Set theory review document

Mark Sullivan

December 5, 2018

Contents

1 Review for Test 1

1.1 Dictionary of terms

Definition 1.1 *A set is a well-defined collection of elements that does not contain itself as an element.*

Definition 1.2 *The empty set is the set $\varnothing$ containing no elements.*

Universal quantifier: $\forall$, “for all,” “for every”
Existential quantifier: $\exists$, “there exists”

Definition 1.3 *Let X be a set. The cardinality of X is the amount of elements of X.*

Notation We often denote the cardinality of X by $|X|$.

Definition 1.4 *Let A and B be sets. We say that A is a subset of B, denoted $A \subseteq B$ or $A \subset B$, provided that $\forall\, x \in A$, $x \in B$.*

Definition 1.5 *Let A and B be sets. We say that A and B are equal, denoted $A = B$, provided that $A \subseteq B$ and $B \subseteq A$.*

Definition 1.6 *Let A and B be sets. We say that A is a proper subset of B provided that $A \subseteq B$ and $A \neq B$.*

Notation We denote the statement “A is a proper subset of B” by “$A \subsetneq B$.”

Definition 1.7 *Let A and B be sets. The union of A and B is the set*

$$A \cup B = \left\{ x \middle| x \in A \text{ or } x \in B \right\}. \tag{1}$$

Definition 1.8 *Let A and B be sets. The intersection of A and B is the set*

$$A \cap B = \left\{ x \middle| x \in A \text{ and } x \in B \right\}. \tag{2}$$

Definition 1.9 *Let A and B be sets. We say that A and B are disjoint provided that $A \cap B = \varnothing$.*

Definition 1.10 *Let A and B be sets. The complement of B in A is the set*

$$A - B = \left\{ x \in A \middle| x \notin B \right\} \tag{3}$$

Notation $A - B$ is also denoted $A \setminus B$.

Definition 1.11 *Let A be a set. The power set of A is the set*

$$\mathcal{P}(A) = \left\{ S \middle| S \subseteq A \right\}. \tag{4}$$

Notation $\mathcal{P}(A)$ is also denoted 2^A.

Definition 1.12 *Let x and y be mathematical objects. The ordered pair of x and y is the set $(x, y) = \{\{x\}, \{x, y\}\}$.*

Definition 1.13 *Let A and B be sets. The Cartesian product of A and B is the set*

$$A \times B = \left\{ (x, y) \middle| x \in A \text{ and } y \in B \right\}. \tag{5}$$

Definition 1.14 *Let X and Y be sets. A graph of a function from X to Y is a subset $f \subseteq X \times Y$ satisfying the following conditions.*
(i) $\forall\, x \in X$, $\exists\, y \in Y$ such that $(x, y) \in f$.
(ii) Given $x \in X$ and $y_1, y_2 \in Y$, if $(x, y_1) \in f$ and $(x, y_2) \in f$, then $y_1 = y_2$.

Definition 1.15 *Let X and Y be sets. A function or map from X to Y is an ordered triple (X, Y, f), where f is the graph of a function from X to Y.*

Notation
(1) We often write the statement "(X, Y, f) is a function" as "$f : X \to Y$ is a function."
(2) We often write the statement "$(x, y) \in f$" as "$f(x) = y$."

Definition 1.16 *Let $f : X \to Y$ be a function. The domain of f is the set X.*

Definition 1.17 *Let $f : X \to Y$ be a function. The codomain of f is the set Y.*

Definition 1.18 *Let X, Y and Z be sets. Given some functions $f : X \to Y$ and $g : Y \to Z$, the composition of g with f is the function $g \circ f : X \to Z$ defined via the relationship $g \circ f\,(x) = g\,(f\,(x))$.*

Definition 1.19 *Let $f : X \to Y$ be a function. Given $A \subseteq X$, the direct image of A under f is the set*

$$f(A) = \left\{ f(a) \middle| a \in A \right\}. \tag{6}$$

Definition 1.20 *Let $f : X \to Y$ be a function. The range or image of f is the direct image $f(X)$.*

Definition 1.21 *Let $f : X \to Y$ be a function. Given $B \subseteq Y$, the inverse image of B under f is the set*

$$f^{-1}(B) = \left\{ x \in X \middle| f(x) \in B \right\}. \tag{7}$$

1.2 Things you should know for the test

1. **ALL** of the definitions. If you do not know the definition of a term used in a problem, then it will be impossible for you to make any progress toward solving it!

2. Given a statement, you should be able to produce the negation.

3. Given an "if...then" statement, you should be able to produce the converse and contrapositive of the statement.

4. You should be able to prove that one set is a subset of another. To show that $A \subseteq B$, begin with the sentence "Let $x_0 \in A$ be arbitrary." The rest of the proof will involve showing that $x_0 \in B$.

5. You should be able to prove that two sets are equal to each other. To show that $A = B$, you need to show that $A \subseteq B$ and that $B \subseteq A$.

6. You should be able to prove "if...then" statements. To prove $p \Rightarrow q$, begin with the sentence "Assume p." The rest of the proof will involve showing q.

7. You should be able to prove "if and only if" statements. To prove $p \Leftrightarrow q$, you need to prove that $p \Rightarrow q$ and $q \Rightarrow p$.

8. You should be able to prove that a set is empty. The easiest way to prove that $A = \varnothing$ is to proceed by contradiction. The first sentence of such a proof would be "Assume, with the expectation of a contradiction, that $A \neq \varnothing$." The rest of the proof will involve showing that this cannot be true.

9. You should be able to work with sets and prove things about them, including operations on sets, such as union, intersection, and complement.

10. You should be able to work with power sets.

11. You should be able to work with Cartesian products.

12. You should be able to determine whether a given subset of $X \times Y$ is the graph of a function from X to Y.

13. Given finite sets X and Y, you should be able to produce all of the functions from X to Y.

14. Given a function $f : X \to Y$ and a subset $A \subseteq X$ of the domain, you should be able to describe the direct image $f(A)$.

15. Given a function $f : X \to Y$ and a subset $B \subseteq X$ of the codomain, you should be able to describe the inverse image $f^{-1}(B)$.

16. You should be able to do **ALL** of the homework problems.

1.3 Sample problems

In order to be sure that you possess the requisite skills, you should be able to prove all of the following theorems.

Theorem 1.22 *Given sets A and B, $A \cup B \subseteq A$ if and only if $B \subseteq A$.*

Theorem 1.23 *Given sets A and B,*

$$(A \setminus B) \cap (B \setminus A) = \varnothing. \tag{8}$$

Theorem 1.24 *Let X be a set. Given subsets $A, B \subseteq X$, $A \subseteq B$ if and only if $X \setminus B \subseteq X \setminus A$.*

Theorem 1.25 *Given sets A, B and C,*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{9}$$

and

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \,. \tag{10}$$

Theorem 1.26 *(de Morgan's laws for sets) Let X be a set. Given $A, B \subseteq X$,*

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \tag{11}$$

and

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B) \,. \tag{12}$$

Theorem 1.27 *(Fundamental property of ordered pairs) Given mathematical objects x, y, a, and b, $(x, y) = (a, b)$ if and only if $x = a$ and $y = b$.*

Theorem 1.28 *If A and B are non-empty sets, then $A \times B = B \times A$ if and only if $A = B$.*

Theorem 1.29 *Given sets A, B and C,*

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \tag{13}$$

and

$$A \times (B \cap C) = (A \times B) \cap (A \times C)\,. \tag{14}$$

Theorem 1.30 *Let $f : X \to Y$ be a function. Given $A \subseteq X$, $A \subseteq f^{-1}(f(A))$.*

Theorem 1.31 *Let $f : X \to Y$ be a function. Given $B \subseteq Y$, $f(f^{-1}(B)) \subseteq B$.*

Theorem 1.32 *Let $f : X \to Y$ be a function. Given $B \subseteq Y$, $B = f(f^{-1}(B))$ if and only if $B \subseteq f(X)$.*

Theorem 1.33 *Let $f : X \to Y$ be a function. Given subsets $A_1, A_2 \subseteq X$,*

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2) \tag{15}$$

and

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)\,. \tag{16}$$

Theorem 1.34 *Let $f : X \to Y$ be a function. Given subsets $B_1, B_2 \subseteq Y$,*

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2) \tag{17}$$

and

$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)\,. \tag{18}$$

1.4 Solutions to sample problems

Proof of Theorem 1.22 ($\Rightarrow$) Assume that $A \cup B \subseteq A$. Let $x_0 \in B$. In that case, $x_0 \in A$ or $x_0 \in B$. We deduce that $x_0 \in A \cup B = A$.

($\Leftarrow$) Assume that $B \subseteq A$. Let $x_0 \in A \cup B$. In that case, $x_0 \in A$ or $x_0 \in B$. Yet if $x_0 \in B$, then $x_0 \in A$, since $B \subseteq A$. Either way, $x_0 \in A$. □

Proof of Theorem 1.23 Assume, with the expectation of a contradiction, that $(A \setminus B) \cap (B \setminus A) \neq \varnothing$. This means that $\exists\, x_0 \in (A \setminus B) \cap (B \setminus A)$. In that case, $x_0 \in A \setminus B$ and $x_0 \in B \setminus A$. In particular, we deduce that $x_0 \in A$ and $x_0 \notin A$. This contradiction leads us to conclude that our assumption that $(A \setminus B) \cap (B \setminus A) \neq \varnothing$ is false; $(A \setminus B) \cap (B \setminus A) = \varnothing$. □

Proof of Theorem 1.24 ($\Rightarrow$) Assume that $A \subseteq B$. Let $x_0 \in X \setminus B$. In that case, $x_0 \notin B$. By assumption, then, $x_0 \notin A$ (for if $x_0 \in A$, then $x_0 \in B$, since $A \subseteq B$.) Therefore, $x_0 \in X \setminus A$.

($\Leftarrow$) Assume that $X \setminus B \subseteq X \setminus A$. Let $x_0 \in A$. In that case, $x_0 \notin X \setminus A$. By assumption, then, $x_0 \notin X \setminus B$. Thus, $x_0 \in B$. □

Proof of Theorem 1.25 (i) ($\subseteq$) Let $x_0 \in A \cap (B \cup C)$. In that case, $x_0 \in A$ and $x_0 \in B \cup C$. Therefore, $x_0 \in A$, and either $x_0 \in B$ or $x_0 \in C$. If $x_0 \in B$, then $x_0 \in A \cap B$. If $x_0 \in C$, then $x_0 \in A \cap C$. Either way, $x_0 \in (A \cap B) \cup (A \cap C)$.

($\supseteq$) Let $x_0 \in (A \cap B) \cup (A \cap C)$. In that case, $x_0 \in A \cap B$ or $x_0 \in A \cap C$. Thus, $x_0 \in A$, and either $x_0 \in B$ or $x_0 \in C$. Ergo, $x_0 \in A$ and $x_0 \in B \cup C$, so $x_0 \in A \cap (B \cup C)$.

(ii) ($\subseteq$) Let $x_0 \in A \cup (B \cap C)$. In that case, $x_0 \in A$ or $x_0 \in B \cap C$. Thus, either $x_0 \in A$ or $x_0 \in B$ and $x_0 \in C$. Either way, $x_0 \in A \cup B$ and $x_0 \in A \cup C$. Thus, $x_0 \in (A \cup B) \cap (A \cup C)$.

($\supseteq$) Let $x_0 \in (A \cup B) \cap (A \cup C)$. In that case, $x_0 \in A \cup B$ and $x_0 \in A \cup C$. Therefore, $x_0 \in A$ or $x_0 \in B$, and $x_0 \in A$ or $x_0 \in C$. If $x_0 \notin A$, then $x_0 \in B$ and $x_0 \in C$. Thus, $x_0 \in A$ or $x_0 \in B \cap C$. We deduce that $x_0 \in A \cup (B \cap C)$. □

Proof of Theorem 1.26 (i) $(\subseteq)$ Let $x_0 \in X \setminus (A \cup B)$. In that case, $x_0 \in X$ and $x_0 \notin A \cup B$. We deduce that $x_0 \notin A$ and $x_0 \notin B$. Ergo, $x_0 \in X \setminus A$ and $x_0 \in X \setminus B$. Thus, $x_0 \in (X \setminus A) \cap (X \setminus B)$.

$(\supseteq)$ Let $x_0 \in (X \setminus A) \cap (X \setminus B)$. In that case, $x_0 \in X \setminus A$ and $x_0 \in X \setminus B$. Therefore, $x_0 \in X$, and $x_0 \notin A$ and $x_0 \notin B$. Thus, $x_0 \notin A \cup B$. We deduce that $x_0 \in X \setminus (A \cup B)$.

(ii) $(\subseteq)$ Let $x_0 \in X \setminus (A \cap B)$. In that case, $x_0 \in X$ and $x_0 \notin A \cap B$. We deduce that $x_0 \notin A$ or $x_0 \notin B$. Thus, $x_0 \in X \setminus A$ or $x_0 \in X \setminus B$. This implies that $x_0 \in (X \setminus A) \cup (X \setminus B)$.

$(\supseteq)$ Let $x_0 \in (X \setminus A) \cup (X \setminus B)$. This means that $x_0 \in X \setminus A$ or $x_0 \in X \setminus B$. Either way, $x_0 \in X$. At the same time, $x_0 \notin A$ or $x_0 \notin B$, so $x_0 \notin A \cap B$. Thus, $x_0 \in X \setminus (A \cap B)$. □

Proof of Theorem 1.27 $(\Rightarrow)$ Let $(x, y) = (a, b)$. In that case,

$$\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}. \tag{19}$$

We consider two cases: either $x = y$ or $x \neq y$.

Consider the case that $x = y$. Now

$$\{\{x\}\} = \{\{a\}, \{a, b\}\}. \tag{20}$$

We deduce that $\{x\} = \{a\}$ and $\{x\} = \{a, b\}$. In particular, $x = a$. Further, we deduce that $\{a\} = \{x\} = \{a, b\}$, and so $b = a = x = y$.

Consider the case that $x \neq y$. We know that $\{x\} \in \{\{a\}, \{a, b\}\}$. Therefore, $\{x\} = \{a\}$ or $\{x\} = \{a, b\}$. Ergo, $x = a$ or $x = b$. However, if $x = b$, then $\{b\} \in \{\{a\}, \{a, b\}\}$, which would mean that $\{b\} = \{a\}$ or $\{b\} = \{a, b\}$. Either way, we would have that $b = a$. To summarize: we have that either $x = a$ or $x = b = a$.

As for y, we know that $\{x, y\} \in \{\{a\}, \{a, b\}\}$. This means that $\{x, y\} = \{a\}$ or $\{x, y\} = \{a, b\}$. However, $x = a$, so we can write this as $\{x, y\} = \{x\}$ or $\{x, y\} = \{x, b\}$. The first case implies that $x = y$, contrary to our assumption in this case. Therefore, $\{x, y\} = \{x, b\}$. Ergo, $y \in \{x, b\}$, which means that either

$y = x$ or $y = b$. Since $y \neq x$ in this case, we have that $y = b$.

($\Leftarrow$) Assume that $x = a$ and $y = b$. In that case,

$$(x, y) = \{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\} = (a, b)\,. \tag{21}$$

□

Proof of Theorem 1.28 ($\Rightarrow$) Assume that $A \times B = B \times A$. Let $x_0 \in A$. Since $B \neq \varnothing$, we can say that $\exists\, y \in B$. Thus, $(x_0, y) \in A \times B = B \times A$. We deduce that $x_0 \in B$. This shows that $A \subseteq B$. Similar arguments show that $B \subseteq A$, and so $A = B$.

($\Leftarrow$) Assume that $A = B$. In that case, $A \times B = A \times A = B \times A$. □

Proof of Theorem 1.29 (i) ($\subseteq$) Let $(x_0, y_0) \in A \times (B \cup C)$. In that case, $x_0 \in A$ and $y_0 \in B \cup C$. Thus, $x_0 \in A$, and either $y_0 \in B$ or $y_0 \in C$. We deduce that $(x_0, y_0) \in A \times B$ or $(x_0, y_0) \in A \times C$. Either way, $(x_0, y_0) \in (A \times B) \cup (A \times C)$.

($\supseteq$) Let $(x_0, y_0) \in (A \times B) \cup (A \times C)$. In that case, $(x_0, y_0) \in A \times B$ or $(x_0, y_0) \in A \times C$. We deduce that $x_0 \in A$ and $y_0 \in B$, or $x_0 \in A$ and $y_0 \in C$. Either way, $x_0 \in A$. At the same time, $y_0 \in B \cup C$. Thus, $(x_0, y_0) \in A \times (B \cup C)$.

(ii) ($\subseteq$) Let $(x_0, y_0) \in A \times (B \cap C)$. In that case, $x_0 \in A$ and $y_0 \in B \cap C$. Thus, $x_0 \in A$, $y_0 \in B$, and $y_0 \in C$. We deduce that $(x_0, y_0) \in A \times B$ and $(x_0, y_0) \in B \times C$. Therefore, $(x_0, y_0) \in (A \times B) \cap (A \times C)$.

($\supseteq$) Let $(x_0, y_0) \in (A \times B) \cap (A \times C)$. In that case, $(x_0, y_0) \in A \times B$ and $(x_0, y_0) \in A \times C$. We deduce that $x_0 \in A$, $y_0 \in B$, and $y_0 \in C$. In particular, $y_0 \in B \cap C$. Therefore, $(x_0, y_0) \in A \times (B \cap C)$. □

Proof of Theorem 1.30 Let $x_0 \in A$. In that case, $f\,(x_0) \in f(A)$. Therefore, $x_0 \in f^{-1}\,(f\,(A))$. □

Proof of Theorem 1.31 Let $y_0 \in f\,(f^{-1}\,(B))$. In that case, $\exists\, x_0 \in f^{-1}\,(B)$ such that $y_0 = f\,(x_0)$. However, this means that $y_0 = f\,(x_0) \in B$. □

Proof of Theorem 1.32 $(\Rightarrow)$ Assume that $B = f\left(f^{-1}(B)\right)$. Let $y_0 \in B$. By assumption, $y_0 \in f\left(f^{-1}(B)\right)$. We deduce that $\exists\, x_0 \in f^{-1}(B)$ such that $y_0 = f(x_0)$. Therefore, $y_0 = f(x_0) \in f(X)$.

$(\Leftarrow)$ Assume that $B \subseteq f(X)$.

$(\subseteq)$ Let $y_0 \in B$. By assumption, $\exists\, x_0 \in X$ such that $y_0 = f(x_0)$. However, this means that $x_0 \in f^{-1}(B)$. Thus, $y_0 = f(x_0) \in f\left(f^{-1}(B)\right)$.

$(\supseteq)$ Theorem 1.31 indicates that $f\left(f^{-1}(B)\right) \subseteq B$. $\square$

Proof of Theorem 1.33 (i) $(\subseteq)$ Let $y_0 \in f(A_1 \cup A_2)$. In that case, $y_0 = f(x_0)$ for some $x_0 \in A_1 \cup A_2$. We note that $x_0 \in A_1$ or $x_0 \in A_2$. Thus, $f(x_0) \in f(A_1)$ or $f(x_0) \in f(A_2)$. We deduce that $y_0 = f(x_0) \in f(A_1) \cup f(A_2)$.

$(\supseteq)$ Let $y_0 \in f(A_1) \cup f(A_2)$. In that case, $y_0 \in f(A_1)$ or $y_0 \in f(A_2)$. We deduce that $y_0 = f(x_0)$ for some $x_0 \in A_1$ or $y_0 = f(x_0)$ for some $x_0 \in A_2$. In other words, $\exists\, x_0 \in A_1 \cup A_2$ such that $y_0 = f(x_0)$. Thus, $y_0 = f(x_0) \in f(A_1 \cup A_2)$.

(ii) Let $y_0 \in f(A_1 \cap A_2)$. In that case, $y_0 = f(x_0)$ for some $x_0 \in A_1 \cap A_2$. We deduce that $x_0 \in A_1$ and $x_0 \in A_2$, so $f(x_0) \in f(A_1)$ and $f(x_0) \in f(A_2)$. Ergo, $y_0 = f(x_0) \in f(A_1) \cap f(A_2)$. $\square$

Proof of Theorem 1.34 (i) $(\subseteq)$ Let $x_0 \in f^{-1}(B_1 \cup B_2)$. In that case, we know that $f(x_0) \in B_1 \cup B_2$. Therefore, $f(x_0) \in B_1$ or $f(x_0) \in B_2$. This means that $x_0 \in f^{-1}(B_1)$ or $x_0 \in f^{-1}(B_2)$. Ergo, $x_0 \in f^{-1}(B_1) \cup f^{-1}(B_2)$.

$(\supseteq)$ Let $x_0 \in f^{-1}(B_1) \cup f^{-1}(B_2)$. This means that either $x_0 \in f^{-1}(B_1)$ or $x_0 \in f^{-1}(B_2)$. Thus, $f(x_0) \in B_1$ or $f(x_0) \in B_2$. Ergo, $f(x_0) \in B_1 \cup B_2$, and so $x_0 \in f^{-1}(B_1 \cup B_2)$.

(ii) $(\subseteq)$ Let $x_0 \in f^{-1}(B_1 \cap B_2)$. In that case, $f(x_0) \in B_1 \cap B_2$. This means that $f(x_0) \in B_1$ and $f(x_0) \in B_2$. Thus, $x_0 \in f^{-1}(B_1)$ and $x_0 \in f^{-1}(B_2)$. We deduce that $x_0 \in f^{-1}(B_1) \cap f^{-1}(B_2)$.

$(\supseteq)$ Let $x_0 \in f^{-1}(B_1) \cap f^{-1}(B_2)$. Now $x_0 \in f^{-1}(B_1)$ and $x_0 \in f^{-1}(B_2)$. We deduce that $f(x_0) \in B_1$ and $f(x_0) \in B_2$. Therefore, $f(x_0) \in B_1 \cap B_2$. This implies that $x_0 \in f^{-1}(B_1 \cap B_2)$. $\square$

2 Review for Test 2

2.1 Dictionary of terms

Definition 2.1 *Let $f_1 : X \to Y$ and $f_2 : X \to Y$ be functions. We say that f_1 and f_2 are equal functions, denoted $f_1 = f_2$, provided that $\forall\, x \in X$, $f_1(x) = f_2(x)$.*

Definition 2.2 *Let X be a set. The identity function defined on X is the function $\mathrm{id}_X : X \to X$ such that $\forall\, x \in X$, $\mathrm{id}_X(x) = x$.*

Definition 2.3 *Let $f : X \to Y$ be a function. Given $g : Y \to X$, we say that g is an inverse function of f provided that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.*

Notation The inverse function of f is denoted f^{-1}.

Definition 2.4 *Let $f : X \to Y$ be a function. We say that f is an invertible function provided that there exists an inverse function f^{-1} of f.*

Definition 2.5 *Let $f : X \to Y$ be a function. We say that f is injective, or one-to-one, provided that $\forall\, x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.*

Definition 2.6 *Let $f : X \to Y$ be a function. We say that f is surjective, or onto, provided that $\forall\, y \in Y$, $\exists\, x \in X$ such that $f(x) = y$.*

Definition 2.7 *Let $f : X \to Y$ be a function. We say that f is bijective, or that f is a bijection, provided that f is both injective and surjective.*

Definition 2.8 *One is the set $1 = \{\varnothing\}$.*

Definition 2.9 *Let A be a set. The successor of A is the set $A' = A \cup \{A\}$.*

Definition 2.10 *The set of natural numbers is the set $\mathbb{N}$ satisfying the following conditions.*
(i) $1 \in \mathbb{N}$.
(ii) $\forall\, n \in \mathbb{N}$, $n' \in \mathbb{N}$.
(iii) If X is any set such that $1 \in X$ and $\forall\, n \in X$, $n' \in X$, then $\mathbb{N} \subseteq X$.

The following are Peano's axioms of the natural numbers.

Definition 2.11 *The following statements are true.*

(i) 1 *is a natural number.*

(ii) For each natural number n*, there exists a unique successor,* n'*.*

(iii) No successor of any natural number is equal to 1*.*

(iv) If m *and* n *are natural numbers and* $m \neq n$*, then* $m' \neq n'$*.*

(v) (Mathematical induction) For each natural number n*, let* $P(n)$ *be a statement. If* $P(1)$ *is true and for every natural number* k*,* $P(k)$ *implies* $P(k')$*, then* $P(n)$ *is true for every natural number* n*.*

Definition 2.12 *The addition of natural numbers is the function* $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *satisfying the following conditions.*

(i) $\forall\, n \in \mathbb{N}$*,* $n + 1 = n'$*.*

(ii) $\forall\, m, n \in \mathbb{N}$*,* $m + n' = (m + n)'$*.*

Definition 2.13 *Let* $m, n \in \mathbb{N}$*. We say that* m *is less than* n*, denoted* $m < n$*, provided that* $\exists\, k \in \mathbb{N}$ *such that* $n = m + k$*.*

Definition 2.14 *Let* $m, n \in \mathbb{N}$*. We say that* m *is less than or equal to* n*, denoted* $m \leq n$*, provided that either* $m < n$ *or* $m = n$*.*

Definition 2.15 *Let* $m, n \in \mathbb{N}$*. If* $m < n$*, then* m *minus* n *is the natural number* $k \in \mathbb{N}$ *such that* $n = m + k$*.*

Notation We denoted m minus n by "$m - n$."

Definition 2.16 *Let* X *be a set. We say that* X *is a well-ordered set provided that* $\forall\, S \subseteq X$*,* $\exists\, t \in S$ *such that* $\forall\, s \in S$*,* $t \leq s$*.*

Definition 2.17 *Define* $0 = \varnothing$*. the set of integers is the set*

$$\mathbb{Z} = (\{0, 1\} \times \mathbb{N}) \cup \{(0, 0)\}\,. \tag{22}$$

Definition 2.18 *The absolute value function is a function* $|| : \mathbb{Z} \to \mathbb{Z}$ *defined via the relationship* $\big|\,(s, n)\,\big| = (0, n)$*.*

Notation
(i) We denote the integer $(0, 0)$ by "0."
(ii) Given $n \in \mathbb{N}$, we denote the integer $(0, n)$ by "n."
(iii) Given $n \in \mathbb{N}$, we denote the integer $(1, n)$ by "$-n$."

Definition 2.19 *The multiplication of integers is the function $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ satisfying the following conditions.*
(i) $\forall\ n \in \mathbb{Z}$, $1 \cdot n = n$.
(ii) $\forall\ a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Definition 2.20 *Let $m, n \in \mathbb{Z}$. We say that m is less than n, denoted $m < n$, provided that $n - m \in \mathbb{N}$.*

Definition 2.21 *Let $x \in \mathbb{Z}$. The exponential function with base x is the function $f_x : \mathbb{N} \to \mathbb{Z}$ satisfying the following conditions.*
(i) $f_x(1) = x$.
(ii) $\forall\ n \in \mathbb{N}$, $f_x\left(n + 1\right) = f_x\left(n\right) x$.

Notation Given $n \in \mathbb{N}$, we denote the value of the exponential function with base x at the argument n by "x^n."

Definition 2.22 *Let X be a nonempty set. A[n] [infinite] sequence in X is a function $s : \mathbb{N} \to X$.*

Notation
(i) We denote the sequence $s : \mathbb{N} \to X$ by "(s_n)," "$(s_n)_{n=1}^{\infty}$," or "$(s_n)_{n\in\mathbb{N}}$."
(ii) Given a sequence $s : \mathbb{N} \to X$ and $n \in \mathbb{N}$, we denote $s(n)$ by "s_n."

Definition 2.23 *Let X be a set, and let $(s_n)_{n\in\mathbb{N}}$ be a sequence in X. We say that (s_n) is a recursive sequence provided that $\exists\ m \in \mathbb{N}$ such that $\forall\ n \in \mathbb{N}$, if $m \leq n$, then $s_{n+1} = c_n s_n + c_{n-1} s_{n-1} + ... + c_k s_k$ for some $k \leq n$.*

Definition 2.24 *Let $m, n \in \mathbb{Z}$. We say that m divides n, that m is a factor of n, that m is a divisor of n, that n is divisible by m, or that n is a multiple of m provided that $\exists\ q \in \mathbb{Z}$ such that $n = mq$.*

Notation We denote the statement “m divides n” by “$m|n$.”

Definition 2.25 *Let $p \in \mathbb{Z}$. We say that p is a prime number provided that $\forall\, m \in \mathbb{Z}$, if $m|p$, then $m = \pm 1$ or $m = \pm p$.*

Definition 2.26 *Let $n \in \mathbb{Z}$. A prime factorization of n is a finite set $\{p_1, p_2, ..., p_k\}$ of prime numbers such that $n = p_1 p_2 ... p_k$.*

Definition 2.27 *Let $n \in \mathbb{Z}$. We say that n is a composite number provided that n is not prime and $n \neq 1$.*

Definition 2.28 *Given $a, b, n \in \mathbb{Z}$ such that $n \neq 0$, we say that a and b are congruent modulo n provided that $n|a - b$.*

Notation We denote “a and b are congruent modulo n” by “$a \equiv b \pmod{n}$” or “$a = b \bmod n$.”

Definition 2.29 *Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. An integral quotient of a by b is an integer $q \in \mathbb{Z}$ such that $a = qb + r$ for some integer $r \in \mathbb{Z}$ such that $0 \leq r < |b|$.*

Definition 2.30 *Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. A remainder when a is divided by b is an integer $r \in \mathbb{Z}$ such that $0 \leq r < |b|$ and $a = qb + r$ for some integer $q \in \mathbb{Z}$.*

2.2 Things you should know for the test

1. **ALL OF THE DEFINITIONS.**

2. You should know how to prove that two functions are equal or not equal.

3. You should know how to prove that two functions are inverses of each other.

4. You should be able to recognize and prove whether a given function is injective and/or surjective or not. You should also be able to produce examples of injective and/or surjective functions.

5. You should know that a function is invertible *if and only if* the function is bijective.

6. You should know how to use the pigeonhole principle, and you should know its limitations.

7. YOU SHOULD BE AWARE THAT INVERSE IMAGES AND INVERSE FUNCTIONS HAVE SIMILAR NOTATIONS, BUT ARE NOT RELATED.

8. You should know Peano's axioms, and you should be able to use Peano's axioms to prove that two natural numbers are not equal.

9. You should be able to determine whether a set is well-ordered or not.

10. You should be able to state the principle of mathematical induction, both in words and without words.

11. You should be able to detect and state the flaw in a false proof that uses mathematical induction.

12. You should be able to prove statements about all natural numbers using mathematical induction.

13. You should be able to determine the closed form of a recursive sequence, and you should be able to prove such a formula by strong mathematical induction.

14. Given a closed formula for a recursive sequence, you should be able to find a recursive relation that it satisfies.

15. You should know that all integers greater than one have unique prime factorizations.

16. You should know how to find the remainder when a given large number is divided by another number.

17. You should know how to find the integral quotient of one number by another.

2.3 Theorems of importance

You should be able to state and apply the following theorems.

The following is known as the pigeonhole principle.

Theorem 2.31 *Let X and Y be finite sets such that $|X| = |Y|$. Given a function $f : X \to Y$, f is injective if and only if f is surjective.*

The following is known as the well-ordering principle.

Theorem 2.32 *Given $S \subseteq \mathbb{N}$, $\exists\, t \in S$ such that $\forall\, s \in S$, $t \leq s$.*

The following is known as strong mathematical induction, or complete mathematical induction.

Theorem 2.33 *For each $n \in \mathbb{N}$, let $P(n)$ be a statement. If $P(1)$ is true and $\forall\, k \in \mathbb{N}$, $P(1), P(2), ..., P(k)$ implies $P(k+1)$, then $\forall\, n \in \mathbb{N}$, $P(n)$ is true.*

The following is known as the unique factorization theorem, or the fundamental theorem of arithmetic.

Theorem 2.34 *Let $n \in \mathbb{N}$ such that $n \neq 1$. There exists a unique prime factorization of n into positive prime numbers.*

2.4 Sample problems

In order to be sure that you possess the requisite skills, you should be able to prove all of the following theorems.

Theorem 2.35 *Given a function $f : X \to Y$, the following statements are true.*
(i) There exists a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ if and only if f is injective.
(ii) There exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ if and only if f is surjective.

Theorem 2.36 *Let $f : X \to Y$ be a function. The following statements are true.*
(i) f is injective if and only if $\forall\ A \subseteq X$, $A = f^{-1}\left(f\left(A\right)\right)$.
(ii) f is surjective if and only if $\forall\ B \subseteq Y$, $B = f\left(f^{-1}\left(B\right)\right)$.

Theorem 2.37 *Given a function $f : X \to Y$, f is bijective if and only if f is invertible.*

Theorem 2.38 *Let $f : X \to Y$ be an invertible function. Given $g_1 : Y \to X$ and $g_2 : Y \to X$, if g_1 and g_2 are both inverse functions of f, then $g_1 = g_2$.*

Theorem 2.39 *Let $f : X \to Y$ and $g : Y \to Z$ be functions. If f and g are invertible, then $\left(g \circ f\right)^{-1} = f^{-1} \circ g^{-1}$.*

Theorem 2.40 *Given $n \in \mathbb{N}$, $n \neq n'$.*

Theorem 2.41 *Given $m, n \in \mathbb{N}$, $m + n \neq m$.*

Theorem 2.42 *Let $m, k_1, k_2 \in \mathbb{N}$. If $m + k_1 = m + k_2$, then $k_1 = k_2$.*

Theorem 2.43 *The following statements are true.*
(i) $\forall\ n \in \mathbb{Z}$, $n0 = 0$.
(ii) $\forall\ m, n \in \mathbb{Z}$, $\left(-m\right)n = -\left(mn\right)$.
(iii) $\forall\ m, n \in \mathbb{Z}$, $\left(-m\right)\left(-n\right) = mn$.
(iv) $\forall\ m, n, k \in \mathbb{Z}$, if $mk = nk$ and $k \neq 0$, then $m = n$.

Theorem 2.44 *The following statements are true.*
(i) $\forall\, m, n, p \in \mathbb{Z}$, *if* $m < n$ *and* $n < p$, *then* $m < p$.
(ii) $\forall\, m, n, k \in \mathbb{Z}$, *if* $m < n$, *then* $m + k < n + k$.
(iii) $\forall\, m, n, k \in \mathbb{Z}$, *if* $m < n$ *and* $0 < k$, *then* $mk < nk$.
(iv) $\forall\, m, n, k \in \mathbb{Z}$, *if* $m < n$ *and* $k < 0$, *then* $nk < mk$.

Theorem 2.45 *The following statements are true.*
(i) $\forall\, x, y \in \mathbb{Z}$, $\forall\, n \in \mathbb{N}$, $(xy)^n = x^n y^n$.
(ii) $\forall\, x \in \mathbb{Z}$, $\forall\, m, n \in \mathbb{N}$, $x^m x^n = x^{m+n}$.
(iii) $\forall\, x \in \mathbb{Z}$, $\forall\, m, n \in \mathbb{N}$, $(x^m)^n = x^{mn}$.

Theorem 2.46 *The following statements are true.*
(i) $\forall\, n \in \mathbb{N}$,

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}. \tag{23}$$

(ii) $\forall\, n \in \mathbb{N}$,

$$1 + 3 + 5 + ... + (2n - 1) = n^2. \tag{24}$$

(iii) $\forall n \in \mathbb{N}$,

$$1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}. \tag{25}$$

(iv) $\forall\, n \in \mathbb{N}$,

$$\frac{1}{1(2)} + \frac{1}{2(3)} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1}. \tag{26}$$

Theorem 2.47 *The following statements are true.*
(i) Given the recursive sequence (s_n) *defined via*

$$\begin{aligned} s_1 &= 1 \\ s_2 &= 7 \\ s_{n+1} &= 2s_{n-1} - s_n \quad \textit{for } n > 1 \end{aligned} \quad , \tag{27}$$

the sequence can be written in closed form as

$$s_n = 3 + (-2)^n. \tag{28}$$

(ii) Given the recursive sequence (s_n) defined via

$$\begin{aligned} s_1 &= -1 \\ s_2 &= -5 \\ s_{n+1} &= 5s_n - 6s_{n-1} \quad \textit{for } n > 1 \end{aligned} \quad , \tag{29}$$

the sequence can be written in closed form as

$$s_n = 2^n - 3^n. \tag{30}$$

Theorem 2.48 *There exist infinitely many prime numbers.*

Theorem 2.49 *Let $a, b, c, d, n \in \mathbb{Z}$, and suppose $a \equiv b\,(\textit{mod } n)$ and $c \equiv d\,(\textit{mod } n)$. The following statements are true.*
(i) $a + c \equiv b + d\,(\textit{mod } n)$.
(ii) $ab \equiv bd\,(\textit{mod } n)$.

Theorem 2.50 *Let $a, b, n \in \mathbb{Z}$, and let m be a natural number. If $a \equiv b\,(\textit{mod } n)$, then $a^m \equiv b^m\,(\textit{mod } n)$.*

2.5 Solutions to sample problems

Proof of Theorem 2.35 (i) $(\Rightarrow)$ Assume that $g \circ f = \mathrm{id}_X$. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. In that case,

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2, \tag{31}$$

and thus f is injective.

$(\Leftarrow)$ Assume that f is injective. Let $x_0 \in X$ be arbitrary. We define $g : Y \to X$ via the following relationship. For each $y \in Y$, if $y \in f(X)$, then select $x \in X$ such that $f(x) = y$. We define

$$g(y) = \begin{cases} x & \text{if } y \in f(X) \\ x_0 & \text{if } y \notin f(X) \end{cases}. \tag{32}$$

By construction, $\forall\, x \in X$, $g(f(x)) = x$, and so $g \circ f = \mathrm{id}_X$.

(ii) $(\Rightarrow)$ Assume that $f \circ g = \mathrm{id}_Y$. Let $y \in Y$. In that case, $f(g(y)) = y$. This shows that f is surjective.

$(\Leftarrow)$ Assume that f is surjective. We define $g : Y \to X$ via the following relationship. For each $y \in Y$, $\exists\, x \in X$ such that $f(x) = y$. Let $g(y) = x$. By construction, $\forall\, y \in Y$, $f(g(y)) = f(x) = y$, and so $f \circ g = \mathrm{id}_Y$. □

Proof of Theorem 2.36 (i) $(\Rightarrow)$ Assume that f is injective. Let $A \subseteq X$. We know that $A \subseteq f^{-1}(f(A))$ because of Theroem 1.30. We claim that $f^{-1}(f(A)) \subseteq A$. Let $x \in f^{-1}(f(A))$. In that case, $f(x) \in f(A)$. Therefore, $\exists\, a \in A$ such that $f(a) = f(x)$. As f is injective, we know that $a = x$, so $x \in A$.

$(\Leftarrow)$ Assume that $\forall\, A \subseteq X$, $A = f^{-1}(f(A))$. We will show that f is injective. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. This means in particular that $x_1 \in f^{-1}(\{f(x_2)\}) = f^{-1}(f(\{x_2\}))$. By assumption, $f^{-1}(f(\{x_2\})) = \{x_2\}$, so $x_1 \in \{x_2\}$. Thus, $x_1 = x_2$. This shows that f is injective.

(ii) $(\Rightarrow)$ Assume that f is surjective. Let $B \subseteq Y$. By Theorem 1.31, we know that $f(f^{-1}(B)) \subseteq B$. Now we claim that $B \subseteq f(f^{-1}(B))$. Let $y \in B$. Since f is surjective, $y = f(x)$ for some $x \in X$. In particular, $x \in f^{-1}(B)$, so

$y = f(x) \in f\left(f^{-1}(B)\right)$.

($\Leftarrow$) Assume that $\forall\ B \subseteq Y$, $B = f\left(f^{-1}(B)\right)$. Let $y \in Y$. By assumption, $\{y\} = f\left(f^{-1}(\{y\})\right)$. Therefore, $\exists\ x \in f^{-1}(\{y\})$, and thus $y = f(x)$ for some $x \in X$. This shows that f is surjective. □

Proof of Theorem 2.37 ($\Rightarrow$) Assume that f is bijective. We will show that f is invertible. We define $g : Y \to X$ via the following relationship. Since f is surjective, given $y \in Y$, $\exists\ x \in X$ such that $f(x) = y$. We define $g(y) = x$.

We claim that g is a well-defined function. Given $y_1, y_2 \in Y$, $\exists\ x_1, x_2 \in X$ such that $f(x_1) = y_1$ and $f(x_2) = y_2$. If $y_1 = y_2$, then $f(x_1) = f(x_2)$. Since f is injective, this implies that $x_1 = x_2$, and thus $g(y_1) = g(y_2)$. This shows that g is well-defined.

We claim that g is an inverse function of f. Let $x \in X$. In that case, by definition of g, $g(f(x)) = x_0$ for some x_0 such that $f(x_0) = f(x)$. As f is injective, $x_0 = x$. This shows that $g \circ f = \mathrm{id}_X$. Let $y \in Y$. As f is surjective, we know that $\exists\ x_1 \in X$ such that $f(x_1) = y$. Therefore, $g(y) = x_1$, and so $f(g(y)) = f(x_1) = y$. This shows that $f \circ g = \mathrm{id}_Y$. We deduce that g is an inverse function of f.

($\Leftarrow$) Assume that f is invertible. We will show that f is bijective. Suppose that $g : Y \to X$ be an inverse function of f. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. As $g \circ f = \mathrm{id}_X$, we note that

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2. \tag{33}$$

This shows that f is injective. Now, let $y \in Y$. We know that $f \circ g = \mathrm{id}_Y$, and so $f(g(y)) = y$. Yet we notice that $g(y) \in X$, so $f(g(y)) = y$ shows that f is surjective. We deduce that f is bijective. □

Proof of Theorem 2.38 Let g_1 and g_2 be inverse functions of f. This means in particular that $f \circ g_1 = \mathrm{id}_Y$ and $f \circ g_2 = \mathrm{id}_Y$. Given $y \in Y$, we know that

$$f(g_1(y)) = y = f(g_2(y)). \tag{34}$$

By Theorem 2.37, we know that f is injective. Therefore, $g_1(y) = g_2(y)$, and so

$g_1 = g_2$. □

Proof of Theorem 2.39 Let $f : X \to Y$ and $g : Y \to Z$ be invertible functions. We will show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

First, we claim that $g \circ f$ is invertible. We know that f and g are both injective, due to Theorem 2.37. Thus, given $x_1, x_2 \in X$, if $g(f(x_1)) = g(f(x_2))$, then $f(x_1) = f(x_2)$, and so $x_1 = x_2$. This shows that $g \circ f$ is injective. Now, given $z \in Z$, $\exists\, y \in Y$ such that $g(y) = z$, since g is surjective. Further, $\exists\, x \in X$ such that $f(x) = y$, since f is surjective. Therefore, $\exists\, x \in X$ such that $g(f(x)) = z$, and so $g \circ f$ is surjective. As $g \circ f$ is bijective, Theorem 2.37 implies that $g \circ f$ is invertible.

Let $h = f^{-1} \circ g^{-1}$. We claim that h is the inverse function of $g \circ f$. Given $x \in X$, we notice that

$$h \circ (g \circ f)(x) = f^{-1}\left(g^{-1}\left(g\left(f\left(x\right)\right)\right)\right) = f^{-1}\left(f\left(x\right)\right) = x. \tag{35}$$

This shows that $h \circ (g \circ f) = \mathrm{id}_X$. Given $z \in Z$, we notice that

$$(g \circ f) \circ h(z) = g\left(f\left(h\left(z\right)\right)\right) = g\left(f\left(f^{-1}\left(g^{-1}\left(z\right)\right)\right)\right) = g\left(g^{-1}\left(z\right)\right) = z. \tag{36}$$

This shows that $(g \circ f) \circ h = \mathrm{id}_Z$. We deduce that $h = (g \circ f)^{-1}$. □

Proof of Theorem 2.40 We proceed by mathematical induction on n. First, we note that $1 \neq 1'$, since by Peano's axioms, no successor can be equal to 1. This establishes a basis for induction. As the induction hypothesis, assume, for some $k \in \mathbb{N}$, that $k \neq k'$. By Peano's axioms, this indicates that $k' \neq (k')'$. This completes the induction. □

Proof of Theorem 2.41 We proceed by mathematical induction on n. First, we note that $m + 1 \neq m$, since, by Theorem 2.40, $m' \neq m$. This establishes a basis for induction. As the induction hypothesis, assume that, for some $k \in \mathbb{N}$, $m + k \neq m$. By definition of addition, we know that $m + k' = (m + k)' \neq m + k$, which completes the induction. □

Proof of Theorem 2.42 Assume, with the expectation of a contradiction, $k_1 \neq k_2$. Suppose, with the understanding that the other choice is similar, that $k_1 < k_2$. In that case, $\exists\, r \in \mathbb{N}$ such that $k_2 = k_1 + r$, and so

$$m + k_1 = m + k_2 = (m + k_1) + r, \tag{37}$$

despite that Theorem 2.41 indicates that $m + k_1 \neq (m + k_1) + r$. This contradiction leads us to conclude that our assumption that $k_1 \neq k_2$ is false; $k_1 = k_2$. □

Proof of Theorem 2.43 (i) We note that

$$n0 + 0 = n0 = n\,(0 + 0) = n0 + n0, \tag{38}$$

which indicates that $0 = n0$, by Theorem 2.42.

(ii) We note that

$$0 = n0 = n\,(m - m) = mn + (-m)\,n, \tag{39}$$

and so $(-m)\,n = -mn$.

(iii) We note that

$$0 = (-m)\,0 = (-m)\,(n - n) = (-m)\,n + (-m)\,(-n)\,. \tag{40}$$

Therefore, $(-m)\,(-n) = -\,(-m)\,n = -\,(-mn) = mn$.

(iv) Let $mk = nk$ with $k \neq 0$. In that case,

$$0 = mk - nk = (m - n)\,k. \tag{41}$$

Since $k \neq 0$, we must have that $m - n = 0$, and so $m = n$. □

Proof of Theorem 2.44 (i) Suppose that $m < n$ and $n < p$. In that case, $\exists\, k, l \in \mathbb{N}$ such that $n = m + k$ and $p = n + l$. This means that $p = m + k + l$, and so $m < p$.

(ii) Suppose that $m < n$. In that case, $n - m = r$ for some $r \in \mathbb{N}$. We notice that

$$(n+k)-(m+k)=n-m=r, \tag{42}$$

and so $m+k<n+k$.

(iii) Suppose that $m<n$ and $0<k$. We know that $k\in\mathbb{N}$, and $\exists\ r\in\mathbb{N}$ such that $n-m=r$. We deduce that

$$nk-mk=(n-m)\,k-rk\in\mathbb{N}, \tag{43}$$

which means that $mk<nk$.

(iv) Suppose that $m<n$ and $k<0$. In that case, $-k\in\mathbb{N}$ and $\exists\ r\in\mathbb{N}$ such that $n-m=r$. We notice that

$$mk-nk=(m-n)\,k=(-r)\,k=r\,(-k)\in\mathbb{N}, \tag{44}$$

and so $nk<mk$. □

Proof of Theorem 2.45 We proceed by mathematical induction on n. First, we notice that $(xy)^1=xy=x^1y^1$. This establishes a basis for induction. Now, as the induction hypothesis, assume, for some $k\in\mathbb{N}$, that $(xy)^k=x^ky^k$. We notice that

$$(xy)^{k+1}=(xy)^k\,(xy)=x^ky^kxy=x^{k+1}y^{k+1}. \tag{45}$$

This completes the induction.

(ii) We proceed by mathematical induction on n. We notice that $x^mx^1=x^{m+1}$. This establishes a basis for induction. As the induction hypothesis, assume, for some $k\in\mathbb{N}$, that $x^mx^k=x^{m+k}$. Now,

$$x^mx^{k+1}=x^mx^kx=x^{m+k}x=x^{m+k+1}, \tag{46}$$

which completes the induction.

(iii) We proceed by mathematical induction on n. First of all, we notice that $(x^m)^1=x^m=x^{m1}$. This establishes a basis for induction. As the induction hypothesis, assume, for some $k \in \mathbb{N}$, that $(x^m)^k = x^{mk}$. Now,

$$(x^m)^{k+1} = (x^m)^k x^m = x^{mk} x^m = x^{mk+m} = x^{m(k+1)}. \tag{47}$$

This completes the induction. □

Proof of Theorem 2.46 (i) We proceed by mathematical induction on n. First, we note that $1 = \frac{1(1+1)}{2}$. This establishes a basis for induction. As the induction hypothesis, assume that $1 + 2 + ... + k = \frac{k(k+1)}{2}$, for some $k \in \mathbb{N}$. We notice that

$$\begin{aligned} 1 + 2 + ... + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+1)(k+2)}{2}. \end{aligned} \tag{48}$$

This completes the induction.

(ii) We proceed by mathematical induction on n. First, we note that $1 = 1^2$. This establishes a basis for induction. As the induction hypothesis, assume that $1 + 3 + ... + (2k-1) = k^2$ for some $k \in \mathbb{N}$. We notice that

$$1 + 3 + ... + (2k-1) + (2(k+1) - 1) = k^2 + 2k + 1 = (k+1)^2. \tag{49}$$

This completes the induction.

(iii) We proceed by mathematical induction on n. First, $1^2 = \frac{1(1+1)(2(1)+1)}{6}$. This establishes a basis for induction. As the induction hypothesis, assume that, for some $k \in \mathbb{N}$, $1^2 + 2^2 + ... + k^2 = \frac{k(k+1)(2k+1)}{6}$. Now,

$$\begin{aligned} 1^2 + 2^2 + ... + k^2 + (k+1)^2 &= \frac{k\left(k+1\right)\left(2k+1\right)}{6} + \left(k+1\right)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)(k+1)}{6} \\ &= \frac{\left(k+1\right)\left(2k^2+7k+6\right)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \\ &= \frac{(k+1)(k+2)(2(k+1)+1)}{6}. \end{aligned} \tag{50}$$

This completes the induction.

(iv) We proceed by mathematical induction on n. First, we note that $\frac{1}{1(2)} = \frac{1}{1+1}$. This establishes a basis for induction. As the induction hypothesis, assume that for some $k \in \mathbb{N}$,

$$\frac{1}{1(2)} + \frac{1}{2(3)} + ... + \frac{1}{k(k+1)} = \frac{k}{k+1}. \tag{51}$$

We note that

$$\begin{aligned} &\frac{1}{1(2)} + \frac{1}{2(3)} + ... + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k^2+2k+1}{(k+1)(k+2)} \\ &= \frac{(k+1)(k+1)}{(k+1)(k+2)} \\ &= \frac{(k+1)}{(k+1)+1}. \end{aligned} \tag{52}$$

This completes the induction. □

Proof of Theorem 2.47 (i) We proceed by strong mathematical induction on n.

First, we note that $1 = s_1 = 3 + (-2)^1$ and $7 = s_2 = 3 + (-2)^2$. This establishes a basis for induction. As the induction hypothesis, assume, for some $k \in \mathbb{N}$, that $\forall\, n \in \{1, 2, ..., k\}$, $s_n = 3 + (-2)^n$. We know that $s_{k+1} = 2s_{k-1} - s_k$ if $k > 1$. By the induction hypothesis, we also know that

$$\begin{aligned} s_{k-1} &= 3 + (-2)^{k-1} \\ s_k &= 3 + (-2)^k \end{aligned} . \tag{53}$$

Thus,

$$\begin{aligned} s_{k+1} = 2s_{k-1} - s_k = 2\left(3 + (-2)^{k-1}\right) - \left(3 + (-2)^k\right) \\ = 6 + (-1)^{k-1}2^k - 3 - (-1)^k 2^k \\ = 3 + (-1)^{k-1}2^k + (-1)^{k+1}2^k \\ = 3 + (-1)^{k+1}2^k + (-1)^{k+1}2^k \\ = 3 + 2(-1)^{k+1}2^k \\ = 3 + (-1)^{k+1}2^{k+1} = 3 + (-2)^{k+1}. \end{aligned} \tag{54}$$

This completes the induction.

(ii) We proceed by strong mathematical induction on n. First, we note that $-1 = 2^1 - 3^1$, and that $-5 = 2^2 - 3^2$. This establishes a basis for induction. As the induction hypothesis, assume, for some $k \in \mathbb{N}$, that $\forall\, n \in \{1, 2, ..., k\}$, $s_n = 2^n - 3^n$. We know that $s_{k+1} = 5s_k - 6s_{k-1}$ if $k > 1$. By the induction hypothesis, we also know that

$$\begin{aligned} s_{k-1} &= 2^{k-1} - 3^{k-1} \\ s_k &= 2^k - 3^k \end{aligned} . \tag{55}$$

Thus,

$$\begin{aligned}s_{k+1} = 5s_k - 6s_{k-1} &= 5\left(2^k - 3^k\right) - 6\left(2^{k-1} - 3^{k-1}\right)\\ &= (5)2^k - (5)3^k - (6)2^{k-1} + (6)3^{k-1}\\ &= (5)2^k - (5)3^k - (3)2^k + (2)3^k\\ &= (2)2^k - (3)3^k = 2^{k+1} - 3^{k+1}. \quad (56)\end{aligned}$$

This completes the induction. □

Proof of Theorem 2.48 Assume, with the expectation of a contradiction, that there exist finitely many prime numbers. Suppose that the prime numbers are $p_1, p_2, ..., p_n$. We define $N = p_1 p_2 ... p_n + 1$. Since N is larger than any prime number, N must be composite. By Theorem 2.34, N has a prime factorization. Therefore, $\exists\ i \in \{1, 2, ..., n\}$ such that $p_i | N$. Thus, $N = qp_i$ for some $q \in \mathbb{Z}$. However,

$$1 = N - p_1 p_2 ... p_n = qp_i - p_1 p_2 ... p_n = p_i \left(q - p_1 p_2 ... p_{i-1} p_{i+1} ... p_n\right). \quad (57)$$

This shows that 1 is composite. This contradiction leads us to conclude that our assumption that there are finitely many prime numbers is false; there exist infinitely many prime numbers. □

Proof of Theorem 2.49 (i) Suppose that $a \equiv b \,(\text{mod}\ n)$ and $c \equiv d \,(\text{mod}\ n)$. This means that $\exists\ q_1, q_2 \in \mathbb{Z}$ such that $a - b = q_1 n$ and $c - d = q_2 n$. Therefore,

$$(a + c) - (b + d) = a - b + c - d = q_1 n + q_2 n = (q_1 + q_2)\, n. \quad (58)$$

This shows that $n | (a + c) - (b + d)$, and so $a + c \equiv b + d \,(\text{mod}\ n)$.

(ii) Suppose that $a \equiv b \,(\text{mod}\ n)$ and $c \equiv d \,(\text{mod}\ n)$. In that case, $\exists\ q_1, q_2 \in \mathbb{Z}$ such that $a - b = q_1 n$ and $c - d = q_2 n$. Therefore, $a = b + q_1 n$ and $c = d + q_2 n$. We deduce that

$$ac = (b + q_1 n)(d + q_2 n) = bd + bq_2 n + dq_1 n + q_1 q_2 n^2 = bd + (bq_2 + dq_1 + q_1 q_2 n)\, n. \quad (59)$$

This shows that $n|ac - bd$, and so $ac \equiv bd \pmod{n}$. □

Proof of Theorem 2.50 We proceed by mathematical induction on m. First, we know that $a^1 \equiv b^1 \pmod{n}$, by assumption. This establishes a basis for induction. As the induction hypothesis, assume that for some $k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$. By Theorem 2.49, since $a \equiv b \pmod{n}$, we have that

$$a^{k+1} \equiv a^k a \equiv b^k b \equiv b^{k+1} \pmod{n}. \tag{60}$$

This completes the induction. □

3 Review for Test 3

3.1 Dictionary of terms

Definition 3.1 *Let $m, n \in \mathbb{Z}$. The greatest common divisor of m and n is the integer $d \in \mathbb{Z}$ satisfying the following conditions.*
(i) $d|m$ and $d|n$.
(ii) Given $k \in \mathbb{Z}$, if $k|m$ and $k|n$, then $k \leq d$.

Notation We denote the greatest common divisor of m and n by "$\gcd(m, n)$."

Definition 3.2 *Let $m, n \in \mathbb{Z}$. We say that m and n are relatively prime, or coprime, provided that* $\gcd(m, n) = 1$.

Definition 3.3 *The factorial is the function $f : \mathbb{N} \cup \{0\} \to \mathbb{N}$ such that $f(0) = 1$ and $\forall\, n \in \mathbb{N}$, $f(n) = nf(n-1)$.*

Notation We denote the factorial of a number $n \in \mathbb{N} \cup \{0\}$ by "$n!$."

Definition 3.4 *Let $n, k \in \mathbb{N} \cup \{0\}$ such that $k \leq n$. The binomial coefficient n choose k is the value*

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}. \tag{61}$$

Definition 3.5 *The Euler totient function is the function $\phi : \mathbb{N} \to \mathbb{N}$ defined via the following relationship: for each $n \in \mathbb{N}$,*

$$\phi(n) = \left| \left\{ m \in \mathbb{N} \middle| m \leq n \textit{ and } \gcd(m, n) = 1 \right\} \right|. \tag{62}$$

Definition 3.6 *Let X be a set. A [binary] relation on X is a subset $R \subseteq X \times X$.*

Notation Given a binary relation R on a set X, we often denote the statement "$(x, y) \in R$" by "xRy."

Definition 3.7 *Let R be a binary relation on a set X. We say that R is reflexive provided that $\forall\, x \in X$, xRx.*

Definition 3.8 *Let R be a binary relation on a set X. We say that R is symmetric provided that $\forall\, x, y \in X$, if xRy, then yRx.*

Definition 3.9 *Let R be a binary relation on a set X. We say that R is transitive provided that $\forall\, x, y, z \in X$, if xRy and yRz, then xRz.*

Definition 3.10 *Let R be a binary relation on a set X. We say that R is an equivalence relation provided that R is reflexive, symmetric, and transitive.*

Definition 3.11 *Let $\sim$ be an equivalence relation on a set X. Given $x_0 \in X$, the equivalence class of x_0 is the set*

$$[x_0] = \left\{ y \in X \middle| y \sim x_0 \right\}. \tag{63}$$

Definition 3.12 *Let $\sim$ be an equivalence relation on a set X. The quotient set of X by $\sim$ is the set*

$$X\, /_{\sim} = \left\{ [x_0] \middle| x_0 \in X \right\}. \tag{64}$$

Definition 3.13 *Let X be a set. A partition of X is a set $S \subseteq \mathcal{P}(X)$ such that $\bigcup S = X$ and $\forall\, A, B \in S$, either $A = B$ or $A \cap B = \varnothing$.*

Definition 3.14 *Let $n \in \mathbb{Z}$ such that $n \neq 0$. The set of integers modulo n is the quotient set*

$$\mathbb{Z}\, /_{n} = \mathbb{Z}\, \Big/_{\equiv\, (\textit{mod}\, n)} \cdot \tag{65}$$

Definition 3.15 *Let X be a nonempty set. A binary operation on X is a function $* : X \times X \to X$.*

Notation Given a binary operation $*$, we commonly denote $*(x, y)$ by "$x * y$."

Definition 3.16 *Let $n \in \mathbb{Z}$ such that $n \neq 0$. The addition of integers modulo n is the binary operation $+$ on $\mathbb{Z}\, /_{n}$ defined via $[a] + [b] = [a + b]$.*

Definition 3.17 *Let $n \in \mathbb{Z}$ such that $n \neq 0$. The multiplication of integers modulo n is the binary operation $\cdot$ on $\mathbb{Z}\, /_{n}$ defined via $[a] \cdot [b] = [ab]$.*

Definition 3.18 *Let $\sim$ be the equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defined via $(a,b) \sim (c,d)$ if and only if $ad = bc$. The set of rational numbers is the quotient set*

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) /_{\sim}. \qquad (66)$$

Notation We commonly denote an element $[(a,b)] \in \mathbb{Q}$ by "$\frac{a}{b}$."

Definition 3.19 *The addition of rational numbers is the binary operation $+$ on $\mathbb{Q}$ defined such that $\forall\ \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$,*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}. \qquad (67)$$

Definition 3.20 *The multiplication of rational numbers is the binary operation $\cdot$ on $\mathbb{Q}$ defined such that $\forall\ \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$,*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \qquad (68)$$

Definition 3.21 *The ordering of rational numbers is the binary relation $<$ on $\mathbb{Q}$ such that $\forall\ \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $\frac{a}{b} < \frac{c}{d}$ if and only if either $bd > 0$ and $ad < bc$ or $bd < 0$ and $ad > bc$.*

Definition 3.22 *Let R be a nonempty set, and let $+$ and $\cdot$ be binary operations on R. We say that $(R, +, \cdot)$ is a ring [with unity] provided that the following statements are true.*

(i) $+$ is associative; $\forall\ a,b,c \in R$, $a + (b + c) = (a + b) + c$.

(ii) $\exists\ 0 \in R$ such that $\forall\ a \in R$, $a + 0 = 0 + a = a$.

(iii) $\forall\ a \in R$, $\exists\ b \in R$ such that $a + b = b + a = 0$.

(iv) $+$ is commutative; $\forall\ a,b \in R$, $a + b = b + a$.

(v) $\cdot$ is associative; $\forall\ a,b,c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(vi) $\cdot$ distributes over $+$; $\forall\ a,b,c \in R$,

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c)\,. \end{aligned} \qquad (69)$$

(vii) $\exists\ 1 \in R$ such that $\forall\ a \in R$, $1 \cdot a = a \cdot 1 = a$.

Notation We often write the statement "$(R, +, \cdot)$ is a ring with unity" as "R is a ring with unity," or as "R is a ring with unity under $+$ and $\cdot$."

Definition 3.23 *Let R be a ring. Given $a \in R$, we say that a is a zero divisor of R provided that $a \neq 0$ and $\exists\, b \in R \setminus \{0\}$ such that $ab = 0$.*

Definition 3.24 *Let R be a ring. We say that R is a commutative ring provided that $\cdot$ is commutative; $\forall\, a, b \in R$, $a \cdot b = b \cdot a$.*

Definition 3.25 *Let R be a ring with unity. We say that R is a field provided that R is a commutative ring and $\forall\, a \in R$, $\exists\, b \in R$ such that $ab = 1$.*

Definition 3.26 *Let $n \in \mathbb{Z}^+$. The ring of $n \times n$ matrices over $\mathbb{R}$ is the ring*

$$M_n(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \middle| a_{11}, a_{12}, \ldots, a_{nn} \in \mathbb{R} \right\}. \tag{70}$$

Definition 3.27 *Let $d \in \mathbb{Z}$. The ring of integers adjoin $\sqrt{d}$ is the ring*

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{ a + b\sqrt{d} \middle| a, b \in \mathbb{Z} \right\}. \tag{71}$$

Definition 3.28 *Let $d \in \mathbb{Z}$. The ring of rational numbers adjoin $\sqrt{d}$ is the ring*

$$\mathbb{Q}\left[\sqrt{d}\right] = \left\{ a + b\sqrt{d} \middle| a, b \in \mathbb{Q} \right\}. \tag{72}$$

Definition 3.29 *Let S be a set. A [linear] ordering on S is a transitive binary relation $<$ on S such that $\forall\, x, y \in S$, exactly one of the following conditions is true: $x = y$, $x < y$, or $y < x$.*

Definition 3.30 *Let S be a set, and let $<$ be a linear ordering on S. We say that $(S, <)$ is an ordered set.*

Definition 3.31 *Let $(X, <_X)$ and $(Y, <_Y)$ be ordered sets. The lexicographic ordering on $X \times Y$ is the ordering $<$ on $X \times Y$ defined such that $(x_1, y_1) < (x_2, y_2)$ if and only if either $x_1 < x_2$ or $x_1 = x_2$ and $y_1 < y_2$.*

Definition 3.32 *Let $(S, <)$ be an ordered set. Given $x \in S$, we say that x is a maximal element of S provided that $\forall\ s \in S$, $s \leq x$.*

Definition 3.33 *Let $(S, <)$ be an ordered set. Given $x \in S$, we say that x is a minimal element of S provided that $\forall\ s \in S$, $x \leq s$.*

Definition 3.34 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. Given $s_1 \in S$, we say that s_1 is an upper bound of T provided that $\forall\ t \in T$, $t \leq s_1$.*

Definition 3.35 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. Given $s_0 \in S$, we say that s_0 is a lower bound of T provided that $\forall\ t \in T$, $s_0 \leq t$.*

Definition 3.36 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. We say that T is bounded above in S provided that there exists an upper bound of T in S.*

Definition 3.37 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. We say that T is bounded below in S provided that there exists a lower bound of T in S.*

Definition 3.38 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. Given $s_1 \in S$, we say that s_1 is a least upper bound of T provided that the following statements are true.*
(i) s_1 is an upper bound of T.
(ii) If s is any upper bound of T, then $s_1 \leq s$.

Definition 3.39 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. Given $s_0 \in S$, we say that s_0 is a greatest lower bound of T provided that the following statements are true.*
(i) s_0 is a lower bound of T.
(ii) If s is any lower bound of T, then $s \leq s_0$.

Definition 3.40 *Let R be a commutative ring, and let $<$ be an ordering on R. We say that $(R, <)$ is an ordered ring provided that the following statements are true.*
(i) $\forall\ x, y, z \in R$, if $x < y$, then $x + z < y + z$.
(ii) $\forall\ x, y, z \in R$, if $x < y$ and $0 < z$, then $xz < yz$.

Definition 3.41 *Let $(S, <)$ be an ordered set. We say that $(S, <)$ satisfies the least upper bound property, or that $(S, <)$ is Dedekind complete, provided that $\forall\, T \subseteq S$, if $T \neq \varnothing$ and T is bounded above in S, then $\exists\, t \in S$ that is a least upper bound of T.*

Definition 3.42 *The field of real numbers is the ordered ring $(\mathbb{R}, <)$ satisfying the following conditions.*
(i) $\mathbb{Q} \subseteq \mathbb{R}$.
(ii) $\mathbb{R}$ is a field.
(iii) $(\mathbb{R}, <)$ satisfies the least upper bound property.

Definition 3.43 *Let $(X, <)$ be an ordered set. Given a nonempty $S \subseteq X$, we say that S is dense in X provided that $\forall\, x_1, x_2 \in X$, if $x_1 < x_2$, then $\exists\, s \in S$ such that $x_1 < s < x_2$.*

Definition 3.44 *Let X and Y be sets. A one-to-one correspondence between X and Y is a bijection $f : X \to Y$.*

Definition 3.45 *Let X and Y be sets. We say that X and Y are equivalent or have the same cardinality provided that there exists a bijection $f : X \to Y$.*

Notation We denote the statement "X and Y have the same cardinality" by "$X \sim Y$" or "$|X| = |Y|$."

Definition 3.46 *Let X be a set. We say that X has a cardinality of 0 provided that $X = \varnothing$.*

Notation We denote the statement "X has a cardinality of zero" by "$|X| = 0$."

Definition 3.47 *Let X be a set. Given $n \in \mathbb{N}$, we say that X has a cardinality of n provided that $X \sim \{1, 2, ..., n\}$.*

Notation We denote the statement "X has a cardinality of n" by "$|X| = n$."

Definition 3.48 *Let X be a set. We say that X is finite provided that $|X| = 0$ or $|X| = n$ for some $n \in \mathbb{N}$.*

Definition 3.49 *Let X be a set. We say that X is infinite provided that X is not finite.*

Definition 3.50 *Let X be a set. We say that X is countable provided that either X is finite or $|X| = |\mathbb{N}|$.*

Definition 3.51 *Let X be a set. We say that X is countably infinite provided that $|X| = |\mathbb{N}|$.*

Definition 3.52 *Let X be a set. We say that X is uncountable provided that X is not countable.*

Definition 3.53 *Aleph naught is the cardinality $\aleph_0 = |\mathbb{N}|$.*

Definition 3.54 *Let X and Y be sets. We say that $|X| \leq |Y|$ provided that $\exists\, S \subseteq Y$ such that $|X| = |S|$.*

3.2 Things you should know for the test

1. **ALL OF THE DEFINITIONS.**

2. You should know how to convert a given number from decimal notation to a different base notation.

3. You should know Bézout's lemma, and how to use it.

4. You should know how to determine the number of k-element subsets of a set of n elements.

5. You should know the binomial theorem and how to use it.

6. You should know how to calculate the values of the Euler totient function.

7. You should know Euler's generalization of Fermat's Little Theorem and how to use it.

8. You should know the statements of Goldbach's Conjecture and the Twin Primes Conjecture, and that at present, no one can either prove or disprove them.

9. You should be able to recognize whether a given binary relation is reflexive, symmetric, and/or transitive.

10. You should be able to produce binary relations that have a given property.

11. Given an equivalence relation on a set and an element of the set, you should be able to describe the equivalence class of the element.

12. You should be able to define and describe a given integer modulo n, based on the definition of the set of integers modulo n.

13. You should be able to define and describe a given rational number, based on the definition of the set of rational numbers.

14. You should be able to prove that a set with a given addition and multiplication is not a ring.

15. You should be able to identify zero divisors of a ring that possesses zero divisors.

16. You should be able to determine whether a given ring is a field.

17. You should understand the notion of lexicographic orderings, and you should be able to describe the lexicographic ordering on a given set.

18. You should be able to determine whether a maximal or minimal element of a given ordered set exists, and you should be able to identify the maximal or minimal element of an ordered set that has a maximal or minimal element.

19. You should know the difference between a minimal element and a lower bound, and the difference between a maximal element and an upper bound.

20. You should be able to determine the least upper bound of a given set of real numbers that is bounded above, and you should be able to determine the greatest lower bound of a given set of real numbers that is bounded below.

21. You should be able to prove or disprove that two given sets have the same cardinality, and to prove or disprove that a set is countable.

22. You should know the statement of the continuum hypothesis, and that it can be neither proven nor disproven.

3.3 Theorems of importance

The following is known as Bézout's lemma.

Theorem 3.55 *Given $m, n \in \mathbb{Z}$, $\exists\, x, y \in \mathbb{Z}$ such that $mx + ny = \gcd(m, n)$.*

The following is known as Euclid's lemma.

Theorem 3.56 *Let $a, b, p \in \mathbb{Z}$. If p is prime and $p|ab$, then $p|a$ or $p|b$.*

The following is known as the binomial theorem.

Theorem 3.57 *Let $x, y \in \mathbb{R}$. Given $n \in \mathbb{N}$,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k. \tag{73}$$

The following is known as Fermat's little theorem.

Theorem 3.58 *Let $p \in \mathbb{Z}$ be a prime number. Given $n \in \mathbb{Z}$, $n^p \equiv n \pmod{p}$.*

The following is known as Euler's generalization of Fermat's little theorem.

Theorem 3.59 *Given $a, n \in \mathbb{Z}$, if a and n are coprime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

The following is known as Fermat's last theorem.

Theorem 3.60 *Let $x, y, z, n \in \mathbb{Z}$. If $n > 2$, then $x^n + y^n \neq z^n$.*

Theorem 3.61 *Let X and Y be sets. If X and Y are countable, then $X \cup Y$ is countable.*

Theorem 3.62 *Let $X \subseteq Y$. If Y is countable, then X is countable.*

Theorem 3.63 *Let X and Y be sets. If X and Y are countable, then $X \times Y$ is countable.*

The following is known as the Gödel incompleteness theorem.

Theorem 3.64 *No finite systems of axioms can imply all of the facts about the natural numbers.*

3.4 Sample problems

In order to be sure that you possess the requisite skills, you should be able to prove all of the following theorems.

Theorem 3.65 *(Euclid's Lemma) Let $a, b, p \in \mathbb{Z}$. If p is prime and $p|ab$, then $p|a$ or $p|b$.*

Theorem 3.66 *Let $a_1, a_2, ..., a_n, p \in \mathbb{Z}$. If p is prime and $p|a_1 a_2 ... a_n$, then there exists $i \in \{1, 2, ..., n\}$ such that $p|a_i$.*

Theorem 3.67 *Let $a, b, n \in \mathbb{Z}$. If $\gcd(a, n) = 1$ and $n|ab$, then $n|b$.*

Theorem 3.68 *Let $p \in \mathbb{Z}^+$ be a prime number. If $k \in \{1, 2, ..., p-1\}$, then $\binom{p}{k}$ is divisible by p.*

Theorem 3.69 *Let $a, b, p \in \mathbb{Z}$. If p is prime, then*

$$(a+b)^p \equiv a^p + b^p \, (mod \, p) \, . \tag{74}$$

Theorem 3.70 *Let $n \in \mathbb{Z}$. The relation on $\mathbb{Z}$ defined via $a \equiv b \, (mod \, n)$ is an equivalence relation.*

Theorem 3.71 *Let $\sim$ be an equivalence relation on a set X. The set ${}^{X}/_{\sim}$ is a partition of X.*

Theorem 3.72 *Let $\sim$ be the binary relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defined such that $\forall \, (a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, $(a, b) \sim (c, d)$ if and only if $ad = bc$. The binary relation $\sim$ is an equivalence relation.*

Theorem 3.73 *Let $n \in \mathbb{Z}$ such that $n \neq 0$. The ring ${}^{\mathbb{Z}}/_{n}$ has zero divisors if and only if n is not prime.*

Theorem 3.74 *Let R be a commutative ring with unity. If R has zero divisors, then R is not a field.*

Theorem 3.75 *Let $(S, <)$ be an ordered set, and let $T \subseteq S$. If $s_1, s_2 \in S$ are least upper bounds of T, then $s_1 = s_2$.*

Theorem 3.76 *Let $n \in \mathbb{Z}$ such that $n \neq 0$ and $n \neq \pm 1$. There exists no ordering $<$ on $\mathbb{Z}/n$ such that $\left(\mathbb{Z}/n, <\right)$ is an ordered ring.*

Theorem 3.77 *There exists no $x \in \mathbb{Q}$ such that $x^2 = 2$.*

Theorem 3.78 *Let $(R, <)$ be an ordered ring. If $(R, <)$ satisfies the least upper bound property, then $\forall\ T \subseteq R$, if $T \neq \varnothing$ and T is bounded below in R, then $\exists\, t \in R$ that is a greatest lower bound of T.*

Theorem 3.79 *The set $\mathbb{Z}$ is countable.*

Theorem 3.80 *The set $\mathbb{Q}$ is countable.*

Theorem 3.81 *The interval $(0, 1)$ is uncountable.*

Theorem 3.82 *Let $a, b, c, d \in \mathbb{R}$ such that $a < b$ and $c < d$. The interval (a, b) has the same cardinality as the interval (c, d).*

Theorem 3.83 *There exists a bijection $f : (-1, 1) \to \mathbb{R}$.*

Theorem 3.84 *The set $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.*

Theorem 3.85 *Let X and Y be sets. The following statements are equivalent.*
(i) $|X| \leq |Y|$.
(ii) There exists an injective function $f : X \to Y$.
(iii) There exists a surjective function $g : Y \to X$.

Theorem 3.86 *Given a set X, $|X| < |\mathcal{P}(X)|$.*

3.5 Solutions to sample problems

Proof of Theorem 3.65 Assume that $p \in \mathbb{Z}$ is prime and that $p|ab$. Suppose that $ab = qp$ for some $q \in \mathbb{Z}$. We consider two cases: either $p|a$ or $p \nmid a$. If $p|a$, then the proof is complete. Consider the case that $p \nmid a$. In that case, since p is a prime number, $\gcd(p, a) = 1$. Therefore, Bézout's lemma (Theorem 3.55) implies that $\exists\, x, y \in \mathbb{Z}$ such that

$$px + ay = 1. \tag{75}$$

Therefore,

$$bpx + aby = b. \tag{76}$$

As $ab = qp$, this implies that

$$p\,(bx + qy) = bpx + qpy = b. \tag{77}$$

We deduce that $p|b$. □

Proof of Theorem 3.66 We proceed by mathematical induction on n. First, if $p|a_1$, then $p|a_1$. This establishes a basis for induction.

Assume, as the induction hypothesis, that if $p|a_1a_2...a_k$, then $p|a_i$ for some $i \in \{1, 2, ..., k\}$. Suppose that $p|a_1a_2...a_ka_{k+1}$. By Euclid's Lemma (Theorem 3.65), we know that $p|a_1a_2...a_k$ or $p|a_{k+1}$. If $p|a_1a_2...a_k$, then the induction hypothesis implies that $p|a_i$ for some $i \in \{1, 2, ..., k\}$. Either way, $p|a_i$ for some $i \in \{1, 2, ..., k, k+1\}$, which completes the induction. □

Proof of Theorem 3.67 Assume that $\gcd(a, n) = 1$ and $n|ab$. In that case, $ab = qn$ for some $q \in \mathbb{Z}$. By Bézout's Lemma (Theorem 3.55), we know that $\exists\, x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Therefore,

$$n\,(qx + by) = nqx + nby = abx + nby = b. \tag{78}$$

This shows that $n|b$. □

Proof of Theorem 3.68 Define $N = \binom{p}{k}$. Assume, with the expectation of a contradiction, that $p \nmid N$. By definition, $N = \frac{p!}{k!(p-k)!}$. Since $p|p!$, we know that $p|N\,(k!)\,((p-k)!)$. By Euclid's Lemma (Theorem 3.65), this implies that $p|N$ or $p|k!\,(p-k)!$. Since $p \nmid N$, we must have that $p|k!(p-k)!$. Using Euclid's Lemma again, we see that $p|k!$ or $p|(p-k)!$. If $p|k!$, then $p|(k)(k-1)(k-2)...(3)(2)(1)$. By Theorem 3.66, this means that $p|k$, $p|k-1$, ..., $p|3$ or $p|2$, despite that $k < p$. If $p|(p-k)!$, then similar arguments show that $p|(p-k)$, $p|(p-k-1)$, ..., $p|3$ or $p|2$, despite that $p-k < p$. This contradiction leads us to conclude that our assumption that $p \nmid N$ is false; $p|N$. □

Proof of Theorem 3.69 By the binomial theorem (Theorem 3.57), we know that

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \binom{p}{1} a^{p-1} b + ... + \binom{p}{p-1} a b^{p-1} + b^p. \quad (79)$$

However, Theorem 3.68 indicates that $\binom{p}{k} \equiv 0 \pmod p$ when $0 < k < p$. Therefore,

$$a^p + \binom{p}{1} a^{p-1} b + ... + \binom{p}{p-1} a b^{p-1} + b^p \equiv a^p + b^p \pmod p\,. \quad (80)$$

□

Proof of Theorem 3.70 We note that $\forall\ a \in \mathbb{Z}$, $n|a-a$. Thus, $a \equiv a \,(\text{mod}\, n)$, and so $\equiv \,(\text{mod}\, n)$ is reflexive. We note that $\forall\ a, b \in \mathbb{Z}$, if $a \equiv b \,(\text{mod}\, n)$, then $n|a-b$. This means that $a - b = qn$ for some $q \in \mathbb{Z}$. In that case, $b - a = (-q)\,n$, and so $b \equiv a \,(\text{mod}\, n)$. This shows that $\equiv \,(\text{mod}\, n)$ is symmetric. Finally, given $a, b, c \in \mathbb{Z}$, assume that $a \equiv b \,(\text{mod}\, n)$ and $b \equiv c \,(\text{mod}\, n)$. This means that $n|a-b$ and $n|b-c$. In other words, $\exists\ q_1, q_2 \in \mathbb{Z}$ such that $a - b = q_1 n$ and $b - c = q_2 n$. By adding these, we deduce that $a - c = (q_1 + q_2)\,n$. Therefore, $n|a-c$, and so $a \equiv c \,(\text{mod}\, n)$. This shows that $\equiv \,(\text{mod}\, n)$ is transitive. □

Proof of Theorem 3.71 First, we claim that $\bigcup X/_\sim = X$. Given $x \in X$, we know that $[x] \in X/_\sim$. Since $x \in [x]$, we deduce that $x \in \bigcup X/_\sim$. This shows that $X \subseteq \bigcup X/_\sim$. Now, given $x \in \bigcup X/_\sim$, we know that $x \in [y]$ for some $y \in X$. This means (by definition) that $x \sim y$, and so $x \in X$. Therefore, $\bigcup X/_\sim \subseteq X$.

Next we claim that $\forall\, [x], [y] \in X/_\sim$, either $[x] = [y]$ or $[x] \cap [y] = \varnothing$. Assume that $[x] \cap [y] \neq \varnothing$. We will show that $[x] \subseteq [y]$. Let $z \in [x]$. This means that $z \sim x$. Since $[x] \cap [y] \neq \varnothing$, we know that $\exists\, w \in [x] \cap [y]$. We deduce that $w \in [x]$ and $w \in [y]$, hence $w \sim x$ and $w \sim y$. Ergo, since $\sim$ is symmetric, $x \sim w$ and $w \sim y$. As $\sim$ is transitive, this implies that $x \sim y$. Thus, since $z \sim x$, $z \sim y$. This implies that $z \in [y]$. This shows that $[x] \subseteq [y]$. Similar arguments can show that $[y] \subseteq [x]$. We deduce that $[x] = [y]$. □

Proof of Theorem 3.72 Given an element $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, we know that $ab = ba$. Therefore, $(a, b) \sim (a, b)$. This shows that $\sim$ is reflexive. Given elements $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, suppose that $(a, b) \sim (c, d)$. This means that $ad = bc$. Therefore, $cb = da$, and so $(c, d) \sim (a, b)$. This shows that $\sim$ is symmetric. Finally, given $(a, b), (c, d), (e, f) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. This means that $ad = bc$ and $cf = de$. We deduce that $adf = bcf = bde$, hence $afd = bed$. Since $(c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, we know that $d \neq 0$, thus $af = be$. This means that $(a, b) \sim (e, f)$. This shows that $\sim$ is transitive. □

Proof of Theorem 3.73 ($\Rightarrow$) Assume that $\mathbb{Z}/_n$ has zero divisors. Assume, with the expectation of a contradiction, that n is prime. Let $[a], [b] \in \mathbb{Z}/_n$ such that $[a] \neq [0]$, $[b] \neq [0]$, and $[a][b] = [0]$. This means that $[ab] = [0]$, and so $n|ab$. By Euclid's Lemma (Theorem 3.65), this means that $n|a$ or $n|b$. However, this implies that $[a] = [0]$ or $[b] = [0]$, despite that $[a] \neq [0]$ and $[b] \neq [0]$. This contradiction leads us to conclude that our assumption that n is prime is false; n is not prime.

($\Leftarrow$) Assume that n is not prime. In that case, $\exists\, a, b \in \mathbb{Z}$ such that $n = ab$, $0 < a < n$ and $0 < b < n$. We deduce that $[0] = [n] = [ab] = [a][b]$. However, $0 < a < n$ and $0 < b < n$, so $[a] \neq [0]$ and $[b] \neq [0]$. Thus, $[a]$ and $[b]$ are zero divisors of $\mathbb{Z}/_{n}$. $\Box$

Proof of Theorem 3.74 Assume that R has zero divisors. Assume, with the expectation of a contradiction, that R is a field. Let $x, y \in R \setminus \{0\}$ such that $xy = 0$. Since $x \neq 0$ and R is a field, $\exists\, z \in R$ such that $zx = 1$. Therefore,

$$y = 1y = zxy = z0 = 0, \tag{81}$$

despite that $y \neq 0$. This contradiction leads us to conclude that our assumption that R is a field is false; R is not a field. $\Box$

Proof of Theorem 3.75 Let s_1 and s_2 be least upper bounds of T. In that case, s_1 is a least upper bound of T and s_2 is an upper bound of T. This implies that $s_1 \leq s_2$. By similar arguments, one can show that $s_2 \leq s_1$. Thus, $s_1 = s_2$. $\Box$

Proof of Theorem 3.76 Assume, with the expectation of a contradiction, that $\mathbb{Z}/_{n}$ is an ordered ring. Since $\mathbb{Z}/_{n}$ is finite, we know that there exists a maximal element of $\mathbb{Z}/_{n}$. Call this element $[t]$. Take $[m] \in \mathbb{Z}/_{n}$ such that $[m] \neq [t]$. We note that $[m] < [t]$. Since $\mathbb{Z}/_{n}$ is an ordered ring, this means that

$$[t] = [m] + [t - m] < [t] + [t - m] = [2t - m], \tag{82}$$

despite that $[t]$ is the maximal element. This contradiction leads us to conclude that our assumption that $\mathbb{Z}/_{n}$ is an ordered ring is false; $\mathbb{Z}/_{n}$ is not an ordered ring. $\Box$

Proof of Theorem 3.77 Assume, with the expectation of a contradiction, that $x \in \mathbb{Q}$ and $x^2 = 2$. We know that $x = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ such that $n \neq 0$. Assume that $\gcd(m, n) = 1$. We have that $2 = \frac{m^2}{n^2}$. Therefore, $m^2 = 2n^2$, and so m^2 is an even number.

We claim that m is an even number. Assume, with the expectation of a contradiction, that m is not an even number. In that case, $m = 2k + 1$ for some $k \in \mathbb{Z}$.

We deduce that

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1. \tag{83}$$

This is an odd number, despite that m^2 is an even number. This contradiction leads us to conclude that our assumption that m is odd is false; m is an even number.

Since m is even, we know that $\exists\, r \in \mathbb{Z}$ such that $m = 2r$. Therefore, $m^2 = 4r$. We deduce that $2n^2 = m^2 = 4r$, and so $n^2 = 2r$. This implies that n^2 is an even number. By the claim, we deduce that n is also an even number. Ergo, $2|m$ and $2|n$, despite that $\gcd(m,n) = 1$. This contradiction leads us to conclude that our assumption that $x^2 = 2$ is false; $x^2 \neq 2$ for any $x \in \mathbb{Q}$. □

Proof of Theorem 3.78 Assume that $(R,<)$ satisfies the least upper bound property. Let $T \subseteq R$ be nonempty and bounded below in R. This means that $\exists\, \alpha \in R$ such that $\forall\, t \in T$, $\alpha \leq t$. We define the set $-T = \left\{-t \in R \middle| t \in T\right\}$. Since R is an ordered ring, we know that $\forall\, t \in T$, $-t \leq -\alpha$. Therefore, $-T$ is bounded above. By the least upper bound property, $-T$ has a least upper bound, call it $\mu \in R$. We have that $\forall\, t \in T$, $-t \leq \mu$, and so $-\mu \leq t$. This shows that $-\mu$ is a lower bound for T.

Suppose that $\beta \in R$ is a lower bound for T. In that case, $\forall\, t \in T$, $\beta \leq t$. As R is an ordered ring, we deduce that $-t \leq -\beta$, $\forall\, t \in T$. However, this implies that $-\beta$ is an upper bound for $-T$, so since μ is the least upper bound of $-T$, we must have that $\mu \leq -\beta$. Therefore, $\beta \leq -\mu$. This shows that $-\mu$ is the greatest lower bound of T. □

Proof of Theorem 3.79 We produce $f : \mathbb{N} \to \mathbb{Z}$ via

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}. \tag{84}$$

Since f is a bijection, $|\mathbb{N}| = |\mathbb{Z}|$. □

Proof of Theorem 3.80 We define $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ via the following relationship. For each $x \in \mathbb{Q}$, we can write $x = \frac{m}{n}$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. We define $f(x) = (m, n)$.

We claim that f is injective. Let $x_1, x_2 \in \mathbb{Q}$ such that $f(x_1) = f(x_2)$. In that case, $(m_1, n_1) = (m_2, n_2)$ for some $m_1, m_2 \in \mathbb{Z}$ and $n_1, n_2 \in \mathbb{N}$ such that $\gcd(m_1, n_1) = 1$ and $\gcd(m_2, n_2) = 1$. We deduce that $m_1 = m_2$ and $n_1 = n_2$. Ergo, $x_1 = \frac{m_1}{n_1} = \frac{m_2}{n_2} = x_2$.

By the claim, $|\mathbb{Q}| \le |\mathbb{Z} \times \mathbb{N}|$. We know that $|\mathbb{Z}| = |\mathbb{N}|$ by Theorem 3.79. Therefore, $|\mathbb{Z} \times \mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$, and so $|\mathbb{Q}| \le |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. □

Proof of Theorem 3.81 (This is called the Cantor diagonalization argument) Assume, with the expectation of a contradiction, that $(0, 1)$ is countable. In that case, there exists a bijection $f : \mathbb{N} \to (0, 1)$. For each $n \in \mathbb{N}$, we write $f(n)$ in a binary expansion as

$$f(n) = 0.x_{n1}x_{n2}x_{n3}..., \tag{85}$$

where for each $i \in \mathbb{N}$, $x_{ni} \in \{0, 1\}$. For each $n \in \mathbb{N}$ and $i \in \mathbb{N}$, if we define $y_{ni} = 0$ if $x_{ni} = 1$ and $y_{ni} = 1$ if $x_{ni} = 0$. We define $y \in (0, 1)$ via the binary expansion

$$y = 0.y_{11}y_{22}y_{33}.... \tag{86}$$

We notice that for each $y \ne f(1)$, since $y_{11} \ne x_{11}$. At the same time, $y \ne f(2)$, since $y_{22} \ne x_{22}$. Moreover, for each $n \in \mathbb{N}$, $y \ne f(n)$, since $y_{nn} \ne x_{nn}$. Therefore, f is not surjective, despite that f is a bijection. This contradiction leads us to conclude that our assumption that $(0, 1)$ is countable is false; $(0, 1)$ is not countable. □

Proof of Theorem 3.82 Define $f : (0, 1) \to (a, b)$ via $f(x) = (b - a)x + a$. One can show that f is a bijection. Similarly, define $g : (0, 1) \to (c, d)$. One can show that g is a bijection. Thus, $|\,(a, b)\,| = |\,(0, 1)\,| = |\,(c, d)\,|$. □

Proof of Theorem 3.83 One can show that $f : (-1, 1) \to \mathbb{R}$ via $f(x) = \frac{x}{1-x^2}$ is a bijection. □

Proof of Theorem 3.84 Assume, with the expectation of a contradiction, that $\mathbb{R} \setminus \mathbb{Q}$ is countable. In that case, we can say that $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$ is countable, contradicting Theorem 3.83. This contradiction leads us to conclude that our assumption that $\mathbb{R} \setminus \mathbb{Q}$ is countable is false; $\mathbb{R} \setminus \mathbb{Q}$ is uncountable. □

Proof of Theorem 3.85 $(i \Rightarrow ii)$ Assume that $|X| \leq |Y|$. In that case, $\exists\, S \subseteq Y$ such that $X \sim S$. We deduce that there exists a bijection $f_0 : X \to S$. Now, we define the function $\iota : S \to Y$ via $\iota(x) = x$. Since ι is injective, the composition $\iota \circ f_0$ is also injective.

$(ii \Rightarrow iii)$ Assume that there exists an injective function $f : X \to Y$. Let $x_0 \in X$ be arbitrary. Define $g : Y \to X$ via the following relationship. Given $y \in Y$, either $y \in f(X)$ or $y \notin f(X)$. If $y \in f(X)$, then there exists a unique $x \in X$ such that $f(x) = y$. In that case, define $g(y) = x$. If $y \notin f(X)$, then define $g(y) = x_0$. Now g is a surjective function.

$(iii \Rightarrow i)$ Assume that there exists a surjective function $g : Y \to X$. For each $x \in X$, define a particular $y_x \in Y$ such that $g(y_x) = x$. Consider the set $S = \left\{ y_x \in Y \middle| x \in X \right\}$. Now the function $h_1 : X \to S$ via $h_1(x) = y_x$ and the function $h_2 : S \to X$ via $h_2(y_x) = x$ are inverse functions. We deduce that $X \sim S$, and so $|X| \leq |Y|$. □

Proof of Theorem 3.86 Assume, with the expectation of a contradiction, that the cardinality $|\mathcal{P}(X)| \leq |X|$. In that case, by Theorem 3.85, there exists a surjective function $g : X \to \mathcal{P}(X)$. Define the set

$$S = \left\{ x \in X \middle| x \notin g(x) \right\}. \tag{87}$$

Since $S \subseteq X$, we know that $S \in \mathcal{P}(X)$. As g is surjective, we can find some $x_0 \in X$ such that $g(x_0) = S$. We consider two cases: either $x_0 \in S$ or $x_0 \notin S$. In the case that $x_0 \in S$, this means that $x_0 \notin g(x_0) = S$. In the case that $x_0 \notin S$, this means that $x_0 \in g(x_0) = S$. Either way, $x_0 \in S$ and $x_0 \notin S$. This contradiction leads us to conclude that our assumption that $|\mathcal{P}(X)| \leq |X|$ is false; $|\mathcal{P}(X)| > |X|$. □