Numbers and Sets

Cambridge University Mathematical Tripos: Part IA

17th May 2024

Contents

1 Proofs

1.1 Motivation for proof

Definition (Proof)**.** A proof is a logical argument that establishes a conclusion.

Clearly there are some things missing from this definition; we have not yet defined a 'logical argument' or a 'conclusion'; however we have to start somewhere, and assuming understanding of logic is a good place to start. There is a 3rd year course called 'Logic and Set Theory' that rigorously defines this.

There are two main reasons to want to prove things.

(i) To be sure that they are true; and

(ii) to understand why they are true.

For the first point, it is easy to make a contrived example that shows why we need to prove statements even though they appear to be true for small n, for example: 'all positive integers n are not equal to 100 trillion'. Understanding the reasoning behind why a statement is true is also very important; an example of this is at the end of this lecture.

1.2 Proofs and non-proofs

Claim. For any positive integer n, $n^3 - n$ is a multiple of 3.

Proof. Given some positive integer n, we have

$$n^3 - n = (n-1)n(n+1)$$

One of $n-1$, n, $n+1$ must be a multiple of 3 as they are 3 consecutive integers.

Therefore, $(n-1)n(n+1)$ must be a multiple of 3. □

There are a couple of things to note about this proof.

- The phrase 'given a positive integer' is important; we need to know where this variable n came from.
- We used the fact that three consecutive numbers contain a multiple of 3 here, but this was not proven. We must prove this fact elsewhere, or we cannot use it in this course!
- It is important to write proofs legibly and linearly down the page; don't just write a long line of symbols.

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

Proof. Given a positive integer n that is even, we have $n = 2k$ for some integer k.

Thus $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$,

so n^2 is even. □

Note. This is a false proof. We proved that $B \implies A$, but we want $A \implies B$. Our result wasn't false, but it didn't show what we set out to prove. The words 'for some integer k' are important: we must specify which set k belongs to. Our proof would be incorrect if we did not state this, as it would be unclear that $2(2k^2)$ is an even number.

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

Proof. Given a positive integer n that is a multiple of 9, we have $n = 9k$ for some integer k.

Therefore, $n^2 = (9k)^2 = 81k^2 = 9(9k^2)$,

so n^2 is a multiple of 9. □

Note. Not only does this fall for the same trap as the previous proof, but the original claim is false (e.g. $n = 6$)! It's entirely irrelevant that the claim is true for some positive integers, because even one counterexample disproves the claim.

Let's return now to the previous incorrect example: 'if n^2 even then n even for all positive integers n'.

Proof. Suppose that n is odd.

We have $n = 2k + 1$ for some integer k.

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

n^2 is odd #

Therefore n is even. □

- We prove things to show *why* something is true. We can see why this claim was true here—it's really a statement about the properties of odd numbers, not the properties of even numbers.
- We started by saying that we need something tangible to work with: just stating that 'n^2 is even' is really hard to work with because square roots just get messy and don't yield any result. So we had to choose a clever first step.
- The symbol # shows that we have a contradiction.

This was a kind of proof by contradiction. Essentially, $A \implies B$ is the same as saying $\neg B \implies \neg A$. This is because:

- $A \implies B$ means that there is no case such that A is false and B is true.
- $\neg B \implies \neg A$ means that there is no case such that $\neg B$ is false and $\neg A$ is true. In other words, there is no case such that B is true and A is false. This is equivalent to the case with $A \implies B$.

Claim. The solution to the real equation $x^2 - 5x + 6 = 0$ is $x = 2$ or $x = 3$.

Note. This is really two assertions:

(i) $x = 2 \vee x = 3 \implies x^2 - 5x + 6 = 0$, and

(ii) $x^2 - 5x + 6 = 0 \implies x = 2 \vee x = 3$

We can denote this using a two-way implication symbol $\iff$:

$$x = 2 \vee x = 3 \iff x^2 - 5x + 6 = 0$$

Proof. We prove case i by expressing the left hand side as a product of factors: $(x-3)(x-2) = 0$. The other case may be proven using factorisation. □

We can do another kind of proof using $\iff$ symbols a lot. However, we need to be absolutely sure that each step really is a bi-implication.

Alternative Proof. For any real x:

$$\begin{aligned} x^2 - 5x + 6 = 0 &\iff (x-2)(x-3) = 0 \\ &\iff x - 2 = 0 \vee x - 3 = 0 \\ &\iff x = 2 \vee x = 3 \end{aligned}$$

□

Claim. Every positive real is at least 1.

Proof. Let x be the smallest positive real. We want to prove $x = 1$, so we prove this by contradiction.

Case 1: if $x < 1$ then $x^2 < x$ #

Case 2: if $x > 1$ then $\sqrt{x} < x$ #

Therefore $x = 1$ □

Note. The assertion that there exists a smallest positive real is not justified. This means that the proof is invalid in its entirety. It is important that every line in a proof must be justified.

2 Elementary number theory

2.1 The natural numbers

Each line in a proof must be justified. So, in number theory, what are you allowed to assume? We must begin with a set of axioms. We define that the natural numbers are a set denoted $\mathbb{N}$, that contains an element denoted 1, with an operation $+1$ satisfying:

(i) $\forall n \in \mathbb{N}, n + 1 \neq 1$

(ii) $\forall m, n \in \mathbb{N}, m \neq n \implies m + 1 \neq n + 1$ (together with the previous rule, this captures the idea that all numbers in $\mathbb{N}$ are distinct)

(iii) For any property $p(n)$, if $p(1)$ is true and $p(n) \implies p(n+1)\ \forall n \in \mathbb{N}$, then $p(n)\ \forall n \in \mathbb{N}$ (induction axiom).

This list of rules is known as the Peano axioms. Note that we did not include 0 in this set. You can show that the list of natural numbers is complete and has no extras (like the rational number 3.5) by specifying $p(n) =$ 'n is on the list of natural numbers'.

Note that while numbers are defined as, for example, $1+1+1+1$, we are free to use whatever names we like, e.g. 4 or 3735928559.

We may also define our own operations, such as $+2$, which is defined to be $+1+1$. In fact, we can define the operation $+k$ for any $k \in \mathbb{N}$ by stating:

$$(n+k)+1 = n+(k+1) \quad (\forall n, k \in \mathbb{N})$$

and using induction to construct the $+k$ operator for all k. We can similarly construct multiplication and exponentiation operators for all natural numbers, although this is omitted here. We can also prove properties on these operators such as associativity, commutativity and distributivity.

We can also define the $<$ operator as follows: $a < b \iff \exists k \in \mathbb{N}$ s.t. $a + k = b$. Of course, we can also prove several properties using this rule, such as transitivity, and the fact that $a \not< a$, which are omitted here.

2.2 Strong induction

The induction axiom states that if we know

- $p(1)$ is true, and
- $p(n) \implies p(n+1)$ for any $n \in \mathbb{N}$

then we can conclude that $p(n)$ is true for all $n \in \mathbb{N}$. We can in fact prove a stronger statement using this axiom, known as 'strong induction'.

Claim. If we know that
- $p(1)$ is true, and
- the fact that $p(k)$ is true for all $k < n$ implies that $p(n)$ is true

then $p(n)$ is true for all $n \in \mathbb{N}$.

Proof. Consider the predicate $q(n)$ defined as: '$p(k)$ is true for all $k < n$'. Given that $p(1)$ is true, $q(1)$ is trivially true since there are no k below 1. Since $q(n) \implies q(n+1)$, we can use the induction axiom, showing that $q(n)$ is true for all n, so $p(n)$ is true for all n. □

This provides a very useful alternative way of looking at induction. Instead of just considering a process from n to $n+1$, we can inject an inductive viewpoint into any proof. When proving something on the natural numbers, we can always assume that the hypothesis is true for smaller n than what we are currently using. This allows us to write very powerful proofs because in the general case we are allowed to refer back to other smaller cases—but not just $n-1$, any k less than n.

We may rewrite the principle of strong induction in the following ways:

(i) If $p(n)$ is false for some n, there must be some m where $p(m)$ is false and $p(k)$ is true for all $k < m$. In other words, if a counterexample exists, there must exist a minimal counterexample.

(ii) If $p(n)$ is true for some n, then there is a smallest n where $p(n)$. In other words, if an example exists, there must exist a minimal example. This is known as the 'well-ordering principle'.

2.3 The integers and rationals

The integers $\mathbb{Z}$ consist of the set of natural numbers $\mathbb{N}$, their additive inverses, and an identity element denoted 0. In other words, $(\mathbb{Z}, +)$ is the group generated by $\mathbb{N}$ and the addition operator: $\mathbb{Z} = \langle \mathbb{N} \rangle$. We define operations in a familiar way, for example $a < b \iff \exists c \in \mathbb{N}$ s.t. $a + c = b$.

The rational numbers $\mathbb{Q}$ consist of all expressions denoted $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$; with $\frac{a}{b}$ regarded as the same as $\frac{c}{d}$ if and only if $ad = bc$. We define, for example,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Note that is important to verify with each operation that it does not matter how you write a given rational number. For example, $\frac{1}{2} + \frac{1}{2} = \frac{2}{4} + \frac{3}{6}$. This means that operations such as $\frac{a}{b} \mapsto \frac{a^3}{b^2}$ cannot exist because then it would depend on how you write the rational number.

2.4 Primes

Proposition. Every $n \geq 2$ is expressible as a product of primes.

Proof. We use induction on an integer n, starting at 2, a trivial case. Given $n > 2$, we have two cases:

- n is prime. Therefore, n is a product of primes as required.
- n is composite. We know that n can be split into two factors, denoted here as a, b. Using (strong) induction, we know that because both a and b are smaller than n, they are expressible as a product of primes. We simply multiply these products together to express n as a product of primes.

□

Proposition. There are infinitely many primes.

Proof. Assume there exists a largest prime. Then, the list of primes is $p_1, p_2 \cdots p_k$. Let $n = p_1 p_2 \cdots p_k + 1$. Then n has no prime factor. This is a contradiction immediately because we know that every number greater than two has a factorisation, but this doesn't. □

We want to prove that prime factorisation is unique (up to the ordering). We need that $p \mid ab \implies p \mid a \vee p \mid b$. However, this is hard to answer—p is defined in terms of what divides it, not what it divides. This is the reverse of its definition, so we need to prove it in a more round-about way.

2.5 Highest common factors

For $a, b \in \mathbb{N}$, a number $c \in \mathbb{N}$ is defined to be the highest common factor if:

- $c \mid a$ and $c \mid b$, and
- For all other factors d ($d \mid a$ and $d \mid b$), we have that $d \mid c$.

The second point implies that it is the *highest* common factor, but it is actually slightly stronger. Note that, for example, if a pair's common factors were 1, 2, 3, 4, 6 then the numbers would not have a highest common factor, because 4 does not divide 6.

2.6 The division algorithm

The division algorithm allows us to write any number $n \in \mathbb{N}$ as a multiple $q \in \mathbb{N}$ of $k \in \mathbb{N}$ with some remainder $r \in \mathbb{N}$ such that $0 \leq r < k$; this can be shortened to $n = qk + r$. We begin by writing 1 in this form: $1 = 0k + 1$. Inductively, n can be written as:

$$n = (n-1) + 1 = q_0 k + r_0 + 1$$

where q_0 and r_0 are the results of q and r for $n - 1$. Note that we have two cases:

- If $r_0 + 1 < k$: the result is simply $n = q_0 k + (r_0 + 1)$
- Else ($r_0 + 1 = k$): the result is $n = (q_0 + 1)k + 0$

2.7 Euclid's algorithm

We can find the highest common factor of two natural numbers a and b (without loss of generality, we assume that $a \leq b$). This process is known as Euclid's algorithm.

- Write a as some multiple q_1 of b, with remainder r_1.
- Write b as some multiple q_2 of r_1, with remainder r_2.
- Write r_1 as some multiple q_3 of r_2, with remainder r_3.
- Continue until $r_{n+1} = 0$. Then, r_n is the highest common factor of a and b. We know that the algorithm terminates because $r_k < r_{k-1}$ so it will terminate in at most b steps.

We now prove that the algorithm works.

Proof. We need to prove that it is a common factor and then that it divides all other common factors.

- On the last line of the algorithm, we have $r_{n-1} = q_{n+1} r_n + 0$, so we know that $r_n \mid r_{n-1}$. On the second last line, we have $r_{n-2} = q_n r_{n-1} + r_n$, but r_n divides r_{n-1}, so r_n must divide r_{n-2}. We can continue this logic up to the start of the algorithm, where we can see that $r_n \mid a$ and $r_n \mid b$. So r_n is a common factor of a and b.
- Given some other common factor $d \neq r_n$, we can look at the first line of the algorithm to see that $d \mid r_1$. Using this, we can use the next line to see that $d \mid r_2$. Continuing to the last line, we have $d \mid r_n$.

So r_n is the highest common factor of a and b. Therefore, the highest common factor exists and is unique for any natural numbers a and b. □

Consider running Euclid's algorithm on the numbers 87 and 52.

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

1 is the highest common factor of 87 and 52. Now, we can write 1 as a linear combination of 87 and 52 by looking at each line of this algorithm in the reverse direction (ignoring the bottom line).

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

Each two lines of this equation represents one line on Euclid's algorithm. We end up with a linear combination of the two input numbers. We can prove that this linear combination exists in the general case.

Theorem. Let $a, b \in \mathbb{N}$. Then there exist some $x, y \in \mathbb{Z}$ such that $xa + yb = \text{HCF}(a, b)$.

Proof. Run Euclid's algorithm on a and b, and let the output be r_n. Then we have $r_n = xr_{n-1} + yr_{n-2}$ for some $x, y \in \mathbb{Z}$. So, r_n can be written as a linear combination of r_{n-1} and r_{n-2}. Also, from the previous line we know that $r_{n-1} = xr_{n-2} + yr_{n-3}$ for some other x and y. So we can rewrite r_n as a linear combination of r_{n-2} and r_{n-3}. Inductively, we can rewrite r_n as a linear combination of a and b by moving up the lines of the algorithm. □

We can also make an alternate proof without using Euclid's algorithm. Note that this algorithm does not show how to generate this linear combination, it just shows that one exists.

Alternate Proof. Let h be the least positive linear combination of a and b. We want to prove that $h = \text{HCF}(a, b)$.

- Assume that there exists some common factor d of a and b, so that $d \mid a$ and $d \mid b$. Then for some x and y, $d \mid (xa + yb)$. So $d \mid h$.
- Suppose h does not divide a. Then $a = qh + r$ where q is the quotient and r is the remainder ($r \neq 0$). Then $r = a - qh = a - q(xa + yb)$ for some integers x and y. So r is a linear combination of a and b. But this is a contradiction because we said that h was the smallest one. So h divides a.

Therefore h is the highest common factor. □

2.8 Linear Diophantine equations

Suppose a, b and c are natural numbers. When can we solve $ax+by = c$ for $x, y \in \mathbb{Z}$? Well, by looking at the previous theorem, we might guess that c must be some multiple of the highest common factor of a and b. This can be proven in the general case.

Corollary (Bézout's Theorem)**.** Let $a, b, c \in \mathbb{N}$. Then $ax + by = c$ where $x, y \in \mathbb{Z}$ has a solution if and only if $\text{HCF}(a, b) \mid c$.

Proof. Let $h = \text{HCF}(a, b)$. We must prove this bi-implication in both directions.

- First, let us assume that $ax + by = c$ has a solution for some integers x and y. Since $h \mid a$ and $h \mid b$ then $h \mid (ax + by)$ so $h \mid c$.
- Conversely, we know that $h = ax+by$ for some x and y by the above theorem. We can multiply both sides by the integer c/h (this is an integer because $h \mid c$). Then we have an expression for c as a linear combination of a and b as required.

□

2.9 The fundamental theorem of arithmetic

Lemma. Let p be a prime, let $a, b \in \mathbb{N}$. Then $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proof. Let $p \mid ab$. Then we have two cases, either p divides a or it does not divide a. If it does, our statement is trivially true. Otherwise, we want to prove that p divides b.

Now $\text{HCF}(p, a) = 1$ as p is a prime, and it does not divide a. So 1 can be written as some linear combination of p and a: $px + ay = 1$ for some $x, y \in \mathbb{Z}$.

Now we can multiply both sides by b, giving $pbx + aby = b$. Since p divides ab, p must divide the left hand side. So p divides b. □

Note that we started with a kind of 'negative' statement: 'p does not divide a'; this told us that we cannot do something (namely, factorise it). We turned it into a 'positive' statement: '$px+ay = 1$'; this allows us to rearrange to find out information about these variables. Converting 'negative' statements to 'positive' statements is a useful tool in making proofs.

Theorem (the fundamental theorem of arithmetic)**.** Every $n \in \mathbb{N}$ is uniquely expressible as a product of primes.

Proof. Note that we have already proven that a prime factorisation is possible in Section 3.4; we just need to prove uniqueness of a factorisation (at least, down to its order). We will use induction on some integer n that we wish to factorise. Clearly the theorem is true for $n = 1$ (assuming empty products are valid) and $n = 2$.

So given that $n > 2$ we suppose that there exist two possible factorisations:

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

We want to prove that $k = l$ and that (after reordering) $p_i = q_i$ for all valid i.

We know that $p_1 \mid n$, so $p_1 \mid (q_1 \cdots q_l)$. So there must exist some i where $p_1 \mid q_i$. But since q_i is prime, $p_1 = q_i$. Let us reorder the list such that q_i is moved to the front, so that $p_1 = q_1$.

$$n = p_1 p_2 \cdots p_k = p_1 q_2 \cdots q_l$$

Now, we divide the entire equation by p_1 to give

$$\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l$$

The integer $\frac{n}{p_1}$ is smaller than n, so we can use induction to assume that its factorisation is unique. Therefore

$$[p_2, p_3 \cdots p_k] = [q_2, q_3 \cdots q_l]$$

So the prime factorisation of n is unique. □

The common factors of two numbers $m = p_1^{a_1} \cdots p_k^{a_k}$ and $n = p_1^{b_1} \cdots p_k^{b_k}$ where a and b are zero or above is given by $p_1^{c_1} \cdots p_k^{c_k}$ where $c_i \leq \min(a_i, b_i)$ So the highest common factor is given by $c_i = \min(a_i, b_i)$.

The common multiples of those two numbers is given by $d_i \geq \max(a_i, b_i)$. So analogously the lowest common multiple is given by $d_i = \max(a_i, b_i)$.

We have the interesting property that $\text{HCF}(m, n)\,\text{LCM}(m, n) = mn$. This is true because any term p_i is given by $p_i^{\min(a_i,b_i)} p_i^{\max(a_i,b_i)} = p_i^{a_i+b_i}$.

3 Modular arithmetic

3.1 Introduction

In modular arithmetic, we need to prove that things like addition and multiplication are valid. In order to do this, we need to show that if $a \equiv a' \mod n$ and $b \equiv b' \mod n$ then, for example, $ab \equiv a'b'$. We can prove these statements trivially by writing $a' = a + kn$ where k is some integer, then evaluating the left and right hand sides in $\mathbb{Z}$.

Many rules of arithmetic are inherited from $\mathbb{Z}$; for example, addition is commutative. This is easy to realise: to prove that $a + b = b + a$ in $\mathbb{Z}_n$ it is sufficient to prove the statement is true in the whole of $\mathbb{Z}$.

As another example, we can transform the unique prime factorisation lemma into $\mathbb{Z}_p$. In $\mathbb{Z}_p$ where p is prime,

$$ab = 0 \implies (a = 0) \vee (b = 0)$$

In general, $\mathbb{Z}_p$ where p is prime is a very well behaved and convenient-to-use subset of $\mathbb{Z}$.

3.2 Inverses

For any $a, b \in \mathbb{Z}_n$, b is an inverse of a if $ab = 1$. Note that unlike in group theory, it is not necessarily the case that all elements will have inverses. For example, in $\mathbb{Z}_{10}$, the elements 3 and 7 are inverses, but 4 has no inverse. Note that:

- Invertible integers are cancellable. For example, $ab = ac \implies b = c$ if a is invertible (by left-multiplying by its inverse).
- In general, you cannot simply cancel an integer multiple in the realm of modular arithmetic. For example $4 \cdot 5 = 2 \cdot 5$ does not imply $4 = 2$.
- Invertible numbers are also called 'units'.

3.3 Invertibility

Proposition. Let $n \geq 2$. Then every $a \not\equiv 0\ (n)$ is invertible modulo n if and only if $(a, n) = 1$. Note that the parenthesis notation means the highest common factor of the parameters. In particular, if n is prime, then all $1 \leq a < n$ are invertible.

Proof. This first proof uses Euclid's algorithm. If a and n satisfy $(a, n) = 1$ then $ax + ny = 1$ for some $x, y \in \mathbb{Z}$. So $ax = 1 - ny$, so $ax \equiv 1\ (n)$. So x is the inverse of a. □

Proof. This alternate proof only works for $n = p$ where p is a prime; our whole proof lies entirely within $\mathbb{Z}_p$. Consider $0a, 1a, 2a, \cdots, (p-1)a$. Take two numbers i, j between 0 and $p-1$, then consider the condition $ia = ja$. This implies that $(i-j)a = 0$, but $a \neq 0$, so $i = j$. So this list $0a, 1a, \cdots$ contains all distinct elements, all of which must be between 0 and $p-1$. Therefore, by the pigeonhole principle, one of these elements must be equal to 1. Therefore there exists an inverse for a. □

3.4 Euler's totient function

Definition. Let $\varphi(n)$ be the amount of natural numbers less than or equal to n that are coprime to n.

Here are some examples.

- If p is prime, then $\varphi(p) = p - 1$ since all naturals less than p are coprime to it.
- $\varphi(p^2) = p^2 - p$ because there are p numbers in this range who shares the common factor p with p^2, specifically the numbers $p, 2p, 3p, \cdots, (p-1)p, p^2$.
- If a, b are coprime, $\varphi(ab) = ab - a - b + 1$. There are ab numbers in total to pick from. There are a multiples of b and b multiples of a, and since we discounted ab itself twice we need to count it again. Note that $\varphi(ab) = \varphi(a)\varphi(b)$.

3.5 Fermat's little theorem and Fermat–Euler theorem

Theorem. Let p be a prime. Then in $\mathbb{Z}_p$, $a \neq 0 \implies a^{p-1} = 1$.

This is actually a special case of the following theorem:

Theorem (Fermat–Euler Theorem)**.** Let $n \geq 2$. Then in $\mathbb{Z}_n$, any unit a satisfies $a^{\varphi(n)} = 1$.

Proof. Let the set of units $\mathbb{Z}_n \supset X = \{x_1, x_2, \cdots, x_{\varphi(n)}\}$. Consider multiplying each unit by a. We have $Y = \{ax_1, ax_2, \cdots, ax_{\varphi(n)}\}$. Since a is invertible, this set is comprised of distinct elements. Further, since they are all products of units, they are all units. So Y is a list of $\varphi(n)$ distinct units, so this list must be equal to X. Now, since the lists are the same, the product of all their elements must be the same. So $\prod X = \prod Y = a^{\varphi(n)} \prod X$. We can cancel the factor of $\prod X$ because it is a product of invertibles, leaving $1 = a^{\varphi(n)}$ as required. □

If alternatively we wanted to prove this just for p prime, then we could replace $\varphi(n)$ with $p-1$, and $\prod X$ with $(p-1)!$.

3.6 Square roots of one

Lemma. Let p be prime. Then in $\mathbb{Z}_p$, $x^2 = 1$ has solutions 1 and -1 only.

Note. In $\mathbb{Z}_8$, for example, we have $1^2 = 3^2 = 5^2 = 7^2 = 1$, so obviously this does not hold in the general case.

Proof. $x^2 = 1$ implies that $(x-1)(x+1) = 0$. Because of the $p \mid ab \implies (p \mid a) \vee (p \mid b)$ lemma, we know that $(x-1) = 0$ or $(x+1) = 0$, so -1 and 1 are the only solutions. □

3.7 Square roots of negative one

Theorem (Wilson's Theorem)**.** Let p be prime. Then $(p-1)! \equiv -1\ (p)$.

Proof. Since this is obviously true for $p = 2$, we will suppose that $p > 2$. In $\mathbb{Z}_p$, let us consider the list $1, 2, 3 \cdots (p-1)$. We can pair each a with its inverse a^{-1} for all $a \neq a^{-1}$. Note that $a = a^{-1} \iff a^2 = 1$ so in this case $a = 1$ or $a = -1$. So let us now multiply each element together, to get

$$(p-1)! = (aa^{-1})(bb^{-1}) \cdots 1 \cdot -1 = (1) \cdot (1) \cdots 1 \cdot -1 = -1$$

□

Proposition. Let $p > 2$ be prime. Then -1 is a square number modulo p if and only if $p \equiv 1\ (4)$.

Proof. If $p > 2$ then p is odd. There are therefore two cases, either $p \equiv 1$ or $p \equiv 3$ modulo 4. Each case is proven individually.

- $(p = 4k+3)$ Suppose that $x^2 = -1$ in $\mathbb{Z}_p$. The only thing we know about powers in modular arithmetic is Fermat's Little Theorem, so we will have to use this. So, $x^{p-1} = x^{4k+2} = 1$. Therefore, $(x^2)^{2k+1} = 1$. But we know that $x^2 = -1$, and we raise this -1 to an odd power, which is -1. So this is a contradiction.
- $(p = 4k+1)$ By Wilson's Theorem, we know that $(4k)! = -1$. We intend to show that this is a square number in the world of $\mathbb{Z}_p$. We will compare the termwise expansion of $(4k)!$ and $[(2k)!]^2$ on consecutive lines.

$$\begin{aligned} (4k)! &= 1 \cdot 2 \cdot 3 \cdots (2k) \cdot (2k+1) \cdot (2k+2) \quad \cdots (4k-1) \quad \cdot (4k) \\ [(2k)!]^2 &= 1 \cdot 2 \cdot 3 \cdots (2k) \cdot 1 \qquad\quad \cdot 2 \qquad\quad \cdots (2k-1) \quad \cdot (2k) \end{aligned}$$

By writing each term as an equivalent negative:

$$= 1 \cdot 2 \cdot 3 \cdots (2k) \cdot (-4k) \quad \cdot (-4k+1) \cdots (-2k-2) \cdot (-2k-1)$$

Extracting out the negatives:

$$= 1 \cdot 2 \cdot 3 \cdots (2k) \cdot (4k) \qquad \cdot (4k-1) \quad \cdots (2k+2) \quad \cdot (2k+1) \cdot (-1)^{2k}$$

which is equal to the first line by rearranging. So $[(2k)!]^2 = (4k)! = -1$. So -1 is a square number modulo p.

□

3.8 Solving congruence equations

Let us try to solve the equation $7x \equiv 4\ (30)$. We take a two-phase approach: first, we will find a single solution, and then we will find all of the other solutions.

Since 7 and 30 are coprime, we can use Euclid's algorithm to find a way of expressing 1 in terms of 7 and 30, in particular $13 \cdot 7 - 3 \cdot 30 = 1$. This allows us to solve $7y \equiv 1\ (30)$, by setting $y = 13$. Then, of course, we can multiply both sides by 4: $7y \cdot 4 \equiv 4\ (30)$, so $x = y \cdot 4 = 13 \cdot 4 = 22$.

We can now find other solutions (apart from trivially adding $30k$). Suppose that there exists some other solution x', i.e. $7x' \equiv 4\ (30)$. Then $7x \equiv 7x'\ (30)$. As 7 is invertible modulo 30, we can simply multiply by the inverse of 7 to give $x \equiv x'\ (30)$. So x is unique modulo 30. Alternatively, we could solve the equation without any of this working out by noticing that 7 is invertible! However, this is not very likely to happen in the general case, since it requires that the coefficient of x is coprime to the modulus.

Now, let's try a different equation, $10x = 12\ (34)$. Since 10 is not invertible, we can't do quite the same thing as above. We can't also just divide the whole thing by 2, there isn't a rule for that in general. We can, however, move into $\mathbb{Z}$ and manipulate the expression there. $10x = 12 + 34y$ for some $y \in \mathbb{Z}$, so we can divide the equation by 2 to get $5x = 6 + 17y$, so $5x = 6\ (17)$ and we can solve from there.

3.9 Chinese remainder theorem

Is there a solution for the simultaneous congruences

$$x \equiv 6\ (17); \quad x \equiv 2\ (19)$$

17 and 19 are coprime, so congruence mod 17 and congruence mod 19 are independent of each other. How about

$$x \equiv 6\ (34); \quad x \equiv 11\ (36)$$

In this instance, there is obviously no solution; should x be even or odd? We can see that, the smallest amount we can adjust x by in one equation while retaining congruence in the other equation is HCF(34, 36), which is 2.

Theorem. Let u, v be coprime. Then for any a, b, there exists a value x such that

$$x \equiv a\ (u); \quad x \equiv b\ (v)$$

and that this value is unique modulo uv.

Proof. We first prove existence of such an x. By Euclid's Algorithm, we have $su + tv = 1$ for some integers s, t. Note that therefore:

$$su \equiv 0\,(u); \quad tv \equiv 0\,(v); \quad su \equiv 1\,(v); \quad tv \equiv 1\,(u);$$

Therefore we can make a linear combination of su and tv that is the required size in each congruence, specifically

$$x = (su)b + (tv)a$$

Now we prove that this value x is unique modulo uv. Suppose there was some other solution x'. Also, $x' \equiv x\,(u)$ and $x' \equiv x\,(v)$. So we have $u \mid (x' - x)$ and $v \mid (x' - x)$ but as u and b are coprime we have $uv \mid (x' - x)$. So x is unique modulo uv. □

3.10 RSA encryption

A practical use of number theory is RSA encryption, which is an asymmetric encryption protocol that allows encryption by using a public and private key pair. We will begin by first choosing two large distinct primes p and q. By large, we mean primes that are hundreds of digits long; in practice, these primes are between around 512 bits and 2048 bits long when represented in binary. Let $n = pq$, and pick a 'coding exponent' e. Our message that we want to send must be an element of $\mathbb{Z}_n$, so if it is not representable in this form we must break it apart into several smaller messages, or perhaps use RSA to share some kind of small symmetric key for another encryption algorithm. Let this message be x, so $x < n$.

To encode x, we raise it to the power e in $\mathbb{Z}_n$. To efficiently compute large powers of x, we can use a repeated squaring technique. For example, we can find x, x^2, x^4, x^8, x^{16} through repeated squaring, and then for example we can calculate $x^{19} = x^{16}x^2x^1$.

To decode x^e, we ideally want some number d such that $(x^e)^d = x$. By the Fermat–Euler Theorem, we have $x^{\varphi(n)} = 1$, so clearly $x^{k\varphi(n)+1} = x$. In other words, we want $ed \equiv 1 \mod \varphi(n)$. By running Euclid's algorithm on e and $\varphi(n)$, we can find such a d. Note that this requires e and $\varphi(n)$ to be coprime; in practice we would choose e after we have chosen n such that this is the case.

Now, we can see that to encode a message, all you need is n and e. However, to decode, you need to also know d, which means you need to know $\varphi(n) = \varphi(pq) = pq - p - q + 1$ which requires that you know the original p and q. If we pick sufficiently large p and q, our n will be so big as to be almost impossible to factorise in any decent length of time. So we can publish n and e as our public key, and anyone may use these numbers to encrypt a message that then only we can decode.

4 The reals

4.1 Motivation for the reals

Why do we need the real numbers in the first place? Well, we introduce new sets of numbers when there are equations that we cannot solve using our current number system. For example, the equation $x + 2 = 0$ is not solvable in $\mathbb{N}$, so we constructed $\mathbb{Z}$. Then we could not solve equations like $2x = 3$, so we created the rationals, $\mathbb{Q}$. Now, we cannot solve equations such as $x^2 = 2$, so we must create a new set of numbers that contains this solution.

Proposition. There does not exist a $q \in \mathbb{Q}$ such that $q^2 = 2$. Note that in this proposition we make no assumption that $q^2 = 2$ is solvable, or that a solution if one exists does not lie within $\mathbb{Q}$; we simply state that confined to the realm of $\mathbb{Q}$ the equation is unsolvable.

Proof 1. Suppose that such a $q \in \mathbb{Q}$ exists, such that $q^2 = 2$. Without loss of generality, we will assume that $q > 0$ because $(-q)^2 = q^2$. So let q be written as a/b where $a, b \in \mathbb{N}$. Then $a^2/b^2 = 2$, so $a^2 = 2b^2$. If we factorise each side as a product of primes, the exponent of the prime 2 on the left hand side must be even, but on the right hand side it must be odd. This contradicts the unique factorisation of natural numbers. So such a q does not exist. □

Proof 2. Suppose that there exists some $q \in \mathbb{Q}$ written similarly to above as a/b. Note that for any $c, d \in \mathbb{Z}$, $cq + d$ is of the form e/b for some integer e. Therefore, if $cq + d > 0$ then $cq + d \geq 1/b$.

Now, note that $0 < (q-1) < 1$, so for a suitably large n, we have $0 < (q-1)^n < 1/b$. However, $(q-1)^n$ is of the form $cq + d$ because $q^2 = 1$ so we can eliminate all exponents. This is a contradiction so such a q does not exist. □

We can see from the proofs above that $\mathbb{Q}$ has a 'gap' at $\sqrt{2}$. How can we express this fact without mentioning $\mathbb{R}$? We can't just say plainly that $\sqrt{2} \notin \mathbb{Q}$ because as far as we know from $\mathbb{Q}$, there is no reason to assume that such a number called $\sqrt{2}$ even exists! We need to find a way to express the concept of $\sqrt{2}$ in the language of $\mathbb{Q}$. One way to do this is by creating sone set $S = \{q \in \mathbb{Q} : q^2 < 2\}$. Then we can write down some upper bounds for this set. For example, 2 is a trivial upper bound, as is 1.5, and as is 1.42. In fact, we can continue making smaller and smaller upper bounds. We can see therefore that there exists no least upper bound in $\mathbb{Q}$.

4.2 Axioms of the reals

We define the reals as follows: the reals are a set written $\mathbb{R}$ with elements 0 and 1 with $0 \neq 1$; with operations $+$ and $\cdot$; and an ordering $<$; such that:

(i) $+$ is commutative, associative, has identity 0, and there are inverses for all elements;

(ii) $\cdot$ is commutative, associative, has identity 1, and there are inverses for all nonzero elements;

(iii) $\cdot$ is distributive over $+$;

(iv) for all a and b in $\mathbb{R}$, exactly one of $a < b$, $a = b$ and $a > b$ are true, and that $a < b$ and $b < c$ implies $a < c$;

(v) for all $a, b, c \in \mathbb{R}$, $a < b$ implies $a + c < b + c$, and $a < b$ implies $ac < bc$ when $c > 0$; and

(vi) for any set S of reals that is non-empty and bounded above, S has a least upper bound.

There are some notable immediate remarks about the definitions of the reals.

- We can contain the rationals inside the reals: $\mathbb{Q} \subset \mathbb{R}$
- The least upper bound axiom is false in $\mathbb{Q}$, which is why it's so important in $\mathbb{R}$.
- Why did we specify 'non-empty' and 'bounded above' in the least upper bound axiom? Of course, if a set is not bounded above, then it has no upper bound, so clearly it can have no least

upper bound. If a set is empty, then every real is an upper bound for this set, and as there is no least real number, there is no least upper bound.

- It is possible to construct $\mathbb{R}$ out of $\mathbb{Q}$, and check that the above axioms hold. However, this is a rare example where the construction of $\mathbb{R}$ is complicated and irrelevant, so it is not covered here.

The reals do not contain infinitely big or infinitesimally small elements.

Proposition (the axiom of Archimedes)**.** $\mathbb{N}$ is not bounded above in $\mathbb{R}$.

Proof. If there were some upper bound $c = \sup \mathbb{N}$, then $c - 1$ is clearly not an upper bound for $\mathbb{N}$. So there exists some natural number n such that $n > c - 1$. But then clearly $n + 1 \in \mathbb{N} > c$ contradicting the existence of this upper bound. □

Corollary. For each $t \in \mathbb{R} > 0$, $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < t$.

Proof. We have some $n \in \mathbb{N}$ with $n > \frac{1}{t}$ by the above proposition. So $\frac{1}{n} < t$. □

4.3 Examples of sets and least upper bounds

Note that a common way to write 'least upper bound' is the word supremum, denoted $\sup S$.

(i) Let $S = \{x \in \mathbb{R} : 0 \leq x \leq 1\} = [0, 1]$. The least upper bound of S is 1, because:

- 1 is an upper bound for S; $\forall x \in S, x \leq 1$; and
- Every upper bound y must have $y \geq 1$ because $1 \in S$.

(ii) Let $S = \{x \in \mathbb{R} : 0 < x < 1\} = (0, 1)$. $\sup S = 1$ because:

- 1 is an upper bound for S; $\forall x \in S, x \leq 1$; and
- No upper bound c has $c < 1$. Indeed, certainly $c > 0$ ($c > \frac{1}{2}$ since $\frac{1}{2} \in S$). So if $c < 1$, then $0 < c < 1$, so the number $\frac{1+c}{2} \in S$ and is larger than c, so it is not an upper bound.

(iii) Let $S = \left\{1 - \frac{1}{n} : n \in \mathbb{N}\right\}$. $\sup S = 1$ because:

- 1 is clearly an upper bound.
- Let us suppose $c < 1$ is an upper bound. Then $\forall n \in \mathbb{N}, 1 - \frac{1}{n} < c$ so $1 - c < \frac{1}{n}$. From the corollary of the Axiom of Archimedes above, this is a contradiction.

Remark. If S has a greatest element, then this element is the supremum of the set: $\sup S \in S$. But if S does not have a greatest element, then $\sup S \notin S$. Also, we do not need any kind of 'greatest lower bound' axiom—if S is a non-empty, bounded below set of reals, then the set $\{-x : x \in S\}$ is non-empty and bounded above, and so has a least upper bound, so S has a greatest lower bound equivalent to its additive inverse. This is commonly called the 'infimum', or $\inf S$.

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

Proof. Let S be the set of all real numbers such that $x^2 < 2$. Of course, it is non-empty (try $x = 0$) and bounded above (try $x = 2$). So let $c = \sup S$; we want to show that $c^2 = 2$. We prove this by eliminating all alternatives; clearly either $c^2 < 2$, $c^2 = 2$ or $c^2 > 2$.

- ($c^2 < 2$) We want to prove that $(c+t)^2 < 2$ for some small t. For $0 < t < 1$, we have $(c+t)^2 = c^2 + 2ct + t^2 \leq c^2 + 5t$, since c is at most 2, and t^2 is at most t. So this value is less than 2 for some suitably small t, contradicting the least upper bound—we have just shown that $(c+t) \in S$.
- ($c^2 > 2$) We want to prove that $(c-t)^2 > 2$ for some small t. For $0 < t < 1$, we have $(c-t)^2 = c^2 - 2ct + t^2 \geq c^2 - 4t$, since c is at most 2, and t^2 is at least zero. So this value is greater than 2 for some suitably small t, contradicting the least upper bound—we have just created a lower upper bound.

So $c^2 = 2$. □

This same kind of proof works for a lot of real values, for example $\sqrt[n]{x}$ for $n \in \mathbb{N}$, $x \in \mathbb{R}$, $x < 0$. Reals that are not rational are called irrational. This is a negative statement however, so it is better in proofs to suppose that something is rational, and then show a contradiction.

Also, the rationals are 'dense'; for any $a, b \in \mathbb{R}$, there is another rational between them. We may assume without loss of generality that they are both non-negative and that $a < b$. Then pick some $n \in \mathbb{N}$ with $\frac{1}{n} < b - a$. Among the list $\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots$, there is a final one that is less than or equal to a, which we will denote $\frac{q}{n}$ (otherwise a is an upper bound to this list, contradicting the axiom of Archimedes). So $a < \frac{q+1}{n} < b$ as required.

The irrationals are also dense; for any reals a and b with the same conditions above, these exists some irrational c with $a < c < b$. We know that there exists a rational c with $a\sqrt{2} < c < b\sqrt{2}$, so $a < \frac{c}{\sqrt{2}} < b$.

4.4 Sequences and limits

How can we ascribe meaning to expressions like this?

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots$$

Certainly, we have a concept of addition, and we can keep adding as many terms as we like, but there is no implicit definition of an infinite sum from the aforementioned axioms.

A definition that makes sense would involve partial sums x_n of this infinite series. However, we could not just say that the partial sums get progressively closer to a value, because then trivially something like $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots$ tends to 107, even though they're clearly getting closer.

A more accurate definition would be to state that we can get arbitrarily close (within some given ε) to a 'limit value' c by taking some amount of terms n of this series: $c - \varepsilon < x_n < c + \varepsilon$. But this is still wrong: the sequence $\frac{1}{2}, 10, \frac{2}{3}, 10, \frac{3}{4}, 10, \frac{4}{5}, 10, \ldots$ could then tend to 1 even though every other term is 10.

The best definition would state that the sequence of partial sums would *stay* within ε of c for all x_k where $k \geq n$ for some $n \in \mathbb{N}$. In less formal words, for any $\varepsilon > 0$, x_n will eventually stay within ε of c. Equivalently, $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ such that $\forall n > N$ we have $|x_n - c| < \varepsilon$.

(i) Consider the sequence $\frac{1}{2}$, $\frac{1}{2} + \frac{1}{4}$, $\frac{1}{2} + \frac{1}{4} + \frac{1}{8}$, ... This is $x_1, x_2, x_3, \ldots$ where $x_n = 1 - \frac{1}{2^n}$ (inductively on n). We want to show that x_n tends to 1. Given some $\varepsilon > 0$, we choose some $N \in \mathbb{N}$ with $N > \frac{1}{\varepsilon}$. Then, for every $n \geq N$, $|x_n - 1| = \frac{1}{2^n} \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon$.

(ii) Consider the constant sequence $c, c, c, c, \ldots$. We want to show that $x_n \to c$. Given some $\varepsilon > 0$, we have $|x_n - c| < \varepsilon$ for all n; $N = 1$ is the time after which the sequence stays within ε of c.

(iii) Consider now $x_n = (-1)^n$, i.e. $-1, 1, -1, 1, \ldots$. We want to show that this does not tend to a limit. Suppose $x_n \to c$ as $n \to \infty$. We may choose some ε that acts as a counterexample—for example, $\varepsilon = 1$. So $\exists N \in \mathbb{N}$ such that $\forall n \geq n$ we have $|x_n - c| < 1$. In particular, $|1 - c| < 1$ and $|-1 - c| < 1$ so $|1 - (-1)| < 2$, by the triangle inequality. This is a contradiction.

(iv) The sequence x_n given by

$$x_n = \begin{cases} \frac{1}{n} & n \text{ odd} \\ 0 & n \text{ even} \end{cases}$$

should tend to zero. Given some $\varepsilon > 0$, we will choose $N \in \mathbb{N}$ with $\frac{1}{N} < \varepsilon$. Then for all $n \geq N$, either $x_n = \frac{1}{n}$ or 0. In either case, $|x_n - 0| \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon$.

We can denote the entirety of a sequence $x_1, x_2, \ldots$ as

$$(x_n) \quad \text{or} \quad (x_n)_{n=1}^{\infty}$$

For example, $((-1)^n)_{n=1}^{\infty}$ is divergent. This isn't saying that it goes to infinity, just that it doesn't converge. Note also that if $x_n \to c$ and $x_n \to d$, then $c = d$. Suppose that $c \neq d$. Then pick $\varepsilon = \frac{|c-d|}{2}$. Then $\exists N \in \mathbb{N}$ with $|x_n - c| < \varepsilon$, and $\exists M \in \mathbb{N}$ with $|x_n - d| < \varepsilon$. After the point $\max(N, M)$, the points must be within ε of both c and d, but as c and d are 2ε apart this is a contradiction (by the triangle inequality).

4.5 Series

A sequence given in the form x_1, $x_1 + x_2$, $x_1 + x_2 + x_3, \ldots$ is called a series. They are often written $\sum_{n=1}^{\infty} x_n$. The kth term of the sequence, given by $\sum_{n=1}^{k} x_n$, is called the kth partial sum. If the series converges to some value c, then we can write $\sum_{n=1}^{\infty} x_n = c$. Note that we cannot use this notation to denote the limit until we know that the limit actually exists. This is just the same as with sequences, where we cannot write $\lim_{n\to\infty} x_n$ until we know that the limit exists.

Limits behave as we would expect. For example, if $x_n \leq d$ for all n, and $x_n \to c$, then $c \leq d$. Suppose $c > d$. Then we will choose $\varepsilon = \frac{|c-d|}{2}$. Then there are no points x_n within this bound of c #.

Proposition. If $x_n \to c$ and $y_n \to d$, then $x_n + y_n \to c + d$.

Proof. Given some $\varepsilon > 0$, let $\zeta = \frac{1}{2}\varepsilon$. Then, after some term x_N, $|x_n - c| < \zeta$, and after some term y_M, $|y_m - d| < \zeta$. So for every $n \geq \max(M, N)$, by the triangle inequality, $|(x_n + y_n) - (c + d)| < 2\zeta = \varepsilon$ as required. □

This is commonly known as an $\varepsilon/2$ argument. Also, if we had instead not taken any ζ value and just stuck with ε, it would still be a good proof because we could just have divided ε at the beginning—it's not expected that you completely rewrite the proof to add in this division.

4.6 Testing convergence of a sequence

A sequence $x_1, x_2, \ldots$ is called 'increasing' if $x_{n+1} \geq x_n$ for all n.

Theorem. If $x_1, x_2, \ldots$ is increasing and bounded above, it converges to a limit.

This is a very important theorem that we will refer back to time and time again.

Note. If we were in $\mathbb{Q}$, this would not necessarily hold. For example, consider the decimal expansion of $\sqrt{2}$.

$$1, 1.4, 1.41, 1.414, 1.4142, \ldots$$

They don't converge to a limit in $\mathbb{Q}$. So our proof will have to be more rigorous than just 'they have to tend to somewhere below the upper bound'; we must use a property that $\mathbb{R}$ has that $\mathbb{Q}$ does not have, i.e. the least upper bound axiom.

Proof. Let $c = \sup\{x_1, x_2, \ldots\}$. We want to prove that $x_n \to c$. Given some $\varepsilon > 0$, there exists some n such that $x_n > c - \varepsilon$ (else, $c - \varepsilon$ would be a smaller upper bound #). As the sequence is increasing, all x_k where $k > n$ are at least x_n. So $|x_k - c| < \varepsilon$ as required. □

Of course, a decreasing sequence works in an identical way; if it is bounded below then it converges. More compactly, a bounded monotone sequence is convergent (where monotone means either increasing or decreasing).

Proposition. The harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

diverges; the solution to the Basel problem

$$\sum_{n=1}^{\infty} \frac{1}{n^2}$$

converges.

There is no closed form for the nth term of either of these sequences, which is one reason that series are often more challenging to work with than regular sequences.

Proof. Since the harmonic series is difficult to deal with, we will compare it to a sequence that we understand easier. Therefore, we show that the first sequence diverges using a comparison test with

powers of 2, one of the simplest series.

$$\begin{aligned} &1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \cdots \\ \geq\ &1 + \frac{1}{2} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{\frac{1}{2}} + \frac{1}{16} + \cdots \end{aligned}$$

By inspection, we can see that the harmonic series is larger than the sum of an infinite amount of $\frac{1}{2}$, so surely it must diverge. More rigorously:

$$\begin{aligned} \frac{1}{3} + \frac{1}{4} &\geq \frac{1}{2} \\ \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} &\geq \frac{1}{2} \\ \frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \cdots + \frac{1}{2^{n+1}} &\geq \frac{2^n}{2^{n+1}} = \frac{1}{2} \end{aligned}$$

So the partial sums of the series are unbounded, so the series diverges. For the sum of reciprocals of squares, we want to do a similar thing because again the only simple sequence we have to work with is the powers of 2.

$$\begin{aligned} &1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} + \frac{1}{8^2} + \frac{1}{9^2} + \cdots \\ \leq\ &1 + \underbrace{\frac{1}{2^2} + \frac{1}{2^2}}_{\frac{2}{2^2}} + \underbrace{\frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2}}_{\frac{4}{4^2}} + \frac{1}{8^2} + \frac{1}{8^2} + \cdots \end{aligned}$$

The bottom sequence simplifies to just the sequence $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots \to 2$, and the upper sequence is bounded above by the lower sequence. More rigorously:

$$\begin{aligned} \frac{1}{2^2} + \frac{1}{3^2} &\leq \frac{2}{2^2} = \frac{1}{2} \\ \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} &\leq \frac{4}{4^2} = \frac{1}{4} \\ \frac{1}{(2^n)^2} + \frac{1}{(2^n + 1)^2} + \cdots + \frac{1}{(2^{n+1} - 1)^2} &\leq \frac{2^n}{(2^n)^2} = \frac{1}{2^n} \end{aligned}$$

So the partial sums are bounded, and hence the series converges by the above theorem. □

In fact, $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. This is proved in the Linear Analysis course in Part II.

4.7 Decimal expansions

What should $0.a_1a_2a_3\ldots$ mean (where each a is a digit from 0 to 9)? It should be the limit of $0.a_1$, $0.a_1a_2$, $0.a_1a_2a_3$ and so on. We will define it by

$$0.a_1a_2a_3\cdots \coloneqq \sum_{n=1}^{\infty} \frac{a_n}{10}$$

This clearly converges as the partial sums are increasing and bounded above by 1, so infinite decimal expansions are valid. Conversely, given some $x \in \mathbb{R}$ with $0 < x < 1$, we can certainly write it as a (potentially infinite) decimal. We will start by choosing the greatest a_1 from 0 to 9 such that $\frac{a_1}{10} \leq x$. Thus $0 < x - \frac{a_1}{10} < \frac{1}{10}$. Now, we can pick the greatest a_2 in the set such that $\frac{a_1}{10} + \frac{a_2}{100} \leq x$. Therefore, $0 \leq x - \frac{a_1}{10} - \frac{a_2}{100} < \frac{1}{100}$. Continue inductively, and then we obtain a decimal expansion $0.a_1a_2a_3\ldots$ such that $0 \leq x - \sum_{n=1}^{k} \frac{a_n}{10^n} < \frac{1}{10^k}$ for any given k. By the definition of convergence, the sequence given for a tends to x as required.

Note, if $0.a_1a_2\ldots$ and $0.b_1b_2\ldots$ are different decimal expansions of the same number, then there exists some $N \in \mathbb{N}$ such that $a_n = b_n$ for all $n < N$ and $a_N = b_N - 1$ and $a_n = 9, b_n = 0$ for all $n > N$ (or vice versa). For example, 0.99999 ... is equivalent to 1.00000 ...

4.8 The number e

We define

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \ldots$$

The partial sums are increasing and bounded above by the powers of two after the first term, so it converges.

4.9 Algebraic and transcendental numbers

A real x is called algebraic if it is a root of a nonzero polynomial with integer coefficients. Otherwise, it is called transcendental. For example, any rational $\frac{p}{q}$ is algebraic as it is the root of $qx - p = 0$. As another example, $\sqrt{2} + 1$ is algebraic as it is a root of the equation $x^2 - 2x - 1 = 0$. The logical next question to ask is whether all reals are algebraic.

Proposition. e is not rational.

Proof. Suppose that e is rational, let it be written $\frac{p}{q}$, where $q > 1$ (if $q = 1$, rewrite it as $\frac{2p}{2q}$). Multiplying up by $q!$ (easier than just q because then we can compare factorials) gives

$$\sum_{n=0}^{\infty} \frac{q!}{n!} \in \mathbb{Z}$$

We know that $\sum_{n=0}^{q} \frac{q!}{n!} \in \mathbb{Z}$. The next terms are:

$$\begin{aligned}
\frac{q!}{(q+1)!} &= \frac{1}{q+1} \\
\frac{q!}{(q+2)!} &= \frac{1}{(q+1)(q+2)} \leq \frac{1}{(q+1)^2} \\
\frac{q!}{(q+3)!} &= \frac{1}{(q+1)(q+2)(q+3)} \leq \frac{1}{(q+1)^3} \\
\frac{q!}{(q+n)!} &\leq \frac{1}{(q+1)^n}
\end{aligned}$$

So the next partial sums are bounded above by the geometric series.

$$\sum_{n=q+1}^{\infty} \frac{q!}{n!} \leq \frac{1}{q} < 1$$

So the whole series multiplied by $q!$ is a whole number plus a fractional part, which is not an integer #. □

Ideally now we'd have a proof that e is transcendental. However, even though the terms of e tend to zero quickly, they don't tend to zero quite quickly enough for us to be able to prove it using what we know now. We instead prove that there exists some transcendental number using a different example, one whose terms tend to zero very quickly indeed.

Theorem. Liouville's constant $c = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental. As a decimal expansion:

$$c = 0.110001000000000000000010\ldots$$

This is a long proof, the hardest in this course. We will cherry-pick some important results about polynomials in order to make this proof, without a proper introduction to features of polynomials.

- For any polynomial P, $\exists k \in \mathbb{R}$ such that $|P(x) - P(y)| \leq k|x - y|$ for all $0 \leq x, y \leq 1$. Indeed, say $P(x) = a_d x^d + \cdots + a_0$, then

$$\begin{aligned} P(x) - P(y) &= a_d(x^d - y^d) + a_{d-1}(x^{d-1} - y^{d-1}) + \cdots + a_1(x - y) \\ &= (x - y)[a_d(x^{d-1} + x^{d-2}y + \cdots + y^{d-1}) + \cdots + a_1] \\ |P(x) - P(y)| &\leq |x - y|[(|a_d| + |a_{d-1}| + \cdots + |a_1|)d] \end{aligned}$$

  because x and y are between 0 and 1.

- A nonzero polynomial of degree d has at most d roots. Given some polynomial P of degree d:
  - If P has no roots, we are trivially done.
  - If P has some root a, then P can be written as $(x - a)Q(x)$. Inductively, $Q(x)$ has at most $d - 1$ roots, so P has at most d roots.

Now we can prove the above theorem.

Proof. We will write $c_n = \sum_{k=0}^{n} \frac{1}{10^{k!}}$, such that $c_n \to c$. Suppose that some polynomial P has c as a root. Then $\exists k$ such that $|P(x) - P(y)| \leq k|x - y|$ when $0 \leq x, y \leq 1$. Let P have degree d, such that

$$P(x) = a_d x^d + \cdots + a_0$$

Now, $|c - c_n| = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} \leq \frac{2}{10^{(n+1)!}}$. This is a trivial upper bound, of course better upper bounds exist.

Also, $c_n = \frac{a}{10^{n!}}$ for some $a \in \mathbb{Z}$. So $P(c_n) = \frac{b}{10^{dn!}}$ for some $b \in \mathbb{Z}$ (since $P(\frac{s}{t}) = \frac{q}{t^d}$ for some integer q, where $\frac{s}{t} \in \mathbb{Q}$).

For n large enough, c_n is not a root, because P only has finitely many roots. So

$$|P(c) - P(c_n)| = |P(c_n)| \leq \frac{1}{10^{dn!}}$$

Therefore

$$\frac{1}{10^{dn!}} \leq k\frac{2}{10^{(n+1)!}}$$

which is a contradiction if n is large enough. □

Here are some remarks about this proof.

- This same proof shows that any real x such that $\forall n \exists \frac{p}{q} \in \mathbb{Q}$ with $0 < \left|x - \frac{p}{q}\right| < \frac{1}{q^n}$ is transcendental. Informally, x has very good rational approximations.
- Such x are often called Liouville numbers; the proof works for all Liouville numbers.
- This proof does not show that e is transcendental (even though it is), because the terms do not go to zero fast enough.
- We now know that there exist some transcendental numbers. Another proof of existence of transcendental numbers will be seen in a later lecture.

4.10 Complex numbers

Some polynomials have no real roots, for example $x^2 + 1$. We'll try to 'force' an x with the property $x^2 = -1$. Note that for example we could not force an x into existence with the property $x^2 = 2, x^3 = 3$; how do we know introducing i will not lead to a contradiction? We will define $\mathbb{C}$ to consist of the plane $\mathbb{R}^2$, i.e. pairs of real numbers, with operations $+$ and $\cdot$ which satisfy:

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

We can view $\mathbb{R}$ as being contained within $\mathbb{C}$ by identifying the real number a with $(a, 0)$. Note that the rules of arithmetic of the reals are inherited inside the first element of the complex plane, so there is no contradiction here. Then let $i = (0, 1)$. Trivially then, any point (a, b) in the complex numbers may be written as $a + bi$ where $a, b \in \mathbb{R}$. And, of course, $i^2 = -1$.

All of the basic rules like associativity and distributivity work in the complex plane. There are multiplicative inverses: given $a + bi$, we know that $(a + bi)(a - bi) = a^2 + b^2$ so $\frac{a-bi}{a^2+b^2}$ is the inverse (provided the point is nonzero). This kind of structure with familiar properties is known as a field, for example $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$ where p is prime. The fundamental theorem of algebra states that any nonzero polynomial with complex coefficients has a complex root; this is proven in the IB course Complex Analysis.

5 Sets

5.1 Sets and subsets

A set is any* collection of mathematical objects. $(\forall x, x \in A \iff x \in B) \iff (A = B)$. In words, two sets which have the same members are considered to be the same; order of members is not important in a set. There is no 'multiple membership' of a set, $\{a, a\} = \{a\}$.

Given a set A and a property $p(x)$, we can form $\{x \in A : p(x)\}$; the subset of all members of A with property p. This is sometimes called the 'subset selection' rule or axiom. We can say that B is a subset of A if $\forall x, x \in B \implies x \in A$, written $B \subseteq A$. Further, $A = B \iff A \subseteq B, B \subseteq A$.

5.2 Composing sets

Given sets A and B, we can form their union $A \cup B = \{x : x \in A \vee x \in B\}$. We can also form their intersection $A \cap B = \{x : x \in A \wedge x \in B\}$. If $A \cap B = \varnothing$, we say A and B are disjoint. Note that we could consider $A \cap B$ as a special case of subset selection; the subset of A with the property that the element is in B. Therefore, $A \cap B \subseteq A$, and $A \cap B \subseteq B$. We define the set difference $A \setminus B = \{x \in A : x \notin B\}$.

Note that $\cap$ and $\cup$ are commutative and associative. Also, $\cup$ is distributive over $\cap$, and $\cap$ is distributive over $\cup$. For example, let us prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- (LHS $\subseteq$ RHS) Given $x \in A \cap (B \cup C)$, we have $x \in A$ and also either $x \in B$ or $x \in C$. If $x \in B$ then $x \in A \cap B$ so $x \in (A \cap B) \cup (A \cap C)$; and vice versa for C.
- (RHS $\subseteq$ LHS) Given $x \in (A \cap B) \cup (A \cap C)$, either $x \in A \cap B$ or $x \in A \cap C$. If $x \in A \cap B$ then $x \in A$ and $x \in B \cup C$ as required; and vice versa for the other case.

As the union is associative, we can have bigger unions of more sets. For example, if we let $A_n = \{n^2, n^3\}$ for each $n \in \mathbb{N}$, the infinite union

$$A_1 \cup A_2 \cup A_3 \cup \cdots = \bigcup_{n=1}^{\infty} A_n = \bigcup_{n \in \mathbb{N}} A_n = \{x \in N : x \text{ is a square or a cube}\}$$

When we use the $n \in \mathbb{N}$ on the large union symbol, we call $\mathbb{N}$ the 'index set'. Note that the infinite union is not defined as a limit of finite unions; it is simply defined using set comprehension. In general, given a set I, and sets A_i, $i \in I$, we can form

$$\bigcup_{i \in I} A_i = \{x : \exists i \in I, x \in A_i\}$$

and

$$\bigcap_{i \in I} A_i = \{x : \forall i \in I, x \in A_i\}$$

Note that we cannot form an intersection when $I = \varnothing$, as will be explained later.

For any a, b, we can form the ordered pair (a, b), where equality is checked component-wise. For sets A, B, we can form their product $A \times B = \{(a, b) : a \in A, b \in B\}$. For example, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ can be viewed as a plane. We can form other sizes of tuples similarly.

For any set X, we can form the power set $\mathcal{P}(X)$ consisting of all subsets of X.

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

For example:

$$\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$$

5.3 Russell's paradox

For a set A, we can always form the set $\{x \in A : p(x)\}$ for any property p. We cannot, however, form the set $\{x : p(x)\}$. Suppose we could form such a set, then we could form the set $X = \{x : x \notin x\}$. Now, is $X \in X$? If this is true, then it fails the defining property $x \notin x$. If this is false, then the defining property is true, so it must be in the set. This is a contradiction in both cases.

Similarly, there is no 'universal' set $\mathcal{E}$, meaning $\forall x, x \in \mathcal{E}$. Otherwise we could form the X above by $\{x \in \mathcal{E} : p(x)\}$. To guarantee that a given set exists, we need to obtain it in some way from known sets.

5.4 Finite sets

We will write $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $n \in \mathbb{N}_0$, we can say that a set A has size n if we can write $A = \{a_1, a_2, \cdots, a_n\}$ where the a_i are distinct. A set is called finite if it has a size $n \in \mathbb{N}_0$.

Note that a set cannot have size n and size m for $n \neq m$. Suppose that A has size n and size m where $n, m > 0$. Then, removing an element, we obtain a set that has size $n-1$ and $m-1$. By induction on the larger of n and m, we will eventually reach a size of both zero and nonzero which is a contradiction.

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

Proof 1. We may assume that our set is simply $\{1, 2, \cdots, n\}$ by relabelling. When constructing a subset S from this set, there are n independent binary choices for whether a given element should be within this subset, since for example either $1 \in S$ or $1 \notin S$ must be true. So there are 2^n distinct choices of subset you can make. □

Proof 2. We will prove this inductively on n, noting that $n = 0$ is trivial. For any subset $T \subseteq \{1, 2, \cdots n-1\}$, how many $S \subseteq \{1, \cdots, n\}$ have $S \cap \{1, 2, \cdots n-1\} = T$? Exactly two: T and $T \cup \{n\}$. So there are two choices for how to extend this subset to the new element n. So the number of subsets is $2 \cdot 2^{n-1} = 2^n$. □

In some sense Proof 2 is a more 'formal' version of Proof 1, using induction rather than intuition. We sometimes say that if A has size n, then $|A| = n$, and that A is an n-set.

5.5 Binomial coefficients

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

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

For example, there are six 2-sets in a 4-set. There is a formula for this, but generally this definition is a lot easier to use. Note that $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, and $\binom{n}{1} = n$ where $n > 0$.

Note that $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$ as each side counts the number of subsets in an n-set. Also:

(i) $\binom{n}{k} = \binom{n}{n-k}$ $(\forall n \in N_0, 0 \leq k \leq n)$. Indeed, specifying which k members to pick for a subset is equivalent to specifying which $n-k$ members not to pick.

(ii) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ $(\forall n \in \mathbb{N}, 0 < k < n)$. Indeed, the number of k-subsets of $\{1, 2, \ldots, n\}$ without n is $\binom{n-1}{k}$. The number of k-subsets of $\{1, 2, \ldots, n\}$ that do contain n is $\binom{n-1}{k-1}$ as we must pick the remaining $k-1$ elements of this new subset. So in total, $\binom{n-1}{k-1} + \binom{n-1}{k}$ encapsulates both possibilities.

This last point illustrates that Pascal's Triangle will give all the binomial coefficients since it perfectly encapsulates the relationship between a given element of the triangle with two elements from the previous row. The exact proof follows from the other known properties of the binomial coefficients.

5.6 Computing binomial coefficients

Proposition.

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots(1)}$$

Proof. The number of ways to name a k-set is $n(n-1)(n-2)\cdots(n-k+1)$ because there are n ways to choose a first element, $n-1$ ways to choose a second element, and so on. We have overcounted the k-sets, though—there are $k(k-1)(k-2)\cdots(1)$ ways to name a given k-set because you have k choices for the first element, $k-1$ choices for the second element, and so on. Hence the number of k-sets in $\{1, 2, \dots, n\}$ is the required result. □

Note that we can also write

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

but this is a very unwieldy formula to use especially by hand, so will be rarely used. Further, we can make asymptotic approximations using this formula, for example $\binom{n}{3} \sim \frac{n^3}{6}$ for large n.

5.7 Binomial theorem

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

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

Proof. When we expand $(a+b)^n = (a+b)(a+b)\dots(a+b)$, we obtain terms of the form $a^k b^{n-k}$. To get a single term of this form, we must choose k brackets for which to take the a value in the expansion, and the other $n-k$ brackets will take the b value. The number of terms of the form $a^k b^{n-k}$ for a fixed k is therefore the amount of ways of choosing k brackets out of a total of n, which is $\binom{n}{k}$. So

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

□

For example, we can tell that $(1+x)^n$ reduces to

$$1 + nx + \frac{1}{2}n(n-1)x^2 + \frac{1}{3!}n(n-1)(n-2)x^3 + \cdots + nx^{n-1} + x^n$$

So when x is small, a good approximation to $(1+x)^n$ is $1+nx$.

5.8 Inclusion-exclusion theorem

Given two finite sets A, B, we have

$$|A \cup B| = |A| + |B| - |A \cap B|$$

For three sets, we have

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

Theorem. Let $S_1, \dots, S_n$ be finite sets. Then,

$$\left| \bigcup_{S \in S_n} S \right| = \sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \sum_{|A|=3} |S_A| - \cdots$$

where

$$S_A = \bigcap_{i \in A} S_i$$

and

$$\sum_{|A|=k}$$

is a sum taken over all $A \subseteq \{1, 2, \dots, n\}$ of size k.

Proof. Let x be an element of the left hand side. We wish to prove that x is counted exactly once on the right hand side. Without loss of generality, let us rename the sets that x belongs to as $S_1, S_2, \dots, S_k$.

Then the number of sets A with $|A| = 1$ such that $x \in S_A$ is k. The number of sets A with $|A| = 2$ such that $x \in S_a$ is $\binom{k}{2}$, since we must choose two of the sets $S_1, \dots, S_k$, so there are $\binom{k}{2}$ ways to do this. So in general, the amount of A with $|A| = r$ with $x \in S_A$ is just $\binom{k}{r}$.

So the number of times x is counted on the right hand side is

$$k - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k+1}\binom{k}{k}$$

But $(1 + (-1))^k$ by the binomial expansion is

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k\binom{k}{k}$$

So the number of times x is counted on the right hand side is $1 - (1 + (-1))^k = 1 - 0 = 1$. □

6 Functions

6.1 Definition

For sets A and B, a function f from A to B is a rule that assigns to each $x \in A$ a unique value $f(x) \in B$. More precisely, a function from A to B is a set $f \subseteq A \times B$ such that for every $x \in A$, there is a unique $y \in B$ with $(x, y) \in f$. Of course therefore, if $(x, y) \in f$ then we can write $f(x) = y$. Here are some examples.

(i) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, or using an alternative notation, $x \mapsto x^2$ is a function.

(ii) A non-example is $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{1}{x}$ since it is undefined at $x = 0$.

(iii) Another non-example is $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \pm\sqrt{|x|}$ since it does not define a unique value in the output space for a given input, such as $x = 2$.

(iv) $f : \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & \text{otherwise} \end{cases}$$

is a function since it clearly satisfies the second definition. Note that even though we don't know if $e + \pi$ is rational or not, the function is still well defined since it produces a unique solution for $f(e + \pi)$, we just don't know which output value it gives.

(v) $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 3, 4\}$, and $f : A \to B$ is given by

$$\begin{aligned} f(1) &= 1 \\ f(2) &= 4 \\ f(3) &= 3 \\ f(4) &= 3 \\ f(5) &= 4 \end{aligned}$$

(vi) $A = \{1, 2, 3\}$, $f : A \to A$ is given by

$$\begin{aligned} f(1) &= 1 \\ f(2) &= 3 \\ f(3) &= 2 \end{aligned}$$

(vii) $A = \{1, 2, 3, 4\}$, $f : A \to A$ is given by

$$\begin{aligned} f(1) &= 1 \\ f(2) &= 3 \\ f(3) &= 3 \\ f(4) &= 4 \end{aligned}$$

(viii) $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3\}$, $f : A \to B$ is given by

$$\begin{aligned} f(1) &= 3 \\ f(2) &= 3 \\ f(3) &= 2 \\ f(4) &= 1 \end{aligned}$$

6.2 Injection, surjection and bijection

Definition. A function $f : A \to B$ is

- injective, if $\forall a, a' \in A$, we have $a \neq a' \implies f(a) \neq f(a')$, or equivalently, $f(a) = f(a') \implies a = a'$, or in words, 'different points stay different' (e.g. example 6 above).
- surjective, if $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$, or in words, 'everything in B is hit' (e.g. examples 6 and 8).
- bijective, if it is injective and surjective, or in words, 'everything in B is hit exactly once', or 'f pairs up elements of A and elements of B' (e.g. example 6, or $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$).

Definition. For a function $f : A \to B$, A is the domain, B is the range, and $\{b \in B : \exists a \in A \text{ s.t. } f(a) = b\}$ is the image.

We must always provide the domain and range of a function; a function's properties depend on this. For example, is the function f defined by $f(x) = f^2$ injective? If $f : \mathbb{N} \to \mathbb{N}$, then it is injective, but if $f : \mathbb{Z} \to \mathbb{Z}$, then it is not.

There are a number of properties that hold specifically for finite sets A, B:

(i) There is no surjection $A \to B$ if $|B| > |A|$.

(ii) There is no injection $A \to B$ if $|A| > |B|$.

(iii) For a function $f : A \to A$, f injective $\iff$ f surjective. Hence, if f is either injective or surjective, it is bijective.

(iv) There is no bijection from A to any proper subset of A.

As counterexamples for infinite sets:

(i) We define $f_0 : \mathbb{N} \to \mathbb{N}$ by $f_0(x) = x + 1$. Then, f_0 is injective but not surjective.

(ii) We define $f_1 : \mathbb{N} \to \mathbb{N}$ by $f_0(x) = x - 1$, or 1 if $x = 1$. Then, f_0 is surjective but not injective.

(iii) We define $g : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ by $g(x) = x + 1$. Then, g is bijective between $\mathbb{N}$ and a proper subset of $\mathbb{N}$.

We provide some more examples of functions.

(i) For any set X we have $1_X : X \to X$ defined by $1_X(x) = x$. This is known as the identity function on X.

(ii) For any set X, and $A \subset X$, we have an indicator function (or characteristic function) $\chi_A : X \to \{0, 1\}$ defined by

$$\chi_A(x) = \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases}$$

(iii) A sequence of reals $x_1, x_2, \ldots$ is a function $f : \mathbb{N} \to \mathbb{R}$ defined by $f(n) = x_n$.

(iv) The operation $+$ on $\mathbb{N}$ is a function $\mathbb{N}^2 \to \mathbb{N}$.

(v) A set X has size $n \iff$ there is a bijection between X and $\{1, 2, \ldots, n\}$.

6.3 Composition of functions

Given $f : A \to B$ and $g : B \to C$, we define the composition $g \circ f : A \to C$, given by $(g \circ f)(a) = g(f(a))$. For example, if $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$, $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x + 1$, then $(f \circ g)(x) = 2(x + 1)$, and $(g \circ f)(x) = 2x + 1$.

In general, the operation $\circ$ is not commutative, as we can see from this example. However, $\circ$ is associative. Given $f : A \to B$, $g : B \to C$, $h : C \to D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$. Indeed, for any input $x \in A$,

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$$

Thus $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ for every $x \in A$, so $h \circ (g \circ f) = (h \circ g) \circ f$.

6.4 Invertibility

We say that a function $f : A \to B$ is invertible if there exists some $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. For example $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x + 1$ has inverse $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \frac{x-1}{2}$. We can prove that this is correct by showing for all real numbers that $(g \circ f)(x) = x$ and vice versa as required.

As an example, consider $f_0 : \mathbb{N} \to \mathbb{N}$ given by $f_0(x) = x + 1$, and $f_1 : \mathbb{N} \to \mathbb{N}$ given by $f_1(x) = x - 1$ if $x \neq 1$ and 1 if $x = 1$. $f_1 \circ f_0 = 1_{\mathbb{N}}$ but $f_0 \circ f_1 \neq 1_{\mathbb{N}}$ because they disagree at 1. So we must check inverses both ways.

In fact, $f : A \to B$ is invertible if and only if it is a bijection.

- (forward implication) Let g be the inverse of f. It is surjective because $\forall b \in B$, we have $b = f(g(b))$. It is injective because given two elements a, a' such that $f(a) = f(a')$, we have $g(f(a)) = g(f(a')) = a = a'$ as required. So it is bijective.
- (backward implication) Suppose f is bijective. Let $g(b)$ be the unique point $a \in A$ with $f(a) = b$ for all $b \in B$. Then this g is the inverse of f.

6.5 Relations

A relation on a set X is a subset of $R \subseteq X \times X$. We usually write aRb to denote $(a, b) \in R$. Here are some examples.

(i) On $\mathbb{N}$, aRb if $a \equiv b$ (5). For example, $2R12$ but not $2R11$.

(ii) On $\mathbb{N}$, aRb if $a \mid b$.

(iii) On $\mathbb{N}$, aRb if $a \neq b$.

(iv) On $\mathbb{N}$, aRb if $a = b \pm 1$.

(v) On $\mathbb{N}$, aRb if $|a - b| \leq 2$.

(vi) On $\mathbb{N}$, aRb if either $a, b \leq 6$ or $a, b > 6$.

A relation may have a number of important properties:

- (reflexive) If $\forall x \in X$, xRx, e.g. examples 1, 2, 5, 6.
- (symmetric) If $\forall x, y \in X$, $xRy \implies yRx$, e.g. examples 1, 3, 4, 5, 6.

- (transitive) If $\forall x, y, z \in X$, $xRy, yRz \implies xRz$, e.g. examples 1, 2, 6.

An equivalence relation is a relation that is reflexive, symmetric and transitive. Examples 1, 6 above are equivalence relations. Here are some more examples.

(i) On $\mathbb{N}$, xRy if $x = y$.

(ii) Considering a partition of set X into subsets $C_1, C_2, \ldots, i \in I$ where the C_i are non-empty and disjoint, and their union is X. Then consider the relation aRb if $\exists i$ such that $a \in C_i$ and $b \in C_i$. aRb is an equivalence relation. In fact, all equivalence relations can be considered to be in this form; we will prove this shortly.

For an equivalence relation R on a set X, and $x \in X$, we define the equivalence class $[x] = \{y \in X : yRx\}$. In the first example 1 above, $[2] = \{y \in \mathbb{N} : y \equiv 2\ (5)\}$.

6.6 Equivalence classes as partitions

Proposition. Let R be an equivalence relation on a set X. Then the equivalence classes of R partition X.

Proof. Each equivalence class $[x]$ is non-empty, since $x = x$. Further,

$$\bigcup_{x \in X} = X$$

since $x \in [x]$ for all $x \in X$. Now we must show that the classes are disjoint, or are equal. Given x, y with $[x] \cap [y] \neq \emptyset$, we need to show that $[x] = [y]$. Choose some z such that $z \in [x] \cap [y]$. Then, zRx and zRy, so xRy. Thus for any t, $tRx \implies tRy$ due to transitivity, and $tRy \implies tRx$ for the same reason. So $[x] = [y]$. □

As an example, does there exist an equivalence relation on $\mathbb{N}$ with three equivalence classes, two of which are infinite, and one of which is finite? Yes—we can break up $\mathbb{N}$ into three parts, for example positive numbers, negative numbers and zero. This defines an equivalence relation.

6.7 Quotients

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

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

The map $q : X \to X/R$ given by $x \mapsto [x]$ is called the 'quotient map' or 'projection map'. As an example, on $\mathbb{Z} \times \mathbb{N}$, let us define $(a, b)R(c, d)$ to be true if $ad = bc$. This is an equivalence relation that demonstrates equivalence of rational numbers, where a, c are the numerators and b, d are denominators. Here, $\mathbb{Z} \times \mathbb{N}/R$ is a copy of $\mathbb{Q}$, associating $[(a, b)]$ with a/b. Then, $q : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ would map (a, b) to a/b.

7 Countability

7.1 Basic properties

We have a notion of 'size' for finite sets. Is there such an analogous notion for infinite sets? We will say that a set X is countable if X is finite, or it bijects with $\mathbb{N}$. Equivalently, we can list out the elements of the set, and each element will appear in the list. Here are some examples.

(i) Clearly any finite set is countable.

(ii) $\mathbb{N}$ is countable.

(iii) $\mathbb{Z}$ is countable, let us construct the list of numbers

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

It makes sense now to consider two sets to have the same size if they biject with each other.

Proposition. A set X is countable if and only if it injects into $\mathbb{N}$.

Proof. The forward implication is trivial: if X is finite, then there must be an injection in to $\mathbb{N}$, and if it bijects with $\mathbb{N}$ then that bijection is a valid injection. This encompasses both cases of countable sets.

Now let us consider the reverse implication. We may assume X is infinite, since if X is finite then by definition X is countable. We know that X injects onto $\mathbb{N}$ under some injective function f, so X bijects with $\operatorname{Im} f$. So it is enough to show that the image $\operatorname{Im} f$ is countable. We will now set a_1 to be the least element of $\operatorname{Im} f$, and a_2 to be the least element not equal to a_1, and so on. In general, $a_n = \min(\operatorname{Im} f \setminus \{a_i : 0 \leq i < n\})$. Then $\operatorname{Im} f$ is the set $\{a_1, a_2, \ldots\}$. There are no extra elements that we have not covered, since each $a \in X$ is a_n for some n, because $a = a_n, n \leq a$. So we have listed elements of $\operatorname{Im} f$, so $\operatorname{Im} f$ is countable, so X is countable. □

Thus, we can view countability as being 'at most as large as $\mathbb{N}$'. For instance, any subset of a countable set is also countable.

Remark. In $\mathbb{R}$, let

$$X = \left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots\right\} \cup \{1\}$$

Then X is countable, as we can list it as

$$1, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots$$

But if we counted from 'least element' to 'most element', we would never reach the element 1 in countable time. Note further that if we find it difficult to construct a list for a set, it does not mean it is uncountable, it could just mean that we haven't found the right list yet.

7.2 Products of countable sets

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

Proof 1. We will define $a_1 = (1,1)$, and inductively define

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

where $a_{n-1} = (p,q)$. Therefore, we are essentially moving across antidiagonals of the plane. This does hit every point $(x,y) \in \mathbb{N} \times \mathbb{N}$, for example by induction on $x+y$, so we have listed all elements of $\mathbb{N} \times \mathbb{N}$. □

Proof 2. If we can define an injective function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, then it is countable. For example, let $f = 2^x 3^y$. f is injective, so $\mathbb{N} \times \mathbb{N}$ is countable. □

7.3 Countable unions of countable sets

Proof 2 is also a way to show the following theorem:

Theorem. Let $A_1, A_2, A_3, \ldots$ be countable sets. Then $A_1 \cup A_2 \cup A_3 \cup \ldots$ is countable. Less formally, 'a countable union of countable sets is countable'.

Proof. For each i, A_i is countable, so we can list A_i as $a_{i1}, a_{i2}, a_{i3}, \ldots$ which may or may not terminate. We can then define

$$f : \bigcup_{n \in \mathbb{N}} A_n \to \mathbb{N}; \quad f(x) = 2^i 3^j$$

where $x = a_{ij}$. If x is in more than one set, just take the least i that is valid. Then f is an injection so the union is countable. □

Here are some examples of using this theorem by partitioning sets as a countable union of countable subsets.

(i) $\mathbb{Q}$ is countable, since it is a countable union of countable sets:

$$\mathbb{Q} = \mathbb{Z} \cup \frac{1}{2}\mathbb{Z} \cup \frac{1}{3}\mathbb{Z} \cup \ldots$$

Each $\frac{1}{n}\mathbb{Z}$ is countable, since they biject with $\mathbb{Z}$ which is a countable set. It doesn't matter if we've counted an element in $\mathbb{Q}$ twice; the above theorem works even with intersecting sets.

(ii) The set $\mathbb{A}$ of all algebraic numbers is countable. It is enough to show that the set of integer polynomials is countable, since each polynomial has a finite amount of roots and then $\mathbb{A}$ is a countable union of finite sets. Now, to show that the set of integer polynomials is countable, it is enough to show that for each degree d it is countable, since it is a countable union of all polynomials of degree d (again using the above theorem). To specify a polynomial of degree d you must name its coefficients, so this set injects into $\mathbb{Z}^{d+1}$, so we must just show that $\mathbb{Z}^{d+1}$ is countable (not a bijection since the first term of the polynomial must be nonzero). We know that $\mathbb{Z}^n$ is countable because we can inductively show that $\mathbb{Z}^2, \mathbb{Z}^3, \mathbb{Z}^4, \ldots$ are countable inductively.

7.4 Uncountable sets

Definition. A set is uncountable if there is no way to count the set.

Theorem. $\mathbb{R}$ is uncountable.

Proof (Cantor's Diagonal Argument). We will show that $(0,1)$ is uncountable, then clearly $\mathbb{R}$ is uncountable. Suppose $(0,1)$ is countable. Then given a sequence $r_1, r_2, \ldots$ in $(0,1)$, we just need to find some number $s \in (0,1)$ not contained within this sequence. For each r_n, we have a decimal expansion $r_n = 0.r_{n1}r_{n2}r_{n3}\ldots$. Let us now write all of these numbers in a matrix-style form:

$$\begin{aligned} r_1 &= 0.r_{11}r_{12}r_{13}\ldots \\ r_2 &= 0.r_{21}r_{22}r_{23}\ldots \\ r_3 &= 0.r_{31}r_{32}r_{33}\ldots \\ &\vdots \end{aligned}$$

We just need to construct some number s that is not in this list. So, let us simply make sure that for any given r value, there is at least one digit that does not match. The easiest way to construct such a number is

$$s = 0.s_1s_2s_3\ldots$$

where $s_1 \neq r_{11}$, $s_2 \neq r_{22}$, $s_3 \neq r_{33}$ and so on. We can pick any numbers we like according to these constraints, but we should avoid picking digits 0 and 9 since $0.1000\cdots = 0.0999\ldots$ for example, which could cause unnecessary ambiguity. Then $s \neq r_1, s \neq r_2, \ldots$ since there is at least one mismatched digit in the expansion for each r_i; they differ in decimal digit i. So $\mathbb{R}$ is uncountable. □

This is another proof that transcendental numbers exist. $\mathbb{R}$ is uncountable and $\mathbb{A}$ is countable, so there exists a transcendental number. Indeed, 'most' numbers are transcendental, i.e. $\mathbb{R} \setminus \mathbb{A}$ is uncountable (because if $\mathbb{R} \setminus \mathbb{A}$ were countable, then $\mathbb{R}$ would be $(\mathbb{R} \setminus \mathbb{A}) \cup \mathbb{A}$ which is a finite union of countable sets #).

Theorem. The power set $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof. Suppose the subsets of $\mathbb{N}$ are listed as $S_1, S_2, S_3, \ldots$ then we want to construct another set S that is not equal to any of the other sets S_i. So for each set S_i, we must ensure that S and S_i differ for at least one value. An easy way to do this is to include the number i in the subset if S_i does not contain the number, and to exclude i if $i \in S_i$. Then S differs from S_i at position i. This is the same logic as the diagonal argument above. We have:

$$S = \{n \in \mathbb{N} : n \notin S_n\}$$

So S is not on the list $S_1, S_2, S_3, \ldots$ no matter what way we choose to list the elements, so $\mathcal{P}(\mathbb{N})$ is uncountable. □

Remark. Alternatively, we could just inject $(0,1)$ into $\mathcal{P}(\mathbb{N})$. For example, consider $x \in (0,1)$ represented as $0.x_1x_2x_3x_4\ldots$ in binary where the $x_1, x_2, \ldots$ are zero or one (not ending with an infinite amount of 1s). We can convert this x into a subset of $\mathbb{N}$ by considering the set $\{n \in \mathbb{N} : x_n = 1\}$. Then the uncountability follows.

In fact, our proof of this theorem shows the following.

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

For example, $\mathbb{R}$ does not biject with $\mathcal{P}(\mathbb{R})$. The proof in fact will show that there is no surjection from X to its power set; i.e. the power set is 'larger' than X.

Proof. Given any function $f : X \to \mathcal{P}(X)$, we will show f is not surjective. Let $S = \{x \in X : x \notin f(x)\}$. Then S does not belong to the image of f because they differ at element x; for all x we have $S \neq f(x)$. □

Remark. Note that:

(i) This is similar in some sense to Russell's paradox.

(ii) This theorem gives another proof that there is no universal set $\mathcal{E}$, since its power set $\mathcal{P}(\mathcal{E}) \subseteq \mathcal{E}$. But of course, there is always a surjection from a set to a subset. This is a contradiction.

Example. Let $A_i, i \in I$ be a family of open, pairwise disjoint intervals. Must this family be countable? Note that it is not as simple as just listing from left to right, for example consider

$$\left(\frac{1}{2}, 1\right), \left(\frac{1}{3}, \frac{1}{2}\right), \left(\frac{1}{4}, \frac{1}{3}\right), \ldots, (-1, 0)$$

Then the leftmost interval is $(-1, 0)$, but there is no 'next interval' just after it. Also consider

$$\left(0, \frac{1}{2}\right), \left(\frac{1}{2}, \frac{2}{3}\right), \left(\frac{2}{3}, \frac{3}{4}\right), \ldots, (1, 2)$$

Then we can list the first infinitely many intervals, but we will never reach $(1, 2)$. The answer turns out to be true; the family is countable. Here are two important proofs.

Proof 1. Each interval A_i contains a rational number a_i. The rationals $\mathbb{Q}$ are countable. So let us just list the a_i. The family is therefore countable. □

Proof 2. $\{i \in I : A_i \text{ has length } \leq 1\}$ is certainly countable, since it injects into $\mathbb{Z}$ (here, as all A_i contain some integer). Further, $\left\{i \in I : A_i \text{ has length } \leq \frac{1}{2}\right\}$ is countable for the same reason. Essentially, for all n, $\left\{i \in I : A_i \text{ has length } \leq \frac{1}{n}\right\}$ is countable. We have written all the intervals as a countable union (over n) of countable sets. □

To summarise, if we want to show a set X is uncountable:

(i) Run a diagonal argument; or

(ii) Inject an uncountable set into X

To show a set X is countable:

(i) List all the elements (usually fiddly); or

(ii) Inject X into $\mathbb{N}$ (or another countable set); or

(iii) Express X as a countable union of countable sets (usually the best); or

(iv) If X is 'in' or 'near' $\mathbb{R}$, consider $\mathbb{Q}$ (see Proof 2 above).

7.5 Comparing sizes of sets

Intuitively, we might think that:

- 'A bijects with B' means 'A has the same size as B'.
- 'A injects into B' means 'A is at most as large as B'.
- 'A surjects onto B' means 'A is at least as large as B'.

Of course, these analogies break down where B is zero, since there are no functions from A to B in this case. For these to make sense, we require (for $A, B \neq \varnothing$) 'A injects into B' to be true if and only if 'B surjects onto A', and vice versa.

- In the forward direction, we are given an injection $f : A \to B$. Pick some point a_0 in A, and define a surjective function $g : B \to A$ given by

$$b \mapsto \begin{cases} a & \text{if } \exists!\ a \in A, f(a) = b \\ a_0 & \text{otherwise} \end{cases}$$

  Since the mapping f is injective, the first case will always provide a unique value of a.

- Proving the converse, we are given a surjection $g : B \to A$. For each a in A, we have some $a' \in B$ with $g(a') = a$ since g is a surjection. Let $f(a) = a'$ for each $a \in A$, and f is injective.

7.6 Schröder–Bernstein theorem

Further, we must also have that if 'A is at most as large as B' and 'B is at most as large as A', then they must be the same size. Otherwise this size intuition would not make sense.

Theorem (Schröder–Bernstein Theorem)**.** If $f : A \to B$ and $g : B \to A$ are injections, then there exists a bijection $h : A \to B$.

Proof. For $a \in A$, we will write $g^{-1}(a)$ to denote the unique $b \in B$ such that $g(b) = a$, if such a b exists (and similarly for $f^{-1}(b)$). The 'ancestor sequence' of $a \in A$ is

$$g^{-1}(a), f^{-1}g^{-1}(a), g^{-1}f^{-1}g^{-1}(a), \ldots$$

which may terminate. So for any ancestor, after undergoing the relevant function f or g repeatedly, we will end up at a. There are three possible behaviours:

- Let A_0 be the subset of A such that the ancestor sequence stops at even time, i.e. the last ancestor is in A;
- Let A_1 be the subset of A such that the ancestor sequence stops at odd time, i.e. the last ancestor is in B; and
- Let A_∞ be the subset of A such that the ancestor sequence does not terminate.

We specify 0 to be even, i.e. if $a \in A$ has no ancestor $g^{-1}(a)$, then $a \in A_0$. We define similar subsets of B: B_0, B_1, B_∞. Now:

- $f : A \to B$ is a bijection between A_0 and B_1. Clearly if some element a has an even number of ancestors, the ancestors of $f(a)$ are exactly a and all of its ancestors, i.e. an odd number. It is surjective because every element in B_1 has an inverse $f^{-1}(b) \in A_0$ by construction.

- $g : B \to A$ is a bijection between B_0 and A_1 due to the same argument.
- f (or g, both functions work for this proof) bijects A_∞ and B_∞. It is surjective because for every element $b \in B$, it has some ancestor $f^{-1}(b) \in A_\infty$.

So the function $h : A \to B$ is given by

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

is a bijection. □

Let us consider an example of this theorem in action. Do $[0, 1]$ and $[0, 1] \cup [2, 3]$ biject? All we need is to find an injection both ways.

- Let $f : [0, 1] \to [0, 1] \cup [2, 3]$ be the identity map $f(x) = x$.
- Let $g : [0, 1] \cup [2, 3] \to [0, 1]$ be given by $g(x) = x/3$.

It would also be nice to have that, for any sets A and B, either A injects into B or B injects into A. Then we can create a total ordering, rather than a partial ordering; we can compare any two sets. This is proven to be true in the Part II course Logic and Set Theory.

7.7 Arbitrarily large sets

We have the sets

$$\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \dots, \mathcal{P}^k(\mathbb{N}), \dots$$

Does every set X inject into one of those? It seems like this might be true, but the set

$$X = \mathbb{N} \cup \mathcal{P}(\mathbb{N}) \cup \mathcal{P}(\mathcal{P}(\mathbb{N})) \cup \dots$$

is a counterexample. Let us continue further with this approach.

$$X' = X \cup \mathcal{P}(X) \cup \mathcal{P}(\mathcal{P}(X)) \cup \dots$$

$$X'' = X' \cup \mathcal{P}(X') \cup \mathcal{P}(\mathcal{P}(X')) \cup \dots$$

and so on. Now, does every set inject into one of these sets? No, consider

$$Y = X \cup X' \cup X'' \cup X''' \cup \dots$$

We can keep going forever. So we can't construct a set that all sets inject into.

7.8 What happens next?

This is the end of the Numbers and Sets course. Here are a few of the courses that feed from this course.

- Factorisation is taken further in the IB Groups, Rings and Modules course.
- Fermat's Little Theorem, squares modulo p etc. are taken further in II Number Theory.
- The analysis chapter is extended by IA Analysis.
- Countability and sizes of sets are taken further in the II Logic and Set Theory course.