Lecture Notes: Quantitative Reasoning and Mathematical Thinking[1]

Subhashis Banerjee

Department of Computer Science
Ashoka University
Sonipat, Haryana, 131029
email: suban@ashoka.edu.in

September 6, 2025

Contents

Chapter 1

Introduction

Courant and Robbins, in What is Mathematics? (1941), present mathematics not as a dry collection of formulas and tools, but as a living, creative discipline rooted in human thought and curiosity. For them, mathematics is both a pathway for understanding the natural world and an autonomous intellectual pursuit that reveals structures of order, beauty, and generality. They stress that its essence lies in the interplay between abstraction and concrete problem-solving: starting from simple, practical problems, mathematics ascends to general concepts and theories that then illuminate new domains.

They emphasize accessibility and unity: mathematics belongs to everyone who is willing to think rigorously, and its spirit combines logic with imagination. Rather than reducing it to calculation or technical skill, Courant and Robbins describe mathematics as "an expression of the human mind" where precision, creativity, and aesthetic appreciation converge. Their central idea is that mathematics is at once useful, philosophical, and artistic—simultaneously a language of science, a training ground for reasoning, and a source of intellectual delight.

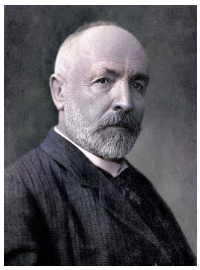
Early mathematics was computational when the emphasis was on finding methods to obtain solutions. However, over the years, the disciplines of mathematics and computer science – the subject of designing algorithms for problem solving – have diverged. In mathematics abstraction is symbolic and logical. It seeks general structures, patterns, and proofs independent of implementation. It often endeavours to seek and capture common structures across different abstractions. The primary aim is truth and understanding – developing rigorous proofs, ensuring logical consistency, and uncovering general laws. Utility often follows from this pursuit but is not always the main driver. In contrast, the role of abstraction in computational thinking is more operational and algorithmic. It emphasizes creating computational process models for natural, social and even abstract phenomena for operational analysis. The primary aim is effective procedure – designing algorithms that solve problems efficiently, often under constraints of time, memory, and real-world complexity. The power lies in execution and exploration—running a program can reveal insights about systems too complex to solve analytically. Both have become fundamental strands of epistemology that are essential for critical scientific thinking.

Data-driven inference represents a third way of knowing, distinct from the deductive rigour of mathematics and the constructive procedures of computational thinking. As practiced in modern data science and machine learning, it seeks knowledge not by proving theorems or designing explicit algorithms, but by discovering patterns and regularities directly from empirical data. Its epistemic core is induction at scale: hypotheses, models, or predictors are justified by their ability to capture hidden correlations and to generalize to new observations. Unlike mathematics, correctness is not absolute, and unlike computational thinking, procedures are not always fully transparent. Instead, credibility arises from empirical adequacy—the degree to which models explain, predict, or align with observed phenomena. This mode of inference expands our epistemic toolkit for a world where complexity and abundance of data overwhelm deductive or constructive methods, but it also brings new philosophical challenges: uncertainty about correctness, bias, and the gap between correlation and causation.

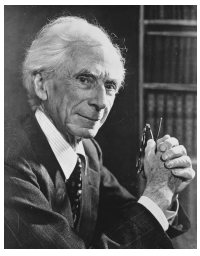
In this course we will try to cover some fundamentals of all of the above.

Chapter 2

God gave us numbers, and human thought created algorithms



"In mathematics the art of proposing a question must be held of higher value than solving it."
"A set is a Many that allows itself to be thought of as a One." – Georg Cantor



"A number will be a set of classes such as that any two are similar to each other, and none outside the set are similar to any inside the set."
"Mathematics rightly viewed possesses not only truth but supreme beauty." – Bertrand Russel

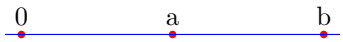
2.1 Numbers

Our discussion on mathematics and computing must start with numbers. What are numbers after all? The same number may be represented with symbols such as 3, III, or even as a line of a fixed length. But what is the underlying concept behind the different representations?

Bertrand Russell defined numbers as sizes (or *cardinality*) of *collections*. Some examples of *equinumerous* collections are $\{Red, Blue, Green\}$, $\{Amir, Salman, Shahrukh\}$, $\{Godavari, Kaveri, Krishna\}$. *Collections* are also called *Sets* or *Classes* in Mathematics. All three Sets above are of cardinality 3.

Russel defined a number as – *the number of a class is the class of all those classes that are similar (equinumerous) to it.* So, according to Russel, a number is a class of classes.

Note that *cardinality* of sets is not the only way to describe the concept of a number. A number may also be a measure of a length. For example, in the straight line below, if we define the segment $\overline{0a}$ to be the *unit length* representing the number 1, then the line segment $\overline{0b}$ which is twice the length of $\overline{0a}$ may represent the number 2.



Without belabouring the point, it will suffice to say for our purpose that all of us intuitively understand what numbers mean.

2.1.1 Numbers may be represented in multiple ways

However, we need to do useful stuff with numbers – we need to add, subtract, multiply and divide them for obvious practical reasons. Indeed, the history of numbers date back to the Mesolithic stone age. The early humans had to figure out – due to a variety of practical considerations – that if they put two similar collections of size two and size three together, the larger collection becomes of size five.

Civilisations have found many ways to represent numbers through the ages. Some examples are as tally marks in the prehistoric to early civilisations – as straight marks on bones, sticks, or stones – as can be observed in the archaeological evidence of the Ishango bones from around 20000 BCE; as Egyptian – a stroke for 1, heel bone for 10, coil of rope for 100, etc. – or Roman – I, V, X, L, C, D, M – numerals; as Base-60 (sexagesimal) numbers written as combinations of "1" and "10" wedges by the Babylonians around 2000 BCE; as used rods arranged on counting boards in base-10 with positional notation in Chinese rod systems; as positional decimal systems in Indian numerals in the Gupta period around 5^{th} century CE; as beads or stones moved on rods or grooves to represent numbers in Abacus systems in China, Rome, Mesopotamia and Jerusalem; with Indo-Arabic numerals in the medieval period; with various mechanical calculators such as Napier's bones, Slide rules, Pascal's calculator, and Leibniz's stepped reckoner in the 17^{th} century; as gears and levers in Charles Babbage's first programmable computer – the Analytic Engine; and as bits and bytes in modern digital computers. Note, also, that the methods of carrying out these operations – the algorithms – will necessarily depend on the representation we choose for numbers.

2.2 Sets

We will use *Sets* quite a bit in this course. We may describe a *Set* or a *Collection* by explicitly listing out its elements without duplicates, such as in the examples above. We may sometimes also describe a Set with a property like "all students enrolled in the QRMT section FC-0306-3". We write this formally using a variable x as $\{x \mid x \text{ is a student in the QRMT section FC-0306-3}\}$. The symbol $\mid$ is read as "such that".

If an element x belongs to a set A, we usually write this as $x \in A$.

Here are some more examples of Sets:

1. $A = \{x \mid x \text{ is a student pursuing a degree in India}\}$
2. $B = \{x \mid x \text{ is a CS Major student at Ashoka University}\}$
3. $C = \{x \mid x \text{ is a CS Major student at Ashoka University } \textbf{and } x \text{ is female}\}$

Clearly, all members of C are also members of B, and all members of B are members of A. We then say that C is a *subset* of B ($C \subseteq B$), and B is a *subset* of A ($B \subseteq A$). Formally, a set B is a *subset* of another set A, denoted as $B \subseteq A$, if $x \in A$ whenever $x \in B$. The empty set is denoted by ϕ, its size is zero (0), and it is a subset of all sets.

Given two sets A and B, the *union* $A \cup B$ is the set of all elements that are in A, or in B, or in both. Formally, $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$. For example, if $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$, then $A \cup B = \{1, 2, 3, 4, 5\}$.

Given two sets A and B, the *intersection* $A \cap B$ is the set of all elements that are in both A and B. Formally, $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$. For example, if $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$, then $A \cap B = \{3\}$.

Clearly, for any set A, $A \cup \phi = A$ and $A \cap \phi = \phi$,

Exercise 2.1 *Suppose $B \subseteq A$. Argue that*

1. $A \cup B = A$
2. $A \cap B = B$

2.3 The set of Natural numbers

Some sets can also be unbounded or infinite. We define the set of *Natural numbers* as $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$[1].

While we all intuitively understand this set, note that the elements of the set are as yet uninterpreted and undefined. We can overcome this lacunae by assuming a *God-gifted* ability to count. Given a number n as the size of a Set or a length, let us assume that we can interpret and construct the successor of n as $S(n) = n + 1$. Then, we can formally define the set of Natural numbers $\mathbb{N}$ as

1. $0 \in \mathbb{N}$, where 0 is the symbol that denotes the size of the empty set, and
2. if $n \in \mathbb{N}$, then $S(n) = n + 1 \in \mathbb{N}$

We can then adopt a suitable representation for successive elements in the set $\mathbb{N}$. Note that the set $\mathbb{N}$ is unbounded, because every number – no matter how large – has a successor.

2.3.1 Addition

We observed that the underlying concept of a number is independent of specific representations. Ideally, so should be the concepts of carrying out various operations with numbers. We may think of addition – the sum $a + b$ of two numbers a and b – as just combining two similar sets of sizes a and b. However, the procedure for "combining" is not representation independent. While simple "putting together" may work if we represent the numbers as collections of stones or marbles, it is not well defined for adding two numbers in the place-value representation that we are familiar with from junior school. Hence "combining" is a somewhat unsatisfactory way of defining addition.

A better way of defining $a + b$ is by using the successor operation $S(a) = a + 1$, b times. As long as we have a primitive method for computing $a + 1$ in any representation for an arbitrary a, this definition of $a + b$ becomes representation independent. We may define the basic property of addition using counting as:

For all $m, n \in \mathbb{N}$:

1. $m + 0 = m$
2. $m + S(n) = S(m + n)$

[1] 0 is usually not included in the Set of Natural numbers in Mathematics. We will however include 0 in the set of Natural numbers in this course. After all, it is quite natural to score a 0 in an examination

In the above definition we have used the same trick as in definition of the set $\mathbb{N}$ above, of defining a larger concept as a successor of a smaller concept. The process repeats, and the actual additions happen in the return path. For example,

$$
\begin{aligned}
&7+5\\
&\quad=(7+4)+1\\
&\quad=((7+3)+1)+1\\
&\quad=(((7+2)+1)+1)+1\\
&\quad=((((7+1)+1)+1)+1)+1\\
&\quad=(((((7+0)+1)+1)+1)+1)+1\\
&\quad=((((7+1)+1)+1)+1)+1\\
&\quad=(((8+1)+1)+1)+1\\
&\quad=((9+1)+1)+1\\
&\quad=(10+1)+1\\
&\quad=11+1\\
&\quad=12
\end{aligned}
$$

Note that the repeated substitution of a larger problem with a smaller problem is bounded, because the first condition of the definition works as a sentinel that we are bound to encounter as we keep reducing n.

We can then describe a procedure for computing $a+b$ (Algorithm 1) based on the above principle, but avoiding the deferred computations. The procedure takes a and b as input and returns *sum* as the output. $sum \leftarrow sum+1$ denotes the operation "*sum* is *assigned* $sum+1$" indicating that *sum* is incremented by 1.

Algorithm 1 An algorithm for $a+b$ by $+1$ b-times.

```
1: procedure ADD(a, b)
2:     counter ← 0
3:     sum ← a
4:     while counter < b do
5:         sum ← sum + 1
6:         counter ← counter + 1
       return sum
```

Exercise 2.2 *1. Assuming that the operation $a+1$ is available as a primitive, convince yourself that the above procedure for adding two numbers are correct.*

2. Argue that if the operation $a+1$ is available as a primitive, then the above algorithm for addition is representation independent.

3. Describe how the algorithm may be implemented using pebbles or marbles to represent numbers.

2.3.2 Multiplication

We can now define multiplication as repeated additions:

1. $n \times 0 = 0$, for all $n \in \mathbb{N}$
2. $n \times S(m) = n \times m + n$, for all $n, m \in \mathbb{N}$

Note that here again we have defined $n \times S(m)$, in terms of a smaller problem $m \times n$ of the same type.

Exercise 2.3 *1. Convince yourself that according to the above definition* $n \times m = \underbrace{n + n + n + \ldots + n}_{m \text{ times}}$.

2. Provide a representation independent algorithm, using only the successor function and addition, for multiplication of two numbers.

3. Describe how the algorithm may be implemented using pebbles or marbles to represent numbers.

2.3.3 Subtraction

To define the subtraction operation $m - n$, we may first define a predecessor operation $P(n)$ – analogous to $S(n)$ – as

1. $P(0)$ is undefined
2. $P(n) = n - 1$ for all $n > 0$.

We assume, as before, that we have a primitive counting based procedure for computing $P(n) = n - 1$ in any representation. We can define the subtraction operation $m - n$ similarly to addition:

For all $m, n \in \mathbb{N}, m \geq n$

1. $m - m = 0$
2. $m - n = S(P(m) - n)$

As before, note that $P(m) - n$ is a smaller problem that $m - n$.

The subtraction algorithm may then be given as:

Algorithm 2 An algorithm for $a - b$, $a \geq b$ by -1 b-times.

```
1: procedure SUBTRACT(a, b)
2:     counter ← 0
3:     while counter < b do
4:         a ← a − 1
5:         counter ← counter + 1
       return a
```

Exercise 2.4 *Provide alternative versions of Algorithms 1 and 2 without using the counter. Instead decrement* b *using* $b \leftarrow b - 1$ *repeatedly till* $b = 0$.

2.3.4 Division

Division is a natural requirement in civilised societies, mainly for sharing. However, it may not always be possible to divide natural numbers in equal proportions. For example, a collection of size 3 cannot be divided in two proportions of equal sizes without breaking up at least one member element. We have the *division theorem*:

Theorem 2.1 *Given two numbers* $a, b \in \mathbb{N}$*, there exist unique* $q, r \in \mathbb{N}$ *(quotient and remainder, respectively) such that* $a = bq + r$ *and* $0 \leq r < b$.

Proof: Let us first argue that such q and r exist. Repeatedly compute $a - b, a - 2b, a - 3b, \ldots, a - kb$, $k \geq 0$, till $a - kb < b$ and subtraction is possible no more. Set $q = k$ and $r = a - kb$. Clearly, q is the total number of times b can be subtracted from a, and $0 \leq r < b$. If $r = 0$ then b divides a exactly.

To argue that that q and r obtained by the above procedure are unique, let us suppose they are not. Then, there exist q_1, r_1 and q_2, r_2 such that

$$a = bq_1 + r_1, 0 \leq r_1 < 0$$
$$a = bq_2 + r_2, 0 \leq r_2 < 0$$

Without loss of generality, let us assume that $q_1 \geq q2$. The above implies that $b(q_1 - q_2) = r_2 - r_1$. One of two cases arise:

1. $q_1 = q_2$. This implies that $r_1 = r_2$, and hence uniqueness.
2. $q_1 > q_2$. This implies that $q_1 - q_2 \geq 1 \in \mathbb{N}$. Hence $r_2 - r_1 \geq b$. But this is not possible because $0 \leq r_1, r_2 < b$. Hence q and r must be unique.

□

In the above proof, we used *explicit construction* as a proof technique for establishing existence of such q and r, and *contradiction* for establishing their uniqueness. We will revisit these techniques later in the course when we discuss proofs.

Exercise 2.5 *Describe an algorithm using repeated subtraction that computes q and r given a and b.*

2.4 The Sets of Integers

We defined the subtraction operation $m - n, m \geq n, m, n \in \mathbb{N}$ as the number of times the successor operation $S()$ needs to be applied to reach m from n. This definition requires the restriction that $m \geq n$. An obvious generalisation is to remove the restriction and measure the difference in terms of either the successor $S()$ or the predecessor $P()$ operator. Subtraction then becomes directional, and we require negative numbers to represent the direction. This leads us to the set of integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$$

Arithmetic in the set $\mathbb{Z}$ follows the same principles as in $\mathbb{N}$, except that they are now directional.

Exercise 2.6 *Rework the definitions and the algorithms for addition, multiplication, subtraction and division in $\mathbb{Z}$.*

2.5 The Sets of Rationals

The division theorem tells us that given $m, n \in \mathbb{N}$, there exist $q, r \in \mathbb{N}$, such that m can be divided in to q parts of size n, possibly leaving a remainder $0 \leq r < n$. Division is an obvious fundamental need for resource sharing. If each unit is indivisible – like live cattle, for example – then the division theorem is the best we can do. However, items measured in units such as weight, volume or length – such as meat from a hunted animal, or a pile of grains – are often divisible in smaller proportions like $1/3^{rd}$, $2/25^{th}$ etc. So, division inevitably leads us to fractions. We define the set of Rational numbers as

$$\mathbb{Q} = \{x | x = p/q, p \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0\}$$

We often also write this as $\frac{p}{q}$. These are numbers of the type $\pm 1/1, \pm 1/2, \pm 1/3, \pm 1/4, \pm 2/5$ etc. We may also insist that p and q should have no common factors (i.e., $gcd(p, q) = 1$; see Section 3.5 for a formal definition of *gcd*) to avoid multiple representations for the same Rational number. Clearly $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Note, however, that we now have a situation where between any two rational numbers there are infinitely many other rational numbers.

Exercise 2.7 *Convince yourself of the above statement.*

This implies that there is no well defined successor function for a rational number, and we need to revisit our definition of addition for rationals. We start by noting that, for example,

$$\frac{1}{3} + \frac{2}{3} = \frac{1+2}{3} = 1$$

i.e., we can add the numerators as in $\mathbb{Z}$ if the denominators are the same. However, the addition

$$\frac{2}{3} + \frac{3}{4}$$

is not well defined unless the two fractions can be expressed in the same unit. But we can multiply the numerator and denominator of the first fraction by 4, and the second by three to convert to the same unit where the denominator of both is 12

$$\frac{2\times 4}{3\times 4}+\frac{3\times 3}{4\times 3}=\frac{8}{12}+\frac{9}{12}=\frac{8+9}{12}=\frac{17}{12}$$

Note that multiplying the numerator and the denominator of a fraction with the same number does not change the fraction. So, we can define the general rule for addition of two rational numbers as

$$\frac{p_1}{q_1}+\frac{p_2}{q_2}=\frac{p_1\times q_2+p_2\times q_1}{q_1\times q_2}$$

where all the additions and multiplications are defined on the set $\mathbb{Z}$.

Exercise 2.8 *Extend the above idea to define subtraction, multiplication and division in the set* $\mathbb{Q}$.

Problems

1. Give three different representations for the number 6 (for example: tally marks, Roman numerals, line segment lengths). Explain how the operation "+1" is carried out in each representation.
2. Research and briefly describe how numbers were represented in one historical number system not discussed in class (e.g., Mayan or Incan). Compare it with the decimal positional system.
3. Let

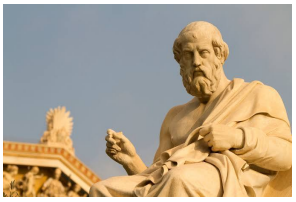
   $$A=\{x \mid x \text{ is an even number less than } 20\},\quad B=\{x \mid x \text{ is a prime number less than } 20\}.$$

   Compute $A\cap B$, $A\cup B$, and $A\setminus B$.
4. Prove or disprove: If $A\subseteq B$ and $B\subseteq C$, then $A\subseteq C$.
5. Construct a real-world example of three sets A, B, C such that $C\subset B\subset A$.
6. Using only the successor function $S(n)=n+1$, show step by step how to compute $4+3$.
7. Show that addition defined by the recursive rules in the text is associative, i.e. prove $(a+b)+c=a+(b+c)$ using the definition.
8. Starting from the definition $n\times S(m)=(n\times m)+n$, compute 3×4 step by step.
9. Write pseudocode (representation-independent) for multiplication using only the successor function and addition.
10. Explain how you could simulate multiplication using only pebbles to represent numbers.
11. Using the predecessor function $P(n)$, compute $7-4$ step by step as in the recursive definition.
12. Implement Algorithm 2 (subtraction by repeated decrementing of b) on the input $a=10, b=6$. Show the intermediate steps.
13. Using the Division Theorem, compute the quotient and remainder when $a=29, b=5$ using repeated subtraction.
14. Prove that the quotient and remainder obtained from the Division Theorem are unique.
15. Extend the recursive definition of addition from natural numbers to integers, and compute $(-3)+5$.
16. Explain why we need negative numbers to generalize subtraction. Give a real-world example where negative numbers are essential.

17. Give an example of two distinct rational numbers between $\frac{1}{3}$ and $\frac{1}{2}$.
18. Prove that between any two rational numbers there exists another rational number. (Hint: use their average.)
19. Compute $\frac{2}{3} + \frac{4}{5}$ using the common-denominator method.
20. Extend the definition to show how to compute $\frac{3}{7} \div \frac{2}{5}$.

Chapter 3

Ruler and compass algorithms



"Geometry is knowledge of the eternally existent... it compels the soul to look upwards, and leads us away from the world of appearance to the vision of truth."
"Let no one ignorant of geometry enter here" – Plato

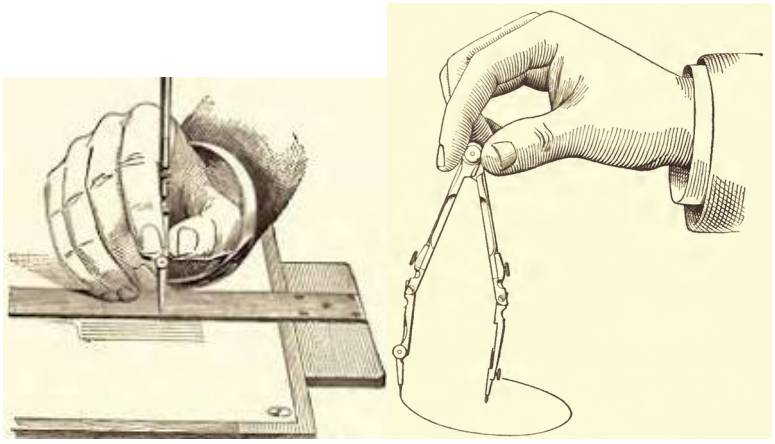


Figure 3.1: Ruler and compass. We will assume that the ruler is unmarked, and lengths can only be measured by adjusting the width of the compass.

Our endeavour so far has been to define numbers, and operations on them, in a representation independent manner. Let us now consider a specific computational model – straightedge and compass constructions introduced by the ancient Greeks – and examine whether the abstract operations we have defined above can be translated in to definite constructible procedures, or *algorithms*. Most of the geometric constructions date back to Euclid's books of Elements from around 300 BCE. We will often – by force of habit – refer to them as *ruler and compass constructions* but with the understanding that the ruler has no markings for length measurements, and can only be used to draw straight edges. See Figure 3.1.

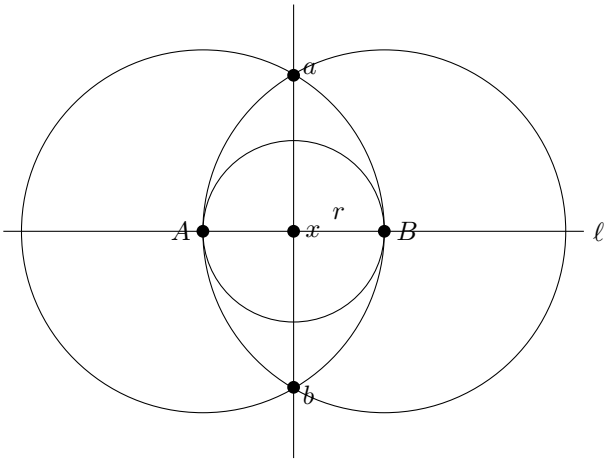


Figure 3.2: Constructing a line perpendicular to a given line passing through a point

Let us first consider some basic constructions. In what follows, the correctness of the constructions will often rely on the basic geometric properties of similar triangles. A reader may revise them from here and here.

3.1 Constructing a line perpendicular to a given line passing through a point

Given a straight line ℓ, and a point x on it, let us consider the problem of constructing a line perpendicular to ℓ and passing through x. We give a construction in Algorithm 3 (See Figure 3.2).

Algorithm 3 Constructing a line perpendicular to a given line passing through a point

1: **procedure** PERPENDICULAR(x, ℓ)
2: $c = CIRCLE(x, r)$, where r is a random length
3: $(A, B) = c \cap \ell$
4: $c_A = CIRCLE(A, 2r)$
5: $c_B = CIRCLE(B, 2r)$
6: $(a, b) = c_A \cap c_B$
7: $result = LINE(a, b)$

We have described the algorithmic procedure using some standard primitives. $c = CIRCLE(x, r)$ denotes the construction of a circle c centred at x of radius r. A and B are the intersection points of c with ℓ, denoted in the algorithm as $(A, B) = c \cap \ell$. Similarly, c_A and c_B are circles of radius $2r$ centred at A and B respectively, and a and b are the intersection points of c_A and c_B. $LINE(a, b)$ joins a and b and is the *result*.

Exercise 3.1 *1. Convince yourself that the above construction is correct. Use properties of similar triangles.*

2. Argue that $LINE(a, b)$ is also the perpendicular bisector of AB.

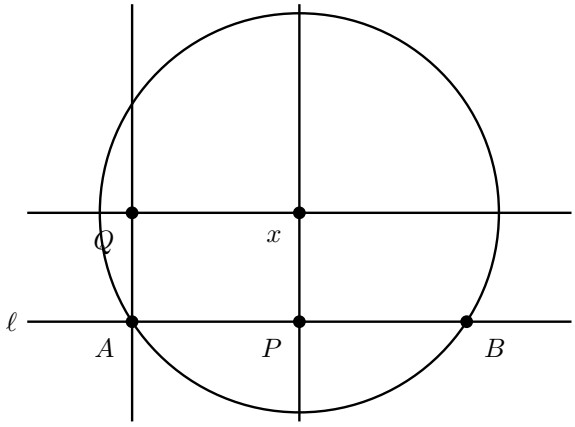


Figure 3.3: Constructing a line parallel to a given line passing through a point

3.2 Constructing a line parallel to a given line passing through a point

Given a line ℓ, and an arbitrary point x, consider the problem of construction of a line parallel to ℓ passing through x. We give a construction in Algorithm 4 (See Figure 3.3).

Algorithm 4 Constructing a line parallel to a given line passing through a point

1: **procedure** PARALLEL(x, ℓ)
2: $c = CIRCLE(x, r)$, where r is a random length
3: $(A, B) = c \cap \ell$
4: Construct p, the perpendicular bisector of AB using Algorithm 3. Argue that p passes through x.
5: $P = p \cap \ell$
6: Construct q, a perpendicular to ℓ passing through A using Algorithm 3.
7: Construct s, a perpendicular to p passing through x using Algorithm 3.
8: $Q = q \cap s$
9: $result = LINE(Q, x)$

Note that in steps 4,6 and 7 of the algorithm, we have used the procedure of Algorithm 3. We will routinely use a previously defined algorithm as a primitive to define a new algorithm.

3.3 Constructibility and the compass equivalence theorem

The above two sections give us several examples of construction of points, lines, line segments and circles. The informal definition of *constructibility* is as follows. Given points are by definition constructible. A line joining two constructible points is constructible. So is the circle centred on one constructible point passing through another constructible point. A point is constructible if it is an intersection of constructible lines and circles.

The compass advocated by the Greek philosopher Plato in these constructions is a *collapsing compass*, i.e., a compass that "collapses" whenever it is lifted from a page, so that it may not be directly used to transfer distances unlike in a modern fixable aperture compass. Note that nowhere in Sections 3.1 and 3.2 have we transferred distances using a fixed size compass lifted from the page.

This is however not a limitation as the following construction shows.

Theorem 3.1 *A collapsing compass can be used to transfer a given length to an arbitrary given*

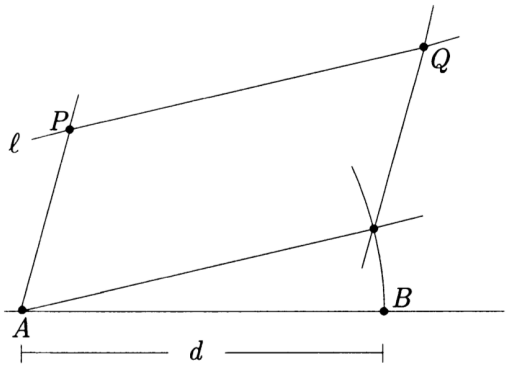


Figure 3.4: A compass-equivalence construction

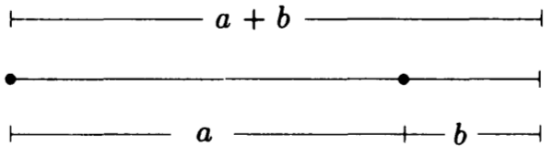


Figure 3.5: Construction of $a + b$.

point on a given line. That is, given an arbitrary length $\overline{AB}$, a line ℓ and a point P on it, it is possible to construct using a collapsing compass a point Q on ℓ such that $\overline{PQ} = \overline{AB}$.

Proof:

Algorithm 5 A compass-equivalence construction

1: **procedure** COMPASS-EQUIVALENCE(A,B,ℓ,P)
2: $c = CIRCLE(A, B)$; note that $\overline{AB} = d$
3: Construct p, the line parallel to ℓ passing through A using Algorithm 4
4: $R = c \cap p$
5: $q = LINE(A, P)$
6: Construct s, the line parallel to q passing through R using Algorithm 4
7: $Q = s \cap \ell$
8: $\overline{PQ}$ is the result on ℓ

Exercise 3.2 *Convince yourself that $\overline{PQ} = \overline{AB}$.*

□

The above is different from the original construction and proof of correctness as given by Euclid in his Book of Elements. Interested readers may study a modern version of the original construction here.

3.4 Rational numbers are constructible

First, we can consider any given length as 1, measure it using a non-collapsing compass – which we just proved is equivalent to a collapsing compass – and add it to any point on a given line by marking it off with the compass. We can similarly subtract. The operations $S(n)$ and $P(n)$ are thus

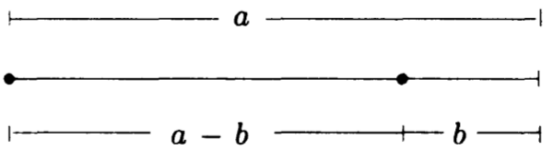


Figure 3.6: Construction of $a - b$.

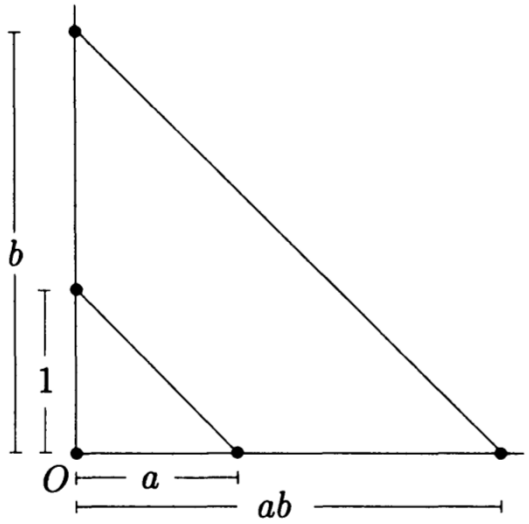


Figure 3.7: Construction of ab given a and b.

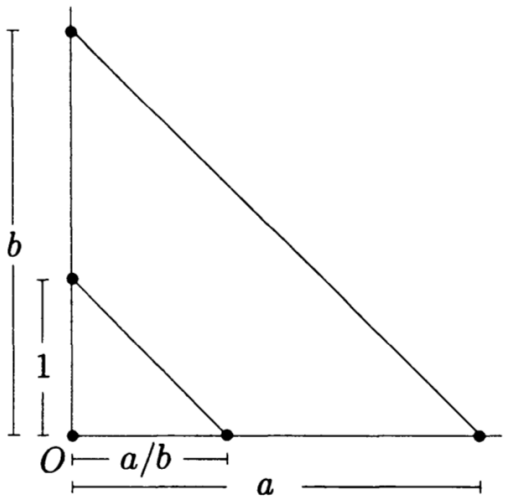


Figure 3.8: Construction of a/b given a and b.

realisable using ruler and compass. Consequently, the elements of the set $\mathbb{Z}$ are constructible. In Figures 3.5 and 3.6 we give the direct constructions for $a+b$ and $a-b$.

Exercise 3.3 *1. Describe a ruler and compass procedure for multiplication using repeated additions.*

2. Describe a ruler and compass procedure for division (computing quotient and remainder) using repeated subtractions.

Given integers a and b as line segments, we can also construct rational number ab and a/b directly using similar triangles. The construction of Figure 3.7 involves marking off the lengths a and b in two perpendicular segments from O, constructing the unit length in the direction of b, and constructing a line parallel to the line $\overline{a1}$ through a or b. The intercept of the parallel line in the direction of a then marks the length ab by similarity of the triangles.

We can similarly construct a/b as depicted in Figure 3.8. Rational numbers are thus constructible.

3.5 Euclid's GCD using ruler and compass

GCD of two integers $a > 0$, $b \geq 0$ is defined as the largest integer $d, d > 0$ that divides both a and b. Consider the following algorithm for computing the GCD:

$$gcd(a,b) = \begin{cases} a & \text{if } b = 0 \\ a & \text{if } a = b \\ gcd(a-b,b) & \text{if } a > b \\ gcd(a,b-a) & \text{if } b > a \end{cases}$$

Exercise 3.4 *1. Convince yourself that the above algorithmic specification (rule) is correct for computing GCD. Carry out the pencil and paper computation using the above algorithm for some special cases.*

2. Describe the procedure for executing the algorithm using ruler and compass.

The algorithm described above is from Euclid's Elements. You can find a description of it here. This is also considered to be the oldest non-trivial algorithm in common use.

Now that we have defined our first computational model, several questions arise. What are the full powers of the model? What are the other things that can be constructed? What are the limits of the model, and are there easily defied concepts that are not constructible? Can there be other computational models more powerful than ruler and compass? These are the kind of questions we interrogate every computational model with. We will revisit some of these questions in the latter chapters.

Problems

1. Construct, using ruler and compass, the perpendicular bisector of a line segment AB. Show that any point P on the perpendicular bisector is equidistant from A and B.

2. Given a triangle ABC, construct the three medians using ruler and compass. Argue that they intersect at a single point (the centroid).

3. Using Algorithm 3 (perpendicular construction), describe step by step how to construct the altitude from a vertex of a triangle. Illustrate your steps with a figure.

4. Given a line ℓ and an external point P, use Algorithm 4 (parallel construction) to draw the line parallel to ℓ through P. Prove that the two lines do not intersect.

5. Show that the compass-equivalence construction (Algorithm 5) indeed allows one to transfer a given length AB to an arbitrary point P on a line ℓ. Verify your construction with a worked example.

6. Describe a ruler and compass procedure for multiplication of two integers a, b using repeated additions. Demonstrate the construction for $a = 3, b = 4$.

7. Similarly, describe a ruler and compass procedure for division using repeated subtractions. Apply your method to compute the quotient and remainder when dividing a segment of length 11 into parts of length 3.

8. Using constructions based on similar triangles, show step by step how to obtain the product ab given line segments a and b.

9. Construct the rational number $\frac{3}{5}$ on a line, starting with a unit segment. Explain each step of your construction.

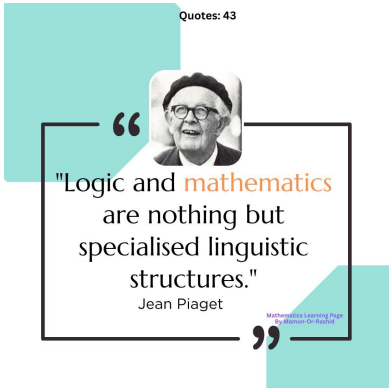
10. Apply Euclid's GCD algorithm (as given in Section 3.5) to the lengths $a = 21$, $b = 15$, using repeated subtraction with compass and ruler. Show all intermediate steps.

11. Prove that Euclid's GCD algorithm terminates in a finite number of steps for all $a, b \in \mathbb{N}$. (Hint: in each step one of the arguments strictly decreases.)

12. Challenge: Try to construct $\sqrt{2}$ using ruler and compass. (Hint: Use the Pythagoras theorem on a right triangle with sides $1, 1$.) Argue why this length is constructible.

Chapter 4

Abstraction turns problems and concepts into principles



Modern mathematics and computer science are built upon a few simple but very powerful ideas. Among the most important are the notions of *relations* and *functions*, which allow us to describe how objects are connected or transformed. Counting, infinity, and the ways in which sets can be grouped into classes help us measure size, structure, and complexity. These ideas may look abstract at first, but they underlie the methods used in algorithms, data structures, and logical reasoning.

In computer science, functions capture the essence of computation: a program takes inputs and produces outputs, just as a function does. Understanding one-one and onto functions helps us reason about whether information is lost, preserved, or fully covered. Equivalence classes and partitions allow us to organise data into categories. Modular arithmetic, often called "clock arithmetic," is fundamental in cryptography, error detection, and digital systems. Learning these concepts gives us a foundation to explore deeper mathematics and to apply it to practical computational problems.

4.1 Relations

The *Cartesian product* of two sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$. Thus,

$$A \times B = \{(a, b) \mid (a \in A) \text{ and } (b \in B)\}$$

A^n is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ such that $a_i \in A$ for all i. i.e.,

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$$

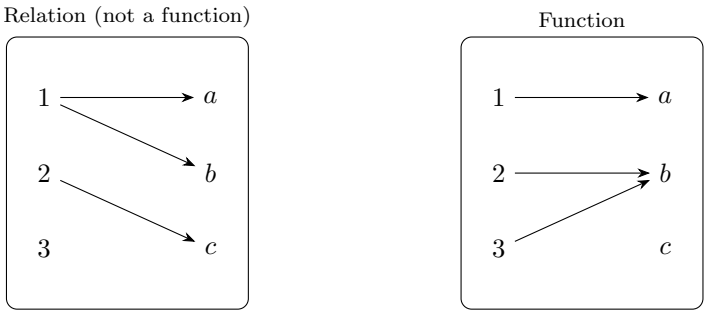


Figure 4.1: Relation vs function: In a relation, an element in A can be mapped to multiple elements in B, but not so in a function. In a function, all elements in A must be covered, but not necessarily so in a relation. The set B need not be fully covered in either.

A *relation* tells us which elements of one set are connected to elements of another.

A *binary relation* R from A to B is a subset of $A \times B$. It is a characterisation of the intuitive notion that some of the elements of A are related to some of the elements of B.

If $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$, then $R = \{(1, a), (2, b), (3, a)\}$ is a relation from A to B. Familiar binary relations from $\mathbb{N}$ to $\mathbb{N}$ are $=$, $\neq$, $<$, $\leq$, $>$, $\geq$. Thus the elements of the set $\{(0, 0), (0, 1), (0, 2), \ldots, (1, 1), (1, 2), \ldots\}$ are all members of the relation $\leq$ which is a subset of $\mathbb{N} \times \mathbb{N}$.

4.2 Function

A *function* from A to B – written as $f : A \to B$ – is a special relation in which:

1. every element of A is related to some element of B, and
2. no element of A is related to more than one element of B.

Equivalently, each input has *exactly one* output.

Some familiar examples of functions are

1. $+$ and $*$ (addition and multiplication) are functions of the type $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
2. $-$ (subtraction) is a function of the type $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$.
3. *div* and *mod* are functions of the type $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. If $a = q * b + r$ such that $0 \leq r < b$ and $a, b, q, r \in \mathbb{N}$ then the functions *div* and *mod* are defined as $div(a, b) = q$ and $mod(a, b) = r$. We will often write these binary functions as $a * b$, a *div* b, a *mod* b etc.
4. The binary relations $=$, $\neq$, $<$, $\leq$, $>$, $\geq$ are also functions of the type $f : \mathbb{N} \times \mathbb{N} \to \mathbb{B}$ where $\mathbb{B} = \{false, true\}$.
5. $f : \mathbb{N} \to \mathbb{N},\ f(x) = x^2$.

We write the definition of a function formally as follows.

A *function* from A to B is a binary relation f from A to B such that for *every* element $a \in A$ there is a *unique* element $b \in B$ so the $(a, b) \in f$ (or $f(a) = b$)[1]. We will use the notation $f : A \to B$ to denote a function f from A to B. The set A is called the *domain* of the function f and the set B is called the *co-domain* of the function f. The *range* of a function $f : A \to B$ is the set $\{b \in B \mid \text{for some } a \in A,\ f(a) = b\}$ denoting the subset of elements in B that are actually covered by f.

[1] This is sometimes written using mathematical notation as $\forall a \in A$, $\exists$ unique $b \in B$. $\forall$ is the usual symbol for *for all*, and $\exists$ is the usual symbol for *there exists*

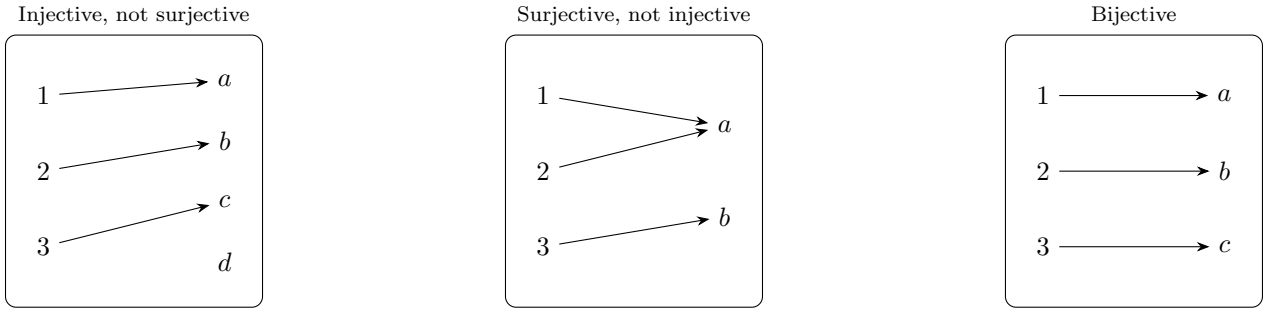


Figure 4.2: *One-one (injective)*: different inputs give different outputs. (like roll numbers: no two students share one roll); *Onto (surjective)*: every element of the codomain gets hit by *some* input. (no empty seats.); *Bijective*: both one-one and onto. (perfect pairing; has an inverse.)

4.2.1 One-One (injective), Onto (surjective), and bijective Functions

When we study functions, it is often not enough to know that "every input has exactly one output." We also want to understand how well the function uses its codomain and whether different inputs remain distinct after applying the function.

Think of a classroom with students and seats:

- If no two students sit in the same seat, the "assignment" of students to seats is one-one (injective).
- If every seat is occupied by at least one student, the assignment is onto (surjective).
- If both conditions happen together — each student has exactly one seat, and every seat is filled — then the assignment is bijective. In such a case we may also define an inverse function from seats to students.

The formal definitions below make the concepts precise.

Let $f : A \to B$ be a function. f is

Injective if whenever $f(a_1) = f(a_2)$ for $a_1, a_2 \in A$, we can conclude that $a_1 = a_2$

Surjective if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.

Bijective if it is both injective and surjective.

Example 4.1 *1.* $f : \mathbb{N} \to \mathbb{R},\ f(n) = 2n$ *is injective but not surjective (odd numbers are not covered).*

2. $g : \mathbb{N} \to \mathbb{N},\ g(0) = 0;\ g(n) = n - 1$ *is surjective but not injective (why?).*

4.3 Counting, Finite and Infinite Sets

Counting is one of the most fundamental activities in mathematics: it is how we measure the size of a set. At first glance this seems very straightforward — counting laddoos in a box or students in a class is familiar to everyone. However, mathematics asks us to extend this simple idea to more abstract settings: What does it mean for a set to be "finite"? How can we formally compare the sizes of different sets, especially when some sets are infinite? For finite sets, the answer is clear: we can match the elements of the set to the numbers $\{1, 2, \ldots, n\}$. For infinite sets, the situation is more subtle, but surprisingly we can still talk about "countable" sets — those whose elements can be placed in a one-to-one correspondence with the natural numbers $\mathbb{N}$. This point of view leads to some striking and important results: for instance, that the set of all even numbers, the set of all

integers, and even the set of all rational numbers are all countably infinite. At the same time, we will see later in this course that there are sets of numbers so large that they cannot even be listed in sequence: these are called uncountable sets. These distinctions between finite, countably infinite, and uncountable sets form the foundation for much of modern mathematics, and are crucial in computer science as well, where questions of size, encoding, and enumeration play a central role.

4.3.1 Finite sets

A set is *finite* if it has a finite number of elements. Formally, a set A is finite if there exists a natural number n and a bijection

$$f : A \to \{1, 2, \ldots, n\}.$$

This means that the elements of A can be paired exactly with the first n natural numbers.

Example 4.2 *The set $\{a, b, c\}$ is finite because we can define $f(a) = 1$, $f(b) = 2$, $f(c) = 3$, which is a bijection to $\{1, 2, 3\}$.*

4.3.2 Infinite sets and bijections to $\mathbb{N}$

A set is *infinite* if it is not finite. Some infinite sets are still "countable" because they can be put in one-to-one correspondence (bijection) with the natural numbers $\mathbb{N}$. In such a case the elements of the set can be enumerated as *first*, *second*. *third*, and so on.

Definition. A set A is *countably infinite* or *denumerable* if there exists a bijection $f : A \to \mathbb{N}$.

Example 4.3

1. *The natural numbers $\mathbb{N}$ are countably infinite via the trivial bijection $f(n) = n$.*
2. *The set of even naturals $E = \{0, 2, 4, 6, \ldots\}$ is countably infinite. Define $f : \mathbb{N} \to E$ by $f(n) = 2n$. This is a bijection.*
3. *The set of odd naturals $O = \{1, 3, 5, 7, \ldots\}$ is also countably infinite. Define $g : \mathbb{N} \to O$ by $g(n) = 2n + 1$. This is a bijection.*

4.3.3 Integers and Rationals are countable

The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ can be enumerated in a sequence:

$$0, -1, 1, -2, 2, -3, 3, -4, 4, \ldots$$

Define a bijection $h : \mathbb{N} \to \mathbb{Z}$ by

$$h(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even,} \\ -\frac{n+1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

This shows that $\mathbb{Z}$ is countable.

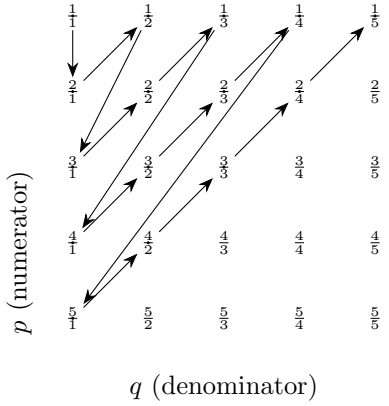
The rationals $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ are also countable, though the proof is less obvious.

Step 1. First, consider only the positive rationals $\mathbb{Q}^+$. We can arrange them in a grid with numerator along one axis and denominator along the other:

	1	2	3	...
1	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	...
2	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	...
3	$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	...
⋮	⋮	⋮	⋮	⋱

Note, however, that this does not give us an enumeration.

Step 2. Use Cantor's method: start at $\frac{1}{1}$, then $\frac{2}{1}, \frac{1}{2}$, then $\frac{3}{1}, \frac{2}{2}, \frac{1}{3}$, and so on, zig-zagging across the grid. This produces a sequence that eventually lists every positive rational.



Exercise 4.1 *1. Convince yourself that above ordering gives a bijection from* $\mathbb{N}$ *to ordered pairs* $(p, q), p > 0, q > 0$.

*2. Can you work out an explicit formula for the bijective function? (***This can be challenging***)*

Step 3. To avoid repetitions, we can restrict to fractions in lowest terms (e.g. $\frac{2}{2}$ is skipped since it equals $\frac{1}{1}$).

Step 4. To cover negative rationals as well, interleave them with positives:

$$0, \tfrac{1}{1}, -\tfrac{1}{1}, \tfrac{2}{1}, -\tfrac{2}{1}, \tfrac{1}{2}, -\tfrac{1}{2}, \ldots$$

This construction defines an explicit enumeration of $\mathbb{Q}$, so $\mathbb{Q}$ is countably infinite.

4.4 Equivalence Relations, Classes, and Partitions

In mathematics, we often want to group objects together when they share some common property. For example, in geometry all shapes that have the same size and shape are considered "congruent," and in number theory two integers that leave the same remainder when divided by n are considered "equivalent." These situations are captured formally by the concept of an *equivalence relation*.

Equivalence relations are important because they let us partition a large and possibly complicated set into smaller, simpler pieces (called *equivalence classes*). Each equivalence class collects all elements that are considered "the same" under the relation. Many areas of mathematics, and even computer science (e.g. hashing, classification, state-space reduction), rely on such partitions.

Definition. A relation R on a set A is an *equivalence relation* if for all $a, b, c \in A$:

- (Reflexive) $(a, a) \in R$,
- (Symmetric) $(a, b) \in R \Rightarrow (b, a) \in R$,
- (Transitive) $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$.

We will also write $(a, b) \in R$ as $a \; R \; b$ or as $a \sim b$.

Definition. Set of elements that are equivalent form an *e*quivalent class. Given $a \in A$, the *equivalence class* of a under relation R is

$$[a] = \{x \in A : (a, x) \in R\}.$$

Here are some example of equivalent relations

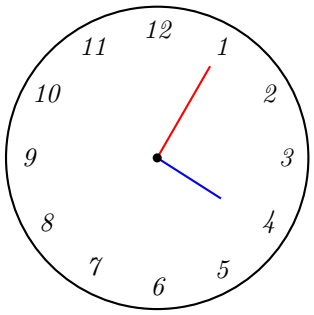
Example 4.4 *1.* ***Same birthday.*** *On the set of all students, define $x \sim y$ if x and y have the same birthday. Each equivalence class is a group of students born on the same day.*

2. ***Congruent triangles.*** *On the set of all triangles in the plane, define $T_1 \sim T_2$ if T_1 and T_2 are congruent (same shape and size). This relation is reflexive (every triangle is congruent to itself), symmetric (if T_1 is congruent to T_2, then T_2 is congruent to T_1), and transitive (if T_1 is congruent to T_2 and T_2 to T_3, then T_1 is congruent to T_3).*

3. ***Sets with same cardinality.*** *Clearly, $A \sim B$ if there exists a bijection between A and B. Since bijective functions have inverses that are bijections, and composition of two bijective functions is a bijection, we have that sets with same cardinality for an equivalent class.*

4. ***Congruence of integers (mod n).*** *Define $a \sim b$ if n divides $a-b$. This is reflexive ($a-a=0$ is divisible by n), symmetric (if $a-b$ divisible by n, so is $b-a$), and transitive (if $a-b$ and $b-c$ divisible by n, so is $a-c$). The equivalence classes are the sets of integers with the same remainder when divided by n.*

For example, on a 12-hour clock, $16 \sim 4 \pmod{12}$; and, for the minutes hand, $65 \sim 5 \pmod{60}$;



Exercise 4.2 *Which of the following relations are not equivalent relations and why?*

1. *a R b if $a = b$.*
2. *a R b if $a \leq b$.*
3. *a R b if $gcd(a, b) = 1$.*

4.4.1 Equivalence classes and partitions

Theorem 4.1 *An equivalence relation defined on set A partitions A into disjoint equivalence classes: every element of A belongs to exactly one equivalence class, and the classes together cover all of A.*

Proof: We have to argue for two things – first, no element belongs to two or more equivalent classes; and second, the union of all the equivalence classes covers the whole set.

Suppose x belongs to two distinct equivalence classes. Then there exits $a, b \in A$ such that $x \sim a$ and $x \sim b$ but $a \not\sim b$. But this is not possible because $\sim$ is symmetric and transitive.

And, by reflexivity, each x is at least equivalent to itself. So, no element is left out. □

Example 4.5 *The relation Congruence of integers (mod 3) split $\mathbb{Z}$ into three classes:*

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}, \quad [1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \quad [2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

These three classes form a partition of $\mathbb{Z}$.

4.5 Modular Arithmetic, Magic Squares, and One-Time Pads

4.5.1 Modular arithmetic

Consider, for example, the set $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ consists of all integers modulo 7. This means that we can perform addition and multiplication, and then reduce the result to its remainder upon division by 7.

Addition. Examples:

$$3 + 5 \equiv 1 \pmod 7, \quad 6 + 4 \equiv 3 \pmod 7.$$

Every element has an *additive inverse*, i.e. a number x such that $a + x \equiv 0 \pmod 7$.

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

Multiplication. Examples:

$$3 \times 5 \equiv 1 \pmod 7, \quad 4 \times 6 \equiv 3 \pmod 7.$$

For multiplication, every nonzero element has a *multiplicative inverse*, i.e. $a \cdot x \equiv 1 \pmod 7$.

$$1^{-1} = 1, \quad 2^{-1} = 4, \quad 3^{-1} = 5, \quad 6^{-1} = 6.$$

Notice that 0 has no multiplicative inverse.

Thus $(\mathbb{Z}_7, +)$ is a finite arithmetic structure under addition, and $(\mathbb{Z}_7^\times, \cdot)$ with $\{1, 2, 3, 4, 5, 6\}$ is a finite arithmetic structure under multiplication. This has many interesting applications.

4.5.2 Magic Squares

A *magic square* is an arrangement of numbers in a square grid such that the sums of each row, column, and both diagonals are the same. Modular arithmetic allows us to construct magic squares in structures like $\mathbb{Z}_n$, where the "magic sum" is computed modulo n. This is a playful illustration of modular addition applied to combinatorial design.

A simple way to build a magic square *modulo* n is to take any ordinary magic square and reduce each entry modulo n. The LuoShu 3×3 square, which has a rich history in occult and numerology is given as

4	9	2
3	5	7
8	1	6

(each line sums to 15)

It reduces modulo 7 to

4	2	2
3	5	0
1	1	6

$\in \mathbb{Z}_7^{3\times 3}$.

Since $15 \equiv 1 \pmod 7$, every row, column, and diagonal now sums to $\overline{1} \in \mathbb{Z}_7$. For instance,

$$4 + 2 + 2 \equiv 8 \equiv 1 \pmod 7, \qquad 3 + 5 + 0 \equiv 8 \equiv 1 \pmod 7, \qquad 1 + 5 + 2 \equiv 8 \equiv 1 \pmod 7.$$

The diagonals also satisfy $4 + 5 + 6 \equiv 15 \equiv 1 \pmod 7$ and $2 + 5 + 1 \equiv 8 \equiv 1 \pmod 7$.

General recipe (odd moduli). Let S be any 3×3 magic square over the integers with magic sum M. For any modulus $n \geq 2$, the entry-wise reduction $\overline{S} \in (\mathbb{Z}_n)^{3\times 3}$ is a magic square in $\mathbb{Z}_n$ with magic sum $\overline{M} \in \mathbb{Z}_n$, because modular addition preserves equality of sums. More generally, for any $\alpha, \beta \in \mathbb{Z}_n$, the entry-wise transform $\alpha S + \beta$ is again a magic square modulo n with magic sum $\alpha M + 3\beta \pmod n$.

4.5.3 Perfect Secrecy and One-Time Pads

The idea of modular arithmetic is also central in cryptography. In the *one-time pad*, a message (plaintext) is converted into numbers (say letters $A = 0, \ldots, Z = 25$). A random secret key of the same length is chosen, and encryption is done by addition modulo 26:

$$\text{ciphertext}_i \equiv \text{plaintext}_i + \text{key}_i \pmod{26}.$$

Decryption uses subtraction modulo 26.

Claude Shannon showed that if the key is truly random, used only once, and kept secret, then the ciphertext reveals no information about the plaintext: this is called *perfect secrecy*. Thus, a simple application of modular addition gives us a theoretically unbreakable cryptosystem.

Summary

Modular arithmetic provides the framework to work with remainders in a structured way. It underlies recreational mathematics like magic squares, as well as fundamental cryptographic protocols such as the one-time pad.

Problems

1. Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. (a) List all elements of the Cartesian product $A \times B$. (b) Define two different binary relations $R_1, R_2 \subseteq A \times B$. (c) Which of them, if any, are functions?

2. Show that the relation $\leq$ on $\mathbb{N}$ is a subset of $\mathbb{N} \times \mathbb{N}$. Explicitly write out the first ten elements of this relation.

3. Give an example of a relation from $\{1, 2, 3\}$ to $\{a, b\}$ that is not a function. Explain why it fails to satisfy the definition of a function.

4. Consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = 2n$. Argue that f is injective but not surjective.

5. Consider the function $g : \mathbb{N} \to \mathbb{N}$ defined by

$$g(0) = 0, \qquad g(n) = n - 1 \text{ for } n > 0.$$

   Show that g is surjective but not injective.

6. Let $h : \mathbb{Z} \to \mathbb{Z}$ be defined by $h(x) = x + 5$. Prove that h is bijective and describe its inverse function.

7. Define the function $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $p(a, b) = a \times b$. Argue formally that p is a well-defined function.

8. Construct an example of a function $f : A \to B$ where $A = \{1, 2, 3, 4\}$, $B = \{a, b\}$ that is neither injective nor surjective. Explain why.

9. Prove that if a function $f : A \to B$ is bijective, then there exists a unique inverse function $f^{-1} : B \to A$ such that $f^{-1}(f(a)) = a$ for all $a \in A$.

10. Consider the function $f : \mathbb{N} \to \mathbb{N}$ defined recursively as

$$f(0) = 0, \quad f(n + 1) = f(n) + (2n + 1).$$

    Show that $f(n) = n^2$. What kind of function is this (injective, surjective, bijective)?

11. Give an everyday example (outside mathematics) of: (a) an injective mapping, (b) a surjective mapping, and (c) a bijective mapping.

12. Challenge: Prove or disprove — the composition of two injective functions is injective, and the composition of two surjective functions is surjective. What about bijective functions?

13. On the set $\{1, 2, 3, 4, 5, 6\}$, define a relation R by $a \sim b$ if $a - b$ is divisible by 2.

    (a) Show that R is an equivalence relation.

    (b) List the equivalence classes.

14. Consider the relation "x has the same number of letters as y" on the set of English words. Prove or disprove that it is an equivalence relation. What do the equivalence classes look like?

15. Work out the addition and multiplication tables of $\mathbb{Z}_5$. Identify all additive and multiplicative inverses.

16. In $\mathbb{Z}_7$, solve the linear congruence $3x \equiv 2 \pmod 7$.

17. Find all solutions to $x^2 \equiv 1 \pmod{15}$.

18. Construct a bijection between the set of even numbers and $\mathbb{N}$. Then, using a diagram, show how integers $\mathbb{Z}$ can be listed in sequence, proving that they are countable.

19. Show that the set of rational numbers $\mathbb{Q}$ is countable by describing an explicit enumeration strategy.

20. Verify that the LuoShu square

4	9	2
3	5	7
8	1	6

    is a magic square. What is its magic sum?

21. Construct a 3×3 magic square modulo 7 using the method of reducing an ordinary magic square. What is the magic sum in $\mathbb{Z}_7$?

22. In a one-time pad over the alphabet $\{A = 0, B = 1, \ldots, Z = 25\}$, encrypt the message `MATH` with the key `CODE`. Show the numerical steps modulo 26 and give the ciphertext.

23. Explain why re-using the same key in a one-time pad scheme can destroy perfect secrecy. Give a simple example with short strings.