Notes on Discrete Mathematics

Michael Pham

Spring 2023

Contents

Chapter 0
Introduction

0.1 Introduction

Before proceeding with the rest of the course notes, we will first review the idea of sets and mathematical notation.

0.1.1 Sets

Definition 0.1 (Set)**.** A **set** is a well defined collection of objects; these objects are referred to as elements or members of the set. They aren't restricted to being just numbers; they can be letters, people, cities, and even other sets.

Sets are usually denoted by capital letters, with the elements surrounded by curly brackets. For example, let A denote the set of the first five prime numbers. Then, to express this set, we can write it as the following: $A = \{2, 3, 5, 7, 11\}$. If x is an element of the set A, we can write $x \in A$. If an element y is not contained in the set of A, we can write $y \notin A$.

Two sets A and B are equal to each other if they contain the same element. Note here that the order in which the elements appear in does not matter; i.e. $\{1, 2, 3\} = \{1, 3, 2\} = \dots$

Sometimes, more complicated sets can be defined by using a different notation. An example of this is the set of all rational numbers, $\mathbb{Q}$, which can be written as: $\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$.

Cardinality

Definition 0.2 (Cardinality)**.** The size of a set is referred to as its **cardinality**. If $A = \{2, 3, 5, 7, 11\}$, then its cardinality, denoted as $|A|$, is 5.

It is possible for a set to have a cardinality of 0; this unique set, called the **empty set**, is denoted by the symbol $\emptyset$.

It is also possible for a set to have an infinite number of elements. Examples of such sets includes the set of all integers, prime numbers, etc.

Subsets and Proper Subsets

Definition 0.3 (Subset)**.** If every element in A is also contained in B, then we say that A is a **subset** of B, denoted by $A \subseteq B$.

Definition 0.4 (Proper Subset)**.** A **proper subset** is a set A that is strictly contained in B; in other words, there's at least one element in B that isn't in A.

Example 0.5. For example, if $B = \{2, 3, 5, 7, 11\}$, then if $A = \{2, 3, 5\}$ then it is a proper subset of B. However, if $A = \{2, 3, 5, 7, 11\}$, then it isn't a proper subset. A proper subset is denoted by $A \subset B$.

The following are a few basic properties of subsets:

1. The empty set, denoted by $\{\}$ or $\emptyset$, is a proper subset of any non-empty set A: $\{\} \subset A$.
2. The empty set is a subset of every set B: $\{\} \subseteq B$.
3. Any set C is a subset of itself: $C \subseteq C$.

Intersections and Unions

Definition 0.6 (Intersection)**.** The **intersection** of a set A and B are all the elements that are contained in both A and B. This is denoted by $A \cap B$.

Two sets are considered **disjoint** if $A \cap B = \emptyset$.

Definition 0.7 (Union)**.** The **union** of A and B, denoted by $A \cup B$, are all elements in A, B, or both.

Example 0.8. For example, let $A = \{2n : n \in \mathbb{Z}\}$ and $B = \{2n + 1 : n \in \mathbb{Z}\}$. In English, A is the set of all even numbers, and B is the set of all odd numbers. Then, for these, $A \cap B = \emptyset$ and $A \cup B = \mathbb{Z}^+$.

The following are properties of intersections and unions:

1. $A \cup B = B \cup A$.
2. $A \cup \emptyset = A$.
3. $A \cap B = B \cap A$.
4. $A \cap \emptyset = \emptyset$.

Complements

Definition 0.9 (Complement)**.** The **complement** of a set A, denoted by A^C or A', is the set of elements not contained in A.

Definition 0.10 (Relative Complement)**.** If A and B are two sets, then the **relative complement** of A in B, or the **set difference** between B and A, is the set of elements in B but not in A. This is denoted as $B - A$ or $B \backslash A = \{x \in B : x \notin A\}$.

Example 0.11. For example, if $B = \{2, 3, 5, 7, 11\}$ and $A = \{2, 3, 7\}$, then $B \backslash A = \{5, 11\}$. Another example is for the set of all real numbers $\mathbb{R}$ and rational numbers $\mathbb{Q}$: $\mathbb{R} \backslash \mathbb{Q}$ is the set of all irrational numbers.

The following are important properties of complements:

1. $A \backslash A = \emptyset$.
2. $A \backslash \emptyset = A$.
3. $\emptyset \backslash A = \emptyset$.

Important Sets

The following are common, important sets in mathematics. These sets have their own special symbol to represent them:

1. $\mathbb{N}$ is the set of all natural numbers: $\{0, 1, 2, \ldots\}$.
2. $\mathbb{Z}$ is the set of all integers: $\{-2, -1, 0, 1, \ldots\}$.
3. $\mathbb{Q}$ is the set of all rational numbers: $\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$.
4. $\mathbb{R}$ is the set of all real numbers.
5. $\mathbb{C}$ is the set of all complex numbers. Note that $\mathbb{R} \subseteq \mathbb{C}$.

Products and Power Sets

Definition 0.12 (Cartesian Product)**.** The **Cartesian product** (also called the **cross product**) of two sets A and B, written as $A \times B$, is the set of all pairs whose first component is an element of A, and whose second component is an element of B.

Example 0.13. For example, if $A = \{2, 3, 5\}$ and $B = \{u, v\}$, then:

$$A \times B = \{(2, u), (3, u), (5, u), (2, v), (3, v), (5, v)\}$$

Definition 0.14 (Power Set)**.** The **power set** of a set S, denoted by $\mathscr{P}(S)$, is the set of all subsets of S: $\{T : T \subseteq S\}$. For example, if $S = 2, 3, 5$, then $\mathscr{P}(S) = \{\{\}, \{2\}, \{3\}, \{5\}, \{2, 3\}, \{2, 5\}, \{3, 5\}, \{2, 3, 5\}\}$.

A property of power sets is the following:

Theorem 0.15. Let $|S| = n$, then $|\mathscr{P}(S)| = 2^n$.

Proof. In order to prove the theorem above, we will be using induction.

First, we will consider the base case of $n = 0$. For this, consider the empty set $S = \emptyset$. Clearly, $|S| = n = 0$. Now, $\mathscr{P}(S) = \{\emptyset\}$. From this, it's clear that $|\mathscr{P}(S)| = 1 = 2^0 = 2^n$. Thus, the theorem holds for our base case of $n = 0$.

Now, let us assume that for $|S| = n$, then $|\mathscr{P}(S)| = 2^n$. We want to prove that this holds true for $n + 1$.

To do this, let $|S| = n + 1$. Now, first let us consider the set $S' = S \backslash \{x\}$, where $x \in S$. Then, we see that $|S'| = n$. Following our assumption from above, $|\mathscr{P}(S')| = 2^n$.

Now, the subsets of S contain S', along with S' with x added to it. Now, note that adding x to each of these subsets doesn't change their numbers. Thus, we see that in S there are 2^n subsets consisting of all the subsets of S' along with another 2^n subsets containing all of the subsets of S' with x added to it. Then, we see that $|S| = 2^n + 2^n = 2(2^n) = 2^{n+1}$.

With this, we see that it is indeed true that for $|S| = n + 1$, then $\mathscr{P}(S) = 2^{n+1}$.

Therefore, for $|S| = n$, then $|\mathscr{P}(S)| = 2^n$. ■

0.1.2 Mathematical Notation

Sum and Products

We can represent summation with the following notation:

$$1 + 2 + \ldots + n = \sum_{k=1}^{n} k$$

A more generalised version of this is that for any function f, we can write the sum of $f(m) + f(m+1) + \ldots + f(n)$ can be written as the following:

$$\sum_{k=1}^{n} f(k)$$

Similarly, we can represent the product $f(m)f(m+1)\ldots f(n)$ as the following:

$$\prod_{k=1}^{n} f(k)$$

Universal and Existential Quantifiers

Definition 0.16 (Quantifiers). Two important symbols that are used commonly in maths are:

1. The **universal quantifier**, $\forall$ ("for all").
2. The **existential quantifier**, $\exists$ ("there exists").

Example 0.17. The following are examples of how to use the two symbols:

1. "For all natural numbers n, $n^2 + n + 41$ is prime." This statement can be written as the following: $(\forall n \in \mathbb{N})(n^2 + n + 41$ is prime).
2. "There exists an integer x less than 2 whose square is equal to 4." This statement can be written as the following: $(\exists x \in \mathbb{Z})(x < 2$ and $x^2 = 4)$.

Of course, we can also write statements using both quantifiers:

1. $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(y > x)$.
2. $(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z})(y > x)$.

However, be careful of the order! Notice that the first statement says that, given an integer x, there exists an integer y which is greater than x. On the other hand, the second statement says something completely different: there exists an integer y which is greater than all integer x. In other words, there exists a largest integer.

We see that the first statement is true, but the second isn't.

0.2 Propositional Logic

Before learning to prove mathematical theorems, we have to first learn about the logical forms they may take, and how we can manipulate them to make them easier to prove.

0.2.1 Propositional Logic

Definition 0.18 (Proposition)**.** Our first building block is the idea of a **proposition**, which is a statement that can be either true or false.

Example 0.19. The following are examples of propositions:

1. $\sqrt{3}$ is irrational.
2. $1 + 1 = 5$.
3. Julius Caesar had 10 eggs on his 10^{th} birthday.

However, the following are not propositions:

1. $2 + 2$.
2. $x^2 + x = 5$. [What is x?]
3. John Cena often eats ice-cream. [What is "often?"]
4. Henry VIII was unpopular. [What is "unpopular"?]

When making propositions, we want to avoid using vague, fuzzy terms (made clear by the last two examples).

Connectives

Propositions may also be joined to form more complex statements. For example, let P and Q represent propositions. The simplest way to join these propositions together is through the words "and", "or", and "not".

Definition 0.20 (Connectives)**.** The following are connectives used to help form propositions:

1. **Conjunction**: $P \wedge Q$ ("P and Q").
2. **Disjunction**: $P \vee Q$ ("P or Q").
3. **Negation**: $\neg P$ ("not P").

Statements like these, involving variables, are called *propositional forms*.

An important principle known as the **law of excluded middle** states that, for any proposition P, either P is true or $\neg P$ is true. However, they can't both be true. From this, we can see that $P \wedge \neg P$ is always false (called a "*contradiction*"), and $P \vee \neg P$ is always true (called a "*tautology*"); this is regardless of P's truth value.

Implications

Definition 0.21 (Implication)**.** The most important, and subtle, propositional form is an **implication**:

Implication: $P \implies Q$ ("If P then Q").

Here, P is the *hypothesis* (or *antecedent*), and Q is the *conclusion* (or *consequent*).

An implication $P \implies Q$ is false only when P is true but Q is false.

Example 0.22. The following are examples of implications:

1. If you stand in the rain, then you'll get wet.
2. If you passed the class, you received a certificate.

We see that for the first statement, it's only false if you stood in the rain but didn't get wet. For the second one, a contradiction would occur if you passed the class but didn't receive a certificate.

When it comes to the implication $P \implies Q$, it is always true when P is false, regardless of what Q is. This results in a lot of nonsensical-sounding propositions in English being considered true mathematically. For example, "If 14 is odd then 1+2=18." We wouldn't make this type of statement in everyday life. In the example given, the implication is true because the hypothesis is false (14 is even, not odd); we call this being *vacuously true*.

Also, note that $P \implies Q \equiv \neg P \vee Q$. We can better visualise this fact using a truth table:

P	Q	$P \implies Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Table 1: Truth table showing that $P \implies Q \equiv \neg P \vee Q$.

Furthermore, if both $P \implies Q$ and $Q \implies P$ are true, then we can say
"P if and only if Q." This can be denoted as $P \iff Q$, and only occurs when P and Q have the same truth value.

Definition 0.23 (Contrapositive and Converse)**.** For $P \implies Q$, we can also define its **contrapositive** and **converse**:

1. **Contrapositive**: $\neg Q \implies \neg P$.
2. **Converse**: $Q \implies P$.

Now, note that while the contrapositive always has the same truth value as the implication, this isn't the case for the converse.

In other words, $P \implies Q \equiv \neg Q \implies P$, but $P \implies Q \not\equiv Q \implies P$.

Now, the implication is the most common form mathematical theorems take. The following are various ways of saying it:

1. If P, then Q.
2. Q if P.
3. P only if Q.
4. P is sufficient for Q.
5. Q is necessary for P.
6. Q unless not P.

0.2.2 Quantifiers

Let's return to the examples used in the previous chapter's section on quantifiers:

1. "For all natural numbers n, $n^2 + n + 41$ is prime." This statement can be written as the following: $(\forall n \in \mathbb{N})(n^2 + n + 41$ is prime).
2. "There exists an integer x less than 2 whose square is equal to 4." This statement can be written as the following: $(\exists x \in \mathbb{Z})(x < 2$ and $x^2 = 4)$.

Now, why are these two statements considered propositions, but something like "$x^2 + x = 5$" isn't? The answer is that, in the examples above, we are working in a "universe" in which these statements are quantified over. We can express this mathematically with the universal $(\forall)$ and existential $(\exists)$ quantifiers.

Note that in a finite universe, we can actually express universally and existentially quantified propositions using conjunctions and disjunctions respectively.

For example, let our universe $U = \{1, 2, 3, 4\}$. Then, $(\exists x \in U)P(x)$ is logically equivalent to $P(1) \vee P(2) \vee P(3) \vee P(4)$. Similarly, $(\forall x \in U)P(x)$ is logically equivalent to $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$.

But, in an infinite universe, this isn't possible.

0.2.3 Negation

For a proposition P to be false, it simply means that its negation $\neg P$ is true. Now, it's useful to have rules when working with negations.

De Morgan's Law

One of the first rules we look at is how negation works with conjunction and disjunction:

$$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$$
$$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$$

Negating the universal and existential quantifiers follows the same rules:

$$\neg(\forall x P(x)) \equiv \exists x \neg P(x)$$
$$\neg(\exists x P(x)) \equiv \forall x \neg P(x)$$

Example 0.24. To see a more complex example, fix some universe and propositional formula $P(x, y)$. Assume that we have the proposition $\neg(\forall x \exists y P(x, y))$. Using De Morgan's Law, we see the following:

$$\neg(\forall x \exists y P(x, y)) \equiv \exists x \forall y \neg P(x, y)$$

Example 0.25. Now, for a trickier example, let's write "there exist at least three distinct integers which satisfy $P(x)$" as a proposition using quantifiers:

$$\exists x \exists y \exists z (x \neq y \wedge x \neq z \wedge y \neq z \wedge P(x) \wedge P(y) \wedge P(z))$$

Now, let's write the sentence "there exists **at most** three distinct integers which satisfy $P(x)$":

$$\exists x \exists y \exists z \forall d (P(d) \implies d = x \vee d = y \vee d = z)$$

An equivalent way of writing this is:

$$\forall x \forall y \forall z \forall d ((x \neq y \wedge x \neq z \wedge x \neq d \wedge y \neq z \wedge y \neq d \wedge z \neq d) \implies \neg(P(x) \wedge P(y) \wedge P(z) \wedge P(d)))$$

Now, if we want to write a proposition for the statement "there exists **only** three distinct integers that satisfy P(x)", we just have to take the conjunction of the two statements above.

CHAPTER 1
PROOF WRITING

1.1 Proofs

A proof is defined as a finite sequence of steps, called *logical deductions*, which establishes the truth of a desired statement. The power of proofs is that, using only finite steps, we can verify the truth of a statement which infinitely many cases.

When writing proofs, we first start with axioms and postulates which we accept without proofs. From these, we follow up with logical deductions; these are steps which apply the rules of logic.

This section will begin with notation and basic facts. Then, we shall transition to the different types of proofs as follow:

1. Direct Proof
2. Proof by Contraposition
3. Proof by Contradiction
4. Proof by Cases

1.1.1 Notation and Basic Facts

First, recall the symbols for common sets. For example, $\mathbb{Z}$ (the set of integers) and $\mathbb{N}$ (the set of natural numbers).

The sum or product of two integers is also an integer; in other words, $\mathbb{Z}$ is closed under addition and multiplication. The same applies to $\mathbb{N}$.

Next, given $a, b \in \mathbb{Z}$, we say that a divides b (denoted by $a \mid b$) iff there exists an integer q such that $b = aq$.

Finally, we use $a \coloneqq b$ to indicate a definition. For example, $q \coloneqq 6$ defines variable q as having the value 6.

1.1.2 Direct Proof

The first technique we will be discussing is using direct proofs.

The outline for direct proofs is as follow:

Goal: To prove $P \implies Q$

Approach:

Assume P

$\vdots$

Therefore Q

Let's look at a simple example first with the following theorem:

Theorem 1.1. For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

Proof. To begin with, assume that $a \mid b$ and $a \mid c$ exist. Then, $\exists x \exists y \in \mathbb{Z}$ such that $b = xa$ and $c = ya$. Then, we see that $b + c = xa + ya = a(x + y)$.

Now, as $\mathbb{Z}$ is closed under addition, we see that $(x + y) \in \mathbb{Z}$, and thus $a \mid (b + c)$ is true. ■

The theorem above was rather easy to prove. So, let's try a more difficult example:

Theorem 1.2. Let $0 < n < 1000$ be an integer. If the sum of the digits of n is divisible by 9, then n is divisible by 9.

Proof. To begin with, we can write n as an integer abc; in other words, $n = 100a + 10b + c$.

Now, assume that the sum of the digits of n is divisible by 9. This is the same as saying the following:

$$\exists k \in \mathbb{Z} \text{ such that } a + b + c = 9k$$

From this, we can add $99a + 9b$ to both sides of the equation above, yielding:

$$\begin{aligned} 100a + 10b + c &= n \\ &= 9k + 99a + 9b \\ &= 9(k + 11a + b) \end{aligned}$$

Once again, recall that as $\mathbb{Z}$ is closed under addition, then $(k + 11a + b) \in \mathbb{Z}$. Therefore, we conclude that n is divisible by 9. ■

Next, let us try and prove the converse:

Theorem 1.3. Let $0 < n < 1000$ be an integer. If n is divisible by 9, then the sum of the digits of n is divisible by 9 as well.

Proof. First, let us assume that n is divisible by 9. Then, there exists a k such that $n = 9k$.

Now, recall that $n = 100a + 10b + c$. Then, we get the following:

$$\begin{aligned} 100a + 10b + c &= 9k \\ (a + b + c) + (99a + 9b) &= 9k \\ a + b + c &= 9k - 99a - 9b \\ &= 9(k - 11a - b) \\ &= 9l, \quad \text{for } l = k - 11a - b \in \mathbb{Z} \end{aligned}$$

Therefore, we can conclude that if n is divisible by 9, then the sum of n's digits is divisible by 9 as well. ■

Now, notice that since we have proven both a theorem and its converse, we can thus conclude that n is divisible by 9 iff the sum of its digits is divisible by 9.

This leads us to an important idea: to prove an "if and only if" statement, we prove $P \implies Q$ and $Q \implies P$.

1.1.3 Proof by Contraposition

The next proof technique we will look at is proving by contraposition. Recall that for any implication $P \implies Q$, its contrapositive $\neg Q \implies \neg P$ has the same truth value. Now, sometimes it is easier to prove the contrapositive of an implication than the implication itself.

The outline for proofs by contraposition is as follow:

> *Goal*: To prove $P \implies Q$
>
> *Approach*:
>
> > Assume $\neg Q$
> >
> > $\vdots$
> >
> > Therefore $\neg P$
>
> *Conclusion*: $\neg Q \implies \neg P$, which is equivalent to $P \implies Q$.

Let's look at an example:

Theorem 1.4. Let n be a positive integer, and let d divide n. Then, if n is odd then d is odd.

Proving this using direct proofs seems difficult; we first assume n is odd. But then, what's next?

Thus, let us proceed with proof by contraposition.

Proof. To prove this theorem, we shall proceed with contraposition.

First, we assume that d is even. That is, $d = 2k$, where $k \in \mathbb{Z}$.

Next, as $d \mid n$ then, by definition, there exists an integer l such that $n = dl = 2kl = 2(kl)$.

As $\mathbb{Z}$ is closed under multiplication, we see that $kl \in \mathbb{Z}$ and thus can conclude that n is even. ■

Also, notice here that the first line of our proof states what technique we are using. This is good practice to do!

Now, let us look at a famous theorem and prove it using contraposition:

Theorem 1.5 (Pigeonhole Theorem)**.** Let n and k by positive integers. Place n objects into k boxes. If $n > k$, then at least one box must contain multiple objects.

Proof. We shall proceed by contraposition.

First, assume that all boxes contain at most one object. Then, this means that there must be at most the same number of objects as there are boxes.

Therefore, we can conclude that $n \leq k$. ■

As a quick aside, the Pigeonhole Theorem is incredibly important as it holds regardless of the configuration of the objects in the box. In situations where the objects are placed in the boxes in a complicated way, the conclusions of the theorem can be non-trivial.

An example of how the theorem can be applied is as follow: the number of hairs on the human head is, on average, around $100,000$. In SF, there are around $800,000$ residents. Now, if we imagine the number of hairs on the human head as the "boxes" and the residents of San Francisco as the "objects," we see that, by the Pigeonhole Theorem, there are two people with the exact same number of hairs on their head!

1.1.4 Proof by Contradiction

The next technique we'll explore is proof by contradiction. The idea for this proof is to assume the claim we want to prove is false; from here, we will show that this leads to a conclusion that doesn't make sense at all — it's a contradiction. Thus, we conclude that our claim must be true.

The outline for proofs by contradiction is as follow:

Goal: To prove P

Approach:

Assume $\neg P$

$\vdots$

R

$\vdots$

$\neg R$

Conclusion: $\neg P \implies \neg R \wedge R$, which is a contradiction. Thus, P.

Now, let us look at an example:

Theorem 1.6. There are infinitely many prime numbers.

Looking at this theorem, we see that utilising the other techniques shown thus far would be incredibly complicated. However, by using contradiction, we can assume that there are only a finite number of primes, leading to nonsensical conclusions.

In order to prove this theorem, we will state a simple lemma (a minor, proven proposition which we'll use in our proof):

Lemma 1.7. Every natural number greater than one is either prime or has a prime divisor.

The proof for this lemma will be left as an exercise in a later section. Now, let us proceed with our proof.

Proof. We shall proceed by contradiction.

First, let us assume that there are only k primes, where k is a finite number. Then, we can write the prime numbers as $p_1, \ldots, p_k$.

Now, let q be defined as the product of all the prime numbers plus one: $q \coloneqq p_1 \ldots p_k$.

Since q is greater than all the prime numbers from p_1 to p_k, we can claim that it is not prime. Therefore, by Lemma 2.1, q must have a prime divisor, p.

Next, since $p_1, \ldots, p_k$ are all primes, then we know that p has to be one of these numbers. Define r as the product of all the prime numbers; $r \coloneqq p_1, \ldots, p_k$. Then, p divides r and p divides q as well.

However, notice that since $p \mid r$ and $p \mid q$, this implies that $p \mid (q - r)$. But, $q - r = 1$ which implies that $p \leq 1$. This means that p is not a prime number, and thus leads to a contradiction. ■

Now, let us look at a classic example of proof by contradiction:

Theorem 1.8. $\sqrt{2}$ is irrational.

Before continuing, recall that a rational number can be written as a fraction of two integers; an irrational number cannot. Now, to prove the theorem above, we will introduce a lemma which will be proven later:

Lemma 1.9. If a^2 is even, then a is even.

Proof. We will proceed by contradiction.

First, let us assume that $\sqrt{2}$ is a rational number. Thus, it can be written as: $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and a, b share no common factor other than 1.

Now, for any number x and y, $x = y \implies x^2 = y^2$. Therefore, $2 = \frac{a^2}{b^2}$.

Next, multiply both sides by b^2, yielding us $2b^2 = a^2$. Notice here that since $\mathbb{Z}$ is closed under multiplication, as b is an integer, then so is b^2. Now, from this, we see that since $a^2 = 2b^2$, then a^2 must be an even number by definition of evenness. Then, using Lemma 2.2, we see that a must be an even number as well. Thus, we can rewrite a as the following: $a = 2c$, where $c \in \mathbb{Z}$.

From this, we see that $2b^2 = 4c^2$, and thus $b^2 = 2c^2$. Now, similarly, as c is an integer, so too is c^2 as $\mathbb{Z}$ is closed under multiplication. Therefore, we see that b^2 is even. Thus, by Lemma 2.2, we see that b must be even too.

However, as both a and b are even, they share a common factor of 2. This is a contradiction. Therefore, we can conclude that $\sqrt{2}$ is irrational. ■

1.1.5 Proof by Cases

We'll informally touch on this technique with a simple example. The idea behind proof by cases is as follow: Sometimes when we wish to prove a claim, we don't know which of a set of possible cases is true, but we know that at least one is. What we can thus do is to prove the result in both cases; then, the general statement must hold.

Let us look at an example of this below:

Theorem 1.10. There exists irrational numbers x and y such that x^y is rational.

Proof. We proceed by cases.

Note that since the statement of our theorem is quantified by an existential quantifier, it's suffice to demonstrate a single x and y such that x^y is rational. To do this, let $x = \sqrt{2}$ and $y = \sqrt{2}$. Let us divide our proof into two cases, exactly one of which must be true:

1. $\sqrt{2}^{\sqrt{2}}$ is rational, or
2. $\sqrt{2}^{\sqrt{2}}$ is irrational.

The first case assumes that $\sqrt{2}^{\sqrt{2}}$ is rational. But this immediately yields our claim, as both x and y are irrational, but x^y is rational.

The second case assumes that $\sqrt{2}^{\sqrt{2}}$ is irrational. From this, we see that our guess was incorrect.

From here, let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Now, let us recall the following property of exponents: $(x^y)^z = x^{yz}$. With this, we see that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$. Thus, we once again see that with two irrational numbers x and y, x^y is a rational number.

Since one of our two cases must hold, we thus conclude that there must exist irrational numbers x and y such that x^y is rational. ■

What is interesting about this proof is that, in the end, we don't actually know the values of x and y at all; is $x = \sqrt{2}$ and $y = \sqrt{2}$, or is it that $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$?

This is what's referred to as a **non-constructive** proof: we've proven that some object X exists, but we haven't revealed what that X actually is.

1.2 Exercises

Now, we shall proceed with some exercises to cement our understanding.

Problem 1.1. Generalise the proof of Theorem 2.2 so that it works for any positive integer n.

We want to generalise the proof of Theorem 2.2 such that it works for any positive integer n. Thus, the new theorem now becomes:

Theorem 1.11. Let n be an integer. If the sum of the digits of n is divisible by 9, then n is divisible by 9.

One way to tackle this theorem is to use modulo. However, as this hasn't been covered yet, we will instead avoid that route. Instead, let's try a different approach to proving this theorem.

First, let us introduce a lemma that we'll later use in our proof:

Lemma 1.12. For all integers i, $10^i - 1$ is divisible by 9.

Now, we will proceed with our proof of Theorem 2.11:

Proof. We shall proceed with a direct proof.

Suppose that for an integer n, it has k digits. Thus, we can rewrite n as the following:

$$n = \sum_{i=0}^{k-1}(10^i a_i), \text{ where } a_i \in \mathbb{Z}$$

Now, suppose that the sum of the digits of n is divisible by 9. That means that there exists an integer l such that the following is true:

$$\sum_{i=0}^{k-1} a_i = 9l$$

Next, let us add $\sum_{i=0}^{k-1}(10^i - 1)a_i$ to both sides of the equation above, yielding us the following:

$$\begin{aligned} n &= \sum_{i=0}^{k-1}(10^i a_i) \\ &= \sum_{i=0}^{k-1} a_1 + \sum_{i=0}^{k-1}(10^i - 1)a_i \\ &= 9l + \sum_{i=0}^{k-1}(10^i - 1)a_i \end{aligned}$$

Now, by Lemma 2.3, we see that $10^i - 1$ is divisible by 9, meaning that for any integer b_i, $(10^i - 1) = 9b_i$. As $\mathbb{Z}$ is closed under multiplication, then we see that $b_i a_i \in \mathbb{Z}$. Furthermore, since $\mathbb{Z}$ is closed under addition, $\sum_{i=0}^{k-1} b_i a_i \in \mathbb{Z}$. Thus, we can rewrite n as the following:

$$\begin{aligned} n &= 9l + \sum_{i=0}^{k-1} (10^i - 1)a_i \\ &= 9l + \sum_{i=0}^{k-1} 9b_i a_i \\ &= 9(l + \sum_{i=0}^{k-1} b_i a_i) \\ &= 9m, \text{ where } m = l + \sum_{i=0}^{k-1} b_i a_i \end{aligned}$$

And from this, we see that n is divisible by 9. Thus, we can conclude that for an integer n, if the sum of its digits is divisible by 9, then n is divisible by 9 as well. ■

Problem 1.2. Prove Lemma 1.9. That is, prove that if a^2 is even, then a is even.

Proof. We will proceed by contraposition.

To begin with, let us assume that a is odd. Then, by definition, there exists an integer b such that $a = 2b + 1$.

Then, we see that $a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$. Now, since $b \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under multiplication, we see that b^2 must be an integer as well. Furthermore, as $\mathbb{Z}$ is closed under addition, then it follows that $2b^2 + 2b$ is an integer as well.

Now, let c be an integer such that $c = 2b^2 + 2b$. This yields the following: $a^2 = 2c + 1$. Then, by definition, a^2 must be an odd number as well.

Therefore, we can conclude that if a is odd, then a^2 is odd as well. And, by contraposition, if a^2 is even, then a is even as well. ■

CHAPTER 2

INDUCTION, RECURSION, AND THE WELL-ORDERING PRINCIPLE

2.1 Mathematical Induction

In this section, we will be introducing the technique of mathematical induction. This is a powerful technique used to establish that a statement holds true for all natural numbers $n \in \mathbb{N}$. Of course, there are infinitely many natural numbers, but induction allows us to reason about them by finite means.

2.1.1 Simple Induction

The outline for induction is as follows:

1. **Base Case**: Prove that P is true for some base case(s) n.
2. **Induction Hypothesis**: For arbitrary $k \geq 0$, assume that $P(k)$ is true.
3. **Inductive Step**: With the assumption of our Induction Hypothesis, show that $P(k+1)$ is true.

Now, let's look at an example:

Theorem 2.1. $\forall n \in \mathbb{N}, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Proof. We shall proceed with induction over n.

Base Case: To begin with, let us begin with the base case $n = 0$: $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$. Thus, we see that the theorem above is true for the base case $n = 0$.

Induction Hypothesis: Next, let us introduce our induction hypothesis: let us assume that for any arbitrary $n = k \geq 0$, $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$.

Inductive Step: Now, let us begin our inductive step. Let $n = k + 1$. Then, we want to prove that $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$:

$$\begin{aligned}\sum_{i=0}^{k+1} i &= \sum_{i=0}^{k} i + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k^2+k}{2} + \frac{2k+2}{2} \\ &= \frac{k^2+3k+2}{2} \\ &= \frac{(k+1)(k+2)}{2}\end{aligned}$$

As our induction hypothesis holds for $n = k + 1$ then, by the principle of mathematical induction, we see that the claim follows. Thus, we can conclude that $\forall n \in \mathbb{N}$, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. ■

Let's look at another example:

Theorem 2.2. For all $n \in \mathbb{N}$, $n^3 - n$ is divisible by 3.

Proof. We shall proceed by induction over n.

Base Case: Let us first start with the base case of $n = 0$. We want to show that for $n = 0$, $n^3 - n$ is divisible by 3. In this case, we see that $0^3 - 0 = 0$, and any non-zero integer divides 0. Thus, the theorem holds for the base case $n = 0$.

Induction Hypothesis: Next, let us introduce our induction hypothesis: suppose that for any $n = k \geq 0$, $k^3 - k$ is divisible by 3. In other words, there exists an integer q such that $k^3 - k = 3q$.

Inductive Step: Now, we shall proceed with our inductive step. Let $n = k + 1$. We want to now prove that $(k+1)^3 - (k+1)$ is divisible by 3. First, let's expand out $(k+1)^3 - (k+1)$ as follow:

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^2+2k+1)(k+1) - (k+1) \\ &= (k^3+2k^2+k+k^2+2k+1) - (k+1) \\ &= k^3+3k^2+3k+1-k-1 \\ &= (k^3-k) + (3k^2+3k) \\ &= (k^3-k) + 3(k^2+k)\end{aligned}$$

Now, from here, we notice that by our induction hypothesis, $k^3 - k = 3q$, for some $q \in \mathbb{Z}$. Thus, we get the following:

$$\begin{aligned}(k+1)^3 - (k+1) &= 3q + 3(k^2+k) \\ &= 3(q+k^2+k)\end{aligned}$$

Therefore, we can conclude that $3 \mid ((k+1)^3 - (k+1))$. Thus, by the principle of mathematical induction, we see that $\forall n \in \mathbb{N}$, $3 \mid (n^3 - n)$. ■

Next, we will look at a more advanced example of using induction by examining a simplified version of the famous Four Colour Theorem: the Two Colour Theorem.

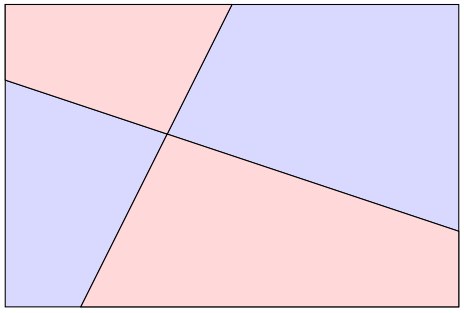

Figure 2.1: Example of a two-colourable map.

Theorem 2.3 (Two Colour Theorem)**.** Let $P(n)$ denote the statement "Any map of the above form with n lines is two-colourable". Then, it holds that $\forall n \in \mathbb{N}$, $P(n)$.

Proof. We shall proceed by induction.

Base Case: First, let us begin with the base case where $n = 0$. In this case, since we have $n = 0$ lines, then the map can be coloured using a single colour. Thus, $P(0)$ holds true.

Induction Hypothesis: Next, we shall introduce our induction hypothesis: suppose that for $n = k \geq 0$, assume that $P(k)$ is true.

Inductive Step: Now, we begin our inductive step: we want to prove that for a map with $k+1$ lines, the map is two-colourable.

Given a map with $k+1$ lines, let us first remove a line. Now, we have a map with k lines and, by our induction hypothesis, it is two-colourable.

Now, observe that for a valid map colouring, swapping the colours will result in a still-valid colouring. With this observation in mind, let us add back the line we removed earlier. Now, on one side, we keep the colours the same; however, on the other side, we shall swap the colours. We claim that this is a valid two-colouring of the map with k+1 lines. Thus, we claim that $\forall n \in \mathbb{N}$, $P(n)$. ■

2.1.2 Strengthening the Induction Hypothesis

When using induction, it's important to choose the correct statement to prove. We will see this importance in the following example:

Suppose we want to prove that, for all $n \geq 1$, the sum of the first n odd numbers is a perfect square.

Let's attempt to prove this with induction:

Proof attempt. We shall proceed by induction on n.

Base Case: First, let us prove for the base case of $n = 1$. We see that the first odd number is 1, which is a perfect square.

Induction Hypothesis: Next, let us proceed with our induction hypothesis. Suppose that the sum of the first $k \geq 1$ odd numbers is a perfect square, m^2.

Inductive Step: Now, our inductive step. We want to prove that our induction hypothesis holds for the first $k+1$ odd numbers. The $(k+1)^{th}$ odd number is $2k+1$. Then, by our induction hypothesis, we see that the sum of the first $k+1$ odd numbers is equal to $m^2 + 2k + 1$. ⊠

However, we see that we are now stuck; why is it that $m^2 + 2k + 1$ has to be a perfect square?

Our induction hypothesis is too "weak" and doesn't give enough structure for us to say anything meaningful about the $(k+1)$ case. So, what do we do?

Well, first, let's take a step back to make sure that our claim isn't wrong. To do this, let's check the first few cases:

- $n = 1$: $1 = 1 = 1^2$
- $n = 2$: $1 + 3 = 4 = 2^2$
- $n = 3$: $1 + 3 + 5 = 9 = 3^2$
- $n = 4$: $1 + 3 + 5 + 7 = 16 = 4^2$

Notice here that our claim isn't wrong. However, what is interesting is that the sum of the first n odd numbers isn't just a perfect square; it is actually n^2. With this in mind, let us instead use a stronger claim.

Theorem 2.4. For all $n \geq 1$, the sum of the first n odd numbers is equal to n^2.

Proof. We shall proceed by induction on n,

Base Case: Let us first begin with the base case $n = 1$. The first odd number is 1, which is equal to 1^2.

Induction Hypothesis: Next, we shall introduce our induction hypothesis: assume that the sum of the first $n = k \geq 1$ odd numbers is equal to k^2.

Inductive Step: Now, our inductive step: we want to prove that our induction hypothesis holds for the first $(k+1)$ odd numbers. Notice that the $(k+1)^{th}$ odd number is $2k + 1$. Then, the sum of the first $(k+1)$ odd numbers is equal to $k^2 + (2k + 1) = (k+1)^2$. Thus, by the principle of induction, the theorem holds. ■

Let's look at a second example:

Suppose that we want to prove that for $n \geq 1$, $\sum_{i=1}^{n} \frac{1}{i^2} \leq 2$.

Once again, let's try using induction:

Proof attempt. We shall proceed by induction on n.

Base Case: First, we look at our base case $n = 1$: we see that $\frac{1}{1^2} = 1 \leq 2$.

Induction Hypothesis: Next, our induction hypothesis: let us assume that for $n = k \geq 1$, $\sum_{i=1}^{k} \frac{1}{i^2} \leq 2$.

Inductive Step: Now, for our inductive step, we want to prove that our induction hypothesis holds for the $(k+1)$ case:

$$\sum_{i=1}^{k+1} \frac{1}{i^2} = \sum_{i=1}^{k} \frac{1}{i^2} + \frac{1}{k+1} \leq 2$$

⊠

But, how do we show that the last line is true? What if $\sum_{i=1}^{k} \frac{1}{i^2}$ is actually equal to 2...?

Instead, let us try and strengthen our induction hypothesis.

Theorem 2.5. For all $n \geq 1$, $\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$.

Proof. We shall proceed by induction on n.

Base Case: For the base case of $n = 1$, we see that $\sum_{i=1}^{i} \frac{1}{i^2} = 1 \leq 2 - \frac{1}{1}$. Thus, our base case holds.

Induction Hypothesis: Next, we shall introduce our induction hypothesis: assume that for all $n = k \geq 1$, $\sum_{i=1}^{k} \frac{1}{i^2} \leq 2 - \frac{1}{k}$.

Inductive Step: Now, our inductive step: we want to prove that our induction hypothesis holds for $n = k+1$:

$$\begin{aligned}
\sum_{i=1}^{k+1} \frac{1}{i^2} = \sum_{i=1}^{k} \frac{1}{i^2} + \frac{1}{k+1} &\leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2} \\
-\frac{1}{k} + \frac{1}{(k+1)^2} &\leq -\frac{1}{k+1} \\
-\frac{k+1}{k} + \frac{1}{k+1} &\leq -1 \\
-(k+1)^2 + k &\leq -(k+1)(k) \\
-(k^2 + 2k + 1) + k &\leq -(k^2 + k) \\
k^2 + 3k + 1 &\geq k^2 + k \\
2k + 1 &\geq 1 \\
k &\geq 0
\end{aligned}$$

Now, we see that this is true as $k \geq 1$. Thus, our induction hypothesis holds for the $(k+1)$ case. Therefore, by the principle of induction, our claim holds. ■

2.1.3 Strong Induction

So far, we've looked at what's referred to as *weak* induction. In this subsection, we'll look at what's known as *strong* induction.

So, what is strong induction exactly? Well, it's similar to simple induction. However, instead of just assuming that $P(k)$ is true, we assume that $P(0)$, $P(1), \ldots, P(k)$ is true. In other words, we assume that $\wedge_{i=0}^{k} P(i)$ is true.

There isn't a difference between the power of either inductions; in other words, there aren't scenarios where one type of induction can prove a statement but the other can't. But, choosing the correct type of induction can make proofs become easier.

Now, let us look at an example of using strong induction:

Theorem 2.6. For every natural number $n \geq 12$, it holds that $n = 4x + 5y$ for some $x, y \in \mathbb{N}$.

Proof. We proceed by induction on n.

Base Case: First, we look at the base case of $n = 12$. We see that $12 = 4(3) + 5(0)$. Thus, our claim holds for $n = 12$.

Next, we look at $n = 13$. We observe that $13 = 4(2) + 5(1)$. Thus, we see that $n = 13$ can be expressed as $4x + 5y$ for some $x, y \in \mathbb{N}$.

Now, we look at $n = 14$, observing that $14 = 4(1) + 5(2)$. Thus, our claim holds for $n = 14$.

Finally, we observe that when $n = 15$, $15 = 4(0) + 5(3)$. Therefore, our claim holds for the base case $n = 15$.

Induction Hypothesis: Suppose that for $12 \leq n \leq k$, and for $k \leq 15$, $k = 4x + 5y$ for some $x, y \in \mathbb{N}$.

Inductive Step: Now, we want to show that our induction hypothesis holds for $n = k + 1 \geq 16$. Now, notice here that $(k+1)-4 \geq 12$, and from here we see that our induction hypothesis implies that for some $x', y' \in \mathbb{N}$, $(k + 1) - 4 = 4x' + 5y'$. Therefore, $(k + 1) - 4 = 4x + 5y$ for $x = x' + 1$ and $y = y' + 1$.

Thus, we see that our claim holds for every natural number $n \geq 12$ by the principle of mathematical induction. ■

Next, we will look at a tougher example which involves strong induction:

Theorem 2.7. Every natural number $n > 1$ can be written as a product of one or more primes.

Proof. We shall proceed by induction on n.

Base Case: First, we look at the base case of $n = 2$. We see that since 2 is a prime number, then our claim holds.

Induction Hypothesis: Suppose that our claim holds true for all $2 \leq n \leq k$.

Inductive Step: Now, we want to show that our induction hypothesis holds for $n = k + 1$. At this point, we have two cases:

1. $k + 1$ is a prime number
2. $k + 1$ isn't a prime number.

In the first case, we see that since $k + 1$ is a prime number, then our induction hypothesis holds.

For the second case, if $k + 1$ isn't a prime number then, by definition, $k + 1 = xy$ for some $x, y \in \mathbb{Z}^+$, where $1 < x, y < k+1$. Now, by the induction hypothesis, we see that both x and y can each be written as a product of one or more primes. Then, this means that $xy = k + 1$ can also be written as a product as one or more primes.

Therefore, by mathematical induction, we conclude that our claim holds for every natural number $n > 1$. ■

2.1.4 The Well-Ordering Principle

We will now introduce a concept which is equivalent to induction: the Well-Ordering Principle.

Definition 2.8 (Well-Ordering Principle)**.** If $S \subseteq \mathbb{N}$, and $S \neq \emptyset$, then S must have a smallest element.

We observe that while using induction, our statement of "for all k, $P(k) \implies P(k+1)$" only makes sense if there is a well-defined order imposed upon the natural numbers (that is, 3 comes before 4, 4 before 5, etc.). This particular property will be used later as an alternate proof to a lemma.

Now, while $\mathbb{N}$ follows the Well-Ordering Principle, not all sets do.

Example 2.9. Consider the following sets, and whether they follow the well-ordering principle or not:

- $S_1 = \{n \in \mathbb{N} : n \text{ is prime}\}$; yes, the smallest element is 2.
- $S_2 = \{n \in \mathbb{Z}\}$; no, there is no lower bound.
- $S_3 = \{n \in \mathbb{Z}^+\}$; yes, the smallest element is 1.

Remark 2.10. What is interesting to note is that the Well-Ordering Principle is actually not a theorem, but rather an axiom; it is part of the definition of $\mathbb{N}$.

2.2 Recursion, Programming, and Induction

If it isn't clear already, there's a very strong connection between the idea of recursion in programming and induction. We will be demonstrating this with the following two examples:

Example 2.11 (Fibonacci's Rabbits)**.** Consider the following puzzle: starting with a pair of rabbits, how many rabbits are there after a year, if each month each pair begets a new pair which, from the second month on, becomes productive?

This model of population growth can be modeled by recursively defining a function $F(n)$; the resulting sequence is now referred to as the *Fibonacci numbers*.

Using induction, we can also show that there is a lower bound to the exponential growth of Fibonacci numbers, which will be shown in Problem 2.1.

Now, as a program, it looks as such:

```
def fib(n):
    if n==0 or n==1:
        return n
    else:
        return fib(n-1) + fib(n-2)
```

Now, we can use induction to show that, in order to find $F(n)$, the number of calls to $F(n)$ is at least $F(n)$ itself. This will be demonstrated later as an exercise problem.

Example 2.12 (Binary Search)**.** For this example, we will be using induction to analyse a recursive algorithm: the binary search.

The code is as follow, in pseudocode:

```
findWord(W, D) {
if (D has precisely one page)
    Look for W in D by brute force.
    If found, return its definition; else, return "W not found".
Let W' be the first word on the middle page of D.
if (W comes before W')
    return findWord(first half of D)
else
    return findWord(second half of D)
}
```

Now, we will use induction to show that our function is correct.

Proof. We shall proceed by induction on n, the number of pages in D.

Base Case: If $n = 1$, we observe that the function will find W in D by brute force, returning either the definition or that the word isn't found as desired.

Induction Hypothesis: Assume that the function is correct for all $1 \leq n \leq k$.

Inductive Step: We will show that the function works for $n = k + 1$ as well. Notice that we know the word W must be in either the first or second half of D depending its position compared to W'. In either cases, we will then recurse through at most k pages and thus, by our induction hypothesis, it will either return the definition or that the word isn't found.

Therefore, by the principle of mathematical induction, our function is correct. ■

From these examples, it should be clear how intimate the ideas of recursion and induction are to one another.

2.3 Exercises

Problem 2.1. Use induction to show that $F(n) \geq 2^{(n-1)/2}$ for all $n \geq 3$.

Proof. We shall proceed by induction on n.

Base Case: First, we see that for $n = 3$, $F(3) = 2 \geq 2^{(3-1)/2}$.

Next, for $n = 4$, we observe that $F(4) = F(3) + F(2) = 3 \geq 2^{(4-1)/2} = 2.828$.

Therefore, our claim holds for the base cases of $n = 3$ and $n = 4$.

Induction Hypothesis: For all $3 \leq n \leq k$, $F(k) \geq 2^{(k-1)/2}$.

Inductive Step: Now, we want to show that our claim holds for $n = k + 1$. Observe that $F(k+1) = F(k) + F(k-1)$. Then, we see that by our induction hypothesis, $F(k) \geq 2^{(k-1)/2}$ and $F(k-1) \geq 2^{(k-2)/2}$. Then, we observe the following:

$$\begin{aligned} F(k) + F(k-1) &\geq 2^{(k-1)/2} + 2^{(k-2)/2} \\ &= 2^{k/2}(2^{-1/2} + 2^{-1}) \\ &> 2^{k/2} && \text{(because } 2^{-1/2} + 2 > 1\text{)} \end{aligned}$$

Thus, we see that our claim holds true for $n = k + 1$.

Therefore, by mathematical induction, we can conclude that our claim holds for all $n \geq 3$. ■

Problem 2.2. Using induction, show that to compute $F(n)$ using our function fib(n), we need at least $F(n)$ calls.

Proof. We shall proceed by induction on n.

Base Case: First, we see that for $n = 0$, $F(0) = 0$, and it requires one call.

For $n = 1$, $F(1) = 1$, and also requires one call to compute the value.

For $n = 2$, we see that $F(2) = F(1) + F(0) = 1$ requires two calls to fib(n).

For $n = 3$, we observe that $F(3) = F(2) + F(1) = 2$, which requires three calls to the function.

For $n = 4$, we see that $F(4) = F(3) + F(2) = 3$, which requires 5 calls to the function to compute the result.

Thus, we see that our claim holds for these base cases.

Induction Hypothesis: Now, for all $0 \leq n \leq k$, assume that our claim holds.

Inductive Step: We want to now prove that for $n = k + 1$, we require at least $F(k + 1)$ calls to compute $F(k+1)$. Now, we see that on the first call to fib with $k+1$, the function will then call on fib(k) and fib(k−1). Then, by our inductive hypothesis, each of these calls will take at least $F(k)$ and $F(k - 1)$ calls respectively to calculate the results. Then, we see that we need at least $F(k) + F(k-1)$ calls to compute $F(k+1)$ which, by definition, is $F(k + 1)$ calls. Thus, our claim holds for $n = k + 1$.

Therefore, by the mathematical principle of induction, our claim holds true for all $n \geq 0$, where $n \in \mathbb{N}$. ■

Problem 2.3. Prove that for any natural number $n \geq 1$, $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Proof. We shall proceed by induction on n.

Base Case: First, consider our base case $n = 1$. We see that $1^2 = \frac{1}{6}(1)(1+1)(2(1)+1) = 1$. Thus, our claim holds for the base case of $n = 1$.

Induction Hypothesis: Now, suppose that for $n = k$, where $k \geq 1$, our claim holds true.

Inductive Step: We want to show that our induction hypothesis holds for $n = k + 1$. Observe the following:

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

Now, by our induction hypothesis, we see the following:

$$\begin{aligned}\sum_{i=1}^{k} i^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)(k)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)(2k^2 + k + 6(k+1))}{6} \\ &= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}\end{aligned}$$

Therefore, our induction hypothesis holds for $n = k+1$. Thus, by mathematical induction, we can conclude that our claim holds true for all natural number $n \geq 1$. ■

Problem 2.4 (Bernoulli's Inequality)**.** Prove that $(1+x)^n \geq 1+nx$ if n is a natural number and $1+x > 0$.

Proof. We shall proceed by induction on n.

Base Case: First, we see that for $n = 0$, then $(1+x)^0 = 1 = 1 + (0)x$. Therefore, the claim holds for our base case of $n = 0$.

Induction Hypothesis: Next, suppose that for $n = k$, where $k \geq 0$, $(1+x)^k \geq 1 + kx$ if $k \in \mathbb{N}$ and $1 + x > 0$.

Inductive Step: Now, we want to show that our claim holds for $n = k+1$. Observe that for $k+1$, $(1+x)^{k+1} = (1+x)^k(1+x)$. Then, we observe the following:

$$\begin{aligned}(1+x)^{k+1} &= (1+x)^k(1+x) \\ &\geq (1+kx)(1+x) && \text{(by our induction hypothesis)} \\ &= 1 + kx + x + kx^2 \\ &\geq 1 + kx + x && \text{(as } k, x^2 \geq 0\text{)} \\ &= (1 + (k+1)x)\end{aligned}$$

Thus, we see that for $n = k+1$, $(1+x)^{k+1} \geq 1 + (k+1)x$.

Therefore, by the principle of mathematical induction, we can conclude that our claim holds for all $n \in \mathbb{N}$. ■

Problem 2.5. A common recursively defined function is the *factorial*, defined for a nonnegative number n as $n! = n(n-1)(n-2)\ldots 1$, with base case $0! = 1$. Let us reinforce our understanding of the connection between recursion and induction by proving the following:

$$\forall n \in \mathbb{N}, n > 1 \implies n! < n^n$$

Proof. We shall proceed by induction on n.

Base Case: We first consider the base case of $n = 2$. For $n = 2$, we see that $2! = 2$, and $2^2 = 4$. Therefore, $n! < n^n$ for $n = 2$, and our base case holds.

Induction Hypothesis: Assume that our claim holds true for $n = k$, where $k \geq 2$.

Inductive Step: Now, we want to show that our claim holds true for $n = k+1$. Notice that $(k+1)! = (k+1)k!$. Now, by our induction hypothesis, we know that $(k+1)k! < (k+1)k^k$. From here, observe the following:

$$\begin{aligned}(k+1)^{k+1} &= (k+1)^k(k+1)\\ k^k(k+1) &< (k+1)^k(k+1)\\ (k+1)k! &< k^k(k+1)\\ &< (k+1)^k(k+1)\\ \therefore (k+1)k! &< (k+1)^{k+1}\end{aligned}$$

Since our claim holds for $n = k+1$ as well then, by the principle of mathematical induction, our claim holds for all $n > 1$. ■

Chapter 3
Stable Matching

3.1 The Stable Matching Problem

In the previous two chapters, we examined proof techniques; now, we will look at how we can apply them to an important problem referred to as the *Stable Matching Problem*.

The Stable Matching problem is as follows:

Definition 3.1 (The Stable Matching Problem)**.** Suppose we have an employment system, and we have to match up n jobs and n candidates. In this case, $n = 3$. Below are a list of jobs and candidates, along with a preference list:

Jobs	Candidates
A	$X > Y > Z$
B	$Y > X > Z$
C	$X > Y > Z$

Candidates	Jobs
X	$B > A > C$
Y	$A > B > C$
Z	$A > B > C$

Table 3.1: The preference lists of the jobs and candidates.

Now, how would we match each job to each candidate such that everybody is "happy"? Not any type of matching would suffice. Can we do it efficiently?

Now, it turns out that there exists an algorithm that helps achieve this: the *Propose-and-Reject Algorithm* (referred to as the Gale-Shapley Algorithm), which we will present now.

3.2 The Propose-and-Reject Algorithm

Definition 3.2 (Propose-and-Reject Algorithm)**.** We think of the algorithm as proceeding in "days" to have a clear unambiguous sense of discrete time.

Every Morning: Each job proposes (i.e. makes an offer) to the most preferred candidate on its list who has not yet rejected this job.

Every Afternoon: Each candidate collects all the offers she received in the morning; to the job offer she likes best among these, she responds "maybe" (she now has it *on a string*), and rejects the other offers.

Every Evening: Each rejected job crosses off the candidate who rejected its offer from its list.

The above loop is repeated each successive day until there are no offers rejected. At that point, each candidate has a job offer on a string; and on this day, each candidate accepts their offered job and the algorithm terminates.

Now, to understand this algorithm later, let's look at the example given earlier and see it in action:

Example 3.3. The following table will show how the algorithm plays out, showing which jobs makes an offer to which candidate on the given day:

Days	Candidates	Offers
1	X Y Z	$A > C$ B —
2	X Y Z	A $B > C$ —
3	X Y Z	A B C

Table 3.2: Depiction of the Propose-and-Reject algorithm.

And thus, the algorithm ends after three days with the following pairings: $\{(X, A), (Y, B), (Z, C)\}$

3.2.1 Properties of the Propose-and-Reject Algorithm

There are two properties which we shall show about the algorithm:

1. The Propose-and-Reject algorithm halts.

2. The algorithm outputs a "good" (i.e. stable) matching.

Now, looking at these two properties, we notice that in order to prove the second property, we must first define what a "stable" matching actually entails.

Stability

Definition 3.4 (Rogue Couple)**.** A rogue couple is where a job J and a candidate C both prefer working with each other over their current matching. This is demonstrated in the following diagram:

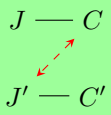

Figure 3.1: Visualisation of a rogue couple.

In the example above, we see that the rogue couple would be the pair (J', C), as they *both* prefer each other. The diagram above is what's referred to as an unstable matching.

So, what exactly is a "stable matching"? Well, it's a matching where there aren't any rogue couples.

What is important to note here is that for it to be a rogue couple, both the job and the candidate have to prefer each other! If C prefers J' but J' prefers C' over C, then it is still a stable matching!

For example, let's go back to our previous example:

Example 3.5. Recall our previous example:

Jobs	Candidates
A	$X > Y > Z$
B	$Y > X > Z$
C	$X > Y > Z$

Candidates	Jobs
X	$B > A > C$
Y	$A > B > C$
Z	$A > B > C$

We found that a stable matching is $\{(X, A), (Y, B), (Z, C)\}$. However, we notice that X prefers job B, so how is this a stable matching?

Well, while X prefers B, B doesn't prefer X over Y. Similarly, although Y would prefer job A over B, job A prefers X over Y. Also, notice here that job C and candidate Z are stuck with each other; it is possible in a stable matching to be stuck with your least preferred option.

Below is a diagram of the scenario which helps to clarify the situation:

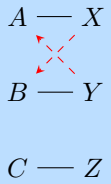

Figure 3.2: A figure explaining stable matching.

Now, before we discuss how to find a stable matching, we first have to ask a more basic question: do stable matchings always exist?

At first, it may seem as though the answer is yes: if a rogue couple exists, we can simply pair them up, right? However, while this does reduce the number of rogue couples by one, it might then also create a new rogue couple. So, it isn't clear whether the algorithm ends or not.

Example 3.6 (Roommates Problem)**.** We will illustrate the fallacy of the reasoning above through this example.

We have $2n$ people who must be paired up to be roommates. The difference between this problem and the Propose-and-Reject algorithm is that the latter has asymmetric partners of a different type, where here a person can be paired up with any of the other $2n-1$ people — there is no asymmetry in type.

Now, using the line of reasoning prior, if there was a rogue couple, we could simply just match them up iteratively until there are no rogue couples. Since this approach doesn't take advantage of the asymmetry, it can be applied to the scenario.

However, this doesn't work. Let's look at the following counterexample:

Roommates			
A	B	C	D
B	C	A	D
C	A	B	D
D	—	—	—

Table 3.3: Illustration of the Roommates Problem.

We claim that in this example, there's a rogue couple for any matching:

- $\{(A,B),(C,D)\}$ would result in a rogue matching, with rogue couple (B,C).
- $\{(B,C),(A,D)\}$ would result in a rogue matching, with rogue couple (A,C).
- $\{(A,C),(B,D)\}$ would result in a rogue matching, with rogue couple (A,B).

And thus, we see that there can never be a stable matching.

From this example, we see that any proof showing that there always exists a stable matching must exploit the asymmetry in types.

3.2.2 Proofs of Properties

We will now prove the first property of the algorithm:

Lemma 3.7. The propose-and-reject algorithm always halts.

Proof. We shall proceed by direct proof.

Observe that for every day that the algorithm doesn't stop, at least one job has to eliminate some candidate from its list (if not then the algorithm's halting condition would activate). Therefore, as there are n elements in n lists, that means that it takes at most n^2 days for the algorithm to terminate. ■

Next, we will prove the second property. First, let us make an observation:

Observation 3.8. Each job begins the algorithm with its first choice as a possibility. However, as time progresses, its best available option gets worse. Meanwhile, the candidate's offers can only get better over time.

From this, we see intuitively that at some point the jobs and candidates must "meet" in the middle, which is where a stable match occurs.

Now, let us formalise this and prove it as well:

Lemma 3.9 (Improvement Lemma)**.** If job J makes an offer to a candidate C on the k^{th} day, then on every subsequent day C has an offer on a string which they like as much as job J.

Proof. We shall proceed by induction on n.

Base Case: First, we consider the case of $k = i$. On the i^{th} day, if C receives at least one offer, one of which is by J, then at the end of the day they will have either an offer from J or from a job J' which they like more.

Induction Hypothesis: We suppose that for some $i \geq k$, our claim holds true.

Inductive Step: We will now prove our claim for $k = i + 1$. We observe that, by the induction hypothesis, on day i, C would have had an offer from a job J' which they like at least as much as the offer from job J. Now, on the $(i + 1)^{th}$ day, J' gives C an offer again; at the end of the day, C will have either J' on a string, or another offer from a job which they like more than J'.

In both cases, we observe that the job C has on a string is one they like at least as much J. Therefore, we see that our claim holds for $k = i + 1$.

Thus, by the principle of mathematical induction, our claim holds for all $k \in \mathbb{N}$. ■

Now, we will show an alternate proof for the Improvement Lemma, using the Well-Ordering Principle:

Proof (using Well-Ordering Principle). As with the original proof, we observe that the claim holds for day $k = i$. Now, suppose, for contradiction, that the i^{th} day, where $i > k$, is the first counterexample where C has either no offer on a string or an offer from a job J^* they like less than J.

Now, on day $i = 1$, C had an offer from some job J' which they liked at least as much as J. According to the algorithm, on day i, J' will make an offer to C again; then, C has the choice of at least one job J'. As such, C's best choice has to be at least as good as J', and it would definitely be better than having no offer or an offer from J^*. Thus, we observe a contradiction.

Therefore, we see that the Improvement Lemma holds true. ■

We see that in the alternate proof using the Well-Ordering Principle, when we assume that there's a first counterexample on the i^{th} day; this notion of a first counterexample wouldn't be valid if $\mathbb{N}$ didn't have a well-defined order.

Chapter 4
Graph Theory

4.1 Introduction

One of the core ideas of computer science is abstraction; that is, representing a complex situation with a simple model. Examples includes the brain, the Internet, maps, etc.

And in all of these cases, there is an underlying "network" — "graphs" — that helps us understand these entities more deeply.

The origin of graph theory stems back to Königsberg, Prussia. Through their city ran the Pregel river, the city into two banks A and C and islands B and D. Connecting the islands to the mainland were seven bridges. The residents tried to figure out a path which would allow them to cross each of the seven bridges exactly once. Below is a representation of this problem using a graph:

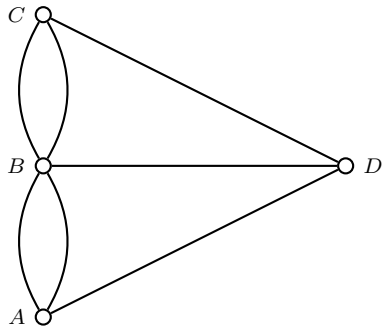

Figure 4.1: The (multi-)graph modeling of the bridge connections in Königsberg.

Euler managed to prove that there was no solution; it was impossible. The key thing to this problem is that the problem is essentially: from a starting point, we have to trace through all the line segments without traversing through a line segment more than once.

Under these tracing rules, we see that the pen must enter each small circle as many times as it exists them; but since there are an odd number of line segments connected to each circle, we see that this is impossible to do!

4.2 Formal Definitions

Definition 4.1 (Undirected Graph)**.** An undirected graph is defined by a set of vertices V and set of edges E. A graph is considered directed if each edge goes in both direction; i.e. $(u, v) \in E \iff (v, u) \in E$, then the graph is undirected.

Looking at Figure 4.1, we observe that the vertices corresponds to each of the small circles, while the edges corresponds to the line segment between each vertices.

Remark 4.2. Note that in Figure 4.1,

- $V = \{A, B, C, D\}$
- $E = \{\{A, B\}, \{A, B\}, \{A, D\}, \{B, D\}, \{B, C\}, \{B, C\}, \{C, D\}\}$

We see that E is a multiset (which is a set in which an element can appear more than once); however, generally we will be not considering such a situation where there are multiple edges between a single pair of vertices.

So, in our definition, we require E to be a set. If there are multiple edges, they'll be collapsed into one single edge. Thus, between any pair of verticies, there can only be 0 or 1 edge.

More generally, we can also define a directed graph. One way to think about the difference between the two is that while the edges in undirected graphs don't have direction, the ones in directed graphs do. More formally, we can define it as such:

Definition 4.3 (Directed Graph)**.** Let V be a set denoting the vertices of a graph G. Then, the set of directed edges E is a subset of $V \times V$; i.e. $E \subseteq V \times V$.

Example 4.4. Let $V = \{1, 2, 3, 4\}$, and $E = \{(1, 2), (1, 3), (1, 4)\}$. Below is the corresponding graphs for the directed graph G_1 and an undirected graph G_2:

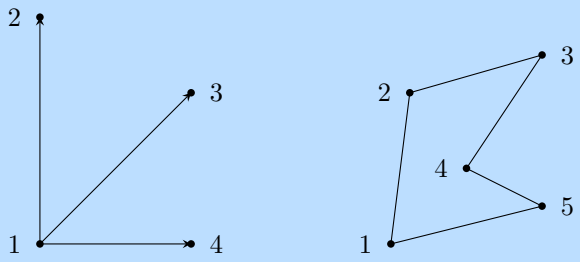

Figure 4.2: Examples of directed graph G_1 and undirected graph G_2, respectively.

Note that each edge in G_1 has a direction specified by an arrow; in other words, $(1, 2) \in E$, but $(2, 1) \notin E$.

On the other hand, in G_2, since each edge goes in both directions, we see that $(u, v) \in E$ and $(v, u) \in E$. For undirected graphs, we drop the ordered pair notation, instead denoting the edge between u and v by the set $\{u, v\}$. For simplicity, we omit the arrowheads for undirected graphs.

From this, we conclude that a graph is formally specified as an ordered pair $G = (V, E)$, where V is the vertex set and E is the edge set.

Moving on from this example, we will now introduce a few more definitions.

Definition 4.5 (Incident Edges)**.** We say that edge $e = \{u, v\}$ is incident on vertices u and v.

Definition 4.6 (Adjacent Vertices)**.** For edge $e = \{u, v\}$, we say that vertices u and v are neighbours, also referred to as being adjacent.

Definition 4.7 (Degree)**.** We have two different definitions of degree depending on whether the graph is directed or undirected:

- If G is an undirected graph, the degree of a vertex $u \in V$ is the number of edges incident to u. In other words, $d(u) = \{v \in V : u, v \in E\}$. A vertex u with a degree of 0 is referred to as an isolated vertex.
- If G is a directed graph, there are two different types of degrees a vertex can have; the in-degree is the number of edges from other vertices to u, and the out-degree which is the number of edges from u to other vertices.

Remark 4.8. Notice here that our definition of a graph allows for a self-loop; that is, we can have edges in the form of $\{u, u\}$ or (u, u). However, as this doesn't give us any useful information, in general we shall assume that graphs don't have any self-loops (unless stated otherwise).

4.2.1 Paths, Walks, and Cycles

In order to understand proofs discussing graphs, we must understand all the terms which they use.

Now, we will define a couple more things that will be essential to our understanding of graph theory, and they are especially crucial to understanding a lot of later theorems that will be discussed.

Definition 4.9 (Path)**.** Let $G = (V, E)$ be an undirected graph. Then, we define a path in G as a sequence of edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-2}, v_{n-1}\}, \{v_{n-1}, v_n\}$. In this case, we can say that there is a path between v_1 and v_n.

Remark 4.10. In the class, we assume that a path is simple, meaning that $v_1 \ldots v_n$ are distinct. Later on in our example, this notion will make more sense.

Definition 4.11 (Cycle)**.** A cycle is defined as a sequence of edges $\{v_1, v_2\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_1\}$, where $v_1, \ldots, v_n$ are all distinct. A cycle is essentially a path that starts and end with the same vertex.

Definition 4.12 (Walk)**.** A walk is a sequence of possibly repeated vertices.

Definition 4.13 (Tour)**.** The relationship of a walk and a tour is analogous to a path and a cycle; a tour is simply a walk that starts and end with the same vertex.

Example 4.14. The following example will help visualise understand each of our definitions:

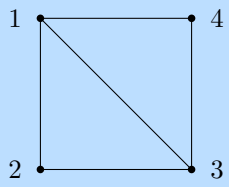

Figure 4.3: Undirected graph G_3, where each vertex corresponds to a house.

- We observe that there exists multiple paths from house 1 to house 3 in G_3; we can either go through 2, 4, or directly to 3 from house 1.
- A possible cycle in G_3, starting from house 1, would be the sequence: $\{1,2\},\{2,3\},\{3,1\}$.
- Now, imagine instead that we wanted to go on a leisurely stroll from house 1 to house 3, taking the path $\{1,2\},\{2,1\},\{1,3\}$. This would be a walk.
- An example of a tour would be $\{1,2\},\{2,1\},\{1,3\},\{3,1\}$. Furthermore, note that a tour could also be a cycle. For example, the sequence of edges $\{1,2\},\{2,3\},\{3,1\}$ would also be considered a tour.

Remark 4.15. In the example above, we see that the notion of paths being simple makes complete sense; if we wanted to go from house 1 to house 3 via house 2, there isn't a need to visit house 2 twice.

As a short summary, below is a table detailing the differences between each of the definitions:

	no repeated vertices	no repeated edges	start = end
Walk			
Path	✓	✓	
Tour			✓
Cycle	✓*	✓	✓

Table 4.1: Table explaining main differences between a walk/path/tour/cycle

Remark 4.16. *Note here that we are excluding the start and end vertices.

4.2.2 Connectivity

Much of what we discuss in this chapter revolves around the idea of connectivity.

Definition 4.17 (Connectivity)**.** A graph is said to be connected if there is a path between any two distinct vertices. Looking at G_3 in Figure 4.3, we see that the graph is connected as we can drive from one house to another via some sequence of edges.

Example 4.18. Below, we will show examples of connected and unconnected graphs.

First, recall the graphs G_1, G_2, and G_3 from previous examples. These are examples of connected graphs:

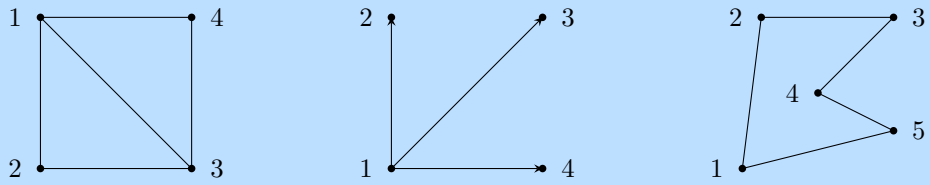

Figure 4.4: Examples of connected graphs.

Meanwhile, below is an example of what is considered an unconnected graph:

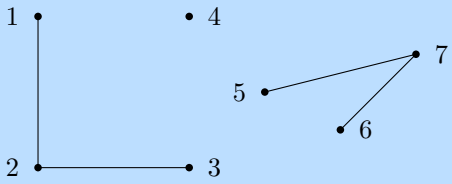

Figure 4.5: Example of an unconnected graph.

Note here that for any graph, even disconnected ones, they always consist of a collection of some connected components; i.e. sets $V_1, \ldots, V_k$ of vertices, such that all vertices in a set V_i are connected. For example, in Figure 4.5, while the graph is unconnected, we observe that it consists of three connected components:

- $V_1 = \{1, 2, 3\}$
- $V_2 = \{4\}$
- $V_3 = \{5, 6, 7\}$

4.3 Eulerian Tours

Now, we shall revisit the problem that helped kickstart graph theory — let us revisit the Seven Bridges of Königsberg.

Before figuring out what the problem is asking exactly, we have to first introduce two more terms:

Definition 4.19 (Eulerian Walk)**.** Any such walk in a graph which only visits each edge once is referred to as an "Eulerian walk"

Definition 4.20 (Eulerian Tour)**.** Moreover, if an Eulerian walk is closed, then it ends at the starting point — this is called an Eulerian tour

Thus, going back to the problem, we see that it's asking if there exists an Eulerian tour for a given graph G. We now give a precise characterisation of this in terms of simpler properties of G. For this, we define an even degree graph as a graph where all of its vertices have an even degree.

Theorem 4.21 (Euler's Theorem (1736))**.** An undirected graph $G = (V, E)$ has an Eulerian tour if and only if G is even degree, and connected (except possibly for isolated vertices).

Proof. In order to prove this theorem, we have to prove it for both directions. To begin with, we will prove the "only if" direction.

Only if. We shall proceed by direct proof.

Let us assume that G has an Eulerian tour.

We will first show that the graph is connected. As G has an Eulerian tour, this means that every vertex which has an edge adjacent to it must lie on the tour, and it must be connected to every other vertices that lies on the tour. Therefore, we see that the graph is connected.

Next, we will show that the graph is even degree. Notice that every time the tour enters a vertex, it has to leave the vertex via a different edge. Therefore, each vertex has two edges adjacent to it which can be paired up.

However, for the starting vertex as the edge leaving it can't be paired up, this doesn't work for the starting vertex. But, notice that by the definition of an Eulerian tour, the tour ends at the start vertex; therefore, we can pair up the first edge with the last edge entering the it. As such, we see that all the edges adjacent to a vertex can be paired up with each other, we see that each vertex has an even degree.

Therefore, we can conclude that if G has an Eulerian tour then G is even degree and is connected. ■

Next, we will prove the other direction; that is, we will prove that if a graph G is even degree and is connected, then it will have an Eulerian tour.

If. We shall proceed by induction on n, where n is the number of vertices a graph G has.

Base Case: First, for $n = 2$, we observe that our graph has 2 vertices. As the graph is even degree, it means that there must be two edges connecting the two vertices. Therefore, it has an Eulerian tour.

Induction Hypothesis: Now, for every graph with $2 \leq n \leq k$ vertices, we suppose that our claim holds true; that is, it will have an Eulerian tour.

Inductive Hypothesis: We will now prove that our induction hypothesis holds for $n = k + 1$. First, let us pick an arbitrary vertex v to start from in our graph G. Then, continue walking around the graph until we return to v. Notice here that since each vertex has an even degree, then we will never get stuck; since when we enter a vertex, we can always leave it.

Now, let's call the result of this tour T. We now remove T from our graph G, leaving us with an even degree graph, G'. We see here that G' is even degree as when we remove T, each vertex can only drop by 0 or 2 degrees. Note here that G' may or may not be connected.

Since each of the connected components of this new graph G' is even degree, so by our induction hypothesis, we observe that each of the connected components must have a Eulerian tour.

Let us now denote each of the connected components of G' as G'_i. Notice now that each component of G' has at least one vertex in common with T. From this, we can create a Eulerian tour for G by splicing together G'_i and T. We do this by first starting on any vertex of T, let's call this v_0. If v_0 is a vertex of some component G'_i, then we traverse the Eulerian tour of G'_i until we return to v_0. We then continue traversing along T until we hit another vertex of some other component of G'_j. We repeat this process until we return to v_0 of T.

Thus, we have created an Eulerian tour as desired for $n = k + 1$. Therefore, by mathematical induction, our claim holds true. ■

As we have proved both directions, we can thus conclude that the theorem holds true. ■

4.4 Planarity, Euler's Formula, and Colouring

4.4.1 Introduction to Trees

Before proceeding with the rest of this section, we will first discuss the idea of "trees" in graph theory.

Definition 4.22 (Tree)**.** A graph is a tree if it is connected and acyclic (meaning, it contains no cycles).

There are other equivalent definitions as well:

- A tree is a graph where the number of vertices is one more than the number of edges.
- A tree is a graph where if you remove any edge, it becomes disconnected.

Example 4.23. Below, we provide an example of a tree graph, with key components labelled.

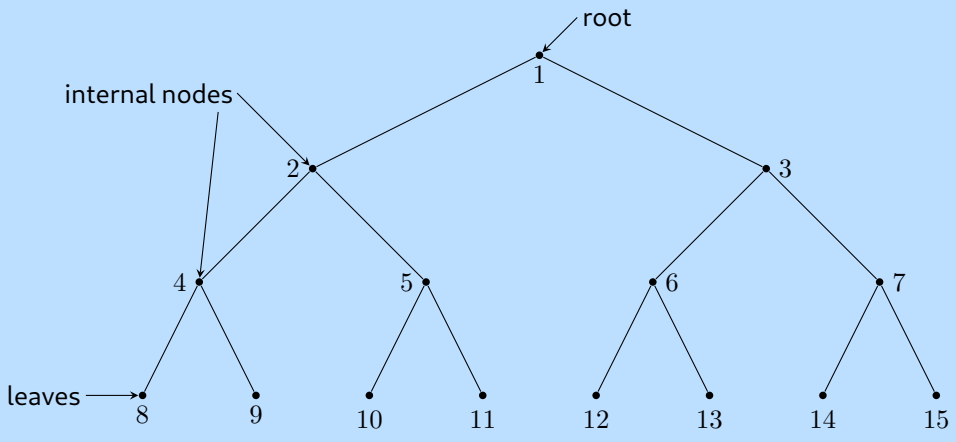

Figure 4.6: A diagram of a (rooted) tree.

If we have done computer science, we'll know that trees are ubiquitous in the field, serving as a good way to visualise problems. For example, we see it appear in tree recursion.

Later on in this chapter, we will revisit the concept of trees and discuss it further.

4.4.2 Planar Graphs

Definition 4.24 (Planar Graphs)**.** A graph is planar if it can be drawn on the plane without crossings.

What is important to note about planar graphs here is that, if there is a way to draw a graph without any crossings, if we then move the line so that there will be a crossing, it doesn't make the graph become non-planar.

We will introduce a few examples below in order to help visualise the idea of (non-)planar graphs better.

Example 4.25. Below are examples of planar and non-planar graphs:

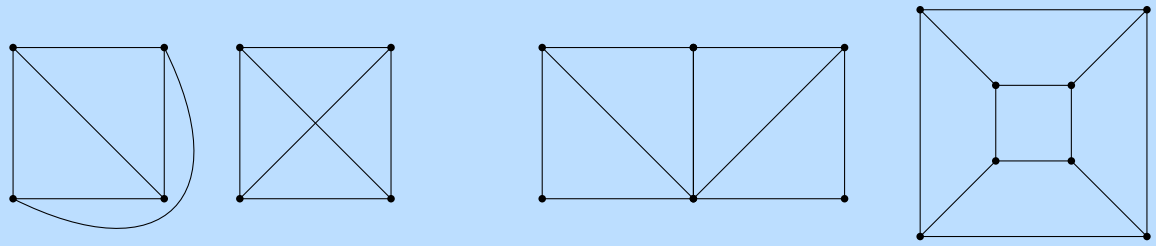

Figure 4.7: Example of various planar graphs.

We see that even though the second graph has crossings, as we can draw it without crossing, it is still considered planar.

Below are examples of non-planar graphs:

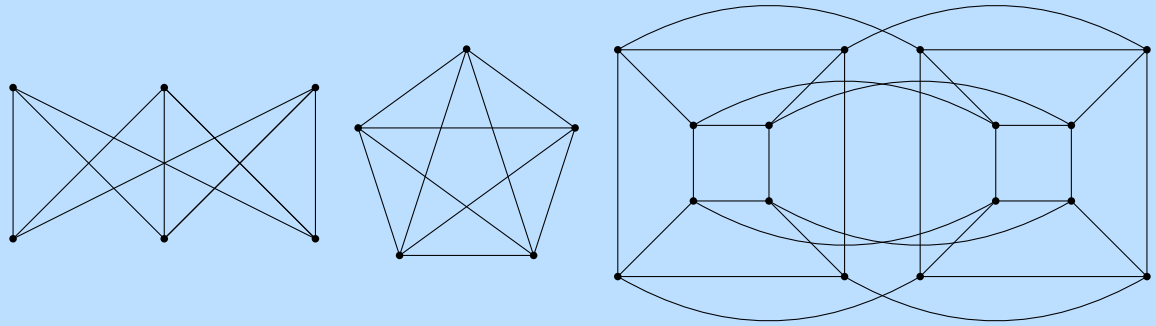

Figure 4.8: Example of various non-planar graphs.

We see that the three graphs above are non-planar.

1. The first one is actually the infamous "three house-three wells graph," also called $K_{3,3}$. The notation tells us that there are two sets of vertices, each of size three and all edges between the two sets of vertices are present.
2. The second graph is the "complete" graph with five nodes, or K_5.
3. The third graph is a four-dimensional cube.

Definition 4.26 (Bipartite Graphs)**.** A useful concept is the notion of a bipartite graph, $G = (V, E)$, which is a graph where the vertices are split into two groups and edges only go between groups.

More formally, we have $V = L \cup R$, and $E \subseteq L \times R$.

From Example 4.25, we see that both $K_{3,3}$ and the hypercube are both bipartite. The latter follows from the fact that every cycle in the cube has an even length; this equivalence will be shown later in this chapter.

Now, when a planar graph is drawn on the plane, other than the number of vertices v and edges e, we can distinguish between them by the number of faces f that they have. The faces are the regions into which the graph subdivides the plane. For example, we see that the first graph has 4 faces, while the third graph has

6.

Now, we will introduce a key formula in regards to planar graphs:

Theorem 4.27 (Euler's formula)**.** For every connected planar graph, $v + f = e + 2$

Proof. We shall proceed by induction on e, the number of edges of our planar graph G.

Base Case: We see that for $e = 0$, G has only one vertex and one face. Thus, $v + f = 2$, and we see that our claim holds for our base case.

Induction Hypothesis: Suppose that for $e - 1$ edges, our claim holds true.

Inductive Step: Now, we want to prove that our induction hypothesis holds for a graph with e. First, we have two cases:

1. G does not contain a cycle. Then, our planar graph is a tree. In this case then, by definition, we observe that the graph has 1 face, and $e = v - 1$. Then, we see the following:

$$\begin{aligned} v + f &= e + 2 \\ v + 1 &= (v - 1) + 2 \\ &= v + 1 \end{aligned}$$

   Thus, we see that our claim holds true in this case.

2. If our graph does contain a cycle, which we will denote as C, then we observe that by removing an edge e' from C, we will reduce the number of faces by 1. Let us call the new graph created by this action G'.

   We now observe that since G' has $e - 1$ edges, we can apply our induction hypothesis. That is, $v + (f - 1) = (e - 1) + 2$. Then, from this, we observe that $v + f = e + 2$.

Thus, by mathematical induction, we can conclude that our claim is true. ■

Now, what happens if the graph isn't connected? How do the number of connected components enter the formula?

Take a planar graph with f faces, and consider one face. It has a number of sides — that is, edges that bound it clockwise. Note that an edge may be counted twice, if it has the same face on both sides (such as in trees).

Now, denote the number of sides of face i by s_i. If we add the s_i's together, we will get $2e$, as each edge is counted twice: once for the face on its right, and once for the face on its left (they may coincide if the edge is a bridge). This observation yields us the following:

Theorem 4.28. For any planar graph, we have

$$\sum_{i=1}^{f} s_i = 2e$$

Now, notice that as we don't allow for parallel edges between the same two nodes and if we assume that there are at least two edges (meaning, there are at least three vertices), then every face has at least three sides. In other words, $s_i \geq 3$ for all i. Then, it follows that $3f \leq 2e$. Using Euler's formula, we observe the following:

$$e \leq 3v - 6$$

What this inequality tells us is that planar graphs are sparse; they can't have too many edges.

Example 4.29. For example, consider a 1000-vertex connected graph. We see that it can have anywhere from 1000 to 500000 edges. Meanwhile, we see that for planar graphs, the range is small: between 999 and 2994.

Now, the inequality also tells us that K_5 is not a planar graph; it has 10 edges, but only 5 vertices; $10 \not\leq 9$.

Now, observe that for $K_{3,3}$, it has 9 edges and 6 vertices; $9 \leq 12$, so it is planar, right? Well, we have to think a bit harder about this graph. Below, we have $K_{3,3}$ with each node labeled clockwise.

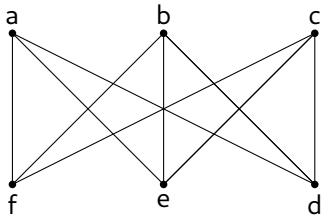

Figure 4.9: $K_{3,3}$ with its nodes labeled.

Now, let us first remove the three vertical edges: $\{(a, f), (b, e), (c, d)\}$. We shall call this graph K'.

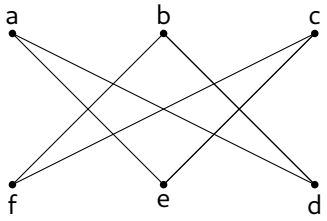

Figure 4.10: A depiction of K', which is $K_{3,3}$ with some edges removed.

From here, we see that K' is a six-vertex planar graph, depicted below, with two of the removed edges added back in using red:

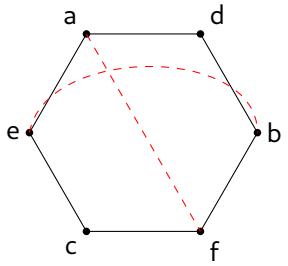

Figure 4.11: A depiction of K' redrawn as a planar graph, along with two edges added back in.

From here, we see that it is impossible for us to have the removed edges be added back in without intersection. As such, we can conclude that $K_{3,3}$ must be non-planar.

Now, from this, we uncover an interesting theorem:

Theorem 4.30. A graph is non-planar if and only if it contains K_5 or $K_{3,3}$.

Of course, one of the direction is very straightforward to prove: we observe that if a graph G contains K_5 or $K_{3,3}$, then as these graphs are non-planar, G must be non-planar as well.

The other direction, however, is harder to prove... and will be left as an exercise for the future.

4.5 Duality and Colouring

Definition 4.31 (Duality)**.** Take a planar graph G, and assume that it has no bridges and no degree-two nodes. Now, draw a new graph $G*$ via the following steps:

1. Start by placing a node on each face of G.
2. Draw an edge between two faces if they touch at an edge — draw the new edge so that it crosses that edge.

Now, the result is a planar graph $G*$. What is interesting is that the dual of $G*$ (that is, $(G*)*$) is the original graph, G.

The idea of duality is a convenient way to look at planar graphs. It also tells us that "colouring a political map so that no two countries sharing a border have the same colour" is the same problem as "colouring the vertices of a planar graph (the dual of a political map) so that no two adjacent vertices have the same colour."

4.5.1 Bipartite Graphs and Colouring

We will briefly talk about bipartite graphs in the context of colouring. Observe that a two-colourable graph is equivalent to a bipartite graph as the colouring splits the vertices into two sets, where the edges only connect vertices in the two colours.

From this observation, we can see that a graph that doesn't have any odd length cycle is bipartite as we can colour any such graph using two colours. This is accomplished by doing the following:

- Colour a vertex x red. Then, colour its neighbour blue. We continue by colouring the next uncoloured neighbour red, then blue, and keep on alternating colours like this.
- Now, if this doesn't work then it means that there must be an edge connecting two vertices of the same colour. Let us denote this edge as (u, v). Then, we can identify an odd cycle by using the path p_1 from x to u and p_2 from v to x. We remove the common portions of p_1 and p_2. Notice that the length of the two paths have the same parity (they're either both even, or both odd) as u and v have the same colour. Then, the total length of the cycle must thus be odd as we include the extra edge (u, v).

4.5.2 The Five Colour Theorem

One of the most famous theorems is the four colour theorem. For this subsection, we will prove a weaker version of it:

Theorem 4.32 (Five Colour Theorem)**.** Every planar graph can be coloured with five colours.

Proof. We shall proceed by induction on v, where v is the vertices of a planar graph G.

Before we start with our induction proof, we first observe that for any valid colouring of a graph, we can swap the colours for each pair of vertices ■

Chapter 5
Modular Arithmetic

5.1 Modular Arithmetic

An intuitive way of thinking about modular arithmetic is about our clock system. Say we are using a 24-hour clock system, and we're at 23:00. If we add 8 hours, we'd get $(23 + 8 =)$ 31:00.

However, this isn't the correct time as we are on a 24-hour system. Instead, it "wraps" around 00:00, and becomes $(31 - 24 =)$ 7:00.

In modular arithmetic, we perform arithmetic operations relative to a fixed n called the modulus. For our 24-hour clock system, $n = 24$. In the example given, we can rewrite it as:

$$31 \pmod{24} = 7$$

The function "$\pmod{24}$" returns the remainder we get when dividing by 24.

5.1.1 Addition, Subtraction, Multiplication

One of the properties of numbers modulo n is the arithmetic operations we are familiar with. First, we will start out with addition.

Say we want to find $42 + 35 \pmod{24}$. We have two ways of doing so:

1. $42 + 35 \pmod{24} = 77 \pmod{24} = 5$
2. $42 + 35 \pmod{24} = [42 \pmod{24}] + [35 \pmod{24}] \pmod{24} = 18 + 11 \pmod{24} = 29 \pmod{24} = 5$

Regardless of the sequence in which we perform arithmetic operations $\pmod{24}$, we will still get the same result; we can reduce $\pmod{24}$ only once at the end, or reduce each or even just some intermediate result $\pmod{24}$ (as long as we reduce the final answer $\pmod{24}$. To see why this is, we have to view numbers modulo n in a different way.

For two integers a and b, we say a is congruent to b modulo n iff $a \pmod{n} = b \pmod{n}$. We write this as:

$$a \equiv_n b \iff n|(a - b)$$

In other words, a and b have the same remainder when we divide them by n. From this, we see that using a or b in arithmetic operations will yield the same result.

Also, note that $p|q$ means p divides q; in other words, $\frac{q}{p}$ returns an integer. Equivalently, we can say that for $k \in \mathbb{Z}$:

$$a = b + kn$$

So, for $n = 24$ we see all of these numbers are congruent to each other:

$$\ldots \equiv_{24} -24 \equiv_{24} 0 \equiv_{24} 24 \equiv_{24} \ldots$$
$$\ldots \equiv_{24} -23 \equiv_{24} 1 \equiv_{24} 25 \equiv_{24} \ldots$$

And there are 24 such disjoint sets where all of the numbers in each set are congruent to one another.

In general, if we work modulo n, then we get n disjoint sets such that the union of these sets forms the set of all integers: these are often called *residue classes mod n*.

There are n residue classes, which are represented by a number $i \in \{0, \ldots, n-1\}$. And the elements in a set represented by the residue i are simply $m = i + kn$, where $k \in \mathbb{Z}$.

Now, we will introduce the following theorem:

Theorem 5.1. For all $n \geq 1$ and $a, b, c, d \in \mathbb{Z}$, the following are true:

1. If $a \equiv_n b$ and $c \equiv_n d$, then $a + c \equiv_n b + d$
2. If $a \equiv_n b$ and $c \equiv_n d$, then $a \cdot c \equiv_n b \cdot d$

Proof. We will proceed to prove the theorem above. Recall that since $a \equiv_n b$, then that means that there's a $k \in \mathbb{Z}$ such that $a = b + kn$. Similarly, $c = d + \ell n$ for $\ell \in \mathbb{Z}$.

Now, we will begin with the first part of the theorem:

$$\begin{aligned} a + c &= (b + kn) + (d + \ell n) \\ &= (b + d) + (kn + \ell n) \\ &= (b + d) + (k + \ell)n \end{aligned}$$

And notice here that since k and ℓ are both integers, then $k\ell$ is also an integer. Thus, we can rewrite the equation as the following:

$$a + c = (b + d) + mn, \quad m \in \mathbb{Z}$$

From this, we can see that $a + c \equiv_n b + d$; we have proven the first part of the theorem. Now, for the second part of the theorem:

$$\begin{aligned} a \cdot c &= (b + kn)(d + \ell n) \\ &= bd + \ell bn + kdn + k\ell n^2 \\ &= bd + (\ell b + kd + k\ell n)n \end{aligned}$$

Similarly, we see here that since $b, d, k, \ell \in \mathbb{Z}$, then $(\ell b + kd + k\ell n) \in \mathbb{Z}$. As such, we can rewrite the equation as:

$$a \cdot c = bd + mn, \quad m \in \mathbb{Z}$$

From this, we can see that $a \cdot c \equiv_n b \cdot d$, and thus the second part of the theorem has been proven; and, with both parts proven, we've proven the theorem. ■

5.1.2 Exponentiation

Another standard operation in arithmetic algorithms is raising a number to a power modulo another number; in other words, how can we compute $x^y \pmod{m}$, where $x, y, m \in \mathbb{N}$, and $m > 0$?

For small numbers of x, y, it may seem redundant

5.1.3 Division and Multiplicative Inverse

In Section 1.1, we discuss addition/subtraction/multiplication in the setting of modular arithmetic. However, division is a little bit more tricky to work with, hence why this subsection will be dedicated to it alone.

First, we will look at division done over rational numbers $\mathbb{Q}$. Here, if we want to divide $x \in \mathbb{Q}$ by $y \in \mathbb{Q}$