Part IA
Numbers and Sets

Dr Zoe Wyatt
Michaelmas 2025
Version 20251204

These are Zixuan's notes for **Part IA – Numbers and Sets** at the University of Cambridge in 2025. The notes are not endorsed by the lecturers or the University, and all errors are my own.

The latest version of this document is available at academic.micfong.space. Please direct any comments to my CRSid email or use the contact details listed on the site.

This document is typeset using Typst. All figures are created using Inkscape.

Contents

Syllabus and Overview

Michaelmas Term [24 Lectures]

Introduction to Number Systems and Logic [2 Lectures]

Overview of the natural numbers, integers, real numbers, rational and irrational numbers, algebraic and transcendental numbers. Brief discussion of complex numbers; statement of the Fundamental Theorem of Algebra.

Ideas of axiomatic systems and proof within mathematics; the need for proof; the role of counter-examples in mathematics. Elementary logic; implication and negation; examples of negation of compound statements. Proof by contradiction.

Sets, Relations and Functions [4 Lectures]

Union, intersection and equality of sets. Indicator (characteristic) functions; their use in establishing set identities. Functions; injections, surjections and bijections. Relations, and equivalence relations. Counting the combinations or permutations of a set. The Inclusion-Exclusion Principle.

The Integers [2 Lectures]

The natural numbers: mathematical induction and the well-ordering principle. Examples, including the Binomial Theorem.

Elementary Number Theory [8 Lectures]

Prime numbers: existence and uniqueness of prime factorisation into primes; highest common factors and least common multiples. Euclid's proof of the infinity of primes. Euclid's algorithm. Solution in integers of $ax + by = c$.

Modular arithmetic (congruences). Units modulo n. Chinese Remainder Theorem. Wilson's Theorem; the Fermat-Euler Theorem. Public key cryptography and the RSA algorithm.

The Real Numbers [4 Lectures]

Least upper bounds; simple examples. Least upper bound axiom. Sequences and series; convergence of bounded monotonic sequences. Irrationality of $\sqrt{2}$ and e. Decimal expansions. Construction of a transcendental number.

Countability and Uncountability [4 Lectures]

Definitions of finite, infinite, countable and uncountable sets. A countable union of countable sets is countable. Uncountability of $\mathbb{R}$. Non-existence of a bijection from a set to its power set. Indirect proof of existence of transcendental numbers.

Lecture 1 · 2025-10-09

1 Introduction to Number Systems and Logic

As an introduction to university-level mathematics, we will look at precise definitions, rigorous proofs, and fundamental theorems. To begin with, let us look at the definitions of a statement and a proof.

Definition 1.1 (Statement)

A **statement** is a sentence that can have a true or false value.

If were to prove a statement, we need a proof.

Definition 1.2 (Proof)

A **proof** is a sequence of true statements without logical gaps, that establishes some conclusions.

We want to prove things because
- we want to know if they are true;
- we want to gain insights into why they are true;
- the proof itself might be cool.

1.1 Number Systems

Notation. These number systems should be fairly familiar:

$\mathbb{N}$ the set of natural numbers (positive integers)
$\mathbb{Z}$ the set of integers
$\mathbb{Q}$ the set of rational numbers, *i.e.* all fractions of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$

Conside the length x of the hypotenuse in a right-angled isosceles triangle with side lengths 1. The Pythagorean realized that $x \notin \mathbb{Q}$. To show that $x = \sqrt{2}$ exists, we need to construct a new number system $\mathbb{R}$, where $\exists x \in \mathbb{R}$ such that $x^2 = 2$.

Definition 1.3 (Algebraic number)

A real number is **algebraic** if it is the root of some polynomial with integer coefficients. *e.g.* $\sqrt{2}$.

Definition 1.4 (Transcendental number)

A real non-algebraic number is **transcendental**. *e.g.* π. [Existence of such transcendental numbers was only shown as late as 1844.]

1.2 Proofs and Non-proofs

Let us take a look at a few examples of proofs (and non-proofs).

> ***Claim.*** For all positive integers n, $n^3 - n$ is always a multiple of 3.

> ***Proof.*** For any $n \in \mathbb{Z}^+$, we have
>
> $$\begin{aligned} n^3 - n &= n\left(n^2 - 1\right) \\ &= (n-1)n(n+1). \end{aligned}$$
>
> One of the 3 consecutive integers $n-1, n, n+1$ must be a multiple of 3, and hence the product.

Here is an example of a false proof.

> ***Claim.*** For any positive integer n, if n^2 is even, then so is n.

> ***Non-proof.*** Given a positive integer n, which is even, we can write $n = 2k$ for some $k \in \mathbb{Z}$.
>
> Then we have $n^2 = 4k^2 = 2\left(2k^2\right)$, which is even.

Note that we have falsely proven the converse above. Here is a corrected version of the proof:

> ***Proof.*** Assume that n^2 is even but n is odd. Then $n = 2k + 1$ where $k \in \mathbb{Z}$, and $n^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1$, which is odd. ※

We have used the technique of *proof by contradiction*, where we assume the contrary and deduce a contradiction (so the assumption would be false).

We can also prove that something is false, usually by a counterexample.

> ***Claim.*** For any positive integer n, if n^2 is a multiple of 9, then so is n.

> ***Disproof.*** A counterexample is $n = 3$.

Lecture 2 · 2025-10-11

We write $A \Rightarrow B$ for the statement "if A then B".

> ***Claim.*** The solution to $x^2 - 5x + 6 = 0$ is $x = 2$ or $x = 3$.

This is in fact 2 assertions:

1. $x = 2$ and $x = 3$ are solutions
2. there are no other solutions

> ***Proof.***
>
> 1. If $x = 2$ or $x = 3$, we have $x - 2 = 0$ or $x - 3 = 0$. Hence $(x-2)(x-3) = 0$.
>
>   Thus, we have $x^2 - 5x + 6 = 0$.
> 2. If $x^2 - 5x + 6 = 0$, then $(x-2)(x-3) = 0$. So $x = 2$ or $x = 3$.
>
>   Hence the only solutions are $x = 2$ and $x = 3$.
>
> Alternatively, we could write the following:

$$\begin{aligned} & x = 2 \text{ or } x = 3 \\ \Leftrightarrow\ & x - 2 = 0 \text{ or } x - 3 = 0 \\ \Leftrightarrow\ & (x-2)(x-3) = 0 \\ \Leftrightarrow\ & x^2 - 5x + 6 = 0. \end{aligned}$$

It is vital that every step is using $\Leftrightarrow$.

Claim. Every positive real number is greater than or equal to 1.

Non-proof. Let r be the least positive real number.

Either $r = 1$ or $r < 1$ or $r > 1$. [This is a trichotony.]

If $r < 1$, then $0 < r^2 < r$. However, r is the least positive real number. ※

If $r > 1$, then $0 < \sqrt{r} < r$. ※

Hence $r = 1$.

We assumed a false claim in the proof: there is no least positive real number.

Moral. Every claim must be justified.

1.3 Basic Logic

If A and B are assertions, we can write:
- $A \wedge B$ for "A AND B",
- $A \vee B$ for "A OR B",
- $\neg A$ for "NOT A".

1.3.1 Truth Tables

The truth of these assertions depends on the truth of A and B, and can be summerized in a **truth table**.

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$
F	F	F	F	T	T
F	T	F	T	T	T
T	F	F	T	F	F
T	T	T	T	F	T

Note, *e.g.*, that $\neg(A \wedge B)$ is equivalent to $(\neg A) \vee \neg B)$, by comparing truth tables.

Also, $A \Rightarrow B$ is equivalent to $(\neg A) \vee B$, and hence $B \vee (\neg A)$, and so to $(\neg B) \Rightarrow (\neg A)$. This is called the **contrapositive**.

A claim may include **quantifiers**, especially $\forall$ "for all" and $\exists$ "there exists".

1.3.2 Negating Quantifiers

We have

$$\neg(\forall x, A(x)) \Leftrightarrow \exists x, \neg A(x)$$
$$\neg(\exists B(x)) \Leftrightarrow \forall x, \neg B(x).$$

> ***Remark.*** The order of quantifiers matters.

2 Sets, Functions and Relations

2.1 Sets

2.1.1 Introduction on Sets

Definition 2.1 (Set)

A **set** is a collection of mathematical objects.

Examples include $\mathbb{R}, \mathbb{N}, \{1, 5, 9\}, (-2, 3]$.

The order of elements in a set is immaterial, and elements are counted only once. *e.g.* $\{1, 3, 7\} = \{1, 7, 3\}$, and $\{1, 4, 4, 5, 2\} = \{1, 2, 5, 4\}$.

Definition 2.2 (Empty set)

There is only one set with no elements, called the **empty set** $\varnothing$.

Definition 2.3 (Set inclusion, equality, subset and proper subset)

We write $x \in A$ if x **is an element of** A, and $x \notin A$ if not.

Two sets are **equal** if they have the same elements. *i.e.* $A = B$ if and only if $\forall x, x \in A \Leftrightarrow x \in B$.

A set B is a **subset** of A, written $B \subseteq A$ or $B \subset A$, if every element of B is an element of A.

B is said to be a **proper subset** of A if $B \subseteq A$ and $B \neq A$. This is also written as $B \subsetneq A$.

Remark. $A = B$ if $A \subseteq B$ and $B \subseteq A$.

If A is a set and P is a property of some elements of A, we can write $\{x \in A : P(x)\}$ for the subset of A comprising those elements for which $P(x)$ holds.

Definition 2.4 (Set operations)

If A and B are sets, then

- their **union** $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
- their **intersection** $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
- A and B are **disjoint** if $A \cap B = \varnothing$.
- their **difference** $A \setminus B = \{x \in A : x \notin B\}$.

2.1.2 Properties of Sets

Proposition 2.5

We have a few properties about intersections and unions.

- we can view intersection as a special case of subset selection:

$$A \cap B = \{x \in A : x \in B\}.$$

- intersection and union are commutative and associative:

$$A \cup B = B \cup A \quad \text{and} \quad (A \cup B) \cup C = A \cup (B \cup C)$$

- union is distributive over intersection, *i.e.*

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

and intersection is distributive over union:

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

Lecture 3 · 2025-10-14

Proposition 2.6 (De Morgan's law)

If A, B, C are sets, then

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

To prove statements in Proposition 2.5 and Proposition 2.6, we can rewrite set notation into a combination of inclusion and logical connectives, and then use a truth table to derive the results. Usually, we need to show that LHS $\subseteq$ RHS and RHS $\subseteq$ LHS.

Notation. If A_1, A_2, A_3 are sets, then

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap A_3 \cap \ldots$$
$$= \{x : x \in A_n \forall n \in \mathbb{N}\}.$$

Similarly,

$$\bigcup_{n=1}^{\infty} A_n = A_1 \cup A_2 \cup A_3 \cup \ldots$$
$$= \{x : x \in A_n \exists n \in \mathbb{N}\}.$$

> ***Important.*** The ∞ does **not** mean the *limit* of anything.

More generally, given an index set I and a collection of sets A_i indexed by $i \in I$, we write

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \forall i \in I\}, \text{and}$$
$$\bigcup_{i \in I} A_i = \{x : x \in A_i \exists i \in I\}.$$

Definition 2.7 (Cartesian product)

Given sets A and B, we can form their **Cartesian product** $A \times B = \{(a, b) : a \in A \wedge b \in B\}$, which is the set of ordered pairs (a, b) with $a \in A$ and $b \in B$.

Remark. To formally define an ordered pair, we can define $(a, b) = \{\{a\}, \{a, b\}\}$.

We can extend Definition 2.7 to ordered triples and so on, *e.g.*

$$\begin{aligned}\mathbb{R}^3 &= \mathbb{R} \times \mathbb{R} \times \mathbb{R} \\ &= \{(x, y, z) : x, y, z \in \mathbb{R}\}.\end{aligned}$$

Definition 2.8 (Power set)

For any set X, the **power set** $\mathcal{P}(X)$ is the set consisting of all subsets of X, *i.e.*

$$\mathcal{P}(X) = \{Y : Y \subseteq X\}.$$

For example, if $X = \{1, 2\}$, then $\mathcal{P}(X) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

Important. Given a set A, we can form $\{x \in A : P(x)\}$ for any property P. However, we cannot always form $\{x : P(x)\}$, due to the following paradox.

Suppose $X = \{x : x \text{ is a set} \wedge x \notin x\}$ were a set. Now, if $X \in X$, it implies by definition that $X \notin X$.

On the other hand, if $X \notin X$, then $X \in X$ by our construction. ※

This is known as Russell's Paradox. More generally, this comes from the fact that there is no *universal set* $\mathcal{U}$ such that $\forall x, x \in \mathcal{U}$. Otherwise, we could form X above using the subset notation as $X = \{x \in \mathcal{U} : x \notin x\}$.

Moral. To guarantee that a set exists, it should be obtained from known sets (*e.g.* $\mathbb{N}, \mathbb{R}$) in one of the ways discussed above.

2.1.3 Finite Sets

Definition 2.9 (Size of a set)

Given $n \in \mathbb{Z}_{\geqslant 0}$, we say a set A has **size** n if we can write $A = \{a_1, a_2, ..., a_n\}$ with the elemtns a_i distinct.

Definition 2.10 (Finite and infinite set)

We say A is **finite** if $\exists n \in \mathbb{Z}_{\geqslant 0}$ such that A has size n, and A is **infinite** otherwise.

2.2 Functions

Definition 2.11 (Function)

Given sets A and B, a **function** f from A to B is a *rule* that assigns to every $x \in A$ uniquely to an element $f(x) \in B$.

More formally, a **function** from A to B is a subset $f \subseteq A \times B$ such that for all $x \in A$, there exists exactly one $y \in B$ such that $(x, y) \in f$. We usually write

$$f : A \to B$$

and

$$f(x) = y \quad \text{or} \quad x \mapsto y.$$

Example 2.12

1. $f : \mathbb{R} \to \mathbb{R}$ with $x \mapsto x^2$ is a function.
2. $f : \mathbb{R} \to \mathbb{R}$ with $x \mapsto \frac{1}{x}$ is not a funciton since it is undefined at $x = 0$.
3. $f : \mathbb{R} \to \mathbb{R}$ with $x \mapsto \pm\sqrt{|x|}$ is not a function.
4. $f : \mathbb{R} \to \mathbb{R}$ with $x \mapsto \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{otherwise} \end{cases}$ is a function.

Definition 2.13 (Domain, range, image, preimage)

Following Definition 2.11, for $f : A \to B$, we say that A is the **domain** of f and B is the **range** (or codomain).

If $x \in A$ and $f(x) \in y$, then y is called the **image** of x, and x is called a **preimage** of y.

Moreover, if $X \subseteq A$ then the **image** of X under f is

$$\begin{aligned} f(X) &= \{f(x) : x \in X\} \\ &= \{b \in B : \exists x \in X, f(x) = b\}. \end{aligned}$$

If $Y \subseteq B$, then the **preimage** of Y under f is

$$f^{-1}(Y) = \{a \in A : \exists y \in Y, f(a) = y\}.$$

Example 2.14

For the function $f(x) = x^2$, the image of 6 is 36, but the preimage of 36 is ± 6.

We also have $\mathrm{Im}(f) = \{y \in \mathbb{R} : y \geqslant 0\}$, and $f(\{x \in \mathbb{R} : -1 \leqslant x < 4\}) = [0, 16)$.

The preimage $f^{-1}(\{y \in \mathbb{R} : -1 \leqslant y < 4\}) = (-2, 2)$.

Lecture 4 · 2025-10-16

Notation. For $f : A \to B$, we usually denote $f(A)$ as $\mathrm{Im}(f)$, which is called the image of f.

Definition 2.15 (Injection, surjection, bijection)

We say $f : A \to B$ is **injective** if $\forall a, a' \in A$, we have $a \neq a' \Rightarrow f(a) \neq f(a')$. Equivalently, f is injective if $f(a) = f(a') \Rightarrow a = a'$ by the contrapositive.

We say $f : A \to B$ is **surjective** if $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$.

We say $f : A \to B$ is **bijective** if it is both injective and surjective.

If $f : A \to B$ is a bijection, then everything in B is mapped to exactly once. That is, f *pairs* elements of A and B.

Definition 2.16 (Permutation)

A **permutation** of A is a bijection $f : A \to A$.

Important. When specifying a function, we must specify its domain and range.

Observation.

1. f is surjective if and only $f(A) = B$.

   For finite sets A and B, if $|B| > |A|$, then there cannot be a surjective function from A to B.
2. For finite sets A and B, there is no injection from A to B if $|A| > |B|$.
3. For a finite set A, $f : A \to A$, then f is injective if and only if f is surjective.
4. For a finite set A, There is no bijection from A to any proper subset of it.
5. A set X has size n if and only if there is a bijection $\{1, 2, ..., n\} \to X = \{a_1, a_2, ..., a_n\}$ where $i \mapsto a_i$.

2.2.1 Examples of Functions

Definition 2.17 (Identity function)

For any set X, the function $\mathrm{id}_X : X \to X$ where $x \mapsto x$ is the **identity function**.

Example 2.18 (Examples of functions)

- A sequence of reals $x_1, x_2, ...$ is a function $\mathbb{N} \to \mathbb{R}$ where $n \mapsto x_n$.
- The operation on $\mathbb{N}$ is a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where $(a, b) \mapsto a + b$.

Definition 2.19 (Indicator function)

Given a set X and $A \subseteq X$, we have the **indicator function** (or characteristic function) of A, defined by

$$\mathbf{1}_A : X \to \{0, 1\} \quad \text{where} \quad x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Proposition 2.20 (Properties of the indicator function)

1. $\mathbf{1}_A = \mathbf{1}_B \Leftrightarrow A = B$
2. $\mathbf{1}_{A\cap B} = \mathbf{1}_A \mathbf{1}_B$
3. $\mathbf{1}_{X\setminus A} = 1 - \mathbf{1}_A$
4. $\mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_{A\cap B}$

Proof. [for property (4)]

We have

$$\begin{aligned}\mathbf{1}_{A\cup B} &= 1 - \mathbf{1}_{X\setminus A\cup B}\\ &= 1 - \mathbf{1}_{A^\complement\cap B^\complement}\\ &= 1 - \mathbf{1}_{A^\complement}\mathbf{1}_B^\complement\\ &= 1 - (1-\mathbf{1}_A)(1-\mathbf{1}_B)\\ &= \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_{A\cap B}.\end{aligned}$$

Lecture 5 · 2025-10-18

Definition 2.21 (Fucntion composition)

Given $f : A \to B$ and $y : B \to C$, the **composition** is $g \circ f : A \to C$, where $a \mapsto g(f(a))$.

Proposition 2.22 (Properties of composition)

- In general, $\circ$ is not commutative.
- $\circ$ is associative. *i.e.* if we have $f : A \to B, g : B \to C, h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. For example, if $f : \mathbb{R} \to \mathbb{R}$ with $x \mapsto 2x$, and $g : \mathbb{R} \to \mathbb{R}$ with $x \mapsto x + 1$, then

$$\begin{aligned}g \circ f = g(2x) &= 2x + 1\\ f \circ g = f(x+1) &= 2(x+1).\end{aligned}$$

Hence, in general, $\circ$ is not commutative.

Now, for every $x \in A$, we have

$$\begin{aligned}(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) \quad &\text{and}\\ ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) \quad &\text{as expected.}\end{aligned}$$

Remark. We may therefore drop the brackets in function composition without ambiguity.

Definition 2.23 (Invertible function)

We say $f : A \to B$ is **invertible** if $\exists g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Example 2.24

Consider $f : \mathbb{R} \to \mathbb{R}$ with $x \mapsto 2x + 1$ and $g : \mathbb{R} \to \mathbb{R}$ with $x \mapsto \frac{x-1}{2}$.

Indeed, $\forall x \in \mathbb{R}$, $(g \circ f)(x) = g(2x + 1) = \frac{2x+1-1}{2} = x$, so $g \circ f = \mathrm{id}_{\mathbb{R}}$.

Similarly, $\forall x \in \mathbb{R}$, $(f \circ g)(x) = f((x - 1)2)) = 2\left(\frac{x-1}{2}\right) + 1 = x$, so $f \circ g = \mathrm{id}_{\mathbb{R}}$.

Hence f is invertible with inverse g.

Important. Consider $f : \mathbb{N} \to \mathbb{N}$ with $x \mapsto x + 1$, $g : \mathbb{N} \to \mathbb{N}$ with $x \mapsto \begin{cases} x-1 & x \neq 1 \\ 1 & x = 1 \end{cases}$.

We have $g \circ f = \mathrm{id}_{\mathbb{N}}$ but $f \circ g \neq \mathrm{id}_{\mathbb{N}}$ since $f \circ g(1) = 2$.

Proposition 2.25

$f : A \to B$ is invertible if and only if f is bijective. We write $f^{-1} : B \to A$ for the inverse of f.

Proof.

1. We shall first consider the necessary condition that, given $f : A \to B$, there is a map $g : B \to A$ such that $g \circ f = \mathrm{id}_A$.

   Necessary condition. If such a g were to exist, and $a, \overline{a} \in A$ such that $f(a) = f(\overline{a})$, then $g(f(a)) = g(f(\overline{a}))$. Hence $a = \overline{a}$. Thus f must be injective.

   Sufficient condition. Now let us consider the sufficient conditions. Conversely, if f is injective, we want to show that we can find g such that $g \circ f = \mathrm{id}_A$. Consider some $b \in B$.

   - If $b \in f(A)$. let $g(b) = a$, where a the unique element of A with $f(a) = b$.
   - If $b \notin f(a)$, then let $g(b)$ be anything in the set A.

   So we have constructed the required function g such that $g \circ f = \mathrm{id}_A$, and the condition of f being injective is sufficient.

2. We can take a step further to consider the conditions for f to be invertible, *i.e.* $f \circ g = \mathrm{id}_B$ as well.

   Necessary condition. We need $f(g(B)) = B$, so f must be surjective.

   Sufficient condition. Conversely, if f is surjective, we want to find $g : B \to A$ with $f \circ g = \mathrm{id}_B$. For each $b \in B$, pick some $a \in A$ with $f(a) = b$. This always exists due to surjectivity of f, and choose $g(b) = a$.

Note that our construction of g in the two parts are consistence. Hence, the result follows.

Remark. The preimage of a function always exists, but the inverse may not.

2.3 Relations

Definition 2.26 (Relation)

A **relation** on a set X is a subset $R \subseteq X \times X$.

We write aRb if $(a, b) \in \mathbb{R}$. We say that a and b are related by R.

Example 2.27 (Examples of relations on $\mathbb{N}$)

1. aRb if a, b share the same final digit
2. aRb if $a < b$
3. aRb if $a \neq b$
4. aRb if $a = b = 1$
5. aRb if $|a - b| \leqslant 3$

There are three properties of a relation that are of special interest.

Definition 2.28 (Relation reflexitivity, symmetry and transitivity)

A relation R on X is...

- **reflexive** if $\forall x \in X$, xRx.
- **symmetric** if $\forall x, y \in X$, $xRy \Rightarrow yRx$.
- **transitive** if $\forall x, y, z \in X$, $xRy \wedge yRz \Rightarrow xRz$.

Example 2.29

Let us do a property check over Definition 2.28 on the examples in Example 2.27.

Example #	1	2	3	4	5
Reflexive	✓	×	×	×	✓
Symmetric	✓	×	✓	✓	✓
Transitive	✓	✓	×	✓	×

Definition 2.30 (Equivalence relation)

A relation R is an **equivalence relation** if it is reflexive, symmetric and transitive.

We usually write $a \sim b$ for the case where aRb and R is an equivalence relation.

In Example 2.27, only (1) is an equivalence relation.

Example 2.31

Let $X = \{\text{IA students}\}$.

Let aRb if two students are born in the same month. Then R is an equivalence relation.

Note that, in the example above, the set X is divided into subsets consisting of related elements.

Lecture 6 · 2025-10-21

Definition 2.32 (Equivalence class)

If $\sim$ is an equivalence relation on X_1, then the **equivalence class** of $x \in X$ is denoted by

$$[x] = \{y \in X : y \sim x\}.$$

Definition 2.33 (Partition)

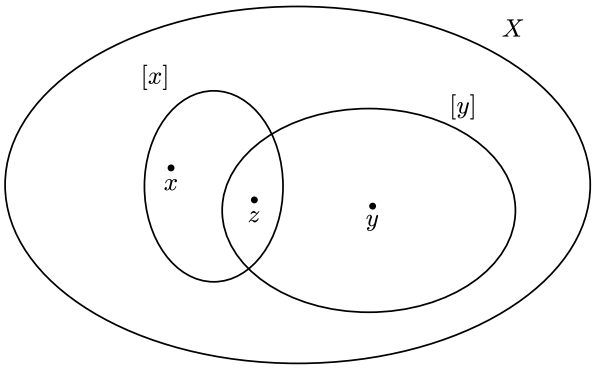
Given a set X, a **partition** of X is a collection of pairwise disjoint subsets whose union is X.

Theorem 2.34

Let $\sim$ be an equivalence relation on X. Then, the equivalence classes from a partition of X.

Proof. Since $\sim$ is reflexive, we have $x \in [x]$ for all $x \in X$. Thus $\bigcup_{x \in X} [x] = X$.

It remains to prove that $\forall x, y \in X$, either $[x] \cap [y] = \varnothing$ or $[x] = [y]$

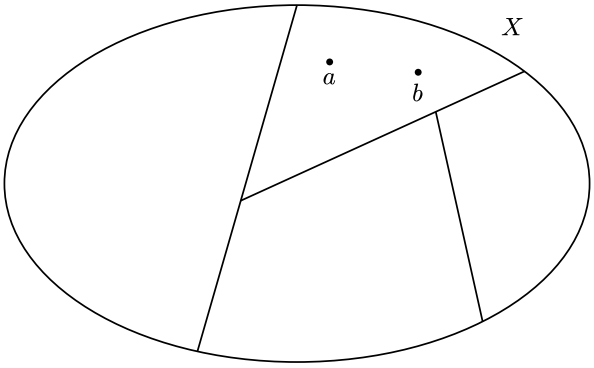


Suppose that $[x] \cap [y] \neq \varnothing$, and let $z \in [x] \cap [y]$. Then $z \sim x$, and so by symmetry, $x \sim z$, and $z \sim y$. By transitivity, $x \sim y$.

Let now $w \in [y]$, so $y \sim w$. Since $x \sim y$, by transitivity, $x \sim w$. Thus $w \in [x]$.

Hence if $[x] \cap [y] \neq \varnothing$ then $[y] \subseteq [x]$. By symmetry, we have $[x] \subseteq [y]$. Therefore, $[x] = [y]$.

Conversely, given any partition of X, there is an equivalence relation R whose equivalence classes are precisely the parts of the partition: just define aRb if a and b lie in the same part.



Definition 2.35

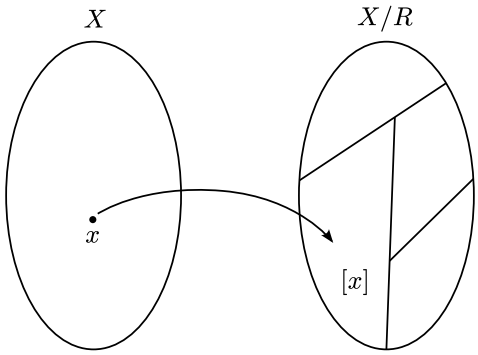
Given an equivalence relation R on a set X, the **quotient** X by R is

$$X/R = \{[x] : x \in X\}$$

e.g. in Example 2.27 (1), $X/R = \{[0], [1], ..., [9]\}$ with size 10.

Definition 2.36

The map $q : X \to X/R$ with $x \mapsto [x]$ is the **quotient map** or the **projection map**.



Example 2.37

On $\mathbb{Z} \times \mathbb{N}$ define $(a, b)R(c, d)$ if $ad = bc$. This is an equivalence relation, and note that

$$[(1, 2)] = \{(1, 2), (2, 4), (3, 6), ...\},$$

so we could regard $\mathbb{Z} \times \mathbb{N}/R$ as a copy of $\mathbb{Q}$ by identifying $[(a, b)]$ with $\frac{a}{b} \in \mathbb{Q}$.

The quotient map is $q : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{N}/\mathbb{R}$ where $(a, b) \mapsto \frac{a}{b}$.

Definition 2.38 (Binary operation)

A **binary operation** $*$ on a set A is a function $* : A \times A \to A$.

Example 2.39 (Examples of binary operations)

1. $+, \times$ on $\mathbb{N}, \mathbb{Z}, ...$
2. $-$ on $\mathbb{Z}, \mathbb{R}, ...$
3. $\div$ on $\mathbb{Q}^*, \mathbb{R}^*, ...$

Definition 2.40 (Commutativity, associativity and distributivity of binary operations)

We say a binary operation $*$ on A is

- **commutative** if $\forall x, y \in A$, $x * y = y * x$.

e.g. set intersection is commutative

- **associative** if $\forall x, y, z \in A$, $x * (y * z) = (x * y) * z$.
- **distributive** over $\odot$ if for another binary operation $\odot$, $\forall x, y, z \in A$, we have

$$x * (y \odot z) = (x * y) \odot (x * z)$$
$$(y \odot z) * x = (y * x) \odot (z * x).$$

e.g. $\times$ is distributive over $+$ on $\mathbb{R}$.

3 How to Count

3.1 Construction of $\mathbb{N}$

We shall construct $\mathbb{N}$ from a set of axioms.

The natural number $\mathbb{N}$ is a set containing a special element 1, together with a map, called the successor function:

$$S : \mathbb{N} \to \mathbb{N}$$

which maps n to its successor [intuitively, this is the "+1" operation.], such that it satisfies the following axioms.

Axiom 3.1 (Peano axioms)

1. $\forall n \in \mathbb{N}, S(n) \neq 1$ [1 is not the successor of anything.]
2. $\forall m, n \in \mathbb{N}$, $S(m) = S(n) \Rightarrow m = n$.
3. Let A be a subset of $\mathbb{N}$ such that
   - $1 \in A$, and
   - $n \in A \Rightarrow S(n) \in A$,

   then $A = \mathbb{N}$.

Note that Axiom 3.1 (3) is the axiom of induction. We can now write $2 = S(1)$, $3 = S(2)$ *etc.* Also, we can define addition recursively by

- $n + 1 = S(n)$
- $n + S(m) = S(n + m)$

Similarly for multiplication, we can define it by

- $n \times 1 = n$
- $n \times S(m) = n \times m + n$

We can show by induction that these satisfy the usual rules of arithmetic, that

- $+$ and $\times$ are commutative and associative
- $\times$ is distributive over $+$

Example 3.2

$$\begin{aligned} 1 + 2 &= 1 + S(1) \\ &= S(1 + 1) \\ &= S(S(1)) \\ &= S(1) + 1 \\ &= 2 + 1. \end{aligned}$$

Example 3.3

To prove that $n + m = m + n$, we will need to do the followings:

- induct on m
- base case is $m = 1$

i.e. $n + 1 = 1 + n$

- prove this by inclusion on n

Lecture 7 · 2025-10-23

3.2 Induction and Ordering

We can also define an ordering: $m < n$ if $m + k = n$ for some $k \in \mathbb{N}$. We may check by induction that the usual rules hold, *i.e.* transitivity holds.

A key feature of $<$ is that for any distinct $m, n \in \mathbb{N}$, exactly one of $m < n$ or $n < m$ holds. This is called a total order.

Example 3.4

We shall show that we cannot get $1 < 2$ and $2 < 1$ at the same time. If $1 < 2$ and $2 < 1$. Then $\exists k, l \in \mathbb{N}$ such that $1 = 2 + k$ and $2 = 1 + l$. By associativity we have

$$1 = 2 + k = 1 + l + k$$

Hence $1 = S(l + k)$. By Axiom 3.1 (1), this is a contradiction. ※

The fact that we have ordering means that we can write down two types of induction.

1. The **weak principle of induction** (WPI), which is just Axiom 3.1 (3):

   If $P(1)$ holds, and $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n + 1)$, then $P(n)$ holds $\forall n \in \mathbb{N}$.

2. The **strong principle of induction** (SPI) is based on the ordering above:

   If we are given that

   1. $P(1)$ holds,
   2. $\forall n \in \mathbb{N}$, $P(1) \wedge P(2) \wedge \ldots \wedge P(n) \Rightarrow P(n + 1)$,

   then $P(n)$ holds $\forall n \in \mathbb{N}$.

   > ***Remark.*** We need ordering since we are effectively saying that to prove $P(n + 1)$, we need $P(k)$ for all $k < n + 1$.

Proposition 3.5

SPI $\Leftrightarrow$ WPI.

> ***Proof.*** Let us first show that SPI implies WPI. We are given the assumptions:
>
> 1. **SPI.** If $P(1)$ holds, and $\forall n \in \mathbb{N}$, $P(1) \wedge P(2) \wedge \ldots \wedge P(n) \Rightarrow P(n + 1)$, then $P(n)$ holds $\forall n \in \mathbb{N}$.
> 2. **WPI's assumption.** $P(1)$ holds, and $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n + 1)$.

We can use (2) to show that $P(1)$ holds. Then using (2) again, we can show that $P(1) \wedge P(2)$ holds. Continuing this way, we can show that $P(1) \wedge P(2) \wedge \ldots \wedge P(n)$ holds for all $n \in \mathbb{N}$. Hence by (1), $P(n)$ holds for all $n \in \mathbb{N}$, and WPI holds.

Conversely, to see that WPI implies SPI, we define a new predicate $Q(n)$ as "$P(k)$ holds for all $k < n$". Then we can use WPI to show that $Q(n)$ holds for all $n \in \mathbb{N}$, which implies that $P(n)$ holds for all $n \in \mathbb{N}$.

The above ordering of $\mathbb{N}$ satisfies a special property called the **well-ordering principle** (WOP).

Axiom 3.6 (Well-ordering principle)

Any non-empty subset of $\mathbb{N}$ has a least element.

i.e. if $P(n)$ holds for $n \in A \subset \mathbb{N}$ with $A \neq \varnothing$, then there exists a least element $m \in A$ such that $P(m)$ holds.

Theorem 3.7

SPI $\Rightarrow$ WOP.

Proof. Assume that $P(n)$ holds for $n \in A \subset \mathbb{N}$ with $A \neq \varnothing$. Suppose, for contradiction, that there is no least $n \in \mathbb{N}$ such that $P(n)$ holds. Consider $Q(n) = \neg P(n)$.

Certainly $P(1)$ is false, because otherwise 1 will be our minimal element. Then $Q(1)$ holds.

Now, given $n \in \mathbb{N}$, suppose $Q(k)$ is true for all $k < n$. Then $P(k)$ must be false for all $k < n$, and so $P(n)$ must also be false (otherwise n will be our minimal element). Hence $Q(n)$ holds.

Hence by SPI, $Q(n)$ holds for all $n \in \mathbb{N}$, and $P(n)$ is false for all $n \in \mathbb{N}$, contradicting our assumption that there exists some n such that $P(n)$ holds. ※

Remark. WOP $\nRightarrow$ SPI, and it fails for certain ordinals. However, in any proof using SPI, one can in fact use WOP.

Example 3.8

Consider the following theorem.

Any natural number $n > 1$ can be written as a product of primes.

> ***Proof.*** Let $C = \{n \in \mathbb{N} : n > 1 \wedge$ n cannot be written as a product of primes$\}$.
>
> We assume $C \neq \varnothing$ and derive a contradiction. By WOP, C has a least element m. Since m is not prime, we can write $m = a \times b$ for some $a, b \in \mathbb{N}$ with $1 < a, b < m$. By minimality of m, both a and b can be written as a product of primes. Hence m can also be written as a product of primes, which is a contradiction. ※

3.3 Finite Sets

Recall a set A has **size** n if we can write $A = \{a_1, a_2, ..., a_n\}$ with the elements a_i distinct. We write $|A| = n$ or $\#A = n$.

Let us recall the definition of finite sets in Definition 2.10. We say A is finite if $\exists n \in \mathbb{Z}_{\geqslant 0}$ such that $|A| = n$, and A is infinite otherwise.

Proposition 3.9

A set of size n has exactly 2^n subsets.

Proof. We shall prove by induction on n.

Base case. This is true for $n = 0$ since the empty set has exactly one subset, itself.

Inductive step. Suppose the result holds for some $n \in \mathbb{N}$. Let A be a set of size $n+1$. Pick some element $a \in A$, and let $B = A \setminus \{a\}$. Then B has size n, and by the inductive hypothesis, B has exactly 2^n subsets.

Now, to form the subsets of A, we can take each subset of B and either include or exclude a. This gives us exactly two choices for each subset of B, leading to a total of $2 \times 2^n = 2^{n+1}$ subsets of A.

Hence, by induction, the result holds for all $n \in \mathbb{N}$.

So this proposition says that if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

3.3.1 Binomial Coefficients

Definition 3.10 (Binomial coefficient)

Given $n \in \mathbb{N}_0$, and $0 \leqslant k \leqslant n$, we can write $\binom{n}{k}$ for the number of subsets of an n-element set that are of size k.

$\binom{n}{k}$ is called a **binomial coefficient**.

In other words,

$$\binom{n}{k} = |\{S \subseteq \{1, 2, ..., n\} : |S| = k\}|.$$

Note that, by definition, $\binom{n}{0} = 1, \binom{n}{n} = 1, \binom{n}{1} = n$ for $n > 0$. Also,

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} = 2^n$$

since this counts all subsets of an n-element set.

Also we have $\binom{n}{k} = \binom{n}{n-k}$ forall $n \in \mathbb{Z}_{\geqslant 0}, 0 \leqslant k \leqslant n$. This is because specifying which k elements to pick is equivalent to specifying which $n - k$ elements to leave out.

Moreover,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad \forall n \in \mathbb{Z}^+, 1 \leqslant k \leqslant n-1.$$

Example 3.11

Consider

$$\binom{8}{3} = \binom{7}{2} + \binom{7}{3}.$$

Suppose that you are in a group of 8 people. To form a commitee of 3 people, either you are in the commitee, in which case you need to choose 2 more people from the remaining 7, or you are not in the commitee, in which case you need to choose all 3 people from the remaining 7.

Lecture 8 · 2025-10-25

This leads to Pascal's triangle:

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \\ 1 & 4 & & 6 & & 4 & 1 \\ 1 & 5 & 10 & & 10 & 5 & 1 \end{array}$$

where each row starts and ends with a 1, and the remaining entries are the sum of the 2 terms immediately above.

Proposition 3.12

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

Proof. Given a set of size n, there are $n(n-1)\cdots(n-k+1)$ to pick k elements, in order, one by one. But each subset of size k is picked in $k!$ ways in this method.

Hence, the number of subsets of size k in $\{1, 2, \ldots, n\}$ is

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

Note that the formula tells us, for example, that

$$\binom{n}{2} = \frac{n(n-1)}{2} \sim \frac{n^2}{2}$$
$$\binom{n}{3} = \frac{n(n-1)(n-2)}{6} \sim \frac{n^3}{6}$$

for large n.

Theorem 3.13 (Binomial theorem)

For all $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$, we have

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.$$

Proof. When we expand $(a+b)^n = (a+b)(a+b)\cdots(a+b)$, we obtain terms of the form $a^{n-k}b^k$ where $0 \leqslant k \leqslant n$, and the number of terms of the form $a^{n-k}b^k$ in the expansion is $\binom{n}{k}$, since we must specify k brackets from which to pick b.

Hence

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

Example 3.14

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{2}x^2 + \binom{n}{3}x^3 + \ldots + \binom{n}{n-1}x^{n-1} + x^n.$$

Thus, for a small x, a good approximation to $(1+x)^n$ is $1+nx$. [This is called the first-order approximation.]

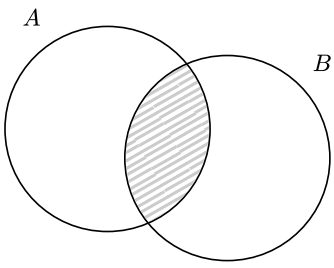
3.3.2 Inclusion-Exclusion Principle

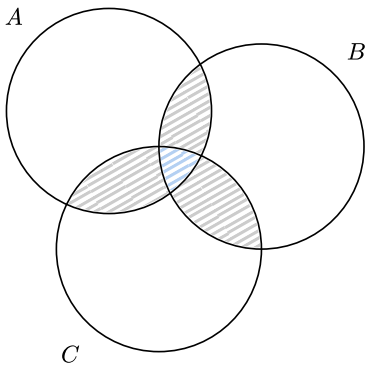
What can we say about the relationship between sizes of union and intersection of finite sets?

Example 3.15

One should have seen the following formulae before:

$$\begin{aligned} |A \cup B| = {} & |A| + |B| - |A \cap B|, \\ |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & -|A \cap B| - |B \cap C| - |C \cap A| \\ & +|A \cap B \cap C|. \end{aligned}$$





Theorem 3.16 (Inclusion-Exclusion Principle)

Let $S_1, S_2, \ldots, S_n$ be finite sets. Then

$$\begin{aligned}|S_1 \cup S_2 \cup \ldots \cup S_n| &= \sum_{i=1}^{n} |S_i| \\ &\quad - \sum_{1 \leqslant i < j \leqslant n} |S_i \cap S_j| \\ &\quad + \sum_{1 \leqslant i < j < k \leqslant n} |S_i \cap S_j \cap S_k| \\ &\quad \vdots \\ &\quad + (-1)^{n+1} |S_1 \cap S_2 \cap \ldots \cap S_n|.\end{aligned}$$

Equivalently,

$$\left|\cup_{i=1}^{n} S_i\right| = \sum_{r=1}^{n} (-1)^{r+1} \sum_{\substack{A \subseteq \{1,2,\ldots,n\} \\ |A|=r}} \left|\bigcap_{i \in A} S_i\right|.$$

Remark. This can be proven using indicator functions, using that if $A \subseteq X$ then

$$|A| = \sum_{x \in X} 1_{A(x)}.$$

Proof. Let $x \in S_1 \cup S_2 \cup \ldots \cup S_n$, say $x \in S_i$ for k of the sets S_i. We want x to be counted exactly once in the RHS.

Indeed, if $A \subseteq \{1, 2, 3, \ldots, n\}$,

$$\begin{aligned}\#\left\{A : |A| = 1 \wedge x \in \bigcap_{i \in A} S_i\right\} &= \binom{k}{1} \\ \#\left\{A : |A| = 2 \wedge x \in \bigcap_{i \in A} S_i\right\} &= \binom{k}{2} \\ \#\left\{A : |A| = 3 \wedge x \in \bigcap_{i \in A} S_i\right\} &= \binom{k}{3} \\ &\vdots \\ \#\left\{A : |A| = r \wedge x \in \bigcap_{i \in A} S_i\right\} &= \begin{cases}\binom{k}{r} & \text{for } r \leqslant k \\ 0 & \text{for } r > k\end{cases}.\end{aligned}$$

Thus the number fo times x is counted on the RHS is

$$
\begin{aligned}
& k - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \ldots + (-1)^{k+1}\binom{k}{k} \\
&= 1 - (1 - k + \binom{k}{2} - \binom{k}{3} + \ldots + (-1)^{k}\binom{k}{k}) \\
&= 1 - (1 - 1)^{k} \\
&= 1 \quad \text{for } k \geqslant 1.
\end{aligned}
$$

4 Elementary Number Theory

4.1 Primes

Given $a, b \in \mathbb{Z}$, we say "a divides b" if $\exists c \in \mathbb{Z}$ such that $b = ac$. We write $a \mid b$.

For any $b \in \mathbb{Z}$, ± 1 and $\pm b$ are always factors; all other factors are called **proper factors**.

Definition 4.1 (Prime and Composite Numbers)

A natural number $n \geqslant 2$ is prime if its only factors are ± 1 and $\pm n$. If $n \geqslant 2$ is not prime, it is called **composite**.

Lecture 9 · 2025-10-28

Proposition 4.2

Every natural number $n > 1$ can be written as a product of primes.

Proof. We will prove by induction on n.

Base case. The statement is true for $n = 2$.

Inductive step. Let $n > 2$ and suppose that the claim holds for all natural numbers $2 \leqslant k \leqslant n - 1$. If n is prime, we are done. Otherwise, n is composite, so there exists $a, b \in \mathbb{N}$ such that $n = ab$ and $1 < a, b < n$. By the inductive hypothesis, both a and b can be written as a product of primes. Thus, n can also be written as a product of primes.

Theorem 4.3

There are infinitely many prime numbers.

Proof. Suppose there are finitely many primes, say $p_1, \ldots, p_k$. Consider $N = p_1 p_2 \ldots p_k + 1$. Then $p_1 \nmid N$, or otherwise p_1 would divide 1. Likewise, none of $p_2, \ldots, p_k$ divide N. Thus, either N is prime itself, or it has a prime factor not in the list $p_1, \ldots, p_k$. In either case, we have a contradiction. ※

One may naturally wonder if all numbers can be written in only one way as a product of primes (up to ordering). This is indeed the case, as we shall see later.

Proposition 4.4 (Euclid's Lemma)

If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

4.2 Highest Common Factor

Definition 4.5 (Highest Common Factor)

Given $a, b \in \mathbb{N}$, a natural number c is the **highest common factor** or the **greatest common divisor** of a and b if

1. $c \mid a$ and $c \mid b$;
2. for any $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$, we have $d \mid c$.

We write $c = \text{hcf}(a, b)$ or $c = \gcd(a, b)$.

Example 4.6

The factors of 12 are $1, 2, 3, 4, 6, 12$. The factors of 18 are $1, 2, 3, 6, 9, 18$.

Thus, the common factors of 12 and 18 are $1, 2, 3, 6$, and the highest common factor is 6. Therefore, $\gcd(12, 18) = 6$.

We will need to show that the highest common factor always exists.

Proposition 4.7 (Division algorithm)

Given $n, k \in \mathbb{N}$, we can write $n = qk + r$, where $q, r \in \mathbb{Z}$ with $0 \leqslant r \leqslant k - 1$. [We are using q and r to denote the quotient and remainder respectively.]

Proof. We will prove this by induction on n.

Base case. The statement is true for $n = 1$.

Inductive step. For $n \geqslant 2$, suppose the statements holds for all natural numbers $1 \leqslant m \leqslant n - 1$. We want to show that it also holds for n. *i.e.* $n - 1 = qk + r$ for some $q, r \in \mathbb{Z}$ with $0 \leqslant r \leqslant k - 1$.

If $r < k - 1$, then $n = (n - 1) + 1 = qk + (r + 1)$.

Otherwise, if $r = k - 1$, then $n = (n - 1) + 1 = (q + 1)k + 0$.

Thus, in either case, we have expressed n in the desired form.

Note that q and r thus obtained are unique: if $n = qk + r = q'k + r'$, then $(q - q')k = r' - r$. Since $0 \leqslant r, r' \leqslant k - 1$, we have $-(k - 1) \leqslant r' - r \leqslant k - 1$. The only multiple of k in this range is 0, so $r' = r$ and hence $q' = q$.

4.3 Euclid's Algorithm

INPUT	a, b	$a = 372 \quad b = 162$
STEP 1	$a = q_1 b + r_1$ with $q_1, r_1 \in \mathbb{Z}, 0 \leqslant r_1 \leqslant b - 1$	$372 = 2 \times 162 + 48$
STEP 2	$b = q_2 r_1 + r_2$ with $0 \leqslant r_2 \leqslant r_1 - 1$	$162 = 3 \times 48 + 18$
STEP 3	$r_1 = q_3 r_2 + r_3$ with $0 \leqslant r_3 \leqslant r_2 - 1$	$48 = 2 \times 18 + 12$
STEP n	$r_{n-2} = q_n r_{n-1} + r_n$ with $0 \leqslant r_n \leqslant r_{n-1} - 1$	$18 = 1 \times 12 + 6$
STEP $n + 1$	$r_{n-1} = q_{n+1} r_n + r_{n+1}$ with $r_{n+1} = 0$	$12 = 2 \times 6 + 0$
OUTPUT	r_n	6

Note that the algorithm terminates in $n < b$ steps, since $b > r_1 > r_2 > \ldots > r_n > 0$.

Theorem 4.8

The output of Euclid's algorithm with input (a, b) is $\gcd(a, b)$.

Proof.

1. We have $r_n \mid r_{n-1}$ as $r_{n-1} = q_{n+1} r_n + 0$. Back-substituting, we get r_n divides r_{n-2}, and continuing inductively, we find that r_n divides both a and b.
2. Given d such that $d \mid a$ and $d \mid b$. Thence we have $d \mid r_1$ as $r_1 = a - q_1 b$. Back-substituting, we get d divides r_2, and continuing inductively, we find that d divides r_n.

Example 4.9

We want $\gcd(87, 52)$. We run Euclid's algorithm:

$$\begin{aligned} 87 &= 1 \times 52 + 35 \\ 52 &= 1 \times 35 + 17 \\ 35 &= 2 \times 17 + 1 \\ 17 &= 17 \times 1 + 0 \end{aligned}$$

The answer is the last non-zero remainder. Thus, $\gcd(87, 52) = 1$.

Lecture 10 · 2025-10-30

Remark. When $\gcd(a, b) = 1$, we say that a and b are **coprime**.

We can reverse the steps of Euclid's algorithm to express the highest common factor as a linear combination of a and b.

Example 4.10

Continuing from the previous example, we have

$$\begin{aligned} 1 &= 35 - 2 \times 17 \\ &= 35 - 2 \times (52 - 1 \times 35) \\ &= 3 \times 35 - 2 \times 52 \\ &= 3 \times (87 - 1 \times 52) - 2 \times 52 \\ &= 3 \times 87 - 5 \times 52 \end{aligned}$$

Thus, we have expressed $\gcd(87, 52) = 1$ as a linear combination of 87 and 52.

This reversal procedure leads to the following important result.

Theorem 4.11 (Bézout's theorem)

Given $a, b \in \mathbb{N}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. *i.e.* we can write the highest common factor of a and b as a linear combination of a and b.

Proof 1. We can run Euclid's algorithm with inputs a, b to obtain an output r_n. Then we have $r_n = xr_{n-1} + yr_{n-2}$ for some $x, y \in \mathbb{Z}$.

But from step $n-1$ we see that r_{n-1} is expressible as a linear combination of r_{n-2} and r_{n-3}. Substituting this into the previous equation, we can express r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing inductively, we can write, for some $x, y \in \mathbb{Z}$,

$$r_n = xr_i + yr_{i-1}$$

for all $1 \leqslant i \leqslant n-1$. In particular,

$$r_n = xb + ya.$$

for some $x, y \in \mathbb{Z}$, by step 1 and 2.

Remark. Euclid's algorithm does not only prove the existsence of such x, y, but also provides a method to compute them.

Proof 2. Let h be the least positive linear combination of a and b, *i.e.* the smallest positive integer of the form $h = ax + by$ for some $x, y \in \mathbb{Z}$. We will show that $h = \gcd(a, b)$. We shall prove the two conditions in Definition 4.5.

To show (2), observe that given d such that $d \mid a$ and $d \mid b$, we have $d \mid ax + by$ for all $x, y \in \mathbb{Z}$. In particular, $d \mid h$.

To show (1), suppose that $h \nmid a$. Then we can write $a = qh + r$ for some $q, r \in \mathbb{Z}$ ans $0 < r < h$. Hence $r = a - qh = a - q(xa + yb)$ is also a positive linear combination of a and b, contradicting the minimality of h. Thus, $h \mid a$. Similarly, we can show that $h \mid b$.

Therefore, $h = \gcd(a, b)$.

Remark. Proof 2 tells us that $\gcd(a, b)$ exists and is a linear combination of a and b, but it gives no method to compute it.

Example 4.12

Consider whether we have integer solutions to the equation

$$87x + 52y = 33.$$

Since $\gcd(87, 52) = 1$ divides 33, by Bézout's identity, we can write $87x' + 52y' = 1$ for some $x', y' \in \mathbb{Z}$, and thus $87(33x') + 52(33y') = 33$. Therefore, integer solutions do exist.

Corollary 4.13 (Bézout's identity, continued)

Let $a, b \in \mathbb{N}$. Then the equation $ax + by = c$ has a solution with $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$.

Proof.

$[\Rightarrow]$ Let $h = \gcd(a, b)$. Suppose that there are $x, y \in \mathbb{Z}$ such that $ax + by = c$. Since $h \mid a$ and $h \mid b$, we have $h \mid (ax + by) = c$.

[⇐] Conversely, suppose $h \mid c$. By Bézout's identity, there exist $x', y' \in \mathbb{Z}$ such that $ax' + by' = h$. Thus, $a\left(\frac{c}{h}x'\right) + b\left(\frac{c}{h}y'\right) = c$, giving a solution.

Recall Proposition 4.4. We shall now prove it.

Proof. [For Proposition 4.4]

Suppose $p \mid ab$ but $p \nmid a$. We wish to show that $p \mid b$. Since p is prime and $p \nmid a$, we have $\gcd(p, a) = 1$. By Bézout's identity, there exist $x, y \in \mathbb{Z}$ such that $px + ay = 1$. Multiplying both sides by b, we get $p(xb) + a(yb) = b$. Since $p \mid ab$ and $p \mid pxb$, we have $p \mid b$.

The other case is similar.

Remark.

1. Similarly $p \mid a_1 a_2 ... a_n \Rightarrow p \mid a_i$ for some $i = 1, 2, ..., n$, by induction on n.
2. The statement is false if p is not prime. For example, $6 \mid 2 \times 3$, but $6 \nmid 2$ and $6 \nmid 3$.

Theorem 4.14 (Fundamental theorem of arithmetic)

Every natural number $n \geqslant 2$ can be written uniquely (up to ordering) as a product of primes.

Proof. The existence of factorisation follows from Proposition 4.2. To show uniqueness, we will use induction on n.

Base case. The statement is true for $n = 2$.

Inductive step. Let $n > 2$ and suppose the statement holds for all natural numbers $2 \leqslant k \leqslant n - 1$. Suppose that $n = p_1 p_2 ... p_k = q_1 q_2 ... q_l$ where p_i, q_j are all primes. We want to prove that $k = l$ and, after reordering, $p_i = q_i$ for all $1 \leqslant i \leqslant k$.

Hence $p_1 \mid n = q_1 ... q_l$. By Proposition 4.4, $p_1 \mid q_j$ for some $1 \leqslant j \leqslant l$. Since q_j is prime, we have $p_1 = q_j$. Without loss of generality, let $j = 1$. Cancelling $p_1 = q_1$ from both sides, we get $p_2 ... p_k = q_2 ... q_l$, which is a natural number less than n. By the inductive hypothesis, we have $k - 1 = l - 1$ and, after reordering, $p_i = q_i$ for all $2 \leqslant i \leqslant k$. Thus, the result holds for n.

Lecture 11 · 2025-11-01

Remark. There are "arithmetic systems" (permitting $+$ and $\times$) in which factorisation is not unique.

Example 4.15

Consider $\mathbb{Z}\left[\sqrt{-3}\right]$, which is the set of all numbers of the form $a + b\left(\sqrt{-3}\right)$ where $a, b \in \mathbb{Z}$. We can define addition and multiplication as usual. For example,

$$\left(1 + \sqrt{-3}\right) + \left(1 - \sqrt{-3}\right) = 2 + 0 = 2$$

$$\left(1 + \sqrt{-3}\right) \times \left(1 - \sqrt{-3}\right) = 1 - (-3) = 4.$$

In $\mathbb{Z}\left[\sqrt{-3}\right]$ we can define what it means to be a "prime", and both $1 \pm \sqrt{-3}$ happens to be primes in this sense. However, we can also write 4 as $4 = 2 \times 2$, so the factorisation is not unique.

We shall consider some applications of the fundamental theorem of arithmetic.

1. The factors of $n = 2^3 \cdot 3^7 \cdot 11$ are all numbers of the form $2^a 3^b 11^c$ where $0 \leqslant a \leqslant 3$, $0 \leqslant b \leqslant 7$ and $0 \leqslant c \leqslant 1$. We can show that there are others: if, for example, $7 \mid n$, then we would have a factorisation of n involving 7, contradicting the uniqueness of factorisation.

   More generally, the factors of $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ are all numbers of the form $p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ where $0 \leqslant b_i \leqslant a_i$ for all $1 \leqslant i \leqslant k$.

2. The common factors of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$ are all numbers of the form $2^a 3^b 11^c$ where $0 \leqslant a \leqslant 3$, $0 \leqslant b \leqslant 2$ and $0 \leqslant c \leqslant 1$. Thus, the highest common factor is $2^3 \cdot 3^2 \cdot 11$.

   More generally, if $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ with $a_i, b_i \geqslant 0$ for all $1 \leqslant i \leqslant k$, then $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_k^{\min(a_k, b_k)}$.

3. The common multiples of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$ are all numbers of the form $2^a 3^b 5^c 11^d 13^e k$ where $a \geqslant 4$, $b \geqslant 7$, $c \geqslant 1$, $d \geqslant 3$, $e \geqslant 1$ and k is any integer. Thus, the lowest common multiple is $2^4 \cdot 3^7 \cdot 5 \cdot 11^3 \cdot 13$.

   More generally, if $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ with $a_i, b_i \geqslant 0$ for all $1 \leqslant i \leqslant k$, then $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_k^{\max(a_k, b_k)}$.

4. We have another proof of infinite prime numbers due to Erdös.

   > ***Proof.*** Let $p_1, p_2, \ldots, p_k$ be all the primes. Since any number is uniquely expressed as a product of primes, consider $p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$ where $j_i \geqslant 0$ for all $1 \leqslant i \leqslant k$.
   >
   > We can rewrite this in the following form:
   >
   > $$p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k} = m^2 \times p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$$
   >
   > where $i_i \in \{0, 1\}$ for all $1 \leqslant i \leqslant k$, and m is some integer.
   >
   > Let $N \in \mathbb{N}$. Given a number less than or equal to N in the form above, we must have $m \leqslant \sqrt{N}$, so there are at most $\sqrt{N} 2^k$ numbers of the form less than or equal to N.
   >
   > If $N > \sqrt{N} 2^k$, *i.e.* $N > 4^k$, there must be a number less than or equal to N that is not of the form above. So this number must have a prime factor not in the list $p_1, p_2, \ldots, p_k$, giving a contradiction.

   Note that Euclid's proof tells us that the kth prime is $< 2^{2^k}$ whereas Erdös' proof tells us that the kth prime is $< 4^k$. In fact, we know that the kth prime is approximately $k \log k$ for large k (the prime number theorem), which is a much stronger result.

4.4 Modular Arithmetic

Definition 4.16 (Integer Modulo n)

Let $n \geqslant 2$ be a natural number. Then the **integer modulo n**, denoted $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$, is the set of integers with two integers regarded as the same if they differ by a multiple of n. More precisely, we say that $a, b \in \mathbb{Z}$ are congruent modulo n, written $a \equiv b \bmod n$, if $n \mid (a - b)$.

We have $x \equiv y \bmod n \Leftrightarrow n \mid x - y \Leftrightarrow x = y + kn$ for some $k \in \mathbb{Z}$.

Note that we can view $\mathbb{Z}_n$ as a circular loop of integers $0, 1, 2, \ldots, n-1$, where after $n-1$ we return to 0.

Remark. If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $n \mid (a - a') + (b - b')$ so $a + b \equiv a' + b' \bmod n$. Similarly, $ab \equiv a'b' \bmod n$.

Example 4.17

Consider whether $2a^2 + 3b^3 = 1$ has a solution with $a, b \in \mathbb{Z}$. If there is a solution, then $2a^2 \equiv 1 \bmod 3$, but $2a^2$ can only be 0 or 2 modulo 3 since $a^2 \equiv 0$ or $1 \bmod 3$. Thus, there are no integer solutions.

Lecture 12 · 2025-11-04

4.5 Solving Congruences

We cannot divide both sides of a congruence by an integer in general. Thus, we need other methods to solve congruences.

Example 4.18

Consider the equation $7x \equiv 2 \bmod 10$.

Note that $3 \cdot 7 \equiv 1 \bmod 10$, so $3 \cdot 7x \equiv 3 \cdot 2 \bmod 10$, and so $x \equiv 6 \bmod 10$ since $3 \cdot 7 \equiv 1 \bmod 10$.

Definition 4.19 (Inverse and Unit Modulo n)

Given $a, b \in \mathbb{Z}$, we say that b is an **inverse of a modulo n** if $ab \equiv 1 \bmod n$.

We say that a is **invertible modulo n**, or that a is a **unit** modulo n, if such a b exists.

Example 4.20

In $\mathbb{Z}_{10}$, 3 is an inverse of 7. Hence, both 3 and 7 are units modulo 10.

But 4 is not a unit modulo 10 since there is no integer b such that $4b \equiv 1 \bmod 10$.

Remark. If a is a unit modulo n, then

1. its inverse is unique: suppose $\exists b, b'$ such that $ab \equiv ab' \equiv 1 \bmod n$. Then

$$b \equiv b(ab) \equiv b(ab') \equiv (ba)b' \equiv b.$$

2. We can write a^{-1} for its inverse.
3. If $ab \equiv ac \bmod n$, then $b \equiv c \bmod n$. *i.e.* we can cancel units, by multiplying both sides by their inverses.

> ***Important.*** This is not true in general. Consider $4 \cdot 3 \equiv 4 \cdot 8 \bmod 10$. Certainly $3 \not\equiv 8 \bmod 10$.

Proposition 4.21

Let p be prime. Then every $a \not\equiv 0 \bmod p$ is a unit modulo p.

Proof. We have $\gcd(a, p) = 1$. By Theorem 4.11 (Bézout's theorem), there exist $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Thus, $ax \equiv 1 \bmod p$, so x is an inverse of a modulo p.

We can rephrase this proposition more generally.

Proposition 4.22

Let $n \geqslant 2$. Then a is a unit modulo n if and only if $\gcd(a, n) = 1$.

Proof.

$$\begin{aligned} \gcd(a, n) = 1 &\Leftrightarrow ax + ny = 1 \quad \text{for some } x, y \in \mathbb{Z} \\ &\Leftrightarrow ax \equiv 1 \bmod n \\ &\Leftrightarrow a \text{ is a unit modulo } n. \end{aligned}$$

Corollary 4.23

If $\gcd(a, n) = 1$, then the congruence $ax \equiv b \bmod n$ has a unique solution. In particular, if $\gcd(a, n) = 1$, there is a unique inverse of a modulo n.

Example 4.24 (Diophantine equations)

Consider whether "New Year's Day" can fall on any day of the week in a year. [Assume a year has 365 days and a week has 7 days.]

Since $\gcd(365, 7) = 1$, so if we put "New Year's Day" as day 0, and our week has 7 days in it, then we need to solve

$$7x \equiv 365y + k.$$

i.e. $365x \equiv k \bmod 7$, which has a unique solution for all $k \in \{0, 1, 2, 3, 4, 5, 6\}$. Thus, "New Year's Day" can fall on any day of the week.

We shall now consider equations of the form $ax \equiv b \bmod n$ with $\gcd(a, n) \neq 1$, say $\gcd(a, n) = d > 1$.

Proposition 4.25

If $\gcd(a,n) = d > 1$, the congruence $ax \equiv b \bmod n$ has no solution if $d \nmid b$, and otherwise the solutions are exactly $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}$.

Proof. Suppose a x equiv b mod n.Then $n \mid ax - b$, and so $d \mid ax - b$ and $d \mid a$. So if there is a solution, we must have $d \mid b$.

Conversely, if $d \mid b$, then $n = d \cdot n'$, $a = d \cdot a'$, and $b = d \cdot b'$, and the equation is

$$\begin{aligned} ax \equiv b \bmod n &\Leftrightarrow ax - b = kn \quad \text{for some } k \in \mathbb{Z} \\ &\Leftrightarrow da'x - db' = kdn' \\ &\Leftrightarrow a'x - b' = kn' \\ &\Leftrightarrow a'x \equiv b' \bmod n'. \end{aligned}$$

Note that $\gcd(a', n') = 1$. Thus, by the previous corollary, there is a unique solution modulo n' to this equation.

So if $\gcd(a,n) = d > 1$, the congruence $ax \equiv b \bmod n$ has no solution if $d \nmid b$, and otherwise the solutions are exactly $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}$.

Example 4.26

1. Consider the equation $7x \equiv 4 \bmod 30$. Hence $\gcd(7, 30) = 1$, so by Bézout's theorem,

   $$13 \cdot 7 - 3 \cdot 30 = 1.$$

   Thus $13 \cdot 7 \equiv 1 \bmod 30$, and thus $x \equiv 13 \cdot 4 \bmod 30$.

   Let us check the uniqueness of the solution. Suppose $7x' \equiv 4 \bmod 30$. Then $7(x - x') \equiv 0 \bmod 30$. Since $\gcd(7, 30) = 1$, 7 is a unit modulo 30, and so $x \equiv x' \bmod 30$.

   Short form. This might be helpful in tackling problems:

   $$\begin{aligned} & 7x \equiv 4 \bmod 30 \\ \Leftrightarrow\ & 13 \cdot 7x \equiv 13 \cdot 4 \bmod 30 \quad \text{backwards implication since 13 is a unit mod 30} \\ \Leftrightarrow\ & x \equiv 22 \bmod 30 \end{aligned}$$

2. Consider $10x \equiv 12 \bmod 34$:

   $$\begin{aligned} 10x \equiv 12 \bmod 34 &\Leftrightarrow 10x = 12 + 34k \quad \text{for some } k \in \mathbb{Z} \\ &\Leftrightarrow 5x = 6 + 17k \\ &\Leftrightarrow 5x \equiv 6 \bmod 17 \end{aligned}$$

   ans so we reduce to the case of example (1).

4.6 Solving Simultaneous Congruence

Consider this old Chinese problem:

How many soldiers are there in Han Xin's army, if you let them parade in rows of 3, 2 are left; and if you let them parade in rows of 4, 1 is left?

This is equivalent to solving the simultaneous congruences

$$\begin{cases} x \equiv 2 \bmod 3 \Rightarrow x \equiv 2, 5, 8, \dots \\ x \equiv 1 \bmod 4 \Rightarrow x \equiv 1, 5, 9, \dots \end{cases}$$

so $x = 5$ is a solution.

Now consider another case:

$$\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 2 \bmod 6 \end{cases}$$

This simultaneous congruence has no solution since $x \equiv 2 \bmod 6$ implies that x is even, but $x \equiv 1 \bmod 4$ implies that x is odd.

Now let us consider the general case.

Theorem 4.27 (Chinese remainder theorem)

Let m, n be coprime, and $a, b \in \mathbb{Z}$. Then there is a unique solution modulo mn to the simultaneous congruences

$$\begin{aligned} x &\equiv a \bmod m, \\ x &\equiv b \bmod n. \end{aligned}$$

i.e. y is another solution if and only if $x \equiv y \bmod(mn)$.

Lecture 13 · 2025-11-06

Proof.

[Existence.] Since $\gcd(m, n) = 1$, by Bézout's theorem, there exist $s, t \in \mathbb{Z}$ such that $sm + tn = 1$.

Note that

$$\begin{aligned} sm &\equiv 1 \bmod n \quad \text{and} \quad tn \equiv 1 \bmod m \\ sm &\equiv 0 \bmod m \quad \text{and} \quad tn \equiv 0 \bmod n. \end{aligned}$$

Hence

$$x = a(tn) + b(sm) \equiv a \bmod n \equiv b \bmod m.$$

[Uniqueness.] Suppose y is another solution. *i.e.*

$$\begin{aligned} & y \equiv a \bmod m && \text{and} \quad y \equiv b \bmod n \\ \Leftrightarrow\ & y \equiv x \bmod m && \text{and} \quad y \equiv x \bmod n \\ \Leftrightarrow\ & m \mid y - x && \text{and} \quad n \mid y - x \\ \Leftrightarrow\ & mn \mid y - x && \text{since} \quad \gcd(m, n) = 1 \\ \Leftrightarrow\ & y \equiv x \bmod mn. \end{aligned}$$

Remark. The Chinese remainder theorem can be generalised to more than two moduli by induction.

If $m_1, m_2, \dots, m_k$ are pairwise coprime, then the simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \bmod m_1, \\ x &\equiv a_2 \bmod m_2, \\ &\vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

has a unique solution modulo $m_1 m_2 ... m_k$.

4.7 Prime Modular Arithmetic

Definition 4.28 (Euler Totient Function)

Let $m \geqslant 2$ be a natural number.

We denote by $\varphi(m)$ the number of integers a with $1 \leqslant a \leqslant m$ such that $\gcd(a, m) = 1$. That is, $\varphi(m)$ is counting the number of units modulo m.

φ is called the **Euler totient function**.

Example 4.29

1. $\varphi(9) = 6$
2. When p is prime, $\varphi(p) = p - 1$, and $\varphi\left(p^2\right) = p^2 - p$.
3. When p, q are distinct primes, we have $\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1)$, where we are counting the numbers not divisible by either p or q.

We shall now consider the behaviour of an integer power modulo n.

Example 4.30

- Consider 2^n modulo 7: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$, $2^4 \equiv 2$, and so on. We see that the powers of 2 modulo 7 are periodic with period 3.
- Consider 2^n modulo 11: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$, $2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 1$, $2^{11} \equiv 2$, and so on. We see that the powers of 2 modulo 11 are periodic with period 10.

Theorem 4.31 (Fermat's Little Theorem)

Let p be a prime. Then $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$. Equivalently, $a^{p-1} \equiv 1 \bmod p$ for all $a \not\equiv 0 \bmod p$.

Proof. If $a \not\equiv 0 \bmod p$, then a is a unit modulo p. Thus $ax \equiv ay \bmod p$ iff $x \equiv y \bmod p$ by cancelling a.

Hence the numbers $a, 2a, 3a, ..., (p-1)a$ are pairwise incongruent (distinct) modulo p, and they are not congruent to 0 modulo p either. Therefore, they must be congruent to $1, 2, 3, ..., (p-1)$ in some order modulo p. Hence

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv (p-1)! \bmod p.$$

Equivalently,

$$a^{p-1}(p-1)! \equiv (p-1)! \bmod p.$$

Since $(p-1)!$ is a unit mod p [it is a prouct of units], we can cancel it to get $a^{p-1} \equiv 1 \bmod p$.

We can generalise this to non-prime moduli.

Theorem 4.32 (Fermat-Euler Theorem)

Let $\gcd(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \bmod m$.

Proof. Let $\mathcal{U} = \{x \in \mathbb{Z} : 0 < x < m, \gcd(x, m) = 1\}$ be the set of units modulo m. Note that $|\mathcal{U}| = \varphi(m)$. Label them $u_1, u_2, \ldots, u_{\varphi(m)}$. Then $au_1, au_2, \ldots, au_{\varphi(m)}$ are all distinct and invertible modulo m [since a is a unit], and hence they are $u_1, \ldots, u_{\varphi(m)}$ up to reordering. Thus,

$$au_1 \cdot au_2 \cdot \ldots \cdot au_{\varphi(m)} \equiv u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)} \bmod m.$$

Equivalently,

$$a^{\varphi(m)}\left(u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)}\right) \equiv \left(u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)}\right) \bmod m.$$

Since $u_1, u_2, \ldots, u_{\varphi(m)}$ are all units modulo m, so is their product [it is a product of units]. Thus, we can cancel it to get $a^{\varphi(m)} \equiv 1 \bmod m$.

Consider $(p-1)!$ modulo p for a prime p.

Example 4.33

When $p = 5$, we have $4! = 24 \equiv -1 \bmod 5$.

When $p = 7$, we have $6! = 720 \equiv -1 \bmod 7$.

Lemma 4.34

Let p be a prime. Then $x^2 \equiv 1 \bmod p \Leftrightarrow x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.

Remark. p must be prime for this to hold. For example, $x^2 \equiv 1 \bmod 8$ has solutions $x \equiv 1, 3, 5, 7 \bmod 8$.

Proof.

$$\begin{aligned} x^2 \equiv 1 \bmod p &\Leftrightarrow x^2 - 1 \equiv 0 \bmod p \\ &\Leftrightarrow (x-1)(x+1) \equiv 0 \bmod p \\ &\Leftrightarrow p \mid (x-1)(x+1) \\ &\Leftrightarrow p \mid (x-1) \text{ or } p \mid (x+1) \\ &\Leftrightarrow x \equiv 1 \bmod p \text{ or } x \equiv -1 \bmod p. \end{aligned}$$

Remark. More generally, a non-zero polynomial of degree k over $\mathbb{Z}_p$ has at most k roots $\bmod p$.

Lecture 14 · 2025-11-08

Theorem 4.35 (Wilson's Theorem)

Let p be a prime. Then $(p-1)! \equiv -1 \bmod p$.

Proof. As an edge case, this is true for $p = 2$. Let us assume $p \geqslant 3$ from now on.

Note that the units modulo p become in pairs where each pair multiplies to 1 modulo p, together with some elements that are self-inverse, *i.e.* x such that $x^2 \equiv 1 \bmod p$.

By Lemma 4.34, the only self-inverse elements are 1 and $p-1$. Thus the remaining $p-3$ units of $\mathbb{Z}_p$ come in inverse pairs. Hence,

$$\begin{aligned}(p-1)! &\equiv 1 \times (p-1) \times (\text{pairs that multiply to } 1) \\ &\equiv (p-1) \\ &\equiv -1 \bmod p.\end{aligned}$$

We may wonder if -1 is a square modulo p for some prime p.

Example 4.36

When $p = 5$, we have $2^2 \equiv -1 \bmod 5$.

When $p = 7$, there is no integer x such that $x^2 \equiv -1 \bmod 7$.

When $p = 13$, we have $5^2 \equiv -1 \bmod 13$.

When $p = 19$, there is no integer x such that $x^2 \equiv -1 \bmod 19$.

Proposition 4.37

Let p be an odd prime. Then -1 is a square modulo p if and only if $p \equiv 1 \bmod 4$.

Proof.

[⇐] Suppose $p \equiv 1 \bmod 4$. By Wilson's theorem, we have

$$\begin{aligned}-1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-3) \cdot (p-2) \cdot (p-1) \bmod p \\ &\equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot \ldots \cdot -3 \cdot -2 \cdot -1 \bmod p \\ &\equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \\ &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \bmod p.\end{aligned}$$

Since $p \equiv 1 \bmod 4$, $p = 4k + 1$ for some $k \in \mathbb{N}$, so $\frac{p-1}{2} = 2k$ is even. Thus, $(-1)^{\frac{p-1}{2}} = 1$. Hence, -1 is a square modulo p.

[$\Rightarrow$] We shall prove by contradiction on the contrapositive. Suppose on the other hand that $p \equiv -1 \bmod 4$. [Note that for odd p, $p \equiv -1 \bmod 4 \Leftrightarrow p \equiv 3 \bmod 4$ and this is the only other choice other than $p \equiv 1 \bmod 4$.] If -1 were a square modulo p, *i.e.* if there were $z \in \mathbb{Z}$ such that $z^2 \equiv -1 \bmod p$, then by Fermat's little theorem (Theorem 4.31), we would have

$$\begin{aligned} 1 &\equiv z^{p-1} \bmod p \\ &\equiv z^{4k+2} \bmod p \\ &\equiv \left(z^2\right)^{2k+1} \bmod p \\ &\equiv (-1)^{2k+1} \bmod p \\ &\equiv -1 \bmod p. \quad ※ \end{aligned}$$

Remark. When $p \equiv 1 \bmod 4$, Wilson's theorem tells us a solution to $x^2 \equiv -1 \bmod p$.

4.8 Public Key Cryptography

Proposition 4.38 (Fermat's Criterion [Non-Examinable])

When $a = 2$, Fermat's little theorem (Theorem 4.31) can be read as

$$2^p \equiv 2 \bmod p.$$

Another way is to state that if $2^p \bmod p = 2$, then there is a good chance that p is prime. If not, then p is called a pseudoprime.

Let us agree to write messages as sequences of numbers, say $A \to 00$, $B \to 01$, ..., $Z \to 25$, space $\to 26$, full stop $\to 27$, comma $\to 28$, and so on. One (say, A) want to send secure messages in an encrypted form in such a way that the intended recipient can decrypt them easily, but an eavesdropper cannot.

We are going to use the RSA (Rivest-Shamir-Adleman) algorithm, which is based on modular arithmetic.

- To set up the encryption scheme,
  - A thinks of two very large primes p and q.
  - A lets $n = pq$ and computes the **encoding exponent** e which is coprime to the **Euler totient** $\varphi(n) = (p-1)(q-1)$.
  - A makes (n, e) public (this is the **public key** or **encryption scheme**).
- To send A an encrypted message,
  - B slices the messages into blocks of numbers less than n.
  - B encodes each block m as $c \equiv m^e \bmod n$ (the **ciphertext**). This can be computed efficiently using repeated squaring.

- B sends the ciphertext c to A.

- To decrypt the message,
  - A computes the **decoding exponent** d such that $ed \equiv 1 \bmod \varphi(n)$ (this can be done using the Euclidean algorithm). This step requires knowledge of $\varphi(n)$, which in turn requires knowledge of p and q for computation within reasonable time.
  - A computes $(m^e)^d = m^{k\varphi(n)+1}$ for some $k \in \mathbb{Z}$. By Fermat-Euler theorem (Theorem 4.32), we have $m^{k\varphi(n)} \equiv 1 \bmod n$ since $\gcd(m, n) = 1$ if $m < n$. Thus, $m^{k\varphi(n)+1} \equiv m \bmod n$.

> ***Remark.*** Finding $\varphi(n)$ without knowing p and q is equivalent to factoring n into p and q, which is believed to be hard for classical computers on large n. This is what makes RSA secure.
>
> It is unknown whether there are efficient algorithms for factoring large integers on quantum computers. If such algorithms exist, they would compromise the security of RSA.

5 The Reals

5.1 Construction of $\mathbb{R}$

Recall the construction of $\mathbb{N}$ using Peano's axioms in Axiom 3.1. We obtain $\mathbb{Z}$ from $\mathbb{N}$ by allowing for subtraction. Formally, $\mathbb{Z}$ is the equivalence classes of $\mathbb{N}\times\mathbb{N}$ under the equivalence relation

$$(a,b)R(c,d) \Leftrightarrow a+d=b+c.$$

We can now think of (a,b) as $a-b$.

Write 0 for $[(1,1)]$, $-a$ for $[(1,1+a)]$ and define addition and multiplication on $\mathbb{Z}$ by

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]$$
$$[(a,b)]\times[(c,d)]=[(ac+bd,ad+bc)]$$

The rules of arithmetic can be verified for $\mathbb{Z}$.

We obtain $\mathbb{Q}$ from $\mathbb{Z}$ by allowing for division. Formally, $\mathbb{Q}$ is the equivalence classes of $\mathbb{Z}\times\mathbb{N}$ under the equivalence relation

$$(a,b)R(c,d) \Leftrightarrow ad=bc.$$

We write $\frac{a}{b}$ for $[(a,b)]$. We can define $+,\times$ on $\mathbb{Q}$ by

$$[(a,b)]+[(c,d)]=[(ad+bc,bd)]$$
$$[(a,b)]\times[(c,d)]=[(ac,bd)]$$

We can also define an order on $\mathbb{Q}, <$, which has the property that

1. If $a,b\in\mathbb{Q}$, then only one of the following holds: $a<b$, $a=b$, $a>b$.
2. If $a<b$ and $b<c$ then $a<c$.

Lecture 15 · 2025-11-11

The ordering $<$ on $\mathbb{Q}$ has the useful property that between any 2 rational numbers there is another rational number: if $p,q\in\mathbb{Q}$ and $p<q$, then $p<\frac{p+q}{2}<q$.

Nonetheless, there are *gaps* in $\mathbb{Q}$.

Proposition 5.1

There is no rational x with $x^2=2$.

Proof. Suppose $x^2=2$, and WLOG assume that $x>0$. If x is rational, then we can write $x=\frac{a}{b}$ for some $a,b\in\mathbb{Z}^+$. Then $\frac{a^2}{b^2}=2$, so $a^2=2b^2$.

But the exponent of 2 in the prime factorisation of a^2 is even, while that in $2b^2$ is odd, contradicting the fundamental theorem of arithmetic. ※

Remark. The same proof shows that if $\exists x\in\mathbb{Q}$ with $x^2=n$ for some $n\in\mathbb{N}$, then n must be a square number.

Now we shall see an alternative proof.

> ***Proof.*** Suppose $x^2 = 2$ for some $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}^+$. Then for any $c, d \in \mathbb{Z}$, $cx + d$ is of the form $\frac{e}{b}$ for some $e \in \mathbb{Z}$.
>
> Thus if $cx + d > 0$, then $(cx + d) \geqslant \frac{1}{b}$. But we have $0 < x - 1 < 1$ as $1 < x < 2$, so if n is sufficiently large,
>
> $$0 < (x-1)^n < \frac{1}{b}.$$
>
> But for any $n \in \mathbb{N}$, $(x-1)^n$ is of the form $cx + d$ [we replace all even powers of x by 2], for some $c, d \in \mathbb{Z}$. Thus $0 < cx + d < \frac{1}{b}$. ※

So $\mathbb{Q}$ clearly has gaps. We shall express this fact making reference only to $\mathbb{Q}$, in order to motivate the construction of $\mathbb{R}$.

Let A be the set of positive rationals p such that $p^2 < 2$. We will show that A contains no largest number. For any $p \in A$, consider $q = p - \frac{p^2-2}{p+2}$. Then $q \in \mathbb{Q}$, and by definition $p^2 - 2 < 0$, so $q > p$. Also,

$$\begin{aligned} q^2 - 2 &= \left(p - \frac{p^2-2}{p+2}\right)^2 - 2 \\ &= \frac{2\left(p^2-2\right)}{(p+2)^2} < 0. \end{aligned}$$

Thus $q \in A$, so A has no largest number. Similarly the set $\left\{q \in \mathbb{Q} : q > 0, q^2 > 2\right\}$ has no smallest number.

> ***Important.*** In $\mathbb{Q}$, there is no least upper bound for the set $A = \left\{p \in \mathbb{Q} : p > 0, p^2 < 2\right\}$. This implies a *gap* in $\mathbb{Q}$.

Definition 5.2 (Real numbers)

The **real numbers**, $\mathbb{R}$, are a set with elements 0 and 1 where $0 \neq 1$, equipped with operations $+$ and $\times$, and an ordering $<$ satisfying the following axioms:

1. $+$ is commutative and associative with identity 0, and every x has an inverse under $+$.
2. $\times$ is commutative and associative with identity 1, and every $x \neq 0$ has an inverse under $\times$.
3. $\times$ is distributive over $+$.
4. $\forall a, b \in \mathbb{R}$, exactly one of the following holds: $a < b$, $a = b$, $b < a$, and $\forall a, b, c \in \mathbb{R}$, if $a < b$ and $b < c$ then $a < c$.
5. $\forall a, b, c \in \mathbb{R}$, if $a < b$ then $a + c < b + c$, and if $a < b$ and $0 < c$ then $ac < bc$.
6. Given any set S of reals that is non-empty and bounded above, there exists a least upper bound of S in $\mathbb{R}$. [This is the least upper bound axiom.]

Definition 5.3 (Bounded above)

A set $S \subset \mathbb{R}$ is **bounded above** if there exists some $x \in \mathbb{R}$ such that $\forall y \in S, y \leqslant x$. Such an x is called an **upper bound** of S.

Definition 5.4 (Least upper bound)

An upper bound x of a set $S \subset \mathbb{R}$ is a **least upper bound** if for any upper bound x' of S, $x \leqslant x'$. We write $\sup S$ for the least upper bound of S.

Remark.

1. In Definition 5.2, from (1-5) we can check for example that $0 < 1$, indeed, if not then $1 < 0$, so
$$0 = 1 - 1 < 0 < 0 - 1 = -1$$
so $0 = 0 \cdot (-1) < (-1) \cdot (-1) = 1$. ※
2. We may consider $\mathbb{Q}$ as contained in $\mathbb{R}$ by identifying $\frac{a}{b} \in \mathbb{Q}$ with $a \times b^{-1} \in \mathbb{R}$.
3. $\mathbb{Q}$ does not satisfy (6), *e.g.* $A = \left\{p \in \mathbb{Q} : p > 0, p^2 < 2\right\}$ as shown above.
4. In (6), it is crucial that S is non-empty and bounded above. If S is empty, then every $x \in \mathbb{R}$ is an upper bound of S, so there is no least upper bound. If S is not bounded above, then there is no upper bound, hence no least upper bound.

Lecture 16 · 2025-11-13

Example 5.5 (Examples of least upper bounds)

1. Consider the set $S = \{x \in \mathbb{R} : 0 \leqslant x \leqslant 1\} = [0, 1]$.

   2 is an upper bound for S, since $\forall x \in S, x \leqslant 2$.

   $\frac{3}{4}$ is not an upper bound for S, since $\frac{7}{8} > \frac{3}{4}$ and $\frac{7}{8} \in S$.

   The LUB is 1 because:

   - 1 is an upper bound of S.
   - Every other upper bound x of S satisfies $x \geqslant 1$ since $1 \in S$.

2. Consider the set $S = \{x \in \mathbb{R} : 0 < x < 1\} = (0, 1)$.

   2 is an upper bound for S.

   $\frac{3}{4}$ is not an upper bound for S.

   We have $\sup S = 1$ because

   - 1 is an upper bound of S.
   - We claim that there is no upper bound c such that $c < 1$:

     Certainly $c > 0$. So if $c < 1$, then $0 < c < 1$, and $\frac{c+1}{2} \in S$ with $\frac{c+1}{2} > c$, contradicting the fact that c is an upper bound of S.

> ***Important.*** If S has a greatest element, then $\sup S = \max S \in S$.
>
> However, it is not necessary that $\sup S \in S$.

3. Consider $S = \left\{0, \frac{1}{2}, \frac{3}{4}, \frac{4}{5}, \ldots\right\} = \left\{1 - \frac{1}{n} : n \in \mathbb{N}\right\}$.

   It is clear that 1 is an upper bound of S. We wish to show that $\sup S = 1$.

Proposition 5.6 (Axiom of Archimedes)

$\mathbb{N}$ is not bounded above in $\mathbb{R}$.

Proof. Suppose, on the contrary, that $\mathbb{N}$ is bounded above. Let $c = \sup \mathbb{N}$. By definition, $c - 1$ cannot be an upper bound of $\mathbb{N}$, so there exists some $n \in \mathbb{N}$ with $n > c - 1$. Then $n + 1 \in \mathbb{N}$, and $n + 1 > c$, contradicting the fact that c is an upper bound of $\mathbb{N}$. ※

Corollary 5.7

For any real number $t > 0$, $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < t$.

Proof. Given $t > 0$, by Axiom of Archimedes, there exists some $n \in \mathbb{N}$ such that $n > \frac{1}{t}$. Thus $\frac{1}{n} < t$.

Definition 5.8 (Bounded below)

A set S is said to be **bounded below** if $\exists x$ such that $x \leqslant y$ for all $y \leqslant S$. Such an x is called a **lower bound** of S.

Definition 5.9 (Greatest lower bound)

If S is a non-empty set and bounded below, then define $-S = \{-y : y \in S\}$, which is non-empty and bounded above. We define the **greatest lower bound** of S by $\inf S = -\sup(-S)$.

Corollary 5.7 immediately implies that

$$\inf\left\{\frac{1}{n} : n \in \mathbb{N}\right\} = 0.$$

Proposition 5.6 and Corollary 5.7 imply that there are no *infinitely large* or *infinitely small* real numbers.

Example 5.10

Consider $S = \left\{1 - \frac{1}{n} : n \in \mathbb{N}\right\}$.

We have $\sup S = 1$. Since if we suppose $c < 1$ is an upper bound of S, then

$$1 - \frac{1}{n} \leqslant c \quad \forall n \in \mathbb{N},$$

$$0 < 1 - c \leqslant \frac{1}{n} \quad \forall n \in \mathbb{N},$$

contradicting Corollary 5.7.

Proposition 5.11

There exists $x \in \mathbb{R}$ with $x^2 = 2$.

Proof. Let $S = \left\{x \in \mathbb{R} : x^2 < 2\right\}$. We have S is non-empty (since $1 \in S$) and bounded above (since $2 \in \mathbb{R}$ is an upper bound of S). Let $c = \sup S$, and identify that $1 < c < 2$. We claim that $c^2 = 2$.

Suppose $c^2 < 2$. For $0 < t < 1$, we have

$$\begin{aligned}(c+t)^2 &= c^2 + 2ct + t^2 \\ &< c^2 + 4t + t \\ &= c^2 + 5t \\ &< 2,\end{aligned}$$

provided we pick a sufficiently small t (*e.g.* $t < \frac{2-c^2}{5}$). Thus $c + t \in S$, contradicting the fact that c is an upper bound of S.

Suppose $c^2 > 2$. For $0 < t < 1$, we have

$$\begin{aligned}(c-t)^2 &= c^2 - 2ct + t^2 \\ &> c^2 - 4t \\ &> 2,\end{aligned}$$

provided we pick a sufficiently small t (*e.g.* $t < \frac{c^2-2}{4}$). Thus $c - t \notin S$ and it is an upper bound, contradicting the fact that $c = \sup S$.

Remark. The same proof shows that $\sqrt[n]{x}$ exists $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}^+$.

Definition 5.12 (Irrational number)

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

Example 5.13

$\sqrt{2}, \sqrt{3}, \sqrt{6}$ are all irrational numbers.

We can also construct irrationals from linear combinations of rationals and irrationals, such as $2 + 3\sqrt{5}$. Indeed, if $2 + 3\sqrt{5} = \frac{a}{b}$ with $a, b \in \mathbb{N}$, then $\sqrt{5} = \frac{\frac{a}{b}-2}{3} \in \mathbb{Q}$, contradicting the fact that $\sqrt{5}$ is irrational.

Proposition 5.14

The rationals are **dense** in $\mathbb{R}$. That is, $\forall a, b \in \mathbb{R}$ with $a < b$, $\exists q \in \mathbb{Q}$ such that $a < q < b$.

Proof. WLOG assume that $a \geqslant 0$. By Corollary 5.7, there exists some $n \in \mathbb{N}$ such that $\frac{1}{n} < b - a$.

Consider the set $T = \left\{k \in \mathbb{N} : \frac{k}{n} \geqslant b\right\}$. By Axiom of Archimedes 5.6, $\exists N \in \mathbb{N}$ such that $N > b$, hence $nN \in T$ and $T \neq \varnothing$.

By the Well-ordering Principle 3.6, T has a least element, say m. Let $c = \frac{m-1}{b}$. Since $m - 1 \notin T$, we have $c < b$.

Suppose $c \leqslant a$. Then $\frac{m}{n} = c + \frac{1}{n} < a + (b - a) = b$. ※

Hence $a < c < b$, and $c \in \mathbb{Q}$ as required.

Note that the irrationals $\mathbb{R} \setminus \mathbb{Q}$ is also dense in $\mathbb{R}$. Indeed, if we take a non-zero rational c with $a\sqrt{2} < c < b\sqrt{2}$, then $\frac{c}{\sqrt{2}}$ is irrational and satisfies $a < \frac{c}{\sqrt{2}} < b$.

5.2 Sequences

Definition 5.15 (Sequence)

A **sequence** is an enumerated collection of objects in which repetitions are allowed, and order matters. We write $a_1, a_2, a_3, \ldots$ or $(a_n)_{n=1}^{\infty}$.

Sequence limits are important in analysis, and we shall define them rigorously. For a sequence $a_1, a_2, a_3, \ldots$ to tend to a limit l, it is not enough to show that the terms get *closer* to l.

For example, we would not want $0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots$ to tend to 35.

And it is also not enough that the terms get *arbitrarily close* to l, in the sense that

$$\forall \varepsilon > 0, \exists n \in \mathbb{N} : l - \varepsilon < a_n < l + \varepsilon.$$

For example, we would not want $0, 10, \frac{1}{2}, 10, \frac{2}{3}, 10, \frac{3}{4}, 10, \ldots$ to tend to 1.

Therefore, we want the sequence to get and stay within ε of l after some point.

Definition 5.16 (Limit of a sequence)

We say that the sequence $a_1, a_2, a_3, \ldots$ tends to the **limit** $l \in \mathbb{R}$ as n tends to ∞, if

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \left|a_n - l\right| < \varepsilon.$$

where the absolute value $|x|$ for $x \in \mathbb{R}$ is defined by

$$|x| = \begin{cases} x & \text{if } x \geqslant 0 \\ -x & \text{if } x < 0 \end{cases}.$$

We think of $|a - b|$ as the *distance between* a and b on our number line. We can also check that the triangle inequality holds:

$$|a-c| \leqslant |a-b| + |b-c|.$$

Remark. We will typically apply the triangle inequality using the the following technique:

$$|a-c| = |a-b+b-c| \leqslant |a-b| + |b-c|.$$

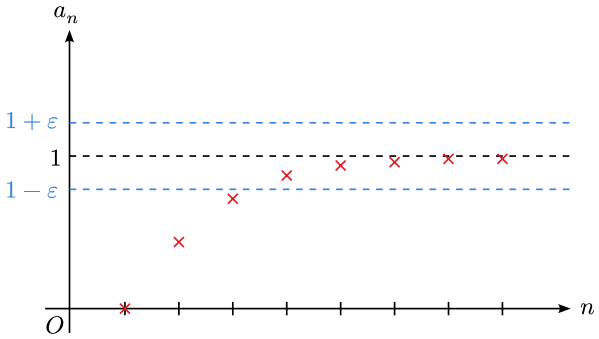
Notation. When $(a_n)_{n=1}^{\infty}$ tends to l as n tends to ∞, we can write $a_n \to l$ as $n \to \infty$ or $\lim_{n\to\infty} a_n = l$.

Definition 5.17 (Sequence convergence)

If there is a limit l such that $a_n \to l$ as $n \to \infty$, we say that the sequence $(a_n)_{n=1}^{\infty}$ **converges**. Otherwise, we say that it **diverges**.

Example 5.18

1. $0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots$, *i.e.* $a_n = 1 - \frac{1}{n}$ tends to 1 as n tends to ∞.



Given $\varepsilon > 0$, choose $N > \frac{1}{\varepsilon}$ (using Axiom of Archimedes 5.6). Then if $n \geqslant N$,

$$|a_n - 1| = \left|1 - \frac{1}{n} - 1\right| = \frac{1}{n} \leqslant \frac{1}{N} < \varepsilon.$$

Hence $a_n \to 1$ as $n \to \infty$.

2. $0, \frac{1}{2}, 0, \frac{1}{4}, 0, \ldots$ defined by

$$a_n = \begin{cases} \frac{1}{n} \text{ if } n \text{ is even} \\ 0 \text{ if } n \text{ is odd} \end{cases}$$

Given $\varepsilon > 0$, pick $N > \frac{1}{\varepsilon}$. If $n \geqslant N$, then

$$|a_n - 0| = \begin{cases} \left|\frac{1}{n} - 0\right| = \frac{1}{n} \leqslant \frac{1}{N} < \varepsilon & \text{if } n \text{ is even} \\ |0-0| = 0 < \varepsilon & \text{if } n \text{ is odd} \end{cases}$$

Hence $a_n \to 0$ as $n \to \infty$.

3. $\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \ldots$ defined by $a_n = 1 - \frac{1}{2^n}$ tends to 1 as n tends to ∞.

Let us consider which N to choose for a given $\varepsilon > 0$. We want

$$|a_n - 1| = \frac{1}{2^n} \leqslant \frac{1}{n} \leqslant \frac{1}{N} < \varepsilon,$$

so choosing $N > \frac{1}{\varepsilon}$ suffices.

Hence $a_n \to 1$ as $n \to \infty$.

Lecture 18 · 2025-11-20

4. $-1, 1, -1, 1, \ldots$ defined by $a_n = (-1)^n$.

   If a_n does not tend to l, we write $a_n \nrightarrow l$. This means

   $$\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \geqslant N, |a_n - l| \geqslant \varepsilon.$$

   We claim that $a_n \nrightarrow 0$. Indeed let $\varepsilon = 1$, and observe that for any $N \in \mathbb{N}$, $|a_n - 0| = 1$ for all $n \in \mathbb{N}$.

   In fact, a_n does not converge to any limit $l \in \mathbb{R}$. Suppose $a_n \to l$ as $n \to \infty$ for some $l \in \mathbb{R}$, let $\varepsilon > 1$. Then $\exists N \in \mathbb{N}$ such that $\forall n \geqslant N$, $|a_n - l| < 1$. In particular,

   $$|1 - l| < 1 \quad \text{and} \quad |-1 - l| < 1.$$

   But we also have

   $$\begin{aligned} 2 &= |1 - (-1)| \\ &= |1 - l + l - (-1)| \\ &\leqslant |1 - l| + |1 + l| \\ &\leqslant |1 - l| + |-1 - l| \\ &< 1 + 1 = 2, \end{aligned}$$

   which is a contradiction. ※

   Hence a_n diverges. [Divergence does not always mean that the terms tend to ∞ or $-\infty$.]

Proposition 5.19

Limits of sequences are unique.

Proof. Suppose $a_n \to l$ and $a_n \to k$ as $n \to \infty$ with $l \neq k$. Choose $\varepsilon = \frac{1}{2}|l - k| > 0$. Then

$$\begin{aligned} &\exists N \in \mathbb{N},\ \forall n \geqslant N, |a_n - l| < \varepsilon, \\ &\exists M \in \mathbb{N}, \forall n \geqslant M, |a_n - k| < \varepsilon. \end{aligned}$$

But then for any $n \geqslant \max\{N, M\}$,

$$2\varepsilon = |l - k| = |l - a_n + a_n - k| \leqslant |l - a_n| + |a_n - k| < \varepsilon + \varepsilon = 2\varepsilon,$$

which is a contradiction. ※

Definition 5.20 (Bounded sequence)

A sequence $(a_n)_{n=1}^{\infty}$ is **bounded** if there exists some $B \in \mathbb{R}$ such that $\forall n \in \mathbb{N}, |a_n| \leqslant B$.

Proposition 5.21

Every convergent sequence is bounded.

Proof. If $a_n \to l$ as $n \to \infty$, then $\exists N \in \mathbb{N}$ such that $\forall n \geqslant N$, $|a_n - l| < 1$.

Hence $|a_n| \leqslant \max\{|a_1|, |a_2|, ..., |a_{N-1}|, |l| + 1\}$ for all $n \in \mathbb{N}$.

Definition 5.22 (Monotonic sequence)

A sequence is **monotonic** if it is either increasing or decreasing. That is,

- **monotonic increasing**: $\forall n \in \mathbb{N}, a_n \leqslant a_{n+1}$,
- **monotonic decreasing**: $\forall n \in \mathbb{N}, a_n \geqslant a_{n+1}$,

Theorem 5.23 (Monotonic convergence theorem)

Every bounded monotonic sequence converges.

Proof. Suppose $(a_n)_{n=1}^{\infty}$ is monotonic increasing and bounded. Then the set $\{a_n : n \geqslant 1\}$ is non-empty and bounded above. By the least upper bound axiom, let $l = \sup\{a_n : n \geqslant 1\}$.

Given $\varepsilon > 0$, $l - \varepsilon$ cannot be an upper bound of $\{a_n : n \geqslant 1\}$, so there exists some $N \in \mathbb{N}$ such that $a_N > l - \varepsilon$. Then for any $n \geqslant N$,

$$l - \varepsilon < a_n \leqslant l,$$

since the sequence is increasing. Thus $|a_n - l| < \varepsilon$ for all $n \geqslant N$, so $a_n \to l$ as $n \to \infty$.

The case where $(a_n)_{n=1}^{\infty}$ is monotonic decreasing is similar.

Remark.

1. Note that for an increasing sequence to converge, we only need to know that it is bounded above.
2. Boundedness is necessary: consider $a_n = n$. This sequence is increasing, unbounded and does not converge.
3. The monotonic convergence theorem is equivalent to the least upper bound axiom.
4. We can show that every sequence has a monotonic subsequence.

Proposition 5.24

If $a_n \leqslant d$ for all $n \in \mathbb{N}$ and $a_n \to c$ as $n \to \infty$, then $c \leqslant d$.

Proof. Suppose $c > d$. Let $\varepsilon = |c - d| > 0$. Then $\exists N \in \mathbb{N}$ such that $\forall n > N$, $|a_n - c| < \varepsilon$. But then for any such n,

$$\begin{aligned} a_n &= c + (a_n - c) \\ &\geqslant c - |a_n - c| \\ &> c - \varepsilon = d, \end{aligned}$$

contradicting the fact that $a_n \leqslant d$ for all $n \in \mathbb{N}$. ⁂

Important. If $a_m < d$ for all $n \in \mathbb{N}$ and $a_n \to c$ as $n \to \infty$, we need not the strict inequality $c < d$.

Proposition 5.25

If $a_n \to c$ as $n \to \infty$ and $b_n \to d$ as $n \to \infty$, then $a_n + b_n \to c + d$ as $n \to \infty$.

Proof. Given $\varepsilon > 0$, then

$$\begin{aligned} \exists N \in \mathbb{N}, \forall n \geqslant N, |a_n - c| &< \frac{\varepsilon}{2}, \\ \exists M \in \mathbb{N}, \forall n \geqslant M, |b_n - d| &< \frac{\varepsilon}{2}. \end{aligned}$$

Choose $N^* = \max\{N, M\}$, then for any $n \geqslant N^*$,

$$\begin{aligned} |(a_n + b_n) - (c + d)| &= |(a_n - c) + (b_n - d)| \\ &\leqslant |a_n - c| + |b_n - d| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Hence $a_n + b_n \to c + d$ as $n \to \infty$.

Lecture 19 · 2025-11-22

5.3 Series

In the reals, the sum of two numbers is defined, so by induction we can define the sum of finitely many numbers. However, we cannot directly define the sum of infinitely many numbers.

Definition 5.26 (Series)

Let (a_n) be a sequence in $\mathbb{R}$. Then

$$s_k = \sum_{n=1}^{k} a_n$$

is the ***k*th partial sum** of the **series** whose nth term is a_n. We write

$$\sum_{n=1}^{\infty} a_n = \lim_{k \to \infty} s_k$$

if the limit exists.

Example 5.27

1. The series whose nth term is $a_n = r^n$ for some $|r| < 1$ is called the **geometric series**:

$$\begin{aligned} s_k &= r + r^2 + \ldots + r^k \\ &= r \cdot \frac{1 - r^k}{1 - r} \\ &\to r \cdot \frac{1}{1 - r} \quad \text{as } k \to \infty \text{ since } r^k < 1. \end{aligned}$$

   Hence $\sum_{n=1}^{\infty} r^n = \frac{r}{1-r}$ for $|r| < 1$.

2. The series whose nth term is $a_n = \frac{1}{n}$ is known as the **harmonic series**:

$$\begin{aligned} s_{2^k} &= 1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\text{each} \geqslant \frac{1}{4}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\text{each} \geqslant \frac{1}{8}} + \ldots + \frac{1}{2^k} \\ &\geqslant 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \ldots + \frac{1}{2^k}. \end{aligned}$$

   In general,

$$\frac{1}{2^m + 1} + \frac{1}{2^m + 2} + \ldots + \frac{1}{2^{m+1}} \geqslant 2^m \cdot \frac{1}{2^{m+1}} = \frac{1}{2}.$$

   Hence

$$\begin{aligned} s_{2^k} &\geqslant 1 + \frac{1}{2} + k \cdot \frac{1}{2} \\ &= 1 + \frac{k}{2}. \end{aligned}$$

   So the partial sums are increasing and unbounded, hence $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

3. The series whose nth term is $a_n = \frac{1}{n^2}$:

$$s_{2^k - 1} = 1 + \underbrace{\frac{1}{2^2} + \frac{1}{3^2}}_{\leqslant 2 \cdot \frac{1}{2^2}} + \underbrace{\frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2}}_{\leqslant 4 \cdot \frac{1}{4^2}} + \ldots + \frac{1}{(2k-1)^2}.$$

   In general,

$$\frac{1}{(2^m)^2} + \frac{1}{(2^m + 1)^2} + \ldots + \frac{1}{(2^{m+1} - 1)^2} \leqslant 2^m \cdot \frac{1}{2^{2m}} = \frac{1}{2^m}.$$

   Hence

$$\begin{aligned} s_{2^k - 1} &\leqslant 1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{k-1}} \\ &= 2 - \frac{1}{2^{k-1}} \\ &< 2. \end{aligned}$$

So the partial sums are increasing and bounded above, hence by Monotonic Convergence Theorem 5.23, $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges.

In fact, $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

5.4 Decimal Expansions

Let (d_n) be a sequence where each $d_n \in \{0, 1, 2, ..., 9\}$. Then $\sum_n = 1^{\infty} \frac{d_n}{10^n}$ converges to some limit x with $0 \leqslant x \leqslant 1$, since te partial sums are increasing and bounded above by

$$\sum_{n=1}^{\infty} \frac{9}{10^n} = \frac{9}{10} \cdot \frac{1}{1 - \frac{1}{10}} = 1.$$

We say that x has **decimal expansion** $0.d_1d_2d_3...$. We shall consider whether every x with $0 \leqslant x < 1$ have a decimal expansion.

We can pick $d_1 \in \mathbb{Z}$ to be maximal such that $\frac{d_1}{10} \leqslant x < 1$.

Then $0 \leqslant d_1 \leqslant 9$ because $0 \leqslant x < 1$ and $0 \leqslant x - \frac{d_1}{10} < \frac{1}{10}$ by maximality of d_1.

Then, pick $d_2 \in \mathbb{Z}$ to be maximal such that $\frac{d_2}{100} \leqslant x - \frac{d_1}{10}$, and we have $0 \leqslant x - \frac{d_1}{10} - \frac{d_2}{100} < \frac{1}{100}$ by maximality of d_2.

Inductively, we can pick $d_n \in \mathbb{Z}$ to be maximal such that

$$\frac{d_n}{10^n} \leqslant x - \sum_{j=1}^{n-1} \frac{d_j}{10^j}$$

so that

$$0 \leqslant x - \sum_{j=1}^{n} \frac{d_j}{10^j} < \frac{1}{10^n}.$$

Since $\frac{1}{10^n} \to 0$ as $n \to \infty$, we have

$$x - \sum_{j=1}^{n} \frac{d_j}{10^j} \to 0 \quad \text{as } n \to \infty.$$

Thus

$$x = \sum_{j=1}^{\infty} \frac{d_j}{10^j} = 0.d_1d_2d_3...$$

Remark.

1. Decimal expansions are not unique: for example, $0.47999999... = 0.48000000...$.

   We show that this happens if and only if the decimal expansion ends in an infinite string of 9 s.

   Suppose $0.a_1a_2a_3... = 0.b_1b_2b_3...$ with a_i and b_i not all equal, then suppose $a_j = b_j$ for all $j < k$ for some k, and WLOG assume $a_k < b_k$.

Then

$$\sum_{j=k+1}^{\infty} \frac{a_j}{10^j} \leqslant \sum_{j=k+1}^{\infty} \frac{9}{10^j} = \frac{9}{10^{k+1}} \cdot \frac{1}{1-\frac{1}{10}} = \frac{1}{10^k}.$$

We must have $b_k = a_k + 1$, for that if $b_k > a_k + 1$, then $b - a \geqslant 2 \cdot 10^{-k} - 10^{-k} > 0$.

Also, for all $j > k$, we have $a_j = 0$ and $b_k = 0$.

Lecture 20 · 2025-11-25

2. A decimal expansion if **periodic** if, after a finite number of terms, it repeats in blocks, of length k say. *i.e.* $\exists l, k$ such that $\forall n > l$, $d_n = d_{n+k}$.

   A periodic decimal is rational, *e.g.*

$$x = 0.\underbrace{7832}_{l}\underbrace{147}_{k=3}147147147\ldots$$

   Then we have

$$\begin{aligned} 10^4 - x - 7832 &= 0.147147147\ldots \\ &= 147 \sum_{j=1}^{\infty} \frac{1}{10^{3j}} \\ &= 147 \cdot \frac{1}{10^3} \cdot \frac{1}{1-\frac{1}{10^3}} \in \mathbb{Q}. \end{aligned}$$

   So $x \in \mathbb{Q}$.

   Conversely, if $x \in \mathbb{Q}$, then it has a periodic decimal expansion. To see that, we write $x = \frac{p}{2^a 5^b q}$ where $a, b, p, q \in \mathbb{Z}$ with $a, b, q \geqslant 0$, and $\gcd(10, q) = 1$. Then

$$10^{\max(a,b)} x = \frac{t}{q} = n + \frac{c}{q}$$

   where $n, c \in \mathbb{Z}$ and $0 \leqslant c < q$.

   By Fermat-Euler Theorem 4.32, since $\gcd(q, 10) = 1$, we have

$$\begin{aligned} 10^{\varphi(q)} &\equiv 1 \bmod q \\ 10^{\varphi(q)} - 1 &= kq \quad \text{for some } k \in \mathbb{N}. \end{aligned}$$

   Hence

$$\frac{c}{q} = \frac{kc}{kq} = \frac{kc}{10^{\varphi(q)} - 1} = kc \cdot \sum_{j=1}^{\infty} \frac{1}{(10^{\varphi(q)})^j}.$$

   Since $0 \leqslant kc < kq$, and kq has at most $10^{\varphi(q)}$ digits (by Fermat-Euler), we can write kc as a $\varphi(q)$-digit number $d_1 d_2 \ldots d_{\varphi(q)}$.

   Thus $\frac{c}{q} = 0.d_1 d_2 \ldots d_{\varphi(q)} d_1 d_2 \ldots d_{\varphi(q)} \ldots$ and so x has a periodic decimal expansion.

5.5 Euler's Number e

We define

$$e = 1 + \frac{1}{1!} + \underbrace{\frac{1}{2!}}_{\leqslant \frac{1}{2}} + \underbrace{\frac{1}{3!}}_{\leqslant \frac{1}{4}} + \underbrace{\frac{1}{4!}}_{\leqslant \frac{1}{8}} + \dots$$

By Monotonic Convergence Theorem 5.23, the series converges, since the partial sums are increasing and bounded above by 3.

If we define $0! = 1$, then $e = \sum_{j=0}^{\infty} \frac{1}{j!}$.

Proposition 5.28

e is irrational.

Proof. Suppose e were rational, *i.e.* $e = \frac{p}{q}$ where $p, q \in \mathbb{N}$ and $q > 1$ (since $2 < e < 3$).

But

$$\begin{aligned} q!e \in \mathbb{N} &= q! + \frac{q!}{1!} + \frac{q!}{2!} + \dots + \frac{q!}{q!} + \frac{q!}{q+1!} + \dots \\ &= N + x \quad \text{for some } N \in \mathbb{N} \end{aligned}$$

where

$$\begin{aligned} x &= \sum_{j=q+1}^{\infty} \frac{q!}{j!} = \sum_{j=1}^{\infty} \frac{q!}{(q+j)!} \\ &= \frac{1}{q+1} + \underbrace{\frac{1}{(q+1)(q+2)}}_{\leqslant \frac{1}{(q+1)^2}} + \underbrace{\frac{1}{(q+1)(q+2)(q+3)}}_{\leqslant \frac{1}{(q+1)^3}} + \dots \end{aligned}$$

and in general,

$$\frac{q!}{(q+j)!} \leqslant \frac{1}{(q+1)^j}.$$

So $x \leqslant \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \dots = \frac{1}{q} \leqslant \frac{1}{2}$. Thus $0 < x < 1$, contradicting the fact that $q!e \in \mathbb{N}$. ⁂

Hence e is irrational.

Recall the definitions of Algebraic Numbers 1.3 and Transcendental Numbers 1.4.

Example 5.29

1. Every rational number is algebraic, since if $x = \frac{p}{q} \in \mathbb{Q}$, then $qx - p = 0$.
2. $\sqrt{2}$ is algebraic, since it satisfies $x^2 - 2 = 0$.

Theorem 5.30 (Liouville number is transcendental)

The number $L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

Proof. We will need two facts about polynomials:

Fact A. For any polynomial p, there exists some K such that $|p(x) - p(y)| \leqslant k|x - y|, \forall 0 \leqslant x, y \leqslant 1$.

Indeed, suppose $p(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$. Then

$$\begin{aligned} p(x) - (y) &= a_d\left(x^d - y^d\right) + a_{d-1}\left(x^{d-1} - y^{d-1}\right) + \ldots + a_1(x - y) \\ &= (x - y)\left[a_d\left(x^{d-1} + x^{d-2}y + \ldots + y^{d-1}\right) + \ldots + a_1\right]. \end{aligned}$$

So

$$|p(x) - p(y)| \leqslant |x - y|\underbrace{\left[d|a_d| + (d-1)|a_{d-1}| + \ldots + |a_1|\right]}_{K}.$$

Fact B. A non-zero polynomial of degree d has at most d real roots.

Lecture 21 · 2025-11-27

Write $L_n = \sum_{k-1}^{n} \frac{1}{10^{k!}}$, so that $L = \lim_{n\to\infty} L_n$.

Suppose that there is a polynomial p of which $p(L) = 0$. Note $0 < L < 1$.

Then by Fact A, there exists some K such that

$$p(x) - p(y) \leqslant K|x - y| \quad \forall 0 \leqslant x, y \leqslant 1.$$

Note

$$\left|L - L_n\right| = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} \leqslant 2 \cdot \frac{1}{10^{(n+1)!}}.$$

Suppose p has degree d, *i.e.*

$$p(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$$

with $a_i \in \mathbb{Z}, a_d \neq 0$.

Notice that $L_n = \frac{s}{10^{n!}}$ for some $s \in \mathbb{N}$. So

$$p(L_n) = \frac{t}{10^{dn!}} \quad \text{for some } t \in \mathbb{Z}.$$

By Fact B, $p(L_n) = 0$ for at most d values of n. So for sufficiently large n, we have $p(L_n) \neq 0$. Hence

$$\left|p(L_n) - p(L)\right| = \left|p(L_n)\right| \geqslant \frac{1}{10^{dn!}}.$$

Therefore,

$$\frac{1}{10^{dn!}} \leqslant \left|p(L_n) - p(L)\right| \leqslant K\left|L_n - L\right| \leqslant 2K\frac{1}{10^{(n+1)!}}.$$

This is a contradiction for sufficiently large n, since $(n+1)!$ grows faster than $dn!$. ※

Remark.

1. Such L are called **Liouville numbers**.
2. This proof does not show that e is transcendental, but nonetheless it is known that e is transcendental.
3. The same proof shows that any real number x that satisfies

$$\forall n \in \mathbb{N}, \exists \frac{p}{q} \in \mathbb{Q} : 0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}$$

is transcendental.

In loose terms, if x has a very good rational approximation, then it is transcendental.

5.6 Brief Introduction to Complex Numbers

Some polynomials have no real roots, *e.g.* $x^2 + 1 = 0$. We will define x, a complex number, satisfying this equation.

The **complex numbers** $\mathbb{C}$ consists of $\mathbb{R}^2$ together with operations $+$ and $\times$ defined by

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b) \times (c, d) = (ac - bd, ad + bc).$$

We can view $\mathbb{R}$ as contained in $\mathbb{C}$ ny identifying $a \in \mathbb{R}$ with $(a, 0) \in \mathbb{C}$.

Note that $(a, 0) + (b, 0) = (a + b, 0)$ and similarly $(a, 0) \times (b, 0) = (ab, 0)$. We define $i = (0, 1) \in \mathbb{C}$. Then $i^2 = (0, 1) \times (0, 1) = (-1, 0)$, so $i^2 + 1 = 0$.

Note that $z \in \mathbb{C}$ is of the form $a + \mathrm{i}b$ with $a, b \in \mathbb{R}$.

Indeed, $(a, b) = a(1, 0) + b(0, 1) = a + b\mathrm{i}$.

Remark.

1. $\mathbb{C}$ obeys all the usual rules of arithmetic. In particualr, if $0 \neq z \in \mathbb{C}$, then there exists some $w \in \mathbb{C}$ such that $zw = 1$.

   Indeed, ,given $z = a + \mathrm{i}b$, note that

$$(a + \mathrm{i}b)(a - \mathrm{i}b) = a^2 + b^2.$$

   So

$$(a + \mathrm{i}b)^{-1} = \frac{a - \mathrm{i}b}{a^2 + b^2}.$$

2. Every non-constant polynomial (allowing complex coefficients) has a complex root. This is known as the Fundamental Theorem of Algebra.

6 Countability

We will now discuss the sizes of infinite sets.

Definition 6.1 (Countable Set)

We say that a set X is **countable** if X is finite or there is a bijection from X to $\mathbb{N}$.

If X is infinite and countable, we say that X is **countably infinite**.

This is to say that X is countable if and only if we can list the elements of X as

$$x_1, x_2, x_3, \ldots$$

which may or may not terminate.

Example 6.2

1. Any finite set is countable by definition.
2. $\mathbb{N}$ is countable.
3. $\mathbb{Z}$ is countable. We can list the integers as

   $$0, 1, -1, 2, -2, 3, -3, \ldots$$

   so we can define a bijection from $\mathbb{N}$ to $\mathbb{Z}$ by

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

Lemma 6.3

Any subset of $\mathbb{N}$ is countable.

Proof. If $S \subseteq \mathbb{N}$ is non-empty, by Well-Ordering Principle 3.6 there is a least element $s_1 \in S$. Remove s_1 from S and repeat the process to get $s_2, s_3, \ldots$. This process either terminates (if S is finite) or continues indefinitely (if S is infinite).

If at some point the process terminates, then we have listed all elements of S and so S is finite and hence countable.

If the process continues indefinitely, then the map

$$g : \mathbb{N} \to S \text{ with } n \mapsto s_n$$

is well-defined and injective. It is also surjective because if $k \in S$, then $k \in \mathbb{N}$ and there are less than k elements of S less than k (by construction of the natural numbers), so $k = s_n$ for some $n \in \mathbb{N}$. Thus g is a bijection and so S is countably infinite.

Lecture 22 · 2025-11-29

Theorem 6.4

The following statements are equivalent for a set X:

1. X is countable
2. There is an injection $X \to \mathbb{N}$
3. There is a surjection $\mathbb{N} \to X$, or $X = \varnothing$

Proof.

[(2) ⇒ (1)] Suppose that there is an injection $g : X \to \mathbb{N}$. Then g is a bijection from X to $g(X) \subseteq \mathbb{N}$. By the previous lemma, $g(X)$ is countable, so X is countable.

[(1) ⇒ (3)] This is clear if $X = \varnothing$. If X is countably infinite, then there is a bijection $f : X \to \mathbb{N}$. The inverse $f^{-1} : \mathbb{N} \to X$ is then a surjection.

[(3) ⇒ (2)] Suppose $X \neq \varnothing$ and there is a surjection $f : \mathbb{N} \to X$. We can define an injection $h : X \to \mathbb{N}$ as follows: for each $x \in X$, let

$$h(x) = \min(\{n \in \mathbb{N} : f(n) = x\}).$$

This is well-defined since f is surjective. To see that h is injective, suppose that $h(x_1) = h(x_2)$ for some $x_1, x_2 \in X$. Then by definition of h, we have

$$f(h(x_1)) = x_1 \quad \text{and} \quad f(h(x_2)) = x_2,$$

so $x_1 = x_2$. Thus h is an injection.

Corollary 6.5

Any subset of a countable set is countable.

Proof. If $Y \subseteq X$ and X is countable, then take the injection $X \to \mathbb{N}$ restricted to Y.

We may thus view *countable* as saying that a set is *at most as big as* $\mathbb{N}$.

Theorem 6.6

$\mathbb{N} \times \mathbb{N}$ is countable.

Proof 1. We can list the elements of $\mathbb{N} \times \mathbb{N}$ as follows:

$$(1,1), (1,2), (2,1), (1,3), (2,2), (3,1), (1,4), (2,3), (3,2), (4,1), \ldots$$

which corresponds to the diagonals in the grid of pairs. This gives a surjection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$, so $\mathbb{N} \times \mathbb{N}$ is countable.

More precisely, define $a_1 = (1,1)$ and a_n inductively. For $n \geqslant 1$, given $a_{n-1} = (p, q)$, then writing

$$a_n = \begin{cases} (p-1, q+1) & p > 1 \\ (q+1, 1) & p = 1 \end{cases}$$

gives a well-defined sequence $(a_n)_{n=1}^{\infty}$ which lists all elements of $\mathbb{N}\times\mathbb{N}$. The map $f:\mathbb{N}\to\mathbb{N}\times\mathbb{N}$ defined by $f(n)=a_n$ is then a surjection.

Proof 2. From Theorem 6.4, it suffices to construct an injection $g:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$. Define

$$g(p,q)=2^p\times 3^q.$$

To see that g is injective, suppose that $g(p_1,q_1)=g(p_2,q_2)$. Then by the Fundamental Theorem of Arithmetic 4.14, we must have $p_1=p_2$ and $q_1=q_2$. Thus g is an injection.

Corollary 6.7

$\mathbb{Z}\times\mathbb{Z}$ is countable.

Proof. Since $\mathbb{Z}$ is countable, there is an injection $f:\mathbb{Z}\to\mathbb{N}$. Then the map

$$h:\mathbb{Z}\times\mathbb{Z}\to\mathbb{N} \text{ with } (x,y)\mapsto g(f(x),f(y))$$

where $g:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ is the injection from Theorem 6.6, is an injection. Thus $\mathbb{Z}\times\mathbb{Z}$ is countable.

Remark. By induction, $\mathbb{Z}^k$ is countable for any $k\in\mathbb{N}$.

Theorem 6.8

A countable union of countable sets is countable.

Proof. We me assume that our countable sets are indexed by $\mathbb{N}$. Given countable sets $A_1, A_2, A_3, \ldots$, we wish to show that $\bigcup_{n\in\mathbb{N}} A_n$ is countable.

For each $i\in\mathbb{N}$, since A_i is countable, we can list its elements as

$$A_i=\left\{a_1^{(i)}, a_2^{(i)}, a_3^{(i)}, \ldots\right\}.$$

Define $f:\bigcup_{n\in\mathbb{N}} A_n\to\mathbb{N}$ by

$$a_j^{(i)}\mapsto 2^i\times 3^j.$$

Note that we need to take the least i such that $a_j^{(i)}$ is in A_i to ensure that f is well-defined. [This is possible since if $a_j^{(i)}$ is in multiple A_is, we can just take the least such index.] This is an injection by the same reasoning as in Proof 2 of Theorem 6.6. Thus $\bigcup_{n\in\mathbb{N}} A_n$ is countable.

Example 6.9

$\mathbb{Q}$ is countable, since we can think of it as $\bigcup_{n\in\mathbb{N}}\frac{1}{n}\mathbb{Z}=\bigcup_{n\in\mathbb{N}}\left\{\frac{m}{n}:m\in\mathbb{Z}\right\}$, then apply Theorem 6.8.

Theorem 6.10

The set $\mathbb{A}$ of all algebraic numbers is countable.

Proof. It suffices to show that the set of all polynomials with integer coefficients is countable, since then $\mathbb{A}$ is a countable union of finite sets.

In fact, it suffices to show that for each $d \in \mathbb{N}$, the set P_d of all polynomials of degree d with integer coefficients is countable. This is by Theorem 6.8.

But the map $P_d \to \mathbb{Z}^{d+1}$ defined by

$$a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0 \mapsto (a_d, a_{d-1}, \ldots, a_1, a_0)$$

is an injection. Since $\mathbb{Z}^{d+1}$ is countable, P_d and hence $\mathbb{A}$ are countable.

Definition 6.11 (Uncountability)

A set is **uncountable** if it is not countable.

Theorem 6.12

$\mathbb{R}$ is uncountable.

Lecture 23 · 2025-12-02

Proof. If $\mathbb{R}$ were countable, we would be able to list all the reals as $r_1, r_2, r_3, \ldots$.

Write each r_n in decimal form in some way

$$r_1 = n_1.d_{11}d_{12}d_{13}d_{14}\ldots$$
$$r_2 = n_2.d_{21}d_{22}d_{23}d_{24}\ldots$$
$$r_3 = n_3.d_{31}d_{32}d_{33}d_{34}\ldots$$

Define $r = 0.d_1d_2d_3\ldots$ by $d_n = 1$, if $d_{nn} \neq 1$, and $d_n = 2$, if $d_{nn} = 1$. This r has only one decimal representation, and is not on the list, since it differs from each r_n at the n-th decimal place. ※

Thus $\mathbb{R}$ is uncountable.

This is known as **Cantor's diagonal argument**. Note that this shows that $(0, 1)$ is uncountable, and hence any interval in $\mathbb{R}$ is uncountable.

Corollary 6.13

There are uncountably many transcendental numbers.

Proof. If there were only countably many transcendental numbers, then since the set of algebraic numbers is countable, $\mathbb{R}$ would be a countable union of countable sets, and hence countable by Theorem 6.8. This contradicts Theorem 6.12.

Theorem 6.14

$\mathcal{P}(\mathbb{N})$ is uncountable.

Proof 1. If $\mathcal{P}(\mathbb{N})$ were countable, we could list it as $S_1, S_2, \ldots$ Let $S = \{n \in \mathbb{N} : n \notin S_n\}$. Then S is not on our list, since $\forall n \in \mathbb{N}, S \neq S_n$. Thus $\mathcal{P}(\mathbb{N})$ is uncountable.

Note that this is a variant of Cantor's diagonal argument.

Proof 2. Note that there is an injection from $(0,1)$ into $\mathcal{P}(\mathbb{N})$: write $x \in (0,1)$ in binary decimal expansion as

$$x = 0.x_1x_2x_3\ldots$$

with $x_i \in \{0,1\}$. [Assume that we do not end with an infinite string of 1s.] Then define $f : (0,1) \to \mathbb{N}$ by

$$f(x) = \{n \in \mathbb{N} : x_n = 1\}.$$

This is an injection. Since $(0,1)$ is uncountable by Theorem 6.12, $\mathcal{P}(\mathbb{N})$ is uncountable by Theorem 6.4.

In fact, Proof 1 shows the following:

Theorem 6.15

For any set X, there is no bijection from X to $\mathcal{P}(X)$.

Proof. Given any map $f : X \to \mathcal{P}(X)$,we will show that f is not surjective.

Indeed, let $S = \{x \in X : x \notin f(x)\}$. Then $S \in \mathcal{P}(X)$ but S does not belong to the image of f, since $\forall x \in X$, the sets S and $f(x)$ differ in the element x, so $S \neq f(x)$ for all x.

Remark.

1. This is reminiscent of Russell's paradox.
2. This gives another proof that there is no universal set. For suppose there were a universal set V. Then $\mathcal{P}(V) \subseteq V$, in which case we would have a surjection $V \to \mathcal{P}(V)$, contradicting the above theorem.

Example 6.16

Let $\{A_i : i \in I\}$ be a family of open pairwise disjoint intervals in $\mathbb{R}$. We shall consider whether this family must be countable.

> ***Claim.*** The family $\{A_i : i \in I\}$ is countable.

> ***Proof 1.*** Each interval A_i contains a rational since $\mathbb{Q}$ is Dense in $\mathbb{R}$ 5.14, and $\mathbb{Q}$ is countable. Hence since the intervals are disjoint, we have an injection [by picking a rational from each interval] from I to $\mathbb{Q}$. Thus I is countable.

> ***Proof 2.*** The set $\{i \in I : A_i \text{ has length } \geqslant 1\}$ is countable, because each such interval contains at least one integer, and the integers are countable.
>
> Similarly, the set $\left\{i \in I : A_i \text{ has length } \geqslant \frac{1}{2}\right\}$ is countable as it injects into the set of half-integers, which is countable.
>
> More generally, for each $n \in \mathbb{N}$, the set $\left\{i \in I : A_i \text{ has length } \geqslant \frac{1}{n}\right\}$ is countable as it injects into the set of integer multiples of $\frac{1}{n}$, which is countable.
>
> Thus $I = \bigcup_{n\in\mathbb{N}}\left\{i \in I : A_i \text{ has length } \geqslant \frac{1}{n}\right\}$ is a countable union of countable sets, and hence countable by Theorem 6.8.

Lecture 24 · 2025-12-04

> ***Summary.*** To show that a set X is countable, we can do one of the following:
>
> 1. list its elements
> 2. inject it into $\mathbb{N}$
> 3. use Countable Union of Countable Sets is Countable 6.8
> 4. if X is near $\mathbb{R}$, consider $\mathbb{Q}$
>
> To show that a set X is uncountable, we can do one of the following:
>
> 1. use a diagonal argument
> 2. inject any uncountable set into X

Intuitively, we think of
- *"A bijects with B"* as *"A and B are of the same size"*,
- *"A injects into B"* as *"A is at most as big as B"*,
- *"A surjects onto B"* as *"A is at least as big as B"*.

For these interpretations to make sense, we need to establish, if *"A is at most as big as B"*, then *"B is at least as big as A"*, *etc.*

Lemma 6.17

Given non-empty sets A and B.

$$\exists \text{ injection } f : A \to B \Leftrightarrow \exists \text{ surjection } g : B \to A.$$

> ***Proof.***
>
> [⇒] Supose $f : A \to B$ is injective. Fix $a_0 \in A$. Define $g : B \to A$ by
>
> $$b \mapsto \begin{cases} f^{-1}(b) & b \in \operatorname{Im}(f) \\ a_0 & b \notin \operatorname{Im}(f) \end{cases}.$$

Then g is a surjection.

[⇐] Suppose $g : B \to A$ is a surjection. For each $a \in A$, pick any $b_a \in g^{-1}(\{a\})$ (this is possible since g is surjective). Define $f : A \to B$ by

$$a \mapsto b_a.$$

Then f is an injection.

We also need that, if *"A is at most as big as B"* and *"B is at most as big as A"*, then *"A and B are of the same size"*.

Theorem 6.18 (Schroeder-Bernstein Theorem)

Given sets A and B.

$$(\exists \text{ injection } f : A \to B) \wedge (\exists \text{ injection } g : B \to A) \Rightarrow (\exists \text{ bijection } h : A \to B).$$

Proof. For $a \in A$, write $g^{-1}(a)$ for the $b \in B$ (if it exists) such that $g(b) = a$.

Similarly, for $b \in B$, write $f^{-1}(b)$ for the $a \in A$ (if it exists) such that $f(a) = b$.

We call $g^{-1}(a), f^{-1}\left(g^{-1}(a)\right), g^{-1}\left(f^{-1}\left(g^{-1}(a)\right)\right), \ldots$ the (possibly finite) ancestor sequence of $a \in A$.

Similarly, define the ancestor sequence of $b \in B$.

Let

$$\begin{aligned} A_0 &= \{a \in A : \text{the ancestor sequence of } a \text{ terminates after an even number of steps}\} \\ A_1 &= \{a \in A : \text{the ancestor sequence of } a \text{ terminates after an odd number of steps}\} \\ A_\infty &= \{a \in A : \text{the ancestor sequence of } a \text{ does not terminate}\} \end{aligned}$$

and similarly for B_0, B_1, B_∞.

Note that f bijects A_0 with B_1 [observing that every $b \in B_1$ has at least one anscestor, so is equal to $f(a)$ for some $a \in A_0$]. Similarly, g bijects B_0 with A_1. Also, f (or g) bijects A_∞ with B_∞.

Then the function $h : A \to B$ defined by

$$a \mapsto \begin{cases} f(a) & a \in A_0 \\ g^{-1}(a) & a \in A_1 \\ f(a) & a \in A_\infty \end{cases}$$

is a bijection.

Example 6.19

Consider whether there is bijection from $[0, 1]$ to $[0, 1] \cup [2, 3]$.

Observe that there is an injection from $[0, 1]$ to $[0, 1] \cup [2, 3]$ given by the inclusion map, and there is an injection from $[0, 1] \cup [2, 3]$ to $[0, 1]$ given by

$$x \mapsto \frac{x}{3}.$$

Thus, by Schroeder-Bernstein Theorem 6.18, there is a bijection from $[0,1]$ to $[0,1] \cup [2,3]$.

Remark.

1. It seems natural to say that for any two sets A and B, either A injects into B, or B injects into A. This is true but its proof is beyond the scope of this course.
2. **Continuum Hypothesis**. $\nexists$ a set X whose size lies between $\mathbb{N}$ and $\mathbb{R}$. *i.e.* any subset of $\mathbb{R}$ is either countable or bijects with $\mathbb{R}$.

END OF DOCUMENT ■