A}$ is the set of subsets where
   (a) The union of all sets in the partition of $\mathcal{A}$ is $\mathcal{A}$
   (b) The intersection of any two different sets in the partition of $\mathcal{A}$ is not equivalent to $\emptyset$.
9. Function: A function f from $\mathcal{A} \to \mathcal{B}$ is a relation from $\mathcal{A}$ to $\mathcal{B}$ that satisfies
   (a) $(a, b) \wedge (a, c) \in f \implies b = c$.
   (b) $\forall a \in \mathcal{A}, \exists b \in \mathcal{B}$ such that $(a, b) \in f$.
10. Image: The image of a function $f : \mathcal{A} \to \mathcal{B}$ is $\{f(a) \mid a \in \mathcal{A}\}$.
11. Inverse Image: For a function $f : \mathcal{A} \to \mathcal{B}$ and sets $\mathcal{B}$ and $\mathcal{D}$ where $\mathcal{D} \subset \mathcal{B}$, the inverse image of $\mathcal{D}$, $f^{-1}(\mathcal{D})$, is defined to be $\{a \in \mathcal{A} \mid f(a) \in \mathcal{D}\}$.
12. Injection: A function f is injective if $\forall (a, b) \in \mathcal{X},\ f(a) = f(b) \implies a = b$.
13. Surjection: A function f is surjective if $\forall y \in \mathcal{Y},\ \exists x \in \mathcal{X}$ such that $f(x) = y$.
14. Bijection: A function f is a bijection if it is an injection and a surjection.

2 Theorems and Important Ideas

1. Division Algorithm: Suppose $a, b \in \mathbb{Z}$ and assume $b > 0$. Then $\exists q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r \leq b$. Moreover, q and r are the only integers satisfying this property. The integer q is commonly called the quotient and r is commonly called the remainder.

   Proof: Let $\mathcal{S} = \{a - nb \mid n \in \mathbb{Z}\}$. We know that

   $$\lim_{n \to -\infty} (a - nb) \to +\infty,$$

   so $\mathcal{S}$ must contain at least one positive integer. Let r be the smallest element of $\mathcal{S}$ that is greater than zero, called the remainder. Then there is a $q \in \mathbb{Z}$ such that $r = a - qb \geq 0$, or $a = qb + r$ for $r \geq 0$. We have shown that this r exists.
   Assume $r \geq b$. Then $r - b \geq 0$, and we know $r = a - qb$, so $a - qb - b \geq 0$. Then $a - b(q+1) \in \mathcal{S}$ is greater than zero but less than r, which is a contradiction since r is the smallest positive integer in $\mathcal{S}$. Therefore $a = qr + b$ and $0 \leq r \leq b$.
   Assume $a = bq + r$ and $a = bg + h$ where $0 \leq r \leq b$ and $0 \leq h \leq g$.