MATH1025 Number Systems

Cheatsheet

2023/24

This document collects together the important definitions and results presented throughout the lecture notes. The numbering used throughout will be consistent with that in the lecture notes.

Contents

1 Number Problems

Prime Numbers and a Fact About Them

Definition 1.2 A whole number is prime if the only numbers dividing it are one and itself.

It is standard to consider 1 as **non**-prime. Therefore, a better alternative to Definition 1.2 may be this: "a whole number is *prime* if it has precisely two unique factors, namely one and itself".

Theorem 1.4 (Euclid's Theorem) *There are infinitely-many prime numbers.*

Proof: Suppose the statement is **not** true, meaning there are a finite number of primes. Let's label these finite primes as $p_1, p_2, ..., p_n$. Then, we consider the number

$$x \coloneqq p_1 p_2 \cdots p_{n-1} p_n + 1.$$

In words, we multiply our finite primes together and add one. If this is a prime, because it is bigger than all of $p_1, p_2, ..., p_n$, it is **not** in that list. Therefore, we must assume that x is **not** a prime. However, every number is divisible by some prime. In particular, let p be a prime which divides x. Because we have a complete list of primes $p_1, ..., p_n$, we know p must be one of them. But clearly we get a remainder of one when dividing x by any of these p's. Therefore, x is **not** divisible by a prime. What we have shown is that x is divisible by a prime (because any number is), and x is not divisible by a prime. Since these statements contradict each other, our original assumption must be false. In other words, there are indeed infinitely-many primes. □

Note: A common mistake here is this: we cannot assert that x is always prime. Indeed, if all of $p_1, ..., p_n$ are odd, then x is even and therefore **not** prime. This is why we have to consider prime factors of this number in the above proof.

Remark 1.5 The above is an example of *proof by contradiction* This is a type of proof that relies on the obvious fact that a statement is either true or false (there is no in-between; this is the Law of the Excluded Middle).

Method – Proof by Contradiction: This is how to write a proof by contradiction.

(i) Assume the opposite of the statement we wish to prove.
(ii) Use logical reasoning to determine what this implies.
(iii) We eventually get to something nonsensical, so we are done.

2 Sets

Definition 2.1 A set is a well-defined collection of objects, known as elements (or members).

We often use capital letters for names of sets and lowercase letters for elements of said said. For instance, if X is a set, we may denote an arbitrary element of it by x. If we want to write out a set in full, we use curly brackets { and } surrounding the list of elements.

Note: The shorthand notation for saying "element x is in set X" is to simply write $x \in X$.

Notation Throughout the module, we use this notation frequently for sets of different numbers:

$$\begin{aligned}
\mathbb{N} &= \text{ the set of natural numbers } \{1, 2, 3, 4, ...\},\\
\mathbb{Z} &= \text{ the set of integers } \{..., -2, -1, 0, 1, 2...\},\\
\mathbb{Q} &= \text{ the set of rational numbers } \{\tfrac{a}{b} : a, b \in \mathbb{Z} \text{ with } b \neq 0\}.\\
\mathbb{R} &= \text{ the set of real numbers.}
\end{aligned}$$

How the real numbers are constructed is complicated, but essentially these contain all the whole numbers, decimals, fractions and irrational numbers (like π and e and $\sqrt{2}$).

Definition 2.2 The set with no elements is called the empty set, denoted by {} or $\emptyset$.

Remark A set can itself be an element of a set. For example, the set $\{1, 5, 8\}$ has three elements, but the set $\{7, \{1, 5, 8\}\}$ has **two** elements; the element 7 and the element $\{1, 5, 8\}$. To make things clearer, if we label $X := \{1, 5, 8\}$, then we see that $Y := \{7, \{1, 5, 8\}\} = \{7, X\}$ and it is much clearer why it has only two elements.

Definition 2.6 Let X and Y be sets. We say that Y is a subset of X if every element of Y is also an element of X (in other words, if $y \in Y$, then $y \in X$). This is denoted $Y \subseteq X$.

Remark 2.8 It is important to distinguish between an *element* of a set and a *subset* of a set. Indeed, if $x \in X$ is an element of a set, then it is true that $\{x\} \subseteq X$. Essentially, this says that we can take any element of a set and put curly brackets around it to give us a subset.

Definition 2.9 Let Y be a subset of X. We say that Y is a proper subset of X if Y is not the same as X. This is denoted $Y \subsetneq X$ (or denoted $Y \subset X$ in analogy with $<$ vs $\leq$).

Remark A great number of authors use $\subset$ and $\subseteq$ interchangeably, so the only true way to emphasise that we are working with **proper** subsets is to use $\subsetneq$. However, this module will use $\subset$ to mean proper subset; please stick to this convention now (but be prepared to change when you study other modules/read other mathematical texts).

Note: If we want to write a number of elements of a set, we just list them as $x, y, z \in X$.

We can define a set using some additional notation. Indeed, if we want to consider a collection of elements x that each satisfy some property P, the easiest way to write this is of the form

$$\{x : x \text{ satisfies property } P\}.$$

Note: Some people use | instead of the colon, meaning "$\{x \mid x$ satisfies property $P\}$".

Definition 2.13 Let X and Y be sets. Their union $X \cup Y$ is the set given by

$$X \cup Y = \{x : x \in X \text{ or } x \in Y\}.$$

We often use "or" non-exclusively. This means that something is in the union $X \cup Y$ if it is in X or Y **or both**. If we want to emphasise that our "or" is exclusive, we instead use "either... or...".

Definition 2.15 Let X and Y be sets. Their intersection $X \cap Y$ is the set given by

$$X \cap Y = \{x : x \in X \textbf{ and } x \in Y\}.$$

In the case of the intersection, we are only keeping the elements that appear in **both** of the sets we are working with. If the intersection of two sets is empty, we say they are "disjoint".

Definition 2.17 Let X and Y be sets. The complement $X \setminus Y$ of Y in X is the set

$$X \setminus Y = \{x : x \in X \text{ and } x \notin Y\}.$$

In other words, the complement is a way to throw out elements we don't want. Here then, we look at the elements of X and remove any of the elements that also appear in Y.

A Theorem

Theorem 2.19 *Set union distributes over set intersection, i.e. for any three sets A, B, C,*

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

Proof: Let $x \in A \cup (B \cap C)$, which means $x \in A$ **or** $x \in B \cap C$. Consider each case separately:

- If $x \in A$, then it is clear $x \in A \cup B$ and $x \in A \cup C$, meaning that $x \in (A \cup B) \cap (A \cup C)$.
- If $x \in B \cap C$, then $x \in B$ and $x \in C$, so $x \in A \cup B$ and $x \in A \cup C$, so $x \in (A \cup B) \cap (A \cup C)$.

Conversely, let $x \in (A \cup B) \cap (A \cup C)$, which means $x \in A \cup B$ **and** $x \in A \cup C$. The former tells us $x \in A$ or $x \in B$; the latter tells us $x \in A$ or $x \in C$. Hence, if $x \in A$, we clearly have $x \in A \cup (B \cap C)$. But if $x \notin A$, it must be that $x \in B$ and $x \in C$, so again $x \in A \cup (B \cap C)$. $\square$

Remark The principle behind Theorem 2.19 is this: to show that two sets are equal, we show that they are subsets of each other. Indeed, let L be the set on the left and R the set on the right. We started by letting $x \in L$ and showing that this means $x \in R$. Going the other way, we start by letting $x \in R$ and showing that $x \in L$. In other words, we establish $L \subseteq R$ and $R \subseteq L$; the only way both are true is when $L = R$.

> **Note:** To summarise, $X = Y$ is equivalent to showing both of $X \subseteq Y$ and $Y \subseteq X$.

3 Induction

Theorem 3.3 (Principle of Mathematical Induction) *Let $A(n)$ be an infinite collection of statements indexed by $n \in \mathbb{N}$. Suppose that the following are both true:*
(i) *$A(1)$ is true.*
(ii) *$A(k)$ true implies $A(k+1)$ true for all $k \in \mathbb{N}$.*
Then, $A(n)$ is true for all $n \in \mathbb{N}$.

Proof: Assume to the contrary that **not all** $A(n)$ are true. Therefore, there exists some smallest natural number j such that $A(j)$ is false. By assumption (i), we know that $j > 1$. By the minimality of j, we know that $A(j-1)$ is true. But assumption (ii) implies that $A(j-1+1) = A(j)$ must be true, a contradiction. □

Definition When proving something inductively, we refer to the steps as follows:
- Assumption (i) is called the initial step.
- Assumption (ii) is called the inductive step.
- Assuming $A(k)$ is true for some $k \in \mathbb{N}$ is called the inductive hypothesis.

Note: We assume $A(k)$ for **one** natural, not all (this is what induction proves!) of them.

Sum of the First n Squares

Proposition *The sum of the first n square numbers is given by the formula*

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

Proof: We proceed with a proof by induction. For the initial case (when $n = 1$), we see that the left-hand side of the formula is $1^2 = 1$ and the right-hand side is $\frac{1}{6} \times 1 \times 2 \times 3 = 1$. Hence, the initial case holds. For the inductive step, assume the formula holds when $n = k$ for **some** $k \in \mathbb{N}$:

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

We wish to use the above to show that the formula is true when $n = k+1$, that is

$$\sum_{i=1}^{k+1} i^2 = \frac{1}{6}(k+1)(k+1+1)\left(2(k+1)+1\right) = \frac{1}{6}(k+1)(k+2)(2k+3).$$

Indeed, we see that

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

$$
\begin{aligned}
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2, && \text{by the inductive hypothesis,} \\
&= \frac{1}{6}\left(k(k+1)(2k+1) + 6(k+1)^2\right) \\
&= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right) \\
&= \frac{1}{6}(k+1)(2k^2+7k+6) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3).
\end{aligned}
$$

By the Principle of Mathematical Induction, the formula is true for all $n \in \mathbb{N}$. □

Remark 3.4 Note the structure of a proof by induction: we *assume* that $A(k)$ is true and use it to *prove* that $A(k+1)$ is true. It is a common error by beginners to assume $A(k+1)$ is true.

Reminder: The factorial of a natural number is the product it with all naturals below it:

$$n! \coloneqq n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1.$$

Proposition *For all $n \in \mathbb{N}$, we have $2^{n-1} \leq n!$.*

Proof: We proceed with a proof by induction. For the initial case (when $n = 1$), we see that the left-hand side of the formula is $2^0 = 1$ and the right-hand side is $1! = 1$. Hence, the initial case holds. For the inductive step, assume the formula holds when $n = k$ for some $k \in \mathbb{N}$, meaning $2^{k-1} \leq k!$. We wish to use this to show that the formula is true when $n = k+1$, that is $2^k \leq (k+1)!$. Indeed, we see that

$$
\begin{aligned}
2^{(k+1)-1} &= 2^k \\
&= 2(2^{k-1}) \\
&\leq 2(k!), && \text{by the inductive hypothesis,} \\
&\leq (k+1)(k!), && \text{by the fact that } 2 \leq k+1, \\
&= (k+1)!.
\end{aligned}
$$

By the Principle of Mathematical Induction, the formula is true for all $n \in \mathbb{N}$. □

How to Write an Induction Proof

Method – Proof by Induction: This is how to write a proof by induction.

(i) Show that the initial case is true.
(ii) State that you are assuming the statement is true for **some** $k \in \mathbb{N}$.
(iii) Use Step (ii) to prove that the statement is true when $n = k+1$.
(iv) Write a conclusion, e.g. "by the Principles of Mathematical Induction,...".

4 Divisors

Divisibility

Definition 4.1 Let $a, b \in \mathbb{Z}$ be integers. We say that a divides b if there exists an integer $k \in \mathbb{Z}$ such that $b = ka$. We denote this by $a \mid b$. If this is not the case, we write $a \nmid b$.

Remark 4.2 In the above definition (as with all definitions), we use the word "if". However, we really mean "if and only if" in definitions because not only are we saying that $a \mid b$ implies $b = ka$, but the converse is true too: if $b = ka$, then we say that $a \mid b$.

Note: If $a \mid b$, we also say that b is divisible by a, or that a is a divisor of b.

Theorem 4.5 *Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any $m, n \in \mathbb{Z}$.*

Proof: Because $a \mid b$, there exists $k_1 \in \mathbb{Z}$ such that $b = k_1 a$ by Definition 4.1. Similarly, the same definition applies to $a \mid c$, which means there exists $k_2 \in \mathbb{Z}$ such that $c = k_1 a$. Now, we see that

$$mb + nc = m(k_1 a) + n(k_2 a) = (mk_1 + nk_2)a.$$

But this is just $a \mid (mb + nc)$ where $k = mk_1 + nk_2$ in Definition 4.1. □

Corollary 4.7 *Let $a, b \in \mathbb{Z}$. If $a \mid b$, then $a \mid b^2$.*

Proof: Simply take $m = b$ and $n = 0$ in Theorem 4.5. □

Remark This is a good opportunity to consider the converse to Corollary 4.7, namely the statement "if $a \mid b^2$, then $a \mid b$". Is this true? It turns out it absolutely is **not**. For example, take $a = 4$ and $b = 2$. It is true that $4 \mid 2^2$ but clearly $4 \nmid 2$.

Theorem 4.8 *Let $a, b, c \in \mathbb{Z}$. Then, we have the following divisibility facts:*
(i) *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
(ii) *If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.*

Proof: (i) By assumption, there exist $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $c = k_2 b$. Substituting the first into the second gives us $c = k_2 k_1 a$; this means that $a \mid c$ by Definition 4.1 (with $k = k_2 k_1$).

(ii) By assumption, there exist $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $a = k_1 b$. Substituting the first into the second gives us $b = k_2 k_1 b$; this means that $k_2 k_1 = 1$ but because they are integers, they are either both 1 or both -1, from which we see that $a = \pm b$. □

A Nice Prime Result

Theorem 4.9 *Let $n \in \mathbb{N}$ with $n > 1$. If $2^n - 1$ is prime, then n is prime.*

Proof: Suppose that n is **not** prime, meaning $n = ab$ for some $a, b \in \mathbb{Z}$ less than n (neither of which is one). Using the factorisation

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1),$$

we see that $2^a - 1$ divides $2^n - 1 = (2^a)^b - 1$. Therefore, $2^n - 1$ is not prime. □

Remark The above is an example of *proof by contrapositive*. This is a type of proof that relies on the fact that a statement of the form "$P \Rightarrow Q$" is equivalent to the statement "not $Q \Rightarrow$ not P".

Note: Knowing $P \Rightarrow Q$ tells us **nothing** about when P is false. In general, not $P \not\Rightarrow$ not Q.

We can actually prove a generalisation of Theorem 4.9 with very little extra effort.

Proposition 4.10 *Let $x, n \in \mathbb{N}$ with $n > 1$. If $x^n - 1$ is prime, then $x = 2$ and n is prime.*

Proof: Like with the proof of Theorem 4.9, we see that $x - 1$ divides $x^n - 1$. But if $x^n - 1$ is prime, this means either that $x - 1 = x^n - 1$ (which is not true since $n > 1$) or $x - 1 = 1$, meaning $x = 2$. The fact that $x^n - 1 = 2^n - 1$ is prime now follows from the same argument as above. □

Fundamental Theorem of Arithmetic

Theorem 4.13 (Strong Induction) *Let $A(n)$ be an infinite collection of statements indexed by $n \in \mathbb{N}$. Suppose that the following are both true:*
(i) *$A(r)$ is true for some $r \in \mathbb{N}$.*
(ii) *For all $k \geq r$, $A(j)$ true for all $r \leq j \leq k$ implies $A(k+1)$ true.*
Then, $A(n)$ is true for all $n \in \mathbb{N}$.

Proof: Omitted; it is similar to that of ordinary induction. □

Remark The idea behind strong induction is that we know one of the statements is true, and that all of the statements $A(r), A(r+1), A(r+1), ..., A(k)$ are true imply the statement $A(k+1)$ is true. The fact it is "strong" induction is because we assume more in the inductive hypothesis.

Theorem 4.14 (Fundamental Theorem of Arithmetic) *Every natural number greater than one is a product of primes, that is every $n \in \mathbb{N}$ can be written in the form*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

for distinct primes $p_1, ..., p_r$ and exponents $a_1, ..., a_r \in \mathbb{N}$.

Proof: Let $A(n)$ be the statement "n is either prime or a product of primes". We will use strong induction to prove this result. For the initial case, we know that $A(2)$ is true since 2 is prime. As for the inductive step, suppose that $A(2), A(3), ..., A(k)$ are true for some $k \geq 2$. We will show that $A(k+1)$ is true. If $k+1$ is prime, the the statement is true. So suppose it is not prime, meaning that $k+1 = xy$ for some $x, y \in \mathbb{N}$ with $1 < x, y < k+1$. By the inductive hypothesis, we know that $A(x)$ and $A(y)$ are true, that is x and y can be written as a product of primes:

$$x = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \qquad \text{and} \qquad y = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_s}.$$

Therefore, $k+1 = xy$ is also a product of primes. Of course, if $p_i = q_j$ for some i and j, then we can take $a_i + b_j$ as the exponent of p_i and disregard q_j (so that each prime only appears once). In other words, $A(k+1)$ is true. By the principle of mathematical induction, the statement is true for all $n \in \mathbb{N}$. □

Note: The full version of the Fundamental Theorem of Arithmetic has the following additional conclusion: the factorisation into a product of primes is unique *up to order*, meaning that if we can write $n \in \mathbb{N}$ in two different ways $x = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $y = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$, then it follows that $r = s$ and for each i, there is a unique j such that $p_i = q_j$ and $a_i = b_j$.

5 The Euclidean Algorithm

Greatest Common Divisor

Definition 5.1 The greatest common divisor of two non-zero integers $a, b \in \mathbb{Z}$ is the largest positive integer that divides both of them. It is denoted $\gcd(a, b)$.

Note: Sometimes, mathematicians will refer to this as the highest common factor $\mathrm{hcf}(a, b)$.

Theorem 5.4 *Let $a, b \in \mathbb{Z}$. Then, the following are true:*

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

(ii) $\gcd(a, b) \geq 1$.

(iii) $\gcd(a, b) = \gcd(|a|, |b|)$.

(iv) $\gcd(a, b) = \gcd(a + nb, b)$ *for all* $n \in \mathbb{Z}$.

(v) $\gcd\left(\dfrac{a}{\gcd(a,b)}, \dfrac{b}{\gcd(a,b)}\right) = 1$.

Proof: (i) and (ii) are trivial observations.

(iii) Recall that $|a| = \pm a$. For $c \in \mathbb{Z}$, if we have $c \mid a$, we immediately see that $c \mid |a|$. On the other hand, if we start with $c \mid |a|$, then $c \mid a$ or $c \mid \pm 1$. However, $\pm 1 \mid a$ and we conclude that $c \mid a$. This shows that a and $|a|$ have exactly the same divisors. An identical argument works for b and $|b|$. Therefore, the sets of *common* divisors of a and b is equal to that of $|a|$ and $|b|$; the largest element in each set is therefore the same too.

(iv) Let $d = \gcd(a, b)$ and $e = \gcd(a + nb, b)$. By definition, $e \mid (a + nb)$ and $e \mid b$, so there exist $k_1, k_2 \in \mathbb{Z}$ with $k_1 e = a + nb$ and $k_2 e = b$. We can combine these two equations to conclude that

$$a = k_1 e - nb = k_1 e - nk_2 e = (k_1 - nk_2)e.$$

This establishes $e \mid a$. Paired with the fact that $e \mid b$ from above, we see that it is a common divisor of a and b. Since d is the **greatest** common divisor of these integers, we see that $e \leq d$. On the other hand, because $d \mid a$ and $d \mid b$, it is clear that $d \mid (a + nb)$. Hence, d is a common factor of $a + nb$ and b, but the **greatest** common factor of these integers is e. This means that $d \leq e$. Combining these inequalities tells us $d = e$, that is $\gcd(a, b) = \gcd(a + nb, b)$.

(v) Let $d = \gcd(a, b)$ and $e = \gcd(a/d, b/d)$. Our goal is to $e = 1$. Assume to the contrary that $e > 1$. Then, since it is the greatest common divisor, it is a common divisor: $e \mid a/d$ and $e \mid b/d$, so we write $k_1 e = a/d$ and $k_2 e = b/d$ for some $k_1, k_2 \in \mathbb{Z}$ by Definition 4.1. Rearranging these tells us also that $dk_1 e = a$ and $dk_2 e = b$. In other words, de is a common divisor of both a and b. But since $e > 1$, we see that $de > d$; this contradicts the fact that d is the **greatest** common divisor. This establishes that $e = 1$. □

The Division Lemma

Lemma 5.5 (Division Lemma) *Let $x, y \in \mathbb{Z}$ be non-zero with $y > 0$. Then, there exist unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < y$ called the* quotient *and* remainder*, respectively, such that $x = qy + r$.*

Proof: Consider the set

$$S \coloneqq \{x - sy : s \in \mathbb{Z} \text{ and } x - sy \geq 0\}.$$

(Existence) We start by showing that this is a non-empty set. Indeed, if $x < 0$, then $x - xy \in S$ but notice that $x - xy = x(1 - y) \geq 0$ since $y > 0$ (so $1 - y \leq 0$). On the other hand, if $x \geq 0$, then $x = x - 0y \in S$. Not only is S non-empty, but it contains only non-negative integers. Thus, it has a smallest element which we denote r. Let $q \in \mathbb{Z}$ be the integer such that $r = x - qy$, which exists because $r \in S$ and so it can be written in this form. To show that $0 \leq r < y$, note first that $r \geq 0$ is clear since we have shown already that S contains non-negative integers. Now,

$$r - y = (x - qy) - y = x - (q + 1)y.$$

But because r is the smallest element of S, and $r - y$ is smaller, we must have $r - y \notin S$. This means that $r - y = x - (q+1)y < 0$, which rearranges to $r < y$ and this completes the argument.

(Uniqueness) Assume to the contrary that q and r are **not** unique, meaning there exist $q', r' \in \mathbb{Z}$ such that $x = q'y + r$ with $0 \leq r' < y$. Assume also that $q' \neq q$ (**or** $r' \neq r$; only one is necessary since $q' = q$ implies $r' = x - q'y = x - qy = r$). Without loss of generality, let $q > q'$. Equating $x = qy + r$ and $x = q'y + r'$ produces $(q - q')y = r' - r$. By assumption, $q - q' > 0$, so $y \leq r' - r$, but this contradicts the fact that $0 \leq r, r' < y$ are less than y. □

Note: The "quotient" and "remainder" are called as such since they are found using $x \div y$.

We can generalise Lemma 5.5 slightly in the following way.

Lemma 5.6 (General Division Lemma) *Let $x, y \in \mathbb{Z}$ be non-zero. Then, there exist unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < |y|$ such that $x = qy + r$.*

The Euclidean Algorithm

Theorem 5.7 (Euclidean Algorithm) *For $x, y \in \mathbb{Z}$, there exist integers $q_1, ..., q_k \in \mathbb{Z}$ and a descending sequence of positive integers $r_1, ..., r_k \in \mathbb{N}$ (meaning $r_1 > \cdots > r_k > 0$) with*

$$\begin{aligned} x &= q_1 y + r_1, \\ y &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k, \\ r_{k-1} &= q_k r_k + 0. \end{aligned}$$

The algorithm terminates when "r_{k+1}" $= 0$ for some $k \in \mathbb{N}$, and we obtain $\gcd(x, y) = r_k$.

Proof: We simply apply the Division Lemma repeatedly. At each stage, we have $0 \leq r_i < r_{i-1}$. Because our sequence of positive integers is descending, it will eventually terminate at zero. The fact that $\gcd(x, y) = r_k$ follows from the fact that $\gcd(x, y) = \gcd(r, y)$ where $r = x - qy$ for some $q \in \mathbb{Z}$; this is Theorem 5.4(v). □

Note: Theorem 5.7 tells us how to compute the greatest common divisor of two integers.

Calculating the Greatest Common Divisor

Theorem 5.11 (Bézout's Identity) *Let $x, y \in \mathbb{Z}$. Then, there exist $k, l \in \mathbb{Z}$ such that*

$$\gcd(x, y) = kx + ly.$$

Sketch of Proof: Rearrange the second-to-last equation in Theorem 5.7 for the greatest common divisor, and substitute it into the equation above it. Continue to do this repeatedly and the result is a linear expression for $\gcd(x, y)$ in terms of x and y. □

Method – Reverse Euclidean Algorithm: Suppose we wish to write $\gcd(x, y) = kx + ly$.

(i) Apply Euclid's Algorithm to find $\gcd(x, y)$.
(ii) Rearrange the penultimate line for the remainder and substitute it into the last line.
(iii) Continue Step (ii) moving up line-by-line and substituting remainders.
(iv) This will terminate when, at the top, you obtain an expression $\gcd(x, y) = kx + ly$.

In other words, the above method provides a means to compute $k, l \in \mathbb{Z}$ satisfying Bézout's Identity. Note however that these integers are **not** unique, but the mere fact we can obtain two such integers is often very helpful.

Euclid's Lemma

Corollary 5.13 (Euclid's Lemma) *Let $n, a, b \in \mathbb{N}$. If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.*

Proof: Since $\gcd(a, n) = 1$, use Bézout's Identity to obtain integers $k, l \in \mathbb{Z}$ with $ka + ln = 1$. Multiplying through by b tells us that $kab + lnb = b$. Clearly, $n \mid lnb$ and we assume that $n \mid ab$. Since n divides the left-hand side, it must also divide the right-hand side: $n \mid b$. □

Definition 5.14 We call two integers $x, y \in \mathbb{Z}$ coprime (or relatively prime) if $\gcd(x, y) = 1$.

Theorem 5.15 *Let $a, b \in \mathbb{Z}$ and p be prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof: Suppose $p \mid ab$ but $p \nmid a$. Then, $\gcd(a, p) = 1$ so Euclid's Lemma tells us that $p \mid b$. □

Note: These types of arguments are quite slick. If ever you need to prove that something satisfies condition P **or** condition Q, it is sufficient to assume that if it does **not** satisfy condition P, then it **must** satisfy condition Q because the only other option is that it does satisfy condition P, and so the statement that it satisfies P or Q is still very much valid.

6 Modular Arithmetic

Modular Arithmetic

Definition 6.1 Let $x, y \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say that x and y are equivalent modulo n if they have the same remainder upon division by n. This is denoted $x = y \pmod{n}$.

Theorem 6.5 *If $n \in \mathbb{N}$ is a square number, then $n \pmod 4$ is either zero or one.*

Proof: By definition, we assume that $n = k^2$ for some $k \in \mathbb{Z}$. Since we are working modulo 4, we need only consider the four possible remainders upon dividing n by 4, namely 0, 1, 2 and 3.

(i) Let $k = 0 \pmod 4$. Then, $k = 4m$ for some $m \in \mathbb{Z}$. We therefore conclude that

$$n = k^2 = 16m^2 = 4(4m^2) = 0 \pmod 4.$$

(ii) Let $k = 1 \pmod 4$. Then, $k = 4m + 1$ for some $m \in \mathbb{Z}$. We therefore conclude that

$$n = k^2 = 16m^2 + 8m + 1 = 4(4m^2 + 2m) + 1 = 1 \pmod 4.$$

(iii) Let $k = 2 \pmod 4$. Then, $k = 4m + 2$ for some $m \in \mathbb{Z}$. We therefore conclude that

$$n = k^2 = 16m^2 + 16m + 4 = 4(4m^2 + 4m + 1) = 0 \pmod 4.$$

(iv) Let $k = 3 \pmod 4$. Then, $k = 4m + 3$ for some $m \in \mathbb{Z}$. We therefore conclude that

$$n = k^2 = 16m^2 + 24m + 9 = 4(4m^2 + 6m + 2) + 1 = 1 \pmod 4.$$ □

Theorem 6.6 *For $x, y \in \mathbb{Z}$, $x = y \pmod n$ if and only if $x - y = kn$ for some $k \in \mathbb{Z}$.*

Proof: ($\Rightarrow$) Suppose $x = y \pmod n$; this means they have the same remainders upon division by n. Hence, we can write $x = k_1 n + r$ and $y = k_2 n + r$ for some $k_1, k_2, r \in \mathbb{Z}$. Therefore,

$$x - y = k_1 n + r - k_2 n - r = (k_1 - k_2)n.$$

($\Leftarrow$) Suppose $x - y = kn$ for some $k \in \mathbb{Z}$, and assume that y has remainder r upon division by n, that is $y = k_1 n + r$ for some $k_1 \in \mathbb{Z}$. We can now see that

$$\begin{aligned} & x - y = kn \\ \Leftrightarrow \quad & x = y + kn \\ \Leftrightarrow \quad & x = k_1 n + r + kn \\ \Rightarrow \quad & x = (k_1 + k)n + r, \end{aligned}$$

so x also has remainder r upon division by n. Consequently, $x = y \pmod n$. □

Note: We can alternatively state Theorem 6.6 as "$x = y \pmod n$ if and only if $n \mid (x - y)$".

The Arithmetic of mod

Theorem 6.8 *Let $x, y \in \mathbb{Z}$ with $x = r \pmod{n}$ and $y = s \pmod{n}$. Then, we have these:*
(i) $x + y = r + s \pmod{n}$.
(ii) $xy = rs \pmod{n}$.

Proof: By assumption, there exist $k, l \in \mathbb{Z}$ such that $x = kn + r$ and $y = ln + s$. Therefore,

$$x + y = kn + r + ln + s \qquad \Rightarrow \qquad (x + y) - (r + s) = (k + l)n,$$

so it follows from Theorem 6.6 that $x + y = r + s \pmod{n}$. Similarly then, we see that

$$xy = (kn + r)(ln + s) = kln^2 + kns + lnr + rs \qquad \Rightarrow \qquad xy - rs = (kln + ks + lr)n$$

and the previous theorem again tells us that $xy = rs \pmod{n}$. □

Note: We can use $x - y = x + (-y)$ with Theorem 6.8(i) to obtain $x - y = r - s \pmod{n}$.

Fermat's Little Theorem

Theorem 6.9 (Fermat's Little Theorem) *Let $x, p \in \mathbb{Z}$ with p prime. Then, $x^p = x \pmod{p}$.*

Proof: We shall assume $x \in \mathbb{N}$ in the proof and use induction; the general case follows by repeating the argument with $-x \in \mathbb{N}$. For the initial case (when $x = 0$), $0^p = 0 = 0 \pmod{p}$ and so the statement holds true. For the inductive step, assume it is true for $x = y$, that is $y^p = y \pmod{p}$ for some $y \in \mathbb{N}$. We use this to prove the formula holds with $x = y + 1$. Well,

$$(y + 1)^p = y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{p-1} y + 1$$

by using the Binomial Theorem. Working modulo p on both sides of the above, we see that

$$\begin{aligned}
(y + 1)^p \pmod{p} &= y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{p-1} y + 1 \pmod{p} \\
&= y + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{p-1} y + 1 \pmod{p} \\
&= y + 1 + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{p-1} y \pmod{p} \\
&= y + 1 \pmod{p},
\end{aligned}$$

where the inductive hypothesis is used to obtain the second equality, and $\binom{p}{r} = 0 \pmod{p}$ for all $1 \leq r \leq p - 1$ is used to obtain the final equality. By the Principle of Mathematical Induction, the statement is true. □

Corollary 6.11 *Let $x, p \in \mathbb{Z}$ with p prime and $p \nmid x$. Then, $x^{p-1} = 1 \pmod{p}$.*

Applications of Fermat's Little Theorem

A quick application allows us to reduce modulo p rather fast, so we can find remainders easily.

Method – Finding Remainders: Suppose we wish to find $a^b \pmod{p}$ where p is a prime.

(i) Write the power $b = kp + r$ for some $k, r \in \mathbb{Z}$; we now work with $a^b = (a^p)^k a^r$.
(ii) Use Fermat's Little Theorem $a^p = a \pmod{p}$ to simplify $a^b \pmod{p}$ from above.
(iii) Continue to reduce everything else modulo p and use Theorem 6.8 to get an answer.

A 'better' use of Fermat's Little Theorem (specifically Corollary 6.11) is for detecting primes. Indeed, the aforementioned corollary says "if p is prime, then $x^{p-1} = 1 \pmod{p}$". Although the converse is **not** true, we know that the contrapositive **is** true. In full, the contrapositive says this:

"if $x^{p-1} \neq 1 \pmod{p}$, then p is **not** prime".

Method – Detecting Non-Primality: Suppose we wish to show that $n \in \mathbb{Z}$ is **not** prime. To do this, we choose some $x \in \mathbb{Z}$ with $n \nmid x$ and consider $x^{n-1} \pmod{n}$. Reducing this modulo n until it is as small as possible, there are two possible outcomes of this process:

- If $x^{n-1} \neq 1 \pmod{n}$, we can say that n is **not** prime.
- If $x^{n-1} = 1 \pmod{n}$, we can only say that n **might** be prime.

Note: The latter allows us only to say n *might* be prime because we selected a particular $x \in \mathbb{Z}$. If $x^{n-1} = 1 \pmod{n}$ but it turns out n is really **not** prime, we call x a Fermat liar.

7 Equivalence Relations

Relations

Definition 7.2 Let X and Y be sets. The Cartesian product is the set of pairs of elements

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

We can take the Cartesian product of a set with itself, e.g. $X \times X$. We can also do this repeatedly and this lends itself to the following notation (where X appears n times on the right-hand side):

$$X^n = X \times X \times \cdots \times X.$$

Definition 7.4 Let X be a set and $R \subseteq X \times X$ a subset of the Cartesian product of X with itself. For $x, y \in X$, x is related to y if $(x, y) \in R$. This is often denoted $x \sim y$.

Note: Some mathematicians write xRy instead of $x \sim y$. We call the set R the relation. In practice, we simply call $\sim$ "the relation" instead of R; this is standard across mathematics.

Equivalence Relations

Definition 7.6 A relation $\sim$ on a set X is an equivalence relation if the following are true:

(i) $x \sim x$ for all $x \in X$. (**Reflexivity**)
(ii) If $x \sim y$, then $y \sim x$ for all $x, y \in X$. (**Symmetry**)
(iii) If $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in X$. (**Transitivity**)

Remark Recall that Definition 6.1 introduced the notion of two integers being *equivalent* modulo n. The choice of language there is no mistake: it turns out that the relation $\sim$ on $\mathbb{Z}$ given by $x \sim y$ if and only if $x = y \pmod{n}$ is indeed an equivalence relation.

Note: It *looks like* we get reflexivity for free: if $x \sim y$, then symmetry implies $y \sim x$ and transitivity (with $z = x$) implies $x \sim x$. However, this is **not** true because we start with "if $x \sim y$"; there is no guarantee that x is related to another (different) element in general!

Equivalence Classes

Definition 7.10 Let $\sim$ be an equivalence relation on X. The equivalence class of $x \in X$ is

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

In words, the equivalence class of an element is the set of all elements that are related to it. The principal here is that we can collect together equivalent elements. If we do this for all elements of the set X, this ultimately produces what we call a *partition* (discussed next).

Partitions

Reminder: Two sets X and Y are disjoint if their intersection is empty, that is $X \cap Y = \emptyset$.

Definition Let X be a set. A partition of X is a collection of non-empty subsets of X such that each $x \in X$ lives in precisely **one** (and only one) of these subsets. In other words, we say the subsets are *pairwise disjoint*.

Theorem 7.12 *Let $\sim$ be an equivalence relation on X. Then, we have the following:*

(i) *For all $x, y \in X$, we have $x \sim y$ if and only if $[x] = [y]$.*

(ii) *For all $x, y \in X$, we have $x \nsim y$ if and only if $[x] \cap [y] = \emptyset$.*

(iii) *The union of all equivalence classes is the entirety of X, that is $\bigcup_{x \in X} [x] = X$.*

Proof: (i) Suppose $x \sim y$. Let $z \in [x]$, meaning that $z \sim x$. But by transitivity, it follows that $z \sim y$ and so $z \in [y]$. This means $[x] \subseteq [y]$. But if $x \sim y$, symmetry implies that $y \sim x$ and we can perform an identical argument: if $z \in [y]$, it means $z \sim y$. But by transitivity, it follows that $z \sim x$ and so $z \in [x]$. This means $[y] \subseteq [x]$. Combining these two results tells us that $[x] = [y]$. Conversely, suppose $[x] = [y]$. Because $x \sim x$ by reflexivity, we have $x \in [x] = [y]$ and so $x \sim y$.

(ii) Suppose $x \nsim y$ and assume to the contrary that $[x] \cap [y] \neq \emptyset$. Since this intersection is non-empty, there exists $z \in X$ such that $z \in [x]$ and $z \in [y]$. In other words, $z \sim x$ and $z \sim y$. By symmetry and transitivity, this tells us that $x \sim y$, a contradiction to the fact that $x \nsim y$. Conversely, suppose $[x] \cap [y] = \emptyset$ and assume to the contrary that $x \sim y$. Because $x \sim y$, we know have $x \in [y]$ (and $x \in [x]$ by reflexivity). Hence, $x \in [x] \cap [y] \neq \emptyset$, a contradiction.

(iii) Let $x \in X$. By reflexivity, $x \sim x$ which can be written as $x \in [x]$. It therefore follows that $x \in \bigcup_{x \in X} [x]$ and this tells us $X \subseteq \bigcup_{x \in X} [x]$. But because each $[x] \subseteq X$, it follows that their union is also a subset, so the reverse inclusion $\bigcup_{x \in X} [x] \subseteq X$ is obvious. Combining these gives

$$X = \bigcup_{x \in X} [x]. \qquad \square$$

Remark 7.13 The result above implies the equivalence classes are either (i) equal or (ii) disjoint.

Note: In other words, Theorem 7.12 tells us the equivalence classes partition the set X.

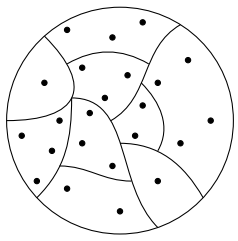

Figure 1: A picture representing the partition of a set.

Modular Arithmetic

We consider the equivalence relation that is equivalence modulo n. The equivalence classes are

$$\begin{aligned}
[0] &= \{..., -3n, -2n, -n, 0, n, 2n, ...\},\\
[1] &= \{..., -2n+1, -n+1, 1, n+1, 2n+1, ...\},\\
[2] &= \{..., -2n+2, -n+2, 2, n+2, 2n+2, ...\},\\
&\vdots\\
[n-1] &= \{..., -2n+(n-1), -n+(n-1), n-1, n+(n-1), 2n+(n-1), ...\}.
\end{aligned}$$

Note: The above is actually a complete list because $[n] = [0]$, $[n+1] = [1]$ and so forth.

Definition The integers modulo n is the set of equivalence classes $\mathbb{Z}_n := \{[0], [1], ..., [n-1]\}$.

We can actually define arithmetic on the set of equivalence classes of integers modulo n (**not** on the set $\mathbb{Z}$ of integers, but indeed on $\mathbb{Z}_n$). This is done by defining the following operations:

$$\begin{aligned}
[x] + [y] &:= [x+y],\\
[x] \cdot [y] &:= [xy].
\end{aligned} \tag{$*$}$$

Definition 7.16 An element in an equivalence class is called a representative of said class.

A potential problem with the operations $(*)$ is that maybe they yield different things depending on the chosen representative of the class. For instance, we have $0 \in [0]$ and we have $n \in [0]$, so does $(*)$ make sense irrespective of which we use? Before we answer this, we state a definition.

Definition 7.17 An operation between equivalence classes that does **not** depend on the representatives chosen is said to be well-defined.

Theorem 7.15 *If* $[x] = [u]$ *and* $[y] = [v]$, *then* $[u] \cdot [v] = [x] \cdot [y]$.

Proof: By assumption, let $x \sim u$ and $y \sim v$; recall this means that each pair of equivalent elements share the same remainder upon division by n. By Theorem 6.6, there exist $k_1, k_2 \in \mathbb{Z}$ where $x - u = k_1 n$ and $y - v = k_2 n$; these mean $x = k_1 n + u$ and $y = k_2 n + v$, respectively. Thus,

$$\begin{aligned}
xy &= (k_1 n + u)(k_2 n + v)\\
&= k_1 k_2 n^2 + k_1 n v + k_2 n u + uv\\
&= (k_1 k_2 n + k_1 v + k_2 u) n + uv.
\end{aligned}$$

We can apply Theorem 6.6 once again to deduce $xy \sim uv$. □

Note: In other words, Theorem 7.15 says that the second operation in $(*)$ is well-defined.

We can also proceed with a similar proof for the first operation in $(*)$ to show well-definedness.

Theorem *If* $[x] = [u]$ *and* $[y] = [v]$, *then* $[u] + [v] = [x] + [y]$.

Proof: By assumption, let $x \sim u$ and $y \sim v$; recall this means that each pair of equivalent elements share the same remainder upon division by n. By Theorem 6.6, there exist $k_1, k_2 \in \mathbb{Z}$ where $x - u = k_1 n$ and $y - v = k_2 n$; these mean $x = k_1 n + u$ and $y = k_2 n + v$, respectively. Thus,

$$\begin{aligned} x + y &= (k_1 n + u) + (k_2 n + v) \\ &= (k_1 + k_2)n + (u + v). \end{aligned}$$

We can apply Theorem 6.6 once again to deduce $x + y \sim u + v$. □

8 Congruence Equations and RSA Encryption

Note: Instead of thinking in terms of equivalence classes, we think of $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ where addition and multiplication are done modulo n per the operations defined in $(*)$.

We want to answer questions like "find integers x between 0 and n such that $ax = b \pmod{n}$". Using the note, this means we want $x \in \mathbb{Z}_n$ satisfying the aforementioned equivalence modulo n.

Theorem 8.1 *Let $a, b, n \in \mathbb{Z}$ with $n \geq 1$ and $h := \gcd(a, n)$.*
(i) *If $h \nmid b$, then $ax = b \pmod{n}$ has* **no** *solutions.*
(ii) *If $h \mid b$, then $ax = b \pmod{n}$ has exactly h solutions in $\mathbb{Z}_n$, which are given by*

$$x = \frac{bk}{h} + m\frac{n}{h}$$

for all $m \in \mathbb{Z}$ with $0 \leq m < h$, where we write $h = ka + ln$ (Theorem 5.11).

Proof: (i) If $x \in \mathbb{Z}$ satisfies $ax = b \pmod{n}$, then $n \mid (ax - b)$. The fact that $h \mid n$ tells us that $h \mid (ax - b)$ by Theorem 4.8(i). But because $h \mid a$ since it is a divisor by assumption, it follows that $h \mid b$. By the contrapositive, if $h \nmid b$, then $ax = b \pmod{n}$ has **no** solutions, as required.

(ii) If $h \mid b$, it is clear that $bk/h \in \mathbb{Z}$ is an integer. More than that, it is a solution. Indeed,

$$a\frac{bk}{h} = \frac{b}{h}(ka) = \frac{b}{h}(h - ln) = b \pmod{n}.$$

We now let $x \in \mathbb{Z}$ be **any** solution of $ax = b \pmod{n}$. If we subtract the above solution from this one, we know from (the note after) Theorem 6.8 that

$$a\left(x - \frac{bk}{h}\right) = 0 \pmod{n}.$$

In other words, $n \mid a(x - bk/h)$ from which it follows $n/h \mid (a/h)(x - bk/h)$. Since $h = \gcd(a, n)$, we can look at the prime factorisations of n/h and a/h to conclude that they share **no common** prime factors. Therefore, Euclid's Lemma (Corollary 5.13) implies that

$$\frac{n}{h} \,\Big|\, \left(x - \frac{bk}{h}\right) \qquad \Rightarrow \qquad x - \frac{bk}{h} = m\frac{n}{h} \qquad \Leftrightarrow \qquad x = \frac{bk}{h} + m\frac{n}{h}.$$

for some $m \in \mathbb{Z}$. To see that we get precisely these solutions in $\mathbb{Z}_n$, we must now observe that

$$\begin{aligned} \frac{bk}{h} + m_1\frac{n}{h} = \frac{bk}{h} + m_2\frac{n}{h} \pmod{n} &\Leftrightarrow n \,\Big|\, \left(m_1\frac{n}{h} - m_2\frac{n}{h}\right) \\ &\Leftrightarrow nh \mid (m_1 n - m_2 n) \\ &\Leftrightarrow h \mid (m_1 - m_2). \end{aligned}$$

□

Note: Use the reverse Euclidean Algorithm to get k and thus solutions to $ax = b \pmod{n}$.

RSA Encryption

The principal behind RSA encryption is the following: it is easy to multiply two primes and note the answer. However, given a 'large' number, it is much more difficult (computationally) to factorise it into a product of primes. Throughout, we let p and q be two 'large' primes and set

$$n \coloneqq pq.$$

Definition 8.3 The private key is a number $k \in \mathbb{Z}$ such that $\gcd(k, (p-1)(q-1)) = 1$.

We care about k modulo $(p-1)(q-1)$, so it is sufficient to restrict to $1 \leq k \leq (p-1)(q-1)$.

Definition 8.4 The public key is the pair (a, n) where $a \in \mathbb{Z}$ comes from Bézout's Identity

$$ak + b(p-1)(q-1) = 1.$$

The existence of $a, b \in \mathbb{Z}$ in Definition 8.4 is guaranteed by Theorem 5.11. Moreover, we again assume that $1 \leq a \leq (p-1)(q-1)$ and we can determine the public key corresponding to a pair of primes by applying the reverse Euclidean Algorithm, assuming we know the private key.

Definition A message is $M \in \mathbb{Z}$ such that $0 \leq M \leq n-1$. In RSA encryption, we say that an encrypted message is $rM^a \pmod{n}$ and a decrypted message is $N^k = M \pmod{n}$.

Method – Encrypting and Decrypting: Let the public and private keys be (a, n) and k.

- To encrypt a message M, we simply reduce M^a modulo n.
- To decrypt a message N, we simply reduce N^k modulo n.

9 Rational and Irrational Numbers

The Rationals

Definition 9.1 A real number $r \in \mathbb{R}$ is rational if there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that

$$r = \frac{m}{n}.$$

We say that such a rational number is in lowest terms if $\gcd(m, n) = 1$.

Recall we denote the set of rationals by $\mathbb{Q}$, because a rational is a *quotient* of two integers.

Note: We have 'known' for years that we can simplify a rational so it is in lowest terms. Being more mathematically precise, this actually follows from Theorem 5.4(iv) by choosing

$$m = \frac{a}{\gcd(a, b)} \qquad \text{and} \qquad n = \frac{b}{\gcd(a, b)}.$$

Remark 9.3 Formally, the rational numbers should be introduced as an equivalence relation $\sim$ on the set $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, where $(a, b) \sim (c, d)$ if and only if $ad = bc$. We then identify the rational number a/b with the equivalence class $[(a, b)]$. We rarely use this definition in practice, but it can be good to keep in mind. The fact a rational is associated to an equivalence class covers the fact that there are infinitely many ways to write a rational $r \in \mathbb{Q}$ as a fraction:

$$\left\{ \frac{m}{n} \right\} = \left\{ \frac{km}{kn} : k \in \mathbb{Z} \setminus \{0\} \right\}.$$

Lemma 9.4 *Suppose we have two rational numbers $a, b \in \mathbb{Q}$. Then, the following are true:*

$$a + b \in \mathbb{Q}, \qquad a - b \in \mathbb{Q}, \qquad ab \in \mathbb{Q}, \qquad \frac{a}{b} \in \mathbb{Q} \text{ if } b \neq 0.$$

Proof: Since $a, b \in \mathbb{Q}$, there exist $m, n, p, q \in \mathbb{Z}$ with $n, q \neq 0$ such that $a = m/n$ and $b = p/q$.

(i) Now, $a + b = \dfrac{m}{n} + \dfrac{p}{q} = \dfrac{mq + np}{nq} \in \mathbb{Q}$ because $mq + np, nq \in \mathbb{Z}$ and $nq \neq 0$.

(ii) Now, $a - b = \dfrac{m}{n} - \dfrac{p}{q} = \dfrac{mq - np}{nq} \in \mathbb{Q}$ because $mq - np, nq \in \mathbb{Z}$ and $nq \neq 0$.

(iii) Now, $ab = \dfrac{m}{n} \cdot \dfrac{p}{q} = \dfrac{mp}{nq} \in \mathbb{Q}$ because $mp, nq \in \mathbb{Z}$ and $nq \neq 0$.

(iv) Now, $\dfrac{a}{b} = \dfrac{m}{n} \div \dfrac{p}{q} = \dfrac{mq}{np} \in \mathbb{Q}$ because $mq, np \in \mathbb{Z}$ and $np \neq 0$ (since $b \neq 0$ so $p \neq 0$). □

Note: It is **not** true in general that $\sqrt{r} \in \mathbb{Q}$ where $r \in \mathbb{Q}$. This motivates the next topic.

The Irrationals

Definition 9.7 A real number $r \in \mathbb{R}$ is irrational if it is **not** rational, that is $r \in \mathbb{R} \setminus \mathbb{Q}$.

We will show how to prove a number is irrational in two ways (you should learn both methods).

Proposition 9.5 *The number $\sqrt{2}$ is irrational.*

Proof (Version 1): Assume to the contrary that $\sqrt{2}$ is rational, meaning there exist $m, n \in \mathbb{N}$ (we can use $\mathbb{N}$ here since $\sqrt{2}$ is positive) in **lowest terms** with $n \neq 0$ such that

$$\sqrt{2} = \frac{m}{n}.$$

If we multiply through by n and square both sides, we get $2n^2 = m^2$; this tells us that m^2 is even, meaning $2 \mid m^2$. By Theorem 5.15, it follows that $2 \mid m$, i.e. m itself is even. Therefore, there exists $k \in \mathbb{Z}$ such that $m = 2k$. Substituting this into the previous equation, we have

$$2n^2 = m^2 = (2k)^2 = 4k^2 \qquad \Rightarrow \qquad n^2 = 2k^2.$$

By the same reasoning, we now see that n^2 is even, and thus n is even. Altogether, we have $2 \mid m$ and $2 \mid n$, contradicting the lowest terms assumption. Thus, $\sqrt{2}$ is irrational. □

Proof (Version 2): Assume to the contrary that $\sqrt{2}$ is irrational, meaning there exist $m, n \in \mathbb{N}$ (not necessarily in lowest terms, this time) with $n \neq 0$ such that

$$\sqrt{2} = \frac{m}{n}.$$

Suppose $p_1 p_2 \cdots p_k$ and $q_1 q_2 \cdots q_l$ are the prime factorisations of m and n, respectively. Then, multiplying the above by n, squaring and substituting in the prime factorisations produces

$$2q_1^2 q_2^2 \cdots q_l^2 = p_1^2 p_2^2 \cdots p_k^2.$$

The left-hand side contains an odd number of factors of 2, whereas the right-hand side contains an even number of factors of 2; this contradicts the Fundamental Theorem of Arithmetic which says the prime factorisation is unique up to reordering of primes. Thus, $\sqrt{2}$ is irrational. □

Remark 9.6 In Proposition 9.5, we have assumed that $\sqrt{2}$ exists, that is there exists a positive real number $x > 0$ such that $x^2 = 2$. The fact this is true isn't trivial, and is something which can be proven rigorously by looking at properties of continuous functions (see MATH1026). For now, we suspend disbelief and assume that all roots of all positive numbers do indeed exist.

Proposition *The number $\sqrt[7]{25}$ is irrational.*

Proof (Version 1): Assume to the contrary that $\sqrt[7]{25}$ is rational, meaning there exist $m, n \in \mathbb{N}$ in **lowest terms** with $n \neq 0$ such that

$$\sqrt[7]{25} = \frac{m}{n}.$$

If we multiply through by n and raise both sides to the power of seven, we get $25n^7 = m^7$; this tells us that $5 \mid m^2$. By Theorem 5.15, it follows that $5 \mid m$. Therefore, there exists $k \in \mathbb{Z}$ such that $m = 5k$. Substituting this into the previous equation, we have

$$25n^7 = m^7 = (5k)^7 = 5^7k^7 \qquad \Rightarrow \qquad n^2 = 5^5k^2.$$

By the same reasoning, we now see that $5 \mid n^2$, and thus $5 \mid n$. Combined with the fact $5 \mid m$, this contradicts the lowest terms assumption. Thus, $\sqrt[7]{25}$ is irrational. □

Proof (Version 2): Assume to the contrary that $\sqrt[7]{25}$ is irrational, meaning there exist $m, n \in \mathbb{N}$ (not necessarily in lowest terms, this time) with $n \neq 0$ such that

$$\sqrt[7]{25} = \frac{m}{n}.$$

Suppose $p_1p_2 \cdots p_k$ and $q_1q_2 \cdots q_l$ are the prime factorisations of m and n, respectively. Then, multiplying the above by n, raising both sides to the power of seven and substituting in the prime factorisations produces

$$25q_1^7q_2^7 \cdots q_l^7 = p_1^7p_2^7 \cdots p_k^7.$$

The number of factors of 5 on the left-hand side is equivalent to 2 (mod 7), whereas the number of factors of 5 on the right-hand side is congruent to 0 (mod 7); this contradicts the Fundamental Theorem of Arithmetic which says the prime factorisation is unique up to reordering of primes. Thus, $\sqrt[7]{25}$ is irrational. □

Proposition 9.8 *Let $p \in \mathbb{Z}$ be prime. Then, $\sqrt{p}$ is irrational.*

Sketch of Proof: Simply adapt either of the proofs of Proposition 9.5. □

Lemma *If $a \in \mathbb{R} \setminus \mathbb{Q}$, then $\sqrt{a} \in \mathbb{R} \setminus \mathbb{Q}$.*

Proof: Suppose to the contrary that $\sqrt{a} \in \mathbb{Q}$. Then, we can write it as $\sqrt{a} = m/n$ for some $m, n \in \mathbb{Z}$ with $n \neq 0$. If we square both sides, we get $a = m^2/n^2 \in \mathbb{Q}$ since $m^2, n^2 \in \mathbb{Z}$ and $n^2 \neq 0$; this contradicts the fact that $a \in \mathbb{R} \setminus \mathbb{Q}$. □

Lemma *If $a \in \mathbb{R} \setminus \mathbb{Q}$ and $b \in \mathbb{Q}$, then $a - b \in \mathbb{R} \setminus \mathbb{Q}$.*

Proof: Suppose to the contrary that $a - b \in \mathbb{Q}$. Then, we can write it as $a - b = m/n$ for some $m, n \in \mathbb{Z}$ with $n \neq 0$. Since $b \in \mathbb{Q}$, we can write it as $b = r/s$ for some $r, s \in \mathbb{Z}$ with $s \neq 0$. Substituting this into the first equation and rearranging gives $a = r/s + m/n \in \mathbb{Q}$ by Lemma 9.4; this contradicts the fact that $a \in \mathbb{R} \setminus \mathbb{Q}$. □

Note: There exist many more irrational numbers, including non-root ones like π and e.

Even though π and e are also irrational, they have a different flavour to the irrationals like $\sqrt{2}$ and $\sqrt[7]{25}$ and what not. Indeed, these root irrationals appear as solutions to polynomial equations with integer coefficients (e.g. $x^2 - 2 = 0$ and $x^7 - 25 = 0$ for these two). However, π and e are **not** the roots of an integer polynomial.

Definition An irrational is called an algebraic number if it is the solution to an integer polynomial equation. Otherwise, it is called a transcendental number.

Remark Although we know π and e are transcendental, it is an open problem (unknown) whether or not the following numbers are even irrational, let alone if they are algebraic or transcendental:

$$\pi + e, \qquad \pi - e, \qquad \pi e, \qquad \frac{\pi}{e}, \qquad \pi^e.$$

There is a relatively straightforward argument which shows that **at least one** of $\pi + e$ and πe is irrational, but there is no known method to prove that they both are (of course, it seems strange to think that they could be rational but without a rigorous proof, we do not know for certain).

10 Decimals

In the number system we use (base 10), we place digits into columns that represent certain powers of 10. If they are to the left of the decimal point, they are non-negative powers; if they are to the right of the decimal point, they are negative powers. Concretely, if we use letters to denote digits, the *numeral* $a_m a_{m-1} \dots a_1 a_0 . b_1 b_2 \dots b_n$ represents the following number:

$$a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10^1 + a_0 + \frac{b_1}{10} + \frac{b_2}{10^2} + \dots + \frac{b_n}{10^n}. \qquad (\dagger)$$

Definition A decimal expression is terminating if it is of the form

$$n.a_1 \dots a_k = n.a_1 \dots a_k 000 \dots,$$

where $n \in \mathbb{Z}$ and each digit $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for $1 \leq i \leq k$.

In other words, there is a non-zero digit in a terminating decimal after which all remaining digits are zero. Before we look at other types of decimal, let's state an important result regarding terminating decimals.

Theorem 10.1 *If a real number is represented by a terminating decimal, then it is rational.*

Proof: This is immediate from the expression (†) and Lemma 9.4 applied repeatedly. □

Note: The converse of Theorem 10.1 is false, since $\frac{1}{3} \in \mathbb{Q}$ but we know that $\frac{1}{3} = 0.33333...$.

Definition 10.3 A decimal expression is recurring (or repeating) if it is of the form

$$n.a_1 \dots a_k b_1 \dots b_l b_1 \dots b_l b_1 \dots b_l \dots,$$

where $n \in \mathbb{Z}$ and each digit $a_i, b_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for $1 \leq i \leq k$ and $1 \leq j \leq l$.

If we write an expression similar to (†) for a recurring decimal, we see that the sum is now infinite! A precise way to deal with this is deferred to the module MATH1026, but we will learn how to use an important result.

Theorem 10.4 (Geometric Series) *Let $r \in \mathbb{R}$ with $|r| < 1$, that is $-1 < r < 1$. Then,*

$$\sum_{i=0}^{\infty} r^i = 1 + r + r^2 + r^3 + r^4 + \dots = \frac{1}{1-r}.$$

Another useful result is a *truncated* geometric series (which is finite, and thus holds for all reals).

Proposition *Let $r \in \mathbb{R}$. Then,*

$$\sum_{i=0}^{n} r^i = 1 + r + r^2 + r^3 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

Proof: We proceed with a proof by induction. For the initial case ($n = 0$), we see that the left-hand side is 1 and the right-hand side is $(1 - r)/(1 - r) = 1$. Hence, the initial case holds. For the inductive step, assume the formula holds when $n = k$ for some $k \in \mathbb{N}$:

$$\sum_{i=0}^{k} r^i = \frac{1 - r^{k+1}}{1 - r}.$$

We wish to use the above to show that the formula is true when $n = k + 1$, that is

$$\sum_{i=0}^{k+1} r^i = \frac{1 - r^{(k+1)+1}}{1 - r} = \frac{1 - r^{k+2}}{1 - r}.$$

Indeed, we see that

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \sum_{i=0}^{k} r^i + r^{k+1} \\
&= \frac{1 - r^{k+1}}{1 - r} + r^{k+1}, && \text{by the inductive hypothesis,} \\
&= \frac{1 - r^{k+1}}{1 - r} + \frac{(1 - r)r^{k+1}}{1 - r} \\
&= \frac{1 - r^{k+1} + r^{k+1} - r^{k+2}}{1 - r} \\
&= \frac{1 - r^{k+2}}{1 - r}.
\end{aligned}$$

By the Principal of Mathematical Induction, the formula is true for all $n \in \mathbb{N}$. □

Note: We use the following shorthand notation for recurring decimal expressions:

$$n.\overline{d} \text{ or } n.\dot{d} \coloneqq n.ddd\ldots \qquad \text{and} \qquad n.a_1 \ldots a_k\overline{b_1 \ldots b_l} \coloneqq n.a_1 \ldots a_k b_1 \ldots b_l b_1 \ldots b_l \ldots.$$

Ultimately, we will derive a means to express any recurring decimal as a fraction (this tells us that all recurring decimals are rational numbers; we prove this properly later).

Lemma *For all $d \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, we have $0.\overline{d} = 0.ddd\ldots = \frac{d}{9}$.*

Proof: Given the decimal expression $0.\overline{d}$, we write this in the form similar to (†) and obtain

$$\frac{d}{10}+\frac{d}{10^2}+\frac{d}{10^3}+\cdots=\frac{d}{10}\left(1+\frac{1}{10}+\frac{1}{10^2}+\cdots\right)=\frac{d}{10}\sum_{i=0}^{\infty}\left(\frac{1}{10}\right)^i.$$

If we use the geometric series formula from Theorem 10.4 with $r=1/10$, the above becomes

$$\frac{d}{10}\cdot\frac{1}{1-1/10}=\frac{d}{10}\cdot\frac{1}{9/10}=\frac{d}{9}.$$

□

Lemma *For all $d,e\in\{0,1,2,3,4,5,6,7,8,9\}$, we have $0.\overline{de}=0.dedede\ldots=\dfrac{10d+e}{99}$.*

Proof: Given the decimal expression $0.\overline{de}$, we write this in the form similar to (†) and obtain

$$\frac{10d+e}{100}+\frac{10d+e}{100^2}+\frac{10d+e}{100^3}+\cdots=\frac{10d+e}{100}\left(1+\frac{1}{100}+\frac{1}{100^2}+\cdots\right)=\frac{10d+e}{100}\sum_{i=0}^{\infty}\left(\frac{1}{100}\right)^i.$$

If we use the geometric series formula from Theorem 10.4 with $r=1/100$, the above becomes

$$\frac{10d+e}{100}\cdot\frac{1}{1-1/100}=\frac{10d+e}{100}\cdot\frac{1}{99/100}=\frac{10d+e}{99}.$$

□

Proposition *For $b_i\in\{0,1,2,3,4,5,6,7,8,9\}$ with $1\leq i\leq l$, we have*

$$0.\overline{b_1\ldots b_l}=\frac{10^{l-1}b_1+10^{l-2}b_2+\cdots+10b_{l-1}+b_l}{10^l-1}.$$

Proof: Given the decimal expression $0.\overline{b_1\ldots b_l}$, we write this in the form similar to (†) and obtain

$$\frac{s}{10^l}+\frac{s}{10^{2l}}+\frac{s}{10^{3l}}+\cdots=\frac{s}{10^l}\left(1+\frac{1}{10^l}+\frac{1}{10^{2l}}+\cdots\right)=\frac{s}{10^l}\sum_{i=0}^{\infty}\left(\frac{1}{10^l}\right)^i.$$

with $s\coloneqq 10^{l-1}b_1+10^{l-2}b_2+\cdots+10b_{l-1}+b_l$ the number with digits b_i in order from left-to-right. If we use the geometric series formula from Theorem 10.4 with $r=1/10^l$, the above becomes

$$\frac{s}{10^l}\cdot\frac{1}{1-1/10^l}=\frac{s}{10^l-1}.$$

□

Note: A slightly unsettling implication from this work is that we have $0.\overline{9}=0.999\ldots=1$.

The above note shows that different decimal expressions can represent the same real number. This is a bit problematic, because it seems we can not introduce the real numbers as the set of all

decimal expression (there will be duplicates). However, the extent of the problem is minimised by the result we now prove.

Proposition 10.8 *If a real number is represented by two different decimal expressions, then one ends in repeating nines and the other ends in repeating zeros (i.e. terminates).*

Proof: Let $x \in \mathbb{R}$ have two different decimal expressions. It suffices to work with decimals that have integer part zero, since there always exists $k \in \mathbb{N}$ such that multiplying each decimal expression by 10^{-k} puts it in this form (we just move the decimal point k places to the left). Hence, suppose the two decimal expressions of x are

$$0.a_1a_2a_3\ldots \qquad \text{and} \qquad 0.b_1b_2b_3\ldots.$$

Let the n^{th} digit be the first place where these expansions differ; the above are of the form

$$0.a_1\ldots a_{n-1}a_na_{n+1}\ldots \qquad \text{and} \qquad 0.a_1\ldots a_{n-1}b_nb_{n+1}\ldots.$$

Without loss of generality, assume that $a_n < b_n$, meaning that $a_n + 1 \leq b_n$ (because they are integers). But since both decimals are equal to x, we get the inequality

$$0.a_1\ldots a_{n-1}b_n000\ldots \leq x \leq 0.a_1\ldots a_{n-1}(a_n+1)000\ldots.$$

This tells us that $b_n \leq a_n+1$. We therefore conclude that $b_n = a_n+1$. It now follows that $a_k = 9$ and $b_k = 0$ for all $k \geq n+1$. If this was **not** the case, we would get the following nonsense:

$$x - x = 0.a_1\ldots a_{n-1}(a_n+1)b_{n+1}\ldots - 0.a_1\ldots a_{n-1}a_na_{n+1} > 0. \qquad \square$$

Note: We now know there are rational numbers with non-terminating decimal expressions.

Theorem 10.10 *A real number is rational if and only if it has a recurring or a terminating decimal expression.*

Proof: ($\Rightarrow$) Let $r \in \mathbb{Q}$ be rational, so it has the form $r = m/n$ for some $m, n \in \mathbb{Z}$ with $n \neq 0$. To convert this into a decimal, we can perform long division; each stage produces a remainder at most $n-1$. After exhausting all the digits of m, we have finitely-many more steps that either give a remainder of zero (the decimal is terminating) or we get a remainder we had before (the decimal is recurring).

($\Leftarrow$) Let $r \in \mathbb{R}$ have a recurring or terminating decimal expression, that is it's of the form

$$r = n.a_1\ldots a_k\overline{b_1\ldots b_l}.$$

Note the terminating case is where $l = 1$ and $b_1 = 0$. Using the proposition-before-last, we have

$$r = n + \frac{10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k}{10^k - 1} + \frac{1}{10^k}\frac{10^{l-1}b_1 + 10^{l-2}b_2 + \cdots + 10b_{l-1} + b_l}{10^l - 1},$$

which is rational by Lemma 9.4. $\square$

Definition A set X is densely ordered if, for all $x, y \in X$ with $x < y$, there exists $z \in X$ such that $x < z < y$. This means there is always an element between two distinct elements.

Lemma 10.11 *The rationals are densely ordered (in the reals).*

Proof: Let $r, s \in \mathbb{Q}$ with $r < s$. We claim that $(r + s)/2 \in \mathbb{Q}$ (which is clear to us) and that

$$r < \frac{r+s}{2} < s.$$

Well, $r + r < r + s < s + s$. This equivalent to $2r < r + s < 2s$, so just divide by two. □

Proposition *The following are true:*

(i) *The irrationals are densely ordered (in the reals).*
(ii) *Between any two rational numbers, there is an irrational number.*
(iii) *Between any two irrational numbers, there is a rational number.*

Sketch of Proof: Omitted; they are not too different from the proof of Lemma 10.11. As for showing that there is an irrational, it is usually the case that we pick a known irrational number (e.g. $\sqrt{2}$) and divide it by a rational; this produces an irrational which is small enough to fit in the gap we want. □

Note: Overall, we have shown the following: $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. However, all of these sets are infinitely large, but it appears some are 'bigger' than others: the denseness tells us that the rational numbers are tightly packed amongst them. We now want to develop some theory which allows us to understand this chain of proper subsets and their sizes.

11 Functions

Definition 11.1 (Vague) A function f from a set A to a set B is a rule that assigns to each $a \in A$ a unique $b \in B$, referred to as $f(b)$. We denote this $f : A \to B$ with $a \mapsto f(a)$.

In practice, we work with Definition 11.1. However, we have glossed over the meaning of "rule" in the above definition. We will make a more precise definition now, but it is infrequently used.

Definition 11.2 (Precise) A function f from a set A to a set B is a non-empty subset $f \subseteq A \times B$ such that for each $a \in A$, there is one and only one pair $(x, y) \in f$ with $x = a$. In other words, for all $a \in A$, there exists $b \in B$ such that $(a, b) \in f$ **and** if $(a, b) \in f$ and $(a, c) \in f$, it follows that $b = c$.

Notation It is important to realise the distinction between f and $f(x)$. The first one f is the name of the function (formally a subset of $A \times B$ as written in Definition 11.2). On the other hand, the second one $f(x)$ is an element of B.

Note: We call the set A the domain of f, and the set B the co-domain (or target) of f.

We often use the term *map* to mean an assignment of elements of one set to elements of another set. Here, there are no restrictions compared to what we demand in the above definitions. As such, given a map, how do we know if it is a function?

Method – Checking if a Map is a Function: Suppose we are given a map $f : A \to B$ from one set to another. In order to see that this is indeed a function, we must check that everything in A indeed has something it goes to in B, and that there is no element of A that goes to two **different** elements of B.

It might be that a function has a large co-domain but doesn't actually 'hit' everything in it.

Definition Let $f : A \to B$ be a function between sets. The image (or range) of f is the set

$$\mathrm{im}(f) = f(A) \coloneqq \{f(a) : a \in A\} \subseteq B.$$

The next definition allows us to build a new function from two pre-existing ones. It may seem a bit random now but this concept will help us give meaning to a special class of functions soon.

Definition 11.8 Let $f : A \to B$ and $g : B \to C$ be two functions. The composition of f and g is the function $g \circ f : A \to C$ which is given by $(g \circ f)(x) = g(f(x))$.

Injective Functions

Definition 11.5 A function $f : A \to B$ is injective (or one-to-one) if for every $b \in B$, there is at most one $a \in A$ such that $f(a) = b$. In other words, a function is injective if $f(a_1) = f(a_2)$ implies $a_1 = a_2$ for all $a_1, a_2 \in A$.

Remark 11.7 For a function $f : \mathbb{R} \to \mathbb{R}$ for which we have a picture of its graph, we can spot very quickly whether or not it is injective. Indeed, f is injective if and only if **no** horizontal line intersects the graph in more than **one** place.

Lemma 11.10 *The composition of two injective functions is itself injective.*

Proof: Let $f : A \to B$ and $g : B \to C$ be injective. We must show that if $(g \circ f)(a_1) = (g \circ f)(a_2)$, then $a_1 = a_2$ for all $a_1, a_2 \in A$. Writing this using Definition 11.8 tells us $g(f(a_1)) = g(f(a_2))$. Since g is injective, we have $f(a_1) = f(a_2)$. But because f is injective, it follows that $a_1 = a_2$. □

Surjective Functions

Definition 11.11 A function $f : A \to B$ is surjective (or onto) if for every $b \in B$, there is at least one $a \in A$ such that $f(a) = b$. In other words, a function is surjective if $\text{im}(f) = B$.

Remark For a function $f : \mathbb{R} \to \mathbb{R}$ for which we have a picture of its graph, we can spot very quickly whether or not it is surjective. Indeed, f is surjective if and only if **every** horizontal line intersects the graph at least once. In other words, if we flatten the function onto the y-axis, it completely covers said axis.

Lemma 11.13 *The composition of two surjective functions is itself surjective.*

Proof: Let $f : A \to B$ and $g : B \to C$ be surjective functions. We must show that for all $c \in C$, there exists $a \in A$ such that $(g \circ f)(a) = c$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. But because f is surjective, there exists $a \in A$ such that $f(a) = b$. Combining these gives $g(f(a)) = c$. □

Bijections

Definition 11.14 A function $f : A \to B$ is bijective if it is both injective and surjective.

Remark 11.15 Looking at Definition 11.5 (resp. Definition 11.11), it says that every element in the co-domain has at most (resp. at least) one element in the domain which gets mapped to it. Therefore, combining these tells us that a bijection $f : A \to B$ is such that for every $b \in B$, there is **exactly one** $a \in A$ such that $f(a) = b$.

Lemma 11.17 *Let $f : A \to B$ be a bijection, viewed as a subset $f \subseteq A \times B$ à la* Definition 11.2. *Then, we get a bijection $f^{-1} : B \to A$ in the opposite direction, viewed as a subset*

$$f^{-1} \coloneqq \{(b, a) \in B \times A : (a, b) \in f\} \subseteq B \times A.$$

Proof: We must show not only that f^{-1} is injective and surjective, but that it is a function.

(i) To show f^{-1} is a function, we must demonstrate that for all $b \in B$, there exists one and only one $a \in A$ such that $a \in A$ with $(b, a) \in f^{-1}$. Well, the surjectivity of f tells us that for every $b \in B$, there is **at least** one $a \in A$ with $(a, b) \in f$, which implies $(b, a) \in f^{-1}$. On the other hand, the injectivity of f tells us there is **at most** one such $a \in A$. Combining these tells us indeed that f^{-1} is a function.

(ii) To show f^{-1} is injective, we must demonstrate that for all $b_1, b_2 \in B$ and $a \in A$, if $(b_1, a), (b_2, a) \in f^{-1}$, then $b_1 = b_2$. Well, $(b_1, a), (b_2, a) \in f^{-1}$ implies $(a, b_1), (a, b_2) \in f$. Because f is a function, this means that $b_1 = b_2$ (directly from Definition 11.2).

(iii) To show f^{-1} is surjective, we must demonstrate that for all $a \in A$, there exists at least one $b \in B$ with $(b, a) \in f^{-1}$. But because f is a function, we know for each $a \in A$, there exists $b \in B$ with $(a, b) \in f$, which implies that $(b, a) \in f^{-1}$. □

Definition 11.18 The inverse of a bijection $f : A \to B$ is the function $f^{-1} : B \to A$ defined in Lemma 11.17, that is a map which sends each $b \in B$ to the unique $a \in A$ with $f(a) = b$.

Note: We use $^{-1}$ to mean "the inverse"; this notation has nothing to do with the reciprocal.

Solving Equations

Method – Solving an Equation: When solving an equation, be mindful of implications. If we apply a function f to both sides of an equation, we must be aware of the following:

- $a = b \Rightarrow f(a) = f(b)$ is true for **all** functions f.
- $f(a) = f(b) \Rightarrow a = b$ is true for **injective** functions f only.

12 Sizes of Sets

Reminder: The cardinality of a set X is the number of elements of X, denoted $|X|$.

Definition 12.1 Two non-empty sets A and B have the same cardinality if there exists a bijection between A and B. We say that A is finite if there exists a bijection between A and $\{1, 2, ...n\}$ for some $n \in \mathbb{N}$. If no such bijection exists, we say that A is infinite.

Note: Of course, $A = B = \emptyset$ have the same cardinality and are finite, with $|A| = |B| = 0$.

Remark 12.2 It seems obvious $|A| = |B|$ implies $|B| = |A|$, but this actually follows from the fact that a bijection $f : A \to B$ admits a reverse bijection $f^{-1} : B \to A$ (see Lemma 11.17).

Definition 12.5 A set S is countably infinite if it has the same cardinality as $\mathbb{N}$, that is there exists a bijection $f : \mathbb{N} \to S$ (or a bijection $f : S \to \mathbb{N}$, whichever is more convenient).

Informally, we think of a bijection $f : \mathbb{N} \to S$ as an infinitely-long list of the elements of S; this really is an assignment $f(1), f(2), f(3), ...$ to each element of S. We are "counting" the elements.

Note: We then call an arbitrary set S countable if it is either finite or countably infinite.

Lemma 12.6 *Let S be countably infinite and $x \notin S$. Then, $S \cup \{x\}$ is countably infinite.*

Proof: Since S is countably infinite, there is a bijection $f : \mathbb{N} \to S$. We now define the function

$$g : \mathbb{N} \to S \cup \{x\} \qquad \text{given by} \qquad g(n) = \begin{cases} x, & \text{if } n = 1 \\ f(n-1), & \text{if } n > 1 \end{cases}.$$

This is a bijection. Indeed, let $g(n) = g(m)$. If $g(n) = g(m) \in \{x\}$, then $n = m = 1$. On the other hand, if $g(n) = g(m) \in S$, then this is equivalent to $f(n-1) = f(m-1)$, which means $n - 1 = m - 1$ since f is bijective and hence injective. Either way, we see that $n = m$. On the other hand, let $s \in S \cup \{x\}$. If $s = x$, then $s = g(1)$. If $s \in S$, then there exists $n \in \mathbb{N}$ such that $s = f(n)$ because f is bijective and hence injective. But this means that $s = g(n + 1)$. Concluding, we see that $S \cup \{x\}$ is countably infinite. □

Note: In words, g shifts the counting f of the elements of S one number to the 'right'. This frees up a spot in the first place which can be filled with x. Disturbingly, this says

$$|S| = \big|S \cup \{x\}\big|.$$

Lemma 12.8 *Any subset of a countable set is also countable.*

Proof: Let S be countable and $A \subseteq S$ any subset. If A is finite, then it is countable by definition. So, assume A is infinite. This means that S must also be infinite. Because S is countable, there is a bijection $f : \mathbb{N} \to S$, so we write $S = \{s_1, s_2, s_3, ...\}$. Define $g : \mathbb{N} \to A$ inductively as follows:

$$g(1) = \text{the element } s_i \in A \text{ that has the smallest index } i,$$
$$g(n+1) = \text{the element } s_i \in A \setminus \{f(1), ..., f(n)\} \text{ that has the smallest index } i.$$

Again, this function g is a bijection, which tells us A is countably infinite and thus countable. □

Note: In words, g picks out the elements of S that are also in A and relabels them. Of course, since $S = \{s_1, s_2, s_3, ...\}$, it may be that our subset looks like $A = \{s_1, s_4, s_7, s_{20}, ...\}$ but we want to change the labelling given by f to one which uses all of the integers $1, 2, 3, ...$

Lemma 12.9 *The union of two countable sets is also countable.*

Proof: Let S and T be countable sets. If they are both finite, then $S \cup T$ is also finite and hence countable. If one is infinite (S say, without loss of generality) and T is finite, we can apply Lemma 12.6 inductively, adding each element of T in turn. This previous result tells us that $S \cup T$ is countably infinite and thus countable. The final (more interesting) case is where S and T are **both** infinite. By assumption, there are two bijections

$$f : \mathbb{N} \to S \qquad \text{and} \qquad g : \mathbb{N} \to T.$$

We can assume that S and T are disjoint ($S \cap T = \emptyset$) without loss of generality; sets don't care about repetitions so if there were elements in both S and T, the union would contain only one copy of any such element. Then, we can define the function

$$h : \mathbb{N} \to S \cup T \qquad \text{given by} \qquad h(n) = \begin{cases} f\left(\dfrac{n+1}{2}\right), & \text{if } n \text{ is odd} \\ g\left(\dfrac{n}{2}\right), & \text{if } n \text{ is even} \end{cases}.$$

This function h is a bijection and so we know $S \cup T$ is countably infinite and thus countable. □

Note: In words, h just lists the elements of S and T in an alternating way and relabels everything so that it uses all of the integers $1, 2, 3, ...$ Indeed, countability means we have $S = \{s_1, s_2, s_3, ...\}$ and $T = \{t_1, t_2, t_3, ...\}$. Their union is $S \cup T = \{s_1, t_1, s_2, t_2, s_3, t_3...\}$.

Proposition 12.10 *The set of integers $\mathbb{Z}$ is countably infinite.*

Proof (Version 1): We can define a bijection as follows, which immediately implies the result:

$$f : \mathbb{N} \to \mathbb{Z} \qquad \text{given by} \qquad f(n) = \begin{cases} \dfrac{1-n}{2}, & \text{if } n \text{ is odd} \\ \dfrac{n}{2}, & \text{if } n \text{ is even} \end{cases}.$$ □

Proof (Version 2): The set $\mathbb{Z}^- = \{0, -1, -2, -3, ...\}$ of non-positive integers is countable since $f : \mathbb{N} \to \mathbb{Z}^-$ given by $f(n) = 1 - n$ is a bijection. But because $\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}^-$ (and obviously $\mathbb{N}$ itself is countable via the trivial bijection $n \mapsto n$), the countability of $\mathbb{Z}$ follows from Lemma 12.9. □

Proposition 12.11 *The Cartesian product $\mathbb{N} \times \mathbb{N}$ is countable.*

Proof (Version 1): We can define a bijection as follows, which immediately implies the result:

$$\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad \text{given by} \qquad \varphi(u, v) = 2^{u-1}(2v - 1). \tag{$\star$}$$

We will show bijectivity. Indeed, $\varphi(a, b) = \varphi(c, d)$ means $2^{a-1}(2b - 1) = 2^{c-1}(2d - 1)$. Without loss of generality, we can assume that $a \geq c$. We now divide by 2^{c-1} to obtain the equation

$$2^{a-c}(2b - 1) = 2d - 1.$$

Because $2d - 1$ is odd, it follows that $2^{a-c} = 1$ (otherwise the left-hand side would be even); this means that $a = c$. The above equation now tells us that $2b - 1 = 2d - 1$, from which it is clear that $b = d$. Hence, $(a, b) = (c, d)$ and thus φ is injective. As for surjectivity, let $n \in \mathbb{N}$. We must find a pair of numbers $(a, b) \in \mathbb{N} \times \mathbb{N}$ such that $n = \varphi(a, b)$. Well, we can write

$$n = 2^k l$$

for integers $k \geq 0$ and l odd; this is a consequence of the Fundamental Theorem of Arithmetic, where l is the product of all odd prime factors of n. Since l is odd, we know that there exists $s \in \mathbb{Z}$ with $l = 2s - 1$. Substituting these above, we obtain $n = 2^k(2s - 1)$. This is nothing more than $\varphi(a, b)$ where we take $a = k + 1$ (note that $k \geq 0$ which means $a \geq 1$) and $b = s$. □

Proof (Version 2): This is more a proof-by-picture. The idea is to list the elements of $\mathbb{N} \times \mathbb{N}$ and 'snake' around, passing through everything in the list precisely once; see it in Figure 2 below. □

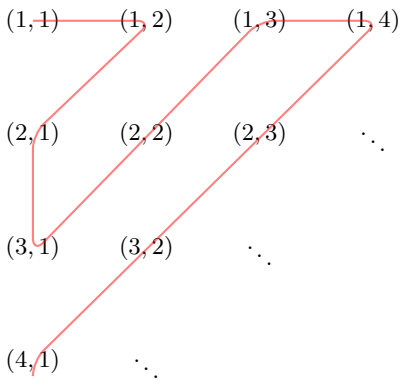

Figure 2: A pictorial argument showing the countability of $\mathbb{N} \times \mathbb{N}$.

Corollary 12.12 *The Cartesian product of two countable sets is also countable.*

Proof: Let S and T be countable. By assumption, there are two bijections

$$f : S \to \mathbb{N} \qquad \text{and} \qquad g : T \to \mathbb{N}.$$

Let $h : A \times B \to \mathbb{N}$ be given by $h(a, b) = \varphi(f(a), g(b))$ where φ is the bijection from $(\star)$. Because f, g, φ are all bijections, it follows that h is also a bijection (it is the composition of bijections, which is bijective by Lemmata 11.10 and 11.13). □

Lemma 12.13 *Let $S \neq \emptyset$ be a non-empty set. Then, the following are equivalent:*
(i) *S is countable.*
(ii) *There is a surjection from $\mathbb{N}$ onto S.*
(iii) *There is a surjection from a countable set T onto S.*

Proof: $\big((\text{i}) \Rightarrow (\text{ii})\big)$ This is trivial; there is a bijection $f : \mathbb{N} \to S$, but this is also a surjection.

$\big((\text{ii}) \Rightarrow (\text{iii})\big)$ This is also trivial; simply take $T = \mathbb{N}$ because we know $\mathbb{N}$ is countable.

$\big((\text{iii}) \Rightarrow (\text{i})\big)$ Let $f : T \to S$ be a surjection where B is countable; either $B = \{b_1, b_2, ..., b_n\}$ (if it is finite) or $B = \{b_1, b_2, b_3, ...\}$ (if it is infinite). Define the function $g : A \to B$ so that $g(a)$ is the element of **smallest index** in $\{b \in B : f(b) = a\}$. We know that this set is non-empty since f is surjective. Therefore, g is a bijection from A onto its image $\text{im}(g)$. Because $\text{im}(g) \subseteq B$ is a subset of a countable set, we know it is countable itself (Lemma 12.8). Therefore, A is countable (because $\text{im}(g) \subseteq B$ is in bijection with $\mathbb{N}$ and therefore so too is A by composition with g). □

Note: An efficient way to show a collection of statements are equivalent is to do as above: show one implies another, which implies another, etc. until we're back to the first one.

Theorem 12.14 *The set of rational $\mathbb{Q}$ is countable.*

Proof: We can define a surjection as follows:

$$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q} \qquad \text{given by} \qquad f(a, b) = \begin{cases} 0, & \text{if } b = 0 \\ \dfrac{a}{b}, & \text{if } b \neq 0 \end{cases}.$$

The surjectivity is clear. Since $\mathbb{Z}$ is countable (Proposition 12.10), it follows from Corollary 12.12 that the Cartesian product $\mathbb{Z} \times \mathbb{Z}$ is countable. Hence, Lemma 12.13 implies $\mathbb{Q}$ is countable. □

Definition 12.19 A set that is not countable is called uncountable.

Is Definition 12.19 redundant (i.e. do uncountable sets exist)? We can find one rather elegantly.

Proposition 12.17 *The power set $\mathcal{P}(\mathbb{N}) \coloneqq \{A \subseteq \mathbb{N}\}$ of $\mathbb{N}$ is uncountable.*

Proof: Assume to the contrary $\mathcal{P}(\mathbb{N})$ is countable, meaning there is a bijection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. In this case, note that each $f(n)$ is an element of $\mathcal{P}(\mathbb{N})$, i.e. $f(n)$ is a subset of $\mathbb{N}$. Let's consider the set $X = \{n \in \mathbb{N} : n \notin f(n)\} \subseteq \mathbb{N}$. Because f is a bijection, there exists $m \in \mathbb{N}$ such that $f(m) = X$. Now, there are two cases to consider:

(i) If $m \in X$, then $m \in f(m)$. But by definition of X, we have $m \notin X$.

(ii) If $m \notin X$, then $m \notin f(m)$. But by definition of X, we have $m \in X$.

Either way, we get a contradiction. Therefore, $\mathcal{P}(\mathbb{N})$ is uncountable. □

Note: We can define the power set of any X as the set of all subsets, i.e. $\mathcal{P}(X) \coloneqq \{A \subseteq X\}$.

Remark 12.18 The type of argument in the above proof is called "diagonal argument". We see another such proof below where it is more clear where the 'diagonal' comes from. Without going into too much depth, the name comes from the fact that $m \notin f(m)$ has m appearing twice.

Theorem 12.20 *The set of real numbers $\mathbb{R}$ is uncountable.*

Proof: Assume to the contrary $\mathbb{R}$ is countable. By Lemma 12.8, the interval $[0, 1) \subseteq \mathbb{R}$ is also countable; there is a bijection $f : \mathbb{N} \to [0, 1)$. Using decimal expressions **without** recurring nines, we write the images under this bijection as

$$\begin{aligned} f(1) &= 0.d_1^1 d_2^1 d_3^1 d_4^1 \ldots, \\ f(2) &= 0.d_1^2 d_2^2 d_3^2 d_4^2 \ldots, \\ f(3) &= 0.d_1^3 d_2^3 d_3^3 d_4^3 \ldots, \\ f(4) &= 0.d_1^4 d_2^4 d_3^4 d_4^4 \ldots, \\ &\vdots \end{aligned}$$

We will define a new real number $r = 0.d_1^* d_2^* d_3^* d_4^* \ldots$ where the digits for all $i \geq 1$ are given by

$$d_i^* = \begin{cases} 4, & \text{if } d_i^i \neq 4 \\ 5, & \text{if } d_i^i = 4 \end{cases}.$$

Clearly, $r \neq f(n)$ for any $n \in \mathbb{N}$ since r is different from $f(n)$ in the n^{th} decimal place. However, we do have $r \in [0, 1)$. This means that $r \notin \text{im}(f)$, so f is **not** surjective, a contradiction. □

Note: To summarise, we have $|N| = |Z| = |Q|$ since they are countable, but $\mathbb{R}$ is 'bigger'.

Corollary *The sets $\mathbb{R} \setminus \mathbb{Z}$ and $\mathbb{R} \setminus \mathbb{Q}$ are uncountable.*

Proof: Assume to the contrary $\mathbb{R} \setminus \mathbb{Z}$ and $\mathbb{R} \setminus \mathbb{Q}$ are countable. Thus, $(\mathbb{R} \setminus \mathbb{Z}) \cup \mathbb{Z}$ and $(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$ are countable by Lemma 12.9; these unions are $\mathbb{R}$, so we have contradicted Theorem 12.20. □

13 Complex Numbers

Basic Definitions

Definition 13.1 A complex number is an expression of the form $x+yi$, where $x, y \in \mathbb{R}$ and i is a symbol with the property that $i^2 = -1$. The set of complex numbers is denoted $\mathbb{C}$.

A more rigorous definition of $\mathbb{C}$ is given at the end, but the one in Definition 13.1 is what is used most commonly in practice. We can think of $i = \sqrt{-1}$, but it is best to *introduce* it as a sort-of mystery letter with the property $i^2 = -1$. If you jump straight in with $i = \sqrt{-1}$, it is a bit ambiguous because $\sqrt{-1}$ doesn't exist yet; this is why we need i!

Note: The expression of a complex number $x + yi$ is the Cartesian form/representation.

We have the standard operations of arithmetic that carry over from what we know; addition and subtraction are easy. Multiplication is almost easy (just replace any i^2 occurrences with -1) and division is a bit more obscure bit isn't too bad; we can express it using complex multiplication:

$$\frac{x+yi}{a+bi} = \frac{(x+yi)(a-bi)}{(a+bi)(a-bi)} = \frac{(x+yi)(a-bi)}{a^2+b^2}.$$

Definition Let $z = x + yi \in \mathbb{C}$. Then, we define the following:

- The real part is the **real** number $\mathrm{Re}(z) = x \in \mathbb{R}$.
- The imaginary part is the **real** number $\mathrm{Im}(z) = y \in \mathbb{R}$.
- The complex conjugate is the **complex** number $\overline{z} \coloneqq x - yi \in \mathbb{C}$.

Proposition 13.4 *Let $z, w \in \mathbb{C}$. Then, we have the following:*

(i) $\overline{zw} = \overline{z}\,\overline{w}$.
(ii) $\overline{z+w} = \overline{z} + \overline{w}$.
(iii) $\overline{\overline{z}} = z$.

Sketch of Proof: Use a Cartesian form and make sure both sides of each equality agree. □

Definition 13.5 Let $z = x + yi \in \mathbb{C}$. The modulus is the non-negative **real** number

$$|z| \coloneqq \sqrt{x^2+y^2} \in \mathbb{R}.$$

Note: A common error is to write "$|x+yi| = \sqrt{x^2+(yi)^2}$", which is **not** as written above. Please correctly forget about the i and only square the real and imaginary parts as above.

Proposition 13.7 *Let $z, w \in \mathbb{C}$. Then, we have the following:*

(i) $|z|^2 = z\overline{z}$.
(ii) $|\overline{z}| = |z|$.
(iii) $|zw| = |z||w|$.
(iv) $\left|\mathrm{Re}(z)\right| \leq |z|$ *and* $\left|\mathrm{Im}(z)\right| \leq |z|$.
(v) $|z| = 0$ *if and only if* $z = 0$.
(vi) $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$.

Proof: (i) and (ii) These are obvious by calculating with a Cartesian form $z = a + bi$.

(iii) If we square the left-hand side and use (i), we can see that

$$\begin{aligned} |zw|^2 &= zw\overline{zw} \\ &= zw\overline{z}\,\overline{w} \\ &= z\overline{z}w\overline{w} \\ &= |z|^2|w|^2, \end{aligned}$$

where the second equality comes from Proposition 13.4(i) and the third equality comes from the fact multiplication of complex numbers is commutative (it doesn't matter what order we do it in). Taking the square root then gives the result.

(iv) This is clear from $\left|\mathrm{Re}(z)\right|^2 = x^2 \leq x^2 + y^2 = |z|^2$ and $\left|\mathrm{Im}(z)\right|^2 = y^2 \leq x^2 + y^2 = |z|^2$.

(v) If $z = 0$, clearly $|z| = 0$. Conversely, if $|z| = 0$, this means $x^2 + y^2 = 0$. But each summand is non-negative, so the only way we get zero is if they are both zero, that is $z = x + yi = 0 + 0i = 0$.

(vi) This is also a consequence of part (i), because

$$\frac{1}{z} = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{|z|^2}.$$

□

Argand Diagrams, Polar and Exponential Forms

Definition An Argand diagram is a plot representing a complex number in the plane.

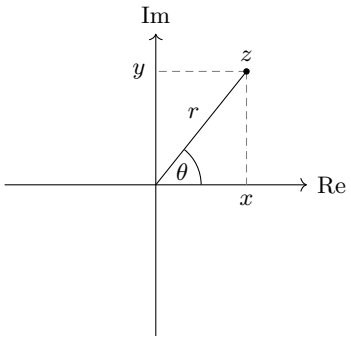

Figure 3: An Argand diagram representing the complex number $z = x + yi \in \mathbb{C}$.

For each $z \neq 0$, we can measure the angle θ between the positive x-axis (labelled Re) and the ray from z through the origin. By taking anti-clockwise as positive, we can make the following important definition (note that we do not even define the angle in the case that $z = 0$).

Definition The principal value of the argument $\mathrm{Arg}(z)$ of $z \in \mathbb{Z}$ is the angle θ such that

$$-\pi < \theta \leq \pi.$$

From the diagram in Figure 3, it is clear that the length $r = |z|$ is the modulus of the complex number. Moreover, the principal value $\theta = \mathrm{Arg}(z)$ satisfies the following by basic trigonometry:

$$x = r\cos(\theta) \qquad \text{and} \qquad y = r\sin(\theta).$$

Note: Substituting the above into $z = x + yi = r(\cos\theta + i\sin\theta)$ gives the polar form of z.

Lemma *For any $z \in \mathbb{C}$ and r as in* Figure 3*, it is indeed true that $r = |z|$.*

Proof: By direct calculation, $|z| = \sqrt{x^2 + y^2} = \sqrt{(r\cos\theta)^2 + (r\sin\theta)^2} = \sqrt{r^2} = r$, as $r \geq 0$. □

The way we obtain θ from the Cartesian form $z = x + yi$ is more subtle. However, we do have

$$\frac{y}{x} = \frac{r\sin(\theta)}{r\cos(\theta)} = \tan(\theta).$$

Because tan is a periodic function, namely $\tan(\theta + n\pi) = \tan(\theta)$ for all $n \in \mathbb{Z}$, it is not injective. Therefore, we cannot define an inverse. One way to get around this is to restrict its domain to the interval $(-\pi/2, \pi/2)$; we now have a bijection and thus an inverse exists.

Definition The arctangent function is the inverse of tan restricted to $(-\pi/2, \pi/2)$, that is

$$\arctan = \left(\tan|_{(-\pi/2,\pi/2)}\right)^{-1}.$$

Lemma *Let $z = x + yi \in \mathbb{C}$. Then, the principal argument is given by*

$$\mathrm{Arg}(z) = \begin{cases} \arctan\big(y/x\big), & \text{if } x > 0 \\ \arctan\big(y/x\big) + \pi, & \text{if } x < 0 \text{ and } y \geq 0 \\ \arctan\big(y/x\big) - \pi, & \text{if } x < 0 \text{ and } y < 0 \\ \pi/2, & \text{if } x = 0 \text{ and } y > 0 \\ -\pi/2, & \text{if } x = 0 \text{ and } y < 0 \\ \textit{undefined}, & \text{if } x = 0 \text{ and } y = 0 \end{cases}.$$

Note: It is convenient to extend the notion of a principal argument to *an* argument: we define an argument $\arg(z)$ (not necessarily principal) of $z = x + yi$ as **any** $\theta \in \mathbb{R}$ such that

$$x = r\cos(\theta) \qquad \text{and} \qquad y = r\sin(\theta).$$

The next definition is important but not rigorous (you must wait until MATH1026/MATH2017).

Definition For any $\theta \in \mathbb{R}$, Euler's formula says that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

Lemma 13.12 *For all $\alpha, \beta \in \mathbb{R}$, we have $e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}$.*

Proof: Starting from the right-hand side, we see that

$$\begin{aligned} e^{i\alpha}e^{i\beta} &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= \cos(\alpha)\cos(\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta) + i^2\sin(\alpha)\sin(\beta) \\ &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\ &= e^{i(\alpha+\beta)}, \end{aligned}$$

where the third equality comes from some compound angle formulae. □

Definition For any $z = x + yi \in \mathbb{C}$, the exponential is $e^z = e^x e^{iy} = e^x(\cos y + i\sin y)$.

Remark 13.13 The best way to define the exponential of a complex number $z \in \mathbb{C}$ is to use the so-called *Taylor series* of the real-valued exponential function $f(x) = e^x$. Indeed, we can write

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

for any $x \in \mathbb{R}$. If we replace x with a complex variable z, then the above still makes sense:

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

Note: The problem is that we do not know if the infinite sum above actually produces a complex number. This is what is discussed in the modules MATH1026 and MATH2017.

Definition Let $z = r(\cos\theta + i\sin\theta) \in \mathbb{C}$. The exponential form of z is

$$z = re^{i\theta}.$$

Because both cos and sin are 2π-periodic, it follows that $re^{i(\theta+2n\pi)} = re^{i\theta}$ for all $n \in \mathbb{Z}$.

Note: Complex multiplication is easy in exponential form. For $z = re^{i\theta}$ and $w = se^{i\phi}$,

$$zw = re^{i\theta}se^{i\phi} = rse^{i(\theta+\phi)}.$$

Corollary *For any $z, w \in \mathbb{C}$, we have* $\arg(zw) = \arg(z) + \arg(w)$.

Proof: This is immediate from the above note; it **fails** for the principal argument Arg though! □

Proposition 13.15 (de Moivre's Theorem) *For all $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, we have*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

Proof: We proceed with a proof by induction where $n \in \mathbb{N}$ (one can similarly work with $-n \in \mathbb{N}$ to extend the proof to all $n \in \mathbb{Z}$). For the initial case ($n = 1$), it is trivial since this is just Euler's formula. For the inductive step, assume the formula holds when $n = k$ for **some** $k \in \mathbb{N}$:

$$(\cos\theta + i\sin\theta)^k = \cos(k\theta) + i\sin(k\theta) \qquad \Leftrightarrow \qquad (e^{i\theta})^k = e^{ik\theta}.$$

We wish to use the above to show that the formula is true when $n = k + 1$, that is

$$(e^{i\theta})^{k+1} = e^{i(k+1)\theta}.$$

Indeed, we see that

$$\begin{aligned}(e^{i\theta})^{k+1} &= (e^{i\theta})^k e^{i\theta} \\ &= e^{ik\theta}e^{i\theta}, && \text{by the inductive hypothesis,} \\ &= e^{i(k+1)\theta}, && \text{by Lemma 13.12.}\end{aligned}$$

By the Principle of Mathematical Induction, the formula is true for all $n \in \mathbb{N}$. □

Fundamental Theorem of Algebra

Theorem 13.16 (Fundamental Theorem of Algebra) *Any polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.*

In other words, we can always solve $p(x) = 0$ for any polynomial p with complex coefficients. The proof is omitted, but there is a neat corollary which can be shown by induction yet again.

Reminder: The degree of a polynomial is the largest power with a non-zero coefficient.

Corollary 13.17 *Let p be a degree n polynomial with coefficients in $\mathbb{C}$. Then, p has n roots.*

Roots of Unity

Definition 13.18 Let $n \in \mathbb{Z}$. The n^{th} roots of unity are solutions to $z^n = 1$ for $z \in \mathbb{C}$.

Note: By the Fundamental Theorem of Algebra (Corollary 13.17), $z^n = 1$ is equivalent to finding roots of the polynomial $z^n - 1$. Because this is degree n, we expect n solutions.

Theorem *Let $n \in \mathbb{Z}$. The n^{th} roots of unity are the complex numbers (in exponential form)*

$$e^{2k\pi i/n}, \qquad \text{for } k \in \mathbb{Z} \text{ with } 0 \leq k < n.$$

Proof: Starting more generally, consider the equation $z^n = a$ for any $a \in \mathbb{C}$ is arbitrary. Now,

$$|z^n| = |a| \;\Leftrightarrow\; |z|^n = |a| \qquad \Rightarrow \qquad |z| = \sqrt[n]{|a|}.$$

We can also see that the argument satisfies

$$\arg(z^n) = \arg(a) + 2k\pi \;\Leftrightarrow\; n\arg(z) = \arg(a) + 2k\pi \qquad \Rightarrow \qquad \arg(z) = \frac{\arg(a) + 2k\pi}{n}.$$

Substituting these into the exponential form of a complex number, solutions of this equation are

$$z = \sqrt[n]{|a|}e^{i(\text{Arg}(a)+2k\pi)/n}, \qquad \text{for all } k \in \mathbb{Z}.$$

In the case of roots of unity, we have that $a = 1$. This means that $|a| = 1$ and $\arg(a) = 0$. Because angles differing by integer multiples of 2π are considered the same, we see that we only get distinct values of $\text{Arg}(z)$ if we restrict $0 \leq k < n$. That is, the principal argument satisfies

$$\text{Arg}(z) \in \left\{0, \frac{2\pi}{n}, \frac{4\pi}{n}, ..., \frac{2(n-1)\pi}{n}\right\}.$$

Combining this with the above exponential form gives the result. □

Solutions versus Functions

Note: The square root $\sqrt{\ }$ is a function, i.e. it is **single-valued**. For example, $\sqrt{25} = 5$ and this is the only output. On the other hand, there are **two** solutions of $x^2 = 25$.

If one is to understand the square root of a complex number, there must be care taken not to mix up solutions to equations and outputs of functions.

Definition Let $a \in \mathbb{C}$. The square root of a is a **pair** of solutions to $z^2 = a$.

If we want to discuss a complex square root *function*, we must now be careful. For $z = re^{i\theta} \in \mathbb{C}$

$$\sqrt{z} = \sqrt{r}e^{i\theta/2}, \qquad \text{where } -\pi < \theta \leq \pi.$$

Note: It is straightforward to see that $(\sqrt{z})^2 = z$. Notice that when $\mathrm{Im}(z) = 0$ (which means $z \in \mathbb{R}$), this produces the same square root function we are used to for real numbers.

Remark A major problem with this definition is that the complex square root function is not continuous (see MATH1026 for a rigorous definition of this) along the negative part of the real axis (the so-called *branch locus*). This can be seen in an Argand diagram and is explained by the fact that the square root of a complex number halves its argument. In this way, we refer to the above function as the *principal* square root.

Corollary *For general $z, w \in \mathbb{C}$, we have $\sqrt{zw} \neq \sqrt{z}\sqrt{w}$.*

Complex Numbers without the Fantasy

We offer another definition of complex numbers without arbitrarily introducing the symbol i.

Definition 13.19 The complex number system is the set of ordered pairs $\mathbb{R}\times\mathbb{R}$ $(= \mathbb{R}^2)$ of real numbers with the following addition and multiplication operations for all $(a, b), (c, d) \in \mathbb{R}^2$:

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

A complex number is then an element of this number system.

Proposition *The number system $\mathbb{R}^2$ above is the same as $\mathbb{C}$ introduced in* Definition 13.1.

Sketch of Proof: For any $\alpha \in \mathbb{R}$, let us define $\alpha(x, y) \coloneqq (\alpha x, \alpha y)$. With this, we can write any

$$\mathbb{R}^2 \ni (x, y) = x(1, 0) + y(0, 1).$$

This corresponds to $x + yi \in \mathbb{C}$ by identifying $(1, 0)$ with 1 and $(0, 1)$ with i. To justify this,

$$(0, 1)^2 = (0, 1) \times (0, 1) = (0 - 1, 0 + 0) = (-1, 0) = -(1, 0)$$

via multiplication rule in Definition 13.19; this corresponds to $i^2 = -1$ as expected. □