Discrete Math Study Guide

Ziyad Rahman
zrahman3004@gmail.com

Contents

1 Logical Symbols and Deductive Reasoning

1.1 Variables and Statements

A **variable** is a symbol that stands in for some specific value, be it a person, number, etc.

A **statement** is a something that may evaluate to true or false. It is usually either in the form P if it does not depend on a variable or $P(x)$ if the statement's truth depends on what the input is.

1.2 Connective Symbols

1.3 Logical Laws

1.3.1 Associative Law

$$(P \wedge Q) \wedge R = P \wedge (Q \wedge R) \quad (1)$$
$$(P \vee Q) \vee R = P \vee (Q \vee R) \quad (2)$$

1.3.2 Communative Law

$$P \wedge Q = Q \wedge P \quad (3)$$
$$P \vee Q = Q \vee P \quad (4)$$

1.3.3 Distributive Law

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R) \quad (5)$$
$$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R) \quad (6)$$

1.3.4 Double Negation Law

$$\neg\neg P = P \quad (7)$$

1.3.5 De Morgan's Law

$$\neg(P \wedge Q) = (\neg P \vee \neg Q) \quad (8)$$
$$\neg(P \vee Q) = (\neg P \wedge \neg Q) \quad (9)$$

1.3.6 Idempotent Law

$$P \wedge P = P \quad (10)$$
$$P \vee P = P \quad (11)$$

1.3.7 Absorption Law

$$P \wedge (P \vee Q) = P \tag{12}$$
$$P \wedge (P \vee Q) = P \tag{13}$$

1.4 Truth Tables

Truth tables are are relative straight forward concept. The aim is to evaluate the truth of statement by breaking it down into its smallest parts, then seeing if the final statement is true or false based on the truth of the sub-statements. Here is a simple example,

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

1.5 Tautologies and Contradictions

1.6 The Conditional

1.6.1 Definition

The conditional can be thought of as an "if, then" statement. It primarily demonstrates some relationship between two statements. In symbols, it is represented as,

$$P \to Q$$

This statement can be read several ways in English:

1. P implies Q
2. P only if Q
3. P is a sufficient condition for Q
4. Q, if P
5. Q is a necessary condition for P

1.6.2 The Truth of a Conditional

We can demonstrate the truth of the conditional via a truth table.

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

To put the truth table into plain words, the conditional is true only if both Q is true or if P and Q are both false. In other words, the conditional is only false if only Q is false.

1.6.3 The Conditonal in Logical Connectives

We can write the conditional in terms of basic logical connectives. The definition of conditional in these terms is as follows.

$$P \to Q \quad \equiv \quad \neg P \vee Q \quad \equiv \quad P \wedge \neg Q$$

Note that the rightmost statement is the same as the middle statement, but De Morgan's Law was applied.

We can verify that these statements are equivalent via another truth table.

P	Q	$P \to Q$	$\neg P \vee Q$	$P \wedge \neg Q$
T	T	T	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

1.6.4 The Converse

The converse of a conditional is simply the conditional, but the statements have been swapped around.

$$P \to Q \quad \not\equiv \quad Q \to P$$

We could write a truth table to demonstrate that these statements are **NOT** equivalent, but we will use the definition of the conditional (the logical symbols version) to demonstrate intuitively that these are not the same.

$$\begin{aligned} P \to Q &\equiv \neg P \vee Q \\ Q \to P &\equiv \neg Q \vee P \qquad (14) \\ \neg P \vee Q &\not\equiv \neg Q \vee P \qquad (15) \end{aligned}$$

1.6.5 The Contrapositive

The contrapositive of a conditional is a negated version of the original statement. Unlike the converse of conditional, the contrapositive is equivalent to the original statement.

$$P \to Q \quad \equiv \quad \neg Q \to P$$

We could use a truth table to show that these statements are equivalent, but we can also use the logical forms of the conditionals achieve the same end.

$$\begin{aligned} P \to Q &\equiv \neg P \vee Q \\ \neg Q \to P &\equiv \neg\neg Q \vee \neg P \\ \neg P \vee Q &\equiv \neg\neg Q \vee P \end{aligned}$$

1.7 The Biconditional

1.7.1 Definition

The biconditional is often read as "if an only if". It can be written in terms of the conditional or logical connectors. It is written as follows.

$$P \leftrightarrow Q$$

In terms of the conditional,

$$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P) \tag{16}$$

The final definition is in terms of logical connectors.

$$P \leftrightarrow \equiv (\neg P \vee Q) \wedge (\neg Q \vee P) \tag{17}$$

Any statements that are equivalent to those above are valid definition of the biconditional.

1.7.2 The Truth of a Biconditional

We can determine the truth of a biconditional via a truth table.

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

As we can see, the biconditional only evaluates to true if (and only if) both statements involved are true.

1.8 Arguments

2 Quantifiers

2.1 Introducing Quantifiers

The Universe of Discourse: The set of all values that a variable can take on. It is often denoted as $\mathcal{U}$.

Quantifier: A symbol that denotes for which values in the Universe of Discourse that some statement is true for. There are two types.

1. **Universal Quantifier**: Denoted by $\forall$. It denotes that a statement is true for all values.
2. **Existential Quantifier**: Denoted by $\exists$. It denotes that a statement is true for some value.

Note: Quantifiers only apply to immediate statements.

$$\forall x(P(x) \land Q(x)) \quad \neq \quad \forall x P(x) \land \forall x Q(x)$$

2.1.1 Uniqueness

$!\exists$ is a special case of the existential quantifier. It denotes that there is only one value that satisfies the statement.

2.1.2 Idomatic and Mathematical English

Statements quantifiers may be translated into idiomatic or mathematical English. The difference between the two is that idiomatic english is a translation (totally different wording but same meaning) whereas mathematical english is a transliteration (where you translate every part directly).

There are no hard and fast rules about this, but generally, you would replace the quantifier directly with its definition and work from there.

For example, take the statement $\forall x \exists y(P(x) \to Q(y))$.

1. **Idiomatic English:** All x have some y.
2. **Mathematical English:** For all x, there exists a y, such that $P(x)$ implies $Q(y)$.

2.2 Bound and Free Variables

Bound Variable: A variable that is bound, or within the scope of, some quantifier related to it.
Free Variable: A variable that is not bound by any quantifier.
Example: In the statement,

$$\forall x P(x, y)$$

x is a bound variable, while y is a free variable.

2.3 Quantifier Negation

Quantifiers have some negation laws associated with them. They are fairly straightforward.

$$\neg\forall x P(x) \equiv \exists x \neg P(x) \tag{18}$$
$$\neg\exists x P(x) \equiv \forall x \neg P(x) \tag{19}$$

3 Set Theory

3.1 Defining Sets

Set: A collection of objects. ex. $\{0, 1, 2, 3\}$
Object: An element of a set. ex. 52.

3.1.1 Important Sets

There are a few very important important sets that we must know. They are as follow:

$$\begin{aligned}
\varnothing &= \{\}\text{; a set with no objects.} \\
\mathbb{N} &= \{x \mid x \text{ is a natural number}\} \\
\mathbb{Z} &= \{x \mid x \text{ is an integer}\} \\
\mathbb{R} &= \{x \mid x \text{ is a real number}\} \\
\mathbb{Q} &= \{x \mid x \text{ is a rational number of form } \frac{p}{q} \text{ where } p, q \in \mathbb{R} \text{ and } q \neq 0\} \\
\text{Truth Set} &= \{x \mid P(x)\}\text{; the set of all objects that makes the statement true}
\end{aligned}$$

3.2 Basic Set Operations

3.2.1 Intersection

The intersection of two sets is the set of elements in both sets.

$$A \cup B = \{x \mid x \in A \wedge x \in B\} \tag{20}$$

3.2.2 Union

The union of two sets is the set of all elements in the sets.

$$A \cap B = \{x \mid x \in A \vee x \in B\} \tag{21}$$

3.2.3 Difference

The difference of two sets is the set of elements in the first but not the second.

$$A \backslash B = \{x \mid x \in A \wedge x \notin B\} \tag{22}$$

3.2.4 Symmetric Difference

The symmetric difference of two sets is the set of all elements not in their intersection.

$$A \triangle B = \{x \mid (A \backslash B) \cup (B \backslash A)\} = \{x \mid (A \cup B) \backslash (A \cap B)\} \tag{23}$$

3.2.5 Subsets, Proper and Improper

An (improper) subset is when all elements in some set is contained in some other set.

$$A \subseteq B \quad = \quad \{x \mid \forall x (x \in A \rightarrow x \in B)\} \tag{24}$$

A proper subset is when all elements in some set are equal to all elements of another set.

$$A \subset B \quad = \quad \{x \mid \forall x (x \in A \leftrightarrow x \in B)\} \tag{25}$$

3.3 Families of Sets

Family of Sets: Any set that is a set of sets, often denoted as $\mathcal{F}$. For example,

$$\mathcal{F} = \{A, B, C\} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{5, 6, 7\}\}$$

3.3.1 Index Sets

Index Set: A set that indexes another set.

An index set does not need to be strictly consecutive integers. For example, both of the following sets are valid index sets.

$$\begin{aligned} I &= \{1, 2, 3\} \\ J &= \{3, 42, 54\} \end{aligned}$$

Indexed Set: A family of sets that has been indexed by an indexed set. It is often defined as the following.

$$\mathcal{A} \quad = \quad \{A_i \mid i \in I\} \tag{26}$$

3.3.2 The Power Set

Power Set: A set whose elements are all subsets of some other set.

$$\mathcal{P}(A) = \{S \mid S \subseteq A\} \tag{27}$$

Example:

$$\begin{aligned} A &= \{1, 2\} \\ \mathcal{P}(x) &= \{\{1\}, \{2\}, \{1, 2\}, \varnothing\} \end{aligned}$$

3.3.3 Operations on Families of Sets

Intersection of Sets: A set of all elements that are common to all the sets in the family.

$$\bigcap \mathcal{F} = \{x \mid \forall A \in \mathcal{F}(x \in A)\} \tag{28}$$

Another way to think about the intersection of sets is as follows.

$$A_1 \cap A_2 \cap ... \cap A_i$$

Union of Sets: A set of all elements that are in all the sets in the family.

$$\bigcup \mathcal{F} = \{x \mid \exists A \in \mathcal{F}(x \in A)\} \tag{29}$$

Another way to think about the intersection of sets is as follows.

$$A_1 \cup A_2 \cup ... \cup A_i$$

4 Proof Strategies

4.1 Theorems, Propositions, and Lemmas

Theorems, Propositions, or Lemma: If certain conditions called hypotheses, premises, or givens are true, then their conclusions are true. The difference between each of these is simply how important they are; theorems are the most important and lemmas are the least important.

Proof: Chain of mathematical statements, where each claim is fully justified using the hypotheses, logical axioms, something you have already proven, and basic arithmetic until a conclusion is reached.

All proofs have the following structure:

Theorem 4.1. *Assumptions and a statement to be proven, say $P \to Q$.*

Proof. A series of logical steps that lead to the conclusion. Thus, Q holds. Therefore, $P \to Q$. □

4.2 Proof Writing Basics

To prove a statement, you must prove that *all* instances are true, not just one. You must somehow show that for all inputs of the variable (within the bounds of our assumptions) to statement holds true. If there is even one instance where the statement evaluates to false, the statement false.

There is no algorithm for proving a statement. There are a few key proof strategies that can help guide your thinking, but ultimately it takes trial and error. Proof writing typically occur in two stages.

1. Scratch work: This is the trial and error stage where you try all the proof strategies. in this stage, you may make use of any logical symbols you need to.

2. Final proof: This is when you formally write your proof. You should keep symbols like quantifiers to a minimum, and write in plain English.

During the scratch work stage, it's often suggested to organize your work into a given and goal column. The given is everything you are assuming about the problem and the goal column is what you are actually trying to prove.

Example:

Lemma 4.2. *Suppose* $x \in \mathbb{R}$ *and* $x > 0$*. If* $x^2 < 1$*, then* $x < 1$*.*

Scratch work:

Given	Goal
$x \in \mathbb{R}$	$(x^2 < 1) \to (x < 1)$
$x > 0$	

4.3 General Proof Strategies

4.3.1 Direct Proofs

Direct proofs are the simplest form of proof. Often times, we will use other methods to make a statement easier to prove, so that we can use a direct proof on it.

Direct proofs will often take the following form.

Theorem 4.3. $P \to Q$

Proof. Assume that P is true. [Arguments using logical laws, definitions, and basic arithmetic]. □

4.3.2 Proof by Contrapositive

Proof by contrapositive takes that statement that needs to be proven, then applies the conditional contrapositive law to it. The idea is, if you can prove the contrapositive of the statement, you can prove the original statement because the contrapositive and the original statement are equivalent.

Contrapositive proofs will often take the following form.

Theorem 4.4. $P \to Q$

Proof. We will argue this theorem by using the contrapositive. Suppose $\neg Q$. [A direct proof on $\neg Q \to P$]. Thus, $\neg P$. Therefore, by the contrapositive law, $P \to Q$. □

4.3.3 Proof by Contradiction

A proof by contradiction requires you take all assumptions and prove the opposite of your conclusion. Then, you show that there must be some contradiction that arises from these assumptions.
Contradiction proofs usually take the following form.

Lemma 4.5. $P \to Q$

Proof. We will argue this lemma via proof by contradiction. Suppose P. Further, assume towards a contradiction that $\neg Q$. [Show how there is some contradiction that arises from these assumptions]. However, this proves a contradiction because [explain what the exact contradiction is]. Therefore, if P then Q. □

This type of proof is often useful for when the conclusion we are seeking is a negative statement (that is $\neg P$). Then you can just assume the statement (that is P) and just find a contradiction.

If you have a given in the form $P \to Q$, there are two rules we can apply:

1. *Modus Ponens*: If you know P and $P \to Q$ are true, then Q is true.
2. *Modus Tolen*: If you know $P \to Q$ is true but Q is false, then P must also be false.

4.3.4 For all Proofs

If you have a proof with the universal quantifier, you present an "arbitrary" variable that is bound to it.

Lemma 4.6. *For all* x, $P(x) \to Q(x)$.

Proof. Let x be arbitrary. [Proof of $P(x)$]. Since x was arbitrary, for all x, $P(x) \to Q(x)$. □

If you have a given that uses the universal quantifier, you can simply *universal instantiation*. Just introduce an arbitrary value such that that given is true.

4.3.5 There Exists Proofs

For proofs with the existence quantifier, you will find a value that satisfies the claim, then present it in the proof by saying let $x =$ that value.

Lemma 4.7. *There exists an x such that $P(x) \to Q$.*

Proof. Let $x =$ the value you found in your scratch work. [Proof of $P(x) \to Q(x)$]. Thus, there exists an $x =$ that value such that $P(x) \to Q(x)$. □

To use a given in the form of $\exists x P(x)$, we can use a strategy called *existential instantiation*. To do this, you introduce a variable x_0 such that $P(x_0)$ is true. Thus, you can assume $P(x_0)$ for your givens.

Lemma 4.8. *Suppose $P(x)$ is true for specific values. Then, show $P(x) \to Q(x)$.*

Proof. Suppose there exists x_0 such that $P(x_0)$ is true. [Proof of $P(x_0) \to Q(x_0)$]. □

4.3.6 There Exists a UNIQUE Proofs

To prove uniqueness, you must show that there exists a value to satisfy the claim, then show that there is only one value to satisfy it. You can split this into two parts. First, prove existence using the there existence proof strategies. Then, to show uniqueness you can do one of two things:

1. Assume two values satisfy the claim, then show that these values are in fact equal to each other. In logical symbols, we are proving the following.

$$\forall x \forall y (P(x) \wedge P(y) \to x = y)$$

2. Slightly more involved, but given the assumptions, prove that one value that can fulfill all necessary traits.

4.4 Proofs Involving Conjunctions and Biconditionals

4.4.1 Conjunction Proofs

Conjunction: A statement of the form $P \wedge Q$. For these proofs, you can use any of the proof strategies; however, you should do it in two parts: first prove P, then prove Q.

Lemma 4.9. $P \wedge Q$

Proof. We will prove this proof in two parts. First, we will prove P, then we will prove Q. [Proof of P]. [Proof of Q]. Having proven P and Q, we have completed this proof. □

4.4.2 Biconditional Proofs

To prove a biconditional, we can use the fact that,

$$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$$

Then, this becomes a conjunction problem, so we prove $P \rightarrow Q$, then prove $Q \rightarrow P$.
There is a "special" case for biconditional proofs. It hinges off the following definition.

$$P = Q \equiv (P \subset Q) \wedge (Q \subset P)$$

From here, we can again use conjunction. This case is called **double containment**. **Containment** is just showing that some set is a subset of another set. So, double containment is just showing two cases of subsets, specific that the first set is a subset of the second set and vice versa.

4.5 Proofs Involving Disjunctions

Disjunction: A statement in the form $P \vee Q$.

For a disjunction proof, prove the first case, then the second case. For a goal of $P \vee Q$, prove P then Q. For a given of that form, prove your goal first by only assuming P then only assuming Q.

5 Relations

5.1 Ordered Pairs and Cartesian Products

Ordered pairs are of the form (x, y) and hold possible values for each variable. As the name suggests, the order in which they are in matters, i.e. (x, y) is different from (y, x).

The **cartesian product** is the set of all ordered pairs such that the first element is in some set A and the second element is in another set B. More formally,

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

5.2 Relations

Suppose A and B are sets. A **relation** R from A to B is defined as,

$$R \subseteq A \times B.$$

There are a few ways to denote a relation. The most common is perhaps $(a, b) \in R$, but you may see other notation such as xRy as well.

Similar to functions, relations have a **domain** and **range**.

$$\begin{aligned} Dom(R) &= \{a \in A \mid \exists b \in B((a,b) \in R)\} \\ Ran(R) &= \{b \in B \mid \exists a \in A((a,b) \in R)\}. \end{aligned}$$

The **inverse** of R is defined as,

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

Last, we consider set composition. Suppose there are three sets A, B, C and R is a relation from A to B and S is a relation from B to C. We can define a composition of S and R as,

$$S \circ R = \{(a,c) \in A \times C \mid \exists b \in B((a,b) \in R \wedge (b,c) \in S)\}.$$

5.3 Equivalence Relations

5.3.1 A Primer

Equivalence relations are a special, very important subset of the cartesian product. Before explaining exactly what this set looks like, we must understand a few possible traits of a relation. Not all sets follow these characteristics, but relations that have the following constructions have special names. Thus, the three most important types.

$$\begin{aligned} \text{Reflexive} &= \forall x \in A((x,x) \in R) \\ \text{Symmetric} &= \forall x,y \in A((x,y) \in R \rightarrow (y,x) \in R) \\ \text{Transitive} &= \forall x,y,z \in A(((x,y),(y,z) \in R) \rightarrow (x,z) \in R). \end{aligned}$$

There is another definition we will cover for a closely related type of set. A **pairwise disjoint** set is one such that

$$\forall X, Y \in \mathcal{F}(X \neq Y \rightarrow X \cap Y = \varnothing).$$

5.3.2 Equivalence Relations and Classes

Equivalence relations are a subset of the cartesian product such that this set is reflexive, symmetric, and transitive.

Let R be an equivalence relation on a set A. Let $x \in A$. The **equivalence class** of x with respect to R is the set denoted by $[x]_R$ is defined by

$$[x]_R = \{y \in A \mid (x,y) \in R\}.$$

The set of all equivalence classes of A with respect to R is called A modulo R and is denoted A/R. That is,

$$A/R = \{[x]_R \mid x \in A\}.$$

5.3.3 Partition of Sets

Let A be a set and $\mathcal{F} \subseteq \mathcal{P}(A)$ (i.e. $\mathcal{F}$ is a subset of the subsets of A). Then, $\mathcal{F}$ is a partition of A if the following properties hold:

1. $\forall X \in \mathcal{F}, X \neq \varnothing$.
2. $\bigcup \mathcal{F} = A$.
3. $\mathcal{F}$ is pairwise disjoint.

5.3.4 The Fundamental Theorem of Equivalence Relations

There is a very important theorem related to equivalence relations and partitions. The theorems and related lemmas are written below. The proofs themselves are left as an excercise to the reader.

Lemma 5.1. *Suppose R is an equivalence relation on set A. Then, for all $x \in A$, $x \in [x]_R$.*

Lemma 5.2. *Suppose R is a relation on A. Then, for all $x \in A$ and $y \in A$, $y \in [x]_R$ if and only if $[y] = [x]$.*

Theorem 5.3. *Suppose R is an equivalence relation on a set A. Then, A/R is a partition of A.*

Lemma 5.4. *Suppose A is a set and $\mathcal{F}$ is a partition on A. Let,*

$$R = \bigcup_{X \in \mathcal{F}} (X \times X).$$

Lemma 5.5. *Suppose A is a set $\mathcal{F}$ is a partition on A. Let R be the equivalence relation determined by $\mathcal{F}$ (given in lemma 5.4). Suppose $X \in \mathcal{F}$ and $x \in X$. Then $[x]_R = X$.*

Theorem 5.6. *Suppose A is a set and $\mathcal{F}$ is partition of A. Then, there exists an equivalence relation R on A so that $A/R = \mathcal{F}$.*

Commentary. Use *lemma 5.1* and *lemma 5.2* to prove *theorem 5.3*. Use *lemma 5.4* and *lemma 5.5* to prove *theorem 5.6*.

6 Functions

6.1 Defining Functions

A **function** is another type of subset of the cartesian product. Like equivalence relations, a set is only considered a function if it meets certain criteria. The formal definition is as follows.

Let A and B be sets. A function from A to B is a relation F from A to B (so, $F \subseteq A \times B$), so that for all $a \in A$, there exists a unique element $b \in B$ so that $(a, b) \in F$. We can also write this in logical symbols as

$$\forall x \in A(\exists! y \in B((a, b) \in F)).$$

Notation. If F is a function from A to B, then we can write it as $F : A \to B$. If $a \in A$ and $(a, b) \in F$ for a unique $b \in B$, then you can denote the value of F at a as $F(a)$. You can also write this as the image of F at a or F of a.

6.1.1 Domain and Range

Let $F : A \to B$. Then,

$$\begin{aligned} Dom(F) &= A \\ Ran(F) &= \{F(a) \mid a \in A\} \end{aligned}$$

6.1.2 Composition

Let $f : A \to B$ and $g : B \to C$. Then, $f \subseteq A \times B$ and $g \subseteq B \times C$. So,

$$g \circ f \subseteq A \times C.$$

Which can be more explicitly defined by

$$g \circ f = \{(a, c) \mid \exists b \in B((a, b) \in f \wedge (b, c) \in g)\}.$$

We can also write the image of g of f on a by

$$(g \circ f)(a) = c = g(b) = g(f(a)).$$

6.2 Injective, Surjective, and Bijective

6.2.1 Injective or One-to-One

Let $f : A \to B$. f is **injective/one-to-one/1-1** if it can be defined by one of the following,

$$\begin{aligned} &\forall a_1, a_2 \in A(f(a_1) = f(a_2) \to a_1 = a_2) \\ &\forall a_1, a_2 \in A(a_1 \neq a_2 \to f(a_1) \neq f(a_2)). \end{aligned}$$

6.2.2 Surjective or Onto

Let $f : A \to B$. f is **surjective/onto** if it can be defined by one of the following.

$$\begin{aligned} &\forall b \in B \exists a \in A(f(a) = b) \\ &Ran(f) = B. \end{aligned}$$

6.2.3 Bijective

A function is **Bijective** if it is injective and surjective. In logical form:

$$(\forall a_1, a_2 \in A(f(a_1) = f(a_2) \rightarrow a_1 = a_2)) \wedge (\forall b \in B \exists a \in A(f(a) = b)),$$

or by using any of the equivalent equations defined above.

6.3 Inverse Functions

6.4 Closures

7 Mathematical Induction

7.1 Proof by Induction

7.2 Recursion

7.3 Strong Induction

7.4 Closures Part II

8 Number Theory

8.1 Greatest Common Divisor

8.2 Prime Factorization

8.3 Modular Arithmetic

8.4 Euler's Theorem

8.5 Public-Key Cryptography

9 Infinite Sets

9.1 Equinumerous Sets

9.2 Countable and Uncountable Sets

9.3 The Cantor-Schröder-Bernstein Theorem