## Introduction to

## Mathematical Thinking

## (Summary)

Name: Oliver

Lee Woongbi

Lee Seungchan,

Woo Soogil

Shin Jongmok

## Chapter 1. What is mathematics?

I want to say the goal of this course. It is for helping to develop a valuable metal ability. It's about thinking, not learning new math techniques. The key mathematical thinking is thinking outside the box. We should stop looking for a formula to apply or a procedure to follow. Instead of that, we should try to understand and always think how and why.

### 1.1 More than arithmetic

- Mathematics is a thriving, worldwide activity.
- Mathematics can be used in a variety field such as engineering, stock and so on.


### 1.2 Mathematical notation.

- The mathematicians' reliance on abstract notation is a reflection of the abstract nature of the patterns they study
- Mathematics is essential to our understanding the invisible pa tterns of the universe


### 1.3 Modern college-level mathematics

- Modern mathematics doesn't focus on performing calculators or computing answers
- It formulates and understands abstract concepts and relationships.
- First one is still important, but not enough, so second one is indispensable.


### 1.4 Why do you have to learn this stuff?

Chapter 2. Getting precise about language

- Mathmaticians have to be aware of the literal meaning of what they write or say.


### 2.1 Mathematical statements

- Our use of language is rarely precise in real life
- However, Modern pure mathematics is primarily concerned with precise statements about mathematical objects.


### 2.2 The logical combinators and, or, and not.

- And makes mathematical language simpler. It is only depends on truth or falsity.
- There are two kinds of or: exclusive-or and inclusive-or -Exclusive-or: There is no possibility of both eventualities occurring at once. Ex) $\mathrm{a}>0$ or the equation $\mathrm{x}^{2}+a=0$ has a real root. -Inclusive-or: There is possible for both eventualities occurring at once.

Ex) $a b=0$ if $a=0$ or $b=0$
※ In mathematics, "or" means inclusive-or.

- Many mathematical statements involve a negation, i.e., a claim that a particular statement is false.

Ex) not-A is $\neg \mathrm{A}$ or $\sim \mathrm{A}$.

### 2.3 Implication

- Now, things get really tricky. Brace yourself for several days of confusion until the ideas sort themselves out in your mind.
- The benefit in this case is helping to develop your mathematical thinking ability.
- The approach we shall adopt is to separate the notion of implication into two part, the truth part and the causation part.
- The truth part is generally known as the conditional, or sometimes the material conditional.
- When we say " $\Phi$ implies $\psi$ ", we mean that $\Phi$ somehow causes or brings about $\Psi$.(delete)
- The point is, implies entails causality. (delete)
- There is nothing to stop us conjoining or disjoining two totally unrelated statements.(deltete)
- Implication=Conditional+Causation. We will use the symbol $\Rightarrow$ to denote the conditional operator.

Ex) $\Phi \Rightarrow \Psi$ (It is referred to as a conditional expression. We refer to $\Phi$ as the antecedent of the conditional and $\Psi$ as the consequent.)

- Whether or not the conditional expression $\Phi \Rightarrow \Psi$ is true will depend entirely upon the truth or falsity of $\Phi$ and $\Psi$, taking no account of whether or not there is any meaningful connection between $\Phi$ and $\Psi$.
- Here, we ignore a causation part. But it will be ok since in the very restricted situations, we need it.
- As long as the definition we do is explicit, we don't need to care about relationship between the antecedent of the conditional and the consequent of it.

Ex) What happens if $\Phi$ is the true statement "Youngho is dead" and $\Psi$ is the true statement " $\pi>3$ "?
(Youngho is dead $) \Rightarrow(\pi>3)$, The conditional has the vale $T$.

- So, we should know all cases of truth table regarding with the antecedent, the consequent and conditional. (Refer to Exercises 2.3.1~2.3.2 for detailed explanations)

| $\phi$ | $\psi$ | $\phi \Rightarrow \psi$ |
| :---: | :---: | :---: |
| T | T | T |


| T | F | F |
| :---: | :---: | :---: |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $T$ |

- When the antecedent is $F$, it is tricky. To deal with this case, we consider not the notion of implication, but its negation. (Refer to Exercise 2.3 for detailed explanations)
- Then, How should the truth or falsity of the statement $\neg(\Phi \Rightarrow \Psi)$ depend upon the truth or falsity of $\Phi$ and $\Psi$ ?
- In terms of truth values, $\Phi$ will not imply $\Psi$ if it is the case that although $\Phi$ is true, $\Psi$ is nevertheless false.
- Therefore we define $\neg(\Phi \Rightarrow \Psi)$ to be true precisely in case $\Phi$ is true and $\Psi$ is false.


## 2.3-1 Equivalence.

Closely related to implication is the notion of equivalence. Actually, it is included in the

- Two statements $\Phi$ and $\Psi$ are said to be (logicaly) equivalent if each implies the other.
- We call equivalence biconditional as well
- $\Phi \Leftrightarrow \Psi$ is abbreviation of $(\Phi \Rightarrow \Psi) \wedge(\Psi \Rightarrow \Phi)$
- $\Phi \Leftrightarrow \Psi$ is true if $\Phi$ and $\psi$ are both true or both false.
- One way to show two statements $\Phi$ and $\Psi$ are equivalent is to show that they have the same truth tables.(!)
- There is some terminology associated with real implication that should be mastered straight away, as it pervades all mathematical discussion.
(1) $\Phi$ implies $\psi$
(2) If $\Phi$ then $\psi$
(3) $\Phi$ is sufficient for $\psi$
(4) $\Phi$ only if $\psi$
(5) $\psi$ if $\Phi$
(6) $\psi$ whenever $\Phi$
(7) $\Psi$ is necessary for $\Phi$
$※$ Notice the contrast between (4) and (5) as far as the order of $\Phi$ and $\psi$ is concerned
※Notice that to say that $\psi$ is a necessary condition for $\Phi$ does not mean that $\psi$ on its own is enough to guarantee $\Phi$.


### 2.4 Quantifiers

- There are two more(mutually related) language constructions that are fundamental to expressing and proving mathematical facts.
- And which mathematicians therefore have to be precise about: the two quantifiers:


## there exists, for all

- The word "quantify" is used in a very idiosyncratic fashion here.
- In normal use, it means specifying the number or amount of something.
- In mathematics, it's used to refer to the two extremes: there is at least one and for all.
- The reason for this restricted use is the special nature of mathematical truths.
- A simple example of an existence statement

Ex) There exists a real number $x$ such that $x^{2}+2 x+1=0$

- When Mathematicians use the symbol, it can be indicated that


## $\exists x$

and it means

There exists an $x$ such that...

- If we use this notatioin, we can change
"There exists a real number $x$ such that $x^{2}+2 x+1=0$ "
to

$$
" \exists x\left[x^{2}+2 x+1=0\right] \text { " }
$$

$※$ The symbol $\exists$ is called the existential quantifier.(!)

- One obvious way to prove an existence statement is to find an object that satisfies the expressed condition.
- However, not all true existence claims are proved by finding a requisite object. Mathematicians have other methods for proving statements of the form $\exists x \mathrm{P}(\mathrm{x})$.

Ex) Prove $x^{3}+3 x+1=0$ has a real root
Note that the curve $\mathrm{y}=\mathrm{x}^{3}+3 x+1=0$ is continuous, that the curve is below the $x$-axis when $x=-1$ and above the $x$-axis when $x=1$, and hence must cross the $x$ axis somewhere between those two values of $x$. When it crosses the $x$-axis, the value of $x$ will be a solution to the given equation. So we have proved that there is a solution without actually finding one.

- Sometimes it is not immediately obvious that a statement is an existence assertion.

Ex) $\sqrt{2}$ is rational.

- If you unpack the meaning of the example and write it in the form
"There exist natural numbers $p$ and $q$ such that $\sqrt{2}=p / q$."
and if we use the existential quantifier symbol, we can indicate it like below

$$
\exists p \exists q(\sqrt{2}=p / q)
$$

- Sometimes the context in which we work guarantees that everyone knows what kinds of entities the various symbols refer to. But that is (very) often not the case.
- So we extend the quantifier notation by specifying the kind of entity under consideration.

$$
E x)(\exists p \in N)(\exists q \in N)(\sqrt{2}=p / q)
$$

- The remaining piece of language we need to examine and make sure we fully comprehend is the universal quantifier, which asserts that something holds for all $x$. We use the symbol

$$
\forall x
$$

to mean

$$
\text { for all } x \text { it is the case that... }
$$

Ex) Express that the square of any real number is greater than or equal to 0 with $\forall x$

$$
\forall x\left(x^{2} \geq 0\right)
$$

If we want to specify the domain as we did before, it is

$$
(\forall x \in \mathrm{R})\left(x^{2} \geq 0\right)
$$

We would read this as "For all real numbers $x$, the square of $x$ is greater than or equal to 0 "

- Most statements in mathematics involve combinations of both kinds of quantifier.

Ex)Express the assertion that there is no largest natural number n requires two quantifiers.

$$
(\forall m \in N)(\exists n \in N)(n>m)
$$

This reads: for all natural numbers $m$ it is the case that there exists a natural

Number n such that n is greater than m .

- Notice that the order in which quantifiers appear can be of paramount importance.

Ex) $(\exists n \in N)(\forall m \in N)(n>m)$

This asserts that there is a natural number which exceeds all natural numbers-an assertion that is clearly false!

- In mathematics(and in everyday life), you often find yourself having to negate a statement involving quantifiers. Of course, you can do it simply by putting a negation symbol in front. But often that's not enough; you need to produce a positive assertion, not a negative one.
- In practice, a positive statement is one that contains no negation symbol, or else one in which any negation symbols are as far inside the statement as is possible without the resulting expression being unduly cumbersome.

Ex) Let $A(x)$ denote some property of $x$
$\neg[\forall x A(x)]$ is equivalent to $\exists x[\neg A(x)]$
(!) It is not the case that all motorists run red lights

Is equivalent to

There is a motorist who does not run red lights.

- Now for the abstract verification.

Ex1) $\neg[\forall x A(x)]$ That is, we assume it is not the case that $\forall x A(x)$ is true. In other words, for at least one $x, \neg A(x)$ must be true. In symbols, this can be written $\exists x[\neg A(x)]$. Hence $\neg[\forall x A(x)]$ implies $\exists x[\neg A(x)]$. You can get the result " $\exists x[\neg A(x)]$ implies $\neg[\forall x A(x)]$ " if you follow what I just did.

Taken together, the two implications just established produce the claimed equivalence.

Ex2)Let $P(x)$ denote the property " $x$ is a prime" and $O(x)$ the property " $x$ is odd". Consider the sentence

$$
\forall x[P(x) \Rightarrow O(x)]
$$

The negation of this sentence will have the (positive) form

$$
\exists x[P(x) \wedge \neg O(x)]
$$

To get to this form, you start with

$$
\neg \forall x[P(x) \Rightarrow O(x)]
$$

Which is equivalent to

$$
\exists x 孔[P(x) \Rightarrow O(x)]
$$

And that in turn is equivalent to

$$
\exists x[P(x) \nRightarrow O(x)]
$$

Which we can reformulate as

$$
\exists x[P(x) \wedge \neg O(x)]
$$

Thus the $\forall$ becomes a $\exists$ and the $\Rightarrow$ becomes a $\wedge$. In words, the negation reads "There is a prime that is not odd," or more colloquially, "There is an even prime."

- Viewed as a symbolic procedure, what I did above was move the negation symbol successively inside the expression.
- And adjust the logical connectives appropriately as I did.
- Sometimes as an illustration of the various pitfalls that can arise, suppose the domain under discussion is the set of natural numbers.

Ex)Let $E(x)$ be the statement ' $x$ is even', and let $O(x)$ be the statement ' $x$ is odd'. The statement

$$
\forall x[E(x) \vee O(x)]
$$

says that for every natural number $\mathrm{x}, \mathrm{x}$ is either even or odd(or both). This is clearly true.

On the other hand, the statement

$$
\forall x E(x) \vee \forall x O(x)
$$

is false, since it asserts that either all natural numbers are even or else all natural numbers are odd(or both), whereas in fact neither of these alternatives is the case.

- Thus, in general you cannot "move a $\forall x$ inside brackets." More precisely, if you do, you can end up with a very different statement, not equivalent to the original one.
- Likewise, "moving a $\exists x$ inside brackets" can also lead to a statement that is not equivalent to the original one.
- Notice that although the last statement above uses the same variable $x$ in both parts of the conjunction, the two conjuncts operate separately.
- Very often, in the course of an argument, we use quantifiers that are restricted to a smaller collection than the original domain. For example, in real analysis(where the unspecified domain is usually the set $R$ of all real numbers)we often need to talk about "all positive numbers" or "all negative numbers".
- One way to handle this has been done already. We can modify the quantifier notation, allowing quantifiers of the form

$$
(\forall x \in A),(\exists x \in A)
$$

where $A$ is some subcollection of the domain.

- Another way is to specify the objects being quantified within the non-quantifier
part of the formula.

Ex)Suppose the domain under discussion is the set of all animals. Thus, any variable $x$ is assumed to denote an animal. Let $L(x)$ mean that " $x$ is a leopard" and let $S(x)$ mean that " $x$ has spots". Then the sentence "All leopards have spots" can be written like this:

$$
\forall x[L(x) \Rightarrow S(x)]
$$

In English, this reads literally as: "For all animals $x$, if $x$ is a leopard then $x$ has spots"

In mathematical version, $(\forall x \in \mathscr{L})$ where $\mathscr{L}$ denotes the set of all leopards.

- Since a mathematical argument where quantifiers refer to different domains could easily lead to confusion and error.
- Beginners often make the mistake of rendering the original sentence "All leopards have spots" as

$$
\forall x[L(x) \wedge S(x)]
$$

In English, what this says is: "For all animals $x, x$ is both a leopard and have spots or "All animals are leopards and have spots" This is obviously false.

- Part of the reason for the confusion is probably the fact that the mathematics goes differently in the case of existential sentences.

Ex)Consider the sentence "There is a horse that has spots". Let $H(x)$ mean that " $x$ is a horse", then this sentence translates into the mathematical sentence

$$
\exists x[H(x) \wedge S(x)]
$$

Literally: "There is an animal that is both a horse and has spots."

Contrast this with the sentence

$$
\exists x[H(x) \Rightarrow S(x)]
$$

This says that "There is an animal such that if it is a horse, then it has spots."This does
not seem to say anything much, and is certainly not at all the same as saying that there
is a spotty horse.

- In symbolic terms, the modified quantifier notation

$$
(\forall x \in \mathcal{A}) \phi(x)
$$

(where the notation $\phi(x)$ indicates that $\phi$ is a statement that involves the variable $x$ )
may be regarded as an abbreviation for the expression

$$
\forall x[A(x) \Rightarrow \phi(x)]
$$

where $A(x)$ is the property of $x$ being in the collection $\mathcal{A}$

Likewise, the notation

$$
(\exists x \in \mathcal{A}) \phi(x)
$$

may be regarded as an abbreviation for

$$
\exists x[A(x) \wedge \phi(x)]
$$

- In order to negate statements with more than one quantifier, you could start at the outside and work inwards, handling each quantifier in turn.
- The overall effect is that the negation symbol moves inwards, changing each $\forall$ to an $\exists$ and each $\exists$ to a $\forall$ as it passes.

Ex) $\lceil[\forall x \exists y \forall z A(x, y, z)] \Leftrightarrow \exists x-[\exists y \forall z A(x, y, z)]$

$$
\begin{aligned}
& \Leftrightarrow \exists x \forall y-[\forall z A(x, y, z)] \\
\Leftrightarrow & \exists x \forall y \exists z-[A(x, y, z)]
\end{aligned}
$$

- One further quantifier that is often useful is

$$
\text { there exists a unique } x \text { such that... }
$$

The usual notation for this quantifier is

## $\exists!$

- This quantifier can be defined in terms of the other quantifiers, by taking

$$
\exists!x \phi(x)
$$

to be an abbreviation for

$$
\exists x[\phi(x) \wedge \forall y[\phi(y) \Rightarrow x=y]]
$$

## Chap 3. Proofs

- In mathematics, truth is determined by constructing a proof(In the natural sciences, truth is established by empirical means.)
- What can be achieved in a short period is gain some understanding of 'what it means to prove a mathematical statement', and 'why mathematicians make such a big deal about proofs'.
$\checkmark$ Proof: a logically sound argument that establishes the truth of the statement.


### 3.1 What is a proof?

- Two main purposes of proof : 1. to establish truth (for myself)

2. to communicate to others.(for someone else)

- Proving a mathematical statement is much more than gathering evidence in its favor.
$\checkmark$ Example) every even number beyond 2 can be expressed as a sum of two
primes. (Goldbach Conjecture) -> Checking the statement from computer(up to $1.6 \times 10^{18}$ ) and it is believed that it is true, but it has not yet been proved.
- There is no particular format that an argument has to have in order to count as a proof
- The one absolute requirement is that it is a logically sound piece of reasoning that establishes the truth of some statement.
- An important secondary requirement is that it is expressed sufficiently well that an intended reader can follow the reasoning.

Goal: Constructing mathematical proofs is one of the most creative acts of the human mind. So, this is very needed

### 3.2 Proof by contradiction

- Proof by contradiction is one of the greatest ways for proof.
- Example of proof by contradiction :

The number $\sqrt{2}$ is irrational.
Proof: Assume, on the contrary, that $\sqrt{2}$ is rational. Then

$$
\sqrt{2}=\frac{p}{q}, p, q: \text { no common factors, and natural numbers }
$$

By squaring and rearranges, $p^{2}=2 q^{2}$ then $p$ must be even $\left(\because p^{2}\right.$ is even, even $^{2}=$ even $)$

Let $p=2 r$ ( $r$ : natural number) so

$$
(2 r)^{2}=2 q^{2} \text { and } 2 r^{2}=q^{2}
$$

It means that $q$ is even ( $\because q^{2}$ is even) also $p$ is even. So, there can be common factors. However, we assume that $p$ and $q$ have no common factors. (Contradiction.)

Hence our original assumption that $\sqrt{2}$ was rational must be false. It means $\sqrt{2}$ must be irrational.

- Approach 1: We want to prove some statement $\phi$. To that end, we begin by assuming $\neg \phi$. We then reason until we establish something that is obviously false. If $\neg \phi$ must be false, $\phi$ must be true.
- Approach 2 : Using method of the contrapositive

Example) $\neg \phi \Rightarrow \varphi$ is equivalent to $\neg \varphi \Rightarrow \phi$

To prove $\phi$ by contradiction, We start with $\neg \phi$ and we deduce $F$ (false statement). It means that we establish $\neg \phi \Rightarrow F$. Because its contrapositive is $T \Rightarrow \phi$, then we proved $T \Rightarrow \phi$. Also by modus ponens, $\phi$ must be true.
$\checkmark$ Modus ponens: If we know $A \Rightarrow B$ is $T$ and $A$ is $T, B$ must be true.

- Proofs by contradiction are a common approach because they have a clear starting point.
$\checkmark$ Cf: In direct proof, we have to generate an argument that culminates in $\phi$. And there are many possible starting points.
- The proof by contradiction approach is particularly suited to establishing that a certain object does not exist. (Assume that object does exist, and we use that object to deduce a false consequence).

Example) A particular kind of equation does not have a solution

### 3.3 Proving conditionals

## - Proof by contradiction:

-when there is no obvious place to start
-useful method to prove non-existence statements

- For example

$$
\phi \Rightarrow \psi
$$

| $\phi$ | $\psi$ | $\phi \Rightarrow \psi$ |
| :---: | :---: | :---: |
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

This conditional is true whenever $\phi$ is false, so we need only consider the case when $\phi$ is true. We can assume $\phi$ is true, and then for this conditional to be valid, $\psi$ must be true.

## - Proving the contrapositive

- using the equivalence of $\phi \Rightarrow \psi$ with the contrapositive $(\neg \psi) \Rightarrow(\neg \phi)$.


### 3.4 Proving quantified statements.

- An existence statement $\exists x A(x)$ could be proved by cases
- Proof by cases : find a particular object $a$ for which $A(a)$.
- Example 1

Theorem : An irrational number exists
Proof : It is enough to show that $\sqrt{2}$ is irrational.

- Example 2

Theorem: There are irrationals $r, s$ such that $r^{s}$ is rational.

Proof : Consider two cases.

Case 1 : If $\sqrt{2}^{\sqrt{2}}$ is rational, we can take $r=s=\sqrt{2}$ : proved
Case 2 : If $\sqrt{2}^{\sqrt{2}}$ is irrational, we can take $r=\sqrt{2}^{\sqrt{2}}, s=\sqrt{2}$
$r^{s}=\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}=(\sqrt{2})^{2}=2$ : rational, proved.
$\checkmark$ We simply showed that such a pair exists.

- Universal statement $\forall x A(x)$
- Approach 1: Take an arbitrary $x$ and show that it must satisfy $A(x)$
- Example of approach 1

Theorem: $(\forall n \in \mathrm{~N})(\exists m \in \mathrm{~N})\left(m>n^{2}\right)$
Proof: Let $n$ : arbitrary natural number. Then $n^{2}$ and $m=n^{2}+1$ is also natural number. So
$(\exists m \in \mathrm{~N})\left(m>n^{2}\right)$ is proved.

- Approach 2 : Sometimes proved by the method of contradiction. By the property of $\neg \forall x A(x)=\exists x(\neg A(x))$, we could start from $\exists x(\neg A(x))$ and find the contradiction.
- Approach 3 : $(\forall n \in \mathrm{~N}) A(n)$ are often proved by Inductions proofs


### 3.5 Induction proofs.

- Principle of mathematical induction :
$\checkmark$ The method of mathematical induction is valid method of proof that works by identifying a repeating pattern.
i. State clearly that the method of induction is being used. (ex: $(\forall n \in \mathrm{~N}) A(n))$
ii. Prove the case $A(1)$ or if $\left(\forall n \geq n_{0}\right)$ then prove the case $A\left(n_{0}\right)$ (Initial step)
iii. Prove the conditional $(\forall n \in \mathrm{~N})(A(n) \Rightarrow A(n+1))$ (Induction step)
- Example 1

Theorem: $(\forall n \in \mathrm{~N})\left(1+2+\ldots+n=\frac{1}{2} n(n+1)\right)$

Proof : Step $1: 1=\frac{1}{2} 1(2) \quad(n=1)$
Step $2:$ from $1+2+\ldots+n=\frac{1}{2} n(n+1): A(n)$
$1+2+\ldots+n+n+1=\frac{1}{2} n(n+1)+(n+1)=\frac{1}{2}(n+1)((n+1)+1): A(n+1)$.

## - Example 2

Theorem : If $x>0$ and $(\forall n \in \mathrm{~N})\left((1+x)^{n+1}>1+(n+1) x\right)$
Proof: Step 1: $(1+x)^{2}=1+2 x+x^{2}>1+2 x: A(1)$ is true
Step 2: $(\forall n \in \mathrm{~N})(A(n) \Rightarrow A(n+1))$
$(1+x)^{n+2}=(1+x)^{1+n}(1+x)>(1+(n+1) x)(1+x)$.
$=1+((n+1)+1) x+(n+1) x^{2}>1+(n+2) x$

- Example 3

Theorem : Every natural number greater than 1 is either a prime or a product of primes.

Proof: The statement is more clear when $B(n)$ is like this
$B(n)$ : every natural number $m$ such that $1<m \leq n$ is either a prime or a product of primes.

Then the statement is $(\forall n \geq 1) B(n)$

Step 1: $1<m \leq 2$ and 2 is prime so $B(2)$ is true.
Step 2 : Assume $B(n)$ and $1<m \leq n+1: B(n+1)$
If $m \leq n$, then by $B(n), m$ is either a prime or a product of primes.
If $n+1$ is prime, $1<m \leq n+1: B(n+1)$ is true.
If $n+1$ is composite, then $1<p, q<n+1$ and $n+1=p q$. By $B(n), p, q$ is also prime or a product of primes, and $n+1=p q$ is also a product of primes. Then,
$(\forall n \geq 1) B(n)$ is proved.

## Chapter 4 Proving results about numbers.

- The integers and the real numbers provide convenient mathematical domains to illustrate mathematical proofs. The principal advantage from an educational perspective being that everyone has some familiarity with both number systems, yet very likely won't have been exposed to their mathematical theories.


### 4.1 The Integers

- The mathematical interest in the integer lies in their arithmetical systems : properties of add, subtract, multiplication, and division.
- If we restrict arithmetic to the integers, division actually leads to two numbers : a quotient and a remainder.
- Theorem 4.1.1 (The Division Theorem) : Let $a, b$ be integers, $b>0$. Then there are unique integers $q, r$ such that $a=q \cdot b+r$ and $0 \leq r<b$.

Proof : Two things to be proved : 'Existence of $q, r$ ' and 'Uniqueness of $q, r$ '

The idea to prove existence : Look at all non-negative integers of the form $a-k b$, $k$ :integer, and show that one of them is less than $b$.

$$
\text { If } k=-|a| \text {, then } a-k b=a+|a| \cdot b \geq a+|a| \geq 0 .(\because b \geq 1)
$$

Integer $a-k b \geq 0$ do exist. Take the smallest value $r$ and let $k=q$ for which it occurs. ( $r=a-q b$ )

To complete the existence proof, we show that $r<b$. Suppose that $r \geq b$, then (Using the contradiction method)

$$
a-(q+1) b=a-q b-b=r-b \geq 0
$$

Thus, $a-(q+1) b$ is non-negative integer of the form $a-k b . r$ was chosen as the smallest one but $a-(q+1) b \leq a-q b=r$. There is a contradiction. So $r<b$ is proved.

The idea to prove uniqueness: Show that $a=q b+r=q^{\prime} b+r^{\prime}\left(0 \leq r, r^{\prime}<b\right)$ actually means that $r=r^{\prime}$ and $q=q^{\prime}$.

From the equation, $r^{\prime}-r=b \cdot\left(q-q^{\prime}\right)$ and $\left|r^{\prime}-r\right|=b \cdot\left|\left(q-q^{\prime}\right)\right|$.
Because $-b<r^{\prime}-r<b$, then $b \cdot\left|\left(q-q^{\prime}\right)\right|<b$ and $\left|\left(q-q^{\prime}\right)\right|<1$

Because we only concern about integers, it has to be $q-q^{\prime}=0$ and $q=q^{\prime}$. From $r^{\prime}-r=b \cdot\left(q-q^{\prime}\right)$, also it becomes $r=r^{\prime}$.

- Conclusively, our focus here is on the method we use to prove that the Division Theorem is true for all pairs of integers. By experience of rigorous proofs on obvious problem, we can accept results that are not at all obvious.
$\checkmark$ Example : David Hilbert's infinite rooms story.
- The significance of understanding infinity is that it is the key to calculus which was bedrock of modern science.
- Theorem 4.1.2 (Generalized Division Theorem) : Let $a, b$ : integers, $b \neq 0$, then there are unique integers $q, r$ such that $a=q \cdot b+r$ and $0 \leq r<|b|$.

Proof: The case $b>0$ was proved from Theorem 4.1.1. Then we assume that $b<0$. It means that $|b|>0$. From the theorem 4.1.1, there are unique integers $q^{\prime}, r^{\prime}$ such that $a=q \cdot|b|+r$ and $0 \leq r<|b|$.

Set $q=-q^{\prime}, r=-r^{\prime}$, and then $|b|=-b$. So we get $a=q \cdot b+r$ and $0 \leq r<|b|$.

- The Division Theorem yields many results that can be of assistance in computational work.
$\checkmark$ Example : odd number is on more than a multiple of 8.
- In case division of $a$ by $b$ produces a remainder $r=0: a$ is divisible by $b$ : $b \mid a$
- The notation $b \mid a$ refers to a relationship between the two numbers $a$ and $b$.

It is either true or false. It is not a notation for a number.

- Theorem 4.1.3 (Basic properties of divisibility) : Let $a, b, c, d$ be integers, $a \neq 0$. Then :
i. $\quad a|0, a| a$;
ii. $\quad a \mid 1$ iff $a= \pm 1$;
iii. If $a \mid b$ and $c \mid d$, then $a c \mid b d$ (for $c \neq 0$ );
iv. If $a \mid b$ and $b \mid c$, then $a \mid c$ (for $b \neq 0$ );
v. $\quad[a \mid b$ and $b \mid a]$ iff $a= \pm b$;
vi. If $a \mid b$ and $b \neq 0$, then $|a| \leq|b|$;
vii. If $a \mid b$ and $a \mid c$, then $a \mid(b x+c y)$ for any integers $x, y$.
$\checkmark \quad$ Proof is in the exercises 4.1.3.
- Prime number : An integer $p>1$ which is only divisible by 1 and $p$.
- Composite number : natural number $n>1$ that is not prime
- Most of the interest in the prime numbers stems from Fundamental Theorem of Arithmetic.
$\checkmark$ Prime decomposition : The expression of a composite number as a product of primes.
- Theorem 4.1.4 (Fundamental Theorem of Arithmetic) : Any natural number greater than 1 is either a prime or can be expressed as a product of prime numbers in a way that is unique except for the order in which they are written.

Proof: The existence of a prime decomposition : it was proved in chapter 3 by induction method.

Uniqueness of a prime decomposition: It could be proved by contradiction. Assume
that n is the smallest composite number which is expressed by two different prime decompositions

$$
n=p_{1} p_{2} \ldots p_{r}=q_{1} q_{2} \ldots q_{s}
$$

By Euclid's Lemma and since $p_{1}$ could divide $n$ and $\left(q_{1}\right)\left(q_{2} \ldots q_{s}\right)$, either $p_{1} \mid q_{1}$ or $p_{1} \mid q_{2} \ldots q_{s}$. It means that $p_{1}=q_{i}$ for $1 \leq i \leq s$. So by removing $p_{1}$ and $q_{i}$, we could obtain a number smaller than $n$ having two different prime decompositions. But $n$ should be smallest one. There is a contradiction.
$\checkmark$ Euclid's lemma: if a prime $p$ divides a product $a b$, then $p$ divides at least one of $a, b$.

### 4.2 The real numbers.

- Number arose from the formalization of two different human-cognitive conceptions: counting and measurement. Numbers themselves abstractions that stand for the number of notches on a bone or the length of a measuring device.
- Two different kinds of number : the discrete counting numbers and the continuous real numbers.
- The connection between the two conceptions of numbers was made by showing how it is possible to define the rationals $\mathbb{Q}$ and then use the rationals to define the real numbers $\mathbb{R}$.
- From the integers, a rational number is simply a ratio of two integers. With the ratinonals, we have a system of numbers adequate for any real-world measurement.
- Theorem 4.2.1: If $r, s$ are rationals, $r<s$, then there is a rational $t$ such that $r<t<s$.

Proof: Let $t$ is average of $r$ and $s$. Clearly $r<t<s$. And letting $r=m / n, s=p / q$, $m, n, p, q \in \mathbb{Z}$, we have

$$
t=\frac{1}{2}(r+s)=\frac{m q+n p}{2 n q}
$$

Since $m q+n p, 2 n q \in \mathbb{Z}$, so $t \in \mathbb{Q}$.

- The property of theorem 4.2.1 is called density : A third rational between any two unequal rationals. It means that between any two rational numbers there are infinitely many other rational numbers. So we can measure anything in the real world.
- But in mathematics although the rationals are dense, there are still holes in the rational lines.
$\checkmark$ The length of the hypotenuse of a right angled triangle with equal height and width is not rationals.
- If we let $A=\left\{x \in \mathbb{Q} \mid x \leq 0 \vee x^{2}<2\right\}$, and $B=\left\{x \in \mathbb{Q} \mid x>0 \wedge x^{2} \geq 2\right\}$, then all element of $A$ is less than every element of $B$ and $A \cup B=\mathbb{Q}$. But $A$ has no greatest elements and $B$ has no smallest elements, So there is still a sort of hole between A and B .
- The numbers that fill in the holes are the irrational numbers. Taken together, the rational numbers and the irrational numbers constitute real numbers.
- In a very precise sense there are 'infinitely more' irrational numbers between them then there are rational numbers between them. So if we were to select a real number at random, the probability that it would be irrational is 1.
- In the case of infinite recurring decimals, the expression denotes a rational number. But if there is no recurring pattern, the result is an irrational number.


### 4.3 Completeness

- One of the most valuable results to come out of the construction of the real number system was the formulation of a simple property of the reals that captures those infinitesimal holes in the rational line and specifies exactly how
they are filled. : Completeness Property
- Some special notations of interval : Let $a, b \in \mathbb{R}, a<b$.
$\checkmark$ Interval : An uninterrupted stretch of the real line.
i. The open interval $(a, b)=\{x \in \mathbb{R} \mid a<x<b\}$.
ii. The closed interval $[a, b]=\{x \in \mathbb{R} \mid a \leq x \leq b\}$.
iii. A left-closed, right-open interval $[a, b)=\{x \in \mathbb{R} \mid a \leq x<b\}$.
iv. A left-open, right-closed interval $(a, b]=\{x \in \mathbb{R} \mid a<x \leq b\}$.
v. $(-\infty, a)=\{x \in \mathbb{R} \mid x<a),(a, \infty)=\{x \in \mathbb{R} \mid x>a)$
- $b$ is an upper bound of A: $(\forall a \in A)[a \leq b], A$ : set of reals.
- $b$ is a least upper bound of A : if for any upper bound $c$ of $A, b \leq c: \operatorname{lub}(A)$.
- Completeness Property of real number system says that any nonempty set of reals that has an upper bound has a least upper bound in $\mathbb{R}$
- Theorem 4.3.1 : The rational line $(\mathbb{Q})$ does not have the completeness property.

Proof: Let $A=\left\{r \in \mathbb{Q} \mid r \geq 0 \wedge r^{2}<2\right\}, x=p / q \in \mathbb{Q}$ : any upper bound of $A$.
First, suppose that $x^{2}<2$, then $2 q^{2}>p^{2}$. If we pick enough large $n \in N$

$$
\frac{n^{2}}{2 n+1}>\frac{p^{2}}{2 q^{2}-p^{2}}
$$

From rearranging,

$$
y^{2}=\left(\frac{n+1}{n} \cdot \frac{p}{q}\right)^{2}<2
$$

Since $(n+1) / n>1, x<y$. Because of $y^{2}<2$, also $y \in A$. But this contradicts the fact that x is an upper bound for $A$.

Next, suppose $x^{2} \geq 2$. Since $x$ is rational, $x^{2} \neq 2$. Then $x^{2}>2$ and $p^{2}>2 q^{2}$. If we
pick enough large $n \in N$.

$$
\frac{n^{2}}{2 n+1}>\frac{q^{2}}{p^{2}-2 q^{2}}
$$

From rearranging,

$$
y^{2}=\left(\frac{n}{n+1} \cdot \frac{p}{q}\right)^{2}>2
$$

Since $n /(n+1)<1, y<x$. But for any $a \in A, a^{2}<2<y^{2}$, so $a<y$. Thus $y$ is upper bound of $A$ less than $x$ (This means that there is no the least one).

### 4.4 Sequences

- Sequence : The set of numbers $a_{n}$, arranged according to the index $n$ : $\left\{a_{n}\right\}_{n=1}^{\infty}=a_{1}, a_{2}, \ldots, a_{n} \ldots$
- The ordering in which the members of the sequence appear is important $(1,2,3, \ldots \neq 2,1,3, \ldots)$.
- In short, there is no restriction on what the members of a sequence $\left\{a_{n}\right\}_{n=1}^{\infty}$ may be, except that they be real numbers. (sequence의 element로 허수는 안되는 건 가...?)
- Rather special property: As we go along the sequence, the sequence number get closer to some fixed number.
$\checkmark$ Example : $\{1 / n\}_{n=1}^{\infty}=1,1 / 2, \ldots 1 / n \ldots: \lim _{n \rightarrow \infty} a_{n}=0$.
- If the sequence $\left\{a_{n}\right\}_{n=1}^{\infty}$ number get closer to fixed number $a$ in this manner, we say that the sequence $\left\{a_{n}\right\}_{n=1}^{\infty}$ tends to the limit $a$, and write $a_{n} \rightarrow a$ as $n \rightarrow \infty$, and common notation is $\lim _{n \rightarrow \infty} a_{n}=a$.
$\checkmark a_{n}$ gets arbitrarily closer to $a=$ The difference $\left|a_{n}-a\right|$ gets arbitrarily close to $0=$ Whenever $\varepsilon$ is a positive real number, the difference $\left|a_{n}-a\right|$ is
eventually less than $\varepsilon$.
- Theorem : $a_{n} \rightarrow a$ as $n \rightarrow \infty$ iff $(\forall \varepsilon>0)(\exists n \in \mathrm{~N})(\forall m \geq n)\left(\left|a_{m}-a\right|<\varepsilon\right)$

Analyze: $(\exists n \in \mathrm{~N})(\forall m \geq n)\left(\left|a_{m}-a\right|<\varepsilon\right)$ : There is an $n$ such that for all $m$ greater than or equal to $n$, the distance from $a_{m}$ to $a$ is less than $\varepsilon$.

In other words, there is an $n$ such that all terms in the sequence $\left\{a_{n}\right\}_{n=1}^{\infty}$ beyond $a_{n}$ lie within the distance $\varepsilon$ of $a$.

Thus, $(\forall \varepsilon>0)(\exists n \in \mathrm{~N})(\forall m \geq n)\left(\left|a_{m}-a\right|<\varepsilon\right)$ says that for every $\varepsilon>0$, the members of the sequence $\left\{a_{n}\right\}_{n=1}^{\infty}$ are eventually all within the distance $\varepsilon$ of $a$. : Formal definition of " $a_{n}$ gets arbitrarily closer and closer to $a$ ".

- Statement: $1 / n \rightarrow 0$ as $n \rightarrow \infty$ iff $(\forall \varepsilon>0)(\exists n \in \mathrm{~N})(\forall m \geq n)(|1 / m-0|<\varepsilon)$

Proof : Let $\varepsilon>0$ be arbitrary. If we pick $n$ large enough, so that $n>1 / \varepsilon$. By $m \geq n, 1 / m \leq 1 / n<\varepsilon$ : proved.

- Statement : $n /(n+1) \rightarrow 1$ as $n \rightarrow \infty$ iff $(\forall \varepsilon>0)(\exists n \in \mathrm{~N})(\forall m \geq n)\left(\left\lvert\, \frac{m}{m+1}-1<\varepsilon\right.\right)$

Proof: If we pick $n$ so large that $n>1 / \varepsilon$, then for $m \geq n$

$$
\left|\frac{m}{m+1}-1\right|=\left|\frac{-1}{m+1}\right|=\frac{1}{m+1}<\frac{1}{m} \leq \frac{1}{n}<\varepsilon: \text { Proved }
$$

- One point to notice here is that our choice of $n$ depended upon the value of $\varepsilon$. The smaller $\varepsilon$ is, the greater our $n$ needs to be.


## Introduction to

## Mathematical Thinking

## (Exercises)

Name: Oliver

Lee Woongbi

Lee Seungchan,

Woo Soogil

Shin Jongmok

## Introduction to Mathematical Thinking.

## Exercise 2.2.1

1. The mathematical concept of conjunction captures the meaning of "and" in everyday language. True or false? Explain your answer.

Sol) No

As we say in the book, "and" in everday language is not always the same meaning of themathematical concept. For example, "I played table tennis and I took shower." Is not the same as I took shower and I played table tennis.", but $\phi \wedge \psi$ is totally equal to $\psi \wedge \phi$ in the mathematical concept
2. Simplify the following symbolic statements as much as you can, leaving your answer in the standard symbolic form.(In case you are not familiar with the notation, I'll answer the first one for you.)

Sol) (a) $0<\pi<10$
(b) $7 \leq p<12$
(c) $5<x<7$
(d) $x<4$
(e) $(y<4) \wedge(-3<y<3) \Leftrightarrow-3<y<3$
(f) $x=0$
3. Express each of your simplified statements from Question 2 in natural English.

Sol) (a) $\pi$ is greater than 0 and $\pi$ is less than 10
(b)p is greater than or equal to 7 , and is less than 12
(c) $x$ is greater than 5 and $x$ is less than 7
(d) $x$ is less than 4 and $x$ is less than 6
(e) $y$ is less than 4 and $y^{2}$ is less than 9
(f) $x$ is greater than or equal to 0 , and is less than or equal to 0
4. What strategy would you adopt to show that the conjunction $\phi_{1} \wedge \phi_{2} \wedge \cdots \wedge \phi_{n}$ is true?

Sol) I would show every single term of $\phi_{1}, \cdots, \phi_{n}$ is true. If it is, $\phi_{1} \wedge \phi_{2} \wedge \cdots \wedge \phi_{n}$ will be true.
5. What strategy would you adopt to show that the conjunction $\phi_{1} \wedge \phi_{2} \wedge \cdots \wedge \phi_{n}$ is false?

Sol) I would show one of $\phi_{1}, \cdots, \phi_{n}$ is false. If it is, $\phi_{1} \wedge \phi_{2} \wedge \cdots \wedge \phi_{n}$ will be false.
6. Is it possible for one of $(\phi \wedge \varphi) \wedge \theta$ and $\phi \wedge(\varphi \wedge \theta)$ to be true and the other false, or does the associative property hold for conjunction? Prove your answer.

Sol) No, it is not possible. Since all elements should be true for the statement of conjunction to be true, definitely, the associative property holds for conjunction.
7. Which of the following is more likely?

Sol) I think (e) is the most likely because $€$ is just a simple statement, but the other statements have at least one requirement.
8. In the following table, T denotes 'true' and F denotes 'false'. The first two columns list all the possible combinations of values of T and F that the two statements $\phi$ and $\psi$ can have. The third column should give the truth value (T or F) $\phi \wedge \psi$ achieves according to each assignment of T or F to $\phi$ and $\psi$.

Sol)


## Exercises 2.2.2

1. Simplify the following symbolic statements as much as you can, leaving your answer in a standard symbolic form(assuming you are familiar with the notation):

Sol) (a) $\pi>3$
(b) $x$ is all number, except for 0
(c) $x \geq 0$
(d) $x \geq 0$
(e) $x<-3, x>3$
2. Express each of your simplified statements from Question 1 in natural English.

Sol)(a) $\pi$ is greater than 3 or $\pi$ is greater than 10
(b) $x$ is less than 0 or $x$ is greater than 0
(c) $x$ is equal to 0 or $x$ is greater than 0
(d) $x$ is greater than 0 or $x$ is greater than or equal to 0
(e) $x$ is greater than 3 or $x^{2}$ is greater than 9
3. What strategy would you adopt to show that the conjunction $\phi_{1} \vee \phi_{2} \vee \cdots \vee \phi_{n}$ is true?

Sol) I would show one of $\phi_{1}, \cdots, \phi_{n}$ is true. If it is, the statement will be true.
4. What strategy would you adopt to show that the conjunction $\phi_{1} \vee \phi_{2} \vee \cdots \vee \phi_{n}$ is false?

Sol) I would show every single term of $\phi_{1}, \cdots, \phi_{n}$ is false. If it is, the statement will be false.
5. Is it possible for one of $(\phi \vee \varphi) \vee \theta$ and $\phi \vee(\varphi \vee \theta)$ to be true and the other false, or does the associative property hold for conjunction? Prove your answer.

Sol) No, it is not possible. To be false, at least one of elements must be false, but if one of them is false, that statement is false. Therefore, the associative property holds for disjunction.
6. Which of the following is more likely?

Sol) I think (a) is the most likely because there are two chances which can be true.
7. Fill in the entries in the fial column of the following truth table:

Sol)


## Exercises 2.2.3

1. Simplify the following symbolic statements as much as you can, leaving your answer in a standard symbolic form (assuming you are familiar with the notation):

Sol) (a) $\pi \leq 3.2$
(b) $x \geq 0$
(c) $x^{2} \leq 0$
(d) $x \neq 1$
(e) $\psi$
2. Express each of your simplified statements from Question 1 in natural English.

Sol)(a) $\pi$ is not greater than 3.2
(b) $x$ is not less than 0
(c) $x^{2}$ is not greater than 0
(d) $x$ isn't equal to 1
(e) $\psi$ is $\psi$
3. Is showing that the negation $\neg \phi$ is true the same as showing that $\phi$ is false?

Explain your answer.

Sol) Yes. I think the statement just says the definition of the negation in mathematics.
4. Fill in the entries in the final column of the following truth table:

Sol)

5. Let $D$ be the statement "The dollar is strong", $Y$ the statement "The Yuan is strong", and T the statement "New US-China trade agreement signed". Express the main content
of each of the following (fictitious) newspaper head-lines in logical notation. (Note that logical notation captures truth, but not the many nuances and inferences of natural language.) Be prepared to justify and defend your answers.
(a) Dollar and Yuan both strong
(b) Trade agreement fails on news of weak Dollar.
(c) Dollar weak but Yuan strong, following new trade agreement
(d) Strong Dollar means a weak Yuan.
(e) Yuan weak despite new trade agreement, but Dollar remains strong
(f) Dollar and Yuan can't both be strong at same time.
(g) If new trade agreement is signed, Dollar and Yuan can't both remain strong.
(h) New trade agreement does not prevent fall in Dollar and Yuan.
(i) US-China trade agreement fails but both currencies remain strong.
(j) New trade agreement will be good for one side, but no one know which.

Sol) (a) $D \wedge Y$
(b) $\neg D \Rightarrow \neg T$
(c) $T \Rightarrow(\neg D \wedge Y)$
(d) $D \Rightarrow \neg Y$
(e) $\neg Y \wedge T \wedge D$
(f) $D \Rightarrow \neg Y$ or $Y \Rightarrow \neg D$
$(\mathrm{g}) T \Rightarrow \neg(D \wedge Y)$
(h) $T \wedge \neg D \wedge \neg Y$
(i) $\neg T \wedge D \wedge Y$
$(\mathrm{j}) \mathrm{T} T \Rightarrow(D \wedge \neg Y) \vee(\neg D \wedge Y)$
6. In US law, a trial verdict of "not guilty" is given when the prosecution fails to prove guilt. This, of course, does not mean the defendant is, as a matter of actual fact, innocent. Is this state of affairs captured accurately when we use "not" in the mathematical sense?(i.e., Do "Not guilty" and " $\neg$ guilty" means the same thing?) What if we change the question to ask if "Not proven" and " $\urcorner$ proven" mean the same thing?

Sol) No, because not guilty, i.e, $\neg$ guilty means innocent in mathematical sense. If we change "not guilty" to "Not proven", it means innocent, so it becomes the same meaning in mathematical sense.
7. The truth table for $\neg \neg \phi$ is clearly the same as that for $\phi$ itself, so the two expressions make identical truth assertions. This is not necessarily true for negation in everyday life. For example, you might find yourself saying "I was not displeased with the movie." In terms of formal negation, this has the form $\neg(\neg$ PLEASED ), but your statement clearly does not mean that you were pleased with the movie. Indeed, it means something considerably less positive. How would you capture this kind of use of language in the formal framework we have been looking at?

## Exercise 2.3.1

1. F
2. In case of that $\phi$ is $T$ and $\psi$ if $F$, the genuine implication must be $F$. Hence, the conditional $[\phi \Rightarrow \psi]$ should be false as well. Because if there were a genuine implication, then the truth of $\psi$ would follow automatically from the truth of $\phi$.

## Exercise 2.3.2

1. In order $T, T$
2. To deal with this case, we consider negation. In terms of truth values, $\phi$ will not imply $\psi$ if it is the case that although $\phi$ is true, $\psi$ is nevertheless false. We therefore define $\phi \nRightarrow \psi$ to be true precisely in case $\phi$ is T, $\psi$ is F. Hence, $\phi \Rightarrow \psi$ will be true. $\phi$ is F, and $\psi$ is T or $\phi$ and $\psi$ are both T.

## Exercise 2.3.3

1.(a) $T \Rightarrow T, \therefore T$
(b) $F \Rightarrow F, \therefore T$
(c) $T \Rightarrow F, \therefore F$
(d) $T \Rightarrow F, \therefore F$
(e) $T \Rightarrow F, \therefore F$
(f) $F \Rightarrow T, \therefore T$
(g) $T \Rightarrow T, \therefore T$
(h) $F \Rightarrow F, \therefore T$
(i) $F \Rightarrow F, \therefore T$
(j) $\Rightarrow F, \therefore T$

All answers are based on truth table we looked through. Although we can't find the truth value of the last one's antecedent, we could get T because the consequent of the last one is $T$. In this case, regardless of the antecedent conditional is $T$.
2.(a) $T \Rightarrow[D \wedge Y]$
(b) $T \Rightarrow[Y \Rightarrow \neg D] \Leftrightarrow[T \wedge Y] \Rightarrow \neg D$
(c) $T \Rightarrow(\neg D \wedge Y)$
(d) $D \Rightarrow \neg Y$
(e) $(T \Rightarrow[Y \Leftrightarrow D]) \Leftrightarrow(T \Rightarrow[(Y \Rightarrow D) \wedge(D \Rightarrow Y)])$
3.

| $\phi$ | $\neg \phi$ | $\psi$ | $\phi \Rightarrow \psi$ | $\neg \phi \vee \psi$ |
| :--- | :--- | :--- | :--- | :--- |
| T | F | T | T | T |
| T | F | F | F | F |
| F | T | T | T | T |
| F | T | F | T | T |

4. $(\phi \Rightarrow \psi) \Leftrightarrow(\neg \phi \vee \psi)$
5. 

| $\phi$ | $\psi$ | $\neg \psi$ | $\phi \Rightarrow \psi$ | $\phi \nexists \psi$ | $\phi \wedge \neg \psi$ |
| :--- | :--- | :--- | :--- | :--- | :--- |
| T | T | F | T | F | F |
| T | F | T | F | T | T |
| F | T | F | T | F | F |

6. $(\phi \nRightarrow \psi) \Leftrightarrow(\phi \wedge \neg \psi)$

## Exercises 2.4.1

The same kind of argument I just outlined to show that the cubic equation $y=x^{3}+3 x+1$ has a real root, can be used to prove the "Wobbly Table Theorem." Suppose you are sitting in a restaurant at a perfectly square table, with four identical legs, one at each corner. Because the floor is uneven, the table wobbles. One solution is to fold a small piece of paper and insert it under one leg until the table is stable. But there is another solution. Simply by rotating the table you will be able to position it so it does not wobble. Prove this.

Sol) A table will always rest on at least three legs, even if one leg is in the air. Suppose the four corners are labeled A, B, C, D going clockwise round the table, and that leg A is in the air.

We assume the following three arguments:

1) Since the length of four legs is identical, we can assume the center of the four points $A, B, C, D$ is on the $z$ axes. If we ask the three legs $A, B, C$ to be on the ground and the direction of the axes $A C$ is given by the $x$ axis, then we can define the angle of point $A$ (angle(x)) and the position of the table.
2) Define the function $f(z)$ which is the signed vertical distance of the leg A point from the ground. This value depends on angle(x). It can be positive if it is above the surface, and it can be negative if it is below the surface.
3) Start with zero degree of point $A$ (angle $x$ ) and leg $A$ is above the ground $(f(z=0)>0)$ Turn the table around on a center of four points A, B, C, D and keep three legs $B, C, D$ stay on the surface. We want to show that angle $(x=p i / 2)$ is smaller than 0 . The intermediate value theorem will then assure that there exists an angle, where $f(z)=0$. It means that there is an angle, where the fourth leg is also on the surface. The other case is similar.

## Exercises 2.4.2

1. Express the following as existence assertions.
(a) The equation $x^{3}=27$ has a natural number solution.

Sol) $(\exists x \in \mathbb{N})\left[x^{3}=27\right]$
(b) 1,000,000 is not the largest natural number.

Sol) $(\exists x \in \mathbb{N})[x>1000000]$
(c) The natural number n is not a prime.

Sol) $\begin{aligned} & (\exists n \in \mathbb{N})(\forall x \in \mathbb{N})[1<x<n \wedge n / x) \\ & (\exists p \in \mathbb{N})(\exists q \in \mathbb{N})[p>1 \wedge q>1 \wedge n=p q]\end{aligned} \quad$ or
2. Express the following as 'for all' assertions.
(a) The equation $x^{3}=28$ does not have a natural number solution.

Sol) $\begin{aligned} & \neg(\exists x \in \mathbb{N})\left[x^{3}=28\right] \\ & (\forall x \in \mathbb{N})\left[x^{3} \neq 28\right]\end{aligned}$ or
(b) 0 is less than every natural number.

Sol) $(\forall x \in \mathbb{N})(x>0)$
(c) The natural number n is a prime.

Sol) $\begin{aligned} & (\exists n \in \mathbb{N})(\forall x \in \mathbb{N})[1<x<n \wedge n X x) \\ & (\forall p \in \mathbb{N})(\forall q \in \mathbb{N})[p=1 \vee q=1 \vee n \neq p q]\end{aligned}$ or
3. Express the following in symbolic form, using quantifiers for people:
(a) Everybody loves somebody.

Sol) Let's define group $P$ is all people. And let's define $L(x, y)$ as " $x$ loves $y$ ".

Then we can express following proposition: $(\forall x \in P)(\exists y \in P)(L(x, y))$
(b) Everyone is tall or short.

Sol) Let's define $T(x)$ as tall people of $x$, and let's define $S(x)$ as short people of $x$.
Then we can express following proposition: $(\forall x \in P)(T(x) \vee S(x))$
(c) Everyone is tall or everyone is short.

Sol) $(\forall x \in P) T(x) \vee(\forall x \in P) S(x)$
(d) Nobody is at home.

Sol) Let's define $S(x)$ as someone $x$ who stays at home.

Then we can express following proposition: $\quad \begin{array}{ll}\neg(\forall x \in P) S(x) \\ (\exists x \in P) \neg S(x)\end{array}$ or
(e) If John comes, all the women will leave.

Sol) Comes(John) $\Rightarrow(\forall x \in$ women $)$ Leaves $(x)$
(f) If a man comes, all the women will leave.

Sol) Comes(man) $\Rightarrow(\forall x \in$ women $)$ Leaves $(x)$
4. Express the following using quantifiers that refer (only) to the sets $\mathbb{R}$ and $\mathbb{N}$ :
(a) The equation $x^{2}+a=0$ has a real root for any real number $a$.

Sol $)(\forall x \in \mathbb{R})(\exists a \in \mathbb{R})\left[x^{2}+a=0\right]$
(b) The equation $x^{2}+2=0$ has a real root for any negative real number $a$.

Sol) $(\forall x \in \mathbb{R})(\exists a \in \mathbb{R})\left[a<0 \wedge x^{2}+a=0\right]$
(c) Every real number is rational.

Sol $)(\forall x \in \mathbb{R})(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})[x=p / q \wedge x=-p / q]$
(d) There is an irrational number.

Sol $)(\exists x \in \mathbb{R})(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(x \neq p / q \wedge x \neq-p / q)$
(e) There is no largest irrational number.

Sol) $(\exists x \in \mathbb{R})(\forall \mathrm{y} \in \mathbb{R})[x>y] \wedge(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})[x \neq p / q]$
5. Let $C$ be the set of all cars, let $D(x)$ mean that $x$ is domestic, and let $M(x)$ mean that $x$ is badly made. Express the following in symbolic form using these symbols:
(a) All domestic cars are badly made.

Sol) $(\forall x \in C)[D(x) \Rightarrow M(x)]$
(b) All foreign cars are badly made.

Sol) $(\forall x \in C)[\neg D(x) \Rightarrow M(x)]$
(c) All badly made cars are domestic.

Sol) $(\forall x \in C)[M(x) \Rightarrow D(x)]$
(d) There is a domestic car that is not badly made.

Sol) $(\exists x \in C)[D(x) \wedge \neg M(x)]$
(e) There is a foreign car that is badly made.

Sol) $(\forall x \in C)[\neg D(x) \wedge M(x)]$
6. Express the following sentence symbolically, using only quantifiers for real numbers, logical connectives, the order relation <, and the symbol $\mathrm{Q}(\mathrm{x})$ having the meaning ' x is rational':

Sol)"There is a rational number between any two unequal real numbers."

$$
(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})[a<b] \Rightarrow \exists x[Q(x) \wedge(a<x<b)]
$$

7. Express the following famous statement (by Abraham Lincoln) using quantifiers for people and times: "You may fool all the people some of the time, you can even fool some of the people all of the time, but you cannot fool all of the people all the time."

Sol)Let's define $F(p, t)$ as "you can fool a person $p$ at time t."

Then,
$\exists t \forall p[F(p, t)] \wedge \forall t \exists p[F(p, t)] \wedge \neg \forall t \forall p[F(p, t)]$
$\exists t \forall p[F(p, t)] \wedge \forall t \exists p[F(p, t)] \wedge \exists t \exists p[\neg F(p, t)]$
8. A US newspaper headline read, "A driver is involved in an accident every six seconds." Let $x$ be a variable to denote a driver, $t$ a variable for a six-second interval, and $A(x, t)$ the property that $x$ is in an accident during interval $t$. Express the headline in logical notation.

Sol) $\exists x \forall t[A(x, t)]$

## Excersises 2.4.3

1. Show that $\neg[\exists x A(x)]$ is equivalent to $\forall x[\neg A(x)]$.

Sol) If we show first quantifier implies second one and second one implies first one, then it means that first one is equivalent to second one.

We assume that $\neg[\exists x A(x)]$, that is, we assume it is not the case $\exists x A(x)$. If it is not the case that there is at least an $x$ satisfying $A(x)$, it must happen that all $x$ must fail to satisfy $A(x)$. In other words, for all $x, \neg A(x)$ must be true. In symbols, it can be represented as $\forall x[\neg A(x)]$. Hence, $\neg[\exists x A(x)]$ implies to $\forall x[\neg A(x)]$.

Now assume that $\forall x[\neg A(x)]$. So, There will be all $x$ for which $A(x)$ fails. Hence, $A(x)$ does not hold for at least an $x$. In other words, it is false that $A(x)$ holds for at least one $x$. In symbols, it can be represented as $\neg[\exists x A(x)]$. Thus, $\forall x[\neg A(x)]$ implies $\forall x[\neg A(x)]$.

Therefore, we show that $\neg[\exists x A(x)]$ is equivalent to $\forall x[\neg A(x)]$.
2. Give an everyday example to illustrate this equivalence, and verify it by an argument specific to your example.

Sol) $1^{\text {st: }}$ It is not the case that there is at least one student who could get a scholarship. is equivalent to
$2^{\text {nd. }}$ For all students, scholarship couldn't be given.

If we show first statement implies second one and second one implies first one, we verify the whole statement I wrote above. Let's do it.

First statement must happen when all students couldn't get a scholarship. In other words, For all students, scholarship must not be given. So, first statement implies second statement.

Second statement says that there will be all students who couldn't get a scholarship. Therefore, what the scholarship must be given can't hold for at least one student. So, second statement implies one statement.

Hence, we verify it by argument.

## Exercises 2.4.4

Prove that the statement

There is an even prime bigger than 2 is false.
So1) Let $\mathrm{P}(\mathrm{x})$ denotes the property " x is a prime" and $\mathrm{O}(\mathrm{x})$ the property " x is even" $(\exists x>2)[P(x) \Rightarrow O(x)]$
(This is False.)

Negation
$(\forall x>2)[P(x) \wedge \neg O(x)]$
(This should become a true.)

To get to this form
$\neg(\exists x>2)[P(x) \Rightarrow O(x)]$
Equivalent $(\forall x>2)-[P(x) \Rightarrow O(x)]$
And that in turn us equivalent $(\forall x>2)[P(x) \neq>O(x)]$
Which we can reformulate as $(\forall x>2)[P(x) \wedge \neg O(x)]$

## Exersises 2.4.5

1. Translate the following sentences into symbolic form using quantifiers. In each case the assumed domain is given in parentheses.
2. Negate each of the symbolic statements you wrote in Question 1, putting your answers in positive form. Express each negation in natural, idiomatic English.
(A solution to each problem is in order, that is, first one is a solution to 1 and second one is a solution to 2.)
(a) All students like pizza. (All people)

Sol) Let P be the set of all people, $\mathrm{S}(\mathrm{x})$ means x is students, $\mathrm{L}(\mathrm{x})$ means x like pizza.
$(\forall x \in P)(S(x) \Rightarrow L(x))$.
Negation: $(\exists x \in P)(S(x) \neq>L(x))$
$(S(x) \neq>L(x))$ is equivalent to $(S(x) \wedge \neg L(x))$.
(b) One of my friends does not have a car. (All people)

Sol) Let P be the set of all people, $\mathrm{O}(\mathrm{x})$ means x is one of my friends, $\mathrm{C}(\mathrm{x})$ means x have a car.
$(\exists x \in P)(O(x) \Rightarrow \neg C(x))$.
Negation: $(\forall x \in P)((O(x) \wedge C(x)))$
(c) Some elephants do not like muffins. (All animals)

Sol) Let $A$ be the set of all animals, $E(x)$ means $x$ is elephants, $M(x)$ means $x$ like muffins.
$(\exists x \in A)(E(x) \Rightarrow \neg M(x))$.
Negation : $(\forall x \in A)(E(x) \neq>\neg M(x))$
$(\forall x \in A)(E(x) \wedge M(x))$.
(d) Every triangle is isosceles. (All geometric figures)

Sol) Let $G$ be the set of geometric figures, $T(x)$ means $x$ is triangle, $I(x)$ means $x$ is isosceles.
$(\forall x \in G)(T(x) \Rightarrow I(x))$.
Negation: $(\exists x \in G)(T(x) \neq>I(x))$
$(\exists x \in G)(T(x) \wedge \neg I(x))$.
(e) Some of the students in the class are not here today. (All people)

Sol) Let P be the set of all people, $\mathrm{S}(\mathrm{x})$ means x is student, $\mathrm{T}(\mathrm{x})$ means x are here today.
$(\exists x \in P)(S(x) \Rightarrow \neg T(x))$.
Negation: $(\forall x \in P)(S(x) \wedge T(x))$
(f) Everyone loves somebody. (All people)

Sol) All people $x$, some man $y$.
$(\forall x)(\exists y) L(x, y)$. Where $\mathrm{L}(\mathrm{x}, \mathrm{y})$ denotes " x loves y "

Negation :
$(\exists x)(\forall y) \neg L(x, y)$.

Somebody does not love everyone.
(g) Nobody loves everybody. (All people)

Sol 1) All people $x$, some man $y$.
$\neg(\exists y)(\forall x) L(x, y)$. Where $L(x, y)$ denotes " $x$ loves $y^{\prime \prime}$

Sol 2) All people $x, y$.
$(\forall x)(\neg(\exists y))(L(x) \Rightarrow L(y))$.

Sol 1) Negation :
$(\exists y)(\forall x) L(x, y)$.
Nobody does not love everyone.

Sol 2) Negation :
$(\exists x)(\exists y)(L(x) \wedge \neg L(y))$
(h) If a man comes, all the women will leave. (All people)

Sol) $x$ are people. Let man set M , women set W .
$(\exists x \in M)[C(x)]=>(\forall x \in W)[L(x)]$.
Negation :
$((\forall x \in M)[C(x)]) \wedge((\exists x \in W) \rightharpoondown[L(x)])$
(i) All people are tall or short. (All people)

Sol) Let $\mathrm{P}(\mathrm{x})$ :" x is person", $\mathrm{T}(\mathrm{x}): \mathrm{x}$ is tall, $\mathrm{S}(\mathrm{x}): \mathrm{x}$ is short
$\forall x(P(x) \Rightarrow(T(x) \vee S(x)))$.
Negation :
$\exists x(P(x) \neq>(T(x) \vee S(x)))$
$\exists x(P(x) \wedge \neg(T(x) \vee S(x)))$
$\exists x(P(x) \wedge(\neg T(x) \wedge \neg S(x)))$
There are people that are not tall and not short.
(j) All people are tall or all people are short. (All people)

Sol) $\forall x((P(x) \Rightarrow T(x)) \vee(P(x) \Rightarrow S(x)))$.
Negation :
$\exists x(((P(x) \neq>T(x)) \wedge(P(x) \neq>S(x)))$
$\exists x((P(x) \wedge \neg(T(x)) \wedge(P(x) \wedge \neg(S(x)))$
There are people that are not tall and not short.
(i=j) $\forall x(\neg P(x) \vee(T(x) \vee S(x)))$.
$\Leftrightarrow \forall x((\neg P(x) \vee T(x)) \vee(\neg P(x) \vee S(x)))$.
$\Leftrightarrow \forall x((P(x) \Rightarrow T(x)) \vee(P(x) \Rightarrow S(x)))$.
(k) Not all precious stones are beautiful. (All stones)

Sol) Let :" x is stones", $\mathrm{P}(\mathrm{x}): \mathrm{x}$ is precious stones, $\mathrm{B}(\mathrm{x}): \mathrm{x}$ is beautiful.
$\forall x(\neg P(x) \Rightarrow B(x))$.
Negation :
$\exists x(\neg P(x) \neq>B(x))$
$\exists x(\neg P(x) \wedge \neg B(x))$
(I) Nobody loves me. (All people)

Sol) All people $\mathrm{x}, \mathrm{y}$ is me.
$\neg(\exists y)(\forall x) L(x, y)$. Where $\mathrm{L}(x, y)$ denotes " x loves $\mathrm{y} "$
Negation :
$(\exists y)(\forall x) L(x, y)$.
I do not love everyone.
(m) At least one American snake is poisonous. (All snakes)

Sol) Snake is $x, A(x)$ is at least one American snake, $P(x)$ is poisonous.
$\forall x(A(x) \Rightarrow P(x))$.
Negation: $\exists x(A(x) \neq>P(x))$
$\exists x(A(x) \wedge \neg P(x))$.
(n) At least one American snake is poisonous. (All animals)

Sol) Let A be the set of all animals, Snake is $\mathrm{x}, \mathrm{A}(\mathrm{x})$ is at least one American snake, $\mathrm{P}(\mathrm{x})$ is poisonous.
$(\forall x \in A)\left(A_{5}(x) \Rightarrow P(x)\right)$.
Negation: $(\exists x \in A)\left(A_{5}(x) \neq>P(x)\right)$
$(\exists x \in A)\left(A_{s}(x) \wedge \neg P(x)\right)$.
2. Which of the following are true? The domain for each is given in parentheses.
(a) $\forall x(x+1 \geq x)$ (Real numbers)

Sol) True. For all real numbers $x, x \geq x-1 . \mathrm{x}$
(b) $\exists x(2 x+3=5 x+1)$ (Natural numbers)

Sol) False. $-3 x=-2, x=2 / 3$. This is not natural numbers. So $x$ not exist.
(c) $\exists x\left(x^{2}+1=2^{x}\right)$ (Real numbers)

Sol) True. $x=1$ exist.
(d) $\exists x\left(x^{2}=2\right)$ (Rational numbers) 유리수

Sol) $x= \pm \sqrt{2}$. False. Root 2 is irrational number.
(e) $\exists x\left(x^{2}=2\right)$ (Real numbers) 실수(유리수 + 무리수)

Sol) $x= \pm \sqrt{2}$. True. Root 2 is irrational number. So real number.
(f) $\forall x\left(x^{3}+17 x^{2}+6 x+100 \geq 0\right)$ (Real numbers)
$\left[x_{1}\right]=\frac{\sqrt[3]{-2 b^{3}+9 a b c-27 a^{2} d+\sqrt{4\left(-b^{2}+3 a c\right)^{3}+\left(-2 b^{3}+9 a b c-27 a^{2} d\right)^{2}}}}{3 \sqrt[3]{2} a}$

$\left[x_{2}\right]=-\frac{\left(1-\sqrt{3} v \cdot \sqrt[3]{-2 b^{3}+9 a b c-27 a^{2} d+\sqrt{4\left(-b^{2}+3 a c\right)^{3}+\left(-2 b^{3}+9 a b c-27 a^{2} d\right)^{2}}}\right.}{6^{3} \sqrt{2} a}$
$+\frac{(1+\sqrt{3} i)\left(-b^{2}+3 a c\right)}{3 \sqrt[3]{4} a \cdot \sqrt[3]{-2 b^{3}+9 a b c-27 a^{2} d+\sqrt{4\left(-b^{2}+3 a c\right)^{3}+\left(-2 b^{3}+9 a b c-27 a^{2} d\right)^{2}}}-\frac{b}{3 a}, ~}$
$\left[x_{3}\right]=-\frac{(1+\sqrt{3} i) \cdot \sqrt[3]{-2 b^{3}+9 a b c-27 a^{2} d+\sqrt{4\left(-b^{2}+3 a c\right)^{3}+\left(-2 b^{3}+9 a b c-27 a^{2} d\right)^{2}}}}{6^{3} \sqrt{2} a}$
$+\frac{(1-\sqrt{3} 2)\left(-b^{2}+3 a c\right)}{3 \sqrt[3]{4} a \cdot \sqrt[3]{-2 b^{3}+9 a b c-27 a^{2} d+\sqrt{4\left(-b^{2}+3 a c\right)^{3}+\left(-2 b^{3}+9 a b c-2\left(a^{2} d\right)^{2}\right.}}-\frac{b}{3 a}}$

Sol) False. When $x=-1000,-982993900 \geq 0$
(g) $\exists x\left(x^{3}+x^{2}+x+1 \geq 0\right)$ (Real numbers)

Sol) True. when $x=1,1+1+1+1 \geq 0$
(h) $\forall x \exists y(x+y=0)$ (Real numbers)

Sol) True. For every real number $x$ there is a real number $y$ such that $x+y=0$. This states that every real number has an additive inverse.
(i) $\exists x \forall y(x+y=0)$ (Real numbers)

Sol) False. All real number $y, x+y=0$ is not exist. There is a real number $x$ such that for every real number $y, x+y=0$.
(j) $\forall x \exists!y\left(y=x^{2}\right)$ (Real numbers)

Sol) $\exists$ ! $y$ means " There exists a unique something such that ..."
True. For all real number $x$ there is unique $y$. when $y=0$
(k) $\forall x \exists!y\left(y=x^{2}\right)$ (Natural numbers)

Sol) $\exists$ ! $y$ means " There exists a unique something such that ..."
False. For all real number $x$ there is not unique $y$.
(I) $\forall x \exists y \forall z(x y=x z)$ (Real numbers)

Sol) $\exists y \forall z(y=z)$.
$\forall x \exists y \forall z(x y=x z)$.
All $z, y=z . y$ is not exist in real numbers.
(m) $\forall x \exists y \forall z(x y=x z)$ (Prime numbers)

Sol) $\exists y \forall z(y=z)$.
$\forall x \exists y \forall z(x y=x z)$.
All $z, y=z . y$ is not exist in prime numbers.
(n) $\forall x \exists y\left(x \geq 0 \Rightarrow y^{2}=x\right)$ (Real numbers)

Sol) False, For all $x$, reason $y$
$\forall x \exists y\left(\neg x \geq 0 \vee y^{2}=x\right)$.
$\forall x \exists y\left(x<0 \vee y^{2}=x\right)$.
(o) $\forall x\left[x<0 \Rightarrow \exists y\left(y^{2}=x\right)\right]$ (Real numbers)

Sol) $\forall x\left[\neg(x<0) \vee \exists y\left(y^{2}=x\right)\right]$.
$\forall x\left[(x \geq 0) \vee \exists y\left(y^{2}=x\right)\right]$.
All $\mathrm{x},(x \geq 0) \vee \exists y\left(y^{2}=x\right)$ is not exist. When $\mathrm{x}<0$ have problem.
False
(p) $\forall x\left[x<0 \Rightarrow \exists y\left(y^{2}=x\right)\right]$ (Positive real numbers)

Sol) $\forall x\left[\neg(x<0) \vee \exists y\left(y^{2}=x\right)\right]$.
$\forall x\left[(x \geq 0) \vee \exists y\left(y^{2}=x\right)\right]$.
All $\mathrm{x},(x \geq 0) \vee \exists y\left(y^{2}=x\right)$ is exist.
True
3. Negate each of the symbolic statements you wrote in Question 1, putting your answers in positive form. Express each negation in natural, idiomatic English.
(There are solutions in Exercises 2.4.5-1.)
4. Negate each of the statements in Question 2, putting your answers in positive form.

Sol)
(a) $\exists x(x+1<x)$ (Real numbers)
(b) $\forall x(2 x+3 \neq 5 x+1) \quad$ (Natural numbers)
(c) $\forall x\left(x^{2}+1 \neq 2^{x}\right)$ (Real numbers)
(d) $\forall x\left(x^{2} \neq 2\right)$ (Rational numbers)
(e) $\forall x\left(x^{2} \neq 2\right)$ (Real numbers)
(f) $\exists x\left(x^{3}+17 x^{2}+6 x+100<0\right)$ (Real numbers)
(g) $\forall x\left(x^{3}+x^{2}+x+1<0\right)$ (Real numbers)
(h) $\exists x \forall y(x+y \neq 0)$ (Real numbers)
(i) $\forall x \exists y(x+y \neq 0) \quad$ (Real numbers)
(j) $\exists x \forall!y\left(y \neq x^{2}\right)$ (Real numbers)
(k) $\exists x \forall!y\left(y \neq x^{2}\right)$ (Natural numbers)
(I) $\exists x \forall y \exists z(x y \neq x z)$ (Real numbers)
(m) $\exists x \forall y \exists z(x y \neq x z)$ (Prime numbers)
(n) $\exists x \forall y\left(x \geq 0 \wedge y^{2} \neq x\right)$ (Real numbers)
(o) $\exists x\left[x<0 \wedge \forall y\left(y^{2} \neq x\right)\right]$ (Real numbers)
(p) $\exists x\left[x<0 \wedge \forall y\left(y^{2} \neq x\right)\right]$ (Positive real numbers)
5. Negate the following statements and put each answer into positive form:
(a) $(\forall x \in \mathrm{~N})(\exists y \in \mathrm{~N})(\mathrm{x}+\mathrm{y}=1)$

Sol) $(\exists x \in \mathrm{~N})(\forall y \in \mathrm{~N})(x+y \neq 1)$.
(b) $(\forall x>0)(\exists y<0)(x+y=0)$ (where $x, y$ are real number variables)

Sol) $(\exists x>0)(\forall y<0)(x+y \neq 0)$
(c) $\exists x(\forall \varepsilon>0)(-\varepsilon<x<\varepsilon)$ (where $x, \varepsilon$ are real number variables)

Sol) $\forall x(\exists \varepsilon>0)(x \leq-\varepsilon \vee x \geq \varepsilon)$.
(d) $(\forall x \in N)(\forall y \in N)(\exists z \in N)\left(x+y=z^{2}\right)\left(x+y=z^{2}\right)$

Sol) $(\exists x \in N)(\exists y \in N)(\forall z \in N)\left(x+y \neq z^{2}\right)$.
6. Give a negation (in positive form) of the quotation which you met in Exercise 2.4.2(7): "You may fool all the people some of the time, you can even fool some of the people all of the time, but you cannot fool all of the people all the time."

Sol) Let $\mathrm{F}(\mathrm{x}, \mathrm{t})$ mean " You can fool person p at the time t."
Quotation is :
$\exists t \forall p F(p, t) \wedge \exists p \forall t F(p, t) \wedge \neg \forall p \forall t F(p, t)$.
Negation
$\forall t \exists p \neg F(p, t) \vee \forall p \exists t \neg F(p, t) \vee \forall p \forall t F(p, t)$.

Quotation is:
$\exists t \forall p F(p, t) \wedge \forall t \exists p F(p, t) \wedge \neg \forall t \forall p F(p, t)$.

## Negation

$\forall t \exists p \neg F(p, t) \vee \exists t \forall p \neg F(p, t) \vee \forall p \forall t F(p, t)$.
At any time, there is someone you can't fool or For every person, you can't always fool them. Or you can fool all the people, all the time.
7. The standard definition of a real function $f$ being continuous at a point $x=a$ is
$(\forall \varepsilon>0)(\exists \delta>0)(\forall x)[|x-a|<\delta \Rightarrow|f(x)-f(a)|<\varepsilon]$
Write down a formal definition for $f$ being discontinuous at a. Your definition should be in positive form.

Sol) $(\exists \varepsilon>0)(\forall \delta>0)(\exists x)[|x-a|<\delta \wedge-[|f(x)-f(a)|<\varepsilon]]$

$$
(\exists \varepsilon>0)(\forall \delta>0)(\exists x)[|x-a|<\delta \wedge|f(x)-f(a)| \geq \varepsilon]
$$



## Exercises 3.2.1

1. Prove that $\sqrt{3}$ is irrational.

Sol) We could prove it by using contradiction.

First method

Assume that $\sqrt{3}$ is rational.
$\sqrt{3}=\frac{p}{q}$, where $p$ and $q$ have no common factors and both are natural numbers.

$$
\begin{aligned}
\sqrt{3}=\frac{p}{q} \leftrightarrow 3=\frac{p^{2}}{q^{2}} \\
\leftrightarrow p^{2}=3 q^{2}
\end{aligned}
$$

Now, we could consider q as either odd or even.

1) q: odd
$q=2 n+1, q^{2}=(2 n+1)^{2} 4 n^{2}+4 n+1=4\left(n^{2}+n\right)+1$
$\therefore 3 q^{2}=12\left(n^{2}+n\right)+2+1$

So, $p^{2}=3 q^{2}$ is odd. Therefore $p$ is odd too. $\left(\right.$ odd $\left.^{2}=o d d\right)$

In conclusion, there can be common factors between $p$ and $q$. However, we assume that $p$ and $q$ have no common factors. (Contradiction.)

Hence, our original assumption that $\sqrt{3}$ was rational must be false. It means $\sqrt{3}$ must be irrational.
2) $q$ :even
$q=2 n, q^{2}=(2 n)^{2}=4 n^{2}$
$\therefore 3 q^{2}=12 n^{2}$
So, $p^{2}=3 q^{2}$ is even. Therefore $p$ is even too. $\left(\right.$ even $^{2}=$ even $)$

In conclusion, there can be common factors between $p$ and $q$. However, we assume that $p$ and $q$ have no common factors. (Contradiction.)

Hence, our original assumption that $\sqrt{3}$ was rational must be false. It means $\sqrt{3}$ must be irrational.

Second method

Assume that $\sqrt{3}$ is rational.
$\sqrt{3}=\frac{p}{q}$, where $p$ and $q$ have no common factors and both are natural numbers.

$$
\begin{aligned}
\sqrt{3}=\frac{p}{q} & \leftrightarrow 3=\frac{p^{2}}{q^{2}} \\
& \leftrightarrow p^{2}=3 q^{2}
\end{aligned}
$$

$n=p_{1} p_{2} \cdots p_{n}$, where $p_{i}$ are some primes and each one should be distinctive
$n^{2}=\left(p_{1} p_{2} \cdots p_{n}\right)\left(p_{1} p_{2} \cdots p_{n}\right)=p_{1}^{2} p_{2}{ }^{2} \cdots p_{n}{ }^{2}$

If p divides $n^{2}$, then p is one of $p_{i}$, so p divides n as well.

Following above, 3 divides $p^{2}$. So, it divides $p$ as well.

Let $p=3 r$ for some integers $r$
$3 q^{2}=(3 r)^{2} \leftrightarrow 3 q^{2}=9 r^{2} \leftrightarrow q^{2}=3 r^{2}$

Again, 3 divides $q^{2}$ and it divides $q$ as well.

In conclusion, there can be common factors between $p$ and $q$. However, we assume that $p$ and $q$ have no common factors. (Contradiction.)

Hence, our original assumption that $\sqrt{3}$ was rational must be false. It means $\sqrt{3}$ must be irrational.
2. Is it true that $\sqrt{N}$ is irrational for every natural number N ?

Sol) No, there is counter example, which is $\mathrm{N}=4$.
3.If not, then for what N is $\sqrt{N}$ irrational? Formulate and prove a result of the form " $\sqrt{N}$ irrational if and only if $\mathrm{N} . .$. ."

Sol) Trial: * $\begin{aligned} & n=p_{1} p_{2} \cdots p_{n} \text {, where } p_{i} \text { are some primes and each one should be distinctive } \\ & n^{2}=\left(p_{1} p_{2} \cdots p\right)\left(p_{1} p_{2} \cdots p\right)=p_{1}^{2} p_{2}^{2} \cdots p^{2}\end{aligned}$.

If p divides $n^{2}$, then p is one of $p_{i}$, so p divides n as well.

From the statement above, we could know when N consists of the product of distinctive,

$$
\sqrt{N} \ldots \text {...failure) }
$$

Prove: If $\sqrt{N}$ is a rational number, then N is perfect square.
Assume that $\sqrt{N}$ is a rational number $\mathrm{B} / \mathrm{A}$, which is the lowest terms.
$\sqrt{N}=\frac{B}{A} \leftrightarrow \sqrt{N} \sqrt{N}=\frac{B}{A} \sqrt{N} \leftrightarrow \frac{N A}{B}=\sqrt{N}$
$\therefore \frac{B}{A}=\frac{N A}{B}$

Since $B / A$ is the lowest terms, there is an integer $C$ such that $B C=N A$ and $A C=B$
Since $A C=B, C=B / A$, that is, $B / A$ is an integer, so $\sqrt{N}$ is an integer and $N$ is a perfect square.

Taking the contrapositive,
If N is not a perfect square, $\sqrt{N}$ is irrational.

## Exercises 3.3.1

Let $r_{1} s$ be irrationals. For each of the following, say whether the given number is necessarily irrational, and prove your answer. (The last one is particularly nice. I'll give the solution in a moment, but you should definitely try it first.)

1. $r+3$

Sol) Irrational

Suppose $r+3$ were rational, then $r+3=\frac{p}{q}$, where $p, q \in Z$. Then $r=\frac{p}{q}-3=\frac{p-3 q}{q} \in Q$ (rational). This is contradiction.
2. $5 r$.

Sol) Irrational

Suppose $5 r$ were rational, then $5 r=\frac{p}{q}$, where $p, q \in Z$. Then $r=\frac{p}{5 q} \in Q$ (rational). This is contradiction.
3. $r+s$

Sol) not necessarily irrational

Here is a counter example of $r+s$. Let's suppose $r=\sqrt{2}$ and $s=-\sqrt{2}$, then $r+s=\sqrt{2}-\sqrt{2}=0$ which is not irrational number.
4. $r s$

Sol)not necessarily irrational

Here is a counter example of $r$. Let's suppose, $r=\sqrt{2}$ and $s=\sqrt{2}$, then $r s=2$, which is not irrational number.
5. $\sqrt{r}$

Sol) Irrational

Suppose $\sqrt{r}$ were rational, then $\sqrt{r}=\frac{p}{q}$, where $p, q \in Z$. Then $r=\frac{p^{2}}{q^{2}} \in Q$ (rational). This is contradiction.
6. $r^{s}$

Sol) not necessarily irrational

Here is a counter example of $r^{s}$. Let's suppose $r=\sqrt{2}^{\sqrt{2}}$ and $s=\sqrt{2}$, then $r^{s}=2$ which is not irrational number.

## Exercise 3.3.2

1. Explain why proving $\phi \Rightarrow \psi$ and $\psi \Rightarrow \phi$ establishes the truth of $\phi \Leftrightarrow \psi$.

Sol) Biconditional can be defined to be an abbreviation for the conjunction

$$
(\phi \Rightarrow \psi) \wedge(\psi \Rightarrow \phi)
$$

Therefore, proving $\phi \Rightarrow \psi$ and $\psi \Rightarrow \phi$ establishes the truth of $\phi \Leftrightarrow \psi$.
2. Explain why proving $\phi \Rightarrow \psi$ and $(\neg \phi) \Rightarrow(\neg \psi)$ establishes the truth of $\phi \Leftrightarrow \psi$.

Sol) Using the equivalence of $\psi \Rightarrow \phi$ with the contrapositive $(\neg \phi) \Rightarrow(\neg \psi)$, proving $\phi \Rightarrow \psi$ and $(\neg \phi) \Rightarrow(\neg \psi)$ becomes $\phi \Rightarrow \psi$ and $\psi \Rightarrow \phi$. According to Exercise 1, proving $\phi \Rightarrow \psi$ and $\psi \Rightarrow \phi$ establishes the truth of $\phi \Leftrightarrow \psi$.
3. Prove that if five investors split a payout of $\$ 2$ million, at least one investor receives at least $\$ 400,000$.

Sol) If $\$ 2,000,000$ is fairly split by 5 , then each has $\$ 400,000$. If one of investors receives less than $\$ 400,000$, then one of the other investors receives more than $\$ 400,000$. Therefore, at least one investor receives at least \$400,000.

As a mathematical form, by using the contrapositive, I'm going to prove
"If all investor receive less than $\$ 400,000$, then five investors can't split a payout of $\$ 2$ million."

Let's suppose the amount of receiving money of five investors are $a, b, c, d, e$. Then,

$$
\begin{aligned}
& a<400,000 \\
& b<400,000 \\
& c<400,000 . \\
& d<400,000 \\
& e<400,000
\end{aligned}
$$

If I sum all the split money, then

$$
a+b+c+d+e<\$ 2,000,000
$$

So, the five investors can't split a payout of $\$ 2$ million.

Thus, the contrapositive holds.
4. Write down the converses of the following conditional statements:
(a) If the Dollar falls, the Yuan will rise.

Sol) If the Yuan rises, the Dollar falls.
(b) If $x<y$ then $-y<-x$. (For $x, y$ real numbers.) - True

Sol) If $-y<-x$, then $x<y$ - True
(c) If two triangles are congruent they have the same area. - True

Sol) If two triangles have the same area, then they are congruent. - False
(d) The quadratic equation $a x^{2}+b x+c=0$ has a solution whenever $b^{2} \geq 4 a$. (Where $a, b, c, x$ denote real numbers and $a \neq 0$.)

Sol) $b^{2} \geq 4 a$ whenever the quadratic equation $a x^{2}+b x+c=0$ has a solution. $(a$ implies $b)=(b$ whenever $a)$
(e) Let $A B C D$ be a quadrilateral. If the opposite sides of $A B C D$ are pairwise equal, then the opposite angles are pairwise equal.

Sol) Let $A B C D$ be a quadrilateral. If the opposite angles are pairwise equal, then the opposite sides of $A B C D$ are pairwise equal.
(f) Let $A B C D$ be a quadrilateral. If all four sides of $A B C D$ are equal, then all four angles are equal.

Sol) Let $A B C D$ be a quadrilateral. If all four angles are equal, then all four sides of $A B C D$ are equal.
(g) If $n$ is not divisible by 3 then $n^{2}+5$ is divisible by 3 . (For $n$ a natural number.)

Sol) For n a natural number, if $n^{2}+5$ is divisible by 3 , then n is not divisible by 3 .
5. Discounting the first example, which of the statements in the previous exercise are true, for which is the converse true, and which are equivalent? Prove your answers.
(b) If $x<y$ then $-y<-x$. (For $x, y$ real numbers.) - True ( $x=1, y=2$ )
(Proof) Using the direct proof, this is very obvious.

Let's suppose $x=a, y=a+\alpha$ where $\alpha>0$, then $x<y$ holds.
$-y=-a-\alpha,-x=-a$. Thus, $-y<-x$ holds.

Converse: If $-y<-x$, then $x<y$ - True $(x=1, y=2)$
(Proof) Similar to the original problem, I'm going to use the direct proof.

Let's suppose $x=a, y=a+\alpha$ where $\alpha>0$, then $-y<-x$ and $x<y$ hold.
(c) If two triangles are congruent (합동) they have the same area. - True

Converse: If two triangles have the same area, then they are congruent. - False
(Proof) Here is counter example. Let triangle $A B C$ have sides as $2 \mathrm{~cm}, 6 \mathrm{~cm}, 2 \sqrt{5} \mathrm{~cm}$ and triangle DEF have sides as $3 \mathrm{~cm}, 4 \mathrm{~cm}, 5 \mathrm{~cm}$. Triangle $A B C$ and DEF have same area but they are not congruent.
(d) The quadratic equation $a x^{2}+b x+c=0$ has a solution whenever $b^{2} \geq 4 a$. (Where $a, b, c, x$ denote real numbers and $a \neq 0$.) - False (a implies b) = (b whenever $a$ )
(Proof) The sufficient condition for the quadratic equation having a solution is $b^{2} \geq 4 a c$. $\left(x=\frac{-b \pm \sqrt{b^{2}-4 a c}}{2 a}\right)$

Converse: $b^{2} \geq 4 a$ whenever the quadratic equation $a x^{2}+b x+c=0$ has a solution. - False
(Proof) Here is a counter example. Let's suppose $a=2, b=2, c=\frac{1}{2}$. Then, $b^{2} \geq 4 a$ holds but the quadratic equation $a x^{2}+b x+c=0$ doesn't have a solution since $b^{2} \geq 4 a c$ doesn't hold.
(e) Let $A B C D$ be a quadrilateral. If the opposite sides of $A B C D$ are pairwise equal, then the opposite angles are pairwise equal. - False

Converse: Let $A B C D$ be a quadrilateral. If the opposite angles are pairwise equal, then the opposite sides of $A B C D$ are pairwise equal. - False
(f) Let $A B C D$ be a quadrilateral (사변형). If all four sides of $A B C D$ are equal, then all four angles are equal. - False
(Proof) When $A B C D$ be a rhombus (마름모), then all four sides of $A B C D$ are equal, but all four angles are not equal.

Converse: Let $A B C D$ be a quadrilateral. If all four angles are equal, then all four sides of $A B C D$ are equal. - False
(Proof) When ABCD be a rectangle (직사각형), then all four angles are equal, but all four sides of $A B C D$ are not equal.
(g) If $n$ is not divisible by 3 then $n^{2}+5$ is divisible by 3 . (For $n$ a natural number.) - True

$$
\begin{aligned}
& \text { (Proof) } \mathrm{n}=3 \mathrm{a}+1, n^{2}+5=(3 a+1)^{2}+5=9 a^{2}+6 a+6=3\left(3 a^{2}+2 a+2\right) \\
& \mathrm{n}=3 a+2, \quad n^{2}+5=(3 a+2)^{2}+5=9 a^{2}+12 a+9=3\left(3 a^{2}+4 a+3\right)
\end{aligned}
$$

Converse: For n a natural number, if $n^{2}+5$ is divisible by 3 , then n is not divisible by 3. - True (Proof) $n^{2}+5=3 a(n \geq 1, a \geq 2)$ then $n=\sqrt{3 a-5}$ is not divisible by 3 .
6. Let $m$ and $n$ be integers. Prove that:

Key facts: $n$ is even iff $n=2 k$ for some $k$. $n$ is odd iff $n=2 k+1$ for some $k$.
(a) If $m$ and $n$ are even, then $m+n$ is even.

Sol) $m=2 a, n=2 b$, then $a+b=2 a+2 b=2(a+b)$
(b) If $m$ and $n$ are even, then $m n$ is divisible by 4 .

Sol) $m=2 a, n=2 b$, then $m n=4 a b$
(c) If $m$ and $n$ are odd, then $m+n$ is even.

Sol) $m=2 a+1, n=2 b+1, m+n=2(a+b+1)$
(d) If one of $m, n$ is even and the other is odd, then $m+n$ is odd.

Sol) $m=2 a, n=2 b+1, m+n=2 a+(2 b+1)=2(a+b)+1$.
(e) If one of $m, n$ is even and the other is odd, then $m n$ is even.

Sol) $m=2 a, n=2 b+1, m n=2(2 a b+a)$
7. Prove or disprove the statement "An integer $n$ is divisible by 12 if and only if $n^{3}$ is divisible by 12."

1) An integer $n$ is divisible by 12 if $n^{3}$ is divisible by 12

Sol) This statement is false. Here is the counter-example. When $n=6, n^{3}=6 \times 6 \times 6=216$ is divisible by 12 . But, $\mathrm{n}=6$ is not divisible by 12 .
2) $n^{3}$ is divisible by 12 if an integer $n$ is divisible by 12

Sol) This statement is true. Let $\mathrm{n}=12 \mathrm{k}$ where k is integer. Then $n^{3}=12^{3} \mathrm{k}^{3}$ which is divisible by 12.
8. If you have not yet solved Exercise 3. 3. 1 (6), have another attempt, using the hint to try $s=\sqrt{2}$.

Sol) We have already solved the problem.

## Exercises 3.4.1

1. Prove or disprove the statement "All birds can fly."

Sol) False. Counter Ex) ostrich 타조, chicken
2. Prove or disprove the claim $(\forall x, y \in R)\left[(x-y)^{2}>0\right]$.

Sol) False. counter ex) $x=y=1(x-y)^{2}>0$.
3. Prove that between any two unequal rationals there is a third rational.

Sol) Let $x, y \in Q($ rational $), x<y$. Then $x=\frac{p}{q}, y=\frac{r}{s}$, where $p, q, r, s \in Z$ (integer) Then $\frac{x+y}{2}=\frac{p / q+r / s}{2}=\frac{\frac{p s+q r}{q s}}{2}=\frac{p s+q r}{2 q s} \in Q($ rational $) \quad$ But, $x<\frac{x+y}{2}<y$.
4. Say whether each of the following is true or false, and support your decision by a proof:
(a) There exist real numbers $x$ and $y$ such that $x+y=y$.

Sol) True.
When $x=0, x+y=y$ is correct.
(b) $\forall x \exists y(x+y=0)$ (where $x$, $y$ are real number variables).

Sol) Ture
For $x, x=0, y=0$.
(c) $(\exists m \in N)(\exists n \in N)(3 m+5 n=12)$.

Sol) False
$m=1,5 n=9$
$m=2,5 n=6$
$m=3,5 n=3$
$n=1,3 m=7$
$n=2,3 m=2$
(d) For all integers $a, b, c$, if a divides $b c$ (without remainder), then either $a$ divides $b$ or $a$ divides c.

Sol) False.
$\mathrm{a} \mid \mathrm{bc}$, then $\mathrm{a} \mid \mathrm{b}$ or $\mathrm{a} \mid \mathrm{c}$.
$\mathrm{a} \left\lvert\, \mathrm{bc} \Leftrightarrow \mathrm{am}=\mathrm{bc} \Leftrightarrow \mathrm{a}\left(\frac{\mathrm{m}}{\mathrm{b}}\right)=\mathrm{c} \quad\right.$ (incorrect) since can be 0. .

Count example) However, $b=6, c=10$, then $a=4$ divides $b c=60$
But a doesn't divide either b or c .
(e) The sum of any five consecutive integers is divisible by 5 (without remainder).

Sol) True.
$x+(x+1)+(x+2)+(x+3)+(x+4)$.
$=5 x+10$.
$=5(x+2)$.
(f) For any integer $n$, the number $n^{2}+n+1$ is odd.

Sol) True.
Assuming that For any integer $n$, the number $n^{2}+n+1$ is odd.

Let $\mathrm{n}=1-3$ (odd)
n=2-7(odd)
$n=3-13($ odd $)$
when $\mathrm{n}=\mathrm{k}, \quad \mathrm{k}^{2}+\mathrm{k}+1$.(odd)
when $\mathrm{n}=\mathrm{k}+1(k+1)^{2}+(k+1)+1=k^{2}+3 k+3=k^{2}+k+1+2(k+1) .(o d d)$
(g) Between any two distinct rational numbers there is a third rational number.

Sol) True.
Rational number $\mathrm{a}, \mathrm{b}$
$a<(a+b) / 2<b$
third rational number $(a+b) / 2$
(h) For any real numbers $\mathrm{x}, \mathrm{y}$, if x is rational and y is irrational, then $\mathrm{x}+\mathrm{y}$ is irrational.

Sol) True.
Suppose not. [We take the negation of the theorem and suppose it to be true.]
Suppose $\exists$ a rational number $x$ and an irrational number $y$ such that $(x+y)$ is rational. [We must derive a contradiction.]

By definition of rational, we have $x=a / b$ for some integers $a$ and $b$ with $b \neq 0$. and $x+y$ $=c / d$ for some integers $c$ and $d$ with $d \neq 0$.

By substitution, we have $x+y=c / d, a / b+y=c / d, y=-a / b+c / d, y=(-a d+b c) / b d$
But ( $-a d+b c$ ) are integers [because $a, b, c, d$ are all integers and products and differences of integers are integers], and bd $\neq 0$ [by zero product property].

Therefore, by definition of rational, y is rational. This contradicts the supposition that y is rational. [Hence, the supposition is false and the theorem is true.] And this completes the proof.
(i) For any real numbers $x, y$, if $x+y$ is irrational, then at least one of $x, y$ is irrational. Sol) True.

We prove the contrapositive, i.e. we prove that if $x$ and $y$ both are rational then $x+y$ is also rational.

Let x and y be both rational. Then we can write:
$x=\frac{a}{b}$ where $b \neq 0$.
$y=\frac{c}{d}$ where $\mathrm{d} \neq 0$.
$\Rightarrow x+y=\frac{a}{b}+\frac{c}{d}=\frac{a d+b c}{b d}$ where $\operatorname{bd} \neq 0$.
So, $x+y$ is rational.
(j) For any real numbers $x, y$, if $x+y$ is rational, then at least on of $x, y$ is rational.

Sol) False.
We prove the contrapositive, i.e. we prove that if $x$ and $y$ both are irrational then $x+y$ is also irrational.

Let x and y be both irrational. Then we can write:
Count example)
$x=\sqrt{2}, y=-\sqrt{2}$.
$x+y=0$ (rational number) .
5. Prove or disprove the claim that there are integers $m, n$ such that $m^{2}+m n+n^{2}$ is a perfect square.

Sol) True.
Take $\mathrm{m}=\mathrm{n}=0$. Then $\mathrm{m}^{2}+m n+n^{2}=0=0^{2}$.
(When $m=0$ or $n=0$,this equation is true.)
6. Prove that for any positive $m$ there is a positive integer $n$ such that $m n+1$ is a perfect square.

Sol) How can we have $m n+1=p^{2}$ ? $m n=p^{2}-1=(p+1)(p-1)$. How $m=(p-1), n=(p+1)$. So, $p=m+1$, then $n=m+2$.

Given m , take $\mathrm{n}=\mathrm{m}+2$. Then, $\mathrm{mn}+1=\mathrm{m}(\mathrm{m}+2)+1=\mathrm{m}^{2}+2 m+1=(m+1)^{2}$.
7. Show that there is a quadratic (이차의) $f(n)=n^{2}+b n+c$, with positive integer coefficients $b$, $c$, such that $f(n)$ is composite (i.., not prime) for all positive integers $n$.

Sol)
Let $f(n)=(n+1)(n+2)=n^{2}+3 n+2$.
8. Prove that for any finite collection of points in the plane, not all collinear, there is a triangle having three of the points as its vertices, which contains none of the other points in its interior.

Sol) For any finite collection of points in the plane, there is a triangle having three of the points as its vertices as below figure.


Sol 2)

Kelly's Proof


The proof below is instead due to Kelly.
Suppose for contradiction that we have a finite set of points not all collinear but with at least three points on each line. Call it S .

Define a connecting line to be a line which contains at least two points in the collection. Let ( $\mathrm{P}, \mathrm{I}$ ) be the point and connecting line that are the smallest positive distance apart among all point-line pairs.

By the supposition, the connecting line I goes through at least three points of S, so dropping a perpendicular from $P$ to $I$ there must be at least two points on one side of the perpendicular (one might be exactly on the intersection of the perpendicular with I).

Call the point closer to the perpendicular $B$, and the farther point $C$. Draw the line $m$ connecting $P$ to $C$. Then the distance from $B$ to $m$ is smaller than the distance from P to I , contradicting the original definition of P and I . One way to see this is to notice that the right triangle with hypotenuse $B C$ is similar to and contained in the right triangle with hypotenuse PC.

Thus there cannot be a smallest positive distance between point-line pairs-every point must be distance 0 from every line. In other words, every point must lie on the same line if each connecting line has at least three points.
9. Prove that if every even natural number greater than 2 is a sum of two primes (the Goldbach Conjecture), then every odd natural number greater than 5 is a sum of three primes.

Sol)
If $\mathrm{n}>5$ is odd, then $\mathrm{n}=2 \mathrm{k}+3$, where $\mathrm{k}>1$.
( 2 k is even number) Since $2 k>2$, by goldbach conjecture, $2 k=p+q$, ( $p, q$ are primes.)
Then, $n=p+q+3 \quad$-sum of three primes-

## Exercises 3.5.1

1. Write down the statement $A(n)$ which is being proved by induction.

Sol) $\mathrm{A}(\mathrm{n})$ : The sum of the first n positive integers is $\frac{1}{2} n(n+1)$ i.e., $1+2+\cdots+n=\frac{1}{2}(n)(n+1)$
2.Write down $A(1)$, the initial step.

Sol) $A(1): 1=\frac{1}{2}(1)(1+1)$
3. Write down the statement $(\forall n \in N)[A(n) \Rightarrow A(n+1)]$, the induction step.

Sol) For every integer $n$, the sum of first $n$ positive integers implies the sum of first $n+1$ positive numbers, i.e., $1+2+\cdots+n=\frac{1}{2}(n)(n+1) \Rightarrow 1+2+\cdots+n+(n+1)=\frac{1}{2}(n+1)[(n+1)+1]$.

## Exercises 3.5.2

1. Use the method of induction to prove that the sum of the first $n$ odd numbers is equal to $n^{2}$.

Sol) We use the method of induction to prove the statement $A(n)$ : $1+3+5+\cdots+(2 n-1)=n^{2}$

- Initial step: set $\mathrm{n}=1$. We get $1=1^{2}=1$, which is true.
- Induction step: We assume that $A(k)$ is true for an arbitrary $k$, that is, $1+3+5+\cdots+(2 k-1)=k^{2}$ is true. We need to prove $1+3+5+\cdots+(2 k-1)+(2 k+1)=(k+1)^{2}$. Now, adding $(2 k+1)$ to both sides of $A(k)$ we get $A(k+1)$, that is,

$$
\begin{aligned}
1+3+5+\cdots+(2 k-1)+(2 k+1) & =A(k)+(2 k+1) \\
& =k^{2}+(2 k+1) \\
& =(k+1)^{2}
\end{aligned}
$$

Which is a formula for $k+1$ in the place of $k$. Hence, by the principle of mathematical induction, we can conclude that the identity does indeed hold for all k .
2. Prove the following by induction:
(a) $4^{n}-1$ is divisible by 3.
(b) $(n+1)!>2^{n+3}$ for all $n \geq 5$.

Sol) (a) Let $A(n)$ is the statement that $4^{n}-1$ is divisible by 3

- Initial step: Set $\mathrm{n}=1$. We get $4^{1}-1=3$, which is true.
- Induction step: We assume that $A(k)$ is true for an arbitrary $k$, That is, $4^{k}-1$ is divisible by 3 is true. We need to prove $4^{k+1}-1$ is also divisible by 3 . Now,

$$
\begin{aligned}
4^{k+1}-1 & =4^{k} 4-1 \\
& =4^{k}(3+1)-1 \\
& =3^{*} 4^{k}+\left(4^{k}-1\right)(\text { multiple of } 3+A(k))
\end{aligned}
$$

Hence, by the principle of mathematical induction, we can conclude that the identity does indeed hold for all k .
(b) Let $\mathrm{A}(\mathrm{n})$ is the statement $(n+1)$ ! $>2^{n+3}$ for all $n \geq 5$.

- Initial step: Set $n=5$. We get(6)! $>2^{9}$, that is, $720>512$, is true
- Induction step: We assume that $A(k)$ is true for an arbitrary $k \geq 5$, that is, $(k+1)!>2^{k+3}$ is true. We need to prove $(k+2)!>2^{k+4}$ for all $k \geq 5$. Let us start with $(k+2)!$, that is,

$$
\begin{aligned}
(k+2)! & =(k+2)(k+1)! \\
& =k(k+1)!+2(k+1)!\quad k \geq 5 \\
& >2(k+1)! \\
& >2 * 2^{k+3}=2^{k+4}
\end{aligned}
$$

Hence, by the principle of mathematical induction, we can conclude that the identity does indeed hold for all k .
3. The notation

$$
\sum_{i=1}^{n} a_{i}
$$

is common abbreviation for the sum

$$
a_{1}+a_{2}+a_{3}+\cdots+a_{n}
$$

For instance,

$$
\sum_{r=1}^{n} r^{2}
$$

Denotes the sum

$$
1^{2}+2^{2}+3^{2}+\cdots+n^{2}
$$

Prove the following by induction:
(a) $\forall n \in N: \sum_{r=1}^{n} r^{2}=\frac{1}{6} n(n+1)(2 n+1)$
(b) $\forall n \in N: \sum_{r=1}^{n} 2^{r}=2^{n+1}-2$
(c) $\forall n \in N: \sum_{r=1}^{n} r \cdot r!=(n+1)!-1$

Sol) (a) Let $\mathrm{A}(\mathrm{n})$ is the statement that $\forall n \in N: \sum_{r=1}^{n} r^{2}=\frac{1}{6} n(n+1)(2 n+1)$

- Initial step: Set $\mathrm{n}=1$. We get $1^{2}=\frac{1}{6}(1)(1+1)(2+1)=1$, which is true.
- Induction step: We assume that $A(k)$ is true for an arbitrary $k$, that is, $\sum_{r=1}^{k} r^{2}=\frac{1}{6} k(k+1)(2 k+1) \quad$ is true. We need to prove $\sum_{r=1}^{k+1} r^{2}=\frac{1}{6}(k+1)(k+2)(2(k+1)+1)$. Let us start with the known fact that

$$
\sum_{r=1}^{k} r^{2}=\frac{1}{6} k(k+1)(2 k+1)
$$

Adding the term $(k+1)^{2}$ on both sides we get

$$
\begin{aligned}
\sum_{r=1}^{k} r^{2} & +(k+1)^{2}=\frac{1}{6} k(k+1)(2 k+1)+(k+1)^{2} \\
\sum_{r=1}^{k+1} r^{2} & =\frac{1}{6} k(k+1)(2 k+1)+\frac{6}{6}(k+1)^{2} \\
& =\frac{1}{6}(k+1)[k(2 k+1)+6(k+1)] \\
& =\frac{1}{6}(k+1)\left[2 k^{2}+7 k+6\right] \\
& =\frac{1}{6}(k+1)(k+2)(2 k+3) \\
& =\frac{1}{6}(k+1)(k+2)(2(k+1)+1)
\end{aligned}
$$

Hence, by the principle of mathematical induction, we can conclude that the identity does indeed hold for all k .
(b) Let $\mathrm{A}(\mathrm{n})$ is the statement that $\forall n \in N: \sum_{r=1}^{n} 2^{r}=2^{n+1}-2$

- Initial step: Set $\mathrm{n}=1$. We get $2^{1}=2^{1+1}-2=2$, which is true.
- Induction step: We assume that $A(k)$ is true for an arbitrary $k$, that is, $\sum_{r=1}^{k} 2^{r}=2^{k+1}-2$ is true. We need to prove $\sum_{r=1}^{k+1} 2^{r}=2^{k+2}-2$. Let us start with the known fact that

$$
\sum_{r=1}^{k} 2^{r}=2^{k+1}-2
$$

Adding the term $2^{k+1}$ on both sides we get

$$
\begin{aligned}
\sum_{r=1}^{k} 2^{r} & +2^{k+1}=2^{k+1}-2+2^{k+1} \\
\sum_{r=1}^{k+1} 2^{r} & =2^{k+1}+2^{k+1}-2 \\
& =\frac{2}{2} 2^{k+1}+\frac{2}{2} 2^{k+1}-2 \\
& =\frac{1}{2} 2^{k+2}+\frac{1}{2} 2^{k+2}-2 \\
& =2^{k+2}-2
\end{aligned}
$$

Hence, by the principle of mathematical induction, we can conclude that the identity does indeed hold for all k .
(c) Let $\mathrm{A}(\mathrm{n})$ is the statement that $\forall n \in N: \sum_{r=1}^{n} r \cdot r!=(n+1)!-1$

- Initial step: Set $\mathrm{n}=1$. We get $1 * 1!=2!-1=1$, which is true.
- Induction step: We assume that $A(k)$ is true for an arbitrary $k$, that is, $\sum_{r=1}^{k} r . r!=(k+1)!-1$ is true. We need to prove $\sum_{r=1}^{k+1} r . r!=(k+2)!-1$. Let us start with the known fact that

$$
\sum_{r=1}^{k} r . r!=(k+1)!-1
$$

Adding the term $(k+1)(k+1)$ ! On both sides we get

$$
\begin{aligned}
& \sum_{r=1}^{k} r \cdot r!+(k+1)(k+1)!=(k+1)!-1+(k+1)(k+1)! \\
& \sum_{r=1}^{k+1} r \cdot r!=(k+1)!+(k+1)(k+1)!-1 \\
& =(k+1)!(1+(k+1))-1 \\
& =(k+2)!-1
\end{aligned}
$$

Hence, by the principle of mathematical induction, we can conclude that the identity does indeed hold for all k .
4. In this section, we used induction to prove the general theorem

$$
1+2+\cdots+n=\frac{1}{2}(n)(n+1)
$$

There is an alternative proof that does not use induction, famous because Gauss used the key idea to solve a "busywork" arithmetic problem his teacher gave to the class when he was a small child at school. The teacher asked the class to calculate the sum of the first hundred natural numbers. Gauss noted that if

$$
1+2+\cdots+100=N
$$

then you can reverse the order of the addition and the answer will be the same:

$$
100+99+\cdots+1=N
$$

So by adding those two equations, you get

$$
101+101+\cdots+101=2 N
$$

and since there are 100 terms in the sum, this can be written as

$$
100 \cdot 101=2 N
$$

and hence

$$
N=\frac{1}{2}(100 \cdot 101)=5050 .
$$

Generalize Gauss's idea to prove the theorem without recourse to the method of induction.

## Exercises 4.1.1

1. The Hilbert Hotel scenario is as before, but this time, two guests arrive at the already full hotel. How can they be accommodated (in separate rooms) without anyone having to be ejected?

Sol) If the clerk ask to move every occupant of room $n$ into the room $n+2$, then room 1 and room 2 will be unoccupied without any ejected people because there are infinitely many rooms. Therefore, two guests can stay this hotel.
2. This time, the desk clerk faces an even worse headache. The hotel is full, but an infinite tour group arrives, each group member wearing a badge that says "HELLO, I'M N", for $N=1,2,3, \ldots$ Can the clerk find a way to give all the new guests a room to themselves, without having to eject any of the existing guests? How?

Sol) If the clerk ask to move every occupant of room $n$ into the room $2 n$, then odd number of room will be unoccupied without any ejected people because there are infinitely many rooms. Therefore, infinite tour group can stay this hotel.

## Exercises 4.1.2

1. Express as concisely and accurately as you can the relationship between $b \mid a$ and $a / b$.

Sol) We can express $b \mid a$ using quantifiers as $\exists c \in \mathbb{Z}\left(c=\frac{b}{a}\right)$
$a / b$ is same as $\frac{a}{b}$, it means reminder of this operation cannot be equal to zero.
2. Determine whether each of the following is true or false. Prove your answers.
(a) $0 \mid 7$

Sol) False, divisor has to be non-zero integer .
(b) $9 \mid 0$

Sol) True, zero can divide by any number, $\frac{0}{9}=0 \in \mathbb{Z}$.
(c) $0 \mid 0$

Sol) False, divisor has to be non-zero integer.
(d) $1 \mid 1$

Sol) True, $\frac{1}{1}=1 \in \mathbb{Z}$.
(e) $7 \mid 44$

Sol) False, $\frac{42}{7} \notin \mathbb{Z}$.
(f) $7 \mid(-42)$

Sol) True, $\frac{-42}{7}=-6 \in \mathbb{Z}$.
(g) $(-7) \mid 49$

Sol) True, $\frac{49}{-7}=-7 \in \mathbb{Z}$.
(h) $(-7) \mid(-56)$

Sol) True, $\frac{-56}{-7}=8 \in \mathbb{Z}$.
(i) $2708 \mid 569401$

Sol) False, $\frac{569401}{2708} \simeq 210.26 \notin \mathbb{Z}$.
(j) $(\forall n \in \mathbb{N})\left[2 \mathrm{n} \mid \mathrm{n}^{2}\right]$

Sol) False, $\frac{n^{2}}{2 n}=\frac{n}{2}$, if n is odd number, then quotient is not integer.
(k) $(\forall n \in \mathbb{Z})\left[2 \mathrm{n} \mid \mathrm{n}^{2}\right]$

Sol) False, $\frac{n^{2}}{2 n}=\frac{n}{2}$, if n is odd number, then quotient is not integer
(I) $(\forall n \in \mathbb{Z})[1 \mid n]$

Sol) True, $\frac{n}{1}=n \in \mathbb{Z}$
(m) $(\forall n \in \mathbb{N})[\mathrm{n} \mid 0]$

Sol) True, zero can divide by any number.
(n) $\quad(\forall n \in \mathbb{Z})[n \mid 0]$

Sol) True, zero can divide by any number.
(o) $(\forall n \in \mathbb{N})[n \mid n]$

Sol) True, $\frac{n}{n}=1 \in \mathbb{Z}$.
(p) $(\forall n \in \mathbb{Z})[\mathrm{n} \mid \mathrm{n}]$

Sol) False, if $\mathrm{n}=0$, then $\frac{0}{0}$ cannot be defined.

## Exercises 4.1.3

1. Prove all the parts of Theorem 4.1.3.
(i) $a|0, a| a$;

Sol) $\frac{0}{a}=0, \frac{a}{a}=1$
(ii) $a \mid 1$ if and only if $a= \pm 1$;

Sol) 1 can be divisible by 1 or -1 .
(iii) if $a \mid b$ and $c \mid d$, then $a c \mid b d($ for $c \neq 0)$;

$$
a \mid b \Leftrightarrow b=a n
$$

Sol) $c \mid d \Leftrightarrow d=c m$

$$
a c \left\lvert\, b d \Rightarrow \frac{b d}{a c}=\frac{a n(c m)}{a c}=\frac{a c(n m)}{a c}=n m \in \mathbb{Z}\right.
$$

Therefore, bd can be divisible by ac.
(iv) if $a \mid b$ and $b \mid c$, then $a \mid c($ for $b \neq 0)$;

$$
a \mid b \Leftrightarrow b=a n
$$

Sol) $\quad b \mid c \Leftrightarrow c=b m$

$$
a \left\lvert\, c \Rightarrow \frac{c}{a}=\frac{b m}{a}=\frac{a n m}{n}=n m \in \mathbb{Z}\right.
$$

Therefore, c can be divisible by a.
(v) $[a \mid b$ and $b \mid a]$ if and only if $a= \pm b$;

Sol)

$$
\begin{aligned}
a \mid b \Leftrightarrow b & =a n \\
b \mid a \Leftrightarrow a & =b m \\
a|b \vee b| a & \Rightarrow b=a n=b m(n) \\
& \Rightarrow m n=1 \\
& \Rightarrow m, n= \pm 1
\end{aligned}
$$

Therefore, $a= \pm b$
(vi) if $a \mid b$ and $b \neq 0$, then $|a| \leq|b|$;

Sol) $a \mid b \wedge b \neq 0 \Leftrightarrow b=a n$

If $n \neq 0,|a| \leq|b|$ is always satisfied.
(vii) if $a \mid b$ and $b \mid c$, then $a \mid(b x+c y)$ for any integers $x, y$.

$$
a \mid b \Leftrightarrow b=a n
$$

Sol) $\quad b \mid c \Leftrightarrow c=b m$

$$
a \left\lvert\,(b x+c y) \Rightarrow \frac{b x+c y}{a}=\frac{a n x+b m y}{a}=\frac{a n x+a n m y}{a}=n x+n m y \in \mathbb{Z}\right.
$$

Therefore, $b x+c y$ can be divisible by $a$.
2. Prove that every odd number is of one of the forms $4 n+1$ or $4 n+3$.
$4 n+1=2(2 n)+1=2($ even number $)+1$
Sol) $4 n+3=2(2 n)+3=2(2 n+1)+1=2$ (odd number) +1
$\Rightarrow 2$ (any natural number) +1

Two times of any natural number plus one is always odd number, and every odd number can describe this form. Therefore, $4 n+1,4 n+3$ are always odd number, and every odd number included one of them.
3. Prove that for any integer $n$, at least one of the integers $n, n+2, n+4$ is divisible by 3.

Sol) Let's divide three cases.
(case 1) $n=3 k$
$n, n+2, n+4 \Rightarrow 3 k, 3 k+2,3 k+4$
In this case, $3 k$ is divisible by 3
(case 2) $n=3 k+1$
$n, n+2, n+4 \Rightarrow 3 k+1,3 k+3,3 k+5$
$\Rightarrow 3 k+1,3(k+1), 3(k+1)+2$
In this case, $3(k+1)$ is divisible by 3
(case 3) $n=3 k+2$
$n, n+2, n+4 \Rightarrow 3 k+2,3 k+4,3 k+6$
$\Rightarrow 3 k+2,3(k+1)+1,3(k+2)$
In this case, $3(k+2)$ is divisible by 3

The proof is now complete.
4. Prove that if $a$ is an odd integer, then $24 \mid a\left(a^{2}-1\right)$.
$a\left(a^{2}-1\right)=a(a+1)(a-1)$
$a=2 k+1$ (odd interger) $\Rightarrow a(a+1)(a-1)=2 k(2 k+1)(2 k+2)$
Sol)
(mathmatical induction)
if $\mathrm{k}=1$, then $2 \times 3 \times 4=24$
$24 \mid 24 \Rightarrow$ True
$k=n \Rightarrow 2 n(2 n+1)(2 n+2)=4 n\left(2 n^{2}+3 n+1\right)$
Assume $4 n\left(2 n^{2}+3 n+1\right)$ can be divisible by 24
$k=n+1 \Rightarrow 2(n+1)\{2(n+1)+1\}\{2(n+1)+2\}$

$$
\begin{aligned}
& =(2 n+2)(2 n+3)(2 n+4) \\
& =4 n\left(2 n^{2}+9 n+13\right)+24 \\
& =4 n\left(2 n^{2}+3 n+1\right)+4 n(6 n+12)+24 \\
& =4 n\left(2 n^{2}+3 n+1\right)+24\left(n^{2}+2 n+1\right)
\end{aligned}
$$

by assumption, $4 n\left(2 n^{2}+3 n+1\right)$ can be divisible by 24
Also, $24\left(n^{2}+2 n+1\right)$ can be divisible by 24 .
Therefore, induction will be satisfied and proof complete.
5. Prove the following version of the Division Theorem. Given integers $a, b$ with $b \neq 0$, there are unique integers $q$ and $r$ such that

$$
a=q b+r \text { and }-\frac{1}{2}|b|<r \leq \frac{1}{2}|b|
$$

[Hint: Write $a=q^{\prime} b+r^{\prime}$ where $0 \leq r^{\prime}<|b|$. If $0 \leq r^{\prime} \leq \frac{1}{2}|b|$, let $r=r^{\prime}, q=q^{\prime}$. If $\frac{1}{2}|b|<r^{\prime}<|b|$, let $r=r^{\prime}-|b|$, and set $q=q^{\prime}+1$ if $b>0$ and $q=q^{\prime}-1$ if $b<0$.]

Sol) (Prove) Let $a=q^{\prime} b+r^{\prime}$ where $0 \leq r^{\prime}<|b|$. This is obvious.
If $0 \leq r^{\prime} \leq \frac{1}{2}|b|$, let $r=r^{\prime}$ and $q=q^{\prime}$. Then, $a=q^{\prime} b+r^{\prime}$ becomes $a=q b+r$ where $0 \leq r^{\prime} \leq \frac{1}{2}|b|$.

If $\frac{1}{2}|b|<r^{\prime}<|b|$, let $r=r^{\prime}-|b|$, and $\begin{aligned} & q=q^{\prime}+1 \text {, if } b>0 \\ & q=q^{\prime}-1 \text {, if } b<0\end{aligned}$. Then, $a=q^{\prime} b+r^{\prime}$ becomes $a=q b+r$ where $\frac{1}{2}|b|<r^{\prime}<|b|$.

Therefore, given integers $a, b$ with $b \neq 0$, there are unique integers $q$ and $r$ such that $a=q b+r$ and $-\frac{1}{2}|b|<r \leq \frac{1}{2}|b|$.

## Exercises 4.1.4

1. Does the following statement accurately define prime numbers? Explain your answer. If the statement does not define the primes, modify it so it does.

$$
p \text { is prime iff }(\forall n \in \mathbb{N})[(n \mid p) \Rightarrow(n=1 \vee n=p)]
$$

Sol) For defining the primes, some parts have to be changed as follows:

$$
p \text { is prime iff }(\forall n \in \mathbb{N})[(n \mid p) \Rightarrow(p=1 \vee p=n)]
$$

2. A classic unsolved problem in number theory asks if there are infinitely many pairs of 'twin primes', pairs of primes separated by 2 , such as 3 and 5,11 and 13 , or 71 and 73 . Prove that the only prime triple (i.e. three primes, each 2 from the next) is 3, 5, 7.

Sol) Except 2, all primes are odd numbers. Odd numbers greater than 3 are 5, 7, 9, 11, 13, $15,17,19,21, \ldots$, every third odd number greater than 3 is divisible by 3 . They are not prime numbers. Therefore, only three consecutive primes, each 2 from the next is $3,5,7$.
3. It is a standard result about primes (known as Euclid's Lemma) that if $p$ is prime, then whenever $p$ divides a product $a b, p$ divides at least one of $a, b$. prove the converse, that any natural number having this property (for any pair $a, b$ ) must be prime.

Sol) (Prove) If whenever $p$ divides a product $a b, p$ divides at least one of $a_{1} b$, then $p$ is prime.

Using contrapositive proof, let's suppose $p$ is not prime. Then, p is composite number, which is $p=a b . p=a b$ cannot divide either a or b . Therefore, the converse of Euclid's Lemma is true.

## Exercises 4.1.5

1. Try to prove Euclid's Lemma. If you do not succeed, move on to the following exercise.
$\rightarrow$ Without loss of generality, suppose $\operatorname{gcd}(\mathrm{p}, \mathrm{a})=1$. By Bezout's Lemma, there exist integers such that $\mathrm{x}, \mathrm{y}$ such that $p x+a y=1$. Hence $b(p x+a y)=b$ and $p b x+a b y=b$. Since $p \mid p$ and $p \mid a b$ (by hypothesis), $p \mid p b x+a b y=b$, as desired. On the other hand, if $p>1$ is not prime, then it must be composite, i.e., $p=a b$, for integers $\mathrm{a}, \mathrm{b}$ both greater than 1 . Then $p \backslash a$ and $p \backslash b$. Thuse the lemma's converse hold as well.
2. You can find proofs of Euclid's Lemma in most textbooks on elementary number theory, and on the Web. Find a proof and make sure you understand it. If you find a proof on the Web, you will need to check that it is correct. There are false mathematical proofs all over the Internet. Though false proofs on Wikipedia usually get corrected fairly quickly, they also occasionally become corrupted when a well-intentioned contributor makes an attempted simplification that renders the proof incorrect. Learning how to make good use of Web resources is an important part of being a good mathematical thinker.
3. A fascinating and, it turns out, useful (both within mathematics and for real-world applications) result about prime number is Fermat's Little Theorem: If $p$ is prime and $a$ is a natural number that is not a multiple of $p$, then $p \mid\left(a^{p-1}-1\right)$. Find (in a textbook
or on the Web) and understand a proof of this result. (Again, be wary of mathematics you find on websites of unknown or non-accredited authorshop.)

Sol) (Proof) Start by listing the first p-1 positive multiples of a:
$a, 2 a, 3 a, \ldots,(p-1) a$
Suppose that $r a$ and sa are the same modulo $p$, then we have $r=s(\bmod p)$, so the $p-1$ multiples of a above are distinct and nonzero; that is, they must be congruent to $1,2,3$, ..., p-1 in some order. Multiply all these congruences together and we find $a \cdot 2 a \cdot 3 a \cdot \ldots \cdot(p-1) a=1 \cdot 2 \cdot 3 \cdot \ldots \cdot(p-1)(\bmod p)$
or better $a^{(p-1)}(p-1)!=(p-1)!(\bmod p)$. Divide both side by $(\mathrm{p}-1)!$ to complete the proof.

## Exercise 4.2.1

1. Take the integers, $\mathbb{Z}$, as a given system of numbers. You want to define a larger system, $\mathbb{Q}$, that extends $\mathbb{Z}$ by having a quotient $a / b$ for every pair $a, b$ of integers, $b \neq 0$. How would you go about defining such a system? In particular, how would you respond to the question, "What is the quotient $a / b$ ?" (You cannot answer in terms of actual quotients, since until $\mathbb{Q}$ has been defined, you don't have quotients.)

Sol) The definition of rational number is like this:
$(\forall a \in Z)(\forall b \in Z)\left[\{\operatorname{gcd}(a, b)=1\} \wedge\{b \neq 0\} \rightarrow\left\{\frac{a}{b}\right.\right.$ is rational number $\left.\left.(Q)\right\}\right]$
So, if there are quotient $c$ about $\frac{a}{b}$, it can be represented as $\frac{a / c}{b / c}$ and again it is rational number. That is, $\frac{a}{b}=\frac{a / c}{b / c}$ and it is rational number.
2. Find an account of the construction of the rationals from the integers and understand if, one again being cautious about mathematics found on the Internet.

Sol) See the answer of problem 1 (Exercise 4.2.1)

## Exercise 4.3.1

1. Prove that the intersection of two intervals is again an interval. Is the same true for unions?

Sol) Let $A=(a, b)$ and $C=(c, d)$. Then

$$
\begin{aligned}
A \cap C & =\{x \mid a<x<b\} \cap\{x \mid c<x<d\} \\
& =\{x \mid \max (a, c)<x<\min (b, d)\} \\
& =(\max (a, c), \min (b, d))
\end{aligned}
$$

It may be empty set(3 ${ }^{\text {rd }}$ case), the empty set is an interval, it still the set of numbers between two points.

Similarly, for closed intervals and for half open intervals.

False for union,

For example, $(0,1) \cup(3,4)$ is not an interval (also it is an counterexample on video)
2. Taking $R$ as the universal set, express the following as simply as possible in terms of intervals and unions of intervals. (Note that $A^{\prime}$ denotes the complement of the set $A$ relative to the given universal set, which in this case is $R$. See the appendix.)

Sol) (a) $[1,3]=(-\infty, 1) \cup(3, \infty)$
(b) $(1,7]^{\prime}=(-\infty, 1] \cup(7, \infty)$
(c) $(5,8]^{\prime}=(-\infty, 5] \cup(8, \infty)$
(d) $(3,7) \cup[6,8]=(3,8]$
(e) $(-\infty, 3)^{\prime} \cup(6, \infty)=[3, \infty) \cup(6, \infty)=[3, \infty)$
(f) $\{\pi\}^{\prime}=(-\infty, \pi) \cup(\pi, \infty)$
(g) $(1,4] \cap[4,10]=(1,10]$
(h) $(1,2) \cap[2,3)=(1,3)$
(i) $A^{\prime}$, were $A=(6,8) \cap(7,9], A^{\prime}=(6,9]^{\prime}=(-\infty, 6] \cup(9, \infty)$
(j) $A^{\prime}$, where $A=(-\infty, 5] \cup(7, \infty), A^{\prime}=((-\infty, 5] \cup(7, \infty))^{\prime}=(5,7]^{\prime}$

## Exercise 4.3.2

1. Prove that if a set $A$ of integers/rationals/reals has an upper bound, then it has infinitely many different upper bounds.

Sol) upper bound b means $(\forall a \in A)(a \leq b)$ or $(\forall a \in A)(a<b)$

So, if we think about upper bound $(\forall a \in A)(a \leq b)$, no matter what domain is choosen (eg : integers, rationals, reals), there are infinitely many other numbers which is larger than b and all of them can be upper bound ( $b<c_{i}$ ).
i.e: $(\forall a \in A)\left(a \leq b<c_{1}<c_{2}<c_{3} \ldots \ldots ..\right)$, all $b$ and $c_{i}$ can be upper bound.
2. Prove that if a set $A$ of integers/rationals/reals has a least upper bound, then it is unique.

Sol) To be a least upper bound, it has to be satisfied two conditions, one thing is $(\forall a \in A)(a \leq b)$ and second thing is $(\forall \varepsilon>0)(\exists a \in A)(a>b-\varepsilon)$. So, in case of lub, there must be an $a$ which is equal with $b$.

If there is $(\forall a \in A)(a \leq c)$ and $b \neq c$, then both $b<c$ and $b>c$ cases meet the contradiction.

In case of $b<c$, than $(\forall a \in A)(a \leq b<c)$ and it violate the $(\forall a \in A)(a \leq c)$ condition. (equal is impossible)

In case of $b>c$, than $(\forall a \in A)(a \leq c<b)$ and it violate the $(\forall \varepsilon>0)(\exists a \in A)(a>b-\varepsilon)$ condition (there are $b>c$ but there is not exist such that $a>c$ ). And it also violate the $(\forall a \in A)(a \leq b)$ condition.

So, it must be $b=c$ : it's unique.
3. Let $A$ be a set of integers, rationals, or reals. Prove that $b$ is the least upper bound of $A$ iff:
(a) $(\forall a \in A)(a \leq b)$; and
(b) whenever $c<b$ there is an a $a \in A$ such that $a>c$.

Sol) Condition (a) says that $b$ is an upper bound.

Condition (b) means that $b$ is a lub iff no $c<b$ is an upper bound
Iff, for any $c<b, c$ is not an upper bound.
Iff, for any $c<b$, there is an $a \in A$ such that $\neg(a \leq c)$

* in here $\neg$ could means "not the case"

Iff, for any $c<b$, there is an $a \in A$, such that $a>c$
4. The following variant of the above characterization is often found. Show that $b$ is the lub of $A$ iff:
(a) $(\forall a \in A)(a \leq b)$; and
(b) $(\forall \varepsilon>0)(\exists a \in A)(a>b-\varepsilon)$.

Sol) In this problem, if we let $b-\varepsilon=c$, then, $(\forall \varepsilon>0)->(\forall c>b)$, and $(a>b-\varepsilon)->(a>c)$. Then, this problem is equal to problem 3.
5. Give an example of a set of integers that has no upper bound.

Sol) $A=\{x \mid x \in N\}$ has no upper bound.
6. Show that any finite set of integers/rationals/reals has a least upper bound.

Sol) Let $A$ is some finite set ('no matter what domain is'). Then, we can express like this :
$(\forall a \in A)(a \leq \max (A))$

Now, if we let the $\max (A)=b$, then automatically, condition of pbm 3 or 4 is satisfied.
7. Intervals: What is lub $(a, b)$ ? What is lub $[a, b]$ ? What is max $(a, b)$ ? What is max $[a, b]$ ? Sol) because of the completeness property,
lub $(a, b)=b-1$ (integer cases)
lub $(\mathrm{a}, \mathrm{b})=$ lub $[a, b]=b$ (other cases / source: Wikipedia 'supremum' explain)
lub $[a, b]=b$
$\max (\mathrm{a}, \mathrm{b})=b-1$ (integer cases) $/$ not defined (other cases)
$\max [\mathrm{a}, \mathrm{b}]=\mathrm{b}$
8. Let $A=\{|x-y| \mid x, y \in(a, b)\}$. Prove that A has an upper bound. What is lub $A$ ?

Sol) $x, y \in(a, b)=(a<x<b)$ and $(a<y<b)$, so
$a-b<x-y<b-a$ and $0 \leq|x-y|<b-a$.

So, $|x-y|$ 's upper bound is $b-a$.
9. Define the notion of a lower bound of a set of integers/rationals/reals.

Sol) <lower bound>

$$
(\forall a \in A)((a \geq b) \operatorname{or}(a>b))
$$

10. Define the notion of a greatest lower bound (glb) of a set of integers/rationals/reals by analogy with our original definition of lub.

Sol) <greatest lower bound>
(a) $(\forall a \in A)(a \geq b)$; and
(b) $(\forall \varepsilon>0)(\exists a \in A)(a<b+\varepsilon)$.
11. State and prove the analog of question 3 for greatest lower bounds.

Sol) (a) $(\forall a \in A)((a \geq b) o r(a>b))$; and
(b) whenever $c>b$ there is an $a \in A$ such that $a<c$.
$\rightarrow$ Condition (a) says that $b$ is an lower bound.

Condition (b) means that $b$ is a glb iff no $c>b$ is an lower bound

Iff, for any $c>b, c$ is not an lower bound.
Iff, for any $c>b$, there is an $a \in A$ such that $\neg(a \geq c)$

* in here $\neg$ could means "not the case"

Iff, for any $c>b$, there is an $a \in A$, such that $a<c$
12. State and prove the analog of question 4 for greatest lower bounds.

Sol) (a) $(\forall a \in A)((a \geq b) o r(a>b))$; and
(b) $(\forall \varepsilon>0)(\exists a \in A)(a<b+\varepsilon)$.
$\rightarrow$ in this problem, if we let $b+\varepsilon=c$, then, $(\forall \varepsilon>0)->(\forall c>b)$, and $(a<b+\varepsilon)->(a<c)$. Then, this problem is equal to problem 11.
13. Show that the Completeness Property for the real number system could equally well have been defined by the statement, "Any nonempty set of reals that has a lower bound has a greatest lower bound."

Sol) Let $A$ is "a nonempty set of reals that has a lower bound". So, let $(\forall a \in A)(a \geq \min (A))$. So, if we let the $\min (A)=b$, then automatically, condition of pbm 11 or 12 is satisfied.
14. The integers satisfy the Completeness Property, but for a trivial reason. What is the reason?

Sol) "Any nonempty set of integers that has a lower bound has a greatest lower bound."
It is trivial. If there is a finite integer set $A$, than definitely there is an $(\forall a \in A)(a \geq \min (A))$. So, if we let the $\min (A)=b$, then automatically, condition of pbm 11 or 12 is satisfied. So, the above statement is valid.

## Exercise 4.3.3

1. Let $A=\left\{r \in Q \mid r>0 \wedge r^{2}>3\right\}$. Show that $A$ has a lower bound in $Q$ but no greatest lower bound in $Q$. Give all details of the proof along the lines of Theorem 4.3.1

Sol) Let $x=\frac{p}{q} \in Q$ be any upper bound of $A$, where $p, q \in N$.

Suppose first that $x^{2}<3$. Thus $3 q^{2}>p^{2}$. Now, as $n$ gets large, the expression $\frac{n^{2}}{2 n+1}$ increases without bound, so we can pick $n \in N$ so large that $\frac{n^{2}}{2 n+1}>\frac{p^{2}}{3 q^{2}-p^{2}}$

Rearranging, this gives $3 n^{2} q^{2}>p^{2}(n+1)^{2}$
Hence $\left(\frac{n+1}{n}\right)^{2} \frac{p^{2}}{q^{2}}<3$
Let $y=\left(\frac{n+1}{n}\right) \frac{p}{q}$
Thus $y^{2}<3$. Now, since $\frac{n+1}{n}>1$, we have $x<y$. But $y$ is rational and we have just seen that $y^{2}<3$, so $y \in A$ (from definition of $A$ ). This contradicts the fact that $x$ is an upper bound for $A$.

It follows that we must have $x^{2} \geq 3$. Since there is no rational whose square is equal to 3 , this means that $x^{2}>3$. Thus $p^{2}>3 q^{2}$, and we can pick $n \in N$ so large now that $\frac{n^{2}}{2 n+1}>\frac{3 p^{2}}{p^{2}-3 q^{2}}$

Rearranging, this gives $n^{2} p^{2}>3 q^{2}(n+1)^{2}$
Hence $\left(\frac{n}{n+1}\right)^{2} \frac{p^{2}}{q^{2}}>3$

Let $y=\left(\frac{n}{n+1}\right) \frac{p}{q}$

Then $y^{2}>3$. Since $n /(n+1)<1, y<x$. But for any $a \in A, a^{2}<3<y^{2}$, so $a<y$. Thus $y$ is an upper bound of $A$ less than $x$, as we set out to prove.

From these prove, the completeness property is not hold in rational line $Q$.
2. In addition to the completeness property, the Archimedean property is an important fundamental property of $R$. It says is that if $x, y \in R$ and $x, y>0$, there is an $n \in N$ such that $n x>y$.

Use the Archimedean property to show that if $r, s \in R$ and $r<s$, there is a $q \in Q$ such that $r<q<s$. (Hint: pick $n \in N, n>\frac{1}{s-r}$, and find an $m \in N$ such that $\left.r<\frac{m}{n}<s\right)$.

Sol) Because $s-r>0$, so we can use the Archimedean property at $s-r$ and 1 . So, if we apply the Archimedean property at $s-r$ and 1 , then there must be an $n \in N$ such that $n(s-r)>1$. It also means that $n r<n s$ and because $n s-n r>1$ (the distance of two number in larger than 1), there must be an $m$ such that $n r<m<n s$. Finally, $r<\frac{m}{n}<s$ and $\frac{m}{n}$ is rational number $(Q)$.

## Exercise 4.4.1

(1) Formulate both in symbols and in words what it means to say that $a_{n} \rightarrow a$ as $n \rightarrow \infty$.

Sol) In symols: $\neg\left(\lim _{n \rightarrow \infty} a_{n}=a\right)$ or $\lim _{n \rightarrow \infty} a_{n} \neq a$
$=>\neg(\forall \varepsilon>0)(\exists n \in N)(\forall m \geq n)\left(\left|a_{m}-a\right|<\varepsilon\right)$
$(\exists \varepsilon>0)(\forall n \in N)(\exists m \geq n)\left(\left|a_{m}-a\right| \geq \varepsilon\right)$
In words: $a_{n}$ don't get arbitrarily closer and closer to $a$
(2) Prove that $\left(\frac{n}{n+1}\right)^{2} \rightarrow 1$ as $n \rightarrow \infty$.

Sol) Let $\varepsilon>0$ be given. We must find an $n \in N$ such that all $m \geq n$,

$$
\left|\left(\frac{m}{m+1}\right)^{2}-1\right|<\varepsilon
$$

$$
\left|\left(\frac{m}{m+1}\right)^{2}-1\right|=\left|\frac{m^{2}-\left(m^{2}+2 m+1\right)}{(m+1)^{2}}\right| \leq \frac{2 m+1}{(m+1)^{2}}<\varepsilon
$$

Pick $n$ so large that $\frac{(n+1)^{2}}{2 n+1}>\frac{1}{\varepsilon}$. Then, for all $m \geq n$,

$$
\left|\frac{2 m+1}{(m+1)^{2}}\right| \leq\left|\frac{2 n+1}{(n+1)^{2}}\right| \leq \varepsilon
$$

(3) Prove that $\frac{1}{n^{2}} \rightarrow 0$ as $n \rightarrow \infty$.

Sol) Let $\varepsilon>0$ be given. We must find an $n \in N$ such that all $m \geq n$,

$$
\left|\frac{1}{m^{2}}-0\right|<\varepsilon
$$

Pick $n$ so large that $n>\frac{1}{\varepsilon}$. Then, for all $m \geq n$,

$$
\left|\frac{1}{m^{2}}-0\right|=\frac{1}{m^{2}}<\frac{1}{m} \leq \frac{1}{n}<\varepsilon
$$

(4) Prove that $\frac{1}{2^{n}} \rightarrow 0$ as $n \rightarrow \infty$.

Sol) Let $\varepsilon>0$ be given. We must find an $n \in N$ such that all $m \geq n$,

$$
\left|\frac{1}{2^{m}}-0\right|<\varepsilon
$$

Pick $n$ so large that $n>\frac{1}{\varepsilon}$. Then, for all $m \geq n$,

$$
\left|\frac{1}{2^{m}}-0\right|=\frac{1}{2^{m}}<\frac{1}{m} \leq \frac{1}{n}<\varepsilon
$$

(5) We say a sequence $\left\{a_{n}\right\}^{\infty}{ }_{n=1}$ tends to infinity if, as $n$ increases, $a_{n}$ increases without bound. For instance, the sequence $\{n\}_{n=1}^{\infty}$ tends to infinity, as does the sequence $\left\{2^{n}\right\}_{n=1}^{\infty}$. Formulate a precise definition of this notion, and prove that both of these examples fulfill the definition.

Sol) $\lim _{n \rightarrow \infty} a_{n}=\infty$
$=>a_{n}$ get arbitrarily closer and closer to infinity

Both $\{n\}^{\infty}{ }_{n=1}$ and $\left\{2^{n}\right\}^{\infty}{ }_{n=1}$ are increasing order, so if $n$ goes infinity, the sequences tend to be infinity.
(6) Let $\left\{a_{n}\right\}^{\infty}{ }_{n=1}$ be an increasing sequence (i.e. $a_{n}<a_{n+1}$ for each $n$ ). Suppose that $a_{n} \rightarrow a$ as $n \rightarrow \infty$. Prove that $a=\operatorname{lub}\left\{a_{1}, a_{2}, a_{3}, \ldots\right\}_{n=1}^{\infty}$.

Sol) Suppose that $\lim _{n \rightarrow \infty} a_{n}=a$, and $(\forall \varepsilon>0)(\exists n \in N)(\forall m \geq n)\left(\left|a_{m}-a\right|<\varepsilon\right)$
$=>$ the conditions of lub are as follows :
(a) $(\forall a \in A)(a \leq b)$ and
(b) $(\forall \varepsilon>0)(\exists a \in A)(a>b-\varepsilon)$.
=> To prove this sentence easily, let $a$ is element of set A, and $b$ is value of lub.
$=>$ Than we can suppose that $\lim _{n \rightarrow \infty} a_{n}=b,(\forall \varepsilon>0)(\exists n \in N)(\forall m \geq n)\left(\left|a_{m}-b\right|<\varepsilon\right)$ and the conditions of lub is $(\forall a \in A)(a \leq b),(\forall \varepsilon>0)(\exists a \in A)(a>b-\varepsilon)$.
$=>$ If we rearrange the statement $\left|a_{m}-b\right|<\varepsilon$, then we can obtain the condition $b-\varepsilon<a_{m}<b+\varepsilon$. Also, if we let the set $A=\left\{a_{n}\right\}_{n=1}^{\infty}$, then we can obtain $(\forall a \in A)(a \leq b)$ and $(\forall \varepsilon>0)(\exists a \in A)(a>b-\varepsilon)$.
$=>$ So we can say that $\lim _{n \rightarrow \infty} a_{n}=a=\operatorname{lub}\left\{a_{1}, a_{2}, a_{3}, \ldots\right\}_{n=1}^{\infty}$
(7) Prove that if $\left\{a_{n}\right\}_{n=1}^{\infty}$ is increasing and bounded above, then it tends to a limit.

Sol) if $\left\{a_{n}\right\}_{n=1}^{\infty}$ is increasing (i.e. $a_{n}<a_{n+1}$ for each $n$ ), and $\left\{a_{n}\right\}_{n=1}^{\infty}$ is bounded(i.e. $(\forall a \in A)(a \leq b)$, all of element in set $A$ is smaller or equal to $b$, if we pick $n$ so large, then it
must be $\left|a_{n}-b\right|<\varepsilon$ and $\varepsilon$ is some positive small number. Also Because $A$ is a increasing sequence, then for all $m$ such that $m \geq n$, also it must be $\left|a_{m}-a\right|<\varepsilon$
$=>$ From these reasons, we can make the statement $(\forall \varepsilon>0)(\exists n \in N)(\forall m \geq n)\left(\left|a_{m}-a\right|<\varepsilon\right)$ and we can say that $\lim _{n \rightarrow \infty} a_{n}=b$ and it tends to a limit.

