Lecture Notes: Quantitative Reasoning and Mathematical Thinking[1]

Subhashis Banerjee

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

October 15, 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.

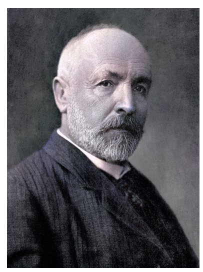
Early mathematics was computational when the emphasis was on finding methods to obtain solutions. However, over the years, the disciplines of mathematics and computer science – the subject of designing algorithms for problem solving – have diverged. In mathematics abstraction is symbolic and logical. 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 to construct effective procedures – designing algorithms that solve problems efficiently, often under constraints of time, memory, and real-world complexity. The power lies in execution and exploration — trying to 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.

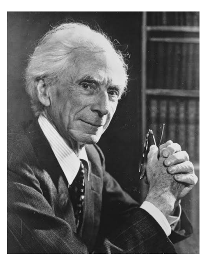
In this course we will try to cover some fundamentals of all of the above.

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

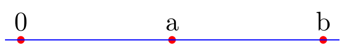
2.1 Numbers

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

```
procedure ADD(a, b)
    counter ← 0
    sum ← a
    while counter < b do
        sum ← sum + 1
        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.

```
procedure SUBTRACT(a, b)
    counter ← 0
    while counter < b do
        a ← a − 1
        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

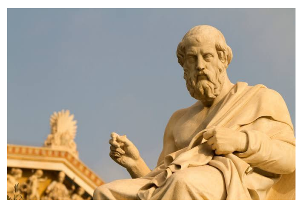
   $$A=\{x \mid x \text{ is an even number less than } 20\},\quad B=\{x \mid x \text{ is a prime number less than } 20\}.$$

   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

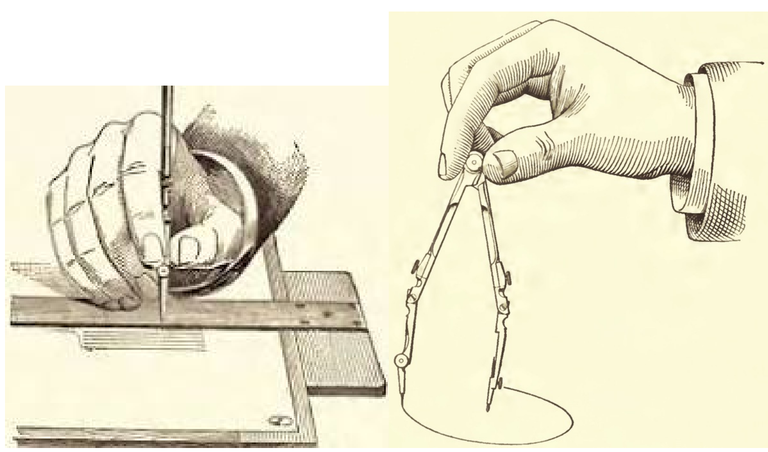


Figure 3.1: Ruler and compass. We will assume that the ruler is unmarked, and lengths can only be measured by adjusting the width of the compass.

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.

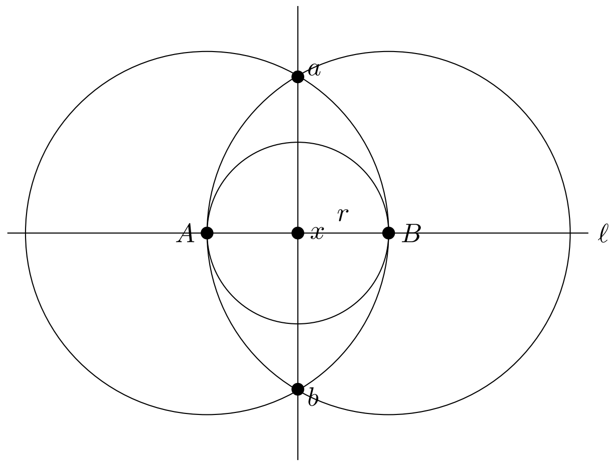


Figure 3.2: Constructing a line perpendicular to a given line passing through a point

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

procedure PERPENDICULAR(x, ℓ)
  $c = CIRCLE(x, r)$, where r is a random length
  $(A, B) = c \cap \ell$
  $c_A = CIRCLE(A, 2r)$
  $c_B = CIRCLE(B, 2r)$
  $(a, b) = c_A \cap c_B$
  $result = LINE(a, b)$

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.

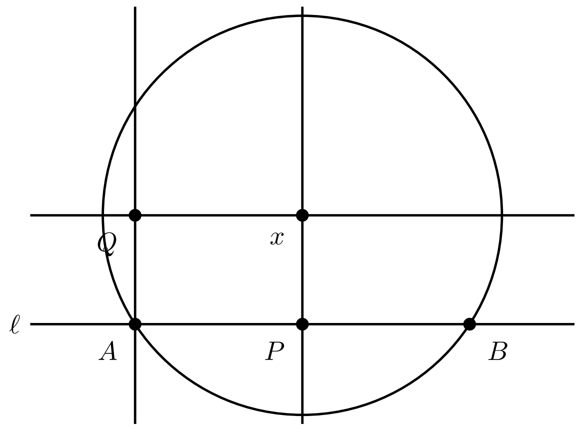


Figure 3.3: Constructing a line parallel to a given line passing through a point

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 point*

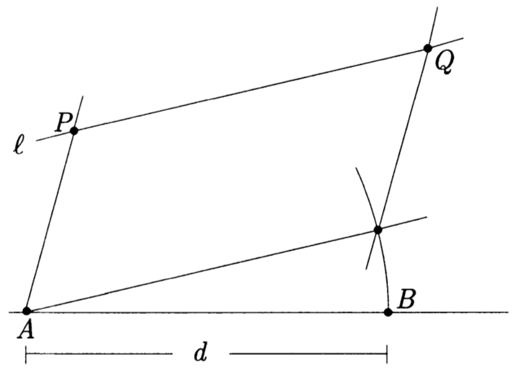


Figure 3.4: A compass-equivalence construction

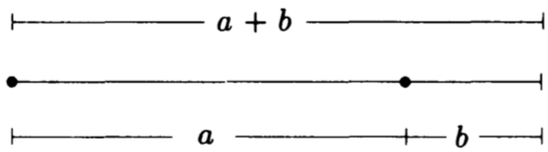


Figure 3.5: Construction of $a + b$.

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

procedure COMPASS-EQUIVALENCE(A,B,ℓ,P)
  $c = CIRCLE(A, B)$; note that $\overline{AB} = d$
  Construct p, the line parallel to ℓ passing through A using Algorithm 4
  $R = c \cap p$
  $q = LINE(A, P)$
  Construct s, the line parallel to q passing through R using Algorithm 4
  $Q = s \cap \ell$
  $\overline{PQ}$ 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

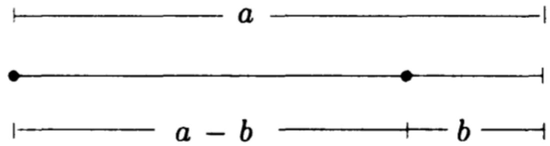


Figure 3.6: Construction of $a - b$.

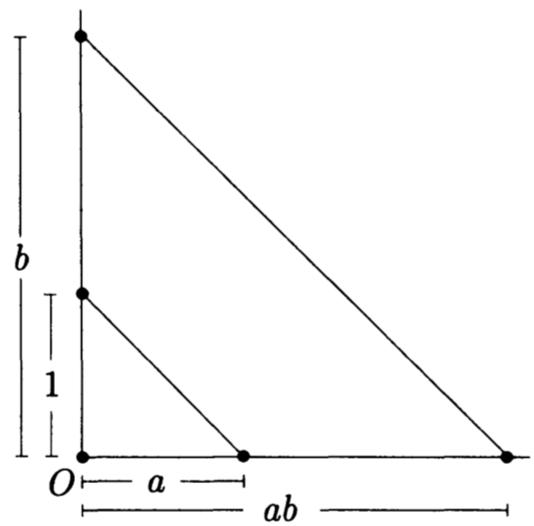


Figure 3.7: Construction of ab given a and b.

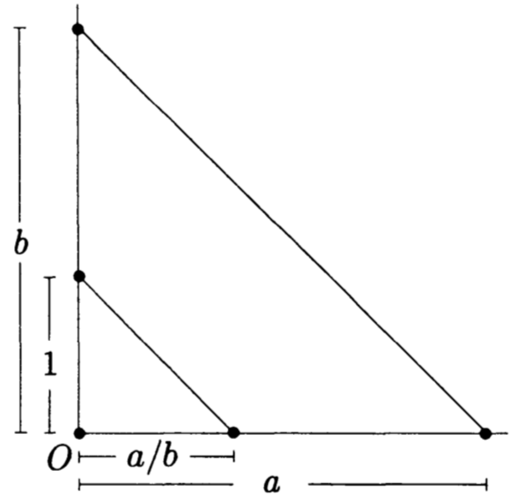


Figure 3.8: Construction of a/b given a and b.

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.

Exercise 3.5 *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.*

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.

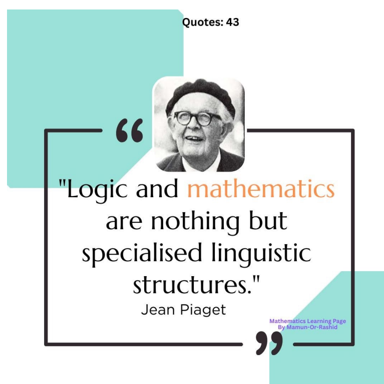
9. Construct the rational number $\frac{3}{5}$ on a line, starting with a unit segment. Explain each step of your construction.

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.)

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.,

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

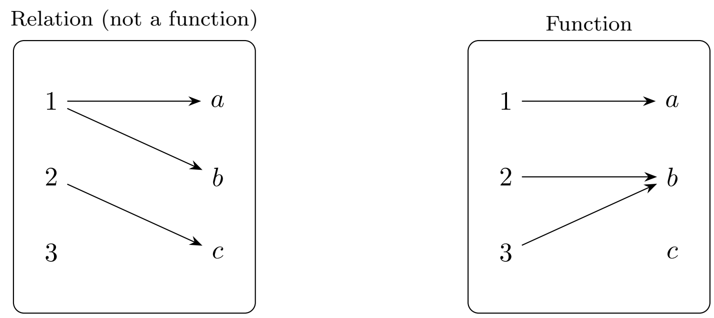


Figure 4.1: Relation vs function: In a relation, an element in A can be mapped to multiple elements in B, but not so in a function. In a function, all elements in A must be covered, but not necessarily so in a relation. The set B need not be fully covered in either.

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*

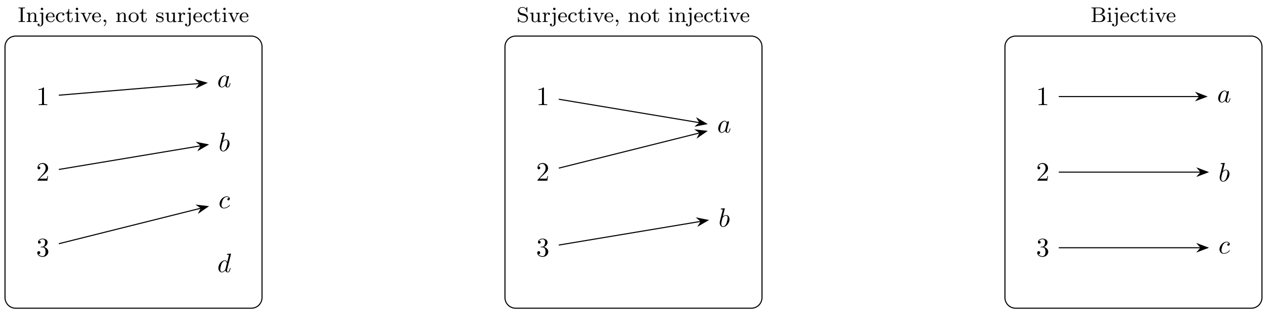


Figure 4.2: *One-one (injective)*: different inputs give different outputs. (like roll numbers: no two students share one roll); *Onto (surjective)*: every element of the codomain gets hit by *some* input. (no empty seats.); *Bijective*: both one-one and onto. (perfect pairing; has an inverse.)

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

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

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* $E = \{0, 2, 4, 6, \dots\}$ *is countably infinite. Define* $f : \mathbb{N} \to E$ *by* $f(n) = 2n$*. This is a bijection.*

3. *The set of odd naturals* $O = \{1, 3, 5, 7, \dots\}$ *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 $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ can be enumerated in a sequence:

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

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.

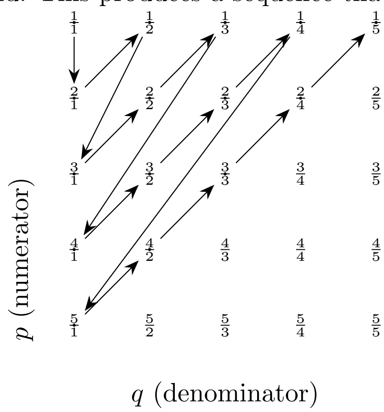
The rationals $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ are also countable, though the proof is less obvious.

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:

$$\begin{array}{c|cccc} & 1 & 2 & 3 & \dots \\ \hline 1 & \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \dots \\ 2 & \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \dots \\ 3 & \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

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 $a \mathrel{R} b$ or as $a \sim b$.

Definition. Set of elements that are equivalent form an equivalent 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

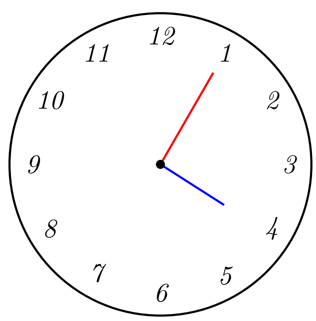
Example 4.4 *1. **Same birthday.** On the set of all students, define $x \sim y$ if x and y have the same birthday. Each equivalence class is a group of students born on the same day.*

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 $a - b$. We write this as $a \sim b \pmod{n}$ or $a \equiv b \pmod{n}$. 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 $A = 0, \dots, Z = 25$). 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?

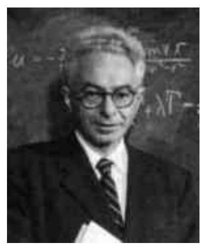
21. Construct a 3×3 magic square modulo 7 using the method of reducing an ordinary magic square. What is the magic sum in $\mathbb{Z}_7$?

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.

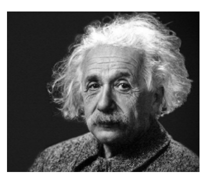
23. Explain why re-using the same key in a one-time pad scheme can destroy perfect secrecy. Give a simple example with short strings.

Chapter 5

We need precision in thought and action to win arguments



“Mathematics as an expression of the human mind reflects the active will, the contemplative reason, and the desire for aesthetic perfection. Its basic elements are logic and intuition, analysis and construction, generality and individuality.” – Richard Courant



“Pure mathematics is, in its way, the poetry of logical ideas.” – Albert Einstein

Logic is the language of reasoning. Whenever we argue in mathematics, make a claim in science, or even decide something in everyday life, we implicitly use the rules of logic. Boolean logic, named after the mathematician George Boole, provides a precise mathematical framework to study truth and falsity.

In this chapter, we will introduce the basic building blocks of logic, learn how to represent them with truth tables, explore important rules like De Morgan’s laws, understand how to work with more than two statements at a time, and examine subtle but important ideas such as vacuous truth. Equally importantly, we will also study some of the standard methods of writing mathematical proofs. These include direct proofs, proofs by counter-examples, proofs by contrapositive, proofs by contradiction, and proofs by induction. Learning these strategies will allow you to apply logical reasoning to establish mathematical results with clarity and rigour.

The aim of this chapter is to provide a foundation that is both rigorous and intuitive, preparing you for deeper study in mathematics and computer science, where careful reasoning and proof techniques are essential.

5.1 Propositions, Basic Boolean Logic and Truth Tables

In mathematics and computer science, many problems boil down to deciding whether something is *true* or *false*. A statement that can be judged true or false is called a *proposition*. For example:

- "2 is an even number" is true.
- "5 is less than 3" is false.
- "$x + 2 = 7$" is a proposition, but its truth depends on the value of x.

Boolean logic studies how we can combine such statements using logical operations like **AND**, **OR**, **NOT**, and **IMPLIES**. These operations are the foundation of digital circuits, programming languages, and formal mathematical proofs.

5.1.1 The basic operations

We denote truth values as T (true) and F (false).

Conjunction (AND). The statement $p \wedge q$ is true only if both p and q are true. *Example:* "I will go for a walk *and* it is sunny." This is only true if both parts are true.

Disjunction (OR). The statement $p \vee q$ is true if at least one of p or q is true. *Example:* "I will have tea *or* coffee." In everyday language, "or" can sometimes mean "one but not both," but in logic the inclusive sense is used: tea, coffee, or both makes the statement true.

Negation (NOT). The statement $\neg p$ has the opposite truth value of p. *Example:* If $p =$"It is raining," then $\neg p =$"It is not raining."

Implication (IF...THEN). The statement $p \Rightarrow q$ means "p implies q" or "If p then q." It is false only when p is true but q is false. In all other cases it is true. Think of it as a promise: "If you pass the QRMT course, then you will get a laddoo."[1] The only way the promise fails is if you pass but still do not get a laddoo. If (unfortunately) you do not pass, the promise is not broken if you still get a laddoo, so the implication is considered true. Passing QRMT is sufficient to get a laddoo, so we say that "p is *sufficient* for q". Passing the course and yet not getting a laddoo will make the promise false, so we say that "q is *necessary* for p".

Biconditional (IF AND ONLY IF). The statement $p \Leftrightarrow q$ is true when both $p \Rightarrow q$ and $q \Rightarrow p$, i.e., p and q have the same truth value, either both true or both false. *Example:* "A number is even if and only if it is divisible by 2."

Exclusive OR (XOR). The statement $p \oplus q$ is true when exactly one of p or q is true, but not both. *Example:* "You can win first prize *or* second prize." You cannot win both at the same time.

5.1.2 Truth tables

Truth tables let us list all possible truth values of statements and see how the logical operations work.

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \oplus q$
T	T	T	T	T	T	F
T	F	F	T	F	F	T
F	T	F	T	T	F	T
F	F	F	F	T	T	F

[1]Note, however, that I am making no such promise. It is just a supposition for making a point.

De Morgan's Laws

These laws explain how negation interacts with AND and OR:

$$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q), \qquad \neg(p \vee q) \equiv (\neg p) \wedge (\neg q).$$

Example 5.1 *Let $p =$ "bring a wizard to the QRMT class" $q =$ "bring a dragon to the QRMT class" Then $\neg(p \vee q)$ means "do not bring a wizard or a dragon to the QRMT class," which is the same as "do not bring a wizard to the QRMT class* and *do not bring a dragon to the QRMT class".*

Example 5.2 *In contrast, $\neg(p \wedge q)$ means "It is not the case that you bring both a wizard and a dragon to the QRMT class," which is logically equivalent to "either you do not bring a wizard to the QRMT class* or *you do not bring a dragon to the QRMT class (or both)."*

Exercise 5.1

1. *Convince yourself that the truth functions given in the table above, and the De Morgan's laws, are reasonable.*
2. *In particular, it is the truth table of $p \Rightarrow q$ that is most commonly used in logical deductions. Try to think of a few example English sentences that corroborate the truth table; especially the third row.*
3. *Argue, using both truth tables and language-based examples, that $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$. This is called* contrapositive*.*
4. *Argue, using both truth tables and language-based examples, that $p \Rightarrow q$ is equivalent to $\neg p \vee q$.*
5. *Argue, using both truth tables and language-based examples, that $p \Leftrightarrow q$ is equivalent to $\neg(p \oplus q)$.*
6. *Sometimes, in everyday life, we observe q, and hypothesize p and $p \Rightarrow q$, i.e., we hypothesize that p may have caused q. This is called* abductive reasoning*. Argue that such abductive reasoning will violate our rules of deduction in mathematics. However, abductive reasoning is essential for the sciences and the social sciences. Can you reason why, perhaps through some examples? The hypotheses generated through abductive reasoning of course need to be validated, even in the sciences and the social sciences.*

The truth tables that underlie propositional logic are not empirical discoveries but conventions inherited from linguistic and philosophical traditions. They represent a form of "agreed upon truth," codifying how we collectively interpret connectives such as "and," "or," "not," and "implies." In this sense they are *axiomatic* in nature: we do not prove that $\neg(p \vee q)$ should behave like $(\neg p \wedge \neg q)$, we simply accept the tabular assignments as the foundation upon which deductions are made. Logical proofs then proceed within this framework of shared agreement. If any one of us refuses to accept these conventions — if, for example, someone insists that "and," "or," or "implies" should work differently — then there is no common ground to move forward, and the very possibility of building logical arguments collapses.

5.1.3 Three-variable examples of truth tables

When we have three propositions p, q, r, there are $2^3 = 8$ possible combinations of truth values. Truth tables become longer, but the method is the same.

Example 1. Consider $p \wedge (q \vee r)$. We first compute $q \vee r$, then combine with p using AND.

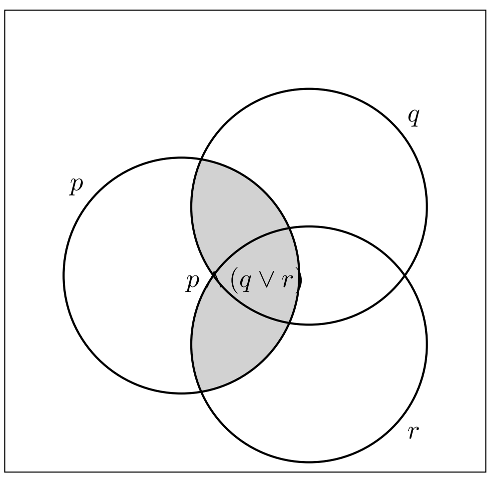
p	q	r	$q \lor r$	$p \land (q \lor r)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

Example 2. Consider $(p \Rightarrow q) \land (q \Rightarrow r)$. This corresponds to chaining two implications: "If p then q, and if q then r."

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \land (q \Rightarrow r)$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	F
T	F	F	F	T	F
F	T	T	T	T	T
F	T	F	T	F	F
F	F	T	T	T	T
F	F	F	T	T	T

Venn diagram illustration

The formula $p \land (q \lor r)$ can also be illustrated with sets. Think of p, q, r as sets of outcomes where each proposition is true. The shaded area corresponds to outcomes where p is true *and* at least one of q or r is true.



5.2 Vacuous Truth

The third line of the truth table for $p \Rightarrow q$, which suggests that if p is *false* and q is *true*, then $p \Rightarrow q$ is *true*, requires special attention. This forms the basis for many subtle logical arguments. A statement of the form "If p then q" is called an implication. As we saw, an implication is only false if p is true and q is false. Therefore, if p is false, the implication is always true. This phenomenon is called *vacuous truth*.

Example 5.3 *1. "If 5 is even, then 5 is prime." Since 5 is not even, the whole statement is true, regardless of the second part.*

2. *"All unicorns have wings." This can be written as "For every x, if x is a unicorn then x has wings." Since there are no unicorns, the condition never applies, and so the statement is vacuously true.*

3. *"If I am the king of France, then $2 + 2 = 5$." Because the condition "I am the king of France" is false, the implication is true.*

Vacuous truth is not a trick — it is a necessary feature of logic. It ensures that statements of the form "All elements of an empty set have property P" are automatically true. For example: "All prime numbers greater than 1000 and less than 1001 are even." There are no such numbers, so the statement is vacuously true.

We will use this quite a bit in the latter chapters.

5.3 Mathematical proofs

A proof is a method for establishing the truth of a statement. We use different methods in different spheres of life:

Rigour	Truth type	Field	Truth teller
0	Word of God	Religion	God/Priests
1	Authoritative truth	Business/School	Boss/Teacher
2	Legal truth	Judiciary	Law/Judge/Lawmakers
3	Philosophical truth	Philosophy	Plausible argument
4	Scientific truth	Physical sciences	Experiments/Observations
5	Statistical truth	Statistics	Data sampling
6	Mathematical truth	Mathematics	Logical deduction

Mathematical reasoning applies the highest standards of rigour for what may be considered as a *proof*, but only for very tightly defined domains. In mathematics we do not accept statements as true merely because they seem plausible or reasonable, or because many examples seem to support them. A *proof* is a logically complete argument that establishes truth from agreed assumptions, which may be definitions, axioms, or previously proved results. This chapter presents some core proof techniques, each with its own "feel" and natural use cases:

1. **Proof by Explicit Construction** — to prove that an element with some qualifying property exists, it is sufficient to construct an example.

2. **Proof by Counter-Example** — to disprove a universal claim, find one instance where it fails.

3. **Direct Proof** — derive the conclusion straight from the hypothesis using definitions and algebra.

4. **Proof by Contradiction** — assume the negation of what you want, reach an impossibility, and conclude the original claim.

5. **Proof by Contrapositive** — prove the logically equivalent statement $\neg Q \Rightarrow \neg P$ instead of $P \Rightarrow Q$.

6. **Proof by the Pigeonhole Principle** — to prove using the principle that if more objects are placed into fewer containers, then at least one container must hold more than one object.

7. **Proof by exhaustion of cases** — prove that statement hold for all of an exhaustive set of cases.

8. **Proof by Induction** — prove a base case and a step that carries truth from n to n+1. We will cover this in the next chapter.

Along the way, we emphasize *how* to think when choosing a technique.

5.3.1 Proof by Explicit Construction

A *proof by explicit construction* demonstrates the truth of a statement of the form "there exists x such that $P(x)$" by actually exhibiting such an x and verifying that it satisfies $P(x)$. This is perhaps the most concrete kind of existence proof: instead of reasoning abstractly, we build or display the required object [2].

In our earlier discussion of *ruler and compass* constructions in Section 3 we showed, step by step, how to construct a length $a+1$ from a given length a, or how to realize the greatest common divisor of two numbers geometrically. Each of those is an instance of explicit construction: the proof of existence of a geometric object lies in the instructions themselves.

Here are some other examples of proof by explicit construction.

Theorem 5.1 *There exist integers x, y such that $14x + 21y = 7$.*

Proof: We explicitly construct one such solution: take $x = -1$, $y = 1$. Then

$$14(-1) + 21(1) = -14 + 21 = 7.$$

Thus such integers exist. In fact, by varying x and y we can generate an infinite family of solutions, but the single explicit example suffices to establish existence. □

Theorem 5.2 *There exist integers a, b, c such that $a^2 + b^2 = c^2$.*

Proof: Exhibit $(a, b, c) = (3, 4, 5)$. Indeed,

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2.$$

Hence such integers exist. This triple is explicitly constructed and is known as the smallest nontrivial Pythagorean triple. □

Theorem 5.3 *For any rationals $r < s$, there exists a rational q with $r < q < s$.*

Proof: Explicitly construct $q = \frac{r+s}{2}$. Because $r < s$, we clearly have $r < q < s$. Moreover, since r and s are rational, their average q is also rational. Thus such a q exists. □

Theorem 5.4 *There exist integers x, y such that*

$$35x + 22y = 1.$$

Proof: To construct a solution, we compute the greatest common divisor of 35 and 22.

$$\begin{aligned} 35 &= 1 \cdot 22 + 13, \\ 22 &= 1 \cdot 13 + 9, \\ 13 &= 1 \cdot 9 + 4, \\ 9 &= 2 \cdot 4 + 1. \end{aligned}$$

Now back-substitute to express 1 as a combination of 35 and 22:

$$1 = 9 - 2 \cdot 4.$$

But $4 = 13 - 1 \cdot 9$, so

$$1 = 9 - 2(13 - 9) = 3 \cdot 9 - 2 \cdot 13.$$

[2] In ancient Mesopotamia (ca 2000 BCE), Babylonian mathematicians used algorithmic procedures to solve linear and quadratic equations for specific examples. The ancient Greeks – most notably Euclid (ca 300 BCE) – introduced geometric construction as a core part of geometric proofs. The kuṭṭaka (pulverizer) algorithm of Āryabhaṭa (5^{th} c) (5^{th} c), Jayadeva (c. 10^{th}–11^{th} c.), and later Bháskara II (12^{th} c.) is a direct construction of integer solutions to linear Diophantine equations. Before the 19^{th} century most proofs were constructive in nature.

Now substitute $9 = 22 - 13$:

$$1 = 3(22 - 13) - 2 \cdot 13 = 3 \cdot 22 - 5 \cdot 13.$$

Next, substitute $13 = 35 - 22$:

$$1 = 3 \cdot 22 - 5(35 - 22) = -5 \cdot 35 + 8 \cdot 22.$$

Thus, one explicit solution is

$$x = -5, \quad y = 8.$$

□

Remark. Equations such as above are called *linear Diophantine equations*. A solution may not always exist. The above method of finding a solution if it exists is called the *Extended Euclidean algorithm*, which not only proves that solutions exist when $\gcd(35, 22) = 1$, but by working through the steps we explicitly *construct* the solution [3].

Theorem 5.5 *The integer* 5 *has a multiplicative inverse modulo* 17*.*

Proof: We need an integer x such that

$$5x \equiv 1 \pmod{17}.$$

This is equivalent to solving the linear Diophantine equation

$$5x + 17y = 1$$

for integers x, y.

Apply the Euclidean algorithm:

$$\begin{aligned} 17 &= 3 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

Now back-substitute:

$$1 = 5 - 2 \cdot 2.$$

But $2 = 17 - 3 \cdot 5$, so

$$1 = 5 - 2(17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17.$$

Thus

$$1 = 7 \cdot 5 + (-2) \cdot 17,$$

which shows that $x = 7$, $y = -2$ is an explicit solution.

Therefore

$$5 \cdot 7 \equiv 1 \pmod{17},$$

so 7 is the multiplicative inverse of 5 modulo 17. □

Remark. This construction not only proves that 5 has an inverse modulo 17, but also produces the explicit inverse 7. In fact, the extended Euclidean algorithm always gives such a construction whenever $\gcd(a, m) = 1$.

[3] The origins of this algorithm can be traced back to the **kuṭṭaka** (pulverizer) algorithm of Āryabhaṭa (5^{th} c), Jayadeva (c. 10^{th}–11^{th} c.) and later Bháskara II (12^{th} c.) refined and applied the kuṭṭaka extensively. Bháskara in the Līlāvatī and Bījagaṇita gives worked examples of solving linear Diophantine equations with what is recognizably the extended Euclid method.

When to prove by explicit construction. Proof by explicit construction is particularly valuable when the question is "does there exist?" and the object in question is concrete enough to build or write down. It contrasts with nonconstructive methods (such as contradiction or pigeonhole arguments, which we will study later) where existence is established without showing a specific example. Both are mathematically valid, but constructive proofs have the added advantage of providing insight into the nature of the object itself.

5.3.2 Proof by Counter-Example

A universal statement $\forall x\, P(x)$ is false if there exists a single x with $\neg P(x)$. Producing such an x *disproves* the claim completely [4]. For example, consider the exchange of Figure 5.1 on social media

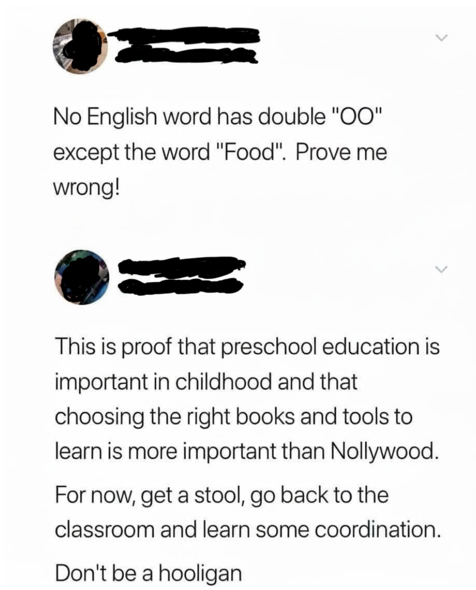


Figure 5.1: A counter-example to a universal claim

Exercise 5.2 *Which basic logical reasoning method has been used here to disprove the universal claim?*

Example 5.4 *Let us consider a few more examples.*

1. **Claim**: *"The product of any two prime numbers is prime."*
   Counter-example. $2 \cdot 3 = 6$ *is not prime.*

2. **Claim**: *"For all integers n, the number $n^2 + n + 41$ is prime."*
   Counter-example. *At $n = 41$, $41^2 + 41 + 41 = 41 \cdot 43$ is composite.*

.

What counter-examples teach. They refine sloppy universal claims. When a statement fails, analyzing *why* the witness breaks it often suggests a corrected statement. The expression $n^2 + n + 41$ produces prime numbers for all integers n with $0 \leq n \leq 39$, but fails afterwards.

[4] Philosophically and logically, the concept of a counterexample existed in ancient Greek dialectics and argumentation, notably in the Socratic method where contradictory examples were used to challenge general claims or definitions. In medieval and early modern mathematics, counterexamples became more systematically used to falsify conjectures. Famous historical examples include Euler's counterexample disproving the conjecture that all Fermat numbers are prime.

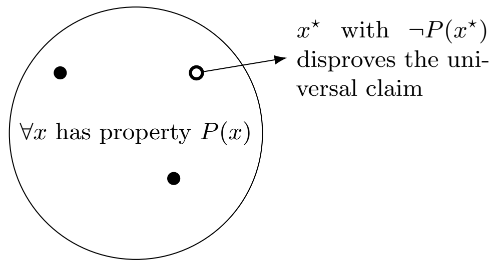


Figure 5.2: One counterexample $x^\star$ inside the “universe” circle shows the claim $\forall x\, P(x)$ is false.

5.3.3 Direct Proof

A direct proof of $P \Rightarrow Q$ proceeds as a straight line: Assume $P \rightarrow$ unpack definitions $\rightarrow$ algebra/logic $\rightarrow Q$.

Consider the following examples.

Definition. An integer n is *even* if $n = 2k$ for some integer k; it is *odd* if $n = 2k + 1$ for some integer k.

Theorem 5.6 *If a and b are even integers, then $a + b$ is even.*

Proof: Let $a = 2k$ and $b = 2m$ for integers k, m. Then

$$a + b = 2k + 2m = 2(k + m),$$

which is a multiple of 2, hence even. □

Theorem 5.7 *If x is odd, then x^2 is odd.*

Proof: Let $x = 2k + 1$. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd. □

Theorem 5.8 $1 + 2 + 3 + \cdots + n = n(n + 1)/2$

Proof: Let $S = 1 + 2 + 3 + \cdots + n$.
Hence, $S = n + (n - 1) + (n - 2) + \cdots + 1$, in the reverse order. This implies that

$$2S = \underbrace{(n+1) + (n+1) + (n+1) + \cdots + (n+1)}_{n \text{ times}}$$

Thus, $S = n(n + 1)/2$. □

Theorem 5.9 *Every odd integer is equal to the difference between the squares of two integers.*

Proof: Let $a = 2k+1$ be an arbitrary odd integer. Then $a = 2k+1 = k^2+2k+1-k^2 = (k+1)^2-k^2$. □

When to prefer direct proofs. They shine when definitions already carry the structure you need, or when simple algebra lifts P to Q. If you find yourself repeatedly “expanding the definitions” as your first move, you are in direct-proof territory.

5.3.4 Proof by Contradiction

To prove $P \Rightarrow Q$ by contradiction, assume both P and $\neg Q$. If these assumptions force an impossibility (a statement that cannot be true), then $\neg Q$ must be false, hence Q true [5]. This style of reasoning is also called reductio ad absurdum.

Consider the following examples.

Theorem 5.10 *If n is odd, then n^2 is odd.*

Proof: Let P be the statement "n is odd," and Q be the statement "n^2 is odd." Assume $P \wedge \neg Q$: that is, n is odd but n^2 is even. If n is odd, then $n = 2k+1$ for some integer k. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

which is odd. This contradicts the assumption that n^2 is even. Therefore, n^2 must be odd. □

Theorem 5.11 *If ab is odd, then both a and b are odd.*

Proof: Let P be the statement "ab is odd," and Q be the statement "both a and b are odd." Assume $P \wedge \neg Q$: that is, ab is odd but at least one of a or b is even. If a is even, say $a = 2k$, then $ab = 2kb$ is even, contradiction. Similarly, if b is even then ab is even, contradiction. Therefore, both a and b must be odd. □

Theorem 5.12 *If n^2 is divisible by 3, then n is divisible by 3.*

Proof: Let P be the statement "n^2 is divisible by 3," and Q be the statement "n is divisible by 3." Assume $P \wedge \neg Q$: that is, n^2 is divisible by 3 but n is not divisible by 3. If n is not divisible by 3, then $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$. In both cases,

$$n^2 \equiv 1 \pmod 3,$$

so n^2 is not divisible by 3. This contradicts our assumption. Therefore, n must be divisible by 3. □

Often, the antecedent P need not be explicit in contradiction proofs. In what follows, we prove that $\sqrt{2}$ which we constructed using ruler and compass in Exercise 3.5 is not a rational number.

Theorem 5.13 *$\sqrt{2}$ is irrational.*

Proof: Assume $\sqrt{2} = \frac{p}{q}$ in lowest terms with $p, q \in \mathbb{Z}_{>0}, gcd(p,q) = 1$. Then $p^2 = 2q^2$, so p is even; write $p = 2r$. Substituting, $4r^2 = 2q^2$ gives $q^2 = 2r^2$, hence q is even. Thus p, q share a factor 2, contradicting lowest terms. □

In this example the antecedent P is the silent statement "the number $\sqrt{2}$ exists", and Q is the statement that $\sqrt{2}$ is irrational.

Also consider the following examples:

Theorem 5.14 *Every integer $n > 1$ has at least one prime factor.*

Proof: Let $n > 1$. If n is prime, then it is its own prime factor.

Otherwise, suppose n is composite. Let d be the smallest divisor of n greater than 1. By definition, d divides n. We claim that d must be prime.

Suppose, for contradiction, that d is composite. Then $d = ab$ with $1 < a < d$ and $1 < b < d$. But then a divides d, and since d divides n, we also have a divides n. This contradicts the minimality of d, because a is a smaller divisor of n greater than 1.

Therefore d must be prime, and hence n has a prime factor in all cases. □

[5] Euclid's Elements contains many early examples of proof by contradiction. For instance, in Book 1, Proposition 6, Euclid proves that if two angles of a triangle are equal, the sides opposite these angles are equal by assuming the contrary and deriving a contradiction. In the section we illustrate two other famous one's – *$\sqrt{2}$ is irrational* and *there are infinitely many primes*. In Indian traditions too, the Jaina mathematicians (c. 6th–9th c.) often used impossibility reasoning, e.g. showing that certain infinite processes yield contradictions, to motivate definitions of infinity and infinitesimals. Bháskara's arguments about the impossibility of certain rational approximations can also be read as of the reductio-style.

Theorem 5.15 *Let p be a prime. If p divides n, then p does not divide $n+1$.*

Proof: Suppose p divides n and p divides $n+1$. Then, for some integers a and b, $n = pa$ and $n+1 = pb$.

We then have that $(n+1) - n = 1 = p(b-a)$, or p divides 1, which is impossible. □

Theorem 5.16 *There exist infinitely many prime numbers.*

Proof:
Assume, to the contrary, that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Consider the number

$$N = p_1 p_2 \cdots p_n + 1.$$

Clearly $N > 1$ and hence must have a prime divisor. But no p_i divides N, since dividing N by any p_i leaves a remainder 1. This contradicts the assumption that $p_1, \ldots, p_n$ were all the primes. Therefore, there must exist infinitely many primes [6] □

Theorem 5.17 *There exists an irrational number x such that x^2 is rational.*

Proof: Suppose, for contradiction, that no such number exists; that is, whenever x is irrational, x^2 is irrational as well. Consider $x = \sqrt{2}$. Then x is irrational, but

$$x^2 = (\sqrt{2})^2 = 2,$$

which is rational. This contradicts our assumption. Hence, there does exist an irrational number x such that x^2 is rational. □

Exercise 5.3 *What are the antecedents P and consequents Q in Theorems 5.16 and 5.17.*

When to use contradiction. Contradiction is powerful for showing that something is impossible – for example irrationality, no smallest positive rational, etc. – but it also works beautifully for proving existence: to show "there exists an object with property P," assume that no such object exists, and derive an inconsistency.

5.3.5 Proof by Contrapositive

In Exercise 5.1 we argued that implications $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are logically equivalent. Sometimes $\neg Q \Rightarrow \neg P$ is cleaner because "failing Q" has a rigid structure (e.g., divisibility, parity), while Q itself would require awkward casework.

Theorem 5.18 *If n^2 is odd, then n is odd.*

Proof: Assume that n is even, i.e., $n = 2k$ for some k. Then, $n^2 = 4k^2 = 2(2k^2)$ is also even. Hence the contrapositive $\neg Q \Rightarrow \neg P$ holds, and thus the original implication. □

Theorem 5.19 *If n^2 is divisible by 3, then n is divisible by 3.*

Proof: Assume that n is not divisible by 3. Then $n \equiv 1$ or $2 \pmod 3$. In both cases $n^2 \equiv 1 \pmod 3$, so n^2 is not divisible by 3. Hence the contrapositive $\neg Q \Rightarrow \neg P$ holds, and thus the original implication. □

Theorem 5.20 *If n does not divide ab, then n does not divide a and n does not divide b.*

[6] This proof was given by Euclid. This is also the first proof from the Proofs from the Book, which was written in the memory of the Hungarian mathematician Paul Erdős, who liked to talk about The Book, in which God maintains the perfect proofs for mathematical theorems.

Proof: Let (n divides a) or (n divides b).

If n divides a, then $a = nd$ for some $d > 0$. Thus $ab = ndb = n(db)$, which implies that n divides ab.

If n divides b, argue similarly.

□

Theorem 5.21 *Let $n \in \mathbb{Z}$. If $n^2 - 6n + 5$ is even, then n is odd.*

Proof: Let n be even, i.e., $n = 2k$ for some k. Then, $n^2 - 6n + 5 = (2k)^2 + 6(2k) + 4 + 1 = 2(2k^2 + 6k + 2) + 1$ which is odd. Hence the contrapositive is proved. □

Exercise 5.4 *Argue that whatever can be proved by* contradiction *can also be proved by* contrapositive*, and vice versa.*

Choosing contrapositive. Look for conclusions phrased as "is divisible by ·, is even, is nonnegative, is a subset of ·"—their negations often have crisp arithmetical or set-theoretic descriptions that are easy to exploit.

$$\boxed{P \Rightarrow Q} \xleftrightarrow{\text{equivalent}} \boxed{\neg Q \Rightarrow \neg P}$$

Figure 5.3: Proving the contrapositive proves the original implication.

5.3.6 Proof by the Pigeonhole Principle

The *Pigeonhole Principle* states that if $n + 1$ or more objects are placed into n boxes, then some box must contain at least two objects. More generally, if N objects are placed into k boxes, then some box contains at least $\lceil N/k \rceil$ objects[7]. The pigeonhole principle itself can be proved by either contradiction or contrapositive [8].

Exercise 5.5 *Prove the pigeonhole principle using both contradiction and contrapositive.*

The pigeonhole principle however merits an independent consideration because this special form makes several proofs easier. This principle often provides quick existence proofs when explicit construction is difficult. It guarantees that a certain configuration must exist, even if we cannot point to the exact example.

Example 5.5 *In a group of 13 people, at least two must share a birth month. Here the "boxes" are the 12 months, and the "objects" are the 13 people. By the pigeonhole principle, some month contains at least two birthdays.*

Here are a few more examples.

Theorem 5.22 *Among any $n + 1$ integers, there exist two with the same remainder when divided by n.*

Proof: The possible remainders upon division by n are $0, 1, 2, \ldots, n - 1$, giving n "boxes." Placing $n + 1$ integers into these boxes, two must land in the same box. Therefore two of the integers have the same remainder. □

[7] $\lceil N/k \rceil$ is the smallest integer q such that $qk \geq N$.

[8] The first known formal appearance of the pigeonhole is often attributed to the German mathematician Peter Gustav Lejeune Dirichlet in 1834, who called it the "Schubfachprinzip" (drawer or box principle). The principle appears indirectly and informally much earlier, dating back at least to 1622 in a Latin work by the French Jesuit mathematician Jean Leurechon. But Indian combinatorial work (e.g. Pingala's prosody, c. 200 BCE) already involved reasoning about distributing syllables into patterns — essentially counting arrangements that could be seen pigeonhole-wise. Later, in combinatorial discussions in the Chandas-ṣāstra and in Bháskara's combinatorics, one finds implicit arguments about "if you have more patterns than slots, something repeats."

Theorem 5.23 *Given n integers $a_1, a_2, \ldots, a_n$, there exists a non-empty subset whose sum is divisible by n.*

Proof: Consider the partial sums

$$s_k = a_1 + a_2 + \cdots + a_k, \quad k = 1, 2, \ldots, n.$$

There are n such sums. If any s_k is divisible by n, we are done. Otherwise, each s_k has a remainder in $\{1, 2, \ldots, n-1\}$. By the pigeonhole principle, two of the s_i, s_j (say $i < j$) have the same remainder. Then $s_j - s_i$ is divisible by n, and this difference is the sum of the subset $\{a_{i+1}, \ldots, a_j\}$. Hence such a subset always exists. □

Theorem 5.24 *In any group of n people, if friendship is always mutual, then at least two people have the same number of friends.*

Proof: Each person can have between 0 and $n-1$ friends. But it is impossible to have simultaneously one person with 0 friends and another with $n-1$ friends, since the "friend of all" would have to be friends with the "friend of none." Therefore, the possible friend counts are at most $n-1$ distinct numbers. With n people, two must share the same friend count. □

5.3.7 Proof by Exhaustion of cases

Sometimes a proposition cannot be proved in one uniform argument, but instead requires us to split the possible situations into a finite number of cases. A *proof by exhaustion of cases* works by checking each case separately and showing that the desired conclusion holds in all of them [9]. The structure is:

1. Partition the domain of the problem into finitely many exhaustive and mutually exclusive cases.
2. Prove the statement in each case individually using any of the proof techniques.
3. Conclude that the statement holds in general.

This method is indispensable when a property depends on a small number of discrete possibilities, such as parity (even/odd), sign (positive/negative/zero), or congruence classes modulo n.

Let us consider a few examples.

Theorem 5.25 *For any integer n, the number $n^2 + n$ is even.*

Proof: We consider two exhaustive cases:

- **Case 1:** n is even. Then $n = 2k$ for some integer k. So $n^2 + n = (2k)^2 + 2k = 4k^2 + 2k = 2(2k^2 + k)$, which is even.
- **Case 2:** n is odd. Then $n = 2k + 1$ for some integer k. So $n^2 + n = (2k+1)^2 + (2k+1) = 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1)$, which is even.

In either case, $n^2 + n$ is even. Therefore the theorem holds. □

Theorem 5.26 *For any integers a and b, $|a| \cdot |b| = |ab|$.*

Proof: We proceed by cases on the signs of a and b:

[9] The earliest history of the method of exhaustion can be traced back to Antiphon of Athens (ca. 480-411 BCE), but the full logical method as a form of a rigorous proof was formalised by Eudoxus of Cnidus (ca 408-355 BCE). There are several examples in Euclid's Elements and the work of Archimedes. Āryabhaṭa (5th c.) and Bháskara II (12th c.) used case-based reasoning to establish divisibility properties and to reduce large problems to smaller congruence classes. In the Bījagaṇita, Bháskara explicitly gives different rules depending on whether numbers are odd or even – an early form of modular case-splitting. The most notable example of proof by case analysis is the modern computer aided proof of the four colour theorem.

- **Case 1:** $a \geq 0$, $b \geq 0$. Then $|a| = a$, $|b| = b$, so $|a||b| = ab = |ab|$.
- **Case 2:** $a \geq 0$, $b < 0$. Then $|a| = a$, $|b| = -b$, and $|a||b| = a(-b) = -ab$. Since $ab < 0$, $|ab| = -ab$, so equality holds.
- **Case 3:** $a < 0$, $b \geq 0$. Then $|a| = -a$, $|b| = b$, and $|a||b| = (-a)b = -ab$. Again $ab < 0$, so $|ab| = -ab$, equality holds.
- **Case 4:** $a < 0$, $b < 0$. Then $|a| = -a$, $|b| = -b$, so $|a||b| = (-a)(-b) = ab$. Here $ab > 0$, so $|ab| = ab$, equality holds.

In all possible cases, $|a||b| = |ab|$. □

Theorem 5.27 *There is no solution in integers to* $(x^2 - y^2)$ *mod* $4 = 2$.

Proof:

- **Case 1:** x is even and y is even $\Rightarrow x^2 = 4m, y^2 = 4n$ for some integers m and $n \Rightarrow (x^2 - y^2) = 4(m - n)$.
- **Case 2:** x is even and y is odd $\Rightarrow x^2 = 4m, y^2 = 4n + 1$ for some integers m and $n \Rightarrow (x^2 - y^2) = 4(m - n) - 1$.
- **Case 3:** x is odd and y is even $\Rightarrow x^2 = 4m + 1, y^2 = 4n$ for some integers m and $n \Rightarrow (x^2 - y^2) = 4(m - n) + 1$.
- **Case 4:** x is odd and y is odd $\Rightarrow x^2 = 4m + 1, y^2 = 4n + 1$ for some integers m and $n \Rightarrow (x^2 - y^2) = 4(m - n)$.

In all these four cases $(x^2 - y^2)$ mod $4 \neq 2$. □

Theorem 5.28 *An irrational raised to an irrational power may be rational.*

Proof: We already know that $\sqrt{2}$ is irrational. Let $a = \sqrt{2}^{\sqrt{2}}$. Two cases arise.

- **Case 1:** a is rational. Then, the proposition is clearly true.
- **Case 2:** a is irrational. In that case consider $a^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$ which is a rational.

□

When to use case analysis. Proof by exhaustion is most effective when the number of cases is small and natural, such as two parities, three sign possibilities, or finitely many congruence classes modulo n. However, it becomes impractical if the number of cases grows large. As a general strategy, one should strive to minimize the cases by exploiting symmetry, structure, or general arguments.

5.3.8 Proofs of Equivalence

Often in mathematics we want to prove a statement of the form

$$P \iff Q,$$

which reads "P if and only if Q" (abbreviated "P iff Q"). This means both $P \Rightarrow Q$ and $Q \Rightarrow P$ hold. To prove such an equivalence, we usually split the work into two parts:

1. Prove the *forward implication* $P \Rightarrow Q$.
2. Prove the *reverse implication* $Q \Rightarrow P$.

Equivalences require a special discussion because sometimes the two directions may use very different arguments. Consider the following examples.

Theorem 5.29 *An integer n is even $\iff$ n^2 is even.*

Proof: **(⇒)** Suppose n is even, say $n = 2k$. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ is even.

(⇐) Conversely, suppose n^2 is even. If n were odd, say $n = 2k+1$, then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd — a contradiction. Hence n must be even. □

Theorem 5.30 *An integer n is divisible by 3 $\iff$ the sum of its digits is divisible by 3.*

Proof: Write n in decimal expansion as

$$n = d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^k d_k,$$

where $d_0, d_1, \ldots, d_k$ are the digits of n.

Since $10 \equiv 1 \pmod 3$, it follows that

$$10^i \equiv 1 \pmod 3 \quad \text{for every } i \geq 0.$$

Therefore

$$n \equiv d_0 + d_1 + \cdots + d_k \pmod 3.$$

(⇒) Suppose n is divisible by 3. Then $n \equiv 0 \pmod 3$. But $n \equiv d_0 + d_1 + \cdots + d_k \pmod 3$. Hence the digit sum is also congruent to 0 modulo 3, i.e. divisible by 3.

(⇐) Conversely, suppose the digit sum is divisible by 3. Then $d_0 + d_1 + \cdots + d_k \equiv 0 \pmod 3$. Since $n \equiv d_0 + \cdots + d_k \pmod 3$, it follows that $n \equiv 0 \pmod 3$, i.e. n is divisible by 3. □

Theorem 5.31 *Let n be a positive integer with decimal form $n = 10q + u$, where u is the units digit and q is the number formed by the remaining digits. Then*

$$n \text{ is divisible by } 7 \iff q - 2u \text{ is divisible by } 7.$$

Proof: Working modulo 7, note first that $10 \equiv 3 \pmod 7$, hence

$$n = 10q + u \equiv 3q + u \pmod 7.$$

Compute the difference

$$(3q + u) - (q - 2u) = 2q + 3u = 2(q - 2u) + 7u.$$

Therefore

$$3q + u \equiv 2(q - 2u) \pmod 7.$$

Since 2 is invertible modulo 7 (indeed $2^{-1} \equiv 4 \pmod 7$), we have

$$3q + u \equiv 0 \pmod 7 \iff q - 2u \equiv 0 \pmod 7.$$

Combining with $n \equiv 3q + u \pmod 7$ yields

$$n \equiv 0 \pmod 7 \iff q - 2u \equiv 0 \pmod 7,$$

Then, **(⇒)** If n is divisible by 7, then $n \equiv 0 \pmod 7$. Hence $q - 2u \equiv 0 \pmod 7$, i.e., $q - 2u$ is divisible by 7.

(⇐) Conversely, if $q - 2u$ is divisible by 7, then $q - 2u \equiv 0 \pmod 7$. Since $n \equiv q - 2u \pmod 7$, it follows that $n \equiv 0 \pmod 7$, i.e., n is divisible by 7.

□

Example. For $n = 483$ we have $q = 48$, $u = 3$, so $q - 2u = 48 - 6 = 42$, a multiple of 7. Hence 483 is divisible by 7.

Exercise 5.6 *Argue that for bigger numbers, the test can be applied repeatedly by computing $q - 2u$ on the result.*

Discussion. When faced with an equivalence, it is often useful to remember that "$P \iff Q$" is logically the same as "$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$." It is also common to use *contrapositive arguments* in one or both directions.

5.3.9 Proof by Induction

Proof by induction is a powerful technique for proving statements that are asserted to be true for all integers $n \geq n_0$. The method rests on two steps: establishing a base case and showing that if the statement holds for an arbitrary integer k, then it must also hold for $k + 1$.

The Induction Principle

Suppose $P(n)$ is a statement depending on an integer n. To prove that $P(n)$ is true for all integers $n \geq n_0$, we proceed as follows:

1. **Base case:** Verify that $P(n_0)$ is true.
2. **Induction step:** Assume $P(k)$ is true for some arbitrary integer $k \geq n_0$ (this assumption is called the *induction hypothesis*), and then show that $P(k+1)$ must also be true.

If both steps succeed, then by the principle of mathematical induction, $P(n)$ is true for all integers $n \geq n_0$ [10]. Think of a staircase: show you can step onto the first stair (base case) and that from any stair you can step to the next (inductive step). Then you can reach all stairs.

Exercise 5.7 *Prove that strong induction is equivalent to the original induction principle.*

Let us consider a few examples of proof by induction below.

Theorem 5.32 *For all $n \geq 1$,*

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

Proof:
Base case: For $n = 1$, the left-hand side is 1, and the right-hand side is $\frac{1 \cdot 2}{2} = 1$. So the statement holds.
Induction hypothesis: Assume the formula holds for $n = k$, i.e.

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

Induction step: Now consider $n = k + 1$:

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

This is exactly the formula with $n = k + 1$. Hence the result follows. □

[10] The idea of proof by induction is ancient, though the formal principle was only stated in the nineteenth century. In the Western tradition, inductive reasoning appears already in Euclid's *Elements* (Book IX, Proposition 8) and in his descent-style proof of prime factorisation (Book VII, Propositions 30–32) [**?**]. Later, Islamic mathematicians such as al-Karaji (10th–11th c.) used inductive arguments for binomial expansions [**?**], and in Europe, Maurolico (16th c.) and Pascal (17th c.) applied the method in combinatorics and series [**?**, **?**]. By the time of Euler and Gauss, induction was common in number theory, and Peano (1889) finally codified it as an axiom of the natural numbers [**?**]. In the Indian tradition, recursive and inductive reasoning also played a central role: Pingala (c. 200 BCE) described prosodic patterns equivalent to Pascal's triangle [**?**], and Bhāskara II (12th c.) used stepwise arguments in the *Līlāvatī* and *Bījagaṇita* to establish general formulas [**?**]. Thus, both traditions employed inductive reasoning long before its modern formal axiomatization.

Theorem 5.33 *For all $n \geq 1$,*

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Proof:
Base case: For $n = 1$, the left-hand side is 1 and the right-hand side is $1^2 = 1$.
Induction hypothesis: Assume true for $n = k$, i.e.

$$1 + 3 + \cdots + (2k - 1) = k^2.$$

Induction step: Then for $n = k + 1$,

$$1 + 3 + \cdots + (2k - 1) + (2(k + 1) - 1) = k^2 + (2k + 1) = (k + 1)^2.$$

Thus the claim holds for $n = k + 1$. □

Theorem 5.34 *For all $n \geq 1$, $10^n - 1$ is divisible by 9.*

Proof:
Base case: For $n = 1$, $10^1 - 1 = 9$, which is divisible by 9.
Induction hypothesis: Assume $10^k - 1$ is divisible by 9, i.e., $10^k - 1 = 9m$ for some m.
Induction step: Then

$$10^{k+1} - 1 = 10 \cdot 10^k - 1 = 10(9m + 1) - 1 = 90m + 9 = 9(10m + 1).$$

Thus $10^{k+1} - 1$ is divisible by 9. □

Theorem 5.35 *For all integers $n \geq 4$, $2^n > n^2$.*

Proof:
Base case: For $n = 4$, $2^4 = 16$ and $4^2 = 16$, so the inequality holds with equality. For $n = 5$, $2^5 = 32 > 25$, so the inequality holds strictly.
Induction hypothesis: Assume $2^k > k^2$ for some $k \geq 5$.
Induction step: Then

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot k^2.$$

Since $k \geq 5$, we have $2k^2 \geq (k + 1)^2$. Thus $2^{k+1} > (k + 1)^2$. □

Theorem 5.36 *Suppose we have stamps of two different denominations, 3 paise and 5 paise. We want to show that it is possible to make up exactly any postage of 8 paise or more using stamps of these two denominations. Thus we want to show that every positive integer $n \geq 8$ is expressible as $n = 3i + 5j$ where $i, j \geq 0$.*

Proof:
Base case: For $n = 8$, we have $n = 3 + 5$, i.e. $i = j = 1$.
Induction hypothesis: $n = 3i + 5j$ for an $n \geq 8$, $i, j \geq 0$.
Induction step: Consider $n+1$. If $j = 0$ then clearly $i \geq 3$ and we may write $n+1$ as $3(i-3)+5(j+2)$. Otherwise $n + 1 = 3(i + 2) + 5(j - 1)$. □

Strong induction. Strong induction is a variant where we assume the statement holds for all integers up to k and use this to prove it for $k + 1$. Suppose $P(n)$ is a statement depending on an integer n. To prove that $P(n)$ is true for all integers $n \geq n_0$, we proceed as follows:

1. **Base case:** Verify that $P(n_0)$ is true.
2. **Induction step:** Assume $P(m)$ is true for all m, $n_0 \leq m \leq k$ for some arbitrary integer k (this assumption is called the strong version of the *induction hypothesis*), and then show that $P(k + 1)$ must also be true.

Consider the following example.

Theorem 5.37 *Let $F_0 = 0,\ F_1 = 1,\ F_2 = 1, \ldots$ be the Fibonacci sequence where for all $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Let $\phi = (1+\sqrt{5})/2$. We now show that $F_n \leq \phi^{n-1}$ for all positive n.*

Proof:
Base case: For $n = 1$, we have $F_1 = \phi^0 = 1$.
Induction hypothesis: $F_n \leq \phi^{n-1}$ for all m, $1 \leq m \leq n$.
Induction step:

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &\leq \phi^{n-1} + \phi^{n-2} && \text{(by the induction hypothesis)} \\ &= \phi^{n-2}(\phi + 1) \\ &= \phi^n && \text{(since } \phi^2 = \phi + 1\text{)} \end{aligned}$$

□

Theorem 5.38 (Fundamental Theorem of Arithmetic) *Every integer $n > 1$ can be written as a product of primes, and this representation is unique up to reordering of the primes.*

Proof: *Existence:* We proceed by induction on n. For $n = 2$, the result holds since 2 is prime. Assume every integer m with $2 \leq m < n$ has a prime factorisation. If n is prime, we are done. Otherwise, $n = ab$ with $1 < a, b < n$. By the induction hypothesis, both a and b factor into primes. Thus n factors into primes.

Uniqueness: Suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

with all p_i, q_j prime. Since $p_1 \mid q_1 q_2 \cdots q_s$, Euclid's Lemma implies $p_1 \mid q_j$ for some j. As both are prime, $p_1 = q_j$. Cancelling p_1 from both sides and repeating the argument gives uniqueness by induction on the number of prime factors. □

Exercise 5.8 *Complete the proof of the unique prime factorization theorem more formally.*

Remarks.

- Induction proofs are especially useful for formulas involving sums, products, inequalities, or divisibility.
- The induction hypothesis is a temporary assumption used to prove the next case; it is not assumed globally.
- Strong induction is a variant where we assume the statement holds for all integers up to k and use this to prove it for $k + 1$.

5.3.10 Conclusion

There is no single "best" technique; experienced problem solvers try viewpoints. If definitions seem aligned, push a direct proof. If "not Q" feels structured, flip to a contrapositive. If a statement ranges over integers, try induction. If you suspect a claim is too strong, hunt a counter-example. And whenever "assuming the opposite" quickly generates an impossibility, contradiction is often the sharpest tool.

Problems

1. **Truth Tables**
   (a) Construct the truth table for $(p \wedge q) \vee (\neg r)$.
   (b) Verify by a truth table that $(p \Rightarrow r) \wedge (q \Rightarrow r)$ is equivalent to $(p \vee q) \Rightarrow r$.

(c) Determine whether $(p \Rightarrow q) \Rightarrow r$ and $p \Rightarrow (q \Rightarrow r)$ are equivalent.

(d) Show by truth table that $p \vee (q \wedge r)$ is not equivalent to $(p \vee q) \wedge (p \vee r)$.

2. **Three-variable Logic**

   (a) Construct the truth table for $(p \oplus q) \oplus r$ and check whether it is associative.

   (b) Verify that $\neg(p \wedge q \wedge r)$ is equivalent to $\neg p \vee \neg q \vee \neg r$.

   (c) Show that $(p \Rightarrow q) \wedge (q \Rightarrow r)$ does not imply $(p \Rightarrow r)$ by giving a truth table.

   (d) Identify all assignments of p, q, r for which $(p \vee q) \Rightarrow (q \vee r)$ is false.

3. **Vacuous Truth**

   (a) State a universally quantified claim about an empty set and explain why it is true.

   (b) Explain why the statement "If n is an integer with $n^2 = -1$, then n is prime" is vacuously true.

   (c) Let $A = \varnothing$. Prove that "For all $x \in A$, $x^2 = 0$" is vacuously true.

   (d) Formulate a vacuous truth involving divisibility (e.g. "All integers divisible by both 2 and 3 and equal to 5 are even"), and justify why it is vacuously true.

4. **Proof by Explicit Construction**

   (a) Find integers x, y such that $17x + 29y = 1$.

   (b) Exhibit an explicit Pythagorean triple different from $(3, 4, 5)$ and $(5, 12, 13)$.

   (c) Construct a rational number between $\frac{7}{9}$ and $\frac{8}{9}$.

   (d) Show by construction that there exists an integer solution to $12x + 18y = 6$.

5. **Proof by Counter-Example**

   (a) Disprove: "For all integers n, $n^2 - n + 41$ is prime."

   (b) Disprove: "For all integers n, $n^3 + 2$ is prime."

   (c) Disprove: "Every integer greater than 2 is the sum of two primes." (Give a counterexample.)

   (d) Find a counterexample to: "If a divides bc, then a divides b."

6. **Direct Proof**

   (a) Prove that the product of two even integers is even.

   (b) Prove that if a is divisible by 12 and b is divisible by 6, then $a + b$ is divisible by 6.

   (c) Show directly that if n is a multiple of 4, then n^2 is a multiple of 16.

   (d) Prove directly that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

7. **Proof by Contradiction**

   (a) Prove by contradiction that $\sqrt{7}$ is irrational.

   (b) Show by contradiction that there is no integer solution to $2x = 2y + 1$.

   (c) Prove by contradiction that there are infinitely many primes congruent to 1 modulo 4.

   (d) Prove by contradiction that $\sqrt[3]{2}$ is irrational.

8. **Proof by Contrapositive**

   (a) Prove: If n^2 is divisible by 9, then n is divisible by 3.

   (b) Prove: If ab is even, then at least one of a or b is even.

   (c) Prove: If n^2 is divisible by 8, then n is divisible by 2.

(d) Prove: If x^2 is divisible by 12, then x is divisible by 6.

9. **Proof by the Pigeonhole Principle**

   (a) Show that among any 8 integers, two leave the same remainder modulo 7.

   (b) Prove that in a group of 32 people, at least two share the same day of the month for their birthday.

   (c) Show that in any set of 6 integers, at least three must have the same parity.

   (d) Prove that in any group of 367 people, at least two have the same exact birthday (ignoring leap years).

10. **Proof by Exhaustion of Cases**

    (a) Prove that the cube of any integer is congruent to $-1, 0$, or 1 modulo 7.

    (b) Show that if n is an integer, then $n^2 \equiv 0, 1, 4 \pmod 5$.

    (c) By checking cases, show that for any integer n, $n^2 - n$ is even.

    (d) Prove by exhaustion of parities that the product of two consecutive integers is even.

11. **Proofs of Equivalence**

    (a) Prove that n is divisible by 2 if and only if n^2 is divisible by 4.

    (b) Prove that $a \equiv b \pmod n$ if and only if a and b leave the same remainder when divided by n.

    (c) Prove that an integer n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

    (d) Prove that a and b are both even if and only if $a + b$ is even and $a - b$ is even.

12. **Proof by Induction**

    (a) Find the fallacy in the following proof by **PMI**.
    Theorem Given any collection of n blonde girls. If at least one of the girls has blue eyes, then all n of them have blue eyes.
    Proof: The statement is obviously true for $n = 1$. The step from k to $k + 1$ can be illustrated by going from $n = 3$ to $n = 4$. Assume, therefore, that the statement is true for $n = 3$ and let G_1, G_2, G_3, G_4 be four blonde girls, at least one of which, say G_1, has blue eyes. Taking G_1, G_2, and G_3 together and using the fact that the statement is true when $n = 3$, we find that G_2 and G_3 also have blue eyes. Repeating the process with G_1, G_2 and G_4, we find that G_4 has blue eyes. Thus all four have blue eyes. A similar argument allows us to make the step from k to $k + 1$ in general. □
    Corollary. All blonde girls have blue eyes.
    Proof: Since there exists at least one blonde girl with blue eyes, we can apply the foregoing result to the collection consisting of all blonde girls. □
    Note: This example is from G. Pólya, who suggests that the reader may want to test the validity of the statement by experiment.

    (b) Suban announces to the QRMT class:
    "There will be a surprise test next week. You will not know in advance on which day it will be held."
    One student in the class reasons as follows, by induction on $n = 5 - k$:

    - The test cannot be on Friday (the last working day of the week, $k = 5, n = 0$), because if it hasn't happened before then, the class would know it must be on Friday — and so it would not be a surprise.
    - Similarly, the test cannot be on Thursday, because if it hasn't happened before then, and Friday has already been ruled out, the class would know it must be on Thursday — and so it would not be a surprise.

- Continuing this reasoning backwards, the test cannot be on Wednesday, Tuesday, or Monday either.
- Therefore, the teacher cannot give a surprise test at all!

Yet, when Suban gives the test on Wednesday, the students are indeed surprised. Identify the flaw in the student's reasoning.

(c) Prove by induction that for all integers $n \geq 1$,

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

(d) Show by induction that $7^n - 1$ is divisible by 6 for all integers $n \geq 1$.

(e) Prove that for all $n \geq 1$, $n^3 - n$ is divisible by 6.

(f) Prove that for all integers $n \geq 4$,

$$n! > 2^n.$$

(g) Show that for all integers $n \geq 1$,

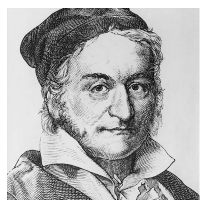
$$3^n \geq n^3.$$

(h) Prove using strong induction that every integer $n > 1$ can be written as a product of prime numbers.

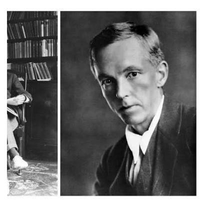
(i) A tiling problem: Prove by strong induction that any $2^n \times 2^n$ chessboard with one square removed can be covered completely by L-shaped trominoes (three-square pieces).

Chapter 6

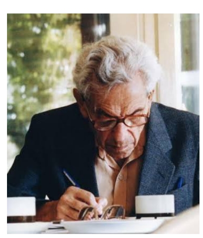
Primes, GCD, and and the intrigue of Cryptography



"The primes are the jewels of arithmetic, scattered without apparent order, yet subject to laws that the human mind may one day discern." – Carl Friedrich Gauss



"A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas. And the primes are the most eternal patterns of all." – G. H. Hardy



"God may not play dice with the universe, but something strange is going on with the prime numbers." – Paul Erdős

The theory of prime numbers and their properties forms the foundation of number theory. At first sight, the study of primes may seem like a purely mathematical pursuit. Yet today prime numbers play a crucial role in modern life, because they underpin cryptographic systems that secure communication over the internet.

In this chapter we introduce the basic ideas of primes and factorisation, methods for computing greatest common divisors, some crucial algorithms and theorems about primes, and finally explain how these notions are used in public-key cryptography, especially the RSA cryptosystem.

6.1 Primes

We have informally discussed primes several times in these notes. We give a formal definition here

Definition 6.1 *A* prime number *is an integer* $p > 1$ *whose only positive divisors are* 1 *and* p *itself.*

Numbers greater than 1 that are not prime are called *composite*. $2, 3, 5, 7, 11$ are some examples of primes, while $12 = 3 \times 4$ is composite. In what follows, we develop some properties of prime numbers.

6.1.1 There are infinitely many primes

In Theorem 5.16 we proved there are infinitely many primes. We repeat the theorem here for the sake of completeness.

Theorem 6.1 (Euclid) *There are infinitely many prime numbers.*

Proof: Suppose there are only finitely many: $p_1, \ldots, p_k$. Consider $N = p_1 \cdot p_2 \cdots p_k + 1$. No p_i divides N, since each leaves remainder 1. Thus N is prime or divisible by a new prime, contradicting the assumption[1]. □

6.1.2 Unique prime factorisation

The *Unique Prime Factorisation theorem* (Theorem 5.38) establishes that primes are the "atoms" of arithmetic: every integer factors into primes, and no further. We again repeat it here for completeness.

Theorem 6.2 (Fundamental Theorem of Arithmetic) *Every integer* $n > 1$ *can be written as a product of primes. This factorisation is unique up to the order of the factors.*

Proof: *Existence:* If n is prime, we are done. Otherwise, assume that the claim is true for all m such that $2 \leq m < n$. Let $n = ab$ with $a, b < n$. By the induction hypothesis, each of a and b has a prime factorisation, hence so does n.

Uniqueness: Suppose

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

with all p_i, q_j prime. Then p_1 divides the right side, hence some q_j. But since q_j is prime, $p_1 = q_j$. Cancelling, we continue inductively to conclude that the multisets $\{p_i\}$ and $\{q_j\}$ are identical. □

6.1.3 The Sieve of Eratosthenes

One of the oldest known algorithms for finding prime numbers is due to *Eratosthenes of Cyrene* (around 200 BCE). The method, called the Sieve of Eratosthenes, systematically eliminates composite numbers from a list, leaving only primes.

> Sift the Two's and Sift the Three's:
> The Sieve of Eratosthenes.
> When the multiples sublime,
> The numbers that remain are Prime.
>
> – Anonymous

[1] Assume you have a finite list of primes. Multiply them together and add 1. Either that number is prime — or you just found a new factor. Either way, you're wrong. Welcome to mathematics!

The Algorithm

To find all primes up to a given number N:

1. Write down the list of integers $2, 3, 4, \ldots, N$.
2. Start with the first number $p = 2$. It is prime.
3. Cross out all multiples of p greater than p itself in the list.
4. Find the next uncrossed number. This is the next prime. Set p to this number and repeat Step 3.
5. Continue until $p^2 > N$. All remaining uncrossed numbers are prime.

Example 6.1 *Primes up to 30*

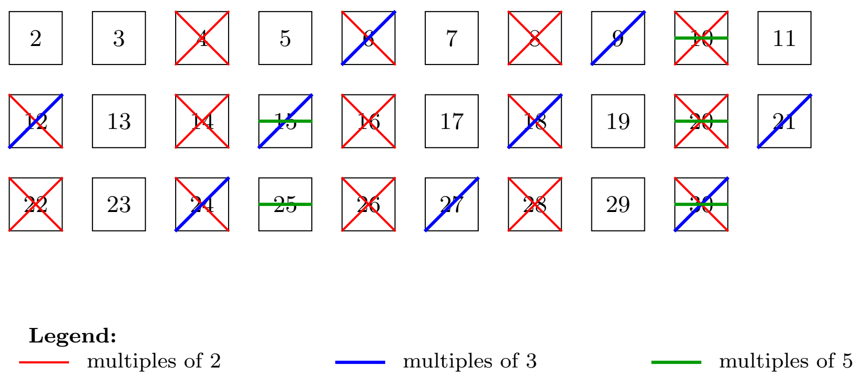


Figure 6.1: Sieve of Eratosthenes up to 30. Uncrossed boxes are primes.

Start with the numbers 2 to 30 (see Figure 6.1).

- 2 is prime. Cross out $4, 6, 8, \ldots, 30$.
- Next uncrossed is 3. Cross out $6, 9, 12, \ldots, 30$.
- Next uncrossed is 5. Cross out $10, 15, 20, 25, 30$.
- Next uncrossed is 7. Since $7^2 = 49 > 30$, we stop.

The remaining numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$, exactly the primes ≤ 30.

Remarks

- The sieve is simple and efficient for generating primes up to a moderately large bound.
- It takes $O(N \log \log N)$ steps for large N, making it far faster than testing each number individually for divisors.
- This method, though ancient, is still used sometimes[2].

Exercise 6.1 *Find all primes between 2 and 100 using the Sieve of Eratosthenes.*

[2]Unfortunately, this algorithm is too inefficient in practice. The problem of primality testing – how to test whether a given integer is a prime – has been open at least since the times of Euclid and Eratosthenes. The first "efficient" solution for the problem was the AKS algorithm from IIT Kanpur in 2002. In practice, an even faster Miller-Rabin test is used, but it uses probabilistic coin tosses as a primitive, and can give a wrong answer with a very small probability. We will study some of these methods later in these otes

6.1.4 The Prime Number Theorem

The distribution of primes among the natural numbers is highly irregular: sometimes primes cluster close together, other times they are far apart. A natural question, posed already by Gauss and Legendre around the year 1800 when he was a teenager[3], is: *How many primes are there up to a large number n?*

Theorem 6.3 (Prime Number Theorem) *Let $\pi(n)$ denote the number of primes $\leq n$. Then*

$$\pi(n) \sim \frac{n}{\ln n}, \quad \textit{as } n \to \infty,$$

meaning that

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

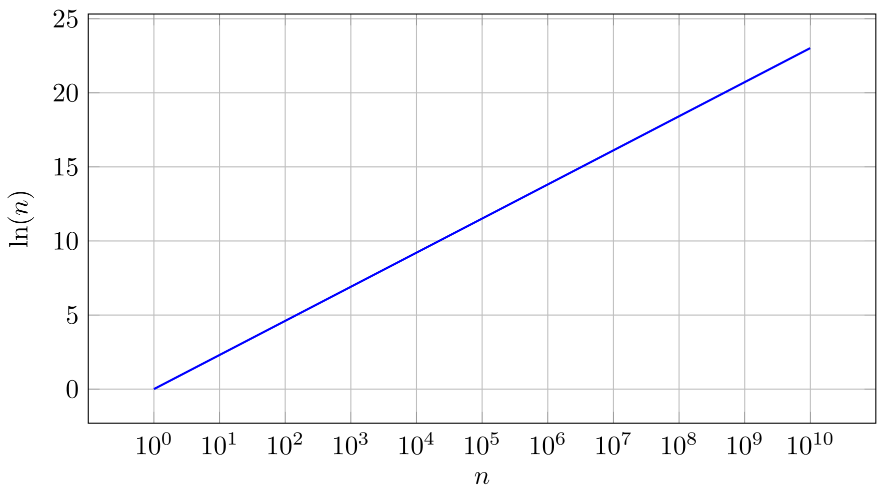


Figure 6.2: The natural logarithm $\ln(n)$ grows very slowly, even as n reaches 10^{10}.

In words: the density of primes around n is roughly $\frac{1}{\ln n}$. The natural logarithm function $\ln n$ is a rather slowly growing function. It can be intuitively understood as a way of answering the question: "How much time does it take to grow from 1 to n, assuming continuous growth at a fixed rate?". See Figure 6.2 for a plot. We will revisit the natural logarithm function later in these notes. So, primes are not very sparse at all[4]. For example, around $n = 10^6$, about one in every 14 numbers is prime.

The proof of the prime number theorem is unfortunately out of the scope of these notes. Interested readers will have to follow up QRMT with some courses on calculus, analysis and algebra for the proof to be accessible.

Exercise 6.2 *Use a calculator to stimate the number of primes between 10^6 and 10^7 using the prime number theorem.*

[3]Historians like to quip: "Even at 15, Gauss preferred to keep his prime secrets private."

[4]Carl Friedrich Gauss (1792–93), as a teenager, investigated prime tables and conjectured the approximation $\pi(n) \approx \mathrm{Li}(n)$, where $\mathrm{Li}(n) = \int_2^n \frac{dt}{\ln t}$ is the logarithmic integral. He recorded this insight in his diary, long before publishing it. Adrien-Marie Legendre independently proposed the formula $\pi(n) \approx \frac{n}{\ln n - 1.08366}$ in 1798. The theorem was finally proved independently in 1896 by Jacques Hadamard and Charles Jean de la Vallée Poussin, using complex analysis and properties of the Riemann zeta function. Their proof showed how deep connections between prime numbers and complex analysis truly are. Interested students will have to wait for a few later course in mathematics to study the proofs

6.1.5 Fermat's Little Theorem

Prime numbers have remarkable properties in modular arithmetic. One of the most beautiful and useful is a result discovered by Pierre de Fermat in 1640, long before the modern development of number theory. It shows that when we raise a number to a large power, the remainder upon division by a prime behaves in a very simple way.

Fermat wrote that if p is a prime and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. He gave no proof, and the first rigorous demonstrations came later from Leonhard Euler and others.

This theorem is central in number theory. It lies behind efficient algorithms for primality testing, and it forms one of the key mathematical tools used in public-key cryptography. Before proving it, let us state it precisely.

Theorem 6.4 (Fermat's Little Theorem) *If p is prime and $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

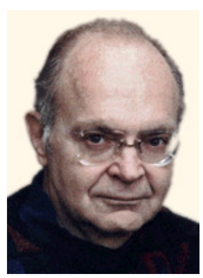
Proof: Multiplication by a permutes the set $\{1, 2, \ldots, p-1\}$ modulo p (why?) Thus

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p}.$$

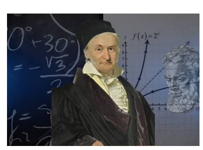
This gives $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Since $(p-1)!$ is not divisible by p, we may cancel to obtain $a^{p-1} \equiv 1 \pmod{p}$. □

Exercise 6.3 *Argue that multiplication by a permutes the set $\{1, 2, \ldots, p-1\}$ modulo p. That is, the operation is injective.*

6.2 The Greatest Common Divisor



"The Euclidean algorithm is one of the oldest nontrivial algorithms that has survived to the present day. It can be considered the first efficient algorithm ever devised." – Donald Knuth



"The algorithm of Euclid is the finest jewel in the crown of elementary number theory." – Carl Friedrich Gauss

When working with integers, one of the most natural questions is: given two numbers, what is the largest number that divides them both? For example, for 18 and 24 the answer is 6, since 6 is the largest integer that divides both without remainder. This simple idea is called the *greatest common divisor*, or *gcd* for short.

The gcd plays a central role in number theory. It captures the notion of the "common part" of two numbers, and it is fundamental for simplifying fractions, solving equations in integers, and developing modular arithmetic. As we will see, the efficient algorithm to compute gcds, due to Euclid, is one of the oldest and most beautiful algorithms in all of mathematics.

Definition 6.2 *The* greatest common divisor $\gcd(a,b)$ *of two integers* a, b *is the largest integer that divides both.*

Example 6.2

$$\gcd(18,24) = 6, \qquad \gcd(13,27) = 1.$$

6.2.1 Euclid's Algorithm

Euclid, over 2000 years ago, discovered a remarkably efficient method for computing $\gcd(a,b)$, $a > 0, b \geq 0$:

$$\begin{array}{ll} \gcd(a,b) = a & \text{if } b = 0 \\ \gcd(a,b) = \gcd(b,\, a \bmod b) & \text{otherwise} \end{array}$$

Repeating this step until the remainder is 0 yields the gcd.

Example 6.3 *To compute* $\gcd(252,105)$*:*

$$252 = 105 \cdot 2 + 42, \quad \gcd(252,105) = \gcd(105,42),$$

$$105 = 42 \cdot 2 + 21, \quad \gcd(105,42) = \gcd(42,21),$$

$$42 = 21 \cdot 2 + 0 \quad \Rightarrow \quad \gcd = 21.$$

Definition 6.3 *Two positive integers are* relatively prime *if their gcd is 1, i.e., they have no non-trivial factors in common.*

6.2.2 The Extended Euclidean Algorithm

Euclid's algorithm is remarkable because it quickly computes the gcd of two numbers. But sometimes we need more than just the gcd: we want to write the gcd as a sum of multiples of the two numbers themselves[5].

For example, for $a = 30$ and $b = 12$, not only is $\gcd(30,12) = 6$, but also

$$6 = 30 \times (-1) + 12 \times 3.$$

In other words, the gcd can be expressed as a whole-number combination of a and b. This means we can "build" the gcd by taking suitable multiples of 30 and 12. This fact is called Bézout's identity.

The *Extended Euclidean Algorithm* is just a way to find these multipliers at the same time as we compute the gcd.

How it works (idea). We start the same way as in Euclid's algorithm:

$$a = q_1 b + r_1, \quad b = q_2 r_1 + r_2, \quad \ldots$$

until we reach a remainder 0. While we do this, we also keep track of how each remainder is made from a and b. At the end, the last nonzero remainder is the gcd, and the numbers in front of a and b give us the multipliers we want.

Example 6.4 *Let's find the gcd of* 26 *and* 7*, and also write it as a combination of* 26 *and* 7*.*

$$26 = 3 \times 7 + 5, \quad 7 = 1 \times 5 + 2, \quad 5 = 2 \times 2 + 1, \quad 2 = 2 \times 1 + 0.$$

So $\gcd(26,7) = 1$.

Now work backwards:

$$1 = 5 - 2 \times 2,$$

[5] Euclid tells us what the gcd is; the extended Euclid tells us how to make it.

$$1 = 5 - 2 \times (7 - 1 \times 5) = 3 \times 5 - 2 \times 7,$$

$$1 = 3 \times (26 - 3 \times 7) - 2 \times 7 = 3 \times 26 - 11 \times 7.$$

So we have

$$1 = 3 \times 26 + (-11) \times 7.$$

This shows that -11 *is a multiplier for* 7 *that makes* $7 \times (-11) \equiv 1 \pmod{26}$. *In other words,* 7 *has an inverse modulo* 26, *and it is* 15 *(since* $-11 \equiv 15 \pmod{26}$*)* [6].

The steps of the general algorithm can then be given as:

General Algorithm (Extended Euclid). Given two integers a and b:

1. If $b = 0$, then $\gcd(a, 0) = a$ and we return $(x, y) = (1, 0)$.
2. Otherwise, divide a by b:
$$a = qb + r, \quad 0 \le r < b.$$
3. Inductively apply the algorithm to (b, r) to get
$$\gcd(b, r) = xb + yr.$$
4. Substitute $r = a - qb$ to express the gcd in terms of a and b:
$$\gcd(a, b) = ya + (x - qy)b.$$
5. Return $(x', y') = (y,\, x - qy)$.

At the end, we obtain integers x, y such that

$$ax + by = \gcd(a, b).$$

Why this matters. The extended Euclidean algorithm is very useful:

- It gives the gcd of two numbers.
- It shows how to write the gcd using those two numbers.
- If the gcd is 1, it also finds a modular inverse, which is essential in cryptography.

6.3 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is one of the most beautiful and useful results in number theory. It says that if we know the remainder of a number when divided by several pairwise coprime moduli, then we can uniquely determine the number modulo the product of those moduli.

In other words, instead of working with a single large modulus, we can break a problem into several smaller ones, solve them separately, and then combine the answers back together. This is extremely powerful in computations, because working modulo small numbers is easier.

The theorem was discovered in ancient China, and first appeared in the work of Sun Tzu around the 3rd century AD, who posed problems like: *"Find a number which leaves remainder 2 when divided by 3, remainder 3 when divided by 5, and remainder 2 when divided by 7."* The answer is unique modulo $3 \cdot 5 \cdot 7 = 105$.

The CRT has many applications:

[6] We had discussed this earlier in Theorem 5.4. The origins of this algorithm can be traced back to Āryabhaṭa (5^{th} c), Jayadeva (c. 10^{th}–11^{th} c.) and later Bháskara II (12^{th} c.). Bháskara in the Līlāvatī and Bījagaṇita gives worked examples of solving linear Diophantine equations with what is recognizably the extended Euclid method.

- Efficient computation in modular arithmetic (e.g. fast exponentiation).
- Cryptography, especially RSA, where it is used to speed up decryption.
- Error correction in coding theory.

Thus, the CRT is not only a striking piece of mathematics but also a practical tool.

Example 6.5 *An example (Sun Tzu, 3rd century AD).*
Suppose we want to find a number N such that

$$N \equiv 2 \pmod 3, \quad N \equiv 3 \pmod 5, \quad N \equiv 2 \pmod 7.$$

Step 1. The moduli $3, 5, 7$ are pairwise coprime, so the CRT applies. The product is $M = 3 \cdot 5 \cdot 7 = 105$.
Step 2. For each congruence, compute

$$M_1 = \frac{M}{3} = 35, \quad M_2 = \frac{M}{5} = 21, \quad M_3 = \frac{M}{7} = 15.$$

Step 3. Find numbers y_i such that

$$M_1 y_1 \equiv 1 \pmod 3, \quad M_2 y_2 \equiv 1 \pmod 5, \quad M_3 y_3 \equiv 1 \pmod 7.$$

- $35 \equiv 2 \pmod 3$, and $2 \cdot 2 \equiv 1 \pmod 3 \implies y_1 = 2$.
- $21 \equiv 1 \pmod 5$, so $y_2 = 1$ works.
- $15 \equiv 1 \pmod 7$, so $y_3 = 1$ works.

Step 4. Combine everything:

$$N \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod M,$$

where $(a_1, a_2, a_3) = (2, 3, 2)$.

$$N \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}.$$

$$N \equiv 140 + 63 + 30 = 233 \pmod{105}.$$

Step 5. Reduce: $233 \equiv 23 \pmod{105}$.

Therefore, the solution is

$$N \equiv 23 \pmod{105}.$$

Indeed, $23 \equiv 2 \pmod 3$, $23 \equiv 3 \pmod 5$, and $23 \equiv 2 \pmod 7$.

Theorem 6.5 (Chinese Remainder Theorem) *Let $n_1, \dots, n_k$ be pairwise coprime and $N = n_1 \cdots n_k$. Then for any integers $a_1, \dots, a_k$ there is a unique solution $x \pmod N$ to*

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, \dots, k.$$

Proof: Let $N_i = N/n_i$. Since $\gcd(N_i, n_i) = 1$, there exists y_i with $N_i y_i \equiv 1 \pmod{n_i}$. Then $x = \sum a_i N_i y_i$ solves the congruences. Uniqueness follows: if x and x' are both solutions, then each n_i divides $x - x'$, hence so does N. □

6.4 Public-Key Cryptography