Numbers & Sets

Hasan Baig

Michaelmas 2020

Contents

0 Proofs

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

We prove things for two reasons
(i) To be sure they are true.
(ii) To understand why they are true.

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

Proof. For any positive integer n:
Have $n^3 - n = n(n^2 - 1) = (n-1)n(n+1)$
but 1 of $n-1, n, n+1$ is a multiple of 3, as they are 3 consecutive integers. □

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

Proof (False)**.** Given a positive integer n that is even:
have $n = 2k$, some integer k.
Thus $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, so n is even. □

Rubbish, we wanted: if A then B but showed if B then A.

Proof (True)**.** Suppose n odd: so $n = 2k+1$, some integer k then

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

so n^2 odd ※
thus n even. □

Note. Claim true because of properties of odd numbers.

To show "if A then B", we showed there is no case where A is true and B is false.
To show $A \implies B$: same as showing not $B \implies$ not A. $A \implies B$ means can't have A true, B, false.
Not $B \implies$ not A means can't have B false, A true.

Claim. Solution of real equation $x^2 - 5x + 6 = 0$ is: $x = 2$ or $x = 3$

This is really 2 assertions:
i) $x = 2$ & $x = 3$ are solutions of $x^2 - 5x + 6 = 0$.
ii) There are no other solutions
equivalently:
i) $x = 2$ or $x = 3 \implies x^2 - 5x + 6 = 0$
ii) $x^2 - 5x + 6 = 0 \implies x = 2$ or $x = 3$

Proof. if $x = 2$ or $x = 3$:
Have $x - 2 = 0$ or $x - 3 = 0$
so $(x - 2)(x - 3) = 0$
ie $x^2 - 5x + 6 = 0$

if $x^2 - 5x + 6 = 0$:
have $(x - 2)(x - 3) = 0$ so $x - 2 = 0$ or $x - 3 = 0$
ie $x = 2$ or $x = 3$ □

Proof (Alternative)**.**

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

Claim. Every positive real is at least 1

Proof (False)**.** Let x be the smallest real: want $x = 1$. (this is nonsense)
if $x < 1$: then $x^2 < x$ ※
if $x > 1$: $\sqrt{x} < x$ ※
Thus x = 1 □

Moral. Every line in a proof must be justified.

1 Elementary Number Theory

Intuitively: the natural numbers written $\mathbb{N}$, consist of:
$1, 1 + 1, 1 + 1 + 1, 1 + 1 + 1 + 1, \ldots$
We want to make this precise.

Definition (Peano Axioms)**.** What we assume: natural numbers $\mathbb{N}$, is a set containing an element '1' with an operation '+1' satisfying:
(i) $\forall n : n + 1 \neq 1$
(ii) If $m \neq n$ then $m + 1 \neq n + 1$
(iii) For any property $P(n)$: If $P(1)$ true and $\forall n\, P(n) \implies P(n+1)$ then $P(n) \forall n$ (induction axiom)

Take $P(n)$ ='n is on that list '
Can write 2 for $1+1$ etc.
have operation '$+2$' by '$n+2=(n+1)+1$
In fact, can define '$+k$' for every number k by induction (Take $P(k)$ to be statement " '$+k$' is defined')
Similarly can define multiplication, powers etc.

Can check usual rules of arithmetic
(i) $\forall a,b: a+b=b+a$
(ii) $\forall a,b: ab=ba$
(iii) $\forall a,b,c: a+(b+c)=(a+b)+c$
(iv) $\forall a,b,c: a(bc)=(ab)c$
(v) $\forall a,b,c: a(b+c)=(ab)+(ac)$

Definition. $a<b$ if $a+c=b$ for some c.

Can check:
(vi) $\forall a,b: a<b \implies a+c<b+c$
(vii) $\forall a,b: a<b \implies ac<bc$
(viii) $\forall a,b,c: a<b, b<c \implies a<c$
(ix) $\forall a:$ NOT $a<a$

1.1 A more useful form of induction

Induction says: if $P(1)$ and $\forall n: P(n) \implies P(n+1)$, then $P(n)\,\forall n$.
A more useful form is strong induction: if $P(1)$ and $\forall n: P(m)\,\forall m \le n \implies P(n+1)$, then $P(n)\,\forall n$.
To deduce from ordinary induction, apply ordinary induction to $Q(n)$ where $Q(n)$ is '$P(m)\,\forall m \le n$.'

Remarks.
(i) Technically don't need to check $P(1)$ separately as implied by condition if interpreted suitably but is safer to check P(1).
(ii) Normally, to prove $P(n)\forall n$, take an n and show $P(n)$. Strong induction says: if it would help to assume $P(m)$ for some $m \le n$, feel free to do so.

Two equivalent forms of (strong) induction:
(i) If $P(n)$ false for some n, then for some n, $P(n)$ false but $P(m)$ true $\forall m < n$. 'If there is a counterexample, then there is a minimal counterexample'.
(ii) If $P(n)$ for some n then there is a least n with $P(n)$ - well-ordering principle.

1.2 Integers

Integers written $\mathbb{Z}$ consist of all symbols $n, -n$ (n a natural number) and 0.
Can define $+$ and $\cdot$ etc. on $\mathbb{Z}$ from $\mathbb{N}$
Plus:

$$\forall a : a + 0 = a$$

$$\forall a \, \exists b \text{ s.t. } a + b = 0$$

Define $a < b$ if $\exists c \in \mathbb{N}$ with $a + c = b$. All previous rules still hold except 1 change,

$$\forall a, b, c \in \mathbb{Z} : \text{ if } a < b \text{ and } c > 0 \text{ then } ac < bc$$

1.3 Rationals

Rationals written $\mathbb{Q}$ consist of all expressions $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ with $b \neq 0$ with $\frac{a}{b}$ regarded the same as $\frac{c}{d}$ if $ad = bc$.
Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
We can check it does not matter how we write $\frac{a}{b}$ and $\frac{c}{d}$.

Note. Cannot define operation on $\mathbb{Q}$ by sending $\frac{a}{b}$ to $\frac{a^2}{b^2}$ as $\frac{1}{2}$ and $\frac{2}{4}$ go to different places.

Similarly for $\cdot$ can check all usual algebraic rules.
Also $\forall a \neq 0 \exists b$ s.t. $ab = 1$
Define $\frac{a}{b} < \frac{c}{d}$ if $ad < bc$
Can check all rules for $\mathbb{Z}$ still hold.
Can view $\mathbb{Z}$ as living inside $\mathbb{Q}$ by identifying a in $\mathbb{Z}$ with $\frac{a}{1}$ in $\mathbb{Q}$

1.4 Primes

Structure of $\mathbb{N}$ under $+$ easy: start at 1, keep doing '+1' but more complicated under $\cdot$
For a natural number n, multiples of n are all integers kn for some integer k e.g. $2n, 3n, -5n, 0$ are all multiples of n.
if m is a multiple of n, can say n divides m or n is a divisor of m or n is a factor of m or $n|m$ 'n divides m'.

Definition. A natural number $n \geq 2$ is **prime** if its only divisors are $1, n$. e.g. 7,11, not 14 as $14 = 2 \cdot 7$.
Aim: break up each number into primes. E.g. $63 = 3 \cdot 3 \cdot 7$

Prop 1.1. Every natural number $n \geq 2$ is expressible as a product of primes.

Proof. induction on n: $n = 2$✓
given $n > 2$:
if n prime: ✓
if n composite: have $n = ab$, some $1 < a, b < n$
So by induction have:

$$a = p_1 p_2 p_3 \dots p_k$$

$$b = q_1 q_2 q_3 \dots q_l$$

some primes $p_1, p_2, p_3 \dots p_k, q_1, q_2, q_3, \dots q_l$
hence $ab = p_1 p_2 p_3 \dots p_k q_1 q_2 q_3 \dots q_l$✓✓✓□

Remark. Can define an empty product (i.e. of no primes) to equal 1. If so, then prop 1 could start at 1.

Theorem 1.2. There are infinitely (i.e. not finitely many) primes

Proof. Suppose not: let $p_1, \dots, p_k$ be all the primes.
Let $n = p_1 p_2 \dots p_k + 1$
Then n has no prime factor (as none of $p_1, \dots, p_k$ divide it)
Contradicting the fact that n may be expressed as a product of primes (prop 1.1) ※□

Remark. There is no 'pattern' to the primes: no (algebraic) formula for the n^{th} prime.

Want: prime factorisation of a number is unique (up to reordering).
Why is that? Why can't we have $41 \cdot 101 = 47 \cdot 73$?
We would need $p|ab \implies p|a$ or $p|b$ (for p prime)
We do need p prime, e.g. $6|8 \cdot 9$ but $6 \nmid 8$ and $6 \nmid 9$.
Should '$p|ab \implies p|a$ or $p|b$' be easy or hard?
It cannot be easy ('straight from definitions') because it is about primes dividing things whereas definition of prime is about things dividing it so it is the wrong way round!

1.5 Highest Common Factors

Definition. For a, b natural numbers, $c \in \mathbb{N}$ is the **HCF** of a and b if:
i) $c|a, c|b$ ('c is a common factor of a and b')
ii) if $d|a, d|b$ then $d|c$ ('every common factor divides c')
[e.g. 18 has factors: 1, 2, 3, 6, 9, 18
12 has factors: 1, 2, 3, 4, 6, 12
so common factors 1, 2, 3, 6
Thus hcf = 6]
so the hcf(if it exists) is the greatest of all common factors
but if a and b have common factors 1,2,3,4,6 then a & b would not have an hcf.
Aim: hcf always exists.
We will need:

Prop 1.3. (Division algorithm): Let n, k be natural numbers. Then, can write $n = qk + r$ where $q, r \in \mathbb{Z}$ with $0 \leq r \leq k - 1$

Proof. Induction on n: $n = 1$✓
Given $n > 1$,
have $n - 1 = qk + r$ for some integers q, r with $0 \leq r \leq k - 1$
if $r < k - 1$, have $n = qk + (r + 1)$
if $r = k - 1$, have $n = (q + 1)k$✓ □

1.6 Euclid's Algorithm

This will both prove hcf exists and give an efficient way to calculate the hcf.
For finding hcf of a & b (say $a \geq b$)

Method.

General	For $a = 372, b = 162$
Write $a = q_1 b + r_1 (q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < b)$	$372 = 2 \cdot 162 + 48$
Write $b = q_2 r_1 + r_2 (q_2, r_2 \in \mathbb{Z}, 0 \leq r_2 < r_1)$	$162 = 3 \cdot 48 + 18$
Write $r_1 = q_3 r_n + r_3 (q_3, r_3 \in \mathbb{Z}, 0 \leq r_3 < r_2)$	$48 = 2 \cdot 18 + 12$
...	$18 = 1 \cdot 12 + 6$
Continue until $r_{n-1} = q_{n+1} r_n + r_{n+1}$ with $r_{n+1} = 0$, output r_n	$12 = 2 \cdot 6$, output 6

Note. Terminates (in $\leq b$ steps since $b > r_2 > r_2 > \dots$)

Theorem 1.4. The output of Euclid's algo on a, b is hcf of a, b.

Proof.

i) have $r_n | r_{n-1}$ (as $r_{n+1} = 0$)
so $r_n | r_{n-2}$ (from 2nd last line)
so $r_n | r_i \forall i$ (inductively)
so $r_n | b$ (2nd line)
so $r_n | a$ (1st line)

ii) given d with $d|a, d|b$:
have $d | r_1$ (1st line)
so $d | r_2$ (2nd line)
and $d | r_i \forall i$ (inductively)
so in particular $d | r_n$✓□

e.g. hcf 87, 52: run Euclid:

$$87 = 1 \cdot 52 + 35$$
$$52 = 1 \cdot 35 + 17$$
$$35 = 2 \cdot 17 + 1$$
$$17 = 17 \cdot 1 + 0$$

so hcf(87, 52) is 1, or (87, 52) = 1 or say 87, 52 are coprime.

Definition (Coprime)**.** Two numbers a, b are **coprime** if $\text{hcf}(a, b) = 1$.

Can we write $1 = 87x + 52y$ some $x, y \in \mathbb{Z}$?
Have:

$$\begin{aligned} 1 &= 1 \cdot 35 - 2 \cdot 17 \text{ (from } 3^{\text{rd}} \text{ line)} \\ &= 1 \cdot 35 - 2(52 - 35) \text{ (from } 2^{\text{nd}} \text{ line)} \\ &= -2 \cdot 52 + 3 \cdot 35 \\ &= -2 \cdot 52 + 3 \cdot (87 - 52) \\ &= 3 \cdot 87 - 5 \cdot 52 \checkmark \end{aligned}$$

Theorem 1.5.

$$\forall a, b \in \mathbb{N}\, \exists x, y \in \mathbb{Z} \text{ s.t. } xa + yb = \text{hcf}(a, b)$$

'Can write hcf as a linear combination of a and b.'

Proof (1^{st})**.** Run Euclid on a, b, say with output r_n
Have $r_n = xr_{n-1} + yr_{n-2}$ some $x, y \in \mathbb{Z}$
But r_{n-1} expressible as $xr_{n-2} + yr_{n-3}$ some $x, y \in \mathbb{Z}$
Whence, $r_n = xr_{n-2} + yr_{n-3}$ some $x, y \in \mathbb{Z}$
Continue: we obain $\forall i : r_n = xr_i + yr_{i-1}$, some $x, y \in \mathbb{Z}$ (inductively)
Thus $r_n = xa + yb$, some $x, y \in \mathbb{Z}$ (from line 2 and then line 1)

Note. Euclid is showing x, y exist & gives a way to actually find then

Proof (2^{nd})**.** Let h be least positive linear combination of a & b

Claim. $h = \text{hcf}(a, b)$

Proof. ii) given $d|a, d|b$: have $d|(xa + yb)\, \forall x, y \in \mathbb{Z}$ and in particular $d|h$
i) suppose $h \nmid a$, then $a = qh + r$, some $q, r \in \mathbb{Z}$ with $0 < r < h$
$\implies r = a - qh = a - q(xa + yb)$ is also a linear combination ※
Thus $h|a$ and similarly $h|b$ ✓✓□

Note. 2^{nd} proof doesn't show how to find

Application: solving integer linear equations
Suppose $a, b \in \mathbb{N}$, when can we solve $ax = b, x \in \mathbb{Z}$? (if $x \in Q$ allowed, always yes)
Answer: $\iff a|b$
What about $(ax + by)|c$?
e.g. $320x + 72y = 33$? no as LHS even, RHS odd.
$87x + 52y = 33$? yes as we have $87x + 52y = 1$ (some $x, y \in \mathbb{Z}$) and multiply up.

Corollary 1.6. Let $a, b, c \in N$ then the equation $ax + by = c$ has an integer solution $\iff \text{hcf}(a, b)|c$.

Proof. let $h = \text{hcf}(a, b)$
$\implies$: have $ax + by = c$, some $x, y \in \mathbb{Z}$ but $h|a, h|b$, so $h|(ax + by)$ ✓
$\impliedby$: have $h = ax + by$ some $x, y \in \mathbb{Z}$.
multiply by $\frac{c}{h}$:

$$c = a(x \cdot \frac{c}{h}) + b(y \cdot \frac{c}{h})$$

Remark. Corollary 6 sometimes called Bezout's Theorem.

Lemma 1.7. Let p be a prime and $a, b \in \mathbb{Z}$ then $p|ab \implies p|a$ or $p|b$.

Proof. Suppose $p \nmid a$: want $p|b$.
Then $\text{hcf}(p, a) = 1$,
so $px + ay = 1$, some $x, y \in \mathbb{Z}$
so $pbx + aby = b$
whence b is a multiple of p as each of pbk and aby are.

Remark. Similarly, $p|a_1 a_2 \dots a_n \implies p|a_i$ some i. Lemma 1.7 tells us $p|a_1$ or $p|a_2 a_3 \dots a_n$ and can show remark holds. Also, we do need p prime.

Theorem 1.8 (Fundamental Theorem of Arithmetic)**.** Every natural number $n \geq 2$ is expressible as a product of primes uniquely up to reordering.

Proof. Existence: prop 1
Uniqueness: induction on $n : n = 2$ ✓
Given $n > 2$: suppose $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$, where p_i, q_i primes.
Task: $k = l$ and after reordering $p_i = q_i \, \forall i$
Have: $p_1 | q_1 q_2 \dots q_l$, so $p_1 | q_i$ some i.
Reorder; we may assume $p_1 | q_1$ hence $p_1 = q_1$ as q_1 prime.
So $\frac{n}{p_1} = p_2 \dots p_k = q_2 \dots q_l$ thus $k = l$ and $p_2 = q_2, p_3 = q_3 \dots p_k = q_k$ (induction) ✓✓□

Digression: in Theorem 1.8, took the 'things that cannot be broken up' (the primes), and broke up each number as a product of these uniquely.
Consider instead $\mathbb{Z}[\sqrt{-3}]$ meaning all complex numbers of form $x + y\sqrt{-3}$ where $x, y \in \mathbb{Z}$ e.g. $2 + t\sqrt{-3}, 1 - 4\sqrt{-3}, 7, \sqrt{-3}$.
Can add/ multiply any 2 elements of $\mathbb{Z}[\sqrt{-3}]$, staying inside $\mathbb{Z}[\sqrt{-3}]$.

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

So unique factorisation fails in $\mathbb{Z}[\sqrt{-3}]$.

1.7 Application of the Fundamental Theorem of Arithmetic

1.7.1 Factors

What are factors of $2^3 \cdot 3^7 \cdot 11$?
Certainly any $2^a 3^b 11^c$, $0 \leq a \leq 3, 0 \leq b \leq 7, 0 \leq c \leq 1$ is a factor.
No others - e.g. if $7|n = 2^3 \cdot 3^7 \cdot 11$, then we'd get a prime factorisation of n involving 7 - contradicting uniqueness of prime factorisation.
So the factors of $n = p_1^{a_1} \dots p_k^{a_k}$ are precisely all numbers $p_1^{b_1} \dots p_k^{b_k}$, $0 \leq b_i \leq a_i \, \forall i$.

1.7.2 HCFs

Common factors of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$ are all $2^a \cdot 3^b \cdot 11^c$, $0 \leq a \leq 3, 0 \leq b \leq 2, 0 \leq c \leq 1$ so hcf is $2^3 \cdot 3^2 \cdot 11$.
In general, HCF of $p_1^{a_1} \dots p_k^{a_k}$ and $p_1^{b_1} \dots p_k^{b_k} (a_k, b_k \geq 0)$ is: $p_1^{\min(a_1,b_1)} \dots p_k^{\min(a_k,b_k)}$.

1.7.3 LCMs

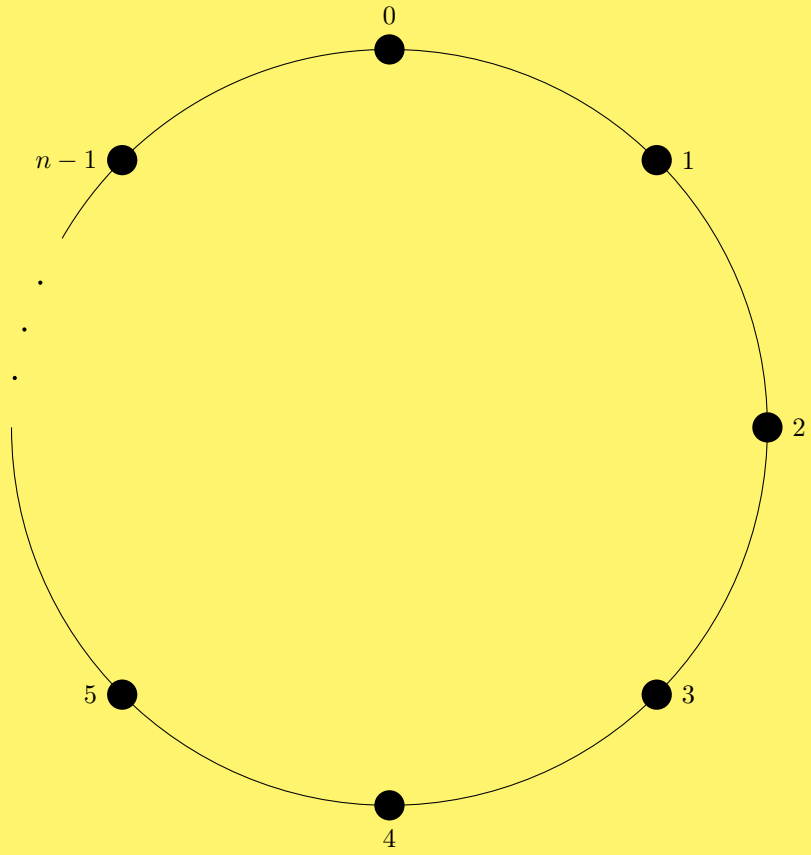
Definition. Common multiples of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$ are all $2^a \cdot 3^b \cdot 11^c \cdot 13^e \cdot$anything where $a \geq 4, b \geq 7, c \geq 1, d \geq 3, e \geq 1$ so $2^4 \cdot 3^7 \cdot 5^1 \cdot 11^3 \cdot 13^1$ is a common multiple and every common multiple is a multiple of it.
We say it is the **LCM** or **Least Common Multiple** of our 2 numbers.
In general, LCM of $p_1^{a_1} \dots p_k^{a_k}$ and $p_1^{b_1} \dots p_k^{b_k} (a_k, b_k \geq 0)$ is: $p_1^{\max(a_1,b_1)} \dots p_k^{\max(a_k,b_k)}$.
Amusing consequence: $\text{hcf}(x, y)\ \text{lcm}(x, y) = xy$. Indeed because $\min(a, b) + \max(a, b) = a + b$, $\forall a, b \in \mathbb{Z}$.

1.8 Modular arithmetic

Definition. Let $n \geq 2$, be a natural number, the **integers mod n**, written $\mathbb{Z}_n$ consist of the integers with two regarded as the same if they differ by a multiple of n.
e.g. in $\mathbb{Z}_7$, 2 is the same as 16.
If x and y are the same in $\mathbb{Z}_n$, can write:
$x \equiv y \pmod{n}$
or $x \equiv y\,(n)$
or $x = y$ in $\mathbb{Z}_n$

$$\text{thus } x \equiv y\,(n) \iff x - y \text{ is a multiple of } n$$
$$\iff x = y + kn, \text{ some } k \in \mathbb{Z}$$

Note. No two of $0, 1, \ldots, n-1$ are congruent mod n and every x is congruent to one of them mod n (division algorithm). So can view $\mathbb{Z}_n$ as:



Do + and × make sense in $\mathbb{Z}_n$?

Note. Even or odd does not work same e.g. $2 \equiv 9\,(7)$

Would need if $a \equiv a'\,(n)$ and $b \equiv b'\,(n)$ then $a+b = a'+b'\,(n)$ and $ab = a'b'\,(n)$
$a' = a + kn$, $k \in \mathbb{Z}$
$b' = b + jn$, $j \in \mathbb{Z}$
so $a' + b' = a + b + (k+j)n \equiv a + b\,(n)$
$a'b' = (a+kn)(b+jn) = ab + (kb + aj + kjn)n \equiv ab\,(n)$✓
All usual rules of arithmetic inherited from $\mathbb{Z}$:
e.g. do have $a + b \equiv b + a\,(n)$, since $a + b = b + a$ in $\mathbb{Z}$.
Some things already done are expressible in modular arithmetic.
e.g. '$p|ab \implies p|a$ or $p|b$ (p prime)' is exactly saying:
$ab \equiv 0\,(p) \implies a \equiv 0\,(p)$ or $b \equiv 0\,(p)$ (in $\mathbb{Z}$ the line)
or equivalently:
In $\mathbb{Z}_p : ab = 0 \implies a = 0$ or $b = 0$ (in $\mathbb{Z}_p$ the circle)

1.8.1 Inverses

For $a, b \in \mathbb{Z}_n$, say b is an inverse of a if $ab = 1$
e.g. in $\mathbb{Z}_{10}$, inverse of 3 is 7. Inverse of 4 does not exist as $\forall x \in \mathbb{Z} : 4x \not\equiv 1\,(10)$ since $4x$ is even.

Note.
(i) if inverse exists, it is unique.
Suppose in $\mathbb{Z}_n$, have $ab = ac = 1$, then $b(ab) = b(ac) \implies 1 \cdot b = 1 \cdot c \implies b = c$
(ii) if a is invertible in $\mathbb{Z}_n$, can write a^{-1} for inverse.
(iii) can 'cancel' an invertible. If a is invertible and $ab = ac$ then $b = c$ (multiply each side by a^{-1}).
(iv) in general, cannot cancel e.g. in $\mathbb{Z}_{10}$ have $4 \cdot 5 = 2 \cdot 5$ but $4 \neq 2$.

Moral. $\mathbb{Z}_p$ very well-behaved, for prime p.

Prop 1.9. Let p be a prime. Then every $a \not\equiv 0\,(p)$ is invertible mod p.
(Equivalently, in $\mathbb{Z}_p : a \neq 0 \implies \exists b$ with $ab = 1$)

Proof. Have $(a, p) = 1$
So $ax + py = 1$, some $x, y \in \mathbb{Z}$
i.e. $ax = 1 - py$
so $ax \equiv 1\,(p)$□
In $\mathbb{Z}_p$, consider $a \cdot 0, a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$
(our task is to show one of these is 1)
But these are distinct in $\mathbb{Z}_p$:
($ia = ja \implies (i-j)a = 0 \implies i - j \equiv 0\,(p)$ or $a \equiv 0\,(p) \implies i - j \equiv 0\,(p) \implies i = j$ (as $0 \leq i, j \leq p-1$).
Hence must be $0, 1, \ldots, p-1$ in some order.
Thus $ia = 1$, some i. □

General n?

Prop 1.9 (more general)**.** Let $n \geq 2$, a invertible mod $n \iff (a, n) = 1$.

Proof.

$$\begin{aligned}(a,n) = 1 &\iff ax + ny = 1 \text{ some } x, y \in \mathbb{Z} \\ &\iff ax = 1 - ny \text{ some } x, y \in \mathbb{Z} \\ &\iff ax \equiv 1\,(n) \text{ some } x, y \in \mathbb{Z}\end{aligned}$$

Definition. The **Euler ϕ function** defined for each $n \in \mathbb{N}$ by $\phi(n) =$ no. of $x, 1 \leq x \leq n$ with $(x, n) = 1$.
So$\phi(n) =$ no. of invertibles(or units) in $\mathbb{Z}_n$,
e.g. p prime: $\phi(p) = p - 1$, $\phi(p^2) = p^2 - p$ ($-p$ comes from $p, 2p, 3p, \ldots, pp$
If p, q distinct primes, $\phi(pq) = pq - p - q + 1$ ($-p$ from multiples of q, similarly multiples of p for $-q$, $+1$ from subtracting pq twice.)

How do powers behave in $\mathbb{Z}_p$?
e.g. powers of 2 in $\mathbb{Z}_7$:

$$\begin{aligned}2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 1\end{aligned}$$

(then $2, 4, 1, 2, 4, 1, \ldots$)
Powers of 2 in $\mathbb{Z}_{11}$:

$$\begin{aligned}2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 5 \\ 2^5 &= 10 \\ 2^6 &= 9 \\ 2^7 &= 7 \\ 2^8 &= 3 \\ 2^9 &= 6 \\ 2^{10} &= 1\end{aligned}$$

(Then $2, 4, 8, 3, \ldots$)

Theorem 1.10. p prime, then in $\mathbb{Z}_p$, $a^{p-1} = 1$, $\forall a \neq 0$.

(Equivalently in $\mathbb{Z} : a \not\equiv 0\,(p) \implies a^{p-1} \equiv 1\,(p)$)

Proof. in $\mathbb{Z}_p$, consider $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$
$(ai = aj \implies i = j$ as a invertible) & non-zero ($ai = 0 \implies a = 0$ or $i = 0$ ※)
so are $1, 2, \ldots, p-1$ in some order.
Multiply $a^{p-1}(p-1)! = (p-1)!$
Now cancel $(p-1)!$ (invertible as product of invertibles)
To obtain: $a^{p-1} = 1$. □

General n?

Theorem 1.10. (More general) Fermat-Euler: Let $n \geq 2$ then in $\mathbb{Z}_n$, every invertible a has $a^{\phi(n)} = 1$.

Proof. Let the units in $\mathbb{Z}_n$ be $x_1, x_2, \ldots, x_{\phi(n)}$
Consider $ax_1, ax_2, \ldots, ax_{\phi(n)}$. These are distinct ($ax_i = ax_j \implies x_i = x_j$, as a invertible) and invertible as product of invertibles.
So are $x_1, x_2, \ldots, x_{\phi(n)}$ in some order. Multiply: $a^{\phi(n)} x_1 x_2 \ldots x_{\phi(n)} = x_1 x_2 \ldots x_{\phi(n)}$
now cancel each x_i to obtain $a^{\phi(n)} = 1$.□

We know $(p-1)! \not\equiv 0\,(p)$. What is it?
$p = 5 : 4! = 24 \equiv -1\,(5)$
$p = 7 : 6! = 720 \equiv -1\,(7)$

Lemma 1.11. Let p be prime. In $\mathbb{Z}_p : x^2 = 1 \implies x = 1$ or $x = -1$.

Note. in $\mathbb{Z}_8 : 1^2 = 3^2 = 5^2 = 7^2 = 1$.

Proof. In $\mathbb{Z}_p : x^2 = 1 \implies x^2 - 1 = 0 \implies (x-1)(x+1) = 0 \implies x - 1 = 0$ or $x + 1 = 0$
(p prime) $\implies x = \pm 1$ □

Remark. Turns out that (non-zero) poly in $\mathbb{Z}_p$ of degree k has $\leq k$ roots in $\mathbb{Z}_p$.

Theorem 1.12. Wilson's Theorem: Let p be a prime. Then $(p-1)! \equiv -1\,(p)$

Proof. may assume $p > 2$ (Theorem true for $p = 2$)
in $\mathbb{Z}_p$, consider $1, 2, 3, \ldots, p-1$.
Can pair up each a with its inverse a^{-1} ($for a \neq a^{-1}$
but $a = a^{-1} \iff a^2 = 1 \iff a = 1$ or $a = -1$.
Thus $1, 2, \ldots, p-1$ consists of some pairs a, a^{-1}&$1, -1$.
Multiply $(p-1)! = 1^{\frac{p-3}{2}} \cdot 1 \cdot (-1) = -1$□

Is -1 a square in $\mathbb{Z}_p$?
e.g. in $\mathbb{Z}_5 : x = 2$ has $x^2 = -1$✓
in $\mathbb{Z}_7 : 0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 2$ so no.
in $\mathbb{Z}_{13} : x = 5$ has $x^2 = -1$✓
in $\mathbb{Z}_{19}$: no

Prop 1.13. Let p be an odd prime. Then -1 is a square mod $p \iff p \equiv 1\,(4)$.

Proof. For $p = 4k + 3$: suppose $x^2 = -1$ (in $\mathbb{Z}_p$)
have $x^{4k+2} = 1$ (Fermat-Euler).
but $x^{4k+1} = (x^2)^{2k+1} = (-1)^{2k+1} = -1$※
For $p = 4k + 1$: have $(4k)! = -1$ (Wilson)
Compare $(4k)! = 1 \cdot 2 \ldots 2k(2k + 1)(2k + 2) \ldots (4k)$
with $(2k)!^2 = 1 \cdot 2 \ldots 2k \cdot 1 \cdot 2 \ldots (2k - 1)(2k)$
but have $4k = -1, 4k - 1 = -2, \ldots, 2k + 1 = -2k$
so $(2k)!^2 = (4k)!(-1)^{2k} = (4k)! = -1$✓□

1.8.2 Solving congruence equations

1) Solve $7x \equiv 4\,(30)$
Finding a solution:
Have $(7, 30) = 1$ so can sum 7, 30 to obtain: $13 \cdot 7 - 3 \cdot 30 = 1$
so $13 \cdot 7 \equiv 1\,(30)$
whence $7 \cdot 52 \equiv 4\,(30)$
so $x = 52$ is a solution.
Other solutions:
any $x' \equiv 52\,(30)$ also works.
No more: if x' a solution, want $x' \equiv x\,(30)$
Have $7x \equiv 4\,(30)$
Have $7x' \equiv 4\,(30)$
so $7x = 7x'\,(30)$
so $x = x'\,(30)$ as 7 invertible ✓
so our solution is all $x \equiv 52\,(30)$
shorter method:
$7x \equiv 4\,(30) \iff 13 \cdot 7x \equiv 13 \cdot 4\,(30) \iff x \equiv 52\,(30)$ (as 13 invertible) ✓

2) Solve $10x = 12\,(34)$

$$\begin{aligned} 10x \equiv 12\,(34) &\iff 10x = 12 + 34y, \text{ some } y \in \mathbb{Z} \\ &\iff 5x = 6 + 17y, \text{ some } y \in \mathbb{Z} \\ &\iff 5x \equiv 6\,(17) \end{aligned}$$

and now same as before.

A simultaneous congruence?
Do we expect solution to $x \equiv 6\,(17)$, $x \equiv 2\,(19)$?
Guess yes as 17, 19 coprime so 'mod 17 & mod 19 should be independent of each other'
how about $x \equiv 6\,(34)$, $x \equiv 11\,(36)$?
no: is x even or odd? (note that $(34, 36) = 2 \neq 1$)

Theorem 1.14 (Chinese Remainder Theorem)**.** Let u, v be coprime:
then for any a, b, there is an x with $x \equiv a\,(u)$ and $x \equiv b\,(v)$
moreover, x is unique mod uv.

Proof. existence: have $su + tv = 1$ some $s, t \in \mathbb{Z}$
now $su \equiv 0(u)$ and $1\,(v)$
Also $tv \equiv 1\,(u)$ and $0\,(v)$
hence $x = a(tv) + b(su)$ has $x \equiv a\,(u)$ and $b\,(v)$
certainly any $x' \equiv x\,(uv)$ also a solution.
Conversely, suppose $x' \equiv a\,(u)$, $x' \equiv b\,(v)$
so $x' \equiv x\,(u)$ and $x' \equiv x\,(v)$
$\implies u|x' - x \,\&\, v|x' - x$
hence $uv|x' - x$ (as u, v coprime)
so $x' \equiv x\,(uv)$✓□

Remark. Similarly, if $u_1, u_2, \ldots, u_k$ pairwise coprime then $\forall a_1, \ldots, a_k \exists x$ s.t. (by induction)

$$\begin{aligned} x &\equiv a_1\,(u_1) \\ x &\equiv a_1\,(u_2) \\ &\vdots \\ x &\equiv a_k\,(u_k) \end{aligned}$$

NOT 6, 10, 15.

1.9 An appication of Fermat-Euler

1.9.1 RSA Coding

Method. Normally, to send a coded message:

Completely 'obvious' that knowing how to encode = knowing how to decode.
However:
pick 2 large distinct primes p & q (e.g. 100 digits long)
Let $n = pq$.
Fix a 'coding exponent' e.
To encode a message x (viewed as an element of $\mathbb{Z}_n$:

$$x \to x^e$$

How to decode?
seek d s.t. $(x^e)^d = x$.
Have $x^{\phi(n)} = 1$ in $\mathbb{Z}_n$, assuming x coprime to n.
So if you publish n & e, then anyone can encode, but only you can decode!

2 The Reals

2.1 The need for reals

Have $\mathbb{N}$ contained in $\mathbb{Z}$ contained in $\mathbb{Q}$: Why not stop there?

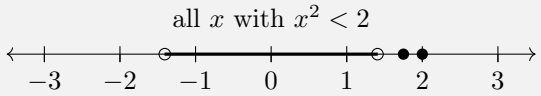
Prop 2.1. There is no rational x with $x^2 = 2$. (In any proof, may assume $x > 0$, since $(-x)^2 = x^2$.)

Proof (1^{st})**.** Suppose $x^2 = 2$, for some $\frac{a}{b}$ where $a, b \in \mathbb{N}$.
So $\frac{a^2}{b^2} = 2$ i.e. $a^2 = 2b^2$ but exponent of 2 in prime factorisation of a^2 even, in $2b^2$ is odd.
Contradicting unique factorisation ※□

Note. Same proof shows if $\exists x \in \mathbb{Q}$ with $x^2 = n$, some $n \in N$, then n must be a square number (each exponent in prime factorisation of n must be even).

Proof (2^{nd})**.** Suppose $x^2 = 2$, some $x = \frac{a}{b}$ where $a, b \in N$
so for any $c, d \in \mathbb{Z}$,
$cx + d$ is of form $\frac{e}{b}$, some $e \in \mathbb{Z}$
and so $cx + d > 0 \implies cx + d \geq \frac{1}{b}$
but $0 < x - 1 < 1$ (as $1 < x < 2$)
so $0 < (x-1)^n < \frac{1}{b}$ if n sufficiently large.
This is contradiction as $(x-1)^n$ is of form $cx + d$, some $c, d \in \mathbb{Q}$ (using $x^2 = 2$) ※□

So “$\mathbb{Q}$ has a gap"
How to express ‘$\mathbb{Q}$ has a gap’ mentioning only $\mathbb{Q}$?



We see that 2 is an upper bound; 1.75 is an upper bound; 1.5 is also an upper bound; so is 1.42.
No LEAST upper bound. This is how we say, inside $\mathbb{Q}$, that ‘$\mathbb{Q}$ has a gap.’

2.2 What we assume about reals

Definition. Reals are a set written $\mathbb{R}$, with elements 0 and 1 ($0 \neq 1$) equipped with operations $+$ and $\cdot$ and an 'ordering'$<$ such that:

(i) $+$ is commutative & associative with identity 0 and every x has an inverse.
(ii) $\cdot$ is commutative & associative with identity 1 and every $x \neq 0$ has an inverse.
(iii) $\cdot$ distributive over $+$ i.e. $(a(b+c) = (ab) + (ac)\, \forall a, b, c)$
(iv) $\forall a, b$: exactly 1 of $a < b, a = b, b < a$ holds and $a < b, b < c \implies a < c$ (all a, b, c)
(v) $\forall a, b, c : a < b \implies a + c < b + c$, and $a < b \implies ac < bc$ if $c > 0$.
(vi) For any set S of reals that is non-empty and bounded above, S has a least upper bound ‘Least upper bound axiom’

(S bounded above if $\exists x \in \mathbb{R}$ with $x \geq y \forall y \in S$ - such an x is an **upper bound** for S. Say x is the least upper bound of S if x is an upper bound for S and every upper bound x' for S satisfies $x \leq x'$)

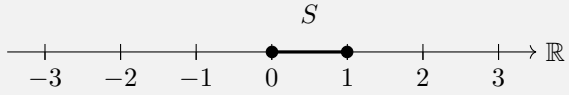
Remarks.

(i) From 1 to 5, can check e.g. $0 < 1$.
Indeed, if not then $1 < 0$, so $0 < -1$ (adding -1)
So $0 < 1$ (multiplying by the 'positive' -1) ※
(ii) May view $\mathbb{Q}$ as contained in $\mathbb{R}$ - by identifying $\frac{a}{b} \in \mathbb{Q}$ with $a \cdot b^{-1} \in \mathbb{R}$
(iii) Least upper bound axiom, 6, FALSE in $\mathbb{Q}$
(iv) Why ‘non-empty and bounded above’ in 6?
- If S not bounded above then it has no U.B. so certainly no least U.B.
- If S empty then every $x \in \mathbb{R}$ is an U.B. so no least U.B.

(v) Can construct $\mathbb{R}$ out of $\mathbb{Q}$, and check that 1 to 6 do hold

2.3 Examples of sets and least upper bounds

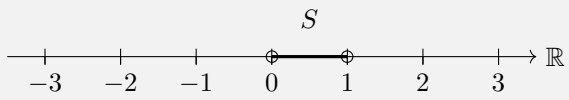
(i) $S = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ - “The set of all $x \in \mathbb{R}$ such that $0 \leq x \leq 1$”



Is 2 an U.B. for S? Yes: $x \leq 2 \forall x \in S$.
Is $\frac{3}{4}$ an U.B. for S? No: $\frac{7}{8} \in S$, but $\frac{7}{8} > \frac{3}{4}$.
Least upper bound of S is 1, because:
- 1 is an U.B: $x \leq 1 \forall x \in S$
- Every U.B. y has $y \geq 1$, since $1 \in S$. ✓

Can also write L.U.B $= 1$ or supremum of $S = 1$ or sup $S = 1$. (Last is usual notation).

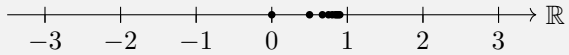
(ii) $S = \{x \in \mathbb{R} : 0 < x < 1\}$



(Can write S as $(0, 1)$ "open interval from 0 to 1". Earlier example can be written $[0, 1]$ "closed interval from 0 to 1".)
Is 2 an U.B.? Yes as $x \leq 2 \forall x \in S$
Is $\frac{3}{4}$ an U.B.? No: $\frac{7}{8} \in S$, but $\frac{7}{8} > \frac{3}{4}$.
$\sup S = 1$ because:

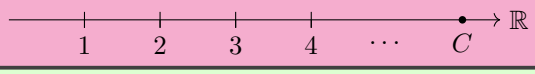
- 1 is an U.B: $x \leq 1 \, \forall x \in S$
- No U.B. c has $c \leq 1$.
  Indeed, certainly $c > 0$ ($c \geq \frac{1}{2}$, since $\frac{1}{2} \in S$)
  So if $c < 1$ then $0 < c < 1$ so $\frac{1+c}{2} \in S$ with $\frac{1+c}{2} > c$ ※.

(iii) $S\{1 - \frac{1}{n} : n \in \mathbb{N}\} = \{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\}$



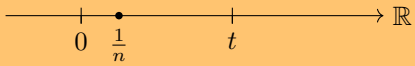
Clearly 1 is an U.B.
Is there an U.B. $x < 1$?

Prop 2.2 (Axiom of Archimedes)**.** $\mathbb{N}$ is not bounded above in $\mathbb{R}$.



Proof. If not, then let $C = \sup \mathbb{N}$.
So $C - 1$ not an U.B. for $\mathbb{N}$,
so $\exists n \in \mathbb{N}$ with $n > C - 1$
but then $n + 1 \in \mathbb{N}$, $n + 1 > C$, contradicting C an U.B ※□

Corollary 2.3. For each $t > 0$, $\exists n \in \mathbb{N}$ with $\frac{1}{n} < t$.



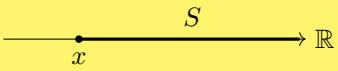
Proof. Have some $n \in \mathbb{N}$ with $n > \frac{1}{t}$ (by prop 2)
So $\frac{1}{n} < t$.□

Note. Prop 2 and Corollary 3 are telling us that $\mathbb{R}$ does not contain any 'infinitely big' or 'infinitely small' elements.

Back to example 3:
Do have $\sup S = 1$, because suppose $C < 1$ is an U.B.
Then $1 - \frac{1}{n} < C \, \forall n \in \mathbb{N}$,
So $1 - C < \frac{1}{n} \forall n \in \mathbb{N}$, contracting Corollary 2.3 ✓

Warning. If S has a greatest element (like $[0,1]$), then the greatest element is sup S - so sup $S \in S$.
But if S has no greatest element(like (0,1)), then sup $S \notin S$.

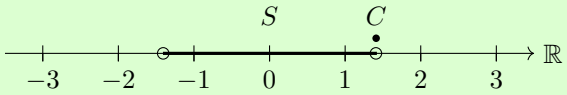
Note. If S is a set of reals that is non-empty and bouned below ($\exists x$ s.t. $x \leq y \, \forall y \in S$ - such an x is a lower bound for S)



Then the set $-S = \{-y : y \in S\}$ is non-empty and bounded above, so has a least upper bound C.
So $-C$ is the greatest lower bound of S - called the infimum of s or inf S.
In particular, if S non-empty and bounded (bounded above and below) then it has a sup and an inf.

Theorem 2.4. $\exists x \in \mathbb{R}$ with $x^2 = 2$.

Proof. Let $S = \{x \in \mathbb{R} : x^2 = 2\}$



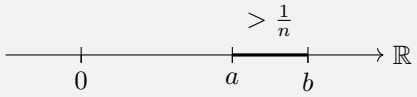
Have S nonempty (e.g. $1 \in S$)
and bounded above (e.g. 2 is an U.B.)
So S has a sup, C say (and $1 \leq C \leq 2$)

Claim. $C^2 = 2$

Proof. Suppose not
If $C^2 < 2$: (Hope $(C+t)^2 < 2$ for t small)
For $0 < t < 1$, have $(C+t)^2 = C^2 + 2Ct + t^2 \leq C^2 + 5t < 2$ for t small ($t < \frac{2-C^2}{5}$)
This contradicts C an U.B. for S (as $C + t \in S$ for t small) ※
If $C^2 > 2$: (Hope $(C-t)^2 > 2$ for t small)
For $0 < t < 1$, have $(C+t)^2 = C^2 - 2Ct + t^2 \geq C^2 - 4t > 2$ for t small ($t < \frac{C^2-2}{4}$)
This contradicts C is the least U.B for S (as $C - t$ an U.B. for t small) ※✓□

Remark. Same proof shows that $\sqrt[n]{x}$ exists $\forall n \in \mathbb{N} \forall x \in \mathbb{R}$, $x > 0$. i.e. $\exists y \in \mathbb{R}$ s.t. $y^n = x$.
A real that is not rational is called irrational
e.g. $\sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{15}$ irrational.
Also, $2 + 3\sqrt{5}$ irrational.
Indeed, if $2 + 3\sqrt{5} = \frac{a}{b}$ $(a, b \in \mathbb{N})$ then $\sqrt{5} = \frac{a-2b}{3b} \in \mathbb{Q}$

Also, "the rationals are dense", meaning that if $a, b \in \mathbb{R}$ with $a < b$ then $\exists c \in \mathbb{Q}$ with $a < c < b$

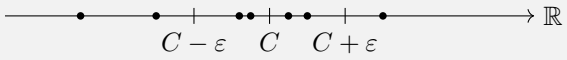


Indeed may assume $a, b \geq 0$ (if $a, b \leq 0$, look at $-a, -b$ instead)
Choose $n \in \mathbb{N}$ with $\frac{1}{n} < b - a$
among $\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots$, there is a final one that is $\leq a$, say $\frac{q}{n}$
(else a would be an U.B for $\{\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots\}$, contradiction axiom of Archimedes)
so $a < \frac{q+1}{n} < b$✓

Also, "the irrationals are dense" $\forall a, b \in \mathbb{R}$ with $a < b$, $\exists$ irrational c with $a < c < b$.
Indeed, $\exists$ rational c with $a\sqrt{2} < c < b\sqrt{2}$,
So $a < \frac{c}{\sqrt{2}} < b$.✓

What should "$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 2$" mean?
what should "$0.33333\cdots = \frac{1}{3}$" mean?

Presumable that, $1 + \frac{1}{2}, 1 + \frac{1}{2} + \frac{1}{4}, 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8}, \ldots$ should "tend to" 2
and $0.3, 0.33, 0.333, 0.3333, \ldots$ should "tend to" $\frac{1}{3}$
Given a sequence $x_1, x_2, x_3, \ldots$ of reals, and $c \in \mathbb{R}$, what should "x_n tends to c" mean?
NOT that the x_n are getting closer to c
e.g. would not want $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots$ to tend to 17.
And NOT that $\forall \varepsilon > 0$, $\exists n$ with $c - \varepsilon < x_n < c + \varepsilon$
e.g. would not want that $\frac{1}{2}, 10, \frac{2}{3}, 10, \frac{3}{4}, 10, \frac{4}{5}, 10, \ldots$ to tend to 1.
We want the sequence to get and stay, within ε of c.
So: we say that $x_1, x_2, x_3, \ldots$ tends to c if $\forall \varepsilon > 0, \exists N$ s.t. $\forall n \in \mathbb{N}$ have $c - \varepsilon < x_n < c + \varepsilon$
"$\forall \varepsilon > 0, x_n$ eventually ($\forall n \geq N$, some N) within ε of c"
Equivalently: $\forall \varepsilon > 0\, \exists N$ s.t. $\forall n \geq N$ have $|x_n - c| < \varepsilon$



eventually within $(C - \varepsilon, C + \varepsilon)$
Where the absolute value, $|a|$, of $a \in \mathbb{R}$ is defined by :

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

So can think of $|a - b|$ as "the distance from a to b on the number line",
e.g. $|9 - 2| = |2 - 9| = 7$
Easy to check the triangle inequality: $|a - c| \leq |a - b| + |b - c|$.

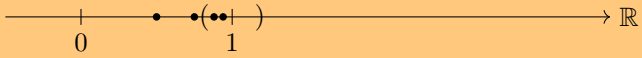
If x_n tends to C, can write $x_n \to C$
or $x_n \to C$ as $n \to \infty$
"x_n tends to C as n tends to infinity"
or $\lim_{n \to \infty} x_n = C$
or "the sequence $x_1, x_2, \ldots$ has limit C"

Examples:

(i) $\frac{1}{2}, \frac{1}{2}+\frac{1}{4}, \frac{1}{2}+\frac{1}{4}+\frac{1}{8}, \ldots$

This is $x_1, x_2, x_3, \ldots$ where $x_n = 1 - \frac{1}{2^n}$ (inductively)

Claim. $x_n \to 1$



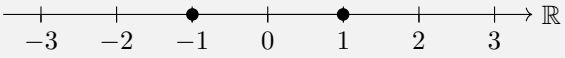
Proof. Given $\varepsilon > 0$:
Choose $N \in \mathbb{N}$ with $N > \frac{1}{\varepsilon}$
Then $\forall n \geq N : |x_n - 1| = \frac{1}{2^n} \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon$

(ii) The constant sequence $C, C, C, C, \ldots$ (i.e. $x_n = C \, \forall n$)

Claim. $x_n \to C$

Proof. Given $\varepsilon > 0$:
Have $|x_n - c| < \varepsilon \, \forall n$✓

(iii) $x_n = (-1)^n : -1, 1, -1, 1, \ldots$



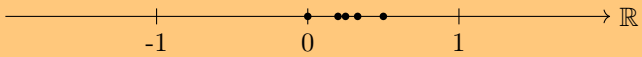
Claim. There is no $c \in \mathbb{R}$ with $x_n \to c$

Proof. suppose $x_n \to C$
Choose $\varepsilon = 1$
So $\exists N \in \mathbb{N}$ s.t. $\forall n \leq N$, have $|x_n - c| < 1$
In particular, $|1 - c|$ and $(-1) - c| < 1$, so $|1 - (-1)| < 2$ (triangle inequality).
※✓

(iv) The sequence x_n given by: $x_n = \begin{cases} \frac{1}{n} & \text{if } n \text{ odd} \\ 0 & \text{if } n \text{ even} \end{cases}$

(sequence need not have a 'nice' or '1-line' definition)

Claim. $x_n \to 0$



Proof. Given $\varepsilon > 0$:
Choose $N \in \mathbb{N}$ with $\frac{1}{N} < \varepsilon$.
Then $\forall n \geq N : x_n \frac{1}{n}$ or 0, so $|x_n - 0| \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon$✓

Note.

(i) If $x_n \to C$, some C, say that the sequence $x_1, x_2, x_3, \ldots$ is convergent
or the sequence (x_n) is convergent
or the sequence $(x_n)_{n=1}^{\infty}$ is convergent
If (x_n) not convergent, say it is divergent.
e.g. $((-1)^n)_{n=1}^{\infty}$ is divergent. (NOT saying 'it goes off to infinity')

(ii) Same idea as in 3rd example shows 'limits are unique'.
If $x_n \to c$ and $x_n \to d$ then $c = d$.
Indeed, suppose $c \neq d$, and choose $\varepsilon = \frac{1}{2}|c - d|$
Then $\exists N \in \mathbb{N}$ with $|x_n - c| < \varepsilon \, \forall n \geq N$
And $\exists M \in \mathbb{N}$ with $|x_n - d| < \varepsilon \, \forall n \geq M$
But now for any $n \geq \max(M, N)$ Have: $|x_n - c|, |x_n - d| < \varepsilon$,
so $|c - d| < 2\varepsilon$ ※

A sequence given in the form $x_1, x_1 + x_2, x_1 + x_2 + x_3, \ldots$ is called a series. Can write it as $\sum_{n=1}^{\infty} x_n$.

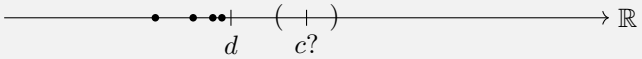
The k-th term of this actual sequence is $\sum_{n=1}^{k} x_n$

If series $x_1, x_1 + x_2, x_1 + x_2 + x_3, \ldots$ is convergent, say to c, can write $\sum_{n=1}^{\infty} x_n = c$

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

Warning. CANNOT write $\sum_{n=1}^{\infty} x_n$ to denote the limit, until we know it exists.
Similarly, CANNOT write $\lim_{n\to\infty} x_n$ until we know the limit exists e.g. CANNOT write $\lim_{n\to\infty} (-1)^n$.

Limits do behave as we expect.
For example: if $x_n \leq d \, \forall n$ and $x_n \to c$ then $c \leq d$

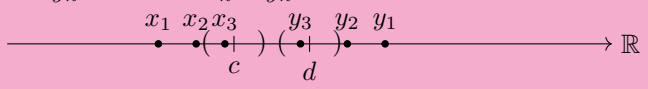


Indeed, suppose $c > d$.
Choose $\varepsilon = |c - d|$
Then $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N$ have $|x_n - c| < \varepsilon$.
But $|x_n - c| < \varepsilon \implies x_n > d$ ※✓

Warning. If $x_n < d \, \forall n$ and $x_n \to c$, need not have $c < d$
e.g. $\frac{1}{2}, \frac{1}{2} + \frac{1}{4}, \frac{1}{2} + \frac{1}{4} + \frac{1}{8}, \ldots$ has all $x_n < 1$ but $\lim_{n\to\infty} x_n = 1$

How about $x_n + y_n$?

Prop 2.5. If $x_n \to c$ and $y_n \to d$ then $x_n + y_n \to c + d$



Idea: "Late x_n are close to c and late y_n are close to d so late $x_n + y_n$ are close to $c + d$".

Plan
Given $\varepsilon > 0$:
...
Choose $N = \ldots$
$\forall n \geq N$, somehow get $|(x_n + y_n) - (c + d)| < \varepsilon$

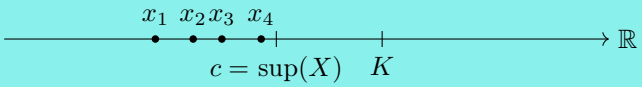
Proof. Given $\varepsilon > 0$:
Have $x_n \to c$,
So $\exists N \in \mathbb{N}$ s.t. $|x_n - c| < \frac{\varepsilon}{2}\, \forall n \geq N$
Also $y_n \to d$,
So $\exists M \in \mathbb{N}$ s.t. $|y_n - d| < \frac{\varepsilon}{2}\, \forall n \geq M$
Thus $\forall n \geq \max(M, N)$, have $|(x_n + y_n) - (c + d)| \leq |x_n - c| + |y_n - d| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \square$

Remark. If we'd used "$|x_n - c| < \varepsilon$" instead, would have got at the end that $|(x_n + y_n) - (c + d)| < 2\varepsilon$ instead which is clearly ok.

2.4 An Important Result on Limits of Sequences Without Having Know the Limit in Advance

Definition. A sequence $x_1, x_2, \ldots$ is **increasing** if $x_{n+1} \geq x_n\, \forall n$

Theorem 2.6. If $x_1, x_2 \ldots$ is increasing and bounded above (i.e. $\{x_1, x_2 \ldots\}$ bounded above) then it converges.

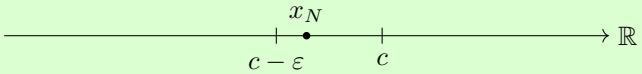


Remark. If we lived in $\mathbb{Q}$, this would be false, e.g. $1, 1.4, 1.41, 1.414, 1.4142, \ldots$ ("want to $\to \sqrt{2}$")

Proof. Let $c = \sup\{x_1, x_2, \ldots\}$

Claim. $x_n \to c$

Proof. Given $\varepsilon > 0$
$\exists N$ a.t. $x_N > c - \varepsilon$ (else $c - \varepsilon$ an U.B. for $\{x_1, x_2, \ldots\}$※
so $\forall n \in N$: $c - \varepsilon < x_N \leq x_n < c$,
whence $|x_n - c| < \varepsilon$ ✓□



Similarly, if (x_n) is decreasing ($x_{n+1} \leq x_n \, \forall n$) and bounded below, then (x_n) convergent.
So "a bounded monotone(increasing or decreasing) sequence is convergent"

2.4.1 Three applications

Firstly:

Prop 2.7. i) $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges

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

Note. No 'closed form' for $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ or $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2}$. This is why series are often harder than sequences.

Idea: $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \ldots$
$\geq 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{16} + \cdots = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots$

Proof. i) have $\frac{1}{3} + \frac{1}{4} \geq \frac{1}{2}$
and $\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \geq \frac{1}{2}$
and in general $\frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}} \geq \frac{1}{2} \, \forall n$
Hence the partial sums of $\sum_{n=1}^{\infty} \frac{1}{n}$ unbounded and so certainly $\sum_{n=1}^{\infty} \frac{1}{n}$ not convergent ✓

Idea: $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} + \frac{1}{8^2} + \ldots$
$\leq 1 + \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{8^2} + \cdots = 1 + \frac{2}{2^2} + \frac{4}{4^2} + \frac{8}{8^2} + \ldots$

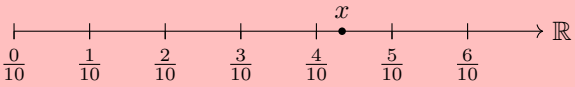
Proof. ii) have $\frac{1}{2^2} + \frac{1}{3^2} \leq \frac{2}{2^2} = \frac{1}{2}$
and $\frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} \leq \frac{4}{4^2} = \frac{1}{4}$
and in general $\frac{1}{(2^n)^2} + \frac{1}{(2^n+1)^2} + \cdots + \frac{1}{(2^{n+1}-1)^2} \leq \frac{2^n}{(2^n)^2} = \frac{1}{2^n} \, \forall n$
Hence partial sums of $\sum_{n=1}^{\infty} \frac{1}{n^2}$ bounded $(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 2)$
so $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges, by thm 6 ✓□

Remarks.
(i) $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$ is called the harmonic series
(ii) In fact, $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ - proved in part II 'Linear Analysis'

Secondly: Decimal expansions

What should "$0.a_1a_2a_3\ldots$" mean ($0 \le a_i \le 9$, each i)?
It should be the limit of $0.a_1, 0.a_1a_2, 0.a_1a_2a_3\ldots$
So we define $0.a_1a_2a_3\ldots$ to be $\sum_{n=1}^{\infty} \frac{a_n}{10^n}$ (converges as all terms ≥ 0 as partial sums bounded, e.g. by 1)

Conversely: Given $x \in \mathbb{R}, 0 < x < 1$,
want to write $x = 0.a_1a_2a_3\ldots$ for some $a_1, a_2, \cdots \in \{0, 1, \ldots, 9\}$



Choose the greatest $a_1, \cdots \in \{0, 1, \ldots, 9\}$ s.t. $\frac{a_1}{10} \le x$
thus $0 \le x - \frac{a_1}{10} < \frac{1}{10}$
Now take greatest $a_2 \in \{0, 1, \ldots, 9\}$ s.t. $\frac{a_1}{10} + \frac{a_2}{100} \le x$
So $0 \le x - \frac{a_1}{10} - \frac{a_2}{100} < \frac{1}{100}$
Continue inductively: we obtain $a_1, a_2, a_3, \cdots \in \{0, 1, \ldots, 9\}$ s.t.
$0 \le x - \sum_{n=1}^{k} \frac{a_n}{10^n} < \frac{1}{10^k}\ \forall k$

Remarks.

(i) Call a decimal expansion $0.a_1a_2a_3\ldots$ recurrent if $a_{n+k} = a_n\ \forall n \ge N$, some N and k
e.g. $0.3178426426426426\ldots$
Can check $x = 0.a_1a_2a_3\ldots$ recurrent $\iff$ x rational

(ii) Decimal expansion need not be unique e.g. $0.37000\cdots = 0.36999\ldots$

(iii) That's the only way to have non-unique decimal expansion: If $0.a_1a_2a_3\cdots = 0.b_1b_2b_3\ldots$ are different decimal expansions of the same number then:
$\exists N \in \mathbb{N}$ s.t. $a_n = b_n \forall n < N$ and $a_N = b_N - 1$ and $a_n = 9$, $b_n = 0\ \forall n > N$ (or vice versa).

Thirdly: the number e

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

This does converge: all terms ≥ 0 and the partial sums are bounded by $1+1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots = 3$ (since $\frac{1}{n!} \le \frac{1}{2^{n-1}}\ \forall n \ge 2$, inductively)
If we write $0! = 1$ then $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.

Definition. A real x is **algebraic** if it is a root of a (non-zero) polynomial with integer coefficients, i.e. $a_dx^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 = 0$, where $a_0, \ldots, a_d \in \mathbb{Z}$ (some d) with $a_d \ne 0$

e.g.
(i) Every rational is algebraic: $\frac{p}{q}$ is a root of $qx - p$ (i.e. satisfies $qx - p = 0$)
(ii) $\sqrt{2}$: is algebraic: it satisfies $x^2 - 2 = 0$.
(iii) $\sqrt{2+1}$: is algebraic: it satisfies $(x-1)^2 - 2 = 0$.
Are all reals algebraic?

Prop 2.8. e is not rational

Proof. Suppose e is rational. Write $e = \frac{p}{q}$ where $p, q \in \mathbb{N}$, with $q > 1$ (if $q = 1$, rewrite as $\frac{2p}{2q}$).
So $\sum_{n=0}^{\infty} \frac{q!}{n!} \in \mathbb{Z}$
(since $x_n \to c$ then $kx_n \to kc$ for any $k \in \mathbb{R}$)
Sum $= (q! + \frac{q!}{1!} + \frac{q!}{2!} + \cdots + \frac{q!}{q!}) + (\frac{q!}{(q+1)!} + \frac{q!}{(q+2)!} + \dots)$ i.e. integer $+ < 1$
Formally:
Now, $\sum_{n=0}^{\infty} \frac{q!}{n!} \in \mathbb{Z}$
Also, $\frac{q!}{(q+1)!} = \frac{1}{q+1}$
$\frac{q!}{(q+2)!} = \frac{1}{(q+1)(q+2)} \leq \frac{1}{(q+1)^2}$
And in general $\frac{q!}{(q+n)!} \leq \frac{1}{(q+1)^n}$.
So $\sum_{n=q+1}^{\infty} \frac{q!}{n!} \leq \frac{1}{(q+1)} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots = \frac{1}{q} < 1$
But this contradicts $\sum_{n=0}^{q} \frac{q!}{n!} + \sum_{n=q+1}^{\infty} \frac{q!}{n!} \in \mathbb{Z}$※

Definition. A real that is not algebraic is called **transcendental**.

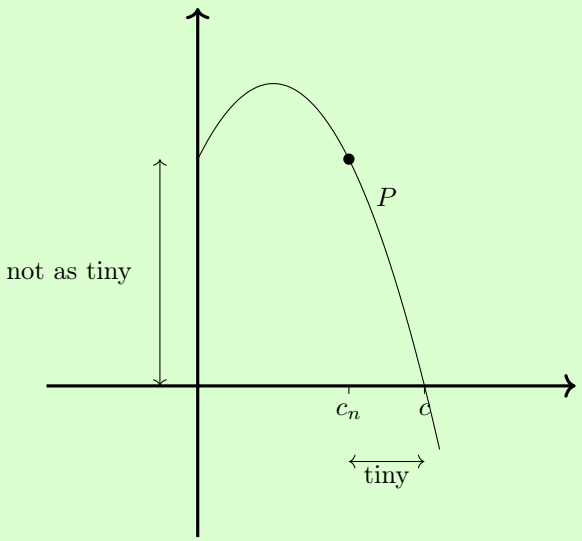
Theorem 2.9. The number $c = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ i.e. $c = 0.11000100000000000000000010\dots$ is transcendental.

We'll need two facts about polynomials:
(i) For any polynomial P, $\exists$ constant K s.t.
$|P(x) - P(y)| \leq K|x - y| \forall 0 \leq x, y \leq 1$.
Indeed, say $P(x) = a_d x^d + \cdots + a_0$
Then

$$\begin{aligned} P(x) - P(y) &= a_d(x^d - y^d) + a_{d-1}(x^{d-1} - y^{d-1}) + \cdots + a_1(x - y) \\ &= (x - y)[a_d(x^{d-1} + x^{d-2}y + \cdots + y^{d-1}) + \cdots + a_1] \\ \text{So } |P(x) - P(y) &\leq |x - y|[(|a_d + a_{d-1} + \cdots + |a_1|)d] \text{ as } 0 \leq x, y \leq 1\checkmark \end{aligned}$$

(ii) A (non-zero) poly of degree d has $\leq d$ roots.
Indeed, given poly P of degree d:
If P has no roots: ✓
If P has a root: say a is a root.
Then $P(x) = (x - a)Q(x)$, some poly Q of degree $d - 1$ (by dividing the poly P)
So each root of P is either a or a root of Q but Q has $\leq d - 1$ roots (induction) ✓

Proof. Write $c_n = \sum_{k=0}^{n} \frac{1}{10^{k!}}$ - so $c_n \to c$.



Suppose poly P has c as a root.
Then $\exists K$ s.t. $|P(x) - P(y)| \leq K|x - y| \, \forall 0 \leq x, y \leq 1$.
Say P has degree $d : P(x) = a_d x^d + \cdots + a_0$ (all $a_i \in \mathbb{Z}, a_d \neq 0$)
Now, $|c - c_n| = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} \leq \frac{2}{10^{(n+1)!}}$
Also $c_n = \frac{a}{10^{n!}}$, some $a \in \mathbb{Z}$, so $P(c_n) = \frac{b}{10^{d \cdot n!}}$, some $b \in \mathbb{Z}$
(since $P(\frac{s}{t}) = \frac{q}{t^d}$, some $q \in \mathbb{Z}$, whenever $s, t \in \mathbb{Z}$)
But for n large enough, c_n not a root of p (by 2^{nd} fact),
so $|P(c_n)| \geq \frac{1}{10^{d \cdot n!}}$, i.e. $|P(c_n) - P(c)| \geq \frac{1}{10^{d \cdot n!}}$
Thus $\frac{1}{10^{d \cdot n!}} \leq K \frac{2}{10^{(n+1)!}}$, a contradiction for n sufficiently large. ※□

Remarks.

(i) Same proof shows that any real x s.t. $\forall n \, \exists$ rational $\frac{p}{q}$ with $0 < |x - \frac{p}{q}| < \frac{1}{q^n}$ is transcendental. "x has very good rational approximations"

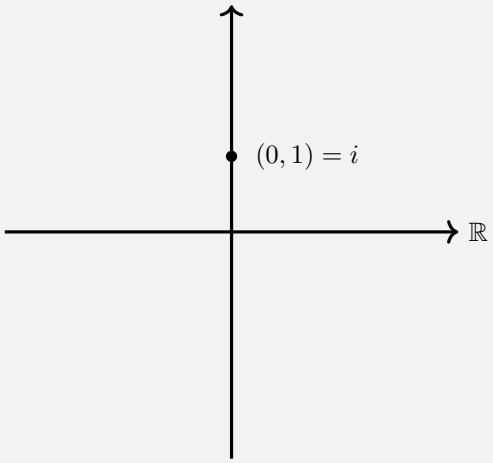
(ii) Such x are called "Liouville numbers". So could view Theorem 9 as saying 'every Liouville number is transcendental"

(iii) This does not show e transcendental. But in fact it is.

(iv) Another proof of existence of transcendentals is coming in chapter 4.

2.5 The Complex Numbers

Some polys have no real roots - e.g. $x^2 + 1$.
We'll try to 'force' an x with $x^2 = -1$ (cannot force an x with $x^2 = 2, x^3 = 3$)



Definition. The **complex numbers**, written $\mathbb{C}$, consists of $\mathbb{R}^2$ (The set of all ordered pairs (a, b) with operations $+$ and $\cdot$ defined by:

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

Can view $\mathbb{R}$ as contained in $\mathbb{C}$ by identifying $a \in \mathbb{R}$ with $(a, 0) \in \mathbb{C}$.

Note. $(a, 0) + (b, 0) = (a + b, 0)$ and $(a, 0) \cdot (b, 0) = (ab, 0)$

Let $i = (0, 1)$. Then $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$

Note. Every $z \in \mathbb{C}$ is of the form $a + bi$, where $a, b \in \mathbb{R}$
Indeed $(a, b) = a(1, 0) + b(0, 1) = a + bi$✓

Remarks.

(i) $\mathbb{C}$ obeys all our usual algebraic rules (rules 1 to 3 in definition of $\mathbb{R}$ - even $\forall z \neq 0\, \exists w$ s.t. $zw = 1$
Indeed, given $z = a + bi$:

$$(a + bi)(a - bi) = a^2 + b^2$$

So

$$(a + bi)\left(\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i\right) = 1\checkmark$$

Such a structure is called a field e.g. $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$ (p prime), NOT $\mathbb{Z}$.

(ii) Amazing fact: every (non-zero) polynomial (even allowing coefficients in $\mathbb{C}$) has a root in $\mathbb{C}$. This is the Fundamental Theorem of Algebra - proved in IB 'Complex Analysis'.

3 Sets and Functions

Definition. A **set** is any (but: see later) collection of (mathematical) objects e.g. $\mathbb{R}, \mathbb{N}, \{1, 5, 9\}, [0, 1]$
Two sets with the same members are the same.
(i.e. 'a set is determined by its members'):

If $\forall x : x \in A \iff x \in B$ then $A = B$.
(Write $x \in A$ if x is a member of A, $x \notin A$ is not).
e.g. $\{1, 3, 7\} = \{1, 7, 3\}$ ("order not important")
and $\{3, 4, 4, 6\} = \{3, 4, 6\}$ ("no multiple membership")

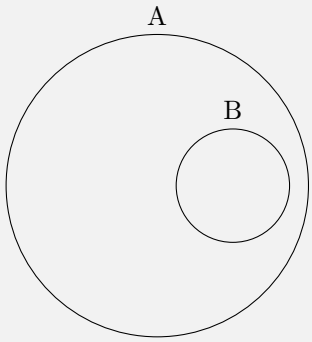
3.1 New sets from old

3.1.1 Subsets

Given a set A and property $P(x)$, can form $\{x \in A : P(x)\}$: the subset of all members with property P ('subset selection').
e.g. $\{x \in \mathbb{N} : x \text{ is prime }\}$

Definition. B is a **subset** of A if $\forall x : x \in B \implies x \in A$.
Written $B \subset A$ or $B \subseteq A$.

Can visualise as:

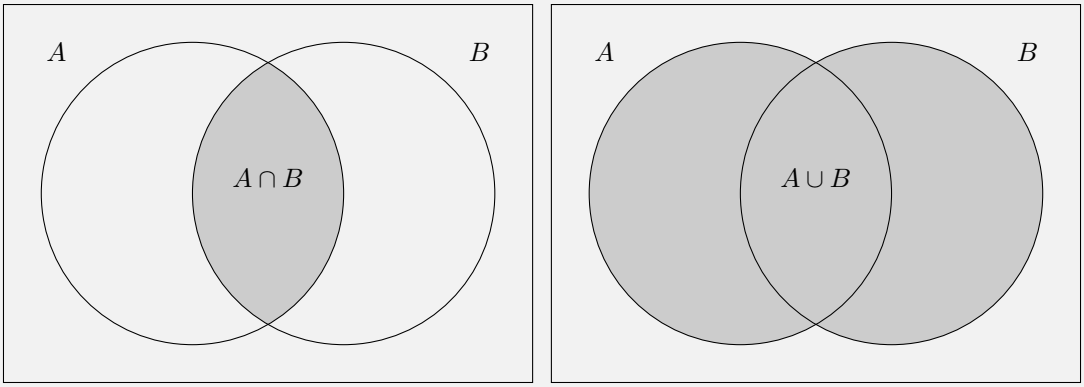


Have $A = B \iff A \subseteq B, B \subseteq A$

3.2 Unions and Intersections

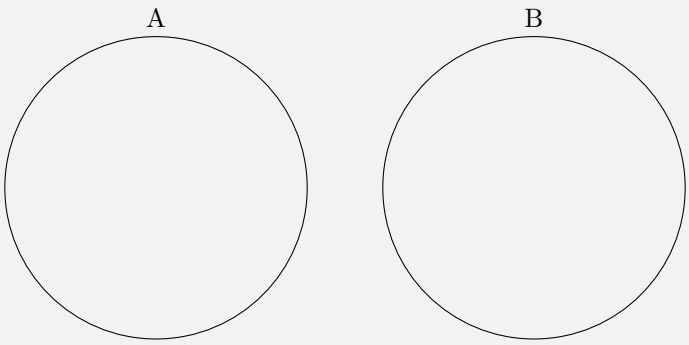
Definition. Given sets A and B, can form their **union** $A \cup B = \{x : x \in A \text{ or } x \in B\}$
And their **intersection** $A \cap B = \{x : x \in A \text{ and } x \in B\}$

Can visualise as:



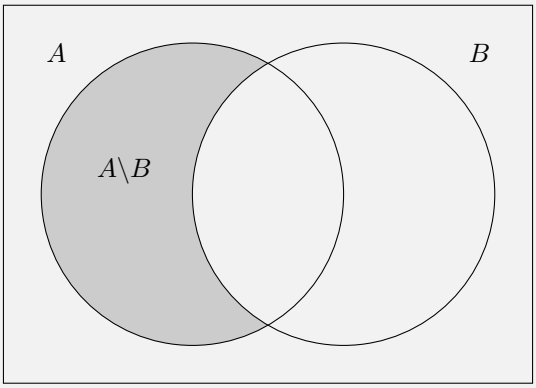
Definition. Say A and B are **disjoint** if $A \cap B = \varnothing$ ("The empty set" or "the set with no elements")

Can visualise as:



Note. Could view intersection as a special case of subset selection: $A \cap B = \{x \in A : x \in B\}$

Can visualise as:



Definition. Similarly, have the **set difference** $A \backslash B = \{x \in A : \notin B\}$ ("A minus B")

Note. $\cup, \cap$ are commutative and associative.
Also $\cup$ distributive over $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
And $\cap$ distributive over $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

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

Proof.
LHS $\subseteq$ RHS: Given $x \in A \cap (b \cup C)$:
Have $x \in A$, and also $x \in B$ or $x \in C$.
If $x \in B$: Have $x \in A, x \in B$, so $x \in A \cap B$, so $x \in$ RHS ✓
If $x \in C$: Have $x \in A, x \in C$, so $x \in A \cap C$, so $x \in$ RHS ✓✓

RHS $\subseteq$ LHS: Given $x \in (A \cap B) \cup (A \cap C)$:
Have $x \in A \cap B$ or $x \in A \cap C$.
If $x \in A \cap B$: Have $x \in A, x \in B \cup C$, so $x \in$ RHS ✓
If $x \in A \cap C$: Have $x \in A, x \in B \cup C$, so $x \in$ RHS ✓✓✓

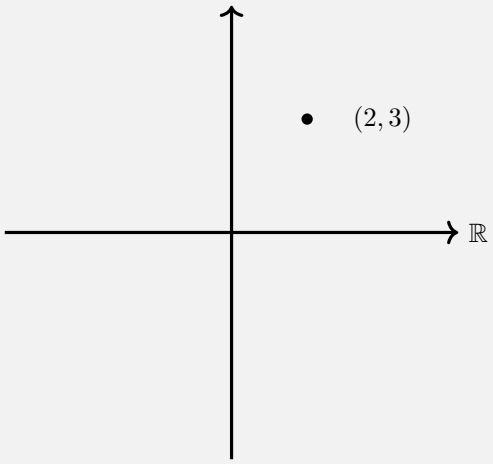
Can also have bigger unions
e.g. if $A_n = \{n^2, n^3\}$, each $n \in \mathbb{N}$, then $A_1 \cup A_2 \cup \cdots = \{x \in \mathbb{N} : x \text{ is a square or a cube}\}$.
Can write this as $\bigcup_{n=1}^{\infty} A_n$ or $\bigcup_{n \in \mathbb{N}} A_n$. ($\mathbb{N}$ is the 'index set')

Warning. $\bigcup_{n \in \mathbb{N}} A_n$ means $\{x : x \in A_n, \text{ some } n\}$

In general, given a set I and sets $A_i : i \in I$, can form
$\bigcup_{i \in I} A_i = \{x : x \in A_i, \text{ some } i \in I\}$
$\bigcap_{i \in I} A_i = \{x : x \in A_i, \forall i \in I\}$ (only for $i \neq \varnothing$ (see later))

3.3 Ordered Pairs

For any a, b, can form the ordered pair (a, b)
- key point being that $(a, b) = (c, d) \iff a = c$ and $b = d$.
For sets A and B, can form their product ("A cross B") $A \times B = \{(a, b) : a \in A, b \in B\}$
eg. can view $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ as a plane:



Similarly, could form A^3 = all 'ordered triples' from A, etc.

Note. If we wished, could define $(a, b) = \{\{a\}, \{a, b\}\}$ and can check 'key point' above.

3.4 Power Set

Definition. For any set X, can form the **power set** $\mathbb{P}(X)$, consisting of all subsets of X:

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

e.g. If $X = \{1, 2\}$ then $\mathbb{P}(X) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$

Warning. For a set A, can form $\{x \in A : p(x)\}$.
CANNOT form $\{x : p(x)\}$
Indeed, if we could, then consider $\{x : x \notin x\} = X$, say.
Do we have $X \in X$?
If yes: then $X \notin X$ by def. of X ※
If no: have $X \in X$ by def. of X ※(called Russell's Paradox).

Similarly, there is no 'universal' set Y meaning $\forall x : x \in Y$.
Otherwise, could form X above by subset selection: $X = \{x \in Y : x \notin x\}$

Moral. To guarantee that a given set exists, it should be obtained in some way (e.g. our 'new sets from old' rule) from known sets (e.g. $\mathbb{N}, \mathbb{R}$).

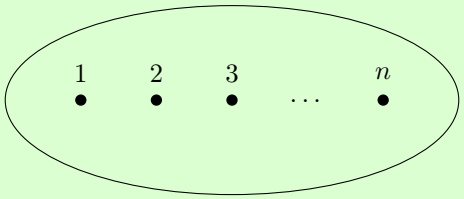
3.5 Finite Sets

Write $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ - so $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$.
For $n \in \mathbb{N}_0$, say that set A has size n if can write $A = \{a_1, a_2, \dots, a_n\}$ with the a_i distinct.
e.g. $\{1, 3, 7\}$ has size 3
$\varnothing$ has size 0.
Say A finite if $\exists n \in \mathbb{N}_0$ s.t. A has size n, infinite otherwise.

Note. A cannot have size n and size m, for $n \neq m$.
Indeed suppose A has size n and size m, where $n, m > 0$.
then, removing an element, we obtain a set of size $n-1$ and size $m-1$ - done by induction on $\max(m, n)$.

Prop 3.1. A set of size n has exactly 2^n subsets.

Proof (1^{st})**.** May assume our set is $\{1, \dots, n\}$



To specify a subset S, we must say if $1 \in S$ or $1 \notin S$. Then if $2 \in S$ or $2 \notin S$, and so on.
So # choices for $S = 2 \times 2 \times \cdots \times 2 = 2^n$ (each '2' comes from if $k \in S$) $\square$

Proof (2^{nd})**.** Induction on $n : n = 0$ ✓
Given $n > 0$:
For $T \subseteq \{1, 2, \dots, n-1\}$, how many $S \subseteq \{1, \dots, n\}$ have $S \cap \{1, \dots, n-1\} = T$
Exactly 2: T and $T \cup \{n\}$
Hence, # subsets of $\{1, \dots, n\} = 2 \cdot$ # subsets of $\{1, \dots, n-1\}$
So done by induction. $\square$

Remark. Could view 2^{nd} proof as a 'more formal version' of 1^{st} proof .
If A has size n, write $|A| = n$ ('size of A' or 'mod A')
So prop 1 says: $|A| = n \implies |\mathbb{P}(A)| = 2^n$.
Can also say that A is an n-set.

3.6 Binomial Coefficients

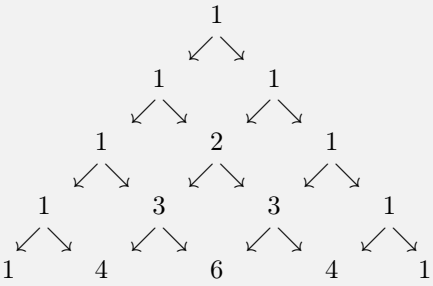
Definition. For $n \in \mathbb{N}_0$ and $0 \leq k \leq n$, write $\binom{n}{k}$ [‘n choose k’] for the number of subsets of an n-set that are of size k:
$\binom{n}{k} = |\{S \subseteq \{1, 2, \ldots, n\} : |S| = k\}|$
e.g. 2-sets in a 4-set $\{1, 2, 3, 4\} : \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$ So $\binom{4}{2} = 6$

Note. $\binom{n}{0} = 1, \binom{n}{n} = 1, \binom{n}{1} = n \, (n > 0)$
Also, $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$
Since each side counts the number of subsets of $\{1, \ldots, n\}$

Also:

(i) $\binom{n}{k} = \binom{n}{n-k} \, \forall n \in \mathbb{N}_0, \, 0 \leq k \leq n$ e.g. $\binom{8}{3} = \binom{8}{5}$
Indeed specifying which k members to prick same as specifying which $n - k$ members not to pick.

(ii) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \, \forall n \geq 1, \, 0 < k < n$ - e.g. $\binom{7}{3} = \binom{6}{2} + \binom{6}{3}$
Indeed, # of k-subsets of $\{1, \ldots, n\}$ without n is $\binom{n-1}{k}$ (pick our k from $1, 2, \ldots, n-1$
and # of k-subsets of $\{1, \ldots, n\}$ with n is $\binom{n-1}{k-1}$ (pick remaining $k-1$ from $1, 2, \ldots, n-1$
Hence $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
Hence Pascal’s Triangle: In each row, we start and end with 1, and each other term is the sum of two terms above it.

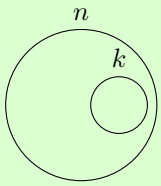


So if n-th row is $a_0, a_1, \ldots, a_n$ then $a_k = \binom{n}{k}$ (induction on n) e.g. $\binom{6}{3} = 20$

Prop 3.2.

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

Proof. # ways to name a k-set $= n(n-1)(n-2)\dots(n-k+1)$ (naming an element, naming different element, etc.)
times a given k-set named $= l(k-1)(k-2)\dots 1$ (naming an element, naming different element, etc.)



Hence, # k-sets in $\{1,\dots,n\} is \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$ □

Notes.
(i) Hence e.g. $\binom{n}{2} = \frac{n(n-1)}{2}$
(ii) Can also write $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
(iii) From our formula, $\frac{n}{3} \sim \frac{n^3}{6}$ for large n.

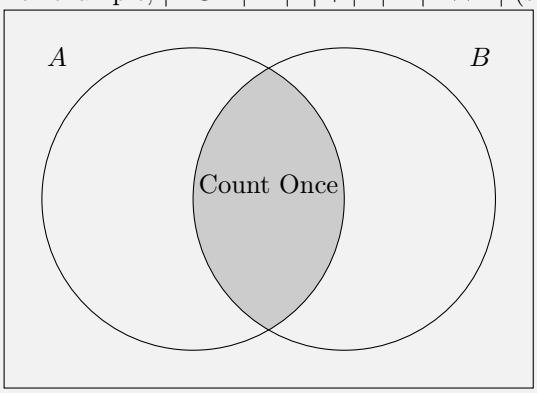
Theorem 3.3 (Binomial Theorem)**.**

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{n}b^n \; \forall a, b \in \mathbb{R},\, n \in \mathbb{N}$$

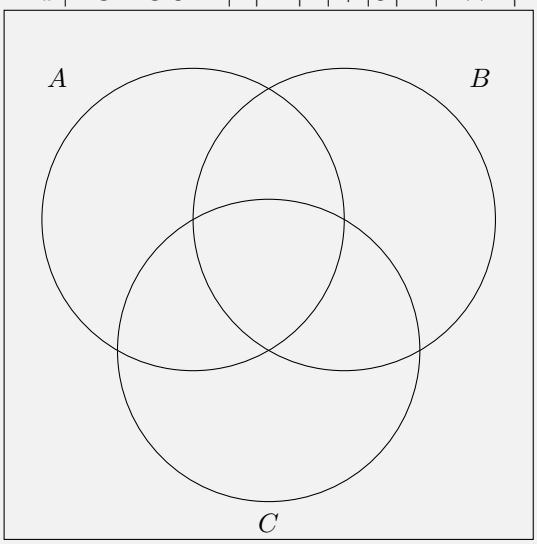
Proof. When we expand $(a+b)^n = (a+b)(a+b)\dots(a+b)$, we obtain terms of the form $a^k b^{n-k}$ $(0 \le k \le n)$
# of terms $a^k b^{n-k} = \binom{n}{k}$ (must specify k brackets where we use the 'a').
So $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{n-k} a^k b^{n-k}$ □

e.g. $(1+x)^n = 1 + nx + \frac{n(n-1)}{2}x^2 + \binom{n}{3}x^3 + \dots + nx^{n-1} + x^n$
So, for x small, a good approximation to $(1+x)^n$ is $1+nx$ (e.g. $1.00001^8 \sim 1.0008$),
And a better approximation is $1 + nx + \frac{n(n-1)}{2}x^2$

What can we say about relationships between sizes of unions and intersections (of finite sets)?
For example, $|A \cup B| = |A| + |B| - |A \cap B|$ (subtract as counted twice)



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



Theorem 3.4 (Inclusion-Exclusion Theorem)**.** Let $S_1, \ldots, S_n$ be finite sets.
Then $|S_1 \cup \cdots \cup S_n| = \sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \sum_{|A|=3} |S_A| - \cdots + (-1)^{n+1} \sum_{|A|=n} |S_A|$
Where $S_A = \bigcap_{i \in A} S_i$ and '$\sum_{|A|=k}$|' is taken over all $A \subseteq \{1, 2, \ldots, n\}$ of size k.

Proof. Let $x \in$ LHS. Say $x \in S_i$ for k of the S_i.

Claim. x counted once on RHS

Proof. $\#A, |A| = 1$, with $x \in S_A = k$
$\#A, |A| = 2$, with $x \in S_A = \binom{k}{2}$ (must choose 2 of the i with $x \in S_i$
In general, $\#A, |A| = r$, with $x \in S_A = \binom{k}{r}$
So # times x counted on RHS $= k - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k+1}\binom{k}{k}$
But $(1 + (-1))^k = 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} - \cdots + (-1)^k\binom{k}{k}$ (Binomial thm),
So # times x counted on RHS $= 1 - (1 + (-1))^k) = 1\,(k \geq 1)$✓□

3.7 Functions

Definition. For sets A and B, a **function** from A to B is a rule that assigns, to each $x \in A$, a unique point $f(x) \in B$.
More precisely, a **function** from A to B is a set $f \subseteq A \times B$ s.t. $\forall x \in A \, \exists$ unique $y \in B$ with $(x, y) \in f$.
(If $(x, y) \in f$, can write $f(x) = y$)

3.7.1 Examples

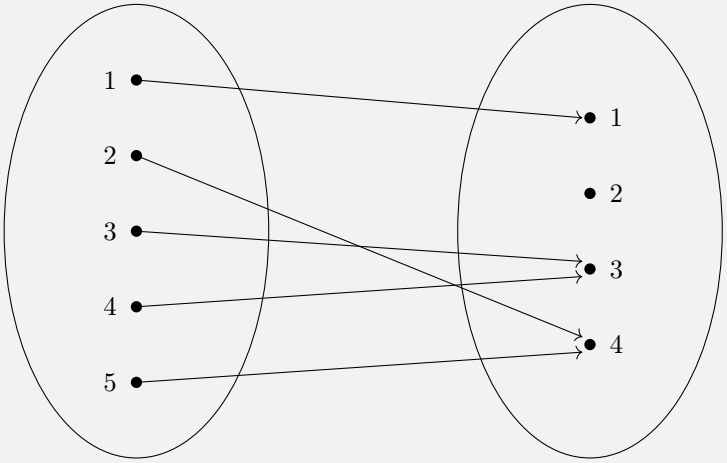
(i) The function $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$.
Can say: the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$
or: the function $f : \mathbb{R} \to \mathbb{R}$ $x \mapsto x^2$

(ii) NOT $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{1}{x}$ as $f(0)$ undefined

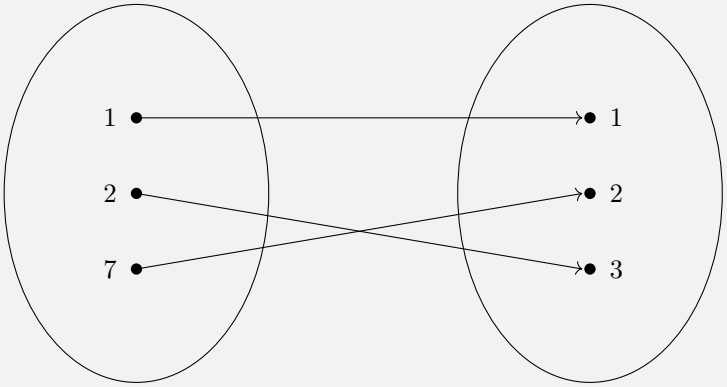
(iii) NOT $f(x) = \pm\sqrt{|x|}$ as $f(2) = \sqrt{2}$ and $-\sqrt{2}$

(iv) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \begin{cases} 1, & \text{if } x \text{ rational,} \\ 0, & \text{if } x \text{ not} \end{cases}$

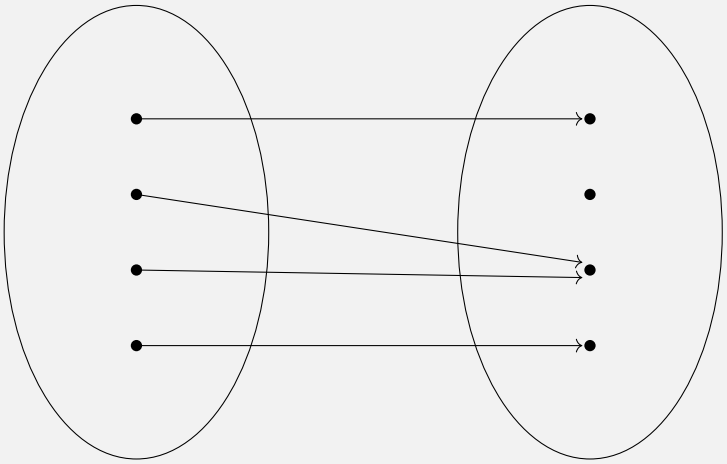
(v) $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 3, 4\}$ and $f : A \to B$ given by:



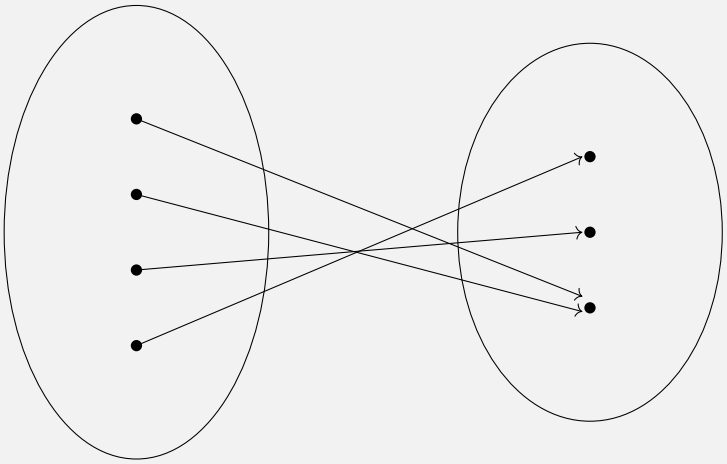
(vi)



(vii)



(viii)



Definition. Say $f : A \to B$ **injective** if $\forall a, a' \in A : a \neq a' \implies f(a) \neq f(a')$
Equivalently, $f(a) = f(a') \implies a = a'$.

e.g.

Function	Injective?
5	x since $f(2) = f(5)$
6	✓
7	x
8	x

Definition. Say $f : A \to B$ **surjective** if $\forall b \in B \, \exists a \in A$ s.t. $f(a) = b$.
"Everything in B is hit."

e.g.

Function	Surjective?
5	x since no $a \in A$ has $f(a) = f(2)$
6	✓
7	x
8	✓

Definition. Say $f : A \to B$ **bijective** if f injective and surjective.
"Everything hit exactly once" or "f pairs up A and B"

e.g.
6 above, or $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$.

Definition. For $f : A \to B$, A is the **domain** and B is the **range**.
The **image** of f is $\{f(a) : a \in A\} = \{b \in B : f(a) = b, \text{ some } a \in A\}$. ('Everything that is hit')

For $f : \mathbb{R} \to \mathbb{R}$, image of f is $\{y \in \mathbb{R} : y \geq 0\}$

Warning. When specifying a function, must say what domain, range are
e.g. "is the function $f(x) = x^2$ injective?" (meaningless)
For example, $f : \mathbb{N} \to \mathbb{N}$ given by $x \mapsto x^2$ is but $g : \mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto x^2$ isn't.

For A, B finite:
(i) No surjection $A \to B$ if $|B| > |A|$
(ii) No injection $A \to B$ if $|A| > |B|$
(iii) For $f : A \to A$, f injective $\implies$ f surjective (and vice versa).
(iv) No bijection from A to any proper subset of A.

But for infinite sets:
(i) Define $f_0 : \mathbb{N} \to \mathbb{N}$ given by $x \mapsto x + 1$ then f_0 injective but not surjective.
(ii) Define $f_1 : \mathbb{N} \to \mathbb{N}$ given by $x \mapsto \begin{cases} x - 1, & \text{if } x \neq 1, \\ 1, & \text{if } x = 1 \end{cases}$ then f_1 surjective but not injective.
(iii) Define $f_0 : \mathbb{N} \to \mathbb{N}\backslash\{1\}$ given by $x \mapsto x + 1$ then g a bijection from $\mathbb{N}$ to a proper subset of $\mathbb{N}$.

3.7.2 More Examples of Functions

(i) For any set X, have $1_X : X \to X$ given by $x \mapsto x$, the identity function on X.
(ii) For any set X, and $A \subseteq X$, have indicator function or characteristic function $\chi_A : X \to \{0,1\}$ given by $x \mapsto \begin{cases} 1, & \text{if } x \in A, \\ 0, & \text{if } x \notin A \end{cases}$

And some we have met before:
(iii) A sequence $x_1, x_2, \ldots$ of reals is a function $\mathbb{N} \to \mathbb{R}$, $n \mapsto x_n$.
(iv) The operation $+$ on $\mathbb{N}$ is a function $\mathbb{N}^2 \to \mathbb{N}$, $(a,b) \mapsto a+b$
(v) A set X has size $n \iff \exists$ bijection $\{1,2,3,\ldots,n\} \to X$, $i \mapsto a_i$ $(X = \{a_1, \ldots, a_n\})$

3.7.3 Composition of Functions

Definition. Given $f : A \to B$ and $g : B \to C$, the **composition** $g \circ f : A \to C$ is defined by $(g \circ f)(a) = g(f(a))$, $a \in A$

e.g. if $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x$ and $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x+1$.
Then $(f \circ g)(x) = f(g(x)) = f(x+1) = 2(x+1)$
And $(g \circ f)(x) = g(f(x)) = g(2x) = 2x+1$
So, in general $\circ$ not commutative - in our example, $f \circ g \neq g \circ f$
(e.g. since $(f \circ g)(1) \neq (g \circ f)(1)$)

However, $\circ$ is associative: given $f : A \to B$, $g : B \to C$, $h : C \to D$, have $h \circ (g \circ f) = (h \circ g) \circ f$.
Indeed, for any $x \in A$:
$(h \circ (g \circ f))(x) = h((g \circ f(x))) = h(g(f(x)))$
$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$
Thus $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)\, \forall x \in A$, so $h \circ (g \circ f) = (h \circ g) \circ f$

Definition. Say $f : A \to B$ is **invertible** if $\exists g : B \to A$ s.t. $g \circ f = 1_A$ and $f \circ g = 1_B$.

e.g. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x+1$ and $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto \frac{x-1}{2}$:
$g \circ f : \forall x \in \mathbb{R} : (g \circ f)(x) = g(f(x)) = g(2x+1) = x$ so $g \circ f = 1_{\mathbb{R}}$✓
$f \circ g : \forall x \in \mathbb{R} : (f \circ g)(x) = f(g(x)) = f(2x+1) = x$ so $f \circ g = 1_{\mathbb{R}}$✓
So f invertible ("with inverse g")

Warning. For f_0, f_1 from above: $f_0 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x+1$. $f_1 : \mathbb{N} \to \mathbb{N}$, $x \mapsto \begin{cases} x-1, & \text{if } x \neq 1, \\ 1, & \text{if } x = 1 \end{cases}$
Have $f_1 \circ f_0 = 1_{\mathbb{N}}$ but $f_0 \circ f_1 \neq 1_{\mathbb{N}}$ as $f_0(f_1(1)) \neq 1$.

Claim. $f : A \to B$ invertible $\iff$ f bijective.

Proof. $\implies$: say g inverse to f. surj: $\forall b \in B, b = f(g(b))$✓
inj: $\forall a, a' \in A : f(a) = f(a') \implies gf(a) = gf(a') \implies a = a'$✓✓

$\impliedby$: Let $g(b) =$ the unique $a \in A$ with $f(a) = b$, each $b \in B$ ✓

3.8 Equivalence Relation

Definition. A **relation** on a set X is a subset R of $X \times X$. Usually write aRb for $a, b \in R$.

e.g.
(i) on $\mathbb{N}$, aRb if $a \equiv b\,(5)$
(ii) on $\mathbb{N}$, aRb if $a|b$
(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 $a, b > 6$
Some properties a relation might have:

Definition. R **refexive** if $\forall x \in X : xRx$

(i) ✓is since $x \equiv x\,(5)\,\forall x \in \mathbb{N}$
(ii) ✓
(iii) x
(iv) x
(v) ✓
(vi) ✓

Definition. R **symmetric** if $\forall x, y \in X : xRy \implies yRx$

(i) ✓
(ii) x
(iii) ✓(since $a \neq b \implies b \neq a$)
(iv) ✓
(v) ✓
(vi) ✓

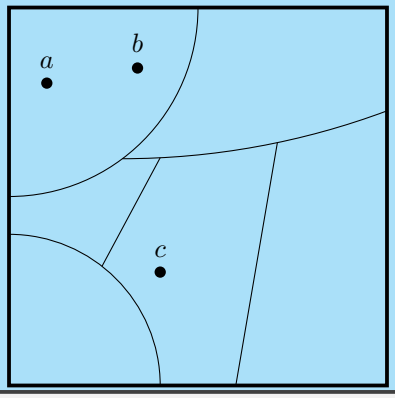
Definition. R **transitive** if $\forall x, y, z \in X : xRy, yRz \implies xRz$

e.g.
(i) ✓
(ii) ✓
(iii) x
(iv) x
(v) x
(vi) ✓

Definition. R is an **equivalence relation** if it is reflexive, symmetric and transitive.

e.g. 1 & 6 above. Also, on $\mathbb{N}$ xRy if $x = y$

Definition. $\{C_i : i \in I\}$ is a **partition** of a set X if each C_i non-empty, and they are (pairwise) disjoint and $\bigcup_{i \in I} C_i = X$



Then aRb if $\exists i$ s.t. $a, b \in C_i$ is an equivalence relation on X.
Aim: All equivalence relations are of this form.

Definition. For an equivalence relation R on a set X, and $x \in X$, the **equivalence class** of x is: $[x] = \{y \in X : yRx\}$, same as $\{y \in X : xRy\}$

e.g. in example 1, $[2] = \{y \in \mathbb{N} : y \equiv 2\,(5)\}$, so $[2] = [7]$ so all the equivalence classes are (5 of them):

All $x \equiv 0$
All $x \equiv 1$
All $x \equiv 2$
All $x \equiv 3$
All $x \equiv 4$

Prop 3.5. Let R be an equivalence relation on a set X. Then the equivalence classes of R partition X.

Proof. Each $[x]$ non-empty ($x \in [x]$),
And $\bigcup_{x \in X} [x] = X$ ($x \in X\, \forall x \in [x]$)
So just need to show that equivalence classes disjoint (or equal).
Given x, y with $[x] \cap [y] \neq \varnothing$, need $[x] = [y]$:
Have $z \in [x] \cap [y]$, some z.
So zRx, zRy whence xRy.
thus $\forall t$, $tRx \implies tRy$ (transitivity).
$\forall t$, $tRx \implies tRy$ (transitivity).
So $[x] = [y]$ ✓□
[Example: is there an equivalence relation on $\mathbb{N}$ with 3 equiv classes: 2 of size ∞, 1 finite?]

Definition. Given equivalence relation R ona set X, the **quotient** of x by R is $X/R = \{[x] : x \in X\}$ ("the set of countries")

e.g. in example 1, X/R has size 5.

Definition. The map $q : X \to X/R$, $x \mapsto [x]$, is the **quotient map** or the **projection map**.

Another example on $\mathbb{Z} \times \mathbb{N}$, define $(a, b)R(c, d)$ if $ad = bc$.
Easy to check this is an equivalence relation.
e.g. $[(1, 2)] = \{(1, 2), (2, 4), (3, 6) \dots\}$
So could regard $\mathbb{Z} \times \mathbb{N}/R$ as a copy of $\mathbb{Q}$. $[(a, b)] \leftrightarrow \frac{a}{b}$
Thus $q : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{N}/R$ would map (a, b) to $\frac{a}{b}$.

4 Countability

Remark. Looking at 'sizes' of infinite sets e.g. $\mathbb{N}$ 'looks smaller' than $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Definition. Say a set X is **countable** if X finite or bijects with $\mathbb{N}$ ($\exists$ bijection $f : \mathbb{N} \to X$.
Equivalently, X countable $\iff$ can list X as $a_1, a_2, a_3, \dots$ (might terminate)

(i) Any finite set
(ii) $\mathbb{N}$
(iii) $\mathbb{Z}$

Can list $\mathbb{Z}$ as $0, 1, -1, 2, -2, 3, -3, \dots$

i.e. $\mathbb{Z}$ is listed as $a_1, a_2, a_3, \dots$, where $a_n = \begin{cases} \frac{n}{2} & \text{if } n \text{ even} \\ -\frac{n-1}{2} & \text{if } n \text{ odd} \end{cases}$

So '$\mathbb{Z}$ is same size as $\mathbb{N}$' (they biject)
Are all sets countable?

Prop 4.1. A set X is countable $\iff$ $\exists$ injection $f : X \to \mathbb{N}$

Proof. $\implies$: ✓(If X finite then X injects into $\mathbb{N}$, and if X bijects with $\mathbb{N}$ then certainly X injects into $\mathbb{N}$)

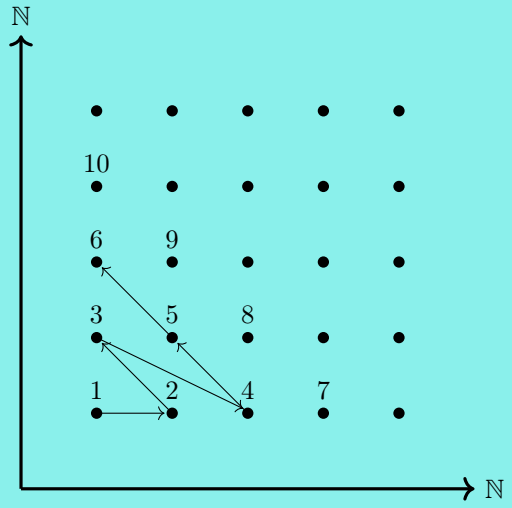
$\impliedby$: May assume X infinite (X finite $\implies$ X countable)
Have X bijects with its image $f(X)$ ($\{f(x) : x \in X\}$ under f),
So enough to show $f(X)$ countable.
Set: $a_1 = \min f(X)$ and $a_2 = \min f(X) \backslash \{a_1\}$
and in general $a_n = \min(f(X) \backslash \{a_1, a_2, \dots, a_{n-1}\})$
Then $f(X) = \{a_1, a_2, a_3, \dots\}$ - each $a \in f(X)$ is a_n, some n, because $a = a_n$, some $n \leq a$ so $f(X)$ countable ✓□
Thus can view countable as 'at most as large as $\mathbb{N}$'
e.g. any subset of a countable set is countable.

Warning. In $\mathbb{R}$, let $X = \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\} \cup \{1\}$
Then X countable as can list as $1, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots$
But if we counted by 'least element' etc. (as in proof of prop 1)
Then:

$$b_1 = 1/2$$
$$b_2 = 2/3$$
$$b_3 = 3/4$$
$$\vdots$$

So 1 would not be on our list!

Theorem 4.2. $\mathbb{N} \times \mathbb{N}$ is countable.



Proof. Define $a_1 = (1, 1)$,
and a_n inductively by writing $a_{n-1} = (p, q) : a_n = \begin{cases} (p-1, q+1) & \text{if } p \neq 1 \\ (1, p+q) & \text{if } p = 1 \end{cases}$
This does hit every point $(x + y) \in \mathbb{N} \times \mathbb{N}$ (e.g. induction on $x + y$), so have listed $\mathbb{N} \times \mathbb{N}$. $\square$

Proof. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$(x, y) \mapsto 2^x 3^y$.
Then f injective. $\square$

The same proof shows:

Theorem 4.2 (More general)**.** Let $A_1, A_2, A_3, \ldots$ be countable sets. Then $\bigcup_{n \in \mathbb{N}} A_n = A_1 \cup A_2 \cup A_3 \cup \ldots$ is countable.
"A countable union of countable sets is countable"

Proof. For each i, have:
A_i countable,
So can list A_i as $a_{i1}, a_{i2}, a_{i3}, \ldots$ (might terminate)
Define $f : \bigcup_{n \in \mathbb{N}} A_n \to \mathbb{N}$
$x \mapsto 2^i 3^j$ where $x = a_{ij}$, least such i.
Then f injective. $\square$

Example. (i) $\mathbb{Q}$ is countable: $\mathbb{Q} = \mathbb{Z} \cup \frac{1}{2}\mathbb{Z} \cup \frac{1}{3}\mathbb{Z} \cup \ldots$,
and each $\frac{1}{n}\mathbb{Z}$ countable (bijects with $\mathbb{Z}$), so $\mathbb{Q}$ countable by Theorem 2.

(ii) The set $\mathbb{A}$ of algebraic numbers is countable.
Indeed enough to show the set of all integer polynomials is countable (as then $\mathbb{A}$ is a countable union of finite sets (using Theorem 2).
Thus enough to show that, for each d, the set of all integer polys of d is countable (again using Theorem 2).
But this set injects onto $\mathbb{Z}^{d+1}$ $(a_d X^d + \cdots + a_1 X + a_0) \mapsto (a_d, \ldots, a_1, a_0))$,
And $\mathbb{Z}^n$ countable $\forall n$ ($\mathbb{Z} \times \mathbb{Z}$ countable by Theorem 2, so $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}$ countable by Theorem 2, etc.) ✓

Definition. A set X is **uncountable** if it is not countable.

Theorem 4.3. $\mathbb{R}$ is uncountable.

Proof. We'll show $(0, 1)$ uncountable.
Given $r_1, r_2, \ldots$ in $(0, 1)$, our task: find $s \in (0, 1)$ not on that list $(\forall n : S \neq r_n)$
For each r_n, have decimal expansion $r_n = 0.r_{n1}r_{n2}r_{n3}\ldots$

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

Define $s = 0.s_1s_2s_3\ldots$ by:

$$s_1 = \begin{cases} 5 & \text{if } r_{11} \neq 5 \\ 6 & \text{if } r_{11} = 5 \end{cases}$$

$$s_2 = \begin{cases} 5 & \text{if } r_{22} \neq 5 \\ 6 & \text{if } r_{22} = 5 \end{cases}$$

And in general $s_n = \begin{cases} 5 & \text{if } r_{nn} \neq 5 \\ 6 & \text{if } r_{nn} = 5 \end{cases}$

Then s not on our list ($s \neq r_n$ as they differ in decimal digit n.) □

Remarks.

(i) Called A diagonal argument, or Cantor's diagonal argument.

(ii) $\mathbb{R}$ is uncountable. $\mathbb{A}$ countable, so $\exists$ transcendental number.
Indeed, 'most' numbers are transcendental: $\mathbb{R}\backslash\mathbb{A}$ uncountable. (because: if $\mathbb{R}\backslash\mathbb{A}$ countable then $\mathbb{R} = \mathbb{A} \cup \mathbb{R}\backslash\mathbb{A}$ would be countable ※).

Another uncountable set

Theorem 4.4. $\mathbb{P}(\mathbb{N})$ is uncountable.

Proof.

To ensure $S \neq S_1$:
Take $1 \in S$ if $1 \notin S_1$,
$1 \notin S$ if $1 \in S_1$
To ensure $S \neq S_1$:
Take $2 \in S$ if $2 \notin S_1$,
$2 \notin S$ if $2 \in S_1$
$\vdots$

Suppose $\mathbb{N}$ listed as $S_1, S_2, S_3, \ldots$
Let $S = \{n \in \mathbb{N} : n \notin S_n\}$
Then S not on our list,
Since $\forall n : S \neq S_n$ (S, S_n differ at element n). ※□

Remarks.

(i) This is a diagonal argument - really the same as our proof that $\mathbb{R}$ uncountable.
(ii) Alternatively, just inject $(0,1)$ into $\mathbb{P}(\mathbb{N})$:
Given $x \in (0,1)$, write x in binary as $0.x_1x_2x_3\ldots$ (not ending with all-1s) and put $f(x) = \{n : x_n = 1\}$
$(0.111000000\cdots \leftrightarrow \{1,2,3\})$
$(0.10101010\cdots \leftrightarrow$ set of odds)

In fact, our proof of theorem 4 shows:

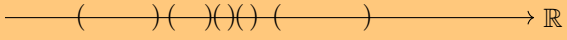
Theorem 4.5. For any set X: there is no bijection(in fact, no surjection) from X to $\mathbb{P}(X)$
e.g. $\mathbb{P}(\mathbb{R})$ does not biject with $\mathbb{R}$

Proof. Given any function $f : X \to \mathbb{P}(X)$, we'll show f not surjective.
Let $S = \{x \in X : x \notin f(x)\}$.
Then S does not belong to the image of f, since $\forall x$ have $S \neq f(x)$ ($S, f(x)$ differ at element x).□

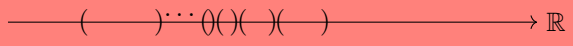
Remarks.

(i) similar to Russell's Paradox.
(ii) Gives another proof that there is no universal set V - as then would have $\mathbb{P}(V) \subseteq V$, whence certainly V would surject to $\mathbb{P}(v)$

Claim. Let $A_i : i \in I$ be a family of open intervals, pairwise disjoint
This family is countable.



Warning. No 'next interval'



Proof (1^{st})**.** Each A_i contains a rational,
And $\mathbb{Q}$ countable,
So the family is countable. ✓

Proof (2^{nd})**.** $\{i \in I : A_i \text{ has length } \geq 1\}$ countable (injects into $\mathbb{Z}$)
$\{i \in I : A_i \text{ has length } \geq \frac{1}{2}\}$ countable (injects into $\mathbb{Z}$)
and $\forall n : \{i \in I : A_i \text{ has length } \geq \frac{1}{n}\}$ countable (injects into $\mathbb{Z}$)
So done - countable union of countable sets. ✓

Moral. To show X uncountable:
(i) Run diagonal argument on X
(ii) Inject favourite uncountable set into X
To show X countable:
(i) List it (usually fiddly)
(ii) Inject into $\mathbb{N}$
(iii) Use 'countable union of countable sets is countable' (usually best)
(iv) If in/ near $\mathbb{R}$, consider $\mathbb{Q}$

Intuitively, think of 'A bijects with B' as saying that A and B "have the same size".
And 'A injects into B' as saying that "A is at most as large as B"
And A 'surjects to B' as saying that "A is at least as large as B" (for $B \neq \varnothing$)

For these to make sense, we'd want that (for $A, B \neq \varnothing$):

Claim. $\exists$ injection $f : A \to B \iff \exists$ surjection $g : B \to A$.

Proof. $\implies$: fix $a_0 \in A$.
Define $g : B \to A$, $b \mapsto \begin{cases} \text{The unique } a \in A \text{ with } f(a) = b, \text{ if it exists} \\ a_0 \text{ if not} \end{cases}$
Then g surjective.

$\impliedby$: For each $a \in A$, have some $a' \in B$ with $g(a') = a$ (as g surjective)
Let $f(a) = a'$, each $a \in A$.
Then f injective. ✓

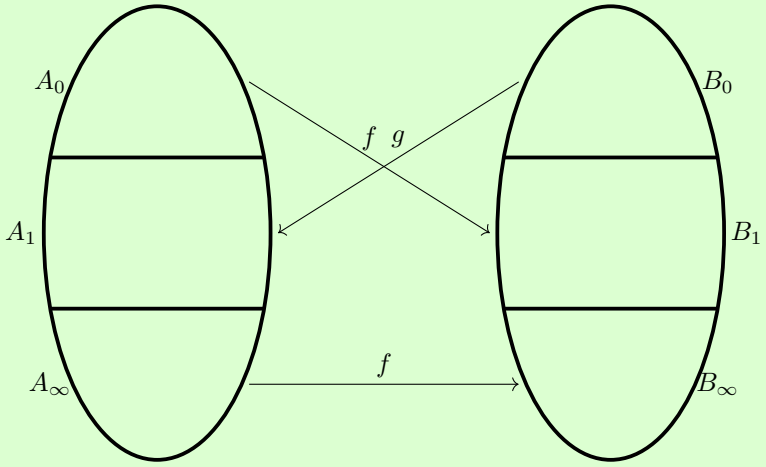
We would also need that if "A is at most as large as B" and "B is at most as large as A" then A and B "have the same size".

Theorem 4.6 (Schröder-Bernstein)**.** If $f : A \to B$ and $g : B \to A$ are injections then $\exists$ bijection $h : A \to B$.

Proof. For $a \in A$, write $g^{-1}(a)$ for the $b \in B$ (if it exists) such that $g(b) = a$.
Similarly for $f^{-1}(b)$, where $b \in B$.
The ancestor sequence of $a \in A$ is:
$g^{-1}(a), f^{-1}(g^{-1}(a)), g^{-1}(f^{-1}(g^{-1}(a))), \ldots$ (may terminate)
Similarly fro $b \in B$:
Let:

$$A_0 = \{a \in A : \text{ ancestor sequence stops at even time (i.e. stops in } A)\}$$
$$A_1 = \{a \in A : \text{ ancestor sequence stops at odd time (i.e. stops in } B)\}$$
$$A_\infty = \{a \in A : \text{ ancestor sequence does not stop}\}$$

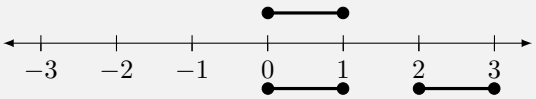
(0 is even: so if $a \in A$ has no $g^{-1}(a)$, then $a \in A_0$)
Similarly for B_0, B_1, B_∞



Then f bijects A_0 with B_1 (noting that every $b \in B$, is $f(a)$, some $a \in A_0$).
And similarly g bijects B_0 with A_1.
And f (or g) bijects A_∞ with B_∞.

So the function $h : A \to B$, $a \mapsto \begin{cases} f(a) & \text{if } a \in A_0 \\ g^{-1}(a) & \text{if } a \in A_1 \\ f(a) & \text{if } a \in A_\infty \end{cases}$ is a bijection. $\square$

Example:
Do $[0, 1]$ and $[0, 1] \cup [2, 3]$ biject?



Have injection $f : [0, 1] \to [0, 1] \cup [2, 3]$ e.g. $f(x) = x$
and have injection $f : [0, 1] \cup [2, 3] \to [0, 1]$ e.g. $f(x) = \frac{x}{3}$
So by Schröder-Bernstein they biject.

Would also be nice to have that, for any sets A and B, either A injects into B or B injects into A. This is true, but harder - see part II 'Set Theory and Logic'.

Have $\mathbb{N}, \mathbb{P}(\mathbb{N}), \mathbb{PP}(\mathbb{N}), \ldots$: does every X inject into one of those?
No, e.g. $\mathbb{N} \cup \mathbb{P}(\mathbb{N}) \cup \mathbb{PP}(\mathbb{N}) \cup \ldots$
Then $X' = X \cup \mathbb{P}(X) \cup \mathbb{PP}(X) \cup \ldots$
Then $X'' = X' \cup \mathbb{P}(X') \cup \mathbb{PP}(X') \cup \ldots$
And so on.
Then $Y = X \cup X' \cup X'' \cup X''' \cup \ldots$
"and can keep going"