MA1100 Tutorial

Xiang Sun[1][2]

Dept. Mathematics

November 15, 2009

[1] Email: xiangsun@nus.edu.sg

[2] Corrections are always welcome.

Self-Introduction

Name	Sun Xiang (in English) or 孙祥 (in Chinese) Second year Ph.D student in Dept. Mathematics
Email	xiangsun@nus.edu.sg
Phone	9053 5550
Office	S9a-02-03
MSN	xiangsun.sunny@hotmail.com
QQ	402197754

Introduction

- There are 10 tutorials;
- Take attendance: 2 point for full attendance, and pro-rated for partial attendance;
- Things to do before Tutorial:
  - Read lecture notes and textbook;
  - Try to work through the tutorial problems before attending tutorial classes.
- Things to do after Tutorial:
  - Understand the problems in the tutorial sets;
  - Read lecture notes and textbook again, and understand everything in them.

Schedule of Today

- Review concepts
- Tutorial: 1.6, 1.7, 1.14, 1.26, 1.35, 1.38, 2.4, 2.11, 2.13, 2.21
- Additional material

Sets I

Notations $\{x \in U \mid p(x)\}$, x is a general element, $p(x)$ is the condition in terms of x, U is the universal set;

Relations

- Subsets: $A \subseteq B$ if every element of A is an element of B;
- Equality: $A = B$ if $A \subseteq B$ and $B \subseteq A$;
- Proper subsets: $A \subseteq B$ and $A \neq B$;
- Empty set: $\varnothing$;

Operations

- Power set: the power set of A is the set of all subsets of A, $\mathcal{P}(A) = \{S \subseteq U \mid S \subseteq A\}$
- Intersection: the intersection of A and B is the set of all elements that are in both A and B, $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$
- Union: the union of A and B is the set of all elements that are in A or in B, $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$
- Complement: the complement of A is the set of all elements of U that are not in A, $A^c = \{x \in U \mid x \notin A\}$
- Relative complement: the relative complement of B w.r.t. A is the set of all elements that are in A but not in B

Sets II

Indexed Collection of Sets $A_1, A_2, A_3, \ldots$ are an indexed collection of sets, N is index set

- Intersection: $\bigcap_{n \in N} A_n = A_1 \cap A_2 \cap A_3 \cap \cdots$
- Union: $\bigcup_{n \in N} = A_1 \cup A_2 \cup A_3 \cup \cdots$

Partitions of Sets A is a non-empty set, and S is a collection of subsets of A. S is a partition of A if

- For each $X \in S$, $X \neq \varnothing$, i.e. each part has at least one element;
- For every $X, Y \in S$, if $X \neq Y$, then $X \cap Y = \varnothing$;
- The union of all elements in the collection S is equal to A.

Cartesian Products of Sets The Cartesian product of A and B: $A \times B = \{(a, b) \mid a \in A, b \in B\}$, (a, b) is an ordered pair

Logic

Statements A statement is a sentence that is either true or false (but not both); We denote a statement by capital letters, usually $P, Q, R, \ldots$;

Open Sentences An open sentence is a (mathematical) sentence that involves variables; We denote an open sentence by capital letters with the variables involved, such as $P(n)$, $Q(x, y)$

Logic operators Let P and Q be two statements,

- **Conjunction** $P \wedge Q$, it is true only when both P and Q are true;
- **Disjunction** $P \vee Q$, it is false only when both P and Q are false;
- **Negating** $\sim P$, if P is true, then $\sim P$ is false, and vice versa;
- **Implication** $P \Rightarrow Q$, the rule is false only when the rule is violated.

Necessary and Sufficient If S happens, then T happens, then S is sufficient for T, and T is necessary for S.

Exercise (1.6)

The set $E = \{2x : x \in \mathbb{Z}\}$ can be described by listing its element, namely $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. List the elements of the following sets in a similar manner.

(a) $A = \{2x + 1 : x \in \mathbb{Z}\}$

(b) $B = \{4n : n \in \mathbb{Z}\}$

(c) $C = \{3q + 1 : q \in \mathbb{Z}\}$

Recall

There are two ways to describe a set: enumerating and describing.
$E_1 = \{2x : x \in \mathbb{Z}\}$–describing; $E_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$–enumerating.

Solution.

For item (c), $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,

q	$\cdots$	-2	-1	0	1	2	$\cdots$
$3q+1$	$\cdots$	-5	-2	1	4	7	$\cdots$

Therefore, We get that C can be listed as $\{\ldots, -5, -2, 1, 4, 7, \ldots\}$.
Similarly, $A = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$, and $B = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$. □

Exercise (1.7)

The set $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ of even integers can be described by means of a defining condition by $E = \{y = 2x : x \in \mathbb{Z}\} = \{2x : x \in \mathbb{Z}\}$. Describe the following sets in a similar manner.

(a) $A = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

(b) $B = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

(c) $C = \{1, 8, 27, 64, 125, \ldots\}$

Method

Find the rule of the sequences: For example, $-1, 2, 5, 8, \_, \ldots$. It is an arithmetic sequence.

Solution.

- $A = \{3x + 2 : x \in \mathbb{Z}\}$
- $B = \{5y : y \in \mathbb{Z}\}$
- $C = \{z^3 : z \in \mathbb{N}\}$

Exercise (1.14)

Find $\mathcal{P}\big(\mathcal{P}(\{1\})\big)$ and its cardinality.

Recall

- Power set: the power set of A is the set of all subsets of A, $\mathcal{P}(A) = \{S \subseteq U \mid S \subseteq A\}$;
- Cardinality: the number of elements of set, denote as $|S|$.

Method

List all subsets.

Solution.

For $\{1\}$, its all subsets are $\varnothing$ and $\{1\}$, then $\mathcal{P}(\{1\}) = \big\{\varnothing, \{1\}\big\}$;
For $\big\{\varnothing, \{1\}\big\}$, its all subsets are $\varnothing$, $\{\varnothing\}$, $\{\{1\}\}$, and $\big\{\varnothing, \{1\}\big\}$, therefore

$$\mathcal{P}\big(\mathcal{P}(\{1\})\big) = \big\{\varnothing, \{\varnothing\}, \{\{1\}\}, \{\varnothing, \{1\}\}\big\},$$

and $\big|\mathcal{P}\big(\mathcal{P}(\{1\})\big)\big| = 4$ □

Exercise (1.26)

For a real number r, define $A_r = \{r^2\}$, B_r as the closed interval $[r-1, r+1]$, and C_r as the interval (r, ∞). For $S = \{1, 2, 4\}$, determine

(a) $\bigcup_{\alpha\in S} A_\alpha$ *and* $\bigcap_{\alpha\in S} A_\alpha$

(b) $\bigcup_{\alpha\in S} B_\alpha$ *and* $\bigcap_{\alpha\in S} B_\alpha$

(c) $\bigcup_{\alpha\in S} C_\alpha$ *and* $\bigcap_{\alpha\in S} C_\alpha$

Solution.

For (a): Since $S = \{1, 2, 4\}$, there are three sets A_1, A_2, A_4. By assumption, we have $A_1 = \{1\}$, $A_2 = \{4\}$, $A_4 = \{16\}$. By definition,

$$\bigcup_{\alpha\in S} A_\alpha = A_1 \cup A_2 \cup A_4 = \{1, 4, 16\}, \qquad \bigcap_{\alpha\in S} A_\alpha = A_1 \cap A_2 \cap A_4 = \varnothing.$$

Similarly, $B_1 = [0, 2]$, $B_2 = [1, 3]$, $B_4 = [3, 5]$, and $\bigcup_{\alpha\in S} B_\alpha = [0, 5]$, $\bigcap_{\alpha\in S} B_\alpha = \varnothing$.

$C_1 = (1, \infty)$, $C_2 = (2, \infty)$, $C_4 = (4, \infty)$, and $\bigcup_{\alpha\in S} C_\alpha = (1, \infty)$, $\bigcap_{\alpha\in S} C_\alpha = (4, \infty)$. □

Exercise (1.35)

Give an example of a set A with $|A| = 4$ and two disjoint partitions S_1 and S_2 of A with $|S_1| = |S_2| = 3$.

Recall

Partition ▸ Click here

Solution.

1. Let $A = \{a, b, c, d\}$, a, b, c, d are different. Now we want to seek some partition S consisting of 3 subsets;
2. There are 6 partitions each of which consists of 3 subsets: $\{\{a, b\}, \{c\}, \{d\}\}$, $\{\{a, c\}, \{b\}, \{d\}\}$, $\{\{a, d\}, \{b\}, \{c\}\}$, $\{\{b, c\}, \{a\}, \{d\}\}$, $\{\{b, d\}, \{a\}, \{c\}\}$, $\{\{c, d\}, \{a\}, \{b\}\}$;
3. Then just choose 2 of them, such that they are disjoint, for example $\{\{a, b\}, \{c\}, \{d\}\}$ and $\{\{c, d\}, \{a\}, \{b\}\}$.

□

Exercise (1.38)

Give an example of a partition of $\mathbb{N}$ into three subsets.

Solution.

Similar with the former exercise. There are many partitions, such as $\{\{1\}, \{2\}, \{3, 4, \ldots\}\}$. □

Exercise (2.4)

The following is an open sentence over the domain $\mathbb{R}$*:* $P(x) : x(x-1) = 6$.

(a) *For what values of* x *is* $P(x)$ *a true statement?*

(b) *For what values of* x *is* $P(x)$ *a false statement?*

Solution.

$P(x)$ is true iff x satisfies the equation $x(x-1) = 6$. Solving the equation, we find $x = 3$ or $x = -2$, that is, $P(x)$ is true iff $x = 3$ or $x = -2$.

(a) When $x = 3$ or $x = -2$, $P(x)$ is a true statement;

(b) When $x \neq 3$ and $x \neq -2$, $P(x)$ is a false statement;

□

Exercise (2.11)

For the sets $A = \{1, 2, \ldots, 10\}$ *and* $B = \{2, 4, 6, 9, 12, 25\}$, *consider the statements:* $P : A \subseteq B$, $Q : |A - B| = 6$. *Determine which of the following statements are true:*

(a) $P \vee Q$;
(b) $P \vee (\sim Q)$;
(c) $P \wedge Q$;
(d) $(\sim P) \wedge Q$;
(e) $(\sim P) \vee (\sim Q)$.

Recall

Logic Operators ▸ Click here

Method

Use definitions.

Solution.

First, we get that P is false since $1 \in A$ but $1 \notin B$; Also we get that Q is true since $A - B = \{1, 3, 5, 7, 8, 10\}$. Then we have

(a) $P \vee Q$ is true;
(b) $P \vee (\sim Q)$ is false;
(c) $P \wedge Q$ is false;
(d) $(\sim P) \wedge Q$ is true;
(e) $(\sim P) \vee (\sim Q)$ is true;

Exercise (2.13)

Let $S = \{1, 2, \ldots, 6\}$ and let $P(A) : A \cap \{2, 4, 6\} = \varnothing$ and $Q(A) : A \neq \varnothing$ be open sentence over the domain $\mathcal{P}(S)$.

(a) *Determine all $A \in \mathcal{P}(S)$ for which $P(A) \wedge Q(A)$ is true.*

(b) *Determine all $A \in \mathcal{P}(S)$ for which $P(A) \vee (\sim Q(A))$ is true.*

(c) *Determine all $A \in \mathcal{P}(S)$ for which $(\sim P(A)) \wedge (\sim Q(A))$ is true.*

Solution.

(a) $P(A) \wedge Q(A)$ is true $\Rightarrow$ (and) $\begin{cases} P(A) \text{ is true} & \Rightarrow A \cap \{2, 4, 6\} = \varnothing \\ Q(A) \text{ is true} & \Rightarrow A \neq \varnothing \end{cases}$ $\Rightarrow A$ must be a non-empty subset of $\{1, 3, 5\}$;

(b) $P(A) \vee (\sim Q(A))$ is true $\Rightarrow$ (or) $\begin{cases} P(A) \text{ is true} \Rightarrow A \cap \{2, 4, 6\} = \varnothing \\ Q(A) \text{ is false} \Rightarrow A = \varnothing \end{cases}$ $\Rightarrow A$ must be a subset of $\{1, 3, 5\}$.

(c) $(\sim P(A)) \wedge (\sim Q(A))$ is true $\Rightarrow$ (and) $\begin{cases} P(A) \text{ is false} \Rightarrow A \cap \{2, 4, 6\} \neq \varnothing \\ Q(A) \text{ is false} \Rightarrow A = \varnothing \end{cases}$ $\Rightarrow$ contradiction, there is no such A.

□

Exercise (2.21)

In each of the following, two open sentences $P(x, y)$ and $Q(x, y)$ are given, where the domain of both x and y is $\mathbb{Z}$. Determine the truth value of $P(x, y) \Rightarrow Q(x, y)$ for the given values of x and y.

(a) $P(x, y) : x^2 - y^2 = 0$ *and* $Q(x, y) : x = y$. $(x, y) \in \{(1, -1), (3, 4), (5, 5)\}$.

(b) $P(x, y) : |x| = |y|$ *and* $Q(x, y) : x = y$. $(x, y) \in \{(1, 2), (2, -2), (6, 6)\}$.

(c) $P(x, y) : x^2 + y^2 = 1$ *and* $Q(x, y) : x + y = 1$.
$(x, y) \in \{(1, -1), (-3, 4), (0, -1), (1, 0)\}$.

Solution.

(a) When $(x, y) = (1, -1)$, $P(x, y)$ is true, $Q(x, y)$ is false, then $P(x, y) \Rightarrow Q(x, y)$ is false; Similarly, truth for $(x, y) = (3, 4)$ and $(x, y) = (5, 5)$;

(b) Truth for $(x, y) = (1, 2)$ and $(x, y) = (6, 6)$, false for $(x, y) = (2, -2)$;

(c) Truth for $(x, y) = (1, -1)$, $(x, y) = (-3, 4)$ and $(x, y) = (1, 0)$, false for $(x, y) = (0, -1)$.

□

Russell's paradox

Exercise

Usually, for any formal criterion, a set exists whose members are those objects (and only those objects) that satisfy the criterion, i.e. $\{x \in U : p(x)\}$ *is a set. Whether does there exist an object with the form* $\{x \in U : p(x)\}$*, which is not a set?*

Russell's paradox

Solution.

This question is disproved by a set containing exactly the sets that are not members of themselves. If such a set qualifies as a member of itself, it would contradict its own definition as a set containing sets that are not members of themselves. On the other hand, if such a set is not a member of itself, it would qualify as a member of itself by the same definition. This contradiction is Russell's paradox.

Let $A = \{X \in U : X \notin X\}$, U is the collection of all sets.

- If $A \in A$, then A does not satisfy $X \notin X$, i.e. $A \notin A$, contradiction;
- If $A \notin A$, then A satisfies $X \notin X$, i.e. $A \in A$, contradiction.

Therefore, the definition is not well-defined, and the error is from $U (\Rightarrow U$ is not a set).

□

Exercise

How to solve this problem?

Solution.

- Roughly speaking, the method is giving some restrictions on the definition of set.
- Russell's paradox (also known as Russell's antinomy), discovered by Bertrand Russell in 1901. In 1908, two ways of avoiding the paradox were proposed, Russell's type theory and Ernst Zermelo's axiomatic set theory, the first constructed axiomatic set theory. Zermelo's axioms went well beyond Frege's axioms of extensionality and unlimited set abstraction, and evolved into the now-canonical Zermelo-Fraenkel set theory (ZF).
- For more information, you can wiki "Russell's paradox".

Schedule of Today

- Review concepts
- Tutorial: 2.31(contradiction), 2.32(tautology), 2.37(equivalence), 2.40(negation), 2.48, 2.49(negation), 2.62(equivalence), 2.67, 2.68

Logic II(lecture 5)

Biconditional P if and only if Q, that is $P \Leftrightarrow Q$.

Converse $Q \Rightarrow P$ is called the converse of $P \Rightarrow Q$.

Contrapositive $(\sim Q) \Rightarrow (\sim P)$ is called the contrapositive of $P \Rightarrow Q$.

Tautology A logical expression that is always true is called a tautology.

Contradiction A logical expression that is always false is called a contradiction.

Logical Equivalence Two logical expressions are said to be logically equivalent to each other if they have the same truth value.

De Morgan's Law $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q), \quad \sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q).$

Distributive Law

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R), \quad P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R).$$

Implication as disjunction $P \Rightarrow Q \equiv (\sim P) \vee Q.$

Negation of implication $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q).$

Implication with disjunction $P \Rightarrow (Q \vee R) \equiv (P \wedge (\sim Q)) \Rightarrow R.$

Logic III(lecture 6)

Universal quantifier The phrase "for each", "for every", "for all", ... is called a universal quantifier. Notation: $\forall$, say "for all".

Existential quantifier The phrase "there exists", "there is", ... is called a existential quantifier. Notation: $\exists$, say "there exist".

$\forall$ vs $\exists$

$P(x)$ true for	$(\forall x)P(x)$	$(\exists x)P(x)$
all the x	True	True
only some x	False	True
none of the x	False	False

Two quantifiers $(\forall x)(\forall y)P(x,y)$, $(\exists x)(\exists y)P(x,y)$, $(\forall y)(\exists x)P(x,y)$, $(\exists x)(\forall y)P(x,y)$.

Negation with quantifier $\sim(\forall x)P(x) \equiv (\exists x)(\sim P(x))$, $\sim(\exists x)P(x) \equiv (\forall x)(\sim P(x))$,
$\sim(\forall x)(\exists y)P(x,y) \equiv (\exists x)(\forall y)(\sim P(x,y))$,
$\sim(\exists x)(\forall y)P(x,y) \equiv (\forall x)(\exists y)(\sim P(x,y))$,
$\sim(\forall x)(\forall y)P(x,y) \equiv (\exists x)(\exists y)(\sim P(x,y))$,
$\sim(\exists x)(\exists y)P(x,y) \equiv (\forall x)(\forall y)(\sim P(x,y))$

Exercise (2.31)

For statements P and Q, show that $\big(P \wedge (\sim Q)\big) \wedge (P \wedge Q)$ is a contradiction.

Recall

A logical expression that is always false is called a contradiction. How to prove that a statement is contradiction?
General method: It suffices to show that the statement is false for all combinations.

Proof of Method 1.

The compound statement $\big(P \wedge (\sim Q)\big) \wedge (P \wedge Q)$ is a contradiction since it is false for all combinations of truth values for the component statements P and Q. See the truth table below.

P	Q	$\sim Q$	$P \wedge Q$	$P \wedge (\sim Q)$	$\big(P \wedge (\sim Q)\big) \wedge (P \wedge Q)$
T	T	F	T	F	F
T	F	T	F	T	F
F	T	F	F	F	F
F	F	T	F	F	F

□

Exercise (2.31)

For statements P and Q, show that $\big(P \wedge (\sim Q)\big) \wedge (P \wedge Q)$ is a contradiction.

Proof of Method 2.

1. By associated law, we have

$$\big(P \wedge (\sim Q)\big) \wedge (P \wedge Q) \equiv P \wedge (\sim Q) \wedge P \wedge Q.$$

2. By commutative law, we have

$$P \wedge (\sim Q) \wedge P \wedge Q \equiv P \wedge P \wedge (\sim Q) \wedge Q.$$

3. Also by associated law, we have

$$P \wedge P \wedge (\sim Q) \wedge Q \equiv (P \wedge P) \wedge (Q \wedge (\sim Q)) \equiv P \wedge (Q \wedge (\sim Q)).$$

4. Since $Q \wedge (\sim Q)$ is always false, we have that $P \wedge (Q \wedge (\sim Q))$ is contradiction, i.e. $\big(P \wedge (\sim Q)\big) \wedge (P \wedge Q)$ is a contradiction.

$\square$

Exercise (2.32)

For statements P and Q, show that $\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$ is a tautology. Then state $\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$ in words. (This is an important logical argument form, called modus ponens.)

Recall

A logical expression that is always true is called a tautology. How to prove that a statement is tautology?
General method: It suffices to show that the statement is true for all combinations.

Proof of Method 1.

The compound statement $\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$ is a tautology since it is true for all combinations of truth values for the component statements P and Q. See the truth table below.

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

$\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$: If P and P implies Q, then Q. □

Exercise (2.32)

For statements P and Q, show that $\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$ is a tautology. Then state $\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$ in words. (This is an important logical argument form, called modus ponens.)

Proof of Method 2.

1. Let $R = P \wedge (P \Rightarrow Q)$, we want to show $R \Rightarrow Q$ is always true, that is, the cases in which $R \Rightarrow Q$ is false will not happen.
2. $R \Rightarrow Q$ is false only when R is true and Q is false. If we prove that there is a contradiction, i.e., this case will not happen, then it is done.
3. Suppose that R is true and Q is false.
4. Since $R = P \wedge (P \Rightarrow Q)$, we have that P and $P \Rightarrow Q$ are both true.
5. We get that Q is true. It is a contradiction. Therefore, this case will not happen, that is, the statement is a tautology.

□

Exercise (2.37)

For statements P and Q, show that $(\sim Q) \Rightarrow (P \wedge (\sim P))$ and Q are logically equivalent.

Recall

Two logical statements are equivalent if they have the same truth value. How to prove that two statements are equivalent?
General method: It suffices to show that two statements have same truth value.

Proof of Method 1.

The statements Q and $(\sim Q) \Rightarrow \big(P \wedge (\sim P)\big)$ are logically equivalent since they have the same truth values for all combinations of truth values for the component statements P and Q. See the truth table below.

P	Q	$\sim P$	$\sim Q$	$P \wedge (\sim P)$	$(\sim Q) \Rightarrow \big(P \wedge (\sim P)\big)$
T	T	F	F	F	T
T	F	F	T	F	F
F	T	T	F	F	T
F	F	T	T	F	F

□

Exercise (2.37)

For statements P and Q, show that $(\sim Q) \Rightarrow (P \wedge (\sim P))$ and Q are logically equivalent.

Proof of Method 2.

1. Since $P \wedge (\sim P)$ is always false, it is enough to consider Q.
2. When Q is true, then $(\sim Q) \Rightarrow (P \wedge (\sim P))$ is true, the same as Q.
3. When Q is false, then $(\sim Q) \Rightarrow (P \wedge (\sim P))$ is false, the same as Q.

□

Exercise (2.40)

Write negations of the following open sentences:

(a) *Either* $x = 0$ *or* $y = 0$.

(b) *The integers* a *and* b *are both even.*

Recall

De Morgan's laws: $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q), \quad \sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$.
Roughly speaking, we can consider $\sim$ as an operator, which changes $\wedge$(and) to $\vee$(or), and changes $\vee$(or) to $\wedge$(and).

Solution.

(a) Let $P : x = 0$ and $Q : y = 0$. Then the statement can be expressed as $P \vee Q$. Therefore the negation is $(\sim P) \wedge (\sim Q)$, i.e. both $x \neq 0$ and $y \neq 0$.

(b) Let $P : a$ is even and $Q : b$ is even, then the statement can be expressed as $P \wedge Q$. Therefore the negation is $(\sim P) \vee (\sim Q)$, i.e. either a is odd or b is odd.

□

Exercise (2.48)

Determine the truth value of each of the following statements.

(a) $\exists x \in \mathbb{R},\ x^2 - x = 0.$
(b) $\forall n \in \mathbb{N},\ n + 1 \geqslant 2.$
(c) $\forall x \in \mathbb{R},\ \sqrt{x^2} = x.$
(d) $\exists x \in \mathbb{Q},\ 3x^2 - 27 = 0.$
(e) $\exists x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y + 3 = 8.$
(f) $\forall x, y \in \mathbb{R},\ x + y + 3 = 8.$
(g) $\exists x, y \in \mathbb{R},\ x^2 + y^2 = 9.$
(h) $\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x^2 + y^2 = 9.$

Recall

	True	False
$(\forall x) P(x)$	$P(x)$ is true for all x	$P(x)$ is false for some x
$(\exists x) P(x)$	$P(x)$ is true for some x	$P(x)$ is false for all x
$(\forall x)(\forall y) P(x, y)$	$P(x, y)$ is true for all x and all y	$P(x, y)$ is false for some x or some y
$(\exists x)(\exists y) P(x, y)$	$P(x, y)$ is true for some x and some y	$P(x, y)$ is false for all x and y
$(\exists x)(\forall y) P(x, y)$	For some x, $P(x, y)$ is true for all y	For any x, $P(x, y)$ is false for some y
$(\forall x)(\exists y) P(x, y)$	For any x, $P(x, y)$ is true for some y	For some x, $P(x, y)$ is false for all y

Solution.

(a) True. 0 and 1 are the solutions of $x^2 - x = 0$.

(b) True. For any $n \in \mathbb{N}$, we have $n \geqslant 1$ since $\mathbb{N} = \{1, 2, 3, \ldots\}$. Therefore $n + 1 \geqslant 2$.

(c) False. Let $x < 0$, then $\sqrt{x^2} = -x \neq x$.

(d) True. 3 and -3 are the solutions of $3x^2 = 27$.

(e) True. $x = 0, y = 5$ is the solution of $x + y + 3 = 8$.

(f) False. $x = 0, y = 0$ does not satisfy $x + y + 3 = 8$.

(g) True. $x = 0, y = 3$ is the solution of $x^2 + y^2 = 9$.

(h) False. $x = 0, y = 0$ does not satisfy $x^2 + y^2 = 9$.

□

Exercise (2.49)

The statement

$$\textit{For every integer } m, \textit{ either } m \leqslant 1 \textit{ or } m^2 \geqslant 4.$$

can be expressed using a quantifier as:

$$\forall m \in \mathbb{Z}, m \leqslant 1 \textit{ or } m^2 \geqslant 4.$$

Do this for the statements in parts (a) and (b).

(a) *There exist integers a and b such that both $ab < 0$ and $a + b > 0$.*

(b) *For all real numbers x and y, $x \neq y$ implies that $x^2 + y^2 > 0$.*

(c) *Express in words the negations of the statements in (a) and (b).*

(d) *Using quantifiers, express in symbols the negations of the statements in both (a) and (b).*

Recall

- Roughly speaking, $\sim$ changes $\forall$ to $\exists$, and changes $\exists$ to $\forall$.
- Implication as disjunction: $P \Rightarrow Q \equiv (\sim P) \vee Q$.
- Negation of implication: $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q)$.

Solution.

(a) $\exists a, b \in \mathbb{Z},\ ab < 0$ and $a + b > 0$.

(b) $\forall x, y \in \mathbb{R},\ x \neq y$ implies $x^2 + y^2 > 0$.

(c-d)

(a) $\forall a, b \in \mathbb{Z}$, either $ab \geqslant 0$ or $a + b \leqslant 0$, that is, for all integers a and b, either $ab \geqslant 0$ or $a + b \leqslant 0$.

(b) $\exists x, y \in \mathbb{R},\ x \neq y$ and $x^2 + y^2 \leqslant 0$, that is, there exist real numbers x and y such that $x \neq y$ and $x^2 + y^2 \leqslant 0$.
Besides, the negation of (b) can be: $\exists x, y \in \mathbb{R},\ x \neq y$ and $x^2 + y^2 = 0$ since $x^2 + y^2 \geqslant 0$ for all $x, y \in \mathbb{R}$.

Exercise (2.62)

(a) *For statements* P, Q, *and* R, *show that*

$$\big((P \wedge Q) \Rightarrow R\big) \equiv \big((P \wedge (\sim R)) \Rightarrow (\sim Q)\big).$$

(b) *For statements* P, Q, *and* R, *show that*

$$\big((P \wedge Q) \Rightarrow R\big) \equiv \big((Q \wedge (\sim R)) \Rightarrow (\sim P)\big).$$

Proof of Method 1.

The logical expressions are said to be locally equivalent to each other if they have the same truth value.

Part(a):

P	Q	R	$\sim Q$	$\sim R$	$P \wedge Q$	$P \wedge (\sim R)$	$\big((P \wedge Q) \Rightarrow R\big)$	$\big((P \wedge (\sim R)) \Rightarrow (\sim Q)\big)$
T	T	T	F	F	T	F	T	T
T	F	T	T	F	F	F	T	T
F	T	T	F	F	F	F	T	T
F	F	T	T	F	F	F	T	T
T	T	F	F	T	T	T	F	F
T	F	F	T	T	F	T	T	T
F	T	F	F	T	F	F	T	T
F	F	F	T	T	F	F	T	T

Part(b):

P	Q	R	$\sim P$	$\sim R$	$P \wedge Q$	$Q \wedge (\sim R)$	$\big((P \wedge Q) \Rightarrow R\big)$	$\big((Q \wedge (\sim R)) \Rightarrow (\sim P)\big)$
T	T	T	F	F	T	F	T	T
T	F	T	F	F	F	F	T	T
F	T	T	T	F	F	F	T	T
F	F	T	T	F	F	F	T	T
T	T	F	F	T	T	T	F	F
T	F	F	F	T	F	F	T	T
F	T	F	T	T	F	T	T	T
F	F	F	T	T	F	F	T	T

□

Proof of Method 2.

(a)

$$\begin{aligned}
(P \wedge Q) \Rightarrow R &\equiv \sim (P \wedge Q) \vee R && \text{by implication as disjunction} \\
&\equiv (\sim P) \vee (\sim Q) \vee R && \text{by De Morgan's law} \\
(P \wedge (\sim R)) \Rightarrow (\sim Q) &\equiv \sim (P \wedge (\sim R)) \vee (\sim Q) && \text{by implication as disjunction} \\
&\equiv (\sim P) \vee R \vee (\sim Q) && \text{by De Morgan's law} \\
&\equiv (\sim P) \vee (\sim Q) \vee R && \text{by commutative law}
\end{aligned}$$

Therefore, we have $\big((P \wedge Q) \Rightarrow R\big) \equiv \big((P \wedge (\sim R)) \Rightarrow (\sim Q)\big)$.

(b)

1. Let $Q' = P$ and $P' = Q$, then the statement can be written as $\big((Q' \wedge P') \Rightarrow R\big) \equiv \big((P' \wedge (\sim R)) \Rightarrow (\sim Q')\big)$.
2. By commutative law, we have $\big((P' \wedge Q') \Rightarrow R\big) \equiv \big((P' \wedge (\sim R)) \Rightarrow (\sim Q')\big)$.
3. Apply part (a).

□

Exercise (2.67)

Do there exist a set S of cardinality 2 and a set $\{P(n), Q(n), R(n)\}$ of three open sentences over the domain S such that the implications $P(a) \Rightarrow Q(a)$, $Q(b) \Rightarrow R(b)$, and $R(c) \Rightarrow P(c)$ are true, where $a, b, c \in S$, and (2) the converses of the implications in (1) are false? Necessarily, at least two of these elements a, b.

Solution.

1. If $Q(a) \Rightarrow P(a)$, $R(b) \Rightarrow Q(b)$, and $P(c) \Rightarrow R(c)$ are false, then $Q(a), R(b), P(c)$ must be true, and $P(a), Q(b), R(c)$ must be false.
2. Since $|S| = 2$, there are at least two of a, b, c which are same.
3. If $a = b$, since $Q(a)$ is true and $Q(b)$ is false, it is a contradiction.
4. If $a = c$, since $P(c)$ is true and $P(a)$ is false, it is a contradiction.
5. If $b = c$, since $R(b)$ is true and $R(c)$ is false, it is a contradiction.
6. Therefore, there does not exist such set S.

Exercise (2.68)

Let $A = \{1, 2, \ldots, 6\}$ *and* $B = \{1, 2, \ldots, 7\}$. *For* $x \in A$, *let* $P(x) : 7x + 4$ *is odd. For* $y \in B$, *let* $Q(y) : 5y + 9$ *is odd. Let*

$$S = \{(P(x), Q(y)) : x \in A, y \in B, P(x) \Rightarrow Q(y) \text{ is false}\}.$$

What is $|S|$*?*

Recall

For given x_0, $P(x_0)$ is a sentence, not a truth value.

Solution.

1. $P(x)$ is true for $x = 1, 3, 5$ and false for $x = 2, 4, 6$.
2. $Q(y)$ is true for $y = 2, 4, 6$ and false for $y = 1, 3, 5, 7$.
3. $P(x) \Rightarrow Q(y)$ is false if $P(x)$ is true and $Q(y)$ is false. Thus $S = \{(P(x), Q(y) : x = 1, 3, 5, y = 1, 3, 5, 7\} = \{P(x) : x = 1, 3, 5\} \times \{Q(y) : y = 1, 3, 5, 7\}$, and $|S| = 3 \times 4 = 12$.

□

Schedule of Today

- Review concepts
- Tutorial: 3.10(parity), 3.18(parity, biconditional, direct proof, contrapositive), 3.20(by cases), 3.22(parity), 3.27, 3.28, 3.29, 4.4(congruent, by cases), 4.12(contrapositive, by cases), 4,15(congruent)

True statements and Proof

True statements

- Definition: Giving the precise meaning of a word or phase that represents some object, property or other concepts.
- Axiom: Basic properties that are regarded as true statement without needing a proof is called an axiom.
- Theorem, lemma, corollary, proposition (need proofs).
- Axioms, Definitions $\Rightarrow$ Theorems, Lemmas, Propositions.

Proof

- Direct proof: Starting from hypothesis P, using some true statements to get conclusion Q.
- Proof by contrapositive: $P \Rightarrow Q \equiv (\sim Q) \Rightarrow (\sim P)$.
- Proof by cases: for convenience, we usually split the assumption to several cases, then prove every case.
- Disjunction in conclusion:
  $(P \Rightarrow (Q \vee R)) \equiv ((P \wedge (\sim Q)) \Rightarrow R)$.
  Advantage: more conditions.
- Proving biconditionals: $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Integers

- Basic properties of $(\mathbb{Z}, +, \cdot)$:
  - Identity: $n + 0 = n$ and $n \cdot 1 = n$;
  - Inverse: $n + (-n) = 0$, but the inverse for multiplication does not exist except $n = \pm 1$;
  - Commutative: $n + m = m + n$ and $m \cdot n = n \cdot m$;
  - Associative: $(m + l) + n = m + (l + n)$ and $(m \cdot l) \cdot n = m \cdot (l \cdot n)$;
  - Distributive: $m \cdot (l + n) = m \cdot l + m \cdot n$, and $(m + l) \cdot n = m \cdot n + l \cdot n$;
- Closure: $\mathbb{Z}$ is closed under $\begin{cases} \text{addition} & m + n \\ \text{multiplication} & m \cdot n \end{cases} \in \mathbb{Z}$ for any $m, n \in \mathbb{Z}$.
- Parity: n is $\begin{cases} \text{odd} \\ \text{even} \end{cases}$, iff there exists an integer m, such that $n = \begin{cases} 2m + 1 \\ 2m \end{cases}$.

  There are some facts:
  - odd$\pm$odd=even, odd$\pm$even=odd, even$\pm$even=even. (By definition)
  - n is even iff n^2 is even; (Theorem 3.12)
  - n is odd iff n^2 is odd; (Contrapositive of Theorem 3.12)
  - ab is even iff a is even or b is even. (Theorem 3.17)
  - ab is odd iff a is odd and b is odd. (Contrapositive of Theorem 3.17)

Integers

- Divisibility: m divides n if there exists an integer q, such that $n = mq$.
  Notation: $m \mid n$, and we say that m is divisor.
  Negation: m does not divide n if for any integer q, $n \neq mq$. Notation: $m \nmid n$.
- Congruence: Let a, b and n be integers with $n > 1$. If n divides $a - b$, we say that a is congruent to b modulo n. Notation: $a \equiv b \pmod{n}$.
  If $a \equiv b \pmod{n}$, then $a = b + nk$ for some integer k.
- Relation: Let a and n be integers with $n > 1$. $a \equiv 0 \pmod{n}$ iff $n \mid a$.
- Division Algorithm[3]: Given two integers a and d, with $d \neq 0$. There exist unique integers q and r such that $a = qd + r$ and $0 \leqslant r < |d|$, where $|d|$ denotes the absolute value of d. q is called the quotient, r is called the remainder, d is called the divisor, and a is called the dividend.
  That is, for any integers a and d (here we assume that d is positive), we have that a can be expressed as $a = qd, a = qd + 1, \ldots,$ or $a = qd + (d - 1)$ for some integer q.
  For example, let $d = 3$, then every integer x can be expressed as $x = 3q$, $x = 3q + 1$, or $x = 3q + 2$ for some integer q.

[3] Ref Theorem 11.4 on page 247

Real Numbers

- Absolute value: $|x| = \begin{cases} x, & \text{if } x \geqslant 0; \\ -x, & \text{if } x < 0. \end{cases}$
- Triangle inequality: $|x+y| \leqslant |x| + |y|$.

Proof.
By definition, we have $-|x| \leqslant x \leqslant |x|$ and $-|y| \leqslant y \leqslant |y|$, then $-(|x| + |y|) \leqslant x+y \leqslant |x| + |y|$, also by definition, we have $|x+y| \leqslant |x| + |y|$. □

- Triangle inequality: $|x-y| \geqslant |x| - |y|$.

Exercise (3.10)

Let $x \in \mathbb{Z}$. Prove that if 2^{2x} is an odd integer, then 4^x is an odd integer.

Proof.

For any $x \in \mathbb{Z}$, we have

$$2^{2x} = \left(2^2\right)^x = 4^x.$$

Therefore 4^x is odd iff 2^{2x} is odd. □

Exercise (3.18)

Let $n \in \mathbb{Z}$. Prove that $(n+1)^2 - 1$ is even if and only if n is even.

Proof of Method 1.

There are two directions to be proved:

"If" Suppose that n is even, we want to show that $(n+1)^2 - 1$ is even. There are two methods to prove it:

- First we use a direct proof: Let $n = 2k$ where k is an integer. Then $(n+1)^2 - 1 = 4k^2 + 4k = 2(2k^2 + 2k)$ is even.
- Also we can use a proof by contrapositive: assume that $(n+1)^2 - 1$ is odd, we want to show that n is odd: $(n+1)^2 - 1 = n(n+2)$ is odd, then both n and $n+2$ are odd (by contrapositive of Thm 3.17).

"Only if" Suppose that $(n+1)^2 - 1$ is even, we want to show that n is even. There are also two methods to prove it:

- First we use a direct proof: Since $(n+1)^2 - 1 = n(n+2)$ is even, we have that n is even or $n+2$ is even. If n is even, okay, there is nothing to prove; if $n+2$ is even, let $n+2 = 2k$, then $n = 2(k-1)$ is even.
- Also we can use a proof by contrapositive: assume that n is odd, we want to show that $(n+1)^2 - 1$ is odd: Let $n = 2m+1$, then $(n+1)^2 - 1 = 4m^2 + 8m + 3$ is odd.

Exercise (3.18)

Let $n \in \mathbb{Z}$. Prove that $(n+1)^2 - 1$ is even if and only if n is even.

Proof of Method 2.

1. We have $(n+1)^2 - 1 = n^2 + 2n + 1 - 1 = n^2 + 2n$.
2. Since $2n$ is always even, $(n+1)^2 - 1$ is even if and only if n^2 is even.
3. n^2 is even if and only if n is even. (By theorem 3.12)

□

Exercise (3.20)

Prove that if $n \in \mathbb{Z}$, then $n^3 - n$ is even.

Recall

This question is about parity, then we will split its assumptions to some cases.

Proof of Method 1.

Let $n \in \mathbb{Z}$. We consider two cases.

1. n is even. Then $n = 2a$ for some integer a. Thus $n^3 - n = 8a^3 - 2a = 2(4a^3 - a)$. Since $4a^3 - a$ is an integer, $n^3 - n$ is even.
2. n is odd. Then $n = 2b + 1$ for some integer b. Observe that

$$\begin{aligned} n^3 - n &= (2b+1)^3 - (2b+1) \\ &= 8b^3 + 12b^2 + 6b + 1 - 2b - 1 \\ &= 8b^3 + 12b^2 + 4b \\ &= 2(4b^3 + 6b^2 + 2b) \end{aligned}$$

Since $4b^3 + 6b^2 + 2b$ is an integer, $n^3 - n$ is even.

□

Exercise (3.20)

Prove that if $n \in \mathbb{Z}$, then $n^3 - n$ is even.

Proof of Method 2.

Let $n \in \mathbb{Z}$, then $n^3 - n = n(n+1)(n-1)$.

- If n is odd, then both $n-1$ and $n+1$ are even, therefore $n^3 - n$ is even (By Theorem 3.17);
- If n is even, then there is nothing to prove since even·integer=even (By Theorem 3.17).

□

Exercise (3.22)

Let $a, b \in \mathbb{Z}$. Prove that if ab is odd, then $a^2 + b^2$ is even.

Proof.

- By theorem 3.17: ab is even iff a is even or b is even, we have that ab is odd iff a is odd and b is odd (by contrapositive).
- By theorem 3.12: n^2 is even iff n is even, we have that both a^2 and b^2 are odd (also by contrapositive).
- Since odd$\pm$odd=even, we have that $a^2 + b^2$ is even.

□

Exercise (3.27)

Below is a proof of a result.
Proof: We consider two cases.

- a *and* b *are even. Then* $a = 2r$ *and* $b = 2s$ *for some integers* r *and* s*. Thus*

$$a^2 - b^2 = (2r)^2 - (2s)^2 = 4r^2 - 4s^2 = 2(2r^2 - 2s^2).$$

  Since $2r^2 - 2s^2$ *is an integer,* $a^2 - b^2$ *is even.*

- a *and* b *are odd. Then* $a = 2r + 1$ *and* $b = 2s + 1$ *for some integers* r *and* s*. Thus*

$$\begin{aligned} a^2 - b^2 &= (2r+1)^2 - (2s+1)^2 = (4r^2 + 4r + 1) - (4s^2 + 4s + 1) \\ &= 4r^2 + 4r - 4s^2 - 4s = 2(2r^2 + 2r - 2s^2 - 2s). \end{aligned}$$

  Since $2r^2 + 2r - 2s^2 - 2s$ *is an integer,* $a^2 - b^2$ *is even.*

Which of the following is being proved?

1. *Let* $a, b \in \mathbb{Z}$*. Then* a *and* b *are of the same parity if and only if* $a^2 - b^2$ *is even.*
2. *Let* $a, b \in \mathbb{Z}$*. Then* $a^2 - b^2$ *is even.*
3. *Let* $a, b \in \mathbb{Z}$*. If* a *and* b *are of the same parity, then* $a^2 - b^2$ *is even.*
4. *Let* $a, b \in \mathbb{Z}$*. If* $a^2 - b^2$ *is even, then* a *and* b *are of the same parity.*

Method

For these questions, we focus on the assumptions and conclusions, and no need to check the proof.

Solution.

- There is only one direction, then (1) is not proved.
- There are two cases: a, b are both even or a, b are both odd, then (2) is not proved.
- (3) is proved. Since (4) is the converse of (3), (4) is not proved.

□

Exercise (3.28)

Below is given a proof of a result. What result is being proved?
Proof: Assume that x *is even. Then* $x = 2a$ *for some integer* a*. So*

$$3x^2 - 4x - 5 = 3(2a)^2 - 4(2a) - 5 = 12a^2 - 8a - 5 = 2(6a^2 - 4a - 3) + 1.$$

Since $6a^2 - 4a - 3$ *is an integer,* $3x^2 - 4x - 5$ *is odd.*
For the converse, assume that x *is odd. So* $x = 2b + 1$*, where* $b \in \mathbb{Z}$*. Therefore,*

$$\begin{aligned} 3x^2 - 4x - 5 &= 3(2b+1)^2 - 4(2b+1) - 5 = 3(4b^2 + 4b + 1) - 8b - 4 - 5 \\ &= 12b^2 + 4b - 6 = 2(6b^2 + 2b - 3). \end{aligned}$$

Since $6b^2 + 2b - 3$ *is an integer,* $3x^2 - 4x - 5$ *is even.*

Solution.

- There are two parts of the proof:
  - The first part: x is even $\Rightarrow 3x^2 - 4x - 5$ is odd;
  - The second part: x is odd $\Rightarrow 3x^2 - 4x - 5$ is even; This statement is equivalent to its contrapositive: x is even $\Leftarrow 3x^2 - 4x - 5$ is odd.
- Therefore, the result which has been proved is that for any integer x, x is even if and only if $3x^2 - 4x - 5$ is odd.
- This can also be restated as: Let $x \in \mathbb{Z}$. Then x is odd if and only if $3x^2 - 4x - 5$ is even.

□

Exercise (3.29)

Evaluate the proof of the following result.
Result: Let $n \in \mathbb{Z}$. *If* $3n - 8$ *is odd, then* n *is odd.*
Proof: Assume that n *is odd. Then* $n = 2k + 1$ *for some integer* k. *Then* $3n - 8 = 3(2k + 1) - 8 = 6k + 3 - 8 = 6k - 5 = 2(3k - 3) + 1$. *Since* $3k - 3$ *is an integer,* $3n - 8$ *is odd.*

Solution.

From "$3n - 8$ is odd", we want to show that "n is odd", but the proof shows its converse. No proof has been given of the result itself. □

Exercise (4.4)

Let $x, y \in \mathbb{Z}$. Prove that if $3 \nmid x$ and $3 \nmid y$, then $3 \mid (x^2 - y^2)$.

Proof of Method 1.

Assume that $3 \nmid x$ and $3 \nmid y$. Then by division algorithm, we have that $x = 3p + 1$ or $x = 3p + 2$ for some integer p and $y = 3q + 1$ or $y = 3q + 2$ for some integer q. Then we consider the following four cases.

1. $x = 3p + 1$ and $y = 3q + 1$. Then

$$\begin{aligned} x^2 - y^2 &= (3p+1)^2 - (3q+1)^2 \\ &= (9p^2 + 6p + 1) - (9q^2 + 6q + 1) \\ &= 3(3p^2 + 2p - 3q^2 - 2q). \end{aligned}$$

   Since $3p^2 + 2p - 3q^2 - 2q$ is an integer, $3 \mid (x^2 - y^2)$.
   Using similar arguments for the remaining cases.

2. $x = 3p + 1$ and $y = 3q + 2$.
3. $x = 3p + 2$ and $y = 3q + 1$.
4. $x = 3p + 2$ and $y = 3q + 2$.

□

Exercise (4.4)

Let $x, y \in \mathbb{Z}$. Prove that if $3 \nmid x$ and $3 \nmid y$, then $3 \mid (x^2 - y^2)$.

Proof of Method 2.

$x^2 - y^2 = (x+y)(x-y)$, then it suffices to show that at least on of $(x+y)$ and $(x-y)$ can be 3 divided (By result 4.3). Also consider the four cases before:

- $x = 3p+1$ and $y = 3q+1$, then $3 \mid (x-y)$.
- $x = 3p+1$ and $y = 3q+2$, then $3 \mid (x+y)$.
- $x = 3p+2$ and $y = 3q+1$, then $3 \mid (x+y)$.
- $x = 3p+2$ and $y = 3q+2$, then $3 \mid (x-y)$.

□

Exercise (4.12)

Let $a, b \in \mathbb{Z}$. Prove that if $a^2 + 2b^2 \equiv 0 \pmod 3$, then either a and b are both congruent to 0 modulo 3 or neither is congruent to 0 modulo 3.

Method

If the conclusion is complicated, we may consider to show its contrapositive. The original statement is $(a^2 + 2b^2 \equiv 0) \Rightarrow \Big((a, b \equiv 0) \vee (a, b \not\equiv 0)\Big)$. Then the contrapositive is

$$\Big(\big(\sim (a, b \equiv 0)\big) \wedge \big(\sim (a, b \not\equiv 0)\big)\Big) \Rightarrow (a^2 + 2b^2 \not\equiv 0).$$

The left hand side is

$$\Big((a \equiv 0, b \not\equiv 0) \vee (a \not\equiv 0, b \equiv 0) \vee (a \not\equiv 0, b \not\equiv 0)\Big) \wedge \Big((a \equiv 0, b \not\equiv 0) \vee (a \not\equiv 0, b \equiv 0) \vee (a \equiv 0, b \equiv 0)\Big).$$

Then by distributive law, left hand side is

$$(a \equiv 0, b \not\equiv 0) \vee (a \not\equiv 0, b \equiv 0).$$

Method

Then the contrapositive is

$$\big((a \equiv 0, b \not\equiv 0) \vee (a \not\equiv 0, b \equiv 0)\big) \Rightarrow (a^2 + 2b^2 \not\equiv 0).$$

Therefore, there are 2 cases, and each of which has two subcases:

$$\begin{cases} a \equiv 0 \pmod 3 \text{ and } b \not\equiv 0 \pmod 3 \begin{cases} a = 3p \text{ and } b = 3q+1 \\ a = 3p \text{ and } b = 3q+2 \end{cases} \\ a \not\equiv 0 \pmod 3 \text{ and } b \equiv 0 \pmod 3 \begin{cases} a = 3p+1 \text{ and } b = 3q \\ a = 3p+2 \text{ and } b = 3q \end{cases} \end{cases}$$

Proof.

Case 1 Assume that $a \equiv 0 \pmod 3$ and $b \not\equiv 0 \pmod 3$.

1. $b = 3q + 1$. Then

$$\begin{aligned} a^2 + 2b^2 &= (3p)^2 + 2(3q+1)^2 = 9p^2 + 2(9q^2 + 6q + 1) \\ &= 9p^2 + 18q^2 + 12q + 2 = 3(3p^2 + 6q^2 + 4q) + 2. \end{aligned}$$

   Since $3p^2 + 6q^2 + 4q$ is an integer, $3 \nmid (a^2 + 2b^2)$ and so $a^2 + 2b^2 \not\equiv 0 \pmod 3$.
2. $b = 3q + 2$. (The proof is similar to that of Subcase 1.1.)

Case 2 Assume that $a \not\equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$.

1. $a = 3p + 1$. Then

$$\begin{aligned} a^2 + 2b^2 &= (3p+1)^2 + 2(3q)^2 = 9p^2 + 6p + 1 + 18q^2 \\ &= 9p^2 + 6p + 18q^2 + 1 = 3(3p^2 + 2p + 6q^2) + 1. \end{aligned}$$

   Since $3p^2 + 2p + 6q^2$ is an integer, $3 \nmid (a^2 + 2b^2)$ and so $a^2 + 2b^2 \not\equiv 0 \pmod 3$.
2. $a = 3p + 2$. (The proof of each subcase is similar to that of Subcase 2.1.)

Exercise (4.12)

Let $a, b \in \mathbb{Z}$. Prove that if $a^2 + 2b^2 \equiv 0 \pmod 3$, then either a and b are both congruent to 0 modulo 3 or neither is congruent to 0 modulo 3.

Method

There is another method based on Disjunction in conclusion:

$$(P \Rightarrow (Q \vee R)) \equiv ((P \wedge (\sim Q)) \Rightarrow R)\,.$$

If we denote $P : a^2 + 2b^2 \equiv 0$, $Q : a \equiv 0, b \equiv 0$, $R : a \not\equiv 0, b \not\equiv 0$, then the original statement is

$$P \Rightarrow (Q \vee R).$$

By Disjunction in conclusion: if we prove that $P \wedge (\sim Q) \Rightarrow R$, i.e.

$$a^2 + 2b^2 \equiv 0, a \not\equiv 0 \text{ or } b \not\equiv 0 \Rightarrow a \not\equiv 0, b \not\equiv 0,$$

then it has been done.

Exercise (4.15)

Let $a, b \in \mathbb{Z}$. Show that if $a \equiv 5 \pmod 6$ and $b \equiv 3 \pmod 4$, then $4a + 6b \equiv 6 \pmod 8$.

Proof.

- Assume that $a \equiv 5 \pmod 6$ and $b \equiv 3 \pmod 4$.
  Then $6 \mid (a-5)$ and $4 \mid (b-3)$.
  Thus $a - 5 = 6x$ and $b - 3 = 4y$, where $x, y \in \mathbb{Z}$.
  So $a = 6x + 5$ and $b = 4y + 3$.
- Observe that

$$\begin{aligned} 4a + 6b &= 4(6x+5) + 6(4y+3) = 24x + 20 + 24y + 18 \\ &= 24x + 24y + 38 = 8(3x + 3y + 4) + 6. \end{aligned}$$

Since $3x + 3y + 4$ is an integer, $8 \mid (4a + 6b - 6)$ and so $4a + 6b \equiv 6 \pmod 8$.

□

Schedule of Today

- Review concepts
- Tutorial: 4.23(absolute value), 4.33(set relation), 4.42(set relation), 5.4(parity, disprove), 5.13(rational, irrational, proof by contradiction), 5.22(parity, existence, proof by contradiction), 5.32(existence, proof by contradiction), 5.33(existence, intermediate value theorem, uniqueness)

Proof by Contradiction

- Direct Proof, Proof by Contrapositive, Proof by contradiction;
- - Prove R is true: Assume $\sim R$ is true, try to get a contradiction;
  - Prove $(\forall x)R(x)$ is true: Assume $(\exists x) \sim R(x)$ is true, try to get a contradiction;
  - Prove $(\forall x)P(x) \Rightarrow Q(x)$ is true: Assume $(\exists x)P(x) \wedge (\sim Q(x))$ is true, try to get a contradiction.
- When to use:
  - When there is no direct proof: "there do not exist...", "A is an emptyset", "p is an irrational number".
  - When it is easy to work with the negation.
- Advantage: For implication $P \Rightarrow Q$, we have more assumption[4] to work with:
  - For direct proof, we have one assumption P;
  - For proof by contradiction, we have more assumption $\sim Q$.

[4] Compare with disjunction in conclusion.

Existence Proof

- Three types:
  - $(\exists x)P(x)$:
  - $(\exists x)(\forall y)P(x, y)$:
  - $(\forall x)(\exists y)P(x, y)$:
- Two approaches:
  - Constructive proof:
    1. Give a specific example of such objects;
    2. Justify that the given examples satisfy the stated conditions.
  - Non-constructive proof:
    1. Use when specific examples are not easy or not possible to find;
    2. Make arguments why such objects have to exist;
    3. Use definitions, axioms or results that involves existence statements.

Irrational Numbers

Rational A rational number is a real number that can be written as a quotient $\frac{m}{n}$ where m and n are integers, with $n > 0$.

Irrational An irrational number is a real number that is not a rational number.

Properties

$$\begin{aligned} \text{Rational} \pm \text{Rational} &= \text{Rational}, \\ \text{Rational} \pm \text{Irrational} &= \text{Irrational}, \\ \text{Irrational} \pm \text{Irrational} &= ?(\text{it depends}). \end{aligned}$$

Decimal Decimal $\begin{cases} \text{finite decimal}, & \text{Rational} \\ \text{non-terminating recurring decimal}, & \text{Rational} \\ \text{non-terminating non-recurring decimal}, & \text{Irrational} \end{cases}$.

Lowest Term A rational number $\frac{m}{n}$ with $n > 0$ is in lowest term if m and n have no common factor which is greater than 1. This property is very useful for proof by contradiction.

Sets Relations

- Element-Chasing Method:
  1. Choose an arbitrary element;
  2. Show that the element satisfies the given property.
  3. Using this method, we can prove: $A \subseteq B$, $A \nsubseteq B$, $A = B$, $A \neq B$.
- Set Operations: $P : x \in A$, $Q : x \in B$,

Set	Meaning	Logic
$A \cap B$	$x \in A$ and $x \in B$	$P \wedge Q$
$A \cup B$	$x \in A$ or $x \in B$	$P \vee Q$
A^c	$x \notin A$	$\sim P$
$A - B$	$a \in A$ and $x \notin B$	$P \wedge (\sim Q)$

- Algebra of Sets:

Idempotent $A \cap A = A$, $A \cup A = A$;
Commutative $A \cap B = B \cap A$, $A \cup B = B \cup A$;
Associative $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$;
Distributive $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
Double Complement $(A^c)^c = A$;
De Morgan $(A \cap B)^c = A^c \cup B^c$, $(A \cup B)^c = A^c \cap B^c$;

Exercise (4.23)

Let $x, y \in \mathbb{R}$. Prove that $|xy| = |x| \cdot |y|$.

Method

For these questions, based on definition of absolute value, we consider some cases.

Recall

Equivalent definitions: $|x| = \begin{cases} x, & \text{if } x \geqslant 0; \\ -x, & \text{if } x < 0. \end{cases} = \begin{cases} x, & \text{if } x > 0; \\ -x, & \text{if } x \leqslant 0. \end{cases} = \begin{cases} x, & \text{if } x > 0; \\ 0, & \text{if } x = 0; \\ -x, & \text{if } x < 0. \end{cases}$.

Proof.

- Assume $x \geqslant 0$ and $y \geqslant 0$: then $xy \geqslant 0$, and $|xy| = xy$, $|x| = x$, $|y| = y$.
  Therefore, $|xy| = xy = |x| \cdot |y|$.
- Assume $x \geqslant 0$ and $y < 0$: then $xy \leqslant 0$, and $|xy| = -xy$, $|x| = x$, $|y| = -y$.
  Therefore, $|xy| = -xy = |x| \cdot |y|$.
- Assume $x < 0$ and $y \geqslant 0$: then $xy \leqslant 0$, and $|xy| = -xy$, $|x| = -x$, $|y| = y$.
  Therefore, $|xy| = -xy = |x| \cdot |y|$.
- Assume $x < 0$ and $y < 0$: then $xy > 0$, and $|xy| = xy$, $|x| = -x$, $|y| = -y$.
  Therefore, $|xy| = xy = (-x)(-y) = |x| \cdot |y|$.

□

Exercise (4.33)

Let A and B be sets. Prove that $A \cup B = A \cap B$ if and only if $A = B$.

Proof.

There are two directions:

"If" Assume $A = B$, then $A \cup B = A = A \cap B$.

"Only if" Assume $A \cup B = A \cap B$, we want to show $A = B$.

- Direct Proof:
  - Since $A = B$ iff $A \subseteq B$ and $B \subseteq A$, it suffices to show $A \subseteq B$ and $B \subseteq A$.
  - Using element-chasing method: for any $x \in A$, then $x \in A \cup B = A \cap B$, therefore $x \in B$, that is, $A \subseteq B$;
  - By symmetry, we also get $B \subseteq A$.
- Proof by contrapositive: assume $A \neq B$, that is $A \nsubseteq B$ or $B \nsubseteq A$, we want to show that $A \cup B \neq A \cap B$:
  - When $A \nsubseteq B$: By definition, there exists $a \in A$ and $a \notin B$. Since $a \notin B$, we have $a \notin A \cap B$. On the other hand, $a \in A$ implies that $a \in A \cup B$. Therefore $A \cup B \neq A \cap B$.
  - When $B \nsubseteq A$: Similar.

Exercise (4.42)

For sets A and B, fine a necessary and sufficient condition for $(A \times B) \cap (B \times A) = \varnothing$. Verify that this condition is necessary and sufficient.

Recall

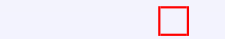
Cartesian Product: $A \times B = \{(x, y) : x \in A, y \in B\}$.

Method

Start from assumption, we try to get some necessary(sufficient) condition, then try to prove the necessary(sufficient) condition is sufficient(necessary).

Solution.

1. Assume $(A \times B) \cap (B \times A) \neq \varnothing$, then there exists $(x, y) \in (A \times B) \cap (B \times A)$, that is $x \in A$, $y \in B$ and $x \in B$, $y \in A$, i.e. $A \cap B \neq \varnothing$. ($A \cap B = \varnothing$ is sufficient condition for original statement.)
2. Guess: when $A \cap B \neq \varnothing$, we have $(A \times B) \cap (B \times A) \neq \varnothing$. (If not, we must try to add more conditions.)
3. Assume $A \cap B \neq \varnothing$, then there exists $x \in A \cap B$, therefore $(x, x) \in (A \times B) \cap (B \times A)$, i.e. $(A \times B) \cap (B \times A) \neq \varnothing$.
4. Therefore, we find a necessary and sufficient condition: $A \cap B = \varnothing$.



Exercise (5.4)

Disprove the statement: Let $n \in \mathbb{N}$. If $\frac{n(n+1)}{2}$ is odd, then $\frac{(n+1)(n+2)}{2}$ is odd.

Method

When disproving a statement, we only need a counterexample, and one counterexample is enough.
For these questions, generally there are two methods:

- Enumerating: try $1, 2, 3, \ldots$;
- Start from assumption, to get some properties, then using the properties and enumerating method to find the number.

Solution of Method 1.

We want to find an integer n, such that $\frac{n(n+1)}{2}$ is odd and $\frac{(n+1)(n+2)}{2}$ is even.

n	1	2	3	4	5	6	7	8
$\frac{n(n+1)}{2}$	1 odd	3 odd	6 even	10 even	15 odd	21 odd	28 even	36 even
$\frac{(n+1)(n+2)}{2}$	3 odd	6 even	10 even	15 odd	21 odd	28 even	36 even	45 odd

Thus $n = 2$ is a counterexample. □

Exercise (5.4)

Disprove the statement: Let $n \in \mathbb{N}$. If $\frac{n(n+1)}{2}$ is odd, then $\frac{(n+1)(n+2)}{2}$ is odd.

Solution of Method 2.

Assume that $\frac{n(n+1)}{2}$ is odd and $\frac{(n+1)(n+2)}{2}$ is even, we want to find some properties of n.

1. Since $\frac{(n+1)(n+2)}{2} = \frac{n(n+1)}{2} + (n+1)$, $\frac{n(n+1)}{2}$ is odd and $\frac{(n+1)(n+2)}{2}$ is even, we have n is even, say $2k$, $k \in \mathbb{N}$;
2. Substitute $n = 2k$ to $\frac{n(n+1)}{2}$ and $\frac{(n+1)(n+2)}{2}$: $k(2k+1)$ is odd and $(k+1)(2k+1)$ is even, therefore k is odd, say $2p+1$, $p \geqslant 0$;
3. We get $n = 2(2p+1)$, $p \geqslant 0$.
4. We can use enumerating method for the restricted set $\{n \in \mathbb{N} : n = 2(2p+1), p \geqslant 0\}$. Letting $p = 0$, we get that $\frac{n(n+1)}{2}$ is odd, then $\frac{(n+1)(n+2)}{2}$ is even when $n = 2$.

□

Exercise (5.13V)

Prove that the product of an irrational number and a nonzero rational number is irrational.

Recall

$\mathbb{R}$ has two parts: rational numbers $\mathbb{Q}$ and irrational number $\mathbb{R} - \mathbb{Q}$. Any rational number a can be expressed as $\frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $q > 0$.

Method

For these questions, in general, we use a proof by contradiction.

Proof.

1. Assume that there exist an irrational number a and a nonzero rational number b such that ab is rational.
2. By definition, b can be expressed as $\frac{r}{s}$, where $r, s \in \mathbb{Z}$ and $r, s \neq 0$; ab can be expressed as $\frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.
3. Then $a = \frac{p}{bq} = \frac{sp}{rq}$. Since $sp, rq \in \mathbb{Z}$ and $rq \neq 0$, it follows that a is a rational number, which is a contradiction.

□

Exercise (5.22V)

Let m be a positive integer of the form $m = 2s$, where s is an odd integer. Prove that there do not exist positive integers x and y such that $x^2 - y^2 = m$.

Method

For these questions, it is difficult to give a direct proof, since the number of integers is infinite.

Proof.

Here we use a proof by contradiction:

1. Assume that there exist positive integers x and y such that $x^2 - y^2 = m = 2s$. Then $(x+y)(x-y) = 2s$, where s is an odd integer.
2. Generally we may consider four cases based on the parities of x and y. While, here we consider two cases, according to whether x and y are of the same parity or of opposite parity.
   - If x and y are of the same parity, then both $x+y$ and $x-y$ are even, then $2s$ has factor 4, i.e. s has factor 2, it is a contradiction;
   - If x and y are of opposite parity, then both $x+y$ and $x-y$ are odd, therefore $2s$ is odd. Contradiction.

Exercise (5.32V)

Show that there exist no nonzero real numbers a and b such that $\sqrt{a^2+b^2} = \sqrt[3]{a^3+b^3}$.

Method

For these questions, it is difficult to give a direct proof, since the number of real numbers is infinite.

Proof.

Here we use a proof by contradiction:

1. Assume that there exist nonzero real numbers a and b such that $\sqrt{a^2+b^2} = \sqrt[3]{a^3+b^3}$.
2. Raising both sides to the 6th power, we obtain

$$a^6 + 3a^4b^2 + 3a^2b^4 + b^6 = a^6 + 2a^3b^3 + b^6.$$

   Thus

$$3a^2 - 2ab + 3b^2 = (a-b)^2 + 2a^2 + 2b^2 = 0.$$

3. Since this can only occur when $a = b = 0$[5], we have a contradiction.

□

[5] Non-negative+Non-negative=0 iff each of them is zero.

Exercise (5.33)

Prove that there exist a unique real number solution to the equation $x^3 + x^2 - 1 = 0$ *between* $x = \frac{2}{3}$ *and* $x = 1$.

Method

For existence of these questions, we will use Intermediate Value Theorem if we can not solve the equation directly.

Recall

Intermediate Value Theorem: If the function $y = f(x)$ is continuous on the interval $[a, b]$, and $f(a)f(b) < 0$, then there is a $c \in [a, b]$ such that $f(c) = 0$.

Proof of existence.

Let $f(x) = x^3 + x^2 - 1$.

1. Since f is a polynomial function, it is continuous on the set of all real numbers and so f is continuous on the interval $[2/3, 1]$.
2. Because $f(2/3) = -7/27 < 0$ and $f(1) = 1 > 0$, it follows by the Intermediate Value Theorem that there is a number c between $x = 2/3$ and $x = 1$ such that $f(c) = 0$. Hence c is a solution.

□

Method

For uniqueness, in general, let c_1 and c_2 be the numbers each of which satisfies the condition, and then prove $c_1 = c_2$.

Proof of uniqueness.

We now show that c is the unique solution of $f(x) = 0$ between $2/3$ and 1.

1. Let c_1 and c_2 be solutions of $f(x) = 0$ between $2/3$ and 1.
2. Then $c_1^3 + c_1^2 - 1 = 0$ and $c_2^3 + c_2^2 - 1 = 0$. Hence $c_1^3 + c_1^2 - 1 = c_2^3 + c_2^2 - 1$, implying that $c_1^3 + c_1^2 = c_2^3 + c_2^2$ and so

$$\begin{aligned} c_1^3 - c_2^3 + c_1^2 - c_2^2 &= (c_1 - c_2)(c_1^2 + c_1 c_2 + c_2^2) + (c_1 - c_2)(c_1 + c_2) \\ &= (c_1 - c_2)(c_1^2 + c_1 c_2 + c_2^2 + c_1 + c_2) = 0. \end{aligned}$$

3. Since $c_1^2 + c_1 c_2 + c_2^2 + c_1 + c_2 > 0$ (because $2/3 \leqslant c_1, c_2 \leqslant 1$), we obtain $c_1 - c_2 = 0$ and so $c_1 = c_2$.

□

- Time: Oct 2nd, 12-2pm;
- Venue: MPSH1;
- Close book with 1 helpsheet;
- Consultation:
  - Sept 28th, Monday, 13:00–17:00;
  - Oct 1st, Thursday, 09:00–11:00, 13:00–17:00, 19:00–21:00;
  - S9a-02-03.
- Wiki for MA1100:
  http://wiki.nus.edu.sg/display/MA1100/MA1100+Home
- Results without proof:
  http://wiki.nus.edu.sg/display/MA1100/MA1100+Basic+Results

Schedule of Today

- Review concepts
- Tutorial: 6.8, 6.9, 6.16, 6.20, 6.22, 6.35, 6.37, 6.51

Principle of Mathematical Induction

Axiom of Induction If T is a subset of $\mathbb{N}$, such that:

- $1 \in T$;
- For every $k \in \mathbb{N}$, if $k \in T$, then $k+1 \in T$.

Then $T = \mathbb{N}$.

Well-Ordered Let $\varnothing \neq S \subset \mathbb{R}$, S is well-ordered if every nonempty subset of S has smallest element.

Well-Ordering Principle The set $\mathbb{N}$ is well-ordered.

PMI Let $P(n)$ be an open sentence, such that

- If $P(1)$ is true;
- For all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

SPMI Let $P(n)$ be an open sentence, such that

- If $P(1)$ is true;
- For all $k \in \mathbb{N}$, if $P(1), P(2), \ldots, P(k)$ are true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Applications and Generalizations

- PMI(or SPMI) can be used to prove $(\forall n \in \mathbb{N})P(n)$ is true:
  - Identify universal set and open sentence $P(n)$;
  - Base case: prove $P(1)$ is true;
  - Inductive step: for all $k \in \mathbb{N}$, if $P(k)$(or $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$) is true, prove $P(k+1)$ is true;
  - Summary the conclusion you get.
- Generalization of universal set with some "good" order.
  - $\{n : n \in \mathbb{Z}, n \geqslant M\}$ with the order:
    $P(M) \to P(M+1) \to P(M+2) \to \cdots \to P(M+n) \to P(M+n+1) \to \cdots$
    where M is an integer;
  - $\mathbb{Z}$ with the order: $\leftarrow P(-n) \leftarrow \cdots \leftarrow P(-2) \leftarrow P(-1) \leftarrow P(0) \to P(1) \to P(2) \to \cdots \to P(n) \to \cdots$;
  - $\mathbb{Q}^+$ with order in lecture notes;
  - $\{n \in \mathbb{N} : n = 3p+1, p \in \mathbb{N}\}$ with the natural order:
    $P(1) \to P(4) \to P(7) \to \cdots \to P(3p+1) \to P(3p+4) \to \cdots$.

Exercise (6.8)

(a) *We have seen that* $1^2 + 2^2 + \cdots + n^2$ *is the number of the squares in an* $n \times n$ *square composed of* n^2 1×1 *squares. What does* $1^3 + 2^3 + 3^3 + \cdots + n^3$ *represent geometrically?*

(b) *Use mathematical induction to prove that* $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$ *for every positive integer* n.

Solution for (a).

Let C be an $n \times n \times n$ cube composed of n^3 $1 \times 1 \times 1$ cubes. Then the number of different cubes that C contains is $1^3 + 2^3 + 3^3 + \cdots + n^3$. □

Proof for (b).

Universal set $\{n : n \in \mathbb{N}\}$, and $P(n) : 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.

(1) Base case: when $n = 1$, LHS $= 1^3 = 1 = \frac{1^2(1+1)^2}{4} =$ RHS, i.e. $P(1)$ is true;

(2) Inductive step: for all $k \geqslant 1$:

- Assume that $P(k)$ is true, i.e. $1^3 + 2^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}$;
- Then we want to show that $P(k+1)$ is true, i.e. $1^3 + 2^3 + \cdots + (k+1)^3 = \frac{(k+1)^2(k+1+1)^2}{4}$:

$$1^3 + 2^3 + \cdots + (k+1)^3 = \underbrace{1^3 + 2^3 + \cdots + k^3}_{k^2(k+1)^2/4} + (k+1)^3$$

$$= \frac{k^2(k+1)^2}{4} + (k+1)^3 = \frac{(k+1)^2(k^2+4k+4)}{4}$$

$$= \frac{(k+1)^2(k+1+1)^2}{4}$$

(3) By the Principle of Mathematical Induction, we have $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$ for every positive integer n.

□

Exercise (6.9)

Prove that $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$ *for every positive integer* n.

Proof.

Universal set is $\{n : n \in \mathbb{N}\}$, and $P(n) : 1 \cdot 3 + 2 \cdot 4 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$.

(1) Base case: when $n = 1$, LHS $= 1(1+2) = 3 = \frac{1 \cdot 2 \cdot 9}{6} =$ RHS, i.e. $P(1)$ is true;

(2) Inductive step: for all $k \geqslant 1$:

- Assume that $P(k)$ is true, i.e. $1 \cdot 3 + 2 \cdot 4 + \cdots + k(k+2) = \frac{k(k+1)(2k+7)}{6}$;
- Then we want to show that $P(k+1)$ is true, i.e. $1 \cdot 3 + 2 \cdot 4 + \cdots + (k+1)(k+1+2) = \frac{(k+1)(k+1+1)(2(k+1)+7)}{6}$:

$$\begin{aligned} & 1 \cdot 3 + 2 \cdot 4 + \cdots + (k+1)(k+1+2) \\ = & \underbrace{1 \cdot 3 + 2 \cdot 4 + \cdots + k(k+2)}_{k(k+1)(2k+7)/6} + (k+1)(k+1+2) \\ = & \frac{(k+1)(k+1+1)(2(k+1)+7)}{6} \end{aligned}$$

(3) By the Principle of Mathematical Induction, we have $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$ for every positive integer n.

Exercise (6.16,T)

Prove that $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}\leqslant 2-\frac{1}{n}$ *for every positive integer* n.

Proof.

Universal set is $\{n : n \in \mathbb{N}\}$, and $P(n) : 1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}\leqslant 2-\frac{1}{n}$.

(1) Base case: when $n=1$, LHS $=1=2-1=$ RHS, i.e. $P(1)$ is true;

(2) Inductive step: for all $k\geqslant 1$:

- Assume that $P(k)$ is true, i.e. $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{k^2}\leqslant 2-\frac{1}{k}$;
- Then we want to show $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{(k+1)^2}\leqslant 2-\frac{1}{(k+1)}$:

$$1+\frac{1}{4}+\cdots+\frac{1}{(k+1)^2}=\underbrace{1+\frac{1}{4}+\cdots+\frac{1}{k^2}}_{\leqslant 2-\frac{1}{k}}+\frac{1}{(k+1)^2}$$

$$\leqslant 2-\frac{1}{k}+\frac{1}{(k+1)^2}=2-\frac{k^2+k+1}{k(k+1)^2}$$

$$<2-\frac{k^2+k}{k(k+1)^2}=2-\frac{1}{k+1}$$

(3) By the Principle of Mathematical Induction, $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}\leqslant 2-\frac{1}{n}$ for every positive integer n.

Exercise (6.20,T)

Prove that $7 \mid (3^{2n} - 2^n)$ *for every nonnegative integer* n.

Proof.

Universal set is $\{n \in \mathbb{Z} : n \geqslant 0\}$, and $P(n) : 7 \mid (3^{2n} - 2^n)$.

(1) Base case: when $n = 0$, $3^0 - 2^0 = 0$ and $7 \mid 0$, i.e. $P(0)$ is true;

(2) Inductive step: for all $k \geqslant 0$:

- Assume that $P(k)$ is true, that is, $7 \mid (3^{2k} - 2^k)$, i.e. $3^{2k} = 2^k + 7a$ for some integer a;
- Then we want to show $7 \mid (3^{2(k+1)} - 2^{k+1})$, and it suffices to show that $3^{2(k+1)} - 2^{k+1}$ has factor 7:

$$3^{2(k+1)} - 2^{k+1} = 3^2 \cdot 3^{2k} - 2 \cdot 2^k = 9(2^k + 7a) - 2 \cdot 2^k = 7(2^k + 9a).$$

(3) By the Principle of Mathematical Induction, we have $7 \mid (3^{2n} - 2^n)$ for every nonnegative integer n. □

Remark

When $n \geqslant 1$, by $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$, we have a direct proof:

$$3^{2n} - 2^n = 9^n - 2^n = (9 - 2)c = 7c,$$

where $c = 9^{n-1}2 + 9^{n-2}2^2 + \cdots + 92^{n-1}$ is an integer.

Exercise (6.22,T)

Prove that if $A_1, A_2, \ldots, A_n$ are any $n \geqslant 2$ sets, then $\overline{A_1 \cap \cdots \cap A_n} = \overline{A_1} \cup \cdots \cup \overline{A_n}$.

Proof.

Universal set is $\{n \in \mathbb{Z} : n \geqslant 2\}$, and
$P(n) : \overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$.

(1) Base case: when $n = 2$, by De Morgan's law, we have $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$ for any sets A_1, A_2, i.e. $P(2)$ is true;

(2) Inductive step: for all $k \geqslant 2$:

- Assume that $P(k)$ is true, i.e. $\overline{A_1 \cap \cdots \cap A_k} = \overline{A_1} \cup \cdots \cup \overline{A_k}$ for any k sets $A_1, \ldots, A_k$;
- Then we want to show that $P(k+1)$ is true, i.e. $\overline{A_1 \cap \cdots \cap A_{k+1}} = \overline{A_1} \cup \cdots \cup \overline{A_{k+1}}$ for any $k+1$ sets $A_1, \ldots, A_{k+1}$:

$$\begin{aligned}
\overline{A_1 \cap A_2 \cap \cdots \cap A_{k+1}} &= \overline{(A_1 \cap \cdots \cap A_k) \cap A_{k+1}} && \text{Associated law} \\
&= \overline{A_1 \cap \cdots \cap A_k} \cup \overline{A_{k+1}} && \text{De Morgan's law} \\
&= \left(\overline{A_1} \cup \cdots \cup \overline{A_k}\right) \cup \overline{A_{k+1}} && \text{Hypothesis} \\
&= \overline{A_1} \cup \cdots \cup \overline{A_{k+1}} && \text{Associated law}
\end{aligned}$$

(3) By the Principle of Mathematical Induction, we have $\overline{A_1 \cap \cdots \cap A_n} = \overline{A_1} \cup \cdots \cup \overline{A_n}$ for any n sets.

Exercise (6.35)

Consider the sequence $F_1, F_2, F_3, \ldots$, where $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5,$ and $F_6 = 8$. The terms of this sequence are called Fibonacci numbers.

(a) *Define the sequence of Fibonacci numbers by means of a recurrence relation.*

(b) *Prove that $2 \mid F_n$ if and only if $3 \mid n$.*

Solution for (a).

The sequence $\{F_n\}$ is defined recursively by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 3$. □

Proof for (b) "if" case.

If $3 \mid n$, we want to show $2 \mid F_n$. Universal set is $\{n : n = 3q, q \in \mathbb{N}\} = \{3, 6, \ldots, 3k, 3(k+1), \ldots\}$, and $P(n) : 2 \mid F_n$.

(1) Base case: when $n = 3$ and $F_3 = 2$, so $2 \mid F_3$, i.e. $P(3)$ is true.

(2) Inductive step, for all n of form $n = 3k$ with $k \in \mathbb{N}$:

- Assume that $P(3k)$ is true, i.e. $2 \mid F_{3k}$;
- Then we want to show that $P(3(k+1))$ is true, i.e. $2 \mid F_{3(k+1)}$: By recurrent relation, we have

$$F_{3(k+1)} = F_{3k+2} + F_{3k+1} = F_{3k+1} + F_{3k} + F_{3k+1} = 2F_{3k+1} + F_{3k}$$

which is even, i.e. $2 \mid F_{3(k+1)}$.

(3) By the Principle of Mathematical Induction, we have that $2 \mid F_n$ for all n which satisfies $3 \mid n$.

□

Proof for (b) "only if" case.

If $3 \nmid n$, we want to show $2 \nmid F_n$. Using prove by cases:

- $n = 3q + 1$ for $q \geqslant 0$. Universal set is
  $\{n : n = 3q + 1, q \geqslant 0, q \in \mathbb{Z}\} = \{1, 4, 7, \ldots, 3k + 1, 3(k + 1) + 1, \ldots\}$,
  $Q(n) : 2 \nmid F_n$.
  (1) Base case: when $n = 1$, $F_1 = 1$, so $2 \nmid F_1$, i.e. $Q(1)$ is true.
  (2) Inductive step, for all n of form $n = 3k + 1$ for $k \geqslant 0$:
    - Assume that $Q(3k + 1)$ is true, i.e. $2 \nmid F_{3k+1}$;
    - Then we want to show that $Q(3(k + 1) + 1)$ is also true, i.e. $2 \nmid F_{3(k+1)+1}$: By recurrent relation, we have
      $$F_{3(k+1)+1} = F_{3k+3} + F_{3k+2} = F_{3k+2} + F_{3k+1} + F_{3k+2} = 2F_{3k+2} + F_{3k+1}$$
      which is odd, i.e. $2 \nmid F_{3(k+1)+1}$.
  (3) By the Principle of Mathematical Induction, we have that $2 \nmid F_n$ for all n which is of form $n = 3q + 1$.
- $n = 3q + 2$ for $q \geqslant 0$. Universal set is
  $\{n : n = 3q + 2, q \geqslant 0, q \in \mathbb{Z}\} = \{2, 5, 8, \ldots, 3k + 2, 3(k + 1) + 2, \ldots\}$,
  $R(n) : 2 \nmid F_n$. By similar method, we can prove $2 \nmid F_n$ for all n of form $n = 3q + 2$.

Exercise (6.37)

Use the Strong Principle of Mathematical Induction to prove that for each integer $n \geqslant 12$, there are nonnegative integers a and b such that $n = 3a + 7b$.

Proof.

Universal set is $\{n \in \mathbb{Z} : n \geqslant 12\}$, and $P(n) : n = 3a + 7b$ for some integers $a, b \geqslant 0$.

(1) Base case: for $n = 12$, it is clear that $12 = 3 \cdot 4$, that is, we can choose $a = 4$ and $b = 0$, such that $12 = 3a + 7b$, i.e. $P(12)$ holds;

(2) Inductive step: for all $k \geqslant 12$:

- Assume that for every integer i with $12 \leqslant i \leqslant k$, there exist integers $a, b \geqslant 0$ such that $i = 3a + 7b$;
- We want to show that there exist integers $x, y \geqslant 0$ such that $k + 1 = 3x + 7y$;
- Since $13 = 3 \cdot 2 + 7 \cdot 1$ and $14 = 3 \cdot 0 + 7 \cdot 2$, we may assume that $k \geqslant 14$;
- Since $k \geqslant k - 2 \geqslant 12$, there exist integers $c, d \geqslant 0$ such that $k - 2 = 3c + 7d$;
- Hence $k + 1 = 3(c + 1) + 7d$.

(3) By the Strong Principle of Mathematical Induction, for each integer $n \geqslant 12$, there are integers $a, b \geqslant 0$ such that $n = 3a + 7b$.

□

Exercise (6.51)

By an n-gon, we mean an n-sided polygon. So a 3-gon is a triangle and a 4-gon is a quadrilateral. It is well known that the sum of the interior angles of a triangle is 180°. Use induction to prove that for every integer $n \geqslant 3$, the sum of the interior angles of an n-gon is $(n-2) \cdot 180^\circ$.

Proof.

For convenience, we use some notations: $\pi = 180^\circ$, S_n denotes the sum of the interior angles of an n-gon.
Universal set is $\{n \in \mathbb{Z} : n \geqslant 3\}$, and $P(n) : S_n = (n-2)\pi$.

(1) Base case: for $n = 3$, $S_3 = \pi = (3-2) \cdot 180^\circ$, i.e. $P(3)$ holds;

(2) Inductive step: for all $k \geqslant 3$,

1. Let Q_{k+1} be a $(k+1)$-gon whose vertices are $v_1, v_2, \ldots, v_k, v_{k+1}$ and whose edges are $v_1v_2, v_2v_3, \ldots, v_kv_{k+1}, v_{k+1}v_1$;
2. Then let Q_k be the k-gon such that whose vertices are $v_1, v_2, \ldots, v_k$ and whose edges are $v_1v_2, v_2v_3, \ldots, v_kv_1$, Q_3 be the 3-gon whose vertices are v_k, v_{k+1}, v_1 and whose edges are $v_kv_{k+1}, v_{k+1}v_1, v_1v_k$;
3. Observe that $S_{k+1} = S_k + S_3$;
4. By the induction hypothesis, S_k is $(k-2)\pi$ and S_3 is π;
5. Therefore, S_{k+1} is $(k-2)\pi + \pi = (k-1)\pi$.

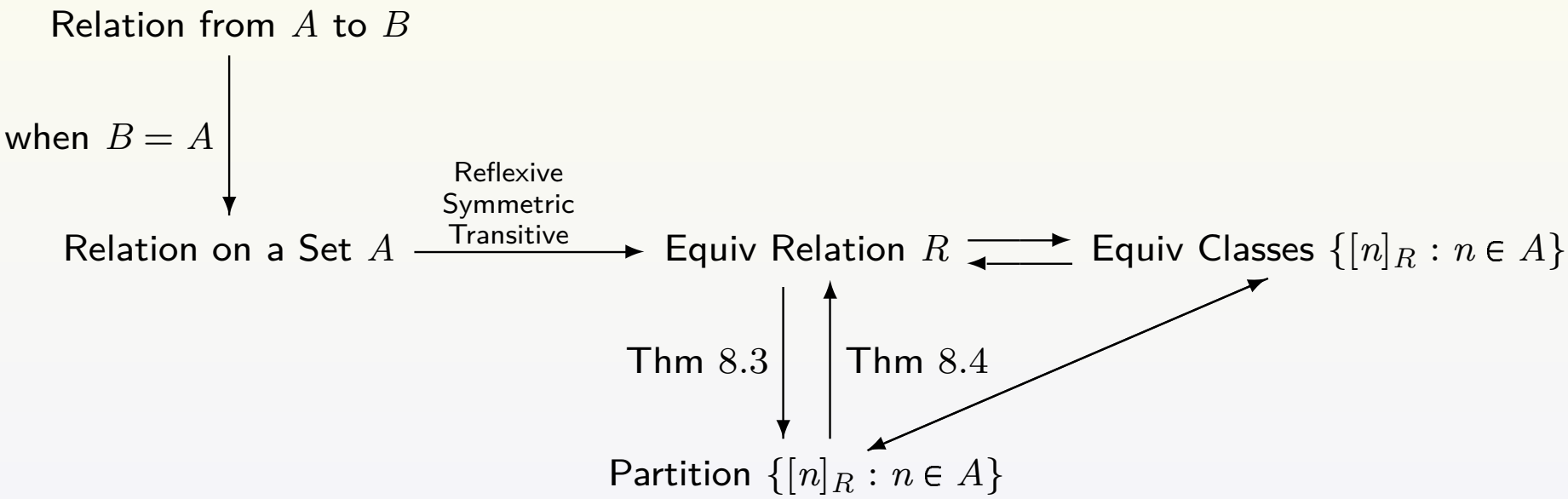
(3) By Principle of Mathematical Induction, the sum of the interior angles of an n-gon is $(n-2) \cdot 180^\circ$.

Schedule of Today

- Review concepts
- Tutorial: 8.6, 8.9, 8.10, 8.14, 8.17, 8.20, 8.23, 8.26

- Let A, B be sets. A relation R from A to B is a subset of $A \times B$, i.e. $R = \{(a, b) \in A \times B : \text{condition on } a \text{ and } b\}$. If $(x, y) \in R$, then x is related to y. Notation: $(x, y) \in R$, $x \sim y$, $x \sim_R y$, xRy.
- Let A be a set. A relation R on A is the subset of $A \times A$, i.e. $R = \{(a, b) \in A \times A : \text{condition on } a \text{ and } b\}$.
- Let R be a relation on A:
  - R is reflexive on A if "for all $x \in A$, xRx";
  - R is symmetric on A if "for all $x, y \in A$, if xRy, then yRx";
  - R is transitive on A if "for all $x, y, z \in A$, if xRy and yRz, then xRz".
- Let R be a relation on A. R is an equivalence relation if it is a reflexive, symmetric, transitive relation on A.
- Let R be an equivalence relation on A. For each $n \in A$, let $[n]_R = \{x \in A : (x, n) \in R\} = \{x \in A : (n, x) \in R\}$. We call this an equivalence class of n determined by the relation R.
- Let R be an equivalence relation on A, then the collection C of all equivalence classes determined by R is a partition of the set A.

Relation


Relation from A to B
when $B = A$
Relation on a Set A
Reflexive
Symmetric
Transitive
Equiv Relation R
Equiv Classes $\{[n]_R : n \in A\}$
Thm 8.3
Thm 8.4
Partition $\{[n]_R : n \in A\}$

Exercise (8.6)

Let $S = \{a, b, c\}$. Then $R = \{(a, a), (a, b), (a, c)\}$ is a relation on S. Which of the properties reflexive, symmetric, and transitive does the relation R possess? Justify your answers.

Solution.

- Not reflexive: $(b, b) \notin R$, $(c, c) \notin R$;
- Not symmetric: $(a, b) \in R$ but $(b, a) \notin R$, $(a, c) \in R$ but $(c, a) \notin R$;
- Transitive: The only ordered pairs (x, y) and (y, z) that belong to R are where $(x, y) = (a, a)$, since y has only one choice a. The possible choices for (y, z) in R are (a, a), (a, b), and (a, c). In every case, $(x, z) = (y, z) \in R$ and so R is transitive.

□

Exercise (8.9T)

A relation R is defined on $\mathbb{Z}$ by aRb if $|a-b| \leqslant 2$. Which of the properties reflexive, symmetric, and transitive does the relation R possess? Justify your answers.

Solution.

$R = \{(a, b) : a, b \in \mathbb{Z}, |a-b| \leqslant 2\}$.

- Reflexive: for all $n \in \mathbb{Z}$, since $|n-n| = 0 \leqslant 2$, we have nRn;
- Symmetric: for all $m, n \in \mathbb{Z}$ such that mRn, i.e $|m-n| \leqslant 2$, it can be rewritten as $|n-m| \leqslant 2$, then we have nRm;
- Not transitive: $(0, 2) \in R$, and $(2, 4) \in R$, but $(0, 4) \notin R$.

□

Exercise (8.10)

Let $A = \{a, b, c, d\}$. How many relations defined on A are reflexive, symmetric, and transitive and contain the ordered pairs $(a, b), (b, c), (c, d)$?

Solution.

We focus on a:

- Since R is reflexive, we have $(a, a) \in R$;
- By the assumption, we have $(a, b) \in R$;
- By the assumption $(a, b), (b, c) \in R$, since R is transitive, we have $(a, c) \in R$;
- Similarly, we have $(a, d) \in R$.

Then $[a]_R = \{a, b, c, d\} = A$. So the associated partition is $\{A\}$, and there is only one way for partition, that is, there is only one equivalence relation. $\square$

Exercise (8.14)

Let R be an equivalence relation on $A = \{a, b, c, d, e, f, g\}$ such that aRc, cRd, dRg, and bRf. If there are three distinct equivalence classes resulting from R, then determine these equivalence classes and determine all elements of R.

Solution.

- R is an equivalence relation and aRc, cRd, dRg: a, c, d, g is in the same equivalence class, namely $[a]_R$. Moreover, $|[a]_R| \geqslant 4$;
- Similarly, b, f is in the same equivalence class, namely $[b]_R$. Moreover, $|[b]_R| \geqslant 2$;
- Similarly, e is in the equivalence class $[e]_R$. Moreover, $|[e]_R| \geqslant 1$;
- Notice: Now we do not know whether $[a]_R, [b]_R, [e]_R$ are pairwise disjoint;
- Since $|A| = 7$, and there are three distinct equivalence classes, therefore $[a]_R, [b]_R, [e]_R$ are pairwise disjoint and the three distinct equivalence classes are just $[a]_R = \{a, c, d, g\}, [b]_R = \{b, f\}, [e]_R = \{e\}$. Otherwise, you can find contradictions easily.

□

Exercise (8.17T)

Let $A = \{1, 2, 3, 4, 5, 6\}$. *The relation* $R = \{(1,1), (1,5), (2,2), (2,3), (2,6), (3,2), (3,3), (3,6), (4,4), (5,1), (5,5), (6,2), (6,3), (6,6)\}$ *is an equivalence relation on* A. *Determine the distinct equivalence classes.*

Solution.

- The elements each of which has relation with 1 are 1 and 5, then the equivalence class of 1 is $[1]_R = \{1, 5\} = [5]_R$;
- The elements each of which has relation with 2 are 2, 3 and 6, then the equivalence class of 2 is $[2]_R = \{2, 3, 6\} = [3]_R = [6]_R$;
- The element which has relation with 4 is just 4 itself, then the equivalence class of 4 is $[4]_R = \{4\}$.

Therefore there are three distinct equivalence classes, namely $\{1, 5\}$, $\{2, 3, 6\}$ and $\{4\}$. □

Exercise (8.20)

A relation R on a nonempty set A is defined to be circular if whenever xRy and yRz, then zRx for all $x, y, z \in A$. Prove that a relation R on A is an equivalence relation if and only if R is circular and reflexive.

Proof.

There are two directions to prove:

- $\Rightarrow$: Assume that R is an equivalence relation: it suffices to show that R is circular. For all $x, y, z \in A$ such that xRy and yRz, then xRz (by transitive), then zRx (by symmetric), therefore R is circular.
- $\Leftarrow$: Assume that R is reflexive and circular: it suffices to show that R is symmetric and transitive.
  - For all $x, y \in A$ such that xRy, also we have xRx, then we have yRx (by circular), therefore R is symmetric;
  - For all $x, y, z \in A$ such that xRy and yRz, then zRx (by circular), then xRz (by symmetric), therefore R is transitive.

$\square$

Exercise (8.23T)

Let R be a relation defined on the set $\mathbb{N}$ by aRb if either $a \mid b$ or $b \mid a$. Prove or disprove: R is an equivalence relation.

Proof.

We have $2R1$ and $1R3$, but $2\not{R}3$. So we have that R is not transitive, therefore R is not an equivalence relation. □

Exercise (8.26)

(a) *Prove that the intersection of two equivalence relations on a nonempty set is an equivalence relation.*

(b) *Consider the equivalence relations R_2 and R_3 defined on $\mathbb{Z}$ by aR_2b if $a \equiv b \pmod 2$ and aR_3b if $a \equiv b \pmod 3$. By (a), $R_1 = R_2 \cap R_3$ is an equivalence relation on $\mathbb{Z}$. Determine the distinct equivalence classes in R_1.*

Proof of (a).

Suppose that R_1 and R_2 are two equivalence relations defined on a set S. Let $R = R_1 \cap R_2$.

- Let $a \in S$. Since R_1 and R_2 are equivalence relations on S, it follows that $(a, a) \in R_1$ and $(a, a) \in R_2$. Thus $(a, a) \in R$ and so R is reflexive;
- For all $a, b \in S$ such that aRb, then $(a, b) \in R = R_1 \cap R_2$. Thus $(a, b) \in R_1$ and $(a, b) \in R_2$. Since R_1 and R_2 are symmetric, $(b, a) \in R_1$ and $(b, a) \in R_2$. Thus $(b, a) \in R$ and so bRa. Hence R is symmetric;
- For all $a, b, c \in S$ such that aRb and bRc, then $(a, b) \in R_1$ and $(a, b) \in R_2$ and $(b, c) \in R_1$ and $(b, c) \in R_2$. Since R_1 and R_2 are transitive, $(a, c) \in R_1$ and $(a, c) \in R_2$. Thus $(a, c) \in R$ and so aRc. Therefore, R is transitive.

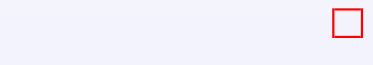
Solution of (b).

Let $a \in \mathbb{Z}$.

- If $x \in [a]_{R_1}$, then $(x, a) \in R_1$ and so $(x, a) \in R_2$ and $(x, a) \in R_3$.
- Therefore, $x \equiv a \pmod 2$ and $x \equiv a \pmod 3$. Hence $x = a + 2m$ and $x = a + 3n$ for some integers m and n.
- Hence $2m = 3n$ and so n is even. Thus $n = 2k$ for some integer k, implying that $x = a + 3n = a + 3(2k) = a + 6k$ and so $x - a = 6k$. Hence $x \equiv a \pmod 6$.
- Thus $[a]_{R_1} \subset \{x \in \mathbb{Z} : x \equiv a \pmod 6\}$.
- When $x \equiv a \pmod 6$, obviously $x \equiv a \pmod 2$ and $x \equiv a \pmod 3$, i.e. $(x, a) \in R_2 \cap R_3 = R_1$, then $x \in [a]_{R_1}$.
- Therefore $[a]_{R_1} = \{x \in \mathbb{Z} : x \equiv a \pmod 6\}$.

Therefore the distinct equivalence classes in R_1 are:

$$[0]_{R_1} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}, \qquad [1]_{R_1} = \{\ldots, -11, -5, 1, 7, 13, \ldots\},$$
$$[2]_{R_1} = \{\ldots, -10, -4, 2, 8, 14, \ldots\}, \qquad [3]_{R_1} = \{\ldots, -9, -3, 3, 9, 15, \ldots\},$$
$$[4]_{R_1} = \{\ldots, -8, -2, 4, 10, 16, \ldots\}, \qquad [5]_{R_1} = \{\ldots, -7, -1, 5, 11, 17, \ldots\}.$$

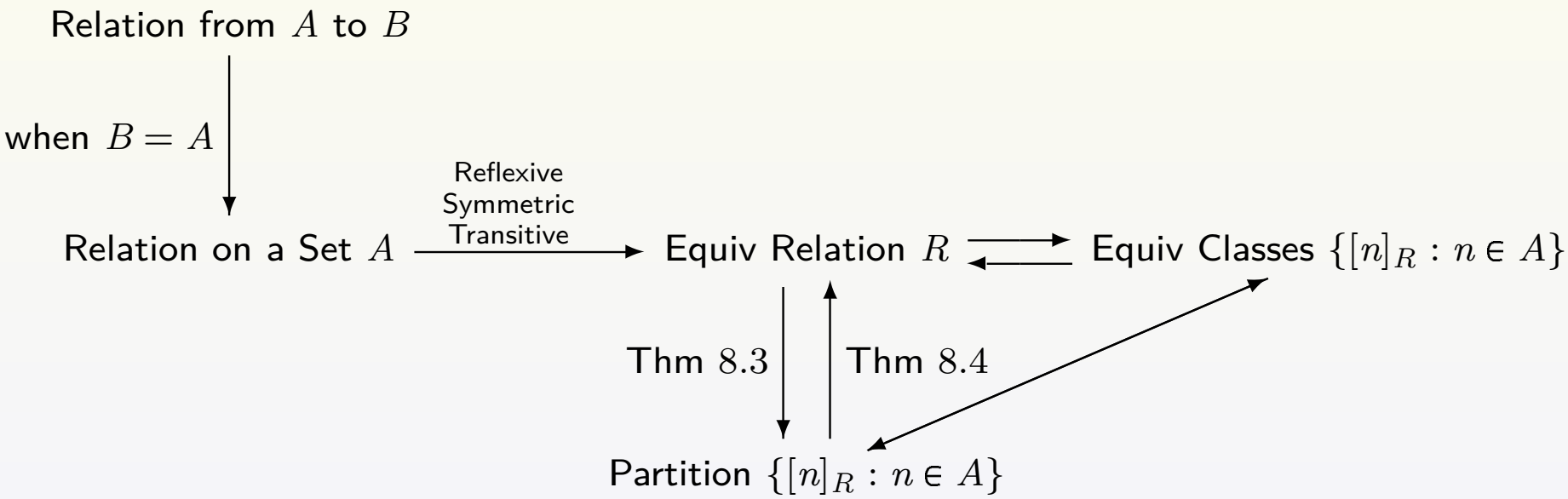


Schedule of Today

- Review concepts
- Tutorial: 8.30, 8.31, 8.36, 8.33, 8.37, 8.38, 8.42, 9.4, 9.7

- Let A, B be sets. A relation R from A to B is a subset of $A \times B$, i.e. $R = \{(a, b) \in A \times B : \text{condition on } a \text{ and } b\}$. If $(x, y) \in R$, then x is related to y. Notation: $(x, y) \in R$, $x \sim y$, $x \sim_R y$, xRy.
- Let A be a set. A relation R on A is the subset of $A \times A$, i.e. $R = \{(a, b) \in A \times A : \text{condition on } a \text{ and } b\}$.
- Let R be a relation on A:
  - R is reflexive on A if "for all $x \in A$, xRx";
  - R is symmetric on A if "for all $x, y \in A$, if xRy, then yRx";
  - R is transitive on A if "for all $x, y, z \in A$, if xRy and yRz, then xRz".
- Let R be a relation on A. R is an equivalence relation if it is a reflexive, symmetric, transitive relation on A.
- Let R be an equivalence relation on A. For each $n \in A$, let $[n]_R = \{x \in A : (x, n) \in R\} = \{x \in A : (n, x) \in R\}$. We call this an equivalence class of n determined by the relation R.
- Let R be an equivalence relation on A, then the collection C of all equivalence classes determined by R is a partition of the set A.

Relation


Relation from A to B
when $B = A$
Relation on a Set A
Reflexive
Symmetric
Transitive
Equiv Relation R
Equiv Classes $\{[n]_R : n \in A\}$
Thm 8.3
Thm 8.4
Partition $\{[n]_R : n \in A\}$

- $a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b) \Leftrightarrow n \mid (b-a) \Leftrightarrow a - b = nk$ for some integer k.
- Arithmetic on $\mathbb{Z}_n$: For $[a]_n, [c]_n \in \mathbb{Z}_n$, define

$$[a]_n + [c]_n = [a+c]_n, \quad [a]_n \cdot [c]_n = [ac]_n.$$

- A function from a set A to a set B is a rule that associate with every element x of A exactly one element of the set B.
  A function is also called a mapping. Notation: $f : A \to B$.
  The set A is called the domain of the function, and the set B is called the codomain of the function.
- If $a \in A$, then the element of B that is associated with a is denoted $f(a)$. $f(a)$ is called the image of a under f, and a is called a preimage of $f(a)$ under f.

Exercise (8.30)

Let R be the relation defined on $\mathbb{Z}$ by aRb if $a+b \equiv 0 \pmod 3$. Show that R is not an equivalence relation.

Proof.

$R = \{(a,b) : a, b \in \mathbb{Z}, a+b \equiv 0 \pmod 3\}$.

- It is obvious that R is a relation.
- Reflexibility: Since $1 \not\sim 1$, the relation R is not reflexive.
- Symmetry: Since $a+b \equiv 0 \pmod 3$ if and only if $b+a \equiv 0 \pmod 3$, R is symmetric.
- Transitivity: Since $2+1 \equiv 0 \pmod 3$, $1+5 \equiv 0 \pmod 3$ and $2+5 \equiv 1 \pmod 3$, let $a=2$, $b=1$, $c=5$, then we have $2R1$, $1R5$ and $2\not R5$. Therefore R is not transitive.

Therefore, R is not an equivalence relation. □

Exercise (8.31)

The relation R on $\mathbb{Z}$ defined by aRb if $a^2 \equiv b^2 \pmod 4$ is known to be an equivalence relation. Determine the distinct equivalence classes.

Solution.

- Since aRb if $a^2 \equiv b^2 \pmod 4$, we consider the 4 cases: $x = 4n$, $x = 4n+1$, $x = 4n+2$ and $x = 4n+3$:
-

x	4n	4n+1	4n+2	4n+3
x^2	$16n^2$	$16n^2+8n+1$	$16n^2+16n+4$	$16n^2+24n+9$
$x^2 \pmod 4$	0	1	0	1

- $x^2 \equiv \begin{cases} 0 \pmod 4, & \text{if } x = 4n \text{ or } x = 4n+2; \\ 1 \pmod 4, & \text{if } x = 4n+1 \text{ or } x = 4n+3. \end{cases}$
- Base on the above, there are 2 equivalence classes:

$$\{x = 4n \text{ or } 4n+2 : n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \ldots\},$$

$$\{x = 4n+1 \text{ or } 4n+3 : n \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \ldots\}.$$

Exercise (8.36)

Let R be the relation defined on $\mathbb{Z}$ by aRb if $a^2 \equiv b^2 \pmod 5$. Prove that R is an equivalence relation, and determine the distinct equivalence classes.

Recall

$a \equiv b \pmod n \Leftrightarrow n \mid (a-b) \Leftrightarrow n \mid (b-a) \Leftrightarrow a - b = nk$ for some integer k.

Proof.

- Reflexibility: For all $a \in \mathbb{Z}$, since $a^2 - a^2 = 0 = 5 \cdot 0$, it follows that $a^2 \equiv a^2$, i.e. aRa. Hence R is reflexive.
- Symmetry: For all $a, b \in \mathbb{Z}$ such that aRb, i.e. $a^2 \equiv b^2 \pmod 5$, then $a^2 - b^2 = 5k$ for some integer k. Then $b^2 - a^2 = 5 \cdot (-k)$, i.e. $b^2 \equiv a^2 \pmod 5$, so bRa. Hnece R is symmetric.
- Transitivity: For all $a, b, c \in \mathbb{Z}$ such that aRb and bRc, then $a^2 \equiv b^2 \pmod 5$ and $b^2 \equiv c^2 \pmod 5$. Then $a^2 - b^2 = 5m$ and $b^2 - c^2 = 5n$, so we have $a^2 - c^2 = 5(m+n)$ i.e. $a^2 \equiv c^2 \pmod 5$. Therefore aRc and R is transitive.

□

Solution.

- Since aRb if $a^2 \equiv b^2 \pmod 5$, we consider the 5 cases: $x = 5n$, $x = 5n+1$, $x = 5n+2$, $x = 5n+3$ and $x = 5n+4$:
-

x	5n	5n+1	5n+2	5n+3	5n+4
x^2	$25n^2$	$25n^2+10n+1$	$25n^2+20n+4$	$25n^2+30n+9$	$25n^2+40n+16$
$x^2 \pmod 5$	0	1	4	4	1

- $x^2 \equiv \begin{cases} 0 \pmod 5, & \text{if } x = 5n; \\ 1 \pmod 5, & \text{if } x = 5n+1 \text{ or } x = 5n+4, \\ 4 \pmod 5, & \text{if } x = 5n+3 \text{ or } x = 5n+3. \end{cases}$
- Base on the above, there are 3 equivalence classes:

$$\{x = 5n : n \in \mathbb{Z}\}, \quad \{x = 5n+1, 5n+4 : n \in \mathbb{Z}\}, \quad \{x = 5n+2, 5n+3 : n \in \mathbb{Z}\}.$$

□

Exercise (8.33)

A relation R is defined on $\mathbb{Z}$ by aRb if $5a \equiv 2b \pmod 3$. Prove that R is an equivalence relation. Determine the distinct equivalence classes.

Method 1.

Since R is a relation, it suffices to show that R is reflexive, symmetric and transitive:

- Reflexibility: For all $a \in \mathbb{Z}$, since $5a - 2a = 3a$ and $3 \mid 3a$, so we have aRa and that R is reflexive.
- Symmetry: For all $a, b \in \mathbb{Z}$ such that aRb, then $5a \equiv 2b \pmod 3$, i.e. $5a - 2b = 3k$ for some integer k. Observe that $5b - 2a = 3(a + b) - (5a - 2b) = 3(a + b - k)$, i.e. $3 \mid (5b - 2a)$, so bRa and R is symmetric.
- Transitivity: For all $a, b, c \in \mathbb{Z}$ such that aRb and bRc, then $5a \equiv 2b \pmod 3$ and $5b \equiv 2c \pmod 3$. So $5a - 2b = 3x$ and $5b - 2c = 3y$ for some integer x, y. Observe that $5a - 2c = (5a - 2b) + (5b - 2c) - 3b = 3(x + y - b)$, i.e. $3 \mid (5a - 2c)$ and $5a \equiv 2c \pmod 3$. Therefore aRc and R is transitive.

□

Method 2.

- Claim: $5a \equiv 2b \pmod 3$ if and only if $a \equiv b \pmod 3$.
- '$\Rightarrow$': Assume $5a \equiv 2b \pmod 3$, then $5a - 2b = 3k$ for some integer k. Then $2(a-b) = 3(k-a)$. Since 2 does not have the factor 3, $a-b$ should have factor 3, i.e. $3|(a-b)$. Hence $a \equiv b \pmod 3$.
- '$\Leftarrow$': Assume $a \equiv b \pmod 3$, then $a - b = 3n$ for some integer n. Observe that $5a - 2b = 5(a-b) + 3b = 3(5n+b)$, then $3|(5a-2b)$ and $5a \equiv 2b \pmod 3$.
- Base on the claim and that $a \equiv b \pmod 3$ is an equivalence relation, we know that $5a \equiv 2b \pmod 3$ is also an equivalence relation.

□

Solution.

Since aRb if $a \equiv b \pmod 3$, it is obvious that

$$[0] = \{\ldots, -3, 0, 3, 6, \ldots\}, \quad [1] = \{\ldots, -5, -2, 1, 4, \ldots\}, \quad [2] = \{\ldots, -4, -1, 2, 5, \ldots\}.$$

□

Exercise (8.37)

Construct the addition and multiplication tables in $\mathbb{Z}_4$ and $\mathbb{Z}_5$.

Solution.

For $\mathbb{Z}_4$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

For $\mathbb{Z}_5$, you can find the tables in lecture notes. □

Exercise (8.38)

In $\mathbb{Z}_8$, express the following sums and products as $[r]$, where $0 \leqslant r < 8$.
(a). $[2] + [6]$; *(b).* $[2] \cdot [6]$; *(c).* $[-13] + [138]$; *(d).* $[-13] \cdot [138]$.

Solution.

- $[2] + [6] = [8] = [0]$;
- $[2] \cdot [6] = [12] = [4]$;
- $[-13] + [138] = [3] + [2] = [5]$;
- $[-13] \cdot [138] = [3] \cdot [2] = [6]$;

□

Exercise (8.42)

Prove or disprove:

(a) *There exists an integer* a *such that* $ab \equiv 0 \pmod 3$ *for every integer* b.

(b) *If* $a \in \mathbb{Z}$, *then* $ab \equiv 0 \pmod 3$ *for every* $b \in \mathbb{Z}$.

(c) *For every integer* a, *there exists an integer* b *such that* $ab \equiv 0 \pmod 3$.

Proof.

(a) Existential quantifier and Universal quantifier: True, consider $a = 0$ and $b = 3$ for example;

(b) Universal quantifier and Universal quantifier: False, consider $a = b = 1$;

(c) Universal and Existential quantifier: True, for a given a, let $b = 0$.

□

Exercise (9.4)

For the given subset A_i of $\mathbb{R}$ and the relation $R_i (1 \leqslant i \leqslant 3)$ form A_i to $\mathbb{R}$, determine whether R_i is a function from A_i to $\mathbb{R}$.

(a) $A_1 = \mathbb{R}$, $R_1 = \{(x, y) : x \in A_1, y = 4x - 3\}$

(b) $A_2 = [0, \infty)$, $R_2 = \{(x, y) : x \in A_2, (y + 2)^2 = x\}$

(c) $A_3 = \mathbb{R}$, $R_3 = \{(x, y) : x \in A_3, (x + y)^2 = 4\}$

Recall

In the definition of function, there is only one restriction: every element x of A exactly one element of the set B.

Solution.

(a) The relation R_1 is a function from A_1 to $\mathbb{R}$.

(b) The relation R_2 is not a function from A_2 to $\mathbb{R}$. For example, both $(9, 1)$ and $(9, -5)$ belong to R_2.

(c) The relation R_3 is not a function from A_3 to $\mathbb{R}$. For example, both $(0, 2)$ and $(0, -2)$ belong to R_3.

□

Exercise (9.7)

Let $A = \{1, 2, 3\}$ *and* $B = \{x, y\}$. *Determine* B^A.

Solution.

$|B^A| = |B|^{|A|} = 2^3 = 8$.

For 1, there are 2 choices; For 2, there are also 2 choices; Similarly for 3. Therefore $B^A = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$, and

$$f_1 = \{(1, x), (2, x), (3, x)\}, \qquad f_2 = \{(1, x), (2, x), (3, y)\},$$
$$f_3 = \{(1, x), (2, y), (3, x)\}, \qquad f_4 = \{(1, x), (2, y), (3, y)\},$$
$$f_5 = \{(1, y), (2, x), (3, x)\}, \qquad f_6 = \{(1, y), (2, x), (3, y)\},$$
$$f_7 = \{(1, y), (2, y), (3, x)\}, \qquad f_8 = \{(1, y), (2, y), (3, y)\}.$$

□

Schedule of Today

- Review concepts
- Tutorial: 9.15, 9.22, 9.24, 9.29, 9.35, 9.36, 9.40, 9.46

Let $f : A \to B$ and $g : B \to C$ be functions.

- Injective or One-to-one:
  - Original definition: $\forall x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
  - Working definition: $\forall x, y \in A$, if $f(x) = f(y)$, then $x = y$.
  - Negation: $\exists x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.
- Surjective or Onto:
  - Original definition: $\forall y \in B$, $\exists x \in A$ such that $y = f(x)$.
  - Alternative definition: Range(f) =Codoman(f).
  - Negation: $\exists y \in B$ such that $\forall x \in A$, $y \neq f(x)$. Or Range(f) $\neq$Codomain(f).
- Bijective: f is both an injective and surjective function.

- Function: A relation f from a set A to a set B to be a function from A to B, if the following two conditions are satisfied:
  - For each element $a \in A$, there is an element $b \in B$, such that $(a, b) \in f$.
  - If $(a, b), (a, c) \in f$, then $b = c$.
- Well-defined: If a function f satisfies the following condition, it is called well-defined: If $(a, b), (a, c) \in f$, then $b = c$.
- Maybe we are confused here since every function must be well-defined by the definition of function. However, there are situations though when the definition of a function f may make it unclear whether f is well-defined. This can often occur when a function is defined on the set of equivalence classes of an equivalence relation.
- In conclusion, when a question ask us to prove that a function f is well-defined, it ask us to prove that this rule or this relation is well-defined. That is to say, we need to show "if $(a, b), (a, c) \in f$, then $b = c$", while we can not use the fact that every function is always well-defined.

- Two functions f_1 and f_2 are equal if and only if $\mathrm{Domain}(f_1) = \mathrm{Domain}(f_2)$ and $f_1(a) = f_2(a)$ for every $a \in \mathrm{Domain}(f)$. Notation: $f_1 = f_2$.
- Composition: Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions. The composition of f and g is the function $g \circ f : A \xrightarrow{f} B \xrightarrow{g} C$ defined by $(g \circ f)(x) = g(f(x))$.
  - Associated law: $h \circ (g \circ f) = (h \circ g) \circ f$.
  - $f \circ \mathrm{id}_A = f$, $\mathrm{id}_B \circ f = f$.
  - If f and g are injective (or surjective), then $g \circ f$ is injective (or surjective).
  - If $g \circ f$ is injective, then f is injective, and g may be not.
  - If $g \circ f$ is surjective, then g is surjective, and f may be not.
- Inverse: Let $f : A \to B$ be a bijection, for $a \in A$ and $b \in B$, we define inverse function by $f^{-1}(b) = a$ if $f(a) = b$. If the inverse function is defined, then f is bijection.
  If f and g are bijections, then $(g \circ f)^{-1} = (f^{-1}) \circ (g^{-1})$.

Exercise (9.15)

A function $f : \mathbb{Z} \to \mathbb{Z}$ is defined by $f(n) = 5n + 2$. Determine whether f is (a) injective, (b) surjective.

Proof.

(a) Injective: Using working definition. Let $m, n \in \mathbb{Z}$. Suppose $f(m) = f(n)$, i.e., $5m + 2 = 5n + 2$, which gives $5m = 5n$, and hence $m = n$. Therefore f is injective.

(b) Not surjective: Suppose $f(n) = 0$. Then $5n + 2 = 0$ which implies $5n = -2$, which is impossible for any integer n. There is no $n \in \mathbb{Z}$ such that $f(n) = 0$. Hence f is not surjective.

□

Exercise (9.22)

Let $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ be a function defined by $f([a]) = [2a + 3]$.

(a) *Show that f is well-defined.*

(b) *Determine whether f is bijective.*

Proof.

(a) Let $[a], [b] \in \mathbb{Z}_5$ such that $[a] = [b]$. We want to show that $f([a]) = f([b])$, that is, $[2a + 3] = [2b + 3]$.

- Since $[a] = [b]$, it follows that $a \equiv b \pmod 5$.
- Then $a - b = 5k$ for some integer k and therefore $(2a + 3) - (2b + 3) = 2(a - b) = 5 \cdot 2k$.
- So $[2a + 3] = [2b + 3]$, i.e., $f([a]) = f([b])$. Therefore f is well-defined.

(b) As we know, $\mathbb{Z}_5 = \{[0].[1], [2], [3], [4]\}$. Since $f([0]) = [3]$, $f([1]) = [0]$, $f([2]) = [2]$, $f([3]) = [4]$ and $f([4]) = [1]$, it follows that f is one-to-one and onto and so f is bijective.

□

Exercise (9.24)

Let $A = [0, 1]$ denote the closed interval of real numbers between 0 and 1. Give an example of two different bijective functions f_1 and f_2 from $A \to A$, neither of which is the identity function.

Solution.

- $f_1(x) = x^2$ on $[0, 1]$;
- $f_2(x) = \sqrt{x}$ on $[0, 1]$;
- $f_3(x) = 1 - x$ on $[0, 1]$.

□

Exercise (9.29)

Prove or disprove the following:

(a) *If two functions $f : A \to B$ and $g : B \to C$ are both bijective, then $g \circ f : A \to C$ is bijective.*

(b) *Let $f : A \to B$ and $g : B \to C$ be two functions. If g is onto, then $g \circ f : A \to C$ is onto.*

(c) *Let $f : A \to B$ and $g : B \to C$ be two functions. If g is one-to-one, then $g \circ f : A \to C$ is one-to-one.*

(d) *There exist functions $f : A \to B$ and $g : B \to C$ such that f is not onto and $g \circ f : A \to C$ is onto.*

(e) *There exist functions $f : A \to B$ and $g : B \to C$ such that f is not one-to-one and $g \circ f : A \to C$ is one-to-one.*

Proof.

(a) True. Corollary 9.8 in textbook;

(b) False. Let $A = \{1, 2\}$, $B = \{a, b\}$ and $C = \{x, y\}$; and let $f : A \to B$ and $g : B \to C$ be defined by $f = \{(1, a), (2, a)\}$ and $g = \{(a, x), (b, y)\}$. Then $g \circ f = \{(1, x), (2, x)\}$. Thus g is onto but $g \circ f$ is not.

(c) False. Counterexample is same as (b).

(d) True. Constructive proof: Let $A = \{1, 2\}$, $B = \{a, b, c\}$ and $C = \{x, y\}$; and let $f : A \to B$ and $g : B \to C$ be defined by $f = \{(1, a), (2, b)\}$ and $g = \{(a, x), (b, y), (c, y)\}$. Thus $g \circ f = \{(1, x), (2, y)\}$ is onto and f is not.

(e) False. We show that for functions $f : A \to B$ and $g : B \to C$, if f is not one-to-one, then $g \circ f : A \to C$ is not one-to-one. Since f is not one-to-one, there exist $a, b \in A$ such that $a \neq b$ and $f(a) = f(b)$. Thus $(g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b)$ and so $g \circ f$ is not one-to-one.

□

Exercise (9.35)

Let the functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 3$ and $g(x) = -3x + 5$.

(a) *Show that f is one-to-one and onto.*

(b) *Show that g is one-to-one and onto.*

(c) *Determine the composition function $g \circ f$.*

(d) *Determine the inverse functions f^{-1} and g^{-1}.*

(e) *Determine the inverse function $(g \circ f)^{-1}$ of $g \circ f$ and the composition $f^{-1} \circ g^{-1}$.*

Proof.

(a) Let $f(a) = f(b)$, where $a, b \in \mathbb{R}$. Then $2a + 3 = 2b + 3$. Adding -3 to both side and dividing by 2, we have $a = b$ and so f is one-to-one.
Let $r \in \mathbb{R}$, we want to find $x \in \mathbb{R}$, such that $f(x) = r$, i.e., $2x + 3 = r$. Hence $x = \frac{r-3}{2}$. Therefore f is surjective.

(b) The proof is similar to that in (a).

□

Solution.

(c) $(g \circ f)(x) = g(f(x)) = g(2x+3) = -3(2x+3)+5 = -6x-4$.

(d) Let $y = 2x+3$. Then $x = \frac{y-3}{2}$. So we have $f^{-1} : \mathbb{R} \to \mathbb{R}$ with $f^{-1}(y) = \frac{y-3}{2}$.
Let $y = 5-3x$. Then $x = \frac{5-y}{3}$. So we have $g^{-1} : \mathbb{R} \to \mathbb{R}$ with $g^{-1}(y) = \frac{5-y}{3}$.

(e) By part (d), we have $f^{-1} \circ g^{-1}(y) = -\frac{y+4}{6}$. Let $y = -6x-4$. Then $x = -\frac{y+4}{6}$.
So we have $(g \circ f)^{-1} : \mathbb{R} \to \mathbb{R}$ with $(g \circ f)^{-1}(y) = -\frac{y+4}{6}$. We have the result:
$f^{-1} \circ g^{-1} = (g \circ f)^{-1}$.

□

Exercise (9.36)

Let $A = \mathbb{R} - \{1\}$ and define $f : A \to A$ by $f(x) = \frac{x}{x-1}$ for all $x \in A$.

(a) *Prove that f is bijective.*

(b) *Determine f^{-1}*

(c) *Determine $f \circ f \circ f$.*

Proof and Solution.

1. Let $a, b \in A$ such that $f(a) = f(b)$. So $\frac{a}{a-1} = \frac{b}{b-1}$. Then $a(b-1) = b(a-1)$. This implies $ab - a = ba - b$, and hence $a = b$. Hence f is injective.
   Let $c \in A$, we want to find $a \in A$, such that $f(a) = c$, i.e., $c = \frac{a}{a-1}$. Then $a = \frac{c}{c-1}$. Hence f is surjective.
2. Let $y = \frac{x}{x-1}$. So $y(x-1) = x$ which implies $yx - y = x$. Thus $yx - x = y$ and so $x(y-1) = y$. This gives $x = \frac{y}{y-1}$. Hence $f^{-1} : A \to A$ with $f^{-1}(y) = \frac{y}{y-1}$. We observe that $f = f^{-1}$.
3. $f \circ f \circ f = f \circ (f \circ f^{-1}) = f \circ \mathrm{id}_A = f$ where id_A is the identity function on A.

□

Exercise (9.40)

Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2 + 3x + 4$.

(a) *Show that f is not injective.*

(b) *Find all pairs r_1, r_2 of real numbers such that $f(r_1) = f(r_2)$.*

(c) *Show that f is not surjective.*

(d) *Find the set S of all real numbers such that if $s \in S$, then there us no real number x such that $f(x) = s$.*

(e) *What well-known set is the set S in (d) related to?*

Proof.

(a-b) Let $a, b \in \mathbb{R}$ such that $f(a) = f(b)$. Thus $a^2 + 3a + 4 = b^2 + 3b + 4$. So $a^2 + 3a = b^2 + 3b$ and
$a^2 - b^2 + 3a - 3b = (a+b)(a-b) + 3(a-b) = (a-b)(a+b+3) = 0$.
Therefore, $a = b$ or $a + b = -3$. Moreover, f is not injective.

(c) $f(x) = x^2 + 3x + 4 = (x + \frac{3}{2})^2 + \frac{7}{4} \geqslant \frac{7}{4}$. Thus there is no $x \in \mathbb{R}$ such that $f(x) = 0$ and so f is not surjective.

(d) $S = \{s \in \mathbb{R} : s < \frac{7}{4}\}$.

(e) This is the complement of the range of f.

□

Exercise (9.46)

For each of the following functions, determine, with explanation, whether the function is one-to-one and whether it is onto.

(a) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, *where* $f(x, y) = (3x - 2, 5y + 7)$

(b) $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, *where* $g(m, n) = (n + 6, 2 - m)$

(c) $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, *where* $h(r, s) = (2r + 1, 4s + 3)$

(d) $\phi : \mathbb{Z} \times \mathbb{Z} \to S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, *where* $\phi(a, b) = a + b\sqrt{2}$

(e) $\alpha : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, *where* $\alpha(x) = (x^2, 2x + 1)$

Solution.

(a) Just checking definition, we get that f is one-to-one and onto.

(b) Let $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ such that $g(a, b) = g(c, d)$. Thus $(b + 6, 2 - a) = (d + 6, 2 - c)$. So $a = b$ and $c = d$. Therefore g is one-to-one. Let $(c, d) \in \mathbb{Z} \times \mathbb{Z}$, $a = 2 - d$ and $b = c - 6$. Then $g(a, b) = (c, d)$. Hence g is surjective.

(c) h is one-to-one by similar method of (b). While h is not onto, here is a counterexample: for $(0, 0) \in \mathbb{Z} \times \mathbb{Z}$, if $(2r + 1, 4s + 3) = (0, 0)$, then $r = -1/2, s = -3/4 \notin \mathbb{Z}$.

(d) It is obvious that ϕ is onto. Let $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ such that $\phi(a, b) = \phi(c, d)$. Thus $a + b\sqrt{2} = c + d\sqrt{2}$. So $a - c = (d - b)\sqrt{2}$. Therefore $a = c$ and $b = d$, that is, ϕ one-to-one.

(e) Let $x, y \in \mathbb{R}$ such that $\alpha(x) = \alpha(y)$. Thus $(x^2, 2x + 1) = (y^2, 2y + 1)$. So $x = y$. Therefore α one-to-one. Since $x^2 \geqslant 0$, α is not onto.

□

Schedule of Today

- Review concepts
- Tutorial: 11.8, 11.9, 11.18, 11.21, 11.30, 11.32, 11.42

- Prime: A prime is an integer $p \geqslant 2$ whose only positive integer divisors are 1 and p. An integer $n \geqslant 2$ that is not prime is called a composite number.
- Common divisor:
  - Let a, b be integers and d a nonzero integer. d is a common divisor of a and b if $d \mid a$ and $d \mid b$.
  - Original definition: Let a, b be integers, not both 0. The largest integer that divides both a and b is called the greatest common divisor of a and b. $\gcd(0, 0)$ is not defined. Notation: $\gcd(a, b)$.
  - Working definition: Let a, b be integers, not both 0, and $d \in \mathbb{N}$. $d = \gcd(a, b)$ if and only if $\begin{cases} d \mid a \text{ and } d \mid b; \\ \text{For all } k \in \mathbb{N}, \text{ if } k \mid a, k \mid b, \text{ then } k \leqslant d. \end{cases}$
  - Theorem: Let a, b be integers, not both 0, and $d \in \mathbb{N}$. $d = \gcd(a, b)$ if and only if $\begin{cases} d \mid a \text{ and } d \mid b; \\ \text{For all } k \in \mathbb{N}, \text{ if } k \mid a, k \mid b, \text{ then } k \mid d. \end{cases}$
- Division Algorithm:
  - Original: For all positive integers a and b, there exist unique integers q and r, such that $b = aq + r$, where $0 \leqslant r < a$.
  - Generalization: For all integers a and b, there exist unique integers q and r, such that $b = aq + r$, where $0 \leqslant r < |a|$. Here allow a and b to be negative.

Euclidean Algorithm

Let a and b be positive integers. If $b = aq + r$ for some integers q and r, then $\gcd(b, a) = \gcd(a, r)$.
Let a, b be integers, not both 0.

$$
\begin{array}{rcl}
b = a \cdot q_1 + r_1 & \gcd(b, a) = \gcd(a, r_1) & 0 \leqslant r_1 < |a| \\
a = r_1 \cdot q_2 + r_2 & \gcd(a, r_1) = \gcd(r_1, r_2) & 0 \leqslant r_2 < r_1 \\
r_1 = r_2 \cdot q_3 + r_3 & \gcd(r_1, r_2) = \gcd(r_2, r_3) & 0 \leqslant r_3 < r_2 \\
\cdots\cdots & \cdots\cdots & \cdots \\
r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} & \gcd(r_{n-3}, r_{n-2}) = \gcd(r_{n-2}, r_{n-1}) & 0 \leqslant r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1} \cdot q_n + r_n & \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) & 0 \leqslant r_n < r_{n-1} \\
r_{n-1} = r_n \cdot q_{n+1} + 0 & \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n &
\end{array}
$$

r_i will become 0 eventually since $|a| > r_1 > r_2 > \cdots > r_{n-1} > r_n \geqslant 0$. Then $\gcd(a, b) = r_n$.

- Linear combination: Given integers a and b.
  - An integer n is called a linear combination of a and b if n can be written in the form $ax + by$ by some integers x and y.
  - a, b not both 0, then $\gcd(a, b)$ is the smallest positive linear combination of a and b.
- Relatively Prime or Co-Prime: Let a and b be integers, not both 0.
  - If $\gcd(a, b) = 1$, then a and b are relatively prime.
  - a and b are relatively prime if and only if 1 is a linear combination of a and b.
  - Let $a, b, c \in \mathbb{Z}$, where a and b are relatively prime nonzero integers. If $a \mid c$ and $b \mid c$, then $ab \mid c$.
- Euclid's Lemma
  - Let a, b be integers, and p be a prime number. If $p \mid ab$, then $p \mid a$ or $p \mid b$.
  - Let $a_1, a_2, \ldots, a_n$ be integers, and p be a prime number. If $p \mid a_1 \cdots a_n$, then $p \mid a_k$ for some $1 \leqslant k \leqslant n$.

- Prime factorization: $n = p_1 p_2 \cdots p_r$ with primes $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$. We call this a prime factorization of n.
- Fundamental Theorem of Arithmetic:
  - Existence of prime factorization: Every integer greater than 1 is either a prime number or a product of prime numbers.
  - Uniqueness of prime factorization: For any integer greater than 1, the prime factorization is unique.
- Canonical factorization: Given any integer $n > 1$. Suppose $p_1 < p_2 < \cdots < p_r$ are the distinct prime divisors of n. Then we can write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ for $k_i \geqslant 1$.

Exercise (11.8)

Prove that $5 \mid (3^{3n+1} + 2^{n+1})$ *for every positive integer* n.

Proof.

We will use mathematical induction. The universal set is $\mathbb{N}$.

- Base case: For $n = 1$, we have $3^{3n+1} + 2^{n+1} = 3^4 + 2^2 = 85$ and $5 \mid 85$. Thus the result is true for $n = 1$.
- Inductive step: For all positive integer k, assume that $5 \mid (3^{3k+1} + 2^{k+1})$ for some positive integer k. We show that $5 \mid (3^{3(k+1)+1} + 2^{k+2})$.
  Since $5 \mid (3^{3k+1} + 2^{k+1})$, it follows that $3^{3k+1} + 2^{k+1} = 5a$ for some integer a.
  Thus $3^{3k+1} = 5a - 2^{k+1}$.
  Now observe that

$$\begin{aligned} 3^{3(k+1)+1} + 2^{k+2} &= 3^3 \cdot 3^{3k+1} + 2^{k+2} \\ &= 27(5a - 2^{k+1}) + 2^{k+2} \\ &= 5(27a) - 25 \cdot 2^{k+1} = 5(27a - 5 \cdot 2^{k+1}). \end{aligned}$$

  Since $27a - 5 \cdot 2^{k+1}$ is an integer, $5 \mid (3^{3(k+1)+1} + 2^{k+2})$.
- The result follows by the Principle of Mathematical Induction.

□

Exercise (11.9)

Prove that for every positive integer n, there exist n consecutive positive integers, each of which is composite.

Solution.

Consider the n numbers:

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1).$$

Observe for $2 \leqslant k \leqslant n+1$ that k divides $k+(n+1)!$. Thus these n numbers are composite. □

Remark

This result implies that we can find two consecutive primes which are as far apart as we want.

Exercise (11.18)

(a) *Prove that for every integer m, one of the integers m, $m+4$, $m+8$, $m+12$, $m+16$ is a multiple of 5.*

(b) *State and prove a generalization of the result in (a).*

Proof.

(a) Observe that $m = 5q + r$, where $q, r \in \mathbb{Z}$ and $0 \leqslant r \leqslant 4$.

- If $m = 5q$, then m is a multiple of 5.
- If $m = 5q + 1$, then $m + 4$ is a multiple of 5.
- If $m = 5q + 2$, then $m + 8$ is a multiple of 5.
- If $m = 5q + 3$, then $m + 12$ is a multiple of 5.
- If $m = 5q + 4$, then $m + 16$ is a multiple of 5.

□

Solution.

- **Result**: Let $n \in \mathbb{Z}$. For every integer m, one of the integers $m, m+(n-1), m+2(n-1), \ldots, m+(n-1)^2$ is a multiple of n.
- **Proof**: By the Division Algorithm, there exist integers q and r such that $m = nq + r$, where $0 \leqslant r \leqslant n-1$. For the number $m + r(n-1)$, we have

$$m + r(n-1) = (nq + r) + r(n-1) = nq + rn = n(q + r).$$

Since $q + r \in \mathbb{Z}$, it follows that $n \mid [m + r(n-1)]$.

□

Exercise (11.21)

(a) *Prove that if an integer n has the form $6q+5$ for some $q \in \mathbb{Z}$, then n has the form $3k+2$ for some $k \in \mathbb{Z}$.*

(b) *Is the converse of (a) true?*

Proof.

(a) Observe that $n = 6q+5 = 3(2q)+3+2 = 3(2q)+1+2$. Letting $k = 2q+1$, we see that $n = 3k+2$.

(b) The converse is false. The integer $2 = 3 \cdot 0 + 2$ is of the form $3k+2$, but 2 is not of the form $6q+5$ since $6q+5 = 2(3q+2)+1$ is always odd.

□

Exercise (11.30)

An integer $n > 1$ has the properties that $n \mid (35m + 26)$ and $n \mid (7m + 3)$ for some integer m. What is n?

Solution.

Since $n \mid (7m + 3)$, it follows that $n \mid 5(7m + 3)$. Hence

$$n \mid [(35m + 26) - 5(7m + 3)] = 11.$$

Thus $n = 11$. □

Exercise (11.32)

Prove that following: Let $a, b, c, m, n \in \mathbb{Z}$, *where* $m, n \geqslant 2$. *If* $a \equiv b \pmod{m}$, $a \equiv c \pmod{n}$, *and* $d = \gcd(m, n)$, *then* $b \equiv c \pmod{d}$.

Proof.

- Since $a \equiv b \pmod{m}$, $a - b = mx$ for some integer x.
- Since $a \equiv c \pmod{n}$, $a - c = ny$ for some integer y.
- Since $d = \gcd(m, n)$, $d \mid m$ and $d \mid n$. Thus $m = dr$ and $n = ds$ for some integers r, s.
-

$$\begin{aligned} b - c &= (a - mx) - (a - ny) \\ &= (a - drx) - (a - dsy) \\ &= d(sy - rx) \end{aligned}$$

Therefore $d \mid (b - c)$, i.e., $b \equiv c \pmod{d}$.

□

Exercise (11.42)

Prove the following: Let $a, b, m, n \in \mathbb{Z}$, *where* $m, n \geqslant 2$. *If* $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, *and* $\gcd(m, n) = 1$, *the* $a \equiv b \pmod{mn}$.

Proof.

- Since $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, we have $m \mid (a - b)$ and $n \mid (a - b)$.
- Since $\gcd(m, n) = 1$, by Theorem 11.16, $mn \mid (a - b)$. Hence $a \equiv b \pmod{mn}$.

□

Schedule of Today

- Review concepts
- Tutorial: 11.46, 11.47, 11.48, 11.53, 10.12, 10.15, 10.18, 10.19

- If there exists a bijective $f: A \to B$, we say that A is numerically equivalent to B.
- If A and B are two finite sets, then A is numerically equivalent to B if and only if $|A| = |B|$.
- If A and B are two infinite sets, we define $|A| = |B|$ if A is numerically equivalent to B.
- If $|A| = |\mathbb{N}|$, then A is called a denumerable set, and write $|A| = |\mathbb{N}| = \aleph_0$.
- A set is called a countable set if it is either finite or a denumerable set. A set that is not countable is called an uncountable set.
- If there exists a injective function $f: A \to B$ but no bijective function, we say that A has smaller cardinality than B, write $|A| < |B|$. From this, we can get: If there exists a injective function $f: A \to B$, then $|A| \leqslant |B|$.
- $$\text{Sets} \begin{cases} \text{finite} \\ \text{infinite} \begin{cases} \text{denumerable: } \aleph_0 \ (\mathbb{N}, \mathbb{Z}, \mathbb{Q}) \\ \text{uncountable} \begin{cases} \text{equivalent to } (0,1): \ \aleph_1, c \ ((a,b), [0,1], [a,b], \mathbb{R}, \mathbb{I}) \\ \text{not equivalent to } (0,1): \ \aleph_2, \aleph_3, \ldots \ (\mathcal{P}(\mathbb{R})) \end{cases} \end{cases} \end{cases}$$

Exercise (11.46)

Prove each of the following:

(a) *Every prime of the form $3n+1$ is also of the form $6k+1$.*

(b) *If n is positive integer of the form $3k+2$, then n has a prime factor of this form as well.*

Proof.

(a) Let $3n+1$ be a prime. We claim that n must be even. If n is odd, then $n = 2k+1$ for some integer k. So $3n+1 = 3(2k+1)+1 = 6k+4 = 2(3k+2)$ where $3k+2 \geqslant 2$. Thus $3n+1$ is composite, which is impossible. Thus, as claimed, n is even and so $n = 2k$ for some integer k. Therefore, $3n+1 = 3(2k)+1 = 6k+1$.

(b) Let n be a positive integer such that $n = 3l+2$, where $l \in \mathbb{Z}$. If n is a prime, then the proof is complete. Assume, to the contrary, that no prime factor of n is of the form $3k+2$ for some $k \in \mathbb{Z}$. We consider two cases.

- Some prime factor p of n is of the form $3k$, where $k \in \mathbb{Z}$. Necessarily then, $3|p$ and so $p = 3$, contradicting our assumption that $n = 3l+2$, where $l \in \mathbb{Z}$.
- Every prime factor of n is of the form $3k+1$, where $k \in \mathbb{Z}$. By Exercise 11.22, n is of the form $3k+1$, which is a contradiction.

Exercise (11.47)

(a) *Express each of the integers 4278 and 71929 as a product of primes.*

(b) *What is* $\gcd(4278, 71929)$*?*

Recall

pp. 258 in the textbook.

- $2|n$ iff the last digit of n is even;
- $3|n$ iff the sum of its digits is divisible by 3;
- $5|n$ iff the last digit of n is 0 or 5;
- Start with the first digit of n and sum alternate digits. Let the sum be a, b be the summation of the remaining digits. Then $11|n$ iff $11|(a-b)$.

Proof.

(a) $4278 = 2 \cdot 3 \cdot 23 \cdot 31$ and $71929 = 11 \cdot 13 \cdot 503$.

(b) $\gcd(4278, 71929) = 1$.

□

Exercise (11.48)

Let k be a positive integer.

(a) *Prove that if $2^k - 1$ is prime, then k is prime.*

(b) *Prove that if $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ is perfect.*

Proof.

(a) Assume that k is not prime. If $k = 1$, then $2^k - 1 = 1$ is not prime (contradiction). If k is a composite number, then $k = ab$, where $a, b \in \mathbb{Z}$ and $1 < a, b < k$. Therefore, $2^k - 1 = 2^{ab} - 1 = (2^a)^b - 1$. Letting $x = 2^a$, we have $2^k - 1 = x^b - 1$, where $x \geqslant 4$. Since $b \geqslant 2$, we have $x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + 1)$, and $x - 1 \geqslant 3$, $x^{b-1} + \cdots + 1 \geqslant 5$. Thus $(x-1) | (x^b - 1)$ and so $2^k - 1$ is not prime.

(b) Assume that $2^k - 1$ is prime. Let $p = 2^k - 1$. Then $k \geqslant 2$. The proper divisors of $n = 2^{k-1}(2^k - 1) = 2^{k-1}p$ are then $p, 2p, 2^2p, \ldots, 2^{k-2}p$ and $1, 2, 2^2, \ldots, 2^{k-1}$. The sum of these integers is

$$\begin{aligned} p(1 + 2 + 2^2 + \cdots + 2^{k-2}) + (1 + 2 + 2^2 + \cdots + 2^{k-1}) &= p(2^{k-1} - 1) + (2^k - 1) \\ &= (2^k - 1)[(2^{k-1} - 1) + 1] \\ &= 2^{k-1}(2^k - 1) = n, \end{aligned}$$

as desired.

Exercise (11.53)

Evaluate the proposed solution of the following problem.
Prove or disprove the following statement: There do not exist three integers n, $n+2$, and $n+4$, all of which are primes.
Solution: *This statement is true.*
Proof: *Assume, to the contrary, that there exist three integers n, $n+2$, and $n+4$, all of which are primes. We can write n as $3q$, $3q+1$, or $3q+2$, where $q \in \mathbb{Z}$. We consider these three cases.*

Case 1 $n = 3q$. *Then $3|n$ and so n is not prime. This is a contradiction.*

Case 2 $n = 3q+1$. *Then $n+2 = 3q+3 = 3(q+1)$. Since $q+1$ is an integer, $3|(n+2)$ and so $n+2$ is not prime. Again, we have a contradiction.*

Case 3 $n = 3q+2$. *Hence we have $n+4 = 3q+6 = 3(q+2)$. Since $q+2$ is an integer, $3|(n+4)$. This produces a contradiction.*

Solution.

It is wrong to say: "Then $3|n$ and so n is not prime." Note that $3|3$ and 3 is prime. □

Exercise (10.12)

Let $A = \{a_1, a_2, a_3, \ldots\}$. *Define* $B = A - \{a_{n^2} : n \in \mathbb{N}\}$. *Prove that* $|A| = |B|$.

Proof.

We need to check the condition of Theorem 10.3

1. Since we can find a bijective function $f : A \to \mathbb{N}$, $a_n \mapsto n$, A is denumerable.
2. It is obvious that B is a subset of A.
3. There are $2n$ numbers between a_{n^2} and $a_{(n+1)^2}$ in B, therefore the number of B is

$$\#B = 2 + 4 + 6 + \cdots = \sum_{n=1}^{\infty} 2n = \infty.$$

   Hence, B is infinite.

Therefore it follows that B is denumerable by Theorem 10.3. □

Exercise (10.15)

Prove that the set of irrational numbers is uncountable.

Proof.

Denote the set of irrational numbers by $\mathbb{I}$. Assume, to the contrary, that $\mathbb{I}$ is denumerable. Since $\mathbb{Q}$ and $\mathbb{I}$ are disjoint denumerable sets, $\mathbb{Q} \cup \mathbb{I}$ is denumerable by Exercise 10.1. Since $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$, it follows that $\mathbb{R}$ is denumerable, which is a contradiction. $\square$

Exercise (10.18)

(a) *Prove that the function* $f : (0, 1) \to (0, 2)$*, mapping the open interval* $(0, 1)$ *into the open interval* $(0, 2)$ *and defined by* $f(x) = 2x$*, is bijective.*

(b) *Explain why* $(0, 1)$ *and* $(0, 2)$ *have the same cardinality.*

(c) *Let* $a, b \in \mathbb{R}$*, where* $a < b$*. Prove that* $(0, 1)$ *and* (a, b) *have the same cardinality.*

Proof.

(a) Assume that $f(a) = f(b)$, where $a, b \in (0, 1)$. Then $2a = 2b$ and so $a = b$. Hence f is one-to-one. For each $r \in (0, 2)$, $x = \frac{r}{2} \in (0, 1)$ and $f(x) = r$. Therefore, f is onto. Thus f is a bijective function from $(0, 1)$ to $(0, 2)$.

(b) It follows by (a).

(c) Define the function $g : (0, 1) \to (a, b)$ by $g(x) = (b - a)x + a$. Then g is bijective and so $(0, 1)$ and (a, b) have the same cardinality.

□

Exercise (Extra)

Construct a bijective function $f : [0, 1] \to (0, 1)$.

Solution.

$$f = \begin{cases} \frac{1}{2}, & \text{when } x = 0; \\ \frac{1}{n+2}, & \text{when } x = \frac{1}{n}, n \in \mathbb{N}; \\ x, & \text{when } x \neq 0 \text{ and is not reciprocal of some positive integer.} \end{cases}$$

□

Remark

From this, we have:

$$|[0, 1]| = |(0, 1)| = |[0, 1)| = |(0, 1]| = |[a, b]| = |(a, b)| = |[a, b)| = |(a, b]| = \mathbb{R}.$$

Exercise (10.19)

Prove or disprove the following:

(a) *If A is an uncountable set, then $|A| = |\mathbb{R}|$.*

(b) *There exists a bijective function $f : \mathbb{Q} \to \mathbb{R}$.*

(c) *If A, B and C are sets such that $A \subset B \subset C$, and A and C are denumerable, then B is denumerable.*

(d) *The set $S = \{\frac{\sqrt{2}}{n} : n \in \mathbb{N}\}$ is denumerable.*

(e) *There exists a denumerable subset of the set irrational numbers.*

(f) *Every infinite set is a subset of some denumerable set.*

(g) *If A and B are sets with the property that there exists an injective function $f : A \to B$, then $|A| = |B|$.*

Proof.

(a) False. For example, $|\mathcal{P}(\mathbb{R})| > |\mathbb{R}|$.

(b) False. $|\mathbb{Q}| \neq |\mathbb{R}|$.

(c) True. Since A is denumerable and $A \subset B$, the set B is infinite. Since B is an infinite subset of the denumerable set C, it follows that B is denumerable.

(d) True. Consider the function $f : \mathbb{N} \to S$ defined by $f(n) = \frac{\sqrt{2}}{n}$. The function f is bijective.

(e) True. (See (d).)

(f) False. Consider $\mathbb{R}$.

(g) False. The function $f : \mathbb{N} \to \mathbb{R}$ defined by $f(n) = n$ is injective but $|\mathbb{N}| \neq |\mathbb{R}|$.

□

Final Exam Information

- Read Exam Info.pdf and Exam Seat Plan.pdf in Workbin on IVLE.
- Consultation:
  - Any time from 14 Nov to 24 Nov, at my office S9a-02-03.
  - Email: xiangsun@nus.edu.sg.
  - MSN: xiangsun.sunny@hotmail.com.
- Read Lecture 24.pdf.
- Results available in final exam (from VT):
  - Short answer: you can use all of them (that we have discussed and prove)
  - Longer answer: you can use the results relative to the question asked. If an exam question can be answered in one or two lines by quoting a result, then you should know that you need to elaborate more.
- Wiki for MA1100: http://wiki.nus.edu.sg/display/MA1100/MA1100+Home.
- Be careful, and do not make any foolish mistakes.
- Good Luck.

Thank you