UCSD

Lecture : MATH 109 Mathematical Reasoning

2020 SP

Lecturer: Yuming Paul Zhang *Scribe:*

Contents

1 The language of mathematics

1.1 Mathematical statements

Mathematical statements is a broad concepts. It includes *proposition* and *predicates*.

A *proposition* is a sentence which is either true or false. A *predicate* is a sentence which depends on some free variables and it can be both true or false depending on the values of the free variables.

Example of two propositions:

(i) $1 + 1 = 2$.

(ii) $\pi = 2$.

Here (i) is true while (ii) is false.

Example 1.1.1. *"Every even integer greater than 2 may be written as the sum of two prime numbers" is a proposition. But we don't know it is true or false. We often call a proposition like this as an open problem.*

This is the *Goldbach's Conjecture*. This conjecture is raised by Christian Goldbach in 1742. The Chinese famous mathematician Jingrun Chen proved a "close" proposition to the Goldbach's Conjecture in 1966: every even integer greater than 2 can be written as the sum of a prime and a semiprime (the product of two primes).

Then let us look at two examples which are not propositions.

Example 1.1.2.

$$(i)\, m < n, \quad (ii)\, x \textit{ is a special number}, \quad (iii)\, n - m.$$

Here (i) is a sentence but it is not a proposition. Because we don't know whether it is true or not until the values of n, m are given. Sentences like this are called predicates. The symbols like n, m are called free variables.

(ii) is a sentence but it is meaningless in mathematics because we don't know what "special" means. (ii) can be a predicates if we define, for example, "special" to be prime numbers' square.

(iii) $n - m$ is not a sentence.

Definition 1.1. The word *statement* will be used to denote a sentence which is either a proposition or a predicate.

1.2 Logical connectives

In mathematics, we often need to consider a large number of statements. We need logical connectives to connect them or to tell the logical relations of them.

We introduce three of the logical connectives: **"or", "and", "not"**.

Suppose we have two statements: P, Q. If one of P and Q is true, then P or Q is true.

Example 1.2.1. *(1) If $P =$ "$n < m$" and $Q =$ "$n \geq m$", then P or Q is true.*
(2) A true proposition: $ab = 0$ if $a = 0$ or $b = 0$.

The connective "or" is sometimes hidden in other notations:

$$a \leq b: \quad \text{means: } a < b \quad \text{or} a = b;$$
$$a = \pm b: \quad \text{means: } a = b \quad \text{or} a = -b;$$

Now we consider **"and"**. We use "and" when we want to assert that two things are both true.

Example 1.2.2. *(1) If $P =$ "$n < m$" and $Q =$ "$n \geq m$", then P and Q has to be false.*
(2) $3 < \pi < 4$ means $\pi > 3$ and $\pi < 4$.

Now we discuss **"not"**. A statement P is true is and only if not P is false.

Example 1.2.3. *Let $f(x)$ be a polynomial and a be a real number. Write the negation of the following statement: if $f(a) = 0$ then a is positive.*

Solution. Consider P to be a statement that $f(a) = 0$ and Q to be a statement that a is positive. Then the assertion (or statement) here is "P implies Q". The negation of this is "not (P implies Q)". The negation is the same as "P does not implies Q". And so it is "(P) and (not Q) can happen at the same time".

Thus the correct negation is: it is possible that $f(a) = 0$ and a is non-positive i.e. there exists $a \leq 0$ such that $f(a) = 0$.

We will discuss this more in Theorem 2.2. □

Example 1.2.4. *Read the tables 1.2.1, 1.2.2 in the textbook.*

2 Implications

Mathematics is primarily concerned with establishing the truth of statements. This is achieved by giving a proof of the statement. Implication is one of the key in proofs.

2.1 Implications

The definition of implications is the following: given two statements P and Q, we say P implies Q if whenever P is true then we must have that Q is true. We use the notation $P \implies Q$.

Example 2.1.1. *Suppose that P is the statement that "$x^2 - x - 2 > 0$", Q_1 is the statement that "$x > 2$ or $x < -1$" and Q_2 is the statement that "$x \neq 0$". Then we have*

$$P \implies Q_1 \implies Q_2.$$

Actually here we also have

$$Q_1 \implies P.$$

But Q_2 does not implies Q_1 written as

$$Q_2 \not\Longrightarrow Q_1.$$

Definition 2.1. In an implication $P \implies Q$, P is called the *hypothesis* or *antecedent* and Q is called the *conclusion* or *consequent*.

Example 2.1.2. *Consider the following statements:*

(i) $(\pi < 4) \implies (1 + 1 = 2)$*;*

(ii) $(\pi < 4) \implies (1 + 1 = 3)$*;*

(iii) $(\pi < 3) \implies (1 + 1 = 2)$*;*

(iv) $(\pi < 3) \implies (1 + 1 = 3)$.

(i)(iii)(iv) is OK. For (i), both the assumption and the conclusion are true. For (iii)(iv), the assumption can never be true, so we do not care what the conclusion is in this case. For (ii), even under the assumption, the conclusion is false.

Theorem 2.2. *The followings are equivalent (have the same meaning)*

- $P \not\Longrightarrow Q$*;*
- *"$P \implies Q$" is false;*
- *"P and (not Q)" is true.*

Reading implications. $P \implies Q$ is the same as

- P implies Q;
- Q if P;
- P only if Q;
- P is sufficient for Q;
- Q is necessary for P.

Definition 2.3. We define *equivalence* of two statements P, Q (written as $P \iff Q$) as

$$(P \implies Q) \quad \text{and} \quad (Q \implies P).$$

We read $P \iff Q$ as

- P is equivalent to Q.
- P is necessary and sufficient for Q.
- P if and only if Q (sometimes written P iff Q).
- P precisely when Q.

Definition 2.4. By *universal* statement we mean the statement is always true for all values of variables in the statement. For example "$a^2 + b^2 \geq 0$ for all real numbers a, b".

3 Proofs

A proof of a mathematical statement is a logical argument which establishes the truth of the statement. The steps of the logical argument are usually provided by implications.

3.1 Direct proofs

Example 3.1.1. *For positive real numbers a and b, prove $a < b \implies a^2 < b^2$.*

Before the proof, we need to list the assumptions that people take for granted. The following basic properties of real numbers are often referred to as *Axioms*. Let a, b, c be any real numbers.

(i) Trichotomy law. For each pair of real numbers a, b, one of the following holds: $a < b$, $a = b$, $a > b$.

(ii) Addition law.

$$a < b \iff a + c < b + c.$$

(ii) Multiplication law.

$$a < b \iff ac < bc \quad \text{if } c > 0,$$
$$a < b \iff ac > bc \quad \text{if } c < 0.$$

(ii) Transitive law.

$$a < b \text{ and } b < c \implies a < c.$$

Now we are able to write a formal proof of example 3.1.1.

Proof. Given positive real numbers a, b and suppose $a < b$. Then by the multiplication law $a^2 < ab$ (multiplying through by $a > 0$) and $ab < b^2$ (multiplying through by $b > 0$). By the transitive law $a^2 < ab < b^2$. Hence $a < b \implies a^2 < b^2$. $\square$

3.2 Constructing proofs backwards

Sometimes the problem would be much easier if we start with the conclusions instead of the assumptions.

Example 3.2.1. *For real numbers a and b such that $a < b$, show $4ab < (a+b)^2$.*

Actually the conclusion holds for all real a, b that are not equal.

Let us construct a proof backwards:

$$\begin{aligned} 4ab < (a+b)^2 &\iff 4ab < a^2 + 2ab + b^2 \\ &\iff 0 < a^2 - 2ab + b^2 \\ &\iff 0 < (a-b)^2 \\ &\iff a \neq b \quad \text{(think about why?)} \\ &\Longleftarrow a < b. \end{aligned}$$

Hence $a < b \implies 4ab < (a+b)^2$. With this backwards proof, if we write it backward, we get a direct proof:

Proof. $a < b \implies a \neq b \implies (a-b)^2 > 0 \implies 0 < a^2 - 2ab + b^2 \implies 4ab < a^2 + 2ab + b^2 \implies 4ab < (a+b)^2$. □

4 Proof by contradiction

In the previous section we construct some simple direct proofs. Here we introduce a different idea of proof: proof by contradiction.

4.1 Proving negative statements by contradiction

Let us explain the idea through the following example:

Example 4.1.1. *There do not exist integers m, n such that*

$$14m + 20n = 101. \tag{1}$$

Idea: The problem is: known that m, n are integers, and the goal is to show that $14m + 20n \neq 101$.

The proof by contradiction method is, instead of starting from what is known, we start with assuming that the goal is incorrect. So in this example, we assume that $14m + 20n = 101$ and m, n are integers. And the goal is to show that this is impossible i.e. contradiction.

This would be easier to argue. Because, when m, n are integers, $14m + 20n$ is an integer and furthermore it equals $2(7m + 10n)$ which is an even number. While 101 is odd, we obtain a contraction. This contraction indicates that the original statement (1) is true.

□

Now we consider a harder problem:

Example 4.1.2. *Let n be a positive integer. Then $4n+3$ can not be one positive integer's square.*

Proof. Suppose for contradiction that there exist a positive integer n such that $4n+3=m^2$ for some positive integer m.

Since m is a positive integer, it is either odd or even. If it is even, we can suppose $m=2k$ for some positive integer k. Then $m^2=4k^2$ is even. However $4n+3$ is odd, $m^2=4n+3$ is not possible.

Now if m is odd, suppose $m=2k+1$. Then $m^2=(2k+1)^2=4k^2+4k+1$ and thus the remainder of dividing m^2 by 4 equals 1. However the remainder of dividing $4n+3$ by 4 equals 3. Therefore m^2 can not equal $4n+3$. We get a contradiction.

In all $4n+3$ can not be one positive integer's square.

□

A template for proofs by contradiction. To show $P \implies Q$.

Proof. Suppose, for contradiction, that the statement Q is false. Then [*present argument which leads to a contradiction*]. Hence our assumption that Q is false must be false. Thus Q is true as required. □

4.2 Proving implications by contradiction

Example 4.2.1. *If a, b, c are integers such that $a > b$, then*

$$ac \leq bc \implies c \leq 0.$$

We are going to use the Multiplication law:

$$a < b \iff ac < bc \quad \text{if } c > 0,$$

However it is difficult to make use of the multiplicative law of inequalities in a direct proof. The easiest thing to do in this case is again a proof by contradiction.

Proof. For integers a, b, c with $a > b$, suppose that $ac \leq bc$ but, for contradiction, that $c > 0$. Then the given statement $a > b$ implies that $ac > bc$ by the multiplicative law. However this contradicts with the statement that $ac \leq bc$. Hence the assumption that $c > 0$ must be false. Thus $ac \leq bc \implies c \leq 0$. □

4.3 Proof by contrapositive

Theorem 4.1. *Let P, Q be two statements. Then $P \implies Q$ is equivalent to $(not\, Q) \implies (not\, P)$.*

Can you prove the theorem?

A proof by contrapositive is to use the theorem and so that we show $(not\, Q) \implies (not\, P)$ to conclude with $P \implies Q$.

Let us again consider Example (4.2.1).

Proof. (of Example (4.2.1)) The contrapositive of the statement

$$ac \leq bc \implies c \leq 0$$

is the statement

$$c > 0 \implies ac > bc$$

which is exactly the multiplicative law. Thus the proposition of Example (4.2.1) is true. □

4.4 Proving "or" statements

In this subsection we constructing a proof for composite statements involving "or".

Example 4.4.1. *If a and b are real numbers, then*

$$ab = 0 \iff a = 0 \textit{ or } b = 0.$$

Before the proof, let us analyze the statement. We are asked to prove a statement of the form $P \iff Q$. Then we are required to give two parts of proofs: $P \implies Q$ and $P \impliedby Q$.

Proof. " $\implies$ ": Known $ab = 0$ and the goal is to show that a or b equals 0. If $a = 0$, the conclusion holds. Otherwise suppose $a \neq 0$. Then dividing $ab = 0$ through by a gives $b = 0$, as required. Hence $ab = 0 \implies a = 0$ or $b = 0$.

"$\impliedby$": If one of a, b equals 0, then it is a basic property of 0 that $ab = 0$. The conclusion holds. □

Actually we can discuss by cases for a, b. there are three possibility for a (b): $a < 0$ or $a = 0$ or $a > 0$ ($b < 0$ or $b = 0$ or $b > 0$). Discussing by cases leads to nine possibilities in all

	a<0	a=0	a>0
b<0	ab>0	ab=0	ab<0
b=0	ab=0	ab=0	ab=0
b>0	ab<0	ab=0	ab>0

5 The induction principle

The induction principle is a special proof technique which is particularly useful when proving statements about the positive integers.

Suppose we wish to prove some property for all the positive integers: 1,2,3,4... That is we want to prove infinitely many statements labeled by n. Suppose the statement involving positive integer n is $P(n)$.

Axiom 5.1. ***(The induction principle)*** *$P(n)$ is true for all $n = 1, 2, 3, \ldots$ if*

(i) $P(1)$ is true, and

(ii) $P(k) \implies P(k+1)$ *for all positive integers* k.

Remark 5.1. (i) is often referred to as the base case. In (ii), we assume $P(k)$ and the goal is to prove $P(k+1)$. The assumption $P(k)$ is called the inductive hypothesis.

Example 5.0.1. *For all positive integers* n *we have* $n \leq 2^n$.

Proof. We use induction on n using the Axiom 5.1.

Base case: For $n = 1$, since $n = 1 \leq 2 = 2^n$, then $n \leq 2^n$.

Inductive step: Suppose now as inductive hypothesis that $k \leq 2^k$ for a positive integer k. Then

$$2^{k+1} = 2 \times 2^k \geq 2k \geq k + 1.$$

So $k + 1 \leq 2^{k+1}$ as required.

Conclusion: Hence, by induction, $n \leq 2^n$ holds for all positive integer n. □

Example 5.0.2. *For all positive integers* n*, the number* $n^2 + n$ *is even.*

Proof. We use induction on n. (Base case) For $n = 1$, $n^2 + n = 1 + 1 = 2$ which is even as required. (Inductive step) Now suppose $n^2 + n$ is even for $n = k$ for some positive integer k. Then we have

$$k^2 + k = 2q \quad \text{for some positive integer } q.$$

For $n = k + 1$,

$$(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + 2(k+1) = 2q + 2(k+1)$$

which is again even. (Conclusion) Hence, by induction, $n^2 + n$ is even for all positive integers n. □

5.1 Changing the base case

Example 5.1.1. *For all integers* n *such that* $n \geq 4$*, we have the inequality* $n^2 \leq 2^n$.

Solution. We use induction on n starting with $n = 4$. (Base case) For $n = 4$, $n^2 = 16 = 2^n$ and so $n^2 \leq 2^n$.

(Inductive step) Suppose now as inductive hypothesis that $k^2 \leq 2^k$ for some $k \geq 4$. Then

$$2^{k+1} \geq 2k^2.$$

So we will have proved that $2^{k+1} \geq (k+1)^2$ if we can show that $2k^2 \geq (k+1)^2$. Notice

$$2k^2 - (k+1)^2 = 2k^2 - k^2 - 2k - 1 = k^2 - 2k - 1 = k(k-2) - 1 \geq 0$$

when $k \geq 4$. Therefore we proved $2^{k+1} \geq (k+1)^2$ to complete the inductive step.

(Conclusion) Hence, by induction, $n^2 \leq 2^n$ for all $n \geq 4$.

□

5.2 Definition by induction

Suppose given a sequence of numbers $a_1, a_2, ...$, recall the summation notation: $\Sigma_{i=1}^n a_i$ for positive integers n. We can interpret the summation notation as a definition by induction:

(i) For $n = 1$, $\Sigma_{i=1}^1 a_i$ is defined as a_1;

(ii) (Suppose $\Sigma_{i=1}^k a_i$ is defined.) For $n = k+1$, $\Sigma_{i=1}^{k+1} a_i = (\Sigma_{i=1}^k a_i) + a_{k+1}$.

Example 5.2.1. *For positive integers n, show*

$$\Sigma_{i=1}^n i = \frac{1}{2}n(n+1),$$

$$\Sigma_{i=1}^n i^2 = \frac{1}{6}n(n+1)(2n+1).$$

Proof. Let me only prove the first equality here.

We use induction on n. (Base case) For $n = 1$, $\Sigma_{i=1}^1 i = 1$ and $\frac{1}{2}n(n+1) = \frac{1}{2} \times 1 \times 2 = 1$ and therefore the equality holds for $n = 1$.

(Inductive step) Suppose as inductive hypothesis that $\Sigma_{i=1}^k i = \frac{1}{2}k(k+1)$ for some positive integer k. Then

$$\begin{aligned}\Sigma_{i=1}^{k+1} i &= \Sigma_{i=1}^k i + (k+1) \quad \text{(by definition of summation notation)}\\ &= \frac{1}{2}k(k+1) \quad \text{(by inductive hypothesis)}\\ &= \frac{1}{2}(k+1)(k+2) \quad \text{(by direct computations)}\end{aligned}$$

and so

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

as required.

(Conclusion) Hence, by induction, $\Sigma_{i=1}^n i = \frac{1}{2}n(n+1)$ holds for all positive integer n. □

Another example is the factorial n.

Definition 5.2. For non-negative integers n, the number factorial n written $n!$, are defined inductively by

(i) $0! = 1;$ and

(ii) $(k+1)! = k! \times (k+1)$ for all non-negative integer k.

5.3 The strong induction principle

Axiom 5.2. ***(The strong induction principle)*** *Suppose that $P(n)$ is a statement involving a general positive integer n. Then $P(n)$ is true for all positive integers n if*

(i) $P(1)$ *is true, and*

(ii) $\big[\, P(n)$ *holds for all positive integers* $n \leq k \,\big] \implies P(k+1)$*, for all positive integers* k*.*

In this case, the basic template is as follows.

Proof. We use (strong) induction on n.

(Base case) $\big[$ *Prove the statement* $P(1)\big]$.

(Inductive step) Suppose now as inductive hypothesis that $\big[P(n)$ *is true for all positive integers* $n \leq k\big]$ for some positive integer k. Then $\big[$*deduce that* $P(k+1)$ *is true*$\big]$. This proves the inductive step.

(Conclusion) Hence, by induction, $\big[\, P(n)$ *is true for all positive integers* $n\big]$. □

As an illustration of the use of this form of induction we introduce the Fibonacci numbers.

Definition 5.3. For each positive integer n define the number F_n inductively as follows.

$$\begin{aligned} &F_1 = 1, \quad F_2 = 1, \\ &F_{k+1} = F_k + F_{k-1} \quad \text{for } k \geq 2. \end{aligned}$$

In this way, we defined a sequence of numbers. The beginning of this sequence is

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...,$$

and the sequence is known as the Fibonacci sequence.

Proposition 5.4. *The Fibonacci numbers are given by the following formula:*

$$F_n = (\alpha^n - \beta^n)/\sqrt{5}$$

where $\alpha, \beta = (1 \pm \sqrt{5})/2$.

Remark 5.5. Here α, β are the roots of

$$x^2 - x - 1 = 0.$$

It is surprising here that these integers F_n involves $\sqrt{5}$ which is not an integer (which is not even a rational number). Actually we will see later that there is a general procedure for finding a general formula for sequences defined inductively in this way.

Proof. (Base case) For $n = 1$, the formula gives $(\alpha - \beta)/\sqrt{5} = 1 = F_1$. Since the inductive formula does not apply until F_3, we have to calculate F_3. For $n = 2$, the formula gives $(\alpha^2 - \beta^2)/\sqrt{5}$. Using that $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$, we get

$$(\alpha^2 - \beta^2)/\sqrt{5} = 1 = F_2.$$

(Inductive step) Now suppose as inductive hypothesis that the formula holds for all positive integers n such that $n \leq k$ for some positive integer $k \geq 2$. Then

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} \quad \text{(by definition of the sequence)} \\ &= ((\alpha^k - \beta^k) + (\alpha^{k-1} - \beta^{k-1}))/\sqrt{5} \quad \text{(by inductive hypothesis)} \\ &= ((\alpha^{k-1}(\alpha + 1) - \beta^{k-1}(\beta + 1))/\sqrt{5} \\ &= (\alpha^{k+1} - \beta^{k+1})/\sqrt{5} \quad \text{(using } \alpha^2 = \alpha + 1, \beta^2 = \beta + 1) \end{aligned}$$

as required to prove the formula for $n = k + 1$.

(Conclusion) Hence, by induction, the formula holds for all positive integers. □

6 The language of set theory

The language of set theory is used throughout mathematics. For example, real numbers, integers etc. are sets of numbers.

We usually use the following symbols:

$\mathbb{Z}$:	the set of all integers;
$\mathbb{Z}^+$:	the set of all positive integers;
$\mathbb{Z}^{\geq}$:	the set of all non-negative integers (same as $\mathbb{N}$, the natural numbers);
$\mathbb{Q}$:	the set of all rational numbers;
$\mathbb{R}$:	the set of all real numbers;
$\mathbb{C}$:	the set of all complex numbers.

6.1 Sets

More generally, a *set* is defined as a collection of objects (not necessarily numbers). The objects in a set are called the *elements, members or points* of the set. We write

$$x \in A$$

to denote that x is an element of the set A. Here x can be a number, a ball, a space or an apple etc. The negation of the statement $x \in A$ is written $x \notin A$. For example $\sqrt{2} \notin \mathbb{Q}$.

If only talking about a set of elements, we DO NOT consider any order of elements in a set; we DO NOT repeat the same element for more than one times in one set.

There are three ways to specify a set:

- **List the elements.** E.g. $A = \{1, 3, \pi, -14, \text{“banana”}\}$.
- **Conditional definition.** E.g. $B = \{n \in \mathbb{Z} \,|\, 0 < n < 6\}$.
- **Constructive definition** by giving a formula of elements. E.g. $\{n^2 \,|\, n \in \mathbb{Z}\}$, $\{a/b \,|\, a, b \in \mathbb{Z},\, b \neq 0\}$ (this is the same as $\mathbb{Q}$). The two set examples here contains infinitely many elements.

Definition 6.1. Equality of sets. Two set A, B are equal, written $A = B$, if they have precisely the same elements, i.e. $A = B$ means $x \in A \iff x \in B$.

Example 6.1.1.

$$\{x \in \mathbb{R} \,|\, x^2 - x - 2 = 0\} = \{-1, 2\} = \{2, -1\} = \{-1, -1, 2\}.$$

Definition 6.2. The empty set is the unique set which has no element at all, denoted as $\emptyset$.

Definition 6.3. Given sets A, B, we say that A *is a subset of* B, written $A \subseteq B$, when every element of A is an element of B, i.e. $x \in A \implies x \in B$. If in addition $A \neq B$, then we say that A is a *proper* subset of B and write $A \subset B$.

Remark 6.4. It can be shown that

$$A = B \iff A \subseteq B \text{ and } B \subseteq A.$$

Next $\in$ and $\subseteq$ have very different meaning. For example $a \in A$ means that a is an element of A. While for $B \subseteq A$, B is a set, but just smaller. We can write

$$a \in A \iff \{a\} \subseteq A,$$

here $\{a\}$ is viewed as a set which contains a single element.

6.2 Operations on sets

Given two sets A, B.

Definition 6.5. The intersection of A and B is denoted by $A \cap B$. We have

$$A \cap B = \{x \,|\, x \in A \text{ and } x \in B\}.$$

A and B are said to be disjoint if $A \cap B = \emptyset$.
The union of A and B is denoted by $A \cup B$. We have

$$A \cup B = \{x \,|\, x \in A \text{ or } B\}.$$

We can also form a set of elements which lie in A but not B. This is called the difference of A and B, denoted as $A - B$. Thus

$$A - B = \{x \,|\, x \in A \text{ and } x \notin B\}.$$

We call use Venn diagram to illustrate the above operations. See page 68 of the textbook.

Example 6.2.1. *Given any two sets A and B, the three sets $A \cap B$, $A - B$ and $B - A$ are pairwise disjoint (i.e. each pair of these sets is disjoint) and*

$$A \cup B = (A \cap B) \cup (A - B) \cup (B - A).$$

6.3 The power set

The power set is a more complected way of constructing sets from one set.

Definition 6.6. The *power set* of a set X is defined as the set of all subsets of the set X, denoted as $\mathcal{P}(X)$.

Thus $A \in \mathcal{P}(X)$ is an alternative way of writing $A \subseteq X$.
We have

$$\emptyset \in \mathcal{P}(X), \quad \text{and} \quad X \in \mathcal{P}(X).$$

Example 6.3.1. *If $X = \{a, b\}$, then*

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

It is often the case that all the sets we are considering are subsets of a fixed set. We refer to this largest set as the *universal set*.

Definition 6.7. Suppose U is a universal set and $A \subseteq U$. Then the complement of A in U is defined as

$$A^c := U - A.$$

Here we can also write $A, A^c \in \mathcal{P}(U)$.

Theorem 6.8. *Let A, B, C be subsets of a set U. Then the following identities hold:*

(i) Associativity:

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C.$$

(ii) Commutativity:

$$A \cup B = B \cup A, \quad A \cap B = B \cap A.$$

(iii) Distributivity:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

(iv) De Morgan laws:

$$(A \cup B)^c = A^c \cap B^c, \quad (A \cap B)^c = A^c \cup B^c.$$

(v) Complementation:

$$A \cup A^c = U, \quad A \cap A^c = \emptyset.$$

(vi) Double complement:

$$(A^c)^c = A.$$

Proof. (of $(A \cup B)^c = A^c \cap B^c$. In the textbook one of the distributive law is proved. Please read it.) (This is like showing "equivalence $\Longleftrightarrow$": we prove "$=$" from two directions.)

Proof of "$\subseteq$": Suppose $x \in (A \cup B)^c$. Then $x \notin (A \cup B)$ and so $x \notin A$ and $x \notin B$. $x \notin A$ implies that $x \in A^c$ and $x \notin B$ implies that $x \in B^c$. Therefore we get $x \in A^c \cap B^c$.

Proof of "$\supseteq$": Suppose $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$. We get $x \notin A$ and $x \notin B$, and so $x \notin A \cup B$ which implies that $x \in (A \cup B)^c$. □

Proposition 6.9. *Show*

$$(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D).$$

Proof. Again here we are asked to prove an equality of sets. In the following, we apply Proposition 6.9 and show the two directions at the same time.

First let us view $A \cup B$ as one single set and apply the distributivity law:

$$(A \cup B) \cap (C \cup D) = ((A \cup B) \cap C) \cup ((A \cup B) \cap D).$$

By distributivity again

$$((A \cup B) \cap C) = (A \cap C) \cup (B \cap C),$$
$$((A \cup B) \cap D) = (A \cap D) \cup (B \cap D).$$

The associativity of the union operation implies that

$$\begin{aligned}(A \cup B) \cap (C \cup D) &= (A \cap C) \cup (B \cap C) \cup (A \cap D) \cup (B \cap D) \\ &= (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D).\end{aligned}$$

□

6.4 Cartesian product of two sets

Cartesian is one way to construct a set from two set.

Definition 6.10. Given sets X, Y, the Cartesian product of X, Y, denoted by $X \times Y$, is the set of all ordered pairs (x, y) where $x \in X$ and $y \in Y$. Thus

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

We say that the ordered pair (x, y) has coordinates x and y.

Example 6.4.1. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ *is the familiar* 2*-dimensional Euclidean space.*

$\mathbb{R}^d = \mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}$ *is the* d*-dimensional Euclidean plane.*

Proposition 6.11. *For all sets* A, B, C *and* D *the following hold:*

(i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$*;*

(ii) $A \times (B \cap C) = (A \times C) \cap (A \times C)$;

(iii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;

(iv) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Proof. (of part (iii), the textbook proved (ii).) A proof that two sets are equal requires us to prove two inclusions. In this case we can do them together as follows.

$$\begin{aligned}
(x, y) \in (A \times B) \cap (C \times D) &\iff (x, y) \in (A \times B) \text{ and } (x, y) \in (C \times D) \\
&\iff x \in A, y \in B \text{ and } x \in C, y \in D \\
&\iff x \in A \cap C \text{ and } y \in B \cap D \\
&\iff x \in A \cap C \text{ and } y \in B \cap D \\
&\iff (x, y) \in (A \cap C) \times (B \cap D).
\end{aligned}$$

□

7 Quantifiers

In this section we consider a set of statements $P(a)$ with a single free variable a taking values in a set A. Recall that $P(a)$ is called a predicate. The statement that all predicates $P(a)$ for $a \in A$ are true is called a *universal statement*.

Next we introduce two notations:

Definition 7.1. The notation $\forall a \in A, P(a)$ means: for each (or for any, for all) $a \in A$, $P(a)$ is true. ($\forall$ is called the *universal quantifier symbol*.)

The notation $\exists a \in A, P(a)$ means there exists (at least) one $a \in A$ such that $P(a)$ is true. ($\exists$ is called the *existential quantifier symbol*. It reads: "there exists", "for some" etc.)

7.1 Proving statements involving quantifiers

Example 7.1.1. *Prove* $\exists n \in \mathbb{Z}^+$, $2n + 1$ *is a prime number.*

Proof. Let $n = 3$ and then $n \in \mathbb{Z}^+$. We find that $2n + 1 = 7$ is a prime number. □

Example 7.1.2. *For integers* n*, if* n *is even then* n^2 *is even.*

This is a universal implication: $\forall n \in \mathbb{Z}$ etc. The hypothesis that n is even is an existence statement, because n is even is the same as $\exists q \in \mathbb{Z}$ such that $n = 2q$.

Proof. Since n is even, $\exists q \in \mathbb{Z}$ such that $n = 2q$. Then $n^2 = (2q)^2 = 2(2q^2)$ which is again even. □

Example 7.1.3. *To disprove the statement* $\forall x \in \mathbb{R}, x \leq 10^{10}$.

Proof. Let $x = 10^{10} + 1$. Then $x \in \mathbb{R}$ and $x > 10^{10}$. $\square$

Here in the example, we are asked to prove:

$$\exists a \in A, \text{ not } P(a).$$

We gave a counterexample as a proof. This is often called *disproof by counterexample* to $P(a)$.

7.2 Predicates involving more than one variable

Let $P(a, b)$ be a predicate involving two free variables $a \in A$, $b \in B$. Then there are several ways to form a proposition.

Example 7.2.1. $\forall a, b \in \mathbb{R}^+$, $a < b \implies a^2 < b^2$.

Here in the examples, "$\forall a, b \in A$" is a shorthand for "$\forall a \in A, \forall b \in A$" and similarly for "$\exists$".

Example 7.2.2. *It is not true that* $\exists m, n \in \mathbb{Z}$, $14m + 20n = 9$.

Statements might also involve both quantifiers:

Example 7.2.3. $\forall \epsilon \in \mathbb{R}^+$, $\exists N \in \mathbb{R}^+$ *such that* $\frac{1}{N} < \epsilon$.

Proof. Given any $\epsilon > 0$, we can pick $N = \frac{1}{\epsilon} + 1$. Then

$$\frac{1}{N} = \frac{1}{\frac{1}{\epsilon} + 1} = \frac{\epsilon}{1 + \epsilon} < \epsilon.$$

$\square$

Example 7.2.4. $\exists N > 0$, $\forall \epsilon \in \mathbb{R}^+$, $N > \frac{2+\epsilon}{1+\epsilon}$.

Proof. Let us pick $N = 2$. Then

$$2 > \frac{2 + \epsilon}{1 + \epsilon}$$

is true because it is equivalent to

$$2(1 + \epsilon) > 2 + \epsilon \iff \epsilon > 0.$$

$\square$

Use quantifiers to define limit.

Definition 7.2. Let $\{a_n,\ n \in \mathbb{Z}^+\}$ be a sequence of real numbers. Then $\lim_{n\to\infty} a_n = c$ if and only if

$$\forall \epsilon > 0,\ \exists N \in \mathbb{Z}^+ \text{ such that } \forall n \geq N, \quad |a_n - c| \leq \epsilon.$$

8 Functions

The notion of *function* is one of the most fundamental in mathematics.

Definition 8.1. Suppose that X and Y are sets. A *function* or *map* from X to Y is the assignment of a unique element of Y to each element of X. We write $f : X \to Y$. We denote the element $y \in Y$ assigned to $x \in X$ as $y = f(x)$. Here y or $f(x)$ is called the *value* or the *image* of x. The set X is called the *domain* and the set Y is called the *codomain*.

Example 8.0.1. *Suppose $X = \{a, b\}$ and $Y = \{0, 1\}$. Then a function f_1 from X to Y can be defined though*

$$f_1(a) = 0, \quad f_1(b) = 0.$$

There are precisely 4 functions from X to Y given as

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
a	*0*	*0*	*1*	*1*
b	*0*	*1*	*0*	*1*

Here f_1, f_4 are called *constant functions*, since the image of X is one fixed element of Y.

Of course a function can have the same set as its domain and codomain i.e. $X = Y$. For example the maps $f_i : X \to X$ for $i = 1, 2, 3, 4$ with $0, 1$ by a, b. Then f_3 becomes a function such that $f_3(a) = a$ and $f_3(b) = b$. This function is called the *identity function*. The definition of identity function is: $f : X \to X$ is given by $f(x) = x$ for all $x \in X$. We often write such functions as I_X.

We can use explicit formulae to define a function. But we need to make sure that we assign exactly one value to each element in the domain.

Example 8.0.2. *The modulus function $x \to |x|$ is defined from $\mathbb{R}$ to $\mathbb{R}^{\geq}$ as*

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x \leq 0. \end{cases}$$

The value of the function at 0 is given twice. Think about why this function is still well-defined?

The following function is not well defined on $\mathbb{R}$ to $\mathbb{R}$, but it is well-defined on $\mathbb{R}^+$ to $\mathbb{R}$ (or $\mathbb{R}^+$):

$$f(x) = 1 + \frac{1}{x}.$$

Definition 8.2. Two functions $f, g : X \to Y$ are *equal*, written $f = g$, if $f(x) = g(x)$ for all $x \in X$.

Definition 8.3. Suppose that $f : X \to Y$ is a function and A is a subset of X, i.e. $A \subseteq X$. Then we can define a function $g : A \to Y$ by setting $g(a) = f(a)$ for all $a \in A$. This function is called the *restriction* of f to A and is denoted as $g = f|A$.

8.1 Composition of functions

Definition 8.4. Given two functions $f : X \to Y$ and $g : Y \to Z$, the *composite* of f and g, denoted by $g \circ f$ is a map from $X \to Z$ defined by

$$g \circ f(x) = g(f(x)) \quad \text{for all } x \in X.$$

The order of f, g is important. In general when $g \circ f$ is well-defined, $f \circ g$ might not be well-defined (e.g. $Z \not\subseteq X$). Even if they are both well-defined (e.g. $X = Y = Z$), they are different functions in general. We can write the following to indicate the order:

$$g \circ f : X \xrightarrow{f} Y \xrightarrow{g} Z.$$

Example 8.1.1. *Let $f, g : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x + 1$ and $g(x) = x^2$. Then*

$$g \circ f(x) = (x+1)^2, \quad f \circ g(x) = x^2 + 1.$$

8.2 Sequences

By "sequence" (alone), we usually mean a sequence of real numbers. Below we use functions to define a sequence of elements in one set A.

Definition 8.5. A function $f : \mathbb{Z}^+ \to A$ is called a *sequence in A*.

In the following use quantifiers to give a rigorous definition of a sequence converging to 0.

Definition 8.6. Given a sequence $f : \mathbb{Z}^+ \to \mathbb{R}$ of real numbers, we say that the sequence is *null*, written $\lim_{n\to\infty} f(n) = 0$, when

$$\forall \epsilon \in \mathbb{R}^+, \exists N \in \mathbb{Z}^+ \text{ such that } \forall n \geq N, \text{ we have } |f(n)| < \epsilon.$$

Example 8.2.1. *The sequence $n \to \frac{1}{\sqrt{n}}$ is null.*

Constructing a proof. By the definition, we are required to show the that sequence converges to 0 i.e.

$$\forall \epsilon \in \mathbb{R}^+, \exists N \in \mathbb{Z}^+ \text{ such that } (n \geq N \implies |f(n)| < \epsilon).$$

The key point is, after fixing $\epsilon > 0$, to find out the value of N.

We study for what n, $|f(n)| < \epsilon$. Notice

$$\frac{1}{\sqrt{n}} < \epsilon \iff \frac{1}{n} < \epsilon^2 \iff n > \frac{1}{\epsilon^2}.$$

Hence we only need to select N to be one integer which is greater than $\frac{1}{\epsilon^2}$.

Proof. For any positive ϵ, let us take N be the smallest positive integer which $> \frac{1}{\epsilon^2}$. Then $n \geq N$ implies that $n \geq N > \frac{1}{\epsilon^2}$. So

$$\frac{1}{\sqrt{n}} < \epsilon$$

as required. $\square$

8.3 The image and the graph of a function

Definition 8.7. Given a function $f : X \to Y$, the *image* of f, denoted as Im f is defined as

$$\text{Im } f = \{f(x) \,|\, x \in X\}.$$

For any $y \in Y$, a pre-image of y is an element $x \in X$ such that $y = f(x)$. We also often call the following set the pre-image of y

$$\{x \in X \,|\, f(x) = y.\}$$

Hence the image of f is a subset of the codomain Y. The pre-image of y of f is a subset of X.

Definition 8.8. Suppose that $f : X \to Y$ is a function. The *graph* of f is defined as

$$G_f = \{(x, f(x)) \in X \times Y\}.$$

Hence the graph of f is a subset of the Cartesian product of $X \times Y$.

In the case that $X = Y = \mathbb{R}$, this definition of the graph of a function is the same as we have seen before.

Example 8.3.1. *Find the graph of $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$.*

Find the graph of f_1 in Example 8.0.1.

9 Properties of functions

9.1 Injections, surjections and bijections

Definition 9.1. Let X, Y be two sets. Suppose $f : X \to Y$ is a function.

(i) If $\forall x_1, x_2 \in X$ and $x_1 \neq x_2$, we have $f(x_1) \neq f(x_2)$, then we say that the function f is *injective* or *one-to-one*.

(ii) If $\forall y \in Y$, we can find $x \in X$ such that $f(x) = y$, then f is *surjective* or *onto*.

(iii) If f is both an injection (f is injective) and a surjection (f is surjective), then we say that it is *bijection* or that it is *bijective* or *one-to-one and onto*.

Example 9.1.1. *Show $f_1 : \mathbb{R} \to \mathbb{R}$ is bijective, where $f_1(x) = x + 1$. Show $f_2 : \mathbb{R} \to \mathbb{R}^+$ is bijective, where $f_2(x) = e^x$.*

Proof. Let us only prove for f_2. First we show that f_2 is injective. Take any two different real numbers x_1, x_2. Then $e^{x_1} \neq e^{x_2}$ and so it is injective. Next we show that f_2 is surjective. Fix any $y \in \mathbb{R}^+$. Let $x = \ln y$ and then $e^x = e^{\ln y} = y$. So f_2 is surjective. In all, it is a bijection. $\square$

For a function $f : X \to Y$, given an element $y \in Y$, recall that a *pre-image* of y is an element of $x \in X$ such that $y = f(x)$.

So f is an injection if and only if every $y \in Y$ has at most one pre-image; f is a surjection if and only if every $y \in Y$ has at least one pre-image.

Remark 9.2. Recall that the image of $f : X \to Y$ is defined as

$$\text{Im } f = \{f(x) \,|\, x \in X\}.$$

Hence we can convert f into a surjection by changing it codomain from Y to Im $f \subseteq Y$.

Example 9.1.2. *To determine whether the function $f : \mathbb{R}^+ \to \{x \geq 1\}$ given by $f(x) = 4x^2 - 4x + 2$ is injective, surjective or bijective.*

Solution. Notice that $y = f(x)$ is equivalent to

$$y = 4x^2 - 4x + 2 \Longleftrightarrow y = (2x-1)^2 + 1 \Longleftrightarrow x = \frac{(1 \pm \sqrt{y-1})}{2}.$$

For any y in the codomain, we have $y \geq 1$ and then $x = \frac{(1\pm\sqrt{y-1})}{2}$ are its pre-image. Thus f is surjective. However it is not injective since for all $y > 1$, there are two pre-images x. And the function is not bijective. □

9.2 Bijections and inverses

Definition 9.3. A function $f : X \to Y$ is called *invertible* if there exists a function $g : Y \to X$ such that

$$y = f(x) \Longleftrightarrow x = g(y)$$

for all $x \in X$ and $y \in Y$. In this case, we call g an *inverse (function)* of f and write $g = f^{-1}$.

Remark 9.4. If $g = f^{-1}$, then $f = g^{-1}$.

Theorem 9.5. *Let $f : X \to Y$. Then f is invertible if and only if it is a bijection. Furtheremore, if f is invertible, its inverse function is unique.*

Intuitively the result is straightforward. Let me present it below demonstrating that how a rigorous proof often looks like.

Proof. The first statement is an equivalence. We need to prove two directions.

(a) "f invertible $\implies$ f bijective": Suppose f is invertible, and then let us write its inverse as g.

Below we show that f is injective. Take any $x_1, x_2 \in X$. We only need to show that

$$f(x_1) = f(x_2) \implies x_1 = x_2.$$

(Compare this with the definition. Here we used that $A \implies B$ is the same as $(not\, B) \implies (not\, A)$.) Since $f(x_1) = f(x_2)$, then $g(f(x_1)) = g(f(x_2))$. Since $g = f^{-1}$, this implies that $x_1 = x_2$.

For surjectivity suppose $y \in Y$. Take $x = g(y) \in X$. Then

$$f(x) = f(g(y)) = y$$

which implies that f is also surjective. In all f is a bijection.

(b) "f bijective $\implies$ f invertible": Suppose that f is bijective. To show that it is invertible we need to construct a function $g : Y \to X$ such that $g = f^{-1}$. For any $y \in Y$, since f is surjective, there is a unique $x \in X$ such that $f(x) = y$. Then we define $g(y) = x$. By this definition we have for any $x \in X$, $y \in Y$

$$y = f(x) \iff x = g(y)$$

and so this function g is the inverse of f.

(c) "f invertible $\implies$ unique inverse": Suppose f has two inverse functions g_1, g_2. We need to show that $g_1 = g_2$. To do this we pick any $y \in Y$ and it suffices to show that $g_1(y) = g_2(y)$. Let us write $x_1 = g_1(y)$ and $x_2 = g_2(y)$. Then

$$f(x_1) = f(g_1(y)) = y = f(g_2(y)) = f(x_2).$$

Since f is bijective, this shows that we must have $x_1 = x_2$ which concludes part (c).

□

Example 9.2.1. *The function* $\sin : \mathbb{R} \to \mathbb{R}$ *is neither injective nor surjective. However notice the image of* $\sin$ *function is* $[-1, 1]$*, and so* $\sin : \mathbb{R} \to [-1, 1]$ *is surjective. But it is not injective.*

The function $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ *is a bijection.*

Remark 9.6. Once we change the domain or the codomain of a function, we view this function as a different one. However with a slight abuse of notation, people sometimes use the same symbol, for example $\sin$ in the above example.

Remark 9.7. By this example, we know that $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ has an inverse

$$\sin^{-1} \text{ (or arcsin) } : [-1, 1] \to [-\frac{\pi}{2}, \frac{\pi}{2}].$$

In making this definition we had to choose a subset of $\mathbb{R}$ on which $\sin$ is a bijection. Notice that the choice $[-\frac{\pi}{2}, \frac{\pi}{2}]$ is not unique. Here, with this choice, $\sin^{-1}$ is called the *principal value* of the inverse.

In the same way, we can obtain

$$\cos^{-1} : [-1, 1] \to [0, \pi],$$

and

$$\tan^{-1} : \mathbb{R} \to (-\frac{\pi}{2}, \frac{\pi}{2}).$$

Remark 9.8. So far, the bijections we gave satisfy that: if the domain is an open (close) set, then the codomain is also an open (close) set. Can you construct a function $f : (0, 1) \to [0, 1]$ such that f has an inverse?

To end this subsection, let me present one proposition. I refer the readers to Proposition 9.2.5 in the book for the proof.

Proposition 9.9. *The functions $f : X \to Y$ and $g : Y \to X$ are inverses of each other if and only if*

$$g \circ f = I_X \quad \text{and } f \circ g = I_Y.$$

Here $\circ$ is the composite operator, I_X, I_Y are identity functions on X, Y.

9.3 Functions and subsets

We can extend the definition of a function $f : X \to Y$ to $f : \mathcal{P}(X) \to \mathcal{P}(Y)$. And then f^{-1} is well-defined without requiring f to be bijective.

Definition 9.10. Suppose that $f : X \to Y$ is a function.

(i) The function $\overrightarrow{f} : \mathcal{P}(X) \to \mathcal{P}(Y)$ is defined by

$$\overrightarrow{f}(A) = \{f(x) \mid x \in A\}$$

for $A \in \mathcal{P}(X)$.

(ii) The function $\overleftarrow{f} : \mathcal{P}(Y) \to \mathcal{P}(X)$ is defined by

$$\overleftarrow{f}(B) = \{x \in X \mid f(x) \in B\}$$

for $B \in \mathcal{P}(Y)$.

Remark 9.11. It can be seen that $\overrightarrow{f}, \overleftarrow{f}$ are really extensions of f, f^{-1}. Because for example, $f(x) = y$ is the same as $\overrightarrow{f}(\{x\}) = \{y\}$ and if f is invertible, $f^{-1}(y) = x$ is the same as $\overleftarrow{f}(\{y\}) = \{x\}$. While if f is not a injection, $\overleftarrow{f}(\{y\})$ will not be a singleton subset of Y. Think about what happens if f is not a surjection?

The notations $\overrightarrow{f}, \overleftarrow{f}$ are non-standard. Most mathematicians denote $\overrightarrow{f}$ simply by f and denote $\overleftarrow{f}$ by f^{-1}. In the words of the book, the is an example of how ambiguity can be better than pedantry. However we will still use $\overrightarrow{f}, \overleftarrow{f}$, since it is potentially confusing to denote different functions by one symbol.

Example 9.3.1. *Let $f : X \to Y$ be a function and $B_1, B_2 \in \mathcal{P}(Y)$. Prove that*

$$B_1 \subseteq B_2 \implies \overleftarrow{f}(B_1) \subseteq \overleftarrow{f}(B_2).$$

Proof. By definition of $\overleftarrow{f}$, for $i = 1, 2$

$$x \in \overleftarrow{f}(B_i) \Longleftrightarrow f(x) \in B_i.$$

Assume $B_1 \subseteq B_2$. Now for any $x \in \overleftarrow{f}(B_1)$, $f(x) \in B_1$. Since $B_1 \subseteq B_2$, we have $f(x) \in B_2$ and then $x \in \overleftarrow{f}(B_2)$. We obtain

$$x \in \overleftarrow{f}(B_1) \implies x \in \overleftarrow{f}(B_2),$$

which implies the statement. □

Axiom 9.1. *(Peano) The set of positive integers $\mathbb{Z}^+$ is a set with a function $s : \mathbb{Z}^+ \to \mathbb{Z}^+$ and an element $1 \in \mathbb{Z}^+$ such that*

(i) s is an injection,

(ii) 1 is not in the image of s,

(iii) for $A \subseteq \mathbb{Z}^+$, if $1 \in A$ and $(n \in A) \implies s(n) \in A$, then $A = \mathbb{Z}^+$.

Remark 9.12. Once known the set is $\mathbb{Z}^+$, the the function s described in the above is the *successor function* and it is given by $s(n) = n + 1$.

With the choice of $s(n) = n + 1$, we can check that (i) holds i.e. s is an injection; (ii) holds i.e. $s(n) \geq 2$ for $n \in \mathbb{Z}^+$; (iii) if $1 \in A$, by the assumption $s(1) = 2 \in A$. By induction it can be shown that $A = \mathbb{Z}^+$. So for the normal $\mathbb{Z}^+$, the criteria (i)-(iii) hold.

However what is important here is that the Axiom is announcing that any set satisfying (i)-(iii) can be seen as a copy of $\mathbb{Z}^+$.

10 Counting finite sets

Counting is a very common acting in real life. Here we provide another way to think of counting in mathematics (we use bijection).

We start with a sequence of standard set

$$\mathbb{N}_n := \{1, 2, ..., n\}.$$

Definition 10.1. Given a set X, if there is a bijection $f : \mathbb{N}_n \to X$ then we say that the cardinality of X, or the number of elements in X, is n and write $|X| = n$. In particular $|\emptyset| = 0$.

For example the cardinality of

$$A = \{k \in \mathbb{Z} \,|\, 25 \leq k < 30\}$$

is 5. The cardinality of

$$A = \{k \in \mathbb{R} \,|\, 25 \leq k < 30\}$$

is infinity. However let me mention that, there are infinitely many different "infinite" that can be defined through bijection.

Proposition 10.2. *Suppose that $f : \mathbb{N}_m \to X$ and $g : \mathbb{N}_n \to X$ are bijections with the same codomain X. Then $m = n$. (But in general we don't have $f = g$.)*

The proposition is very important to our Definition 10.1. Imagine, if the proposition fails, then according to Definition 10.1, the cardinality of X can then be both n and m, which certainly does not make sense.

The proof of the proposition can be found in the textbook. The key idea is to use that 1. bijections have inverse functions. 2. the following lemma.

Lemma 10.3. *If there exists an injection $N_m \to N_n$, then $m \leq n$.*

Proof. Let us give a proof by induction on n.

Base case: $n = 1$. Suppose for contradiction that if $m > 1$ and we have $f : \mathbb{N}_m \to \mathbb{N}_1$ is an injection. Then $1, 2 \in \mathbb{N}_m$ and $f(1), f(2) \in \mathbb{N}_1 = \{1\}$. Thus we have $f(1) = f(2)$ which contradicts with the assumption that f is injective, and so $m = 1 \leq n$.

Inductive step: suppose for some $k \geq 1$, the result holds for $n = k$. We need to show the result for $n = k + 1$. We consider two cases:

(1) Suppose $f(i) < k + 1$ for all $i \in \mathbb{N}_m$. Then we can restrict the codomain of the function f from N_{k+1} to N_k. Then by inductive hypothesis, $m \leq k < k + 1$.

(2) On the other hand, suppose that $k + 1$ is a value of f, say $f(i_0) = k + 1$. By re-arranging $\mathbb{N}_m$, without loss of generality, we can assume that $i_0 = m$. By injectivity of f, $f(i) \leq k$ for $i \leq m - 1$. Hence if we define $f_1 : \mathbb{N}_{m-1} \to \mathbb{N}_k$ by

$$f_1(i) := f(i),$$

the function f_1 is an injection. By inductive hypothesis, $m-1 \leq k$ and therefore we get $m \leq k+1$ as required.

Conclusion: by induction on n, if $f : \mathbb{N}_m \to \mathbb{N}_n$ is an injection then $m \leq n$. □

Definition 10.4. Given a set X, if $|X| = n$ for some n, then we say the set is *finite*. Otherwise, we say that the set is *infinite*.

For example, natural numbers $\mathbb{N}$ is infinite, and real numbers $\mathbb{R}$ is also infinite.

10.1 Properties

Theorem 10.5. *Suppose that X and Y are disjoint finite sets. Then $X \cup Y$ is finite and*

$$|X \cup Y| = |X| + |Y|.$$

Proof. Let $|X| = n$ and $|Y| = m$. If one of n, m is 0, then one of X, Y is an empty set. And the statement holds automatically. So let us consider the case that $n, m \geq 1$.

We know there are bijections $f : \mathbb{N}_n \to X$ and $g : \mathbb{N}_m \to Y$. The goal is define a bijection $h : \mathbb{N}_{n+m} \to X \cup Y$. Let

$$h(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq n, \\ g(i-n) & \text{if } n+1 \leq i \leq n+m. \end{cases}$$

This this is indeed the bijection required. Because, injectivity follows from the injectivity of f, g and $X \cap Y =$; surjectivity follows from that f, g are surjective. $\square$

Theorem 10.6. *Suppose that X, Y are finite sets such that $|X| = n$ and $|Y| = m$. Then the Cartesian product of $X \times Y$ is a finite set and $|X \times Y| = mn$.*

We omit the proof.

Example 10.1.1. *The cardinality of $\mathbb{N}_9 \times \mathbb{N}_9$ is $9 \times 9 = 81$.*

The diagonal set in $\mathbb{N}_9 \times \mathbb{N}_9$ is

$$\{(x, x) \mid x \in \mathbb{N}_9\}.$$

We denote the set as $\Delta(\mathbb{N}_9)$ and then $|\Delta(\mathbb{N}_9)| = 9$.

What is the number of ordered pair of distinct positive integers no greater than 9? The answer is 36. One reason can be:

$$\frac{|\mathbb{N}_9 \times \mathbb{N}_9| - |\Delta(\mathbb{N}_9)|}{2} = \frac{81 - 9}{2} = 36.$$

Think about why.

The following proposition is often referred to as the inclusion-exclusion principle.

Proposition 10.7. *Suppose that X, Y are finite set. Then*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

More generally, Suppose X, Y, Z are finite sets. Then

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|.$$

Example 10.1.2. *At an international conference of 100 people, 80 speak English, 60 speak Spanish and 40 speak Chinese (any everyone present speaks at least one of these language). What is the maximum possible number of the people who can speak the three languages.*

Solution. Let X be the set of people who speak English, Y Spanish and Z Chinese. Then from the assumption

$$|X \cup Y \cup Z| = 100, \quad |X| = 80, \quad |Y| = 60, \quad |Z| = 40.$$

From the inclusion-exclusion principle,

$$100 = 80 + 60 + 40 - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|,$$

which simplifies to

$$|X \cap Y| + |X \cap Z| + |Y \cap Z| = 80 + |X \cap Y \cap Z|$$

The people who can speak the three languages are $X \cap Y \cap Z$. Since $|X \cap Y|, |X \cap Z|, |Y \cap Z| \geq |X \cap Y \cap Z|$, we have

$$80 + |X \cap Y \cap Z| \geq 3|X \cap Y \cap Z|.$$

So

$$|X \cap Y \cap Z| \leq 40.$$

The maximum number of people who can speak the three languages are 40. This can be obtained (why?).

$\square$

11 Properties of finite sets

11.1 The pigeonhole principle

The principle says: you want to put objects into holes. If you have more objects than you have holes, at least one hole must have multiple objects in it.

Theorem 11.1. *Suppose that $f : X \to Y$ is a function between non-empty finite sets such that $|X| > |Y|$. Then f is not an injection, i.e. there exists distinct elements $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.*

The proof can be constructed using Lemma 10.3.

Example 11.1.1. *In a party there are more than 366 people. Then there must be two people with birthdays in the same month and same date (probably different years).*

Theorem 11.2. *Suppose that $f : X \to Y$ is a function between non-empty finite sets such that $|X| < |Y|$. Then f is not a surjection.*

Proof. Suppose for contradiction that f is a surjection. Then $\overleftarrow{f} : \mathcal{P}(Y) \to \mathcal{P}(X)$ satisfies that for any $y \in Y$, $\overleftarrow{f}(\{y\}) \neq \emptyset$ i.e. $|\overleftarrow{f}(\{y\})| \geq 1$. Also for any y_1, y_2,

$$\overleftarrow{f}(\{y_1\}) \cap \overleftarrow{f}(\{y_2\}) = \emptyset.$$

Therefore

$$|X| = |\cup_{y \in Y} \overleftarrow{f}(\{y\})| = \Sigma_{y \in Y} |\overleftarrow{f}(\{y\})| \geq \Sigma_{y \in Y} 1 = |Y|,$$

which is a contradiction. □

Theorem 11.3. *Suppose that X, Y are non-empty finite sets of the same cardinality. Then a function $X \to Y$ is an injection if and only if it is a surjection.*

Proof. Suppose the function $f : X \to Y$ is an injection. Suppose for contradiction that f is not a surjection. Let us write the codomain of f as Y', and then $|Y'| < |Y| = |X|$. We know that $f : X \to Y'$ is still an injection which contradicts with Theorem 11.1.

Next suppose the function $f : X \to Y$ is a surjection but not an injection. Then there exist distinct $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. We consider the restricting map $f : X \backslash \{x_2\} \to Y$ which is still a surjection. Notice that $|X \backslash \{x_2\}| < |X| = Y$. Thus we get a contradiction to Theorem 11.2. □

This theorem is not true if X, Y are not finite sets. For example $X = Y = \mathbb{Z}^+$, and $f : X \to Y$ is defined by

$$f(n) = n + 1.$$

Then f is an injection but it is not a surjection.

Therefore it is not hard to believe that finite sets have many nice property that infinite sets do not have. The following shows that finite non-empty set of real numbers has a greatest and a smallest element.

Definition 11.4. Let A be a set of real numbers. Then b is a minimum element of A or $b = \min A$ when (i)$b \in A$, (ii) $a \in A \implies b \leq a$.

Similarly c is a maximum element of A or $c = \max A$ when (i)$c \in A$, (ii) $a \in A \implies c \geq a$.

Proposition 11.5. *If A is a finite non-empty set of real numbers, A has a minimum element and a maximum element.*

The textbook provides us a proof by induction on n. Think about, how you would prove the proposition.

11.2 Common divisor

Now we discuss the *common divisor*.

Recall that we say a non-zero integer d divides a when there is an integer q such that $a = dq$. In this case, we say that d is a *divisor* or a *factor* of a. Alternatively we say that a is a multiple of d.

Proposition 11.6. *Every non-zero integer divides* 0.

Let us write the set of divisors of a as,

$$D(a) := \{n \in \mathbb{Z} \,|\, n \text{ divides } a\}.$$

For example,

$$D(-12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}.$$

For any $a \in \mathbb{Z}$, $D(a)$ is a finite set and

$$\min D(a) = -|a|, \quad \max D(a) = |a|.$$

Now consider two integers a, b, not both zero, then the set of *common divisors* of a, b is given by $D(a) \cap D(b)$. Notice that

$$\pm 1 \in D(a) \cap D(b).$$

We define the largest number of $D(a) \cap D(b)$ as the *greatest common divisor* or *highest common factor* of a and b. And we denote it as (a, b) or $\gcd(a, b)$.

Example 11.2.1. *Find* $\gcd(-12, 28)$.

Solution. Since

$$D(-12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

and

$$D(28) = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28\},$$

then

$$\gcd(-12, 28) = \max\{D(-12) \cap D(28)\} = \max\{\pm 1, \pm 2, \pm 4\} = 4.$$

□

Definition 11.7. Two integers a and b, not both zero, are called *coprime* or *relatively prime* when $(a, b) = 1$.

Definition 11.8. A positive number n is said to be *prime* when $n > 1$ and the only positive divisor of n are 1 and n.

12 Counting functions and subsets

12.1 Counting functions

Let us count the number of functions from X to Y where X, Y are finite sets.

Example 12.1.1. *Let $X = \{a, b, c\}$ and $Y = \{d, e\}$. In order to define a function $f : X \to Y$, we must list the elements $f(a), f(b), f(c)$. Since each of them has two choices: either d or e, there are $2 \times 2 \times 2 = 8$ ways. So altogether we have 8 functions from X to Y.*

In general, we have

Proposition 12.1. *Suppose that X, Y are non-empty finite sets with $|X| = m$ and $|Y| = n$. Then the number of functions $X \to Y$ is given by n^m.*

Definition 12.2. Given sets X, Y, we denote the set of functions from X to Y by $\text{Fun}(X, Y)$.

Proposition 12.3. *Let X, Y as in Proposition 12.1. Then the number of injections $X \to Y$ is given by $n(n-1)...(n-m+1)$. Let us denote the injections as Inj(X, Y).*

Notice if $n \geq m - 1$, $n(n-1)...(n-m+1) = 0$. This means that if $n < m$, there is no injection from X to Y.

Proof. The proof is by induction on m.

Base case: For $m = 1$ suppose that $X = \{x_1\}$ and Y is any finite set. Then any function $X \to Y$ is a injection and a function is determined by the value of $f(x_1)$. Thus $|\text{Inj}(X, Y)| = |Y| = n$ as required.

Inductive step: Suppose that, for some $k \geq 1$, the result holds for $m = k$ and all positive n and the goal is to deduce the result for $m = k + 1$. Let X be a set of $k + 1$ elements:

$$X = \{x_1, ..., x_{k+1}\},$$

and Y be a set of n elements:

$$Y = \{y_1, ..., y_n\}.$$

Then we can rewrite the set of injections as

$$\text{Inj}(X, Y) = \bigcup_{i=1}^{n} \{f \in \text{Inj}(X, Y) \mid f(x_{k+1}) = y_i\},$$

a disjoint union. For each set, we can view the elements (functions) as those from $X - \{x_{k+1}\}$ to $Y - \{y_i\}$. In other words, we have the bijection

$$\{f \in \text{Inj}(X, Y) \mid f(x_{k+1}) = y_i\} \longleftrightarrow \text{Inj}(X - \{x_{k+1}\}, Y - \{y_i\}).$$

The latter are injections from a set of k elements to a set of $n - 1$ elements. Then, by inductive hypothesis

$$\begin{aligned} |\{f \in \text{Inj}(X, Y) \mid f(x_{k+1}) = y_i\}| &= |\text{Inj}(X - \{x_{k+1}\}, Y - \{y_i\})| \\ &= (n-1)(n-2)...((n-1) - k + 1) \\ &= (n-1)(n-2)...(n-k). \end{aligned}$$

Hence, by the addition principle,

$$\begin{aligned} |\text{Inj}(X, Y)| &= \Sigma_{i=1}^{n} |\{f \in \text{Inj}(X, Y) \mid f(x_{k+1}) = y_i\}| \\ &= n \times (n-1)(n-2)...(n-k) \end{aligned}$$

as required and so completing the inductive step.

Conclusion: Hence, by induction on m, the results holds for all positive n, m. □

Definition 12.4. Given a set X, a bijection $X \to X$ is called a *permutation* of the set X.

And then from the above proposition, we know that for a set X of cardinality n, the number of permutations of X is given by $n!$.

12.2 Counting sets of subsets

Example 12.2.1. *Consider $X = \{1, 2, 3\}$. Recall that $\mathcal{P}(X)$ denotes the power set of X. Then*

$$|\mathcal{P}(X)| = |\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}| = 8 = 2^3.$$

Proposition 12.5. *Suppose that X is a set of cardinality n. Then*

$$|\mathcal{P}(X)| = 2^{|X|}.$$

Definition 12.6. For any set X and $A \subseteq X$, the *characteristic function* $\chi_A : X \to \{0, 1\}$ is defined by

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \notin A, \\ 1 & \text{if } x \in A. \end{cases}$$

Lemma 12.7. *The function $\mathcal{P}(X) \to$ Fun$(X, \{0, 1\})$ given by $A \to \chi_A$ is a bijection.*

Proof. The inverse function is given by

$$\chi \to \{x \in X \mid \chi(x) = 1\}.$$

Note that the above also equals $\chi \to \overleftarrow{\chi}(1)$. □

Proof. (of Proposition 12.5) From the previous Lemma

$$|\mathcal{P}(X)| = |\text{Fun}(X, \{0,1\})|.$$

It follows from Proposition 12.1 that $|\mathcal{P}(X)| = 2^{|X|}$.

□

Definition 12.8. Given a set X and a non-negative integer r, an $r-$subset of X is a subset $A \subseteq X$ of cardinality r. We denote the set of r-subset by $\mathcal{P}_r(X)$ i.e.

$$\mathcal{P}_r(X) = \{A \subseteq X \mid |A| = r\}.$$

We define the *binomial coefficient* or *binomial number* $\binom{n}{r}$ (read "n choose r") to be the cardinality of the set $\mathcal{P}_r(X)$ when $|X| = n$.

$\binom{n}{r}$ equals the number of ways that we can choose r objects from n projects without considering the order.

Example 12.2.2. *Compute* $\binom{4}{3}$.

Solution. Suppose $X = \{1,2,3,4\}$, then

$$\mathcal{P}_3(X) = \{\{2,3,4\}, \{1,3,4\}, \{1,2,4\}, \{1,2,3\}\}.$$

Thus $\binom{4}{3} = 4$. □

Proposition 12.9. *For n, r non-negative integers*

(i) $\binom{n}{r} = 0$ *if* $r > n$,

(ii) $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{n} = 1$,

(iii) $\binom{n}{r} = \binom{n}{n-r}$ *for* $0 \leq r \leq n$.

Proof. Suppose X is a set with n elements.

(i) X has no subsets of cardinality greater than n.

(ii) Since $\mathcal{P}_0(X) = \{\emptyset\}$, $\mathcal{P}_n(X) = \{X\}$, $\binom{n}{0} = 1, \binom{n}{n} = 1$. Considering subsets with 1 element, $\mathcal{P}_1(X)$ has n elements.

(iii) There is a bijection $\mathcal{P}_r(X) \to \mathcal{P}_{n-r}(X)$. For any $A \in \mathcal{P}_r(X)$, A is a subset of cardinality r. We map it to A^c which is then a subset of cardinality $n-r$. Hence $\binom{n}{r} = \binom{n}{n-r}$. □

Proposition 12.10. *(Pascal's rule) For positive integers n, r such that $1 \leq r \leq n$*

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Proof. Here let us give a combinatorial argument.

Recall that $\binom{n}{r}$ equals the number of subsets with r elements from a set X with n elements. Suppose one particular element is uniquely labeled x in X.

Every subset of X either contains x or not. To construct a subset of r elements containing x, we need to choose $r-1$ elements from the remaining $n-1$ elements in X. Thus there are $\binom{n-1}{r-1}$ such subsets. For subsets not containing x, we choose r elements from the remaining $n-1$ elements. The total number of subsets is the sum of the above two. We have

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

□

Remark 12.11. The proposition has been first discovered in the eleventh century in China. It is referred to as Yanghui triangle:

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

Theorem 12.12. *For non-negative integers n, r such that $r \leq n$,*

$$\binom{n}{r} = \frac{n(n-1)...(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}.$$

Proof. The textbook uses a proof by induction. Let us sketch a combinatorial argument.

Recall that $\binom{n}{r}$ equals the number of subsets with r elements from a set X with n elements. If we randomly pick elements one by one from X for r times, we get a subset of cardinality r. The first time we pick an element, we have n choices. The second time we pick an element, we have $n-1$ choices... Thus to pick r times, altogether the number of choices we have is

$$n(n-1)(n-2)...(n-r+1).$$

Now consider a r-subset of X: $\{x_1, x_2, ..., x_r\}$. Each permutation of it provides a way of picking r elements one by one from X. We have proved that the a set with cardinality r, there are $r!$ permutations. Therefore

$$\binom{n}{r} \times r! = n(n-1)(n-2)...(n-r+1)$$

and we proved the theorem. □

Theorem 12.13. *(Binomial Theorem) For any real numbers a, b and a non-negative integers n*

$$(a+b)^n = \Sigma_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{2}$$

Special Cases of binomial theorem were known since at least the 4th century BC mentioned by Greek mathematician Euclid for exponent 2. The earliest known reference to this problem is by the Indian Iyricist Pingala in 200 BC.

Example 12.2.3.

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 3ab^4 + b^4 ...$$

Proof. (of Theorem 12.13) The textbook uses a proof by induction. Here we present a combinatorial argument.

Expanding $(a+b)^n$ yields the sum of the 2^n products of the form $e_1 e_2 ... e_n$ where each e_i is a or b. Rearranging factors shows that each product equals $a^{n-k}b^k$ for some $0 \leq k \leq n$. For each k, the number of copies $a^{n-k}b^k$ in the expansion is the same as the number of $n-$character a, b strings having b exactly k positions. This number is then the same as picking b for k times in the n brackets which equals by definition $\binom{n}{k}$. □

Corollary 12.14. *If picking $a = b = 1$ in (2), we get*

$$2^n = \Sigma_{k=0}^{n} \binom{n}{k}.$$

13 Number systems

We have different number systems, for example: natural numbers, integers, rational numbers, real numbers, complex numbers etc. A brief discussion about these numbers (the history of different numbers' discovery) can be found in the beginning of Chapter 13 in the textbook.

13.1 The rational numbers

Definition 13.1. We will use *fraction* to denote an expression of the form $\frac{a}{b}$ where a, b are integers and $b \neq 0$; a is the *numerator* and b the *denominator* of the fraction.

Given integers a and non-zero b, we say that the fraction $\frac{a}{b}$ represents the *rational number* q which satisfies $bq = a$. The set of rational numbers is denoted by the symbol $\mathbb{Q}$.

Proposition 13.2. *Two fractions $\frac{a}{b}$, $\frac{c}{d}$ represent the same rational number q, if and only if $ad = bc$.*

Definition 13.3. The fraction $\frac{a}{b}$ is *in lowest terms* when b is positive and a and b are coprime.

Every rational number has a fraction representation in lowest terms and the representation is unique.

Definition 13.4. We define *sum* and *product* of two fractions by

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}.$$

Think about how we should define subtraction and division.

Proposition 13.5. *Addition and multiplication of rational numbers are well-defined by the above formulae.*

Before the proof, let me explain what is the problem in the proposition. This is because a rational number has (infinitely) many different fraction representations. We need to show that using different fractions for $\frac{a}{b}, \frac{c}{d}$, addition and multiplication defined leads to fractions representing the same rational number.

To be precise, we need to check for $\frac{a}{b}=\frac{a'}{b'}$, $\frac{c}{d}=\frac{c'}{d'}$, whether or not

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}, \quad \frac{a}{b}\times\frac{c}{d}=\frac{a'}{b'}\times\frac{c'}{d'}.$$

Proof. Let us only prove that addition is well-defined. Suppose $\frac{a}{b}=\frac{a'}{b'}$, $\frac{c}{d}=\frac{c'}{d'}$ and so

$$ab'=a'b, \quad cd'=c'd. \tag{3}$$

To show

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'},$$

by the formulae, it suffices to check that

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}.$$

We only need to show

$$(ad+bc)b'd'=(a'd'+b'c')bd.$$

In view of (3), this is certainly true. □

$\sqrt{2}$ is not a rational number.

Theorem 13.6. *There does not exist a rational number whose square is* 2.

A real number that is not rational is called a irrational number.

Proof. Suppose for contradiction that there is a rational number q such that $q^2=2$. Write q as a fraction in lowest terms, $q=\frac{a}{b}$, so that a, b are positive integers and $\gcd(a,b)=1$. Now

$$q^2=2 \implies \frac{a^2}{b^2}=2 \implies a^2=2b^2 \implies a^2 \text{ is even.}$$

Thus we obtain that a is also even and we can write $a=2a'$ for some integer a'. Then

$$a^2=2b^2 \implies 2a'^2=b^2 \implies b \text{ is even.}$$

Hence 2 divides both a and b which contradicts with $\gcd(a,b)=1$.

Hence there does not exist a rational number whose square is 2. □

There are a lot of irrational numbers (actually far more than rational numbers). For example: $e, \pi, \sqrt{5}, \sqrt{2+\sqrt{2}}$.

Determine whether a number is rational or not can be a very hard problem. It is not known yet that if

$$\pi \pm e,\ \pi e,\ \pi/e,\ 2^e,\ \pi^e,\ \pi^{\sqrt{2}},\ \ln \pi \ldots$$

are rational or not.

13.2 Real numbers and infinite decimals

In this section, we will discuss one criteria which can be used to distinguish rational numbers and irrational numbers.

We use *infinite decimals* to describe real numbers: every non-negative real number may be represented by an infinite decimal

$$a_0.\, a_1\, a_2\, a_3 \ldots a_i \ldots$$

where a_0 is a positive integer and $0 \leq a_i \leq 9$ for $i \geq 1$.

For example,

$$\frac{1}{2} = 0.5, \quad \frac{1}{3} = 0.333333..., \quad \pi = 3.1415926535...$$

If we only have a finite decimal $a_0.a_1a_2...a_n$, then it is a rational number. Because:

$$a_0.a_1a_2...a_n = (a_0a_1a_2...a_n)/(10^n) = \frac{a_0(10)^n + a_1(10)^{n-1} + ... + a_n}{10^n}.$$

So the set of finite decimals is a subset of the set of rational numbers.

Below we give the definition of infinite decimal representation of real numbers.

Definition 13.7. Given an infinite decimal $a_0.a_1a_2...a_i...$, we say that it represents a real number q, written $a = a_0.a_1a_2...a_i...$, when for each $n \in \mathbb{Z}^+$

$$a_0.a_1a_2...a_n \leq a \leq a_0.a_1a_2...a_n + \frac{1}{10^n}.$$

The intuitive idea of an infinite decimal is that finite parts of the decimal approximate the real number.

It is not hard to see that every real number has a infinite decimal representation, and any infinite decimal represents one real number. But it is not true that there is a one-to-one correspondence between infinite decimals and real numbers. In fact, two infinite decimals might lead to the same real number.

Example 13.2.1. *Let us consider which real number is represented by the infinite decimal* $0.99999...$ *each of whose entries after the decimal point is* 9.

The finite decimals $0.99...9$ *are certainly less than* 1*. Indeed,*

$$0.\underbrace{999...9}_{n} = \underbrace{999..9}_{n}/10^n = 1 - \frac{1}{10^n}.$$

Thus for $a = 0.9999...$*, we have for all* $n \in \mathbb{Z}^+$

$$1 - \frac{1}{10^n} \leq a \leq 1.$$

Then a *has to be* 1*. We get that*

$$0.9999... = 1.$$

An alternative way to see this is that $\frac{1}{3} = 0.3333....$ *Then* $1 = 3 \times \frac{1}{3} = a$*.*

Definition 13.8. A *repeating* or *recurring* decimal is decimal representation of a number whose digits are periodic (repeating its values at regular intervals) and the infinitely repeated portion is not zero.

We indicate the repeating block by placing a dot over the first and last digits in the block.

Example 13.2.2.

$$0.99999... = 0.\dot{9},$$

$$7.320008140081400814... = 7.320\dot{0}0814\dot{}.$$

Theorem 13.9. *A recurring infinite decimal is equal to a rational number.*

Instead of proving the theorem, let us write a concrete recurring decimal as a rational number below. The proof in general follows similarly.

Example 13.2.3. *To find the rational number* $12.79\dot{3}1\dot{7}$*.*

Solution. Let $x = 12.79\dot{3}1\dot{7}$. Then we can write

$$x = 12.79 + y \quad \text{where } y = 0.00\dot{3}1\dot{7}.$$

After multiplying y by 1000, we obtain

$$1000y = 3.17\dot{3}1\dot{7} = 3.17 + y.$$

Thus

$$y = \frac{3.17}{999} = \frac{317}{99900}$$

and

$$x = 12.79 + y = \frac{1278038}{99900}.$$

□

The converse of this theorem is also true. This means that rational numbers correspond precisely to the recurring decimals.

Theorem 13.10. *Every rational number can be written as a recurring infinite decimal.*

The proof will be given later (see Problems IV, Question 5).

14 Counting infinite sets

In chapter 10, we considered *finite* sets which are sets of finite carnality (including the empty set). In this section we consider sets with infinitely many elements, for example $\mathbb{N}$.

14.1 Denumerable sets

Definition 14.1. Two sets X, Y are *equipotent* if there is a bijection $X \to Y$.

Definition 14.2. A set X is said to be *denumerable* or *enumerable* if there is a bijection $\mathbb{Z}^+ \to X$. A set is *countable* if either it is finite or denumerable. A set is *uncountable* if it is not countable.

If the set X is denumerable then it is said to have cardinality $\aleph_0$.

Remark 14.3. Intuitively we understand denumerable sets as a set such that we can list all its element into a sequence. We will see below that there are (a lot of) sets (e.g. any set on $\mathbb{R}$ containing an interval) that we cannot list all its element into a sequence. We will call those sets uncountable.

Remark 14.4. The notation $\aleph$ uses the Hebrew letter aleph and "$\aleph$" reads "aleph null".

Example 14.1.1. *The set of natural number $\mathbb{N}$ is denumerable.*

Solution. Recall $\mathbb{N}$ contains all non-negative integers. The bijection from $\mathbb{Z}^+ \to \mathbb{N}$ is defined by $n \to n - 1$. $\square$

Example 14.1.2. *The set of all integers $\mathbb{Z}$ is denumerable, for a bijection $\mathbb{Z}^+ \to \mathbb{Z}$ can be defined by*

$$n \to \begin{cases} n/2 & \text{if } n \text{ is even}, \\ -(n-1)/2 & \text{if } n \text{ is odd}. \end{cases}$$

This gives the listing $\mathbb{Z} = \{0, 1, -1, 2, -2, ..., n, -n, ...\}$.

The set of perfect squares $X = \{n^2 \mid n \in \mathbb{N}\}$ is denumerable, for a bijection $n \to (n-1)^2$.

A Paradox.

Galileo Galilei observed the following paradox in his book in 1638. We can not say that: "the number" of elements of a set X strictly larger than "the number" of elements of a proper subset of X (if X contains infinitely many elements). Though this is true for finite sets.

To compare the size of two sets, we use bijections. The above example shows that the natural number N has the same cardinality with it subset: perfect squares $X = \{n^2 \mid n \in \mathbb{N}\}$.

In fact we have the following theorem:

Theorem 14.5. *(Dedekind) A set X is infinite if and only if it is equipotent to a proper subset of itself.*

Proof. If X is equipotent to a proper subset (say Y) of itself, suppose for contradction that X is a finite set. Since Y is a proper subset of X, $X - Y$ is non-empty. By Theorem 10.5, $|X| = |Y| + |X - Y| > |Y|$. However by the assumption we have a bijection from X to Y, and then $|X| = |Y|$ which is a contradiction.

For the other direction, let us suppose X is infinite and we construct a bijection from X to a proper subset Y of X.

Since X is infinite, we can take a infinite sequence of elements from X and let them be $A = \{a_1, a_2, a_3, ..., a_n...\}$. Now we define a bijection from X to $Y = X - \{a_1\}$ as follows:

$$f(x) = \begin{cases} a_{n+1} & \text{if } x = a_n \in A, \\ x & \text{if } x \notin A. \end{cases}$$

Hence X and the proper subset Y are equipotent.

□

Proposition 14.6. *Given a denumerable set X, a set Y is also denumerable if and only if it is equipotent to X.*

Lemma 14.7. *If there exists a injection from X to $\mathbb{Z}^+$, then X is countable.*

Proof. If X is a finite set, then it is countable and there is nothing to prove.

Suppose X is a infinite set. To prove it is denumerable, we need to construct a bijection $f : \mathbb{Z}^+ \to X$. Let us define $f(n)$ inductively as follows.

From the assumption, there is an injection $g : X \to \mathbb{Z}^+$. By restricting the codomain to the image of g, we get a bijection (let us still call it g):

$$g : X \to \text{Image}(g) \subseteq \mathbb{Z}^+.$$

Since X is infinite, Image(g) is also infinite. We know that the function $g^{-1} : \text{Image}(g) \to X$ is a bijection.

Now we define $f(1)$ to be $g^{-1}(a_1)$ where a_1 is the least element of the set Image(g) (the least element exists because Image(g) is a subset of positive integers). Suppose for induction that $f(j)$ is defined for $1 \leq j \leq k$ and $f(j) = a_j$ where $a_j \in \text{Image}(g)$. Let us define $f(k+1)$. Let a_{k+1} be the least of element of

$$\{a \in \text{Image}(g) \mid a > a_k\},$$

and then we define $f(k+1)$ to be $g^{-1}(a_{k+1})$.

This function f is injective since $\{a_k\}_k$ is a strictly increasing sequence and (since g^{-1} is a bijection from Image(g) to X) $g^{-1}(a_i) \neq g^{-1}(a_j)$ if $a_i \neq a_j$.

The function f is also surjective because for any $x \in X$, there exists $a \in \text{Image}(g)$ such that $g^{-1}(a) = x$. By the way we select the sequence a_j, there is exactly $i \in \mathbb{Z}^+$ such that $a_i = a$. Then $f(i) = g^{-1}(a_i) = x$.

Hence X is denumerable.

□

Proposition 14.8. *If A and B are denumerable sets, then so is their union.*

Proof. Let us construct a injection from $A \cup B$ to $\mathbb{Z}^+$ and then by Lemma 14.7 we can conclude.

Since A, B are denumerable, there are bijections f, g from $\mathbb{Z}^+$ to A, B respectively. Now we construct $h : A \cup B \to \mathbb{Z}^+$ as follows.

$$h(x) = \begin{cases} 2f^{-1}(x) & \text{if } x \in A, \\ 2g^{-1}(x) + 1 & \text{if } x \in B - A. \end{cases}$$

To see h is an injection, we prove by contradiction. Suppose there are $x, y \in A \cup B$ such that $h(x) = h(y)$. Then $x, y \in A$ or $x, y \in B - A$, because according to the definition for the former case h is even, while for the latter case h is odd. If x, y are inside A or $B - A$, since f, g are bijections, $h(x)$ and $h(y)$ still can not equal. In all we proved that h is an injection. □

Proposition 14.9. *If A, B are denumerable sets, then so is their Cartesian product $A \times B$.*

Idea: we can display the elements of $A \times B$ in a double array. If we start to count these elements by going along one row which is infinite, then we will never get to the other rows. However if we count along the diagonals, all elements will be reached and we can rearrange the into a sequence of elements.

Proposition 14.10. *If A is a denumerable set then so is A^n for every positive integer n.*

The proof is given by inductively applying Proposition 14.9.

Theorem 14.11. *(Cantor 1874) The set of rationals $\mathbb{Q}$ is denumerable.*

Proof. We may define a function

$$f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}^+$$

by $f(q) = (m, n)$ where $q = \frac{m}{n}$ and the fraction $\frac{m}{n}$ is in lowest terms. This is clearly an injection. Also the codomain $\mathbb{Z} \times \mathbb{Z}^+$ is denumerable and there is a bijection $\mathbb{Z}^+ \to \mathbb{Z} \times \mathbb{Z}^+$. Then we are able to get a injection from $\mathbb{Q}$ to $\mathbb{Z}^+$. By Lemma 14.7, $\mathbb{Q}$ is denumerable. □

14.2 Uncountable sets

In 1874, Georg Cantor published a remarkable paper which he proved not only that the set of rational numbers is denumerable but also that there is a hierarchy of infinite sets ordered by cardinality (to be explained later).

Theorem 14.12. *(Cantor 1874) The set of real numbers $\mathbb{R}$ is uncountable.*

We need to show that there is no bijection between $\mathbb{Z}^+ \to \mathbb{R}$. Using proof by contradiction implies that it suffices to show that for any map $\mathbb{Z}^+ \to \mathbb{R}$, the map can not be surjective.

Proof. Suppose $f : \mathbb{Z}^+ \to \mathbb{R}$ is a function. Let

$$f(m) = a_{m0}.a_{m1}a_{m2}a_{m3}...a_{mn}...$$

as an infinite decimal (not ending in recurring 9's).

Set $b = 0.b_1b_2...b_n...$ where

$$b_n = \begin{cases} 1 & \text{if } a_{nn} = 0, \\ 0 & \text{if } a_{nn} \neq 0. \end{cases}$$

Notice that this infinite decimal representing b certainly does not end in recurring 9s. Furthermore for each $n \geq 1$, the nth decimal place of b, namely b_n, differs from the nth decimal place of $f(n)$, namely a_{nn}. So $b \neq f(n)$ for each n. We find that the real value b is not in the image of f which shows that f is not a surjection. Hence $\mathbb{R}$ is not denumerable. □

Roughly the theorem announces that the set of real numbers is in real sense larger than the set of integers. We can make this precise below.

Definition 14.13. Two sets X, Y have the same cardinality, written $|X| = |Y|$, if they are equipotent. If there is an injection $X \to Y$ then we write $|X| \leq |Y|$. We write $|X| < |Y|$ to mean $|X| \leq |Y|$ and $|X| \neq |Y|$ and say that X has smaller cardinality than Y

Example 14.2.1.

$$|\mathbb{R}| > |\mathbb{Z}^+|, \quad |\mathbb{Q}| = |\mathbb{Z}^+| = |\mathbb{Z}|.$$

One natural question is whether there is a set larger than $\mathbb{R}$. Cantor was able to show that there is such a set and indeed the power set of $\mathbb{R}$ is necessarily larger.

Theorem 14.14. *For any set X, $|X| < |\mathcal{P}(X)|$.*

The theorem is Theorem 14.3.3 in the textbook and the proof is given after. Let us only present the key part.

Proof. We only show below that for any function f from $X \to \mathcal{P}(X)$, f can not be surjective.

Define

$$A = \{x \in X \mid x \notin f(x)\}.$$

Clearly A is a subset of X i.e. $A \in \mathcal{P}(X)$. We claim that A is not in the image of f. Suppose for contradiction, it is in the image of f. Then there exists $a \in X$ such that $f(a) = A$.

If $a \in A$, by the definition of A, $a \notin f(a) = A$ which is a contradiction. If $a \notin A$, then by the definition $a \in A$ which is again a contradiction.

We conclude that f is not a surjection.

□

To end this chapter let us present the pigeonhole principle for infinite sets.

Theorem 14.15. *(Cantor-Schröder-Bernstein theorem) Suppose that X, Y are non-empty set such that $|X| > |Y|$. Then any function $f : X \to Y$ is not an injection.*

The proof is hard but also very interesting. Here is one reference: https://artofproblemsolving.com/wiki/index.php/Schroeder-Bernstein_Theorem.

15 The division theorem

From now on, we will illustrate how the methods of proof and the language of sets and functions introduced so far are applied in arithmetic and the theory of numbers.

The following theorem is the main result in this chapter.

Theorem 15.1. *(The division theorem) Let a, b be two integers. Then there are unique integers q, r such that*

$$a = bq + r \quad \text{and } 0 \leq r < |b|.$$

Here q is called the quotient and r is called the remainder. If $r = 0$, we say that b divides a.

Example 15.0.1. *If $a = 7$ and $b = 3$, then $q = 2$ and $r = 1$, since $7 = 3 \times 2 + 1$.*

If $a = -7$ and $b = 3$, then $q = -3$ and $r = 2$, since $-7 = 3 \times (-3) + 2$.

Proof. (of Theorem 15.1) **Existence**. Consider first the case $b < 0$. Setting $b' = -b$ and $q' = -q$, the equation $a = bq + r$ may be rewritten as $a = b'q' + r$ and the inequality $0 \leq r < |b|$ may be rewritten as $0 \leq r < |b'|$. This reduces the existence for the case $b < 0$ to that of the case $b > 0$.

Similarly, if $a < 0$ and $b > 0$, set $a' = -a, q' = -q - 1, r' = b - r$ if $r > 0$ or $a' = -a, q' = -q, r' = 0$ if $r = 0$. Let us only discuss the case when $r > 0$ below. The equation $a = bq + r$ may be rewritten as $a' = bq' + r'$, and the inequality $0 \leq r < |b|$ may be rewritten as $0 \leq r' < |b|$. Thus the proof of the existence is reduced to the case $a \geq 0$ and $b > 0$.

Consider the set

$$A = \{k \in \mathbb{N} \mid k \geq 0 \text{ and } bk \leq a\}.$$

This set is non-empty since $0 \in A$ and it is finite since $k \in A \implies k \leq a$. Thus it is a finite set of natural numbers, and then it contains a maximum element q. Put $r := a - bq$.

To prove that q, r are as claimed in the theorem, it remains to show that $0 \leq r < b$. Clearly $r \geq 0$ since $bq \leq a$ by the definition of set A. If $r \geq b$, then $a - bq \geq b$ so that $b(q + 1) \leq a$ i.e. $q + 1 \in A$ contradicting the maximality of q. Hence $r < b$ as required.

Uniqueness. Suppose, if we have another division of a by b, say $a = bq' + r'$ with $0 \leq r' < |b|$, then we are required to show that

$$q' = q \text{ and } r' = r.$$

To prove this statement, we first start with the assumptions that

$$0 \leq r < |b|, \quad 0 \leq r' < |b|, \quad a = bq + r, \quad a = bq' + r'.$$

Subtracting the two equations yields

$$b(q - q') = r' - r.$$

So b is a divisor of $r' - r$. As $|r' - r| < |b|$, by the above inequalities, one gets $r' - r = 0$, and $b(q - q') = 0$. Since $b \neq 0$, we get that $r = r'$ and $q = q'$, which proves the uniqueness part of the Euclidean division theorem.

□

Example 15.0.2. *If $n \in \mathbb{Z}^+$ is a perfect square, then $n = 3q$ or $n = 3q + 1$ for some $q \in \mathbb{Z}$.*

Proof. If n is a perfect square, then $n = a^2$ for some $a \in \mathbb{Z}$. By the division theorem $a = 3q_0$ or $a = 3q_0 + 1$ or $a = 3q_0 + 2$ for some $q_0 \in \mathbb{Z}$. Then $a^2 = 3(3q_0^2)$ or $3(3q_0^2 + 2q_0) + 1$ or $3(3q_0^2 + 4q_0 + 1) + 1$ so that $n = 3q$ or $3q + 1$ as required. □

Example 15.0.3. *A positive integer is divisible by 9 if the sum of all the individual digits is divisible by 9. For example, the sum of the digits of the number 3627 is 18, which is divisible by 9 so 3627 is divisible by 9.*

Hint: If we divide 10^n by 9, the remainder is always 1.

16 The Euclidean algorithm

In this section, let us find the greatest common divisor.

Recall the definition:

Definition 16.1. Let a, b be two integers and at least one of them is non-zero. Then the *greatest common divisor* of a and b is the unique positive integer d such that

(i) d is a common divisor, i.e. d divides a and d divides b,

(ii) d is greater than every other common divisor.

We denote the greatest common divisor by $\gcd(a, b)$.

We are going to introduce the Euclidean algorithm that is used to find $\gcd(a, b)$. The method is based on the following observations.

Lemma 16.2. *If a positive integer b divides a, then $\gcd(a, b) = b$.*

Lemma 16.3. *For non-zero integers a and b suppose*

$$a = bq + r \quad \text{where } q, r \in \mathbb{Z}.$$

Then $\gcd(a, b) = \gcd(b, r)$.

The proofs are given in chapter 16 in the book. Please think about how you are going to prove the two Lemmas.

Suppose $a \geq b > 0$. Lemma 16.3 suggests that we can reduce the problem of finding $\gcd(a, b)$ to a simpler problem of finding $\gcd(b, r)$ where $b \leq a$ and $r \leq b$.

Let us do this in the following example:

Example 16.0.1. *Find $\gcd(72, 30)$.*

Solution. We begin by dividing 30 into 72 which gives

$$72 = 30 \times 2 + 12$$

and so, by Lemma 16.1.2, $\gcd(72, 30) = \gcd(30, 12)$. Next

$$30 = 12 \times 2 + 6$$

giving $\gcd(30, 12) = \gcd(12, 6)$. Finally 6 divides 12 and so by Lemma 16.2 we have

$$\gcd(72, 30) = \gcd(30, 12) = \gcd(12, 6) = 6.$$

□

Theorem 16.4. *(The Euclidean algorithm) Suppose that a and b are positive integers. The following procedure defines a finite sequence of positive integers $a_0, a_1, ..., a_n$ such that $a_n = \gcd(a, b)$.*

Algorithm: The goal is to find the sequence described above.

Put $a_0 = a$, $a_1 = b$. Step k: By induction, suppose we have $a_0, a_1, ..., a_k$ have been defined and $a_k > 0$. Using the division theorem, write

$$a_{k-1} = a_k q_k + r_k \quad \text{where } q_k, r_k \in \mathbb{Z} \text{ and } 0 \leq r_k < a_k.$$

If $r_k > 0$, put $a_{k+1} = r_k$ and continue with step $k + 1$.

Otherwise $r_k = 0$, stop and we conclude with

$$a_k = \gcd(a, b).$$

17 Consequences of the Euclidean algorithm

17.1 Integral linear combinations

Theorem 17.1. *Let a, b be integers at least one of which is non-zero. Then there exist integers m, n such that*

$$\gcd(a, b) = ma + nb.$$

Definition 17.2. Given integers a and b, we say that an integer c is an *integral linear combination* of a and b if there exist integers m, n such that $c = ma + nb$.

We sometimes call m, n here the *coefficients* of the linear combination.

Example 17.1.1. *Let us look at the procedure of Example 16.0.1:*

1. $72 = 30 \times 2 + 12$,
2. $30 = 12 \times 2 + 6$,

3. $12 = 6 \times 2 + 0$.

We can rewrite the above as

1. $12 = 72 - 30 \times 2$,
2. $6 = 30 - 12 \times 2$.

If we write the two steps backward, we obtain

$$\begin{aligned} 6 &= 30 - 12 \times 2 \\ &= 30 - (72 - 30 \times 2) \times 2 \\ &= 30 \times 5 - 72 \times 2. \end{aligned}$$

Hence

$$\gcd(72, 30) = 6 = 30 \times 5 - 72 \times 2.$$

Proof. (of Theorem 17.1) Let me only prove the case that a, b are positive. Let $a_0, a_1, ..., a_n$ be the sequence of positive numbers generated by the Euclidean algorithm. Then by the algorithm $a_{k-1} = a_k q_k + a_{k+1}$ and $a_{n+1} = 0$. Let us prove by induction that a_k are integral linear combinations of a, b.

When $k = 0$, $a_0 = a \times 1 + b \times 0$. When $k = 1$, $a_1 = b = a \times 0 + b \times 1$. Now suppose that for all $0 \leq i \leq k$, $a_i = a \times m_i + b \times n_i$ for some integers m_i, n_i. To prove the result for $i = k + 1$, we use the algorithm and get

$$\begin{aligned} a_{k+1} &= a_{k-1} - a_k q_k \\ &= (am_{k-1} + bn_{k-1}) - (am_k + bn_k)q_k \\ &= a(m_{k-1} - m_k q_k) + b(n_{k-1} - n_k q_k), \end{aligned}$$

which is an integral linear combination of a, b. We complete the inductive step. □

17.2 Coprime pairs

Recall

Definition 17.3. Two integers a and b, not both zero, are called *coprime* when $\gcd(a, b) = 1$.

Proposition 17.4. *Two non-zero integers a and b are coprime if and only if there exist integers m, n such that*

$$ma + nb = 1.$$

The proposition is a corollary of Theorem 17.1.

Theorem 17.5. *Suppose that a, b and c are positive integers with a and b coprime. Then*

$$a \text{ divides } bc \implies a \text{ divides } c.$$

Proof. Since a divides bc, $bc = aq$ for some $q \in \mathbb{Z}$. Since $\gcd(a, b) = 1$, there are integers m and n such that $ma + bn = 1$. Plugging in $bc = aq$ into the equality to remove b implies

$$ma + \frac{aq}{c}n = 1.$$

We get

$$c = mac + aqn = a(mc + qn)$$

so that a divides c. □

18 Linear diophantine equations

In this chapter we present a striking application of the Euclidean algorithm, for example the following ancient problem:

Example 18.0.1. *Given integers a, b, c, find all integers m, n such that $am + bn = c$.*

This problem is an example of a *diophantine equation*. This term refers to an equation in one or more unknowns which is to be solved in the integers.

Another famous example of diophantine equation is finding integers a, b, c that satisfy

$$a^3 + b^3 = c^3.$$

This belongs to Fermats Last Theorem: no three integers satisfy

$$a^n + b^n = c^n$$

for $n \geq 3$. The proposition was first conjectured by Pierre de Fermat in around 1637 in the margin of a copy of Arithmetica. He proved for the case when $n = 4$. Fermat added that he had a proof that was too large to fit in the margin. However, there were doubts that he had a correct proof because his claim was published by his son without his consent and after his death. After 358 years of effort by mathematicians, the first successful proof was released in 1994 by Andrew Wiles.

Let us study the Example 18.0.1.

Theorem 18.1. *For positive integers a, b, c, there exist integers m, n such that*

$$am + bn = c$$

if and only if $\gcd(a, b)$ divides c.

Proof. If $\gcd(a, b)$ divides c, then we can write $c = dq$ where $d := \gcd(a, b)$ and $q \in \mathbb{Z}$. By theorem 17.1, there are integers m_0, n_0 such that

$$m_0 a + n_0 b = d.$$

Then

$$qm_0a + qn_0b = qd = c.$$

Letting $m = qm_0$, $n = qn_0$ provides the required equation.

Now suppose that there are $m, n \in \mathbb{Z}$ such that

$$ma + nb = c.$$

Since d divides a, b, we can write $a = da'$ and $b = db'$. Then

$$c = ma + nb = d(ma' + nb')$$

and so d divides c.

□

Example 18.0.2. *Find a solution to*

$$140m + 63n = 35. \tag{4}$$

Solution. We apply the Euclidean algorithm to get that $\gcd(140, 63) = 7$ and

$$140 \times (-4) + 63 \times 9 = 7.$$

Multiplying the above by 5, we get

$$140 \times (-20) + 63 \times 45 = 35.$$

Thus a solution is $m = -20$, $n = 45$. □

One natural question is what are the other solutions of (4). To solve the question, we consider the following.

Example 18.0.3. *Find all the solutions to Diophantine equation*

$$140m + 63n = 0.$$

Solution. The equality is the same as

$$20m + 9n = 0 \iff 20m = -9n.$$

Since $20, 9$ are coprime, 9 divides m. Write $m = 9q$ and then

$$20 \times 9q = -9n \iff n = -20q.$$

So all solutions are

$$m = 9q, \quad n = -20q \quad \text{for } q \in \mathbb{Z}.$$

□

$140m + 63n = 35$ is called an inhomogeneous equation while $140m + 63n = 0$ is called a homogenous equation associated with $140m + 63n = 35$. Similarly as the second order linear equation discussed in Math 20D, every solution to the inhomogeneous can be written as one particular solution of the inhomogeneous solution plus one solution to the homogeneous one.

Proposition 18.2. *Suppose* $(m_0, n_0) \in \mathbb{Z}^2$ *satisfies* $am_0 + bn_0 = c$ *Then for* $(m, n) \in \mathbb{Z}^2$*,*

$$am + bn = c \Longleftrightarrow a(m - m_0) + b(n - n_0) = 0.$$

Example 18.0.4. *Find all the solutions to*

$$140m + 63n = 35.$$

Solution. From the previous example, we found one particular solution $m = -20$, $n = 45$. Thus

$$\begin{aligned} 140m + 63n = 35 &\Longleftrightarrow 140(m + 20) + 63(n - 45) = 0 \\ &\Longleftrightarrow (m + 20, n - 45) = (9q, -20q) \text{ for some } q \in \mathbb{Z} \\ &\qquad \text{(By Example 18.0.3)} \\ &\Longleftrightarrow (m, n) = (-20 + 9q, 45 - 20q) \text{ for some } q \in \mathbb{Z}. \end{aligned}$$

Therefore the set of all solutions to $140m + 63n = 35$ is

$$\{(m, n) = (-20 + 9q, 45 - 20q), \quad q \in \mathbb{Z}\}.$$

□

19 Congruence of integers

Definition 19.1. Two integers a, b are *congruent modulo* m when $a - b$ is divisible by m, i.e. there exists an integer q such that $a - b = mq$. We write $a \equiv b \mod m$.

For example

$$14 \equiv 2 \mod 3, \quad 20 \equiv 0 \mod 10.$$

Properties of the relation of congruence:

Proposition 19.2. *(i) Reflexive property. For all integers* a*,* $a \equiv a \mod m$*.*

(ii) Symmetric property. If $a \equiv b \mod m$*, then* $b \equiv a \mod m$*.*

(iii) Transitive property. If $a \equiv b \mod m$ *and* $b \equiv c \mod m$*, then* $a \equiv c \mod m$*.*

Suppose that $a_1 \equiv a_2 \mod m$ *and* $b_1 \equiv b_2 \mod m$*. Then we have the following Modular arithmetic*

(i) $a_1 + b_1 \equiv a_2 + b_2 \mod m$*,*

(ii) $a_1 - b_1 \equiv a_2 - b_2 \mod m$,

(iii) $a_1 b_1 \equiv a_2 b_2 \mod m$.

Please prove the proposition as an exercise.

Example 19.0.1.

$$4^n + 5 \equiv 1^n + 2 \equiv 3 \equiv 0 \mod 3.$$

$$12345678 \equiv 1 + 2 + 3 + 4 + ... + 8 \equiv 0 \mod 9.$$

19.1 The remainder map

The set of integers

$$R_m = \{0, 1, 2, ..., m-1\}$$

is called the set of *(least, non-negative) remainders modulo* m or the set of *residues modulo* m. Clearly for any $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$, there is a unique $r \in R_m$ such that

$$a \equiv r \mod m.$$

Definition 19.3. We define *the remainder map* $r_m : \mathbb{Z} \to R_m$ by

$$r_m(a) = r \Longleftrightarrow a \equiv r \mod m \text{ and } r \in R_m.$$

Proposition 19.4. *Two integers* a, b *are congruent modulo* m *if and only if* $r_m(a) = r_m(b)$.

Example 19.1.1. *Prove that there do not exist integers* a, b *such that* $a^2 + b^2 = 1234567$.

Solution. From modular arithmetic

$$\begin{aligned} a \equiv 0 \mod 4 &\Longrightarrow a^2 \equiv 0 \mod 4, \\ a \equiv 1 \mod 4 &\Longrightarrow a^2 \equiv 1 \mod 4, \\ a \equiv 2 \mod 4 &\Longrightarrow a^2 \equiv 0 \mod 4, \\ a \equiv 3 \mod 4 &\Longrightarrow a^2 \equiv 1 \mod 4. \end{aligned}$$

Thus for any $a \in \mathbb{Z}$, $a^2 \equiv 0$ or $1 \mod 4$. Therefore $a^2 + b^2 \equiv 0$ or 1 or $2 \mod 4$. However $1234567 \equiv 3 \mod 4$. Hence it is impossible to have $a^2 + b^2 = 1234567$ with $a, b \in \mathbb{Z}$. □

Consider $30 \equiv 2 \mod 4$. If we try to divide the equation by 2, we are able to get $15 \equiv 1 \mod 2$. Actually we have the following proposition.

Proposition 19.5. *Suppose that* a *is an integer which divides* m. *Then*

$$ab \equiv ac \mod m \Longleftrightarrow b \equiv c \mod (m/a).$$

Proof. From the definition of congruence,

$$ab \equiv ac \mod m \iff a(b-c) \equiv 0 \mod m$$

$$\iff a(b-c) = mq \text{ for some } q \in \mathbb{Z} \iff b - c = q(m/a) \text{ for some } q \in \mathbb{Z}$$

which is the same as

$$b \equiv c \mod (m/a).$$

□

At the other extreme, division by numbers which are coprime to the modulus is also clear. For example $30 \equiv 2 \mod 7 \iff 15 \equiv 1 \mod 15$.

Proposition 19.6. *Suppose* $\gcd(a, m) = 1$. *Then*

$$ab \equiv ac \mod m \iff b = c \mod m.$$

The proof follows from Theorem 17.5.

Example 19.1.2. *Solve the congruence* $6x \equiv 15 \mod 21$.

Solution. By the above two propositions,

$$\begin{aligned} 6x \equiv 15 \mod 21 &\iff 2x \equiv 5 \mod 7 \\ &\iff 2x \equiv 5 \equiv 12 \mod 7 \\ &\iff x \equiv 6 \mod 7. \end{aligned}$$

Hence

$$6x \equiv 15 \mod 21 \iff x \equiv 6 \mod 7.$$

The solutions are $x = 7q + 6$ for all $q \in \mathbb{Z}$. □

20 Linear congruence

In this chapter we discuss theoretically the linear congruence equation $ax \equiv b \mod m$.

Recall

(1) If a divides m, then

$$ab \equiv ac \mod m \iff b \equiv c \mod (m/a).$$

(2) If $\gcd(a, m) = 1$, then

$$ab \equiv ac \mod m \iff b \equiv c \mod m.$$

Example 20.0.1. *Show that the linear congruence* $6x \equiv 14 \mod 21$ *has no solutions.*

Proof. Suppose for contradiction that there is a solution x. Then there exist an integer q such that

$$6x - 14 = 21q$$

which is the same as $6x - 21q = 14$. However the right-hand side is divisible by 3 but the left-hand side is not. Hence the solution does not exist.

□

Proposition 20.1. *Let a, b be integers. If there exists a common divisor of a, m which does not divide b, then the linear congruence $ax \equiv b \mod m$ has no solutions.*

The proof is of the same idea as given in the proof of the example above. Please complete it.

Example 20.0.2. *Prove that $12468x \equiv 34567 \mod 48732$ has no solutions.*

Proof. There are no solutions because 3 is a common divisor of 12468 and 48732 but does not divide 34567. □

Proposition 20.2. *Suppose $\gcd(a, m) = 1$. Then there exists a unique $x \in R_m$ such that for any integer b we have $ax \equiv b \mod m$.*

Proof. Since $\gcd(a, m) = 1$, by Proposition 17.4 (Euclidean algorithm) there exist integers n, l such that

$$an + ml = 1.$$

Hence

$$a(bn) = b - bml$$

which implies that bn is a solution to

$$ax \equiv b \mod m.$$

Thus $x = r_m(bn)$ is the desired solution.

To show uniqueness, suppose that $x, y \in R_m$ are two solutions. Then

$$a(x - y) = ax - ay \equiv 0 \mod m.$$

Since $\gcd(a, m) = 1$, by (2), $x - y \equiv 0 \mod m$. Now it follows from $x, y \in R_m$ that $|x - y| < m$. So $x = y$ which implies uniqueness. □

Theorem 20.3. *The linear congruence $ax \equiv b \mod m$ has a solution if and only if $\gcd(a, m)$ divides b. In this case the number of different solutions modulo m is $\gcd(a, m)$.*

Proof. If $\gcd(a, m)$ divides b, let us write

$$a = a' \gcd(a, m), \quad m = m' \gcd(a, m), \quad b = b' \gcd(a, m),$$

and we have that a', m' are coprime. By (1), solving the linear congruence is the same as solving

$$a'x \equiv b' \mod m'.$$

It follows from Proposition 20.2, there exists a solution.

Next if there is a solution to the linear congruence, then there exist $x, n \in \mathbb{Z}$ such that

$$ax - b = mn \text{ which is } \iff ax - mn = b.$$

The right-hand side is divisible by $\gcd(a, m)$ and so b is also divisible by $\gcd(a, m)$.

Finally we determine the number of incongruent solutions (with respect to $\mod m$). Recall that x is a solution if and only if

$$a'x \equiv b' \mod m'.$$

From Proposition 20.2, among $R_{m'}$, there exists a unique $r_0 \in R_{m'}$ satisfying the equation. Here the goal for us is to find solutions in the congruence class modulo m. Suppose x is congruent modulo m to $r \in R_m$. Then x is a solution is and only if

$$r \equiv r_0 \mod m'.$$

This means that $r = r_0 + m'q$ for some $q \in \mathbb{Z}$.

Since $r \in R_m$, $0 \leq r_0 + m'q < m$. Using $0 \leq r_0 < m'$, we get

$$0 \leq q < \frac{m - r_0}{m'} = \gcd(a, m) - \frac{r_0}{m'}.$$

Thus q can be any number from $0, 1, ..., \gcd(a, m) - 1$. This provides us exactly $\gcd(a, m)$ many q's as well as $\gcd(a, m)$ many solutions modulo m.

□

21 Congruence class

First let us define the congruence class below. It is not a very new definition and we have more or less encounter it before.

Definition 21.1. Given integers a and $m > 0$, the *congruence class of a modulo m* is the set of integers which are congruent to a modulo m. We denote this congruence class by $[a]_m$.

Then we have

$$[a]_m = \{x \in \mathbb{Z} \,|\, x \equiv a \mod m\}.$$

Each number in

$$R_m = \{0, 1, ..., m - 1\}$$

can be viewed as a representative of one class in $[a]_m$. However the advantage of using $[a]_m$ instead of R_m is the natural arithmetic of $[a]_m$ to be introduced below.

Example 21.0.1.

$$[0]_2 = \{0, \pm 2, \pm 4, ...\} = [10]_2 = \{ \textit{all even numbers}\}.$$

$$[1]_6 = \{6q + 1 \,|\, q \in \mathbb{Z}\}.$$

Proposition 21.2. *For integers a, b,*

(i) $a \equiv b \mod m \iff [a]_m = [b]_m$,

(ii) $a \not\equiv b \mod m \iff [a]_m \cap [b]_m = \emptyset$.

We skip the proof which should not be hard.

Definition 21.3. We write $\mathbb{Z}_m$ for the set of congruence classes modulo m.

21.1 The arithmetic of congruence class

Definition 21.4. Addition, substraction and multiplication of elements of $\mathbb{Z}_m$ are defined by

$$\begin{aligned}
[a]_m + [b]_m &= [a+b]_m, \\
[a]_m - [b]_m &= [a-b]_m, \\
[a]_m \times [b]_m &= [ab]_m.
\end{aligned}$$

Proposition 21.5. *Addition, substraction and multiplication in $\mathbb{Z}_m$ are well-defined.*

Proof. Suppose $a_1 \equiv a_2 \mod m$ and $b_1 \equiv b_2 \mod m$. To show that addition and substraction are well-defined, it suffices to show that

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \mod m,$$

which is certainly true. To see that multiplication is well-defined, we need to verify

$$a_1 b_1 \equiv a_2 b_2 \mod m$$

which is again true by the definition. □

Then we can view elements in $\mathbb{Z}_m$ as numbers with arithmetic (then by definition, each element is a again a set of integers).

Recall the linear congruence equation. Now let us use the language of congruence class to restate our Proposition 20.2.

Theorem 21.6. *Suppose that a and b are integers such that a and m are coprime. Then the equation*

$$[a]_m \times [x]_m = [b]_m$$

has a solution in $\mathbb{Z}_m$. This solution is unique.

Proof. Define a function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ by

$$f([x]_m) = [a]_m \times [x]_m.$$

We have

$$\begin{aligned} f([x_1]_m) = f([x_2]_m) &\implies [ax_1]_m = [ax_2]_m \\ &\implies ax_1 \equiv ax_2 \mod m \\ &\implies x_1 \equiv x_2 \mod m \quad (\text{ use that } \gcd(a,m) = 1) \\ &\implies [x_1]_m = [x_2]_m. \end{aligned}$$

This implies that the map f is an injection. Since $\mathbb{Z}_m$ is a finite set (with m elements), by the pigeonhole principle, f is a bijection. Thus there is a unique element $[x_0]_m \in \mathbb{Z}_m$ such that $f([x_0]_m) = [b]_m$, i.e.

$$[a]_m \times [x_0]_m = [b]_m.$$

□

Definition 21.7. The element $[a]_m \in \mathbb{Z}_m$ is called *invertible* if there is an integer $[a']_m \in \mathbb{Z}_m$ such that

$$[a]_m \times [a']_m = [1]_m.$$

Here $[a']_m$ is called the *inverse* of $[a]_m$ and we write $[a']_m = ([a]_m)^{-1}$. Alternatively we might also say that a' is an inverse of a modulo m.

Example 21.1.1.

$$\begin{aligned} ([1]_m)^{-1} &= [1]_m; \\ ([3]_{10})^{-1} &= [7]_{10} \end{aligned}$$

because

$$3 \times 7 \equiv 1 \mod 10.$$

Proposition 21.8. *Suppose that a' is an inverse of a modulo m. Then*

$$ax \equiv b \mod m \iff x \equiv a'b \mod m.$$

Proof. By the assumption $aa' \equiv 1 \mod m$. Thus

$$ax \equiv b \mod m \implies a'ax \equiv a'b \mod m \implies x \equiv a'b \mod m$$

and

$$x \equiv a'b \mod m \implies ax \equiv aa'b \mod m \implies ax \equiv b \mod m.$$

□

As a corollary, if p is a prime number, then $[1]_p, [2]_p, ..., [p-1]_p$ are all invertible in $\mathbb{Z}_p$.

22 Partitions and equivalence relations

Definition 22.1. Let X be a set. A *partition* of X is a subset Π of $\mathcal{P}(X)$ such that

(i) the subsets in Π are non-empty;

(ii) the subsets in Π are disjoint, i.e.

$$\forall A_1, A_3 \in \Pi, \text{ then either } A_1 = A_2 \text{ or } A_1 \cap A_2 = \emptyset,$$

(iii) the subsets in Π cover X, i.e. $\cup_{A \in \Pi} A = X$.

Example 22.0.1. *(1) One partition of the set $\{1, 2, 3, ..., 8\}$ is given by*

$$\Pi = \{\{1, 2, 3, 4, 5\}, \{6, 7, 8\}\}.$$

(2) The set of subsets $\mathbb{Z}^+, \{0\}$ is not a partition of $\mathbb{Z}$.

(3) The two sets of $\{n \in \mathbb{Z} \,|\, n \geq 0\}$, $\{n \in \mathbb{Z} \,|\, n \leq 0\}$ are not a partition of $\mathbb{Z}$.

(4) The set of congruence classes modulo 7,

$$\mathbb{Z}_7 = \{[a]_7 \,|\, a = 0, 1, ..., 6\}$$

is a partition of $\mathbb{Z}$ into 7 subsets.

Proposition 22.2. *Let $f : X \to Y$ be a surjection. Then the value of the function f gives a partition of X by*

$$\Pi = \{\overleftarrow{f}(\{y\}) \,|\, y \in Y\}.$$

Example 22.0.2. *Consider the remainder map $r_m : \mathbb{Z} \to R_m = \{0, 1, 2, ..., m-1\}$. Then*

$$\{\overleftarrow{r_m}(\{i\}) \,|\, i = 0, 1, 2, ..., m-1\}$$

is a partition of $\mathbb{Z}$. Actually the partition is given by the congruence class modulo m.

Proof. (of Proposition 22.2) The sets of $\overleftarrow{f}(\{y\})$with $y \in Y$ are non-empty because f is a surjection; they are disjoint because f is well-defined; and they cover X because each element in x has a preimage in Y. $\square$

22.1 Relations

Given a partition Π of a set X, we can define a *equivalence relation* on X: two elements are equivalent if and only if they are in the same subset of the partition.

We write $a \sim_\Pi b$ to denote that a, b are related (or equivalent). By the definition, this is the same as: there exists $A \in \Pi$ such that $a \in A$ and $b \in A$. We have the following properties:

Proposition 22.3. *Let a, b, c be elements of X.*

(i) Reflexive property. For all $a \in X$, $a \sim_\Pi a$.

(ii) Symmetric property. If $a \sim_\Pi b$, then $b \sim_\Pi a$.

(iii) Transitive property. If $a \sim_\Pi b$ and $b \sim_\Pi c$, then $a \sim_\Pi c$.

In general, a (binary) *relation* is a broad concepts:

Definition 22.4. A (binary) relation over X is a set R of ordered pairs (x, y) consisting of elements $(x, y) \in X \times X$. It encodes the information of relation: x is related to y (written $x \sim y$), if and only if the pair $(x, y) \in R$.

Example 22.1.1.

- *The relation "$\leq$" on $\mathbb{R}$.*
- *The relation "$=$" on $\mathbb{R}$.*
- *The relation "$<$" on $\mathbb{R}$.*
- *We can define a relation on $\mathbb{R}$ by $a \sim b \iff ab > 0$.*

Definition 22.5. Suppose $\sim$ is a relation on a set X. If it is reflexive, symmetric and transitive, then the relation is an *equivalence relation*.

Example 22.1.2.

- *The relation "$\leq$" on $\mathbb{R}$ is reflexive, is not symmetric and is transitive.*
- *The relation "$=$" on $\mathbb{R}$ is not reflexive, is not symmetric and is transitive.*
- *The relation "$<$" on $\mathbb{R}$ is an equivalence relation.*
- *We can define a relation on $\mathbb{R}$ by $a \sim b \iff ab > 0$ is not reflexive, is symmetric and is transitive.*

22.2 Equivalence relation

If a relation of a set X is an equivalence relation, we can define the equivalence class from the relation. For example, consider congruence modulo m relation on $\mathbb{Z}$ i.e. $a \sim b$ is and only if $a \equiv b \mod m$. This is an equivalence relation. Though the relation, we have defined the congruence class modulo m: $\mathbb{Z}_m$.

The more general case is given below:

Definition 22.6. Suppose that $\sim$ is an equivalence relation on a nonempty set X. For each $a \in X$, we define the *equivalence class of a* to be

$$[a] = \{x \in X \mid x \sim a\}.$$

Observe that each equivalence class is a subset of X. We denote the set of all equivalence classes by $X/\sim$, i.e.

$$X/\sim = \{[a] \mid a \in X\} \subseteq \mathcal{P}(X).$$

Theorem 22.7. *Suppose that $\sim$ is an equivalence relation on the set X. Then for $a, b \in X$,*

(i) $a \sim b \iff [a] = [b]$,

(ii) $a \not\sim b \iff [a] \cap [b] = \emptyset$.

Note that the conclusions of the theorem are not true if the relation is not an equivalence relation.

23 Prime numbers

Definition 23.1. A positive integer n is said to be *prime* when $n > 1$ and the only positive divisors of n are 1 and n. If an integer $n > 1$ is not prime then it is said to be composite.

The first few prime numbers are as follows:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...$$

Notice that 2 is the only even number in primes.

Proposition 23.2. *Every integer greater than 1 can be written as a product of prime numbers.*

Here we think of a prime number as a product of a single prime number, namely itself.

Proof. The proof is by strong induction.

When $n = 2$, it is a prime number and so a product of a single prime.

Suppose as inductive hypothesis that for some $k \geq 2$, if $2 \leq n \leq k$ then n can be written as a product of primes. Now for $n = k + 1$, if n is prime then the it is a product of a single prime. If n is not a prime, then $n = k + 1 = ab$ where $a, b \geq 2$. By inductive hypothesis, a, b can be written as products of primes and hence $k + 1 = ab$ can be written as a product of primes. $\square$

The following result is the key property of prime numbers.

Theorem 23.3. *If p is a prime number and p divides ab where a, b are positive integers, then p divides a or p divides b.*

The proof follows from Theorem 17.5.

Example 23.0.1. *Find all prime numbers not exceeding* 100.

Theorem 23.4. *(Fundamental theorem of arithmetic) Every positive integer greater than* 1 *can be written uniquely as a product of prime numbers with the prime factors in the product written in non-decreasing order.*

The theorem says that for any integer $n > 1$, it can be written uniquely in the form

$$n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$$

where $r \geq 1, k_i \geq 1$ and p_i is a prime number with $p_1 < p_2 < ... < p_r$. Instead of proving the theorem, let us take a look at some examples.

Now let us prove that there are infinitely many primes.

Theorem 23.5. *There are infinitely many primes.*

Proof. Suppose for contradiction that the set of primes is finite, say

$$\{p_1, ..., p_n\}.$$

Consider the positive integer

$$m = p_1 p_2 ... p_n + 1.$$

This number is an odd number because 2 is the only even number in primes. Moreover m is not divisible by p_i by the definition. However we know that m can be written as a product of primes which contradicts with the assumption that $p_1, ..., p_n$ are the only primes. Hence we conclude that the set of primes must be infinite.

□

To end this section, let me present some of the well-known conjectures about primes that people do not know how to prove or disprove. If you are able to solve one of them, you will stamp your name on the page of mathematics history!

- Goldbach's Conjecture: Every even $n > 2$ is the sum of two primes. (Chen Jingrun in 1973, and Hugh Montgomery and Robert Charles Vaughan in 1975 made great progresses towards the conjecture.)
- Every even number is the difference of two primes.
- Twin Prime Conjecture: There are infinitely many twin primes (both n and $n+2$ are primes).
- For every even number $2n$, are there infinitely many pairs of consecutive primes which differ by $2n$? (The work of Yitang Zhang in 2013, as well as work by James Maynard, Terence Tao and others, has made substantial progress towards proving that there are infinitely many twin primes, but at present this remains unsolved.)
- Is there always a prime between n^2 and $(n+1)^2$?
- Wiki page "Conjectures about prime numbers".